ARKA KAPI

www.arkakapidergi.com

2 Aylık Siber Güvenlik Dergisi • 10 TL • 2. SAYI
Nisan-Mayıs 2018

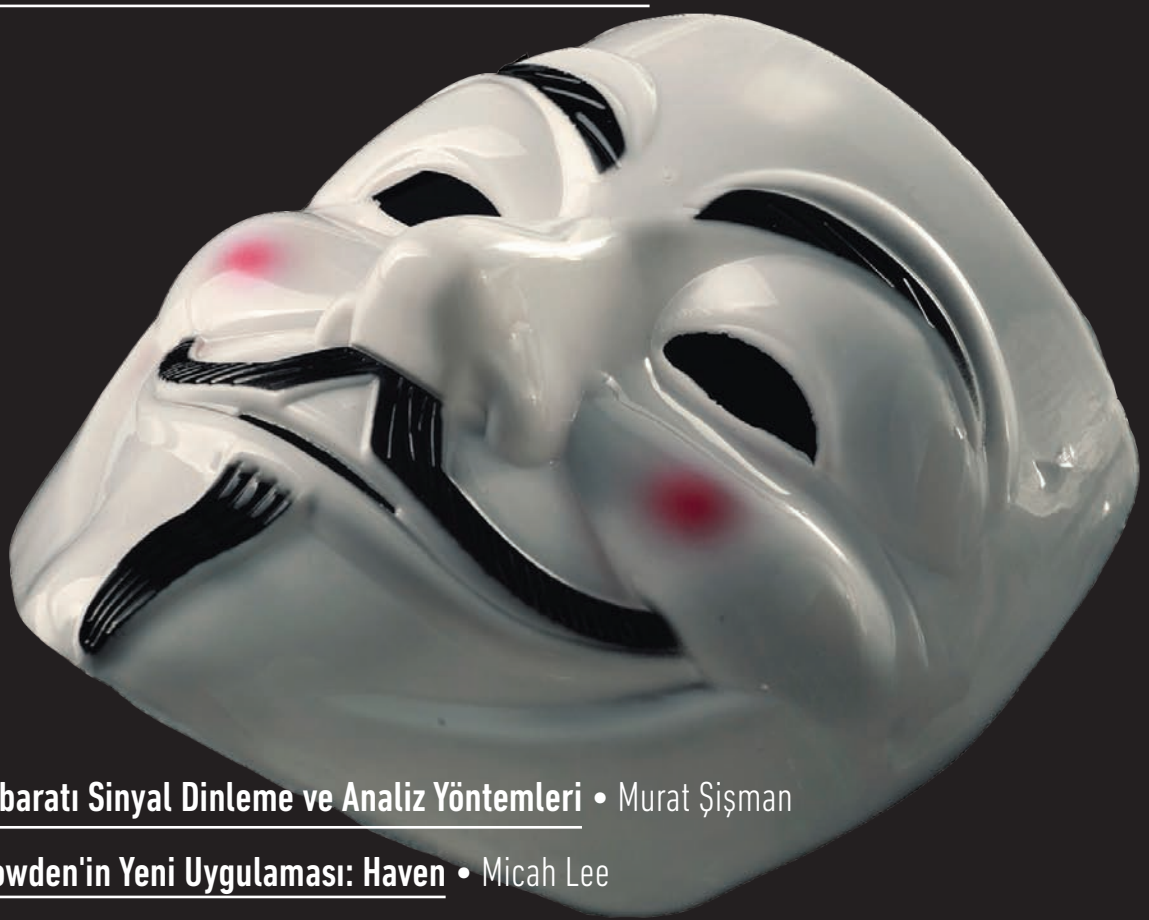
Internette Gizli Kalın: TOR (The Onion Router) • Mehmet Enes Özen

HTS, CGNAT, METADATA ve ByLock • Koray Peksayar (Röportaj: Şahin Solmaz)

Saman Altından Okyanus Yürütmek DNS Tünelleme ile Engelleri Aşın • Arka Kapı Dergi

Veri Gizleme Sanatı: STEGANOGRAFİ • Huriye Özdemir

GPS Olmadan Kullanıcıları İzlemenin Farklı Bir Yolu: PinMe • Recep Kızılarslan



Sinyal İstihbaratı Sinyal Dinleme ve Analiz Yöntemleri • Murat Şişman

Edward Snowden'in Yeni Uygulaması: Haven • Micah Lee

Meltdown Bilgisayarın Yapısı ve Tarihi • Chris Stephenson

Kral Çıplak Diyebilmek: Blokzincirinin Kısıtları • Mert Susur

Derinlemesine Ethereum • Musa Baş

ISSN 2618-6373 02
9 772618 637008

ARKA KAPI DERGİ ABONELİK

YILLIK DİJİTAL ABONELİK 40 TL
YILLIK BASILI DERGİ ABONELİK 75 TL

abone@arkakapidergi.com / www.abakuskitap.com

EDİTÖRDEN

Arka Kapı Dergi'nin ikinci sayısından herkese merhaba! Bu sayımızın teması Anonymity (Anonimlik).

Kişisel bilgilerin nelere mal olabileceği, sıradan gibi görünen küçük verilerin nasıl toplumsal manipülasyonlara varan vakalara yol açabileceğini Cambridge Analytica firmasının adı ile özdeşleşen hadiseden açıkça gözlemledik. Anonimlik, tüm hayatın dijitalleştiği dünyada diyebiliriz ki en önemli insani taleplerden biri.

Benim saklayabilecek bir şeyim yok diyenler, aşağıda bulunan e-posta adresime, parolalarını gönderebilirler mi lütfen?

Yahut bugün tümden engellenmesi söz konusu olan VPN hizmetleri! VPN, sadece yasaklı sitelere erişimin değil, hizmet sınırları dünya hinterlandına yayılmış şirket ve iş modellerinin yerel kaynaklarına erişebilmek için kullandıkları güvenli bir bağlantı protokolü. Evet her şey gibi VPN'i de suçlular kullanıyor! Tıpkı suçluların otoyolları, yaya geçitlerini, telefon hatlarını kullandıkları gibi kriminal aktivitelerde bulunan insanlar VPN'i de kullanıyorlar. Ama nasıl bu suçluların diğer başka şeylerden istifade etmeleri, bu vasıtaların toplumsal hayattan men edilmesinin akl-ı selim bir çözümü olarak görülmüyorsa, niçin aynı şeyi VPN için de düşünmüyoruz? Aynı itirazı VPN için de yükseltemiyoruz?

Keza sansür meselesi! İnternet sahip olduğu zenginlikler sayesinde bizi zengin kılan bir teknoloji. Bu zenginlikleri engellemek hangi saik ile olursa olsun kullandığımız zemini çoraklaştıracak bir hamledir. Elinizde TV kumandası varsa, bir TV programından şikayet etme hakkınız yok. Faaliyetleri aşikar olan sitelere girip girmemek kullanıcının kendi tercihindedir. Elbette toplumsal yaşantıyı felce uğratacak, nesillerin sağlıklı gelişimlerine zarar verebilecek yayınların varlığından gençleri, genç dimağları korumak zorundayız. Ama bu yasaklarla savuşturulabilecek bir hadise değil, bireysel sorumluluğun ön plana çıktığı/çıkması gereken bir alan. Devletin, ya da siyasal erkin vatandaşları adına her şeye karar verdiği rejimler totaliter rejimlerdir. Ve bu yol bir kere açıldı mı, Orwell'ın 1984 distopyasına rahmet okutacak gelişmeler birbirini izler. Her siyasi erk kendince uygun bulduğunu dayatır, sevmediğini yasaklar. Gelin buna dur diyelim! Modern insan, tercih edebilen insandır.

İlk sayımızın yayınından hemen sonra 17 Şubat tarihinde Çırak Atölye'de gerçekleşen bir etkinlikte buluşarak dergimizin ilk sayısını dostlarımız ile kutladık. Tahmin edeceğiniz gibi kahve bahane idi!

Chris Hoca, Abaküs Yayınları'nın sahibi Cevahir Ağabey'den sonra birkaç kelam etmek üzere söz bendenize verildi. Öylesine heyecanlıydım ki isim isim çalışmamıza omuz veren arkadaşlarımızı sayarken fahiş bir hata yaptım!

Bazı insanlar vardır, öylesine hayatınızdadırlar ki, varlıklarının sağlamasını dahi yapmanıza gerek kalmaz. Hep oradadırlar. Hep desteklerini hissedersiniz. Sanki hiç gitmeyecek gibidirler. Hayatımdaki böyle dostlardan biri, varlığı ve desteği benim için tekrarına hacet olmayacak kadar tabii olan dostlarımdan biri, Bayram Gök. Dergimize kriptoloji yazıları ile renk katan bir dostumuz. O heyecanla, benim için hayattaki de-factolardan biri olan Bayram Ağabey'in adını zikretmeyi ihmal etmişim. İşte sebebi budur. Hem kendisi teşekkür beklemeyecek kadar kalenderdir, hem de hayatımızdaki rolü teşekkürü bile unutturacak kadar tabii ve içten.

Hayatımda bana bu duyguyu tattıran ilk insan ise Annem! İlk sayıyı hazırladığımız esnada yoğun bakımda olan anneciğimi maalesef 22 Şubat tarihinde ebediyete uğurladık. Rahmet-i rahmana kavuştu. Dilerim kabri pür nur, mekânı cennet olsun. Hakk, bendenizi de yarattıklarına hizmetle ve hürmetle anneciğimin kapanmayan amel defteri için bir vasıta kılsın.

Bir teknoloji dergisi için çok duygusal satırlar. Af buyurun!

Takdir edersiniz ki hayat sayılardan ve vesilelerden öte...

Ziyahan Albeniz
editor@arkakapidergi.com

KÜNYE

YIL: 1 Sayı: 2 - ISSN: 2618-6373 - www.arkakapidergi.com
2 ayda bir yayımlanır.

Abaküs Kitap Yayın Dağıtım Hizmetleri adına sahibi: Selda Ustabaş Demiryakan

Merkez: Hobyar Mah. Cemal Nadir Sok. No:24/178 Cağaloğlu - İST. Tel: 0212 514 68 61

Genel Yayın Yönetmeni: Cevahir Demiryakan - cevahir@cirakdergi.com

Sorumlu Yazı İşleri Müdürü: Ziyahan Albeniz - ziyahan@arkakapidergi.com

Grafik Tasarım: Cem Demirezen - grafik@abakuskitap.com

Düzelti: Huriye Özdemir

Dış Haber: İrem Aşkan - Oğuz Aydınyılmaz

Yayın Koordinatörü: Şahin Solmaz

Hukuk Müşaviri: Avukat Mehmet Pehlivan - Pehlivan İlkakın Hukuk Bürosu

Sosyal Medya: Oğuz Aydınyılmaz - Recep Kızılarslan

Web: www.arkakapidergi.com

Twitter.com/arkakapidergi

abone@arkakapidergi.com

editor@arkakapidergi.com

etkinlik@arkakapidergi.com

Baskı: Ezgi Matbaacılık San. Tic. Ltd. Şti. Sanayi Cad. Altay Sok. No:14 Çobançeşme-Yenibosna/İSTANBUL Tel: 0212 452 23 02 Matbaa Sertifika No: 12142

İÇİNDEKİLER

Haberler 3
Siber Takvim 6
GPS Olmadan Kullanıcıları İzlemenin Farklı Bir Yolu 7
PinMe - Recep Kızılarslan 7
BitLocker ile Disklerinizi Şifreleyin - Arka Kapı 9
Internette Gizli Kalın: The Onion Router - Mehmet Enes Özen 13
Haven - Micah Lee 20
Veri Gizleme Sanatı: STEGANOGRAFİ - Huriye Özdemir 23
Saman Altından Okyanus Yürütmek DNS Tünelleme ile Engelleri Aşın - Arka Kapı 30
KEVIN MITNICK'TEN BYLOCK'A KADAR HTS, CGNAT, METADATA ve DAHA FAZLASI!
Koray Peksayar - Röportaj: Şahin Solmaz 36
Mühür Kimdeyse Süleyman O'dur: Kullanıcı Sözleşmeleri - Av. Mehmet Pehlivan 41
Kriptoloji'nin Altın Çağı - Bayram Gök 47
Kral Çıplak Diyebilmek: Blokzincirinin Kısıtları - Mert Susur 52
Derinlemesine Ethereum - Musa Baş 55
Blockchain Tabanlı Telif Hakları Projeleri - Mihraç Cerrahoğlu 57
Meltdown Bilgisayarın Yapısı ve Tarihi - Chris Stephenson 59
Sinyal İstihbaratı Sinyal Dinleme ve Analiz Yöntemleri - Murat Şişman 67
Google'a Ortak Olmak: Google AdSense Gelirinizi Bine Katlayın! - Sönmez Ertem 73
Hacker Palas Bir Hacking Hikâyesi - Yusuf Yaltırık 77
Projman'ın Kaleminden TR Scene ve TCG Dergileri'nin Hikâyesi - Projman 79
Esir Yeni Dünya Bugünün Hikâyesi - Çağatay Çalı 82
Ubuntu Kurulumu ve Meraklısına Notlar - Erhan Altındaş 85
Siber Güvenlik Sektörü Hacktrick '18 ile BTK'da Buluşuyor! 92
Nedir Bu Amatör Telsizcilik Dedikleri? - TA1IHE Murat KAYGISIZ 93
KUANTUM BİLGİSAYAR- Esra Serttaş 95

Haberler

{SİBERBÜLTEN
siber güvenliğin türkçe hafızası

Türkiye Zeytin Dalı harekatını siber alana mı taşıdı?

Türkiye'nin komşu Suriye'nin kuzeyindeki terör örgütü YPG'ye yönelik askeri operasyonları sürerken operasyonun siber alanda bazı yansımaları olduğu iddia edildi.

Kanada merkezli Citizen Lab, Türk Telekom ağında Derin Paket İncelemesinde (Deep Packet Inspection) kullanılan middlebox (önceden belirlenmiş kurallara göre yönlendirme uygulayan bir tür cihaz) bulunduğuna dair bir rapor yayınladı. Rapora göre, bu middlebox'lar ile Türkiye ve Suriye'deki yüzlerce internet kullanıcısı, zararsız Windows uygulamaları indirmeye çalıştıklarında devlet destekli bir casus yazılıma yönlendirildi. Türkiye'de 5 bölgede kullanıldığı öne sürülen yöntemle aynı zamanda Suriye'de bulunduğu halde Türk Telekom servislerini kullananların da etkilendiği raporda yer aldı. Sınırın diğer tarafına kadar uzanan Wi-Fi bağlantıları ile bazı durumlarda tek bir Türkiye IP'sinden 100'den fazla Suriye'de bulunan internet kullanıcısının casus yazılımdan etkilendiği ifade edildi.

Citizen Lab, açık kaynaklardan ulaştığı Wi-Fi router bilgilerine göre hedef alınan IP adreslerinden en az bir tanesinin YPG tarafından kullanıldığını tespit etti. Ocak ayında başlayan Zeytin Dalı operasyonu ile casus yazılımın yayılma yoğunluğunun kesişmesi iki olay arasında bağlantı olabileceği haberlerini gündeme getirdi. Casus yazılımdan sadece Afrin bölgesi değil, operasyonun dışında kalan İdlib'in kuzeyinin de etkilendiği gelen bilgiler arasında.

Amerikan AP haber ajansı, Türkiye'nin Suriye sınırındaki internet kullanıcılarını hacklemek için Kanadalı bir şirketin teknolojisinin kullanıldığı iddiasını gündeme taşıdı. Araştırmacıların tespitlerine dayandırılan iddiaya göre, bu siber saldırı ile Suriye'de YPG'yi destekleyen Kürtlerin hedef alınmış olabileceğine dair izler bulunuyor.

İddianın sahibi İnternet Gözlemci Grubu Citizen Lab'ın direktörü Ron Deibert'e göre, Kürt gruba yönelik siber saldırının Kanadalı bir şirketin teknolojisinin kullanılarak düzenlenmesi ironik. Bu şirketlerin sıkı bir şekilde denetlenmediğini söyleyen Deibert, "Bunun da dış politika çıkarlarımızı ve insan hakları kaygılarımıza zarar vermek gibi çeşitli sonuçları olabiliyor. Bu tür teknolojiler üzerinde devlet denetiminin artırılması çok önemli" şeklinde konuştu.

Citizen Lab, bu hacklemenin ardındaki donanımın Procera tarafından üretilen PacketLogic cihazları olduğunu ileri sürdü. Procera ise Kaliforniya-Fremont merkezli bir şirket ve kısa bir süre önce ABD'li özel bir aracı kurum olan Francisco Partners'in sahip olduğu Kanada merkezli Sandvine şirketine dahil oldu.

Raporun ortaya çıkmasından önce yayımlanan bir açıklamada Sandvine şirketi, suistimale yönelik bütün iddiaları araştırdıklarını ancak Citizen Lab'in elde ettiği bulguları kendilerine tam anlamıyla açıklamayı reddettiği için soruşturmayı tamamlayamadıklarını söylemişti.

Açıklamada ayrıca Citizen Lab'in iddialarının teknik olarak hatalı ve kasten yanıltıcı olduğu ifade edilmişti. Citizen Lab ise sözkonusu hacklemeyi Avrupalı bir siber güvenlik şirketinin kimliği belirlenemeyen iki ülkedeki ağ hizmet sağlayıcılarının, kullanıcılarını 'network injection' olarak bilinen güçlü bir hackleme tekniği ile tehlikeye sokmaya çalıştıklarını rapor etmesini ardından keşfettiklerini belirtti.

Citizen Lab casusluk izini bulmak için interneti taradığını ve sonunda izlerin Adana, Hatay, Gaziantep, Diyarbakır ve Ankara gibi Suriye'nin kuzeyi ve Mısır'a kadar uzandığını fark ettiklerini açıkladı.

Saldırı biçimi, zararlı yazılımın networkün sahibi kimse onun tarafından günlük internet trafiğine enjekte edildiği için 'Network Injection' olarak tabir ediliyor. Bu tür bir saldırı tekniğinin hükümetlerin casusluk faaliyetlerinin önemli bir parçası olmasından korkuluyordu.

Raporun yazarı Bill Marczak, Türkiye ve Mısır'da hedef alınan kişilerin kimliğinin belli olmamasına rağmen iletişim ağına yüklenen aparatın Türk Telekom'a ait olduğunun açık olduğunu öne sürdü. Türk Telekom ise yaptığı açıklamada Türkiye Cumhuriyeti kanunlarına bağlı olduklarını ve internet kullanıcılarının erişimlerine müdahale etmediklerini söyledi. Şirketten yapılan açıklamada ayrıca herhangi bir internet kullanıcısını popüler uygulama yazılımlarının zararlı yüklemelerini almaya yönlendirmedikleri belirtildi.

Haberler

{ SİBERBÜLTEN
siber güvenliğin türkçe hafızası

Kuzey Kore'li hackerlar 'Bankshot' ile Türk bankalarını hedef aldı

'Gizli Kobra' (Hidden Cobra) adıyla bilinen Kuzey Koreli siber saldırganların Türk kamu bankalarına yönelik yönelik saldırı düzenlediği iddia edildi.

ABD merkezli bilgisayar güvenliği firması McAfee'nin raporunda yer alan iddialara göre, Kuzey Koreli saldırganlar, 2-3 Mart tarihlerinde mali kuruluşları hedef aldı. Saldırı sırasında para çalınmasının söz konusu olmadığı ancak saldırıların Türkiye'de önümüzdeki dönemde geniş çaplı saldırılar için bir ön hazırlık niteliğinde olduğu bildirildi.

Siber suç kapsamında hackerler, Bankshot adlı zararlı yazılımın geliştirilmiş bir sürümünü kullandılar. Bankshot, ağlar ve sunucular üzerinde takılıp kalabilirken bir kez bulaşmanın ardından devam eden suistimallerin önünü açıyor.

İddialar arasında ilk zararlı yazılım yerleştirmenin hükümet denetimindeki büyük bir mali kuruluşa yönelik yapıldığı belirtiliyor. McAfee'nin açıklamasında, ikinci saldırının da yine hükümete bağlı mali bir kuruluşa yönelik gerçekleştirildiği, kurbanlar arasında üç büyük finans kuruluşunun daha olduğu ifade edildi. McAfee kuruluşların isimlerini açıklamadı.

'Oltaya gelmişler'

Hedefteki Türk kuruluşları virüslü dosyalarının 'oltalama' yöntemiyle Microsoft Word ekli e-postalar aracılığıyla yayıldığı bildirildi. Euronews'ta yayınlanan haberde virüslü dosyaların kullanıcıları Bitcoin satın almaya yönlendirdiği iddiası yer aldı.

McAfee'nin kıdemli analisti Ryan Sherstobitoff yaptığı açıklamada saldırının motivasyon kaynağını tam olarak belirleyememekle birlikte hacklemeyi saldırganların finansal kuruluşların şerefini tehlikeye atma gayretinin bir parçası olarak düşündüklerini söyledi.

Son olarak 2017 yılında görülen Bankshot zararlı yazılımının uzun süredir Kuzey Kore'nin hackleme tekniklerinden biri olduğu düşünülüyor.

İsrail'den 'sıfırıncı gün' mektubu: Açıklıkları bize satın

Bazen bir şeyi elde etmenin en iyi yolu onu direkt istemektir. İsrail hükümeti de sıfırıncı gün açığı olarak bilinen 'zero-day' bulan çok sayıda Amerikalı araştırmacıya ve firmaya e-posta yollarken bunu düşünmüş olmalı. "Sıfırıncı gün açıkları"nı bir sistem üzerinde keşfedilip, üretici/geliştiricisinin dahi henüz bilmediği güvenlik açıkları olarak tarif etmek mümkün.

Motherboard.vice.com sitesinin elde ettiği bilgilere göre en az beş Amerikan firması bu türde e-postalar aldı. Başka kaynaklar ise daha çok sayıda kişiye ve firmaya söz konusu e-postalardan gönderildiğini ileri sürdü. E-postada hükümetlerin sıfırıncı gün açığı tespit eden, geliştiren ve bundan istifade eden araştırmacılara nasıl yaklaştığını ortaya koyuyor.

İsrailli bir yetkili, 2015 yılında şirketlere ve uzmanlara attığı e-postada şu ifadeleri kullanmış: "İsrail Savunma Bakanlığı kendi bünyesindeki emniyet teşkilatları ve güvenlik ajanslarının ihtiyaç halinde kullanabilmeleri için sıfırıncı gün açıkları ile yüksek düzeyde ilgileniyor."

Söz konusu e-postalardan alan bir kişi kimliğinin gizli kalması koşuluyla yaptığı açıklamada, "Bu durumun normal olduğuna dair tek bir şey yok. Bu tuhaf şeyin yapılmasındaki amaç ne bilmiyorum" dedi.

Kimliğini açıklamayan başka bir kaynak da e-postaları 'teamüllere son derece aykırı' olarak tanımladı. Bununla birlikte söz konusu e-postalardan alan bir başka kişi ise durumu olağan dışı ya da tuhaf görmediğini söyledi. Bu kişiye göre konuyla ilgili e-posta yollamak çeşitli satıcılardan kaynaklanabilecek olası zararı öğrenmenin oldukça dobra bir yolu.

Hükümetlerin suçluları, teröristleri ve çocuk tacizcilerini izlemek için zaman zaman hackleme araçlarını kullandığı bir sır değil. Bazen hükümetler kendi bünyelerinde bu tür hackleme araçları geliştirebiliyor. Bazen de hükümetler siber güvenlik endüstrisinin en az bilinen ve anlaşılan kısmı olan sıfırıncı gün açıkları geliştiricilerinden bizzat hizmet satın alabiliyor.

Haberler

{SİBERBÜLTEN
siber güvenliğin türkçe hafızası

Şaşırtan iddia: Tor Project'in finansörü ABD'nin ta kendisi

Kişilere kimliklerini belli etmeden internette gezinme imkânı sağlamak amacıyla oluşturulan ve kâr amacı gütmeyen özel bir girişim olan Tor Projesi'ne, neredeyse yüzde yüz oranında ABD hükümeti tarafından fon sağlandığı öne sürüldü.

Söz konusu iddia surveillancevalley.com sitesinde Yasha Levine adlı kişi tarafından dile getirildi. "Surveillance Valley" aslında Yasha Levine tarafından yazılan bir kitap ve internetin gizli askeri geçmişini anlatıyor. Kitabın internet sitesinde yazarın imzasıyla yayımlanan yazıda iddiaların FOIA (Bilgi Edinme Hakkı) vesilesiyle 2500 sayfalık yazışmalardan elde ettiği bilgiye dayandırıldığı belirtiliyor. Levine, söz konusu belgelerin strateji oturumları, sözleşmeler, bütçeler ve Tor Projesi ile onun başlıca fon sağlayıcısı olan ve CIA'in yan ürünü olarak bilinen Uluslararası Yayıncılık Dairesi (BBG) arasındaki durum güncellemelerini içerdiğini ifade ediyor.

Belgeleri 2015 yılında elde ettiğini söyleyen Levine, o günden sonra birkaç yıl boyunca Tor'un ABD hükümeti ile gizli ve derin ilişkilerine dair ayrıntılı araştırmalar yaptığını belirtiyor. İşin maddi yönüne odaklandıktan sonra Tor'un bir halk hareketi olmadığını iddia eden Levine, sözlerine şunları ekliyor: "Bunu Tor'un radikal hükümet karşıtı duruşuna rağmen ortaya koyabildim: Tor neredeyse yüzde yüz oranında ABD ulusal güvenlik ajansları (Donanma, Dışişleri Bakanlığı ve Uluslararası Yayıncılık Dairesi (BBG)) tarafından fonlanıyordu."

Bunun şoke eden bir ifşaat olduğunu yazan Levine devam ediyor: "Signal gibi diğer hükümet destekli kripto araçlar gibi Tor Projesi de yıllardır insanları hükümetin online ajanlık faaliyetlerinden koruyan bir platform gibi görülüyordu." Ancak gerçeklerin böyle olmadığını söyleyen Levine, elde ettiği ilk kanıtların Tor'un ABD hükümetinin dış politika silahı olduğuna dair şüpheyi tam olarak karşılamadığını ileri sürüyor. Fakat Levine, BBG'den elde ettiği FOIA belgelerinin kanıtları yeni bir boyuta taşıdığını belirtiyor. Yazının devamında Levine "Peki ABD hükümeti kendi gücünü sınırlayan bir örgütü neden desteklesin ki?" diye sorarak, cevabı yine kendi veriyor: "Tor ABD'nin gücünü tehdit etmiyor; onu artırıyordu."

Levine'in sitesine göre "FOIA belgeleri federal hükümet, Tor Projesi ve internet özgürlüğü hareketinin anahtar üyeleri arasında bir işbirliği olduğunu gösteriyordu. Belgeler Tor çalışanlarının federal hükümette görevli işbirlikçilerinden emir aldığını gösteriyordu. Bu emirler arasında ABD'nin istikrarsızlaştırmaya çalıştığı Çin, Vietnam, Rusya gibi ülkelerde Tor'un anonimliğini kullanma yoluyla planlar yapmak bulunuyordu. Belgeler, haberleri etkileme ve muhalif basını kontrol altına almaya yönelik ihtiyaçlar üzerine yapılan tartışmaları ortaya koyuyordu."

İddialara dair daha ayrıntılı bilgiler internet sitesi ile aynı adı taşıyan Surveillance Valley adlı kitapta yer alıyor.

www.siberbulten.com tarafından hazırlanmıştır.

Siber Takvim

İnternet Haftası Etkinlikleri

11 Nisan 2018 | 09:00 - Muğla Sıtkı Koçman Üniversitesi

MUCyber İnternet haftası etkinlikleri kapsamında eğitim, sunum, CTF yarışmaları ve sosyal aktiviteler sizleri bekliyor. Eğitimler ücretsiz, kayıt gerekiyor.

https://www.mucyber.org/ihe/

Kamu Siber Güvenlik Zirvesi 2018

18-19 Nisan 2018 - Ankara Bilkent Otel

Kamu Bilişimcileri Derneği'nin düzenlediği etkinlik kamuda siber güvenliğin sağlanması kapsamında kamu bilişim yöneticileri ve uzmanları ile sektör temsilcilerinin katılımı ile düzenleniyor. Zirve, kamu çalışanlarına ve sponsor firma çalışanlarına açıktır.

http://www.kamusiberguvenlik.com/

Entegre Siber Güvenlik Teknoloji Platformu

26 Nisan 2018 | 09:00 - CVK Park Bosphorus Otel, İstanbul

Bilişim Zirvesi'nin düzenlediği etkinlikte milli güvenlik politikalarıyla ulusal siber güvenlik, dijital dünyada entegre siber güvenlik ve kurumlarda entegre güvenlik mimarisinin oluşturulması konuları ele alınacaktır. Kayıt gerekiyor.

http://bit.ly/2ppgXHP

BTG DAY

BTG DAY 2018

28-29 Nisan 2018 - Ankara Yıldırım Beyazıt Üniversitesi

Biltek CyberSec Kulübü, ikincisini düzenlediği "Siber Güvenlik ve Yapay Zeka" temalı konferansında alanında uzman 15 konuşmacı bilgi paylaşımı ve farkındalığı artırmayı hedefliyor. Kayıt gerekiyor.

https://btg.aybucyber.club/

Gazi Siber Güç CTF Yarışması

27 Nisan 2018 - Gazi Üniversitesi, Ankara

Gazi Üniversitesi, gençlerin ilgisini siber güvenlik alanına çekmek ve siber saldırılarla mücadele edebilecek insanları geliştirmek amacıyla bir CTF yarışması düzenliyor. Ücretsiz olan etkinliğe kayıt gerekiyor.

http://ctf.gazi.edu.tr/

INIT 0 - Siber Güvenlik ve Veri Bilimi

28-29 Nisan 2018 - Eskişehir Anadolu Üniversitesi

Anadolu Üniversitesi IEEE'nin düzenlediği konferansın ayrıntılarını kulübün web sitesinde bulabilirsiniz.

http://www.ieeeanadolu.org/

Samsun Bilgi Güvenliği Günleri

26-27 Nisan 2018 - Ondokuz Mayıs Üniversitesi

OMÜSiber tarafından düzenlenen konferans ve CTF yarışmasının ayrıntılarını topluluğun web sitesinde bulabilirsiniz.

http://www.omusiber.org/

NOPcon Istanbul

3-5 Mayıs 2018 - ISOV Sakıp Sabancı Konf. Salonu, İstanbul

TRAPMINE tarafından düzenlenen, Türkiye'nin en büyük siber güvenlik konferanslarından biri olan NOPcon güvenlik araştırmacıları, danışmanlar, hacker ve geliştiriciler için bilgi alışverişi ve öğrenmeyi hedefleyen bir buluşma ortamı sağlıyor. Etkinlik kâr amacı gütmüyor, kayıt gerekiyor.

http://www.nopcon.org/

HACKTRICK '18

4-6 Mayıs 2018 - Bilgi Teknolojileri Kurumu, Ankara

Octosec ekibi tarafından her yıl geleneksel olarak düzenlenen, 2 günün eğitime 1 günün konferansa ayrıldığı, toplamda 3 gün süren bir Siber Güvenlik etkinliğidir. Eğitimler ve konferans ücretsiz, kayıt gerekiyor.

https://www.hacktrickconf.com/

PHPKonf 2018

20-21 Mayıs 2018 - Nişantaşı Üniversitesi, İstanbul

İstanbul PHP Topluluğu tarafından yer yıl düzenlenen PHPKonf, 5. yılında en iyi konuşmacıların son teknolojileri, ilgi çekici başlıkları ve php hakkında güncel konuları konuştuğu, çeşitli sosyal aktiviteleri de kapsayan bir etkinliktir. Konuşmacılar, program ayrıntıları ve bilet bilgileri web sitesinde yer alıyor.

https://phpkonf.org/

Özgür Yazılım Zirvesi

28 Nisan 2018 İstanbul Teknik Üniversitesi Bilgisayar ve Bilişim Fakültesi

İTÜ Kültür ve Sanat Birliği'ne bağlı Özgür Yazılım Kulübü 28 Nisan 2018 tarihinde Özgür Yazılım Zirvesi(ÖYZ)'nin ilkini gerçekleştirmeyi planlıyor.

2. Siber Güvenlik Yerli Çözümler Zirvesi: "Kişisel Verileri Koruma"

8 Mayıs Nisan 2018 - BÜSİBER Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Siber Güvenlik Merkezi,

Güney Kampüs, Büyük Toplantı Salonu

http://www.siber.boun.edu.tr

Recep Kızılarslan - recepkizilarslan@gmail.com

PinMe

GPS Olmadan Kullanıcıları İzlemenin Farklı Bir Yolu

Princeton Üniversitesi'nden bir grup araştırmacı tarafından geliştirilen PinMe uygulaması genel kullanıma açık tüm bilgileri ve kompakt sensörleri kullanarak konum tespiti yapıyor. Üstelik konum tespitinde kullandığı bu sensörler için izninize de ihtiyaç duymuyor.

Örneğin GoogleMaps'in bu verilere ulaşması için telefonunuzda GPS'nin açık olması ve sizin erişim iznini vermiş olmanız gerekirken, PinMe jiroskop ve ivmeölçer sensörlerinden aldığı saat dilimi ve IP gibi vb. dataları işleyerek sizin lokasyonunuzu tespit edebiliyor. Hatta hangi vasıta ile hangi istikametlere gittiğinizi **OpenStreetMap** (OSM) üzerinden ortaya çıkarabiliyor. PinMe'nin kullandığı bilgi kaynaklarını yakından inceleyelim.

İvmeölçer

İvmeölçer kütleye uygulanan ivmeyi ölçen cihazlardır ve içindeki test kütlesine referans eksenindeki, kütleden kaynaklı uygulanan kuvvetlere bakar. Akıllı telefonlarda hızlanmayı hesaplar ve GPS'e daha verimli bilgi gönderilmesine yardımcı olur. Ayrıca siz hareket halinde iken net fotoğraflar çekebilesiniz diye kameranız ivmeölçer sensöründen yardım almaktadır.

PinMe ivmeölçerden aldığı veriler ile nasıl hareket ettiğinizi anlamaya çalışır. Örneğin yavaş bir şekilde hareket ederseniz yürüdüğünüze, hızlı bir şekilde hareket ederseniz araba veya motorsiklet kullandığınıza kanaat getiriyor.

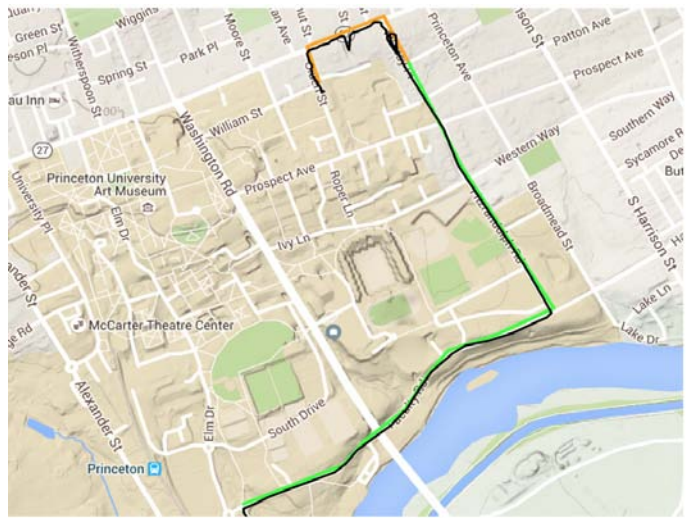
Barometre

Adından da anlayacağımız gibi barometre atmosfer basıncını ölçmeye yarar. Mobil teknolojide daha çok GPS'e yardımcı olmak maksadıyla kullanılmaktadır.

PinMe'nin barometreden aldıkları veriler ile de kullanıcının hangi araçla hareket ettiğini anlamaya çalışır. Alınan verilerde basıncın yüksek ve düşük olmasından hareketle tren veya uçak ile yolculuk edildiği çıkarımı yapılır.

Jiroskop

Türkçe adı ile "Düzdöner" olan jiroskop sensörü, yön ölçümü ve ekran ayarlamasında kullanılıyor. Jiroskop akıllı telefonumuzu yan yatırdığınızda, ekranın yan yatmasını sağlayan ve sağ sol hareketli ile oyun oynamamızı sağlayan sensördür.



Arabanız ile A konumundan çıkıp B konumuna gideceksiniz. PinMe ivmeölçer sensöründen aldığı datalar ile (düzensiz po-

zitif hızlanmalar, ani frenler vs.) sizin motorsiklet ya da araba ile gittiğinizi saptayabilir. 90 derecelik bir dönüş yaptığınız takdirde jiroskop sensöründeki değişme verilerini de işleyen PinMe iki konum arasında araba ile gittiğinize karar verebiliyor.

IP adresi & Ağ Durumu

IP kısaca interneti ya da TCP/IP protokolünü kullanan cihazların, ağ üzerinden birbirleri ile veri alışverişi yapmak için kullandıkları adrese denmektedir.

PinMe ilk olarak mobil cihazın IP bilgilerine ve son Wi-Fi bağlantısına bakıp konum tespitinde kullanır.

Saat Dilimi & Hava Durumu

Meridyen, Greenwich başlangıç boylamından başlayarak yeryüzünü 24 parçaya ayıran 15 derecelik bölümlerden her biri. PinMe algoritması konum verilerini elde edebileceği tüm dataları işler. Mobil cihazın bulunduğu saat dilimi de bunlardan bir tanesidir.

Hızlıca farklı saat dilimlerinden geçtiğinizi düşünün. İvmeölçerden alınan hız verileri, barometreden alınan basınç değerleri ve saat dilimi değişikliklerinizi işleyen PinMe uçakla seyahat ettiğinizi rahatlıkla ortaya çıkarabiliyor.

Ayrıca hava durumu istasyonları aracılığı ile elde ettiği dataları işleyip işlemi kolaylaştırıyor.

OpenFlights

PinMe'nin bulduğu konum/izlenen yol verilerinin ne denli sağlam olduğunun göstergelerinden bir tanesi olarak; OpenFlights veri tabanındaki datalarını da işleyebilmesidir. OpenFlights dünya çapında uçuşların detaylarını haritalandırıp kullanıcıya sunan bir sistemdir. Başlangıç-varış noktaları, uçuş saatleri gibi elde ettiği bilgilerde doğruluğu teyit etmeye yardımcı olur.

Ayrıca PinME GoogleMaps üzerinden elde ettiği istasyon bilgileri ile de tren seyahatlerinin doğrulanmasını sağlayabiliyor.

Örnek Senaryo

İstanbul'dan Ankara'ya uçak ile seyahat edeceksiniz. Evinizden çıkıp taksi durağına doğru yürümeye başladınız. PinMe ivmeölçer'den aldığı hız verileri ile sizin yürüdüğünüzü anladı. Ayrıca evden çıkarken son olarak evin modemine bağlı olduğunuz için başlangıç noktası olarak da orayı kabul etti. Ardından köşedeki taksi durağından taksiye bindiniz. Trafik sıkışık olduğu için sürekli değişen hız ivmeniz, ve 90 derecelik dönemeçlerde aracın manevralarından dolayı jiroskop'un verdiği değerleri işleyen PinMe algoritması yolun devamını otomobille gittiğinizi saptadı. Ardından hava alanına vardınız ve bir koşu uçağınıza yetiştiniz. Uçak havalandıktan sonra belirli bir feet'e ulaştı ve 600 km hızla Ankara'ya doğru ilerlemeye başladı. PinMe, barometreden aldığı basınç değerleri, ivme ölçerden aldığı hız değerleri ile uçakla uçtuğunuza kanaat getirdi. Ankara'ya iniş yaptıktan sonra OpenFlights üzerinden aldığı datalar ile bu uçuşu teyit etti.

Araştırmacılar, telefon üreticilerinin kullanıcıların gizliliğini korumak adına, tüm sensörleri bir tuşla devredışı bırakıp / etkinleştirme imkânı veren bir fonksiyon koymasını öneriyorlar.

Kaynak:

PinMe: Tracking a Smartphone User around the World,
https://arxiv.org/pdf/1802.01468v1.pdf

BitLocker ile Disklerinizi Şifreleyin

Neden Sürücü Şifreleme?

Bilgisayarımızı hâlihazırda koruduğumuz parolalar var. Bu parolalar girilmediği takdirde işletim sistemlerimizde oturum açılamıyor. Endişelenecek ne var, diyenlerden misiniz?

Peki ya bilgisayarınıza fiziksel erişim elde eden biri, örneğin laptopunuzu çalan biri, çok önemli verilerinizi sakladığınız HDD'nize doğrudan erişim sağlasa, bu çok güvendiğiniz parolalar sizi koruyabilecek mi? Elbette hayır!

Fiziksel erişim için her zaman laptopunuzdan fersah fersah uzak olmanız gerekmez. Bu sayımızda yer alan ve Edward Snowden'in geliştirdiği Haven uygulamasını konu alan yazıda da belirtildiği gibi, bir öğle yemeği için ayrıldığınız otel odasında dahi Evil Maid dediğimiz saldırıya muhatap olabilirsiniz. Yani temizlik görevlisi kılığında birileri odanıza girip, PC'nize fiziksel erişim elde edebilir.

Tedbir olarak disklerimizi şifrelemeliyiz. Böylece çok güvendiğiniz hırsızlık sigortasından daha fazlasını, kişisel verileriniz için yapmış olacaksınız. Bu yazıda Windows ile birlikte disklerimizi şifrelemeye olanak sağlayan BitLocker'ın nasıl etkinleştirilebileceğine değineceğiz.

Bitlocker Nedir?

BitLocker Sürücü Şifrelemesi, etkin olduğu sürücüdeki her şeyi şifreleyen yerel bir güvenlik özelliğidir. Cihaz şifreleme, verilerinizi şifreleyerek korumaya yardımcı olur. Sadece doğru şifreleme anahtarı olan bir kişi (kişisel kimlik numarası gibi), cihazdaki verilerin şifresini çözebilir.

Nasıl Çalışır?

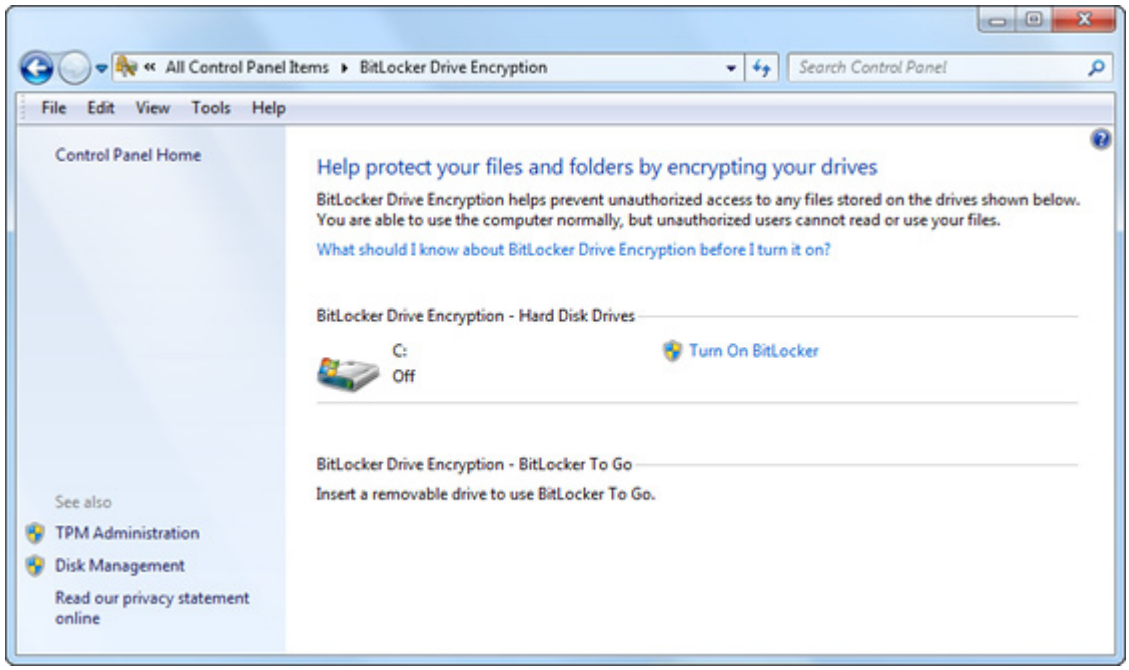
BitLocker, Trusted Platform Module (TPM) adı verilen bir donanım bileşeni ile birlikte kullanılır. TPM, bilgisayar üreticisinin daha yeni bilgisayarlarda yüklü olduğu anakartta akıllı kart benzeri bir modüldür. BitLocker kurtarma anahtarını TPM'de (sürüm 1.2 veya üstü) saklar.

BitLocker'ı etkinleştirdiğinizde, bilgisayarınızı her başlattığınızda kişisel bir kimlik numarası (PIN) girmeniz gerekir. BitLocker'ı etkinleştirirken, bir kurtarma anahtarı oluşturulur. Şifreyi unuttuğunuzda kurtarma anahtarı, bilgisayarınıza erişmek için kullanılır. Kurtarma anahtarı üretildikten sonra, makineyi yeniden başlatmanız istenir. Şifreleme işlemi, bilgisayar yeniden başlatıldığında başlar.

BitLocker'ı Aktifleştirme

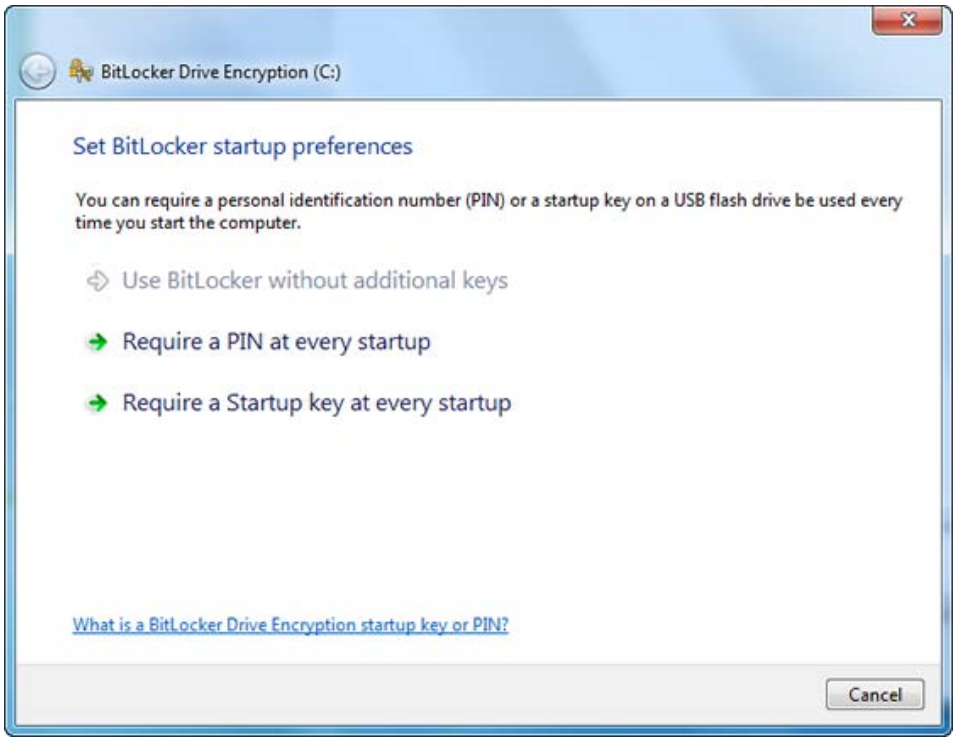
1- Önce Start'a, ardından Control Panel'e, onun ardından System and Security'ye tıklayın. Bu adımlar sonrasında "BitLocker Drive Encryption" görmüş olmanız gerekiyor. "BitLocker Drive Encryption"a tıklayın. *Not: BitLocker, Windows'un tüm versiyonlarında mevcut değildir.*

2- "Turn on BitLocker"a tıklayın.

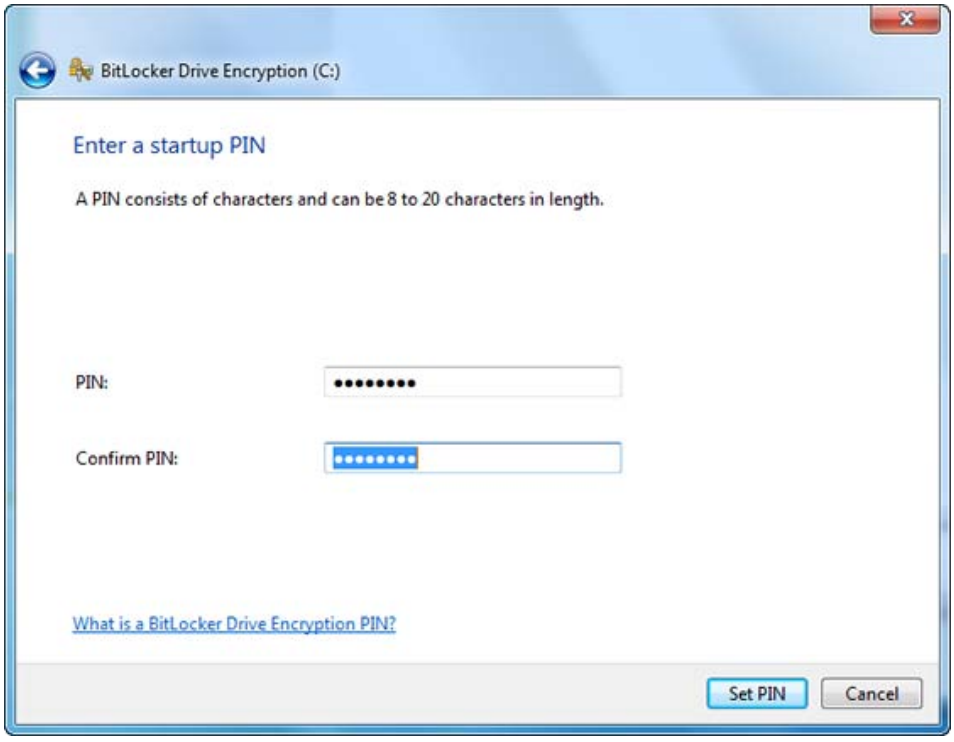


3- BitLocker, sistem gereksinimlerini karşıladığını doğrulamak için bilgisayarınızı tarayacaktır. Herhangi bir problem ile karşılaşmazsanız "Next"e tıklayın.

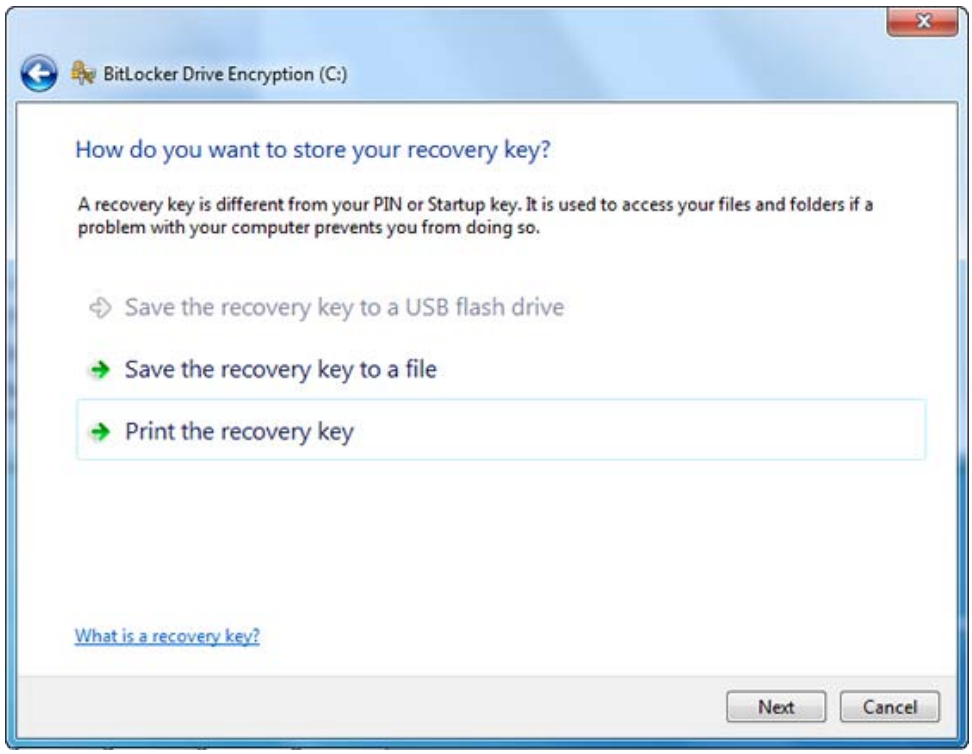
4- BitLocker başlangıç tercihleri sayfası görüntülendiğinde,"Require a PIN at every startup" seçeneğini tıklayın.



5- 8 ila 20 karakter uzunluğunda bir PIN girin ve ardından "Confirm PIN" alanına tekrar girin. "Set PIN"e tıklayın.



6- Kurtarma anahtarınızı saklamak için “Print the recovery key”i seçin ve “Next”e tıklatın.



Şifreleme işlemini başlatmak için bilgisayarınızı yeniden başlatmanız istenecektir. Bilgisayarınız yeniden başladıktan sonra bilgisayarınızı güvenle kullanabilirsiniz!

Internette Gizli Kalın
The Onion Router

Tor (The Onion Router), kişilerin kimliklerini gizli tutarak internette gezinmelerine olanak sağlayan, internet erişiminin yasaklı ya da kısıtlı olduğu bölge ve ülkelerde de internet erişim engellerinin aşılmasına olanak sağlayan hem bir network, hem de bir tarayıcıdır.

Tor ilk olarak Amerikan Donanması ile birlikte devlet içi iletişim için geliştirilmiştir. Şu an ise herkesin erişebildiği (gazeteci, aktivist, ordu vs.) sanal tünellerden gizlilik ve güvenlik sağlamaktadır.

Tor Tarayıcı, Mozilla Firefox'un güncel ve gizlilik açısından optimize edilmiş bir versiyonudur. Çevrimiçi anonimlik ve engellenmiş sitelere erişim sağlayan ücretsiz ve açık kaynaklı bir yazılımdır. Diğer tarayıcılardan farklı olarak Tor Tarayıcısı;

- Kullanıcının IP adresini gizleyerek internette anonim dolaşmayı sağlar,
- Engellenmiş sitelere erişim sağlar,
- Normalde varsayılan olarak gelen çevrimiçi izleme özellikleri içermez,
- Kullanıcı verilerinden para kazanmaz,

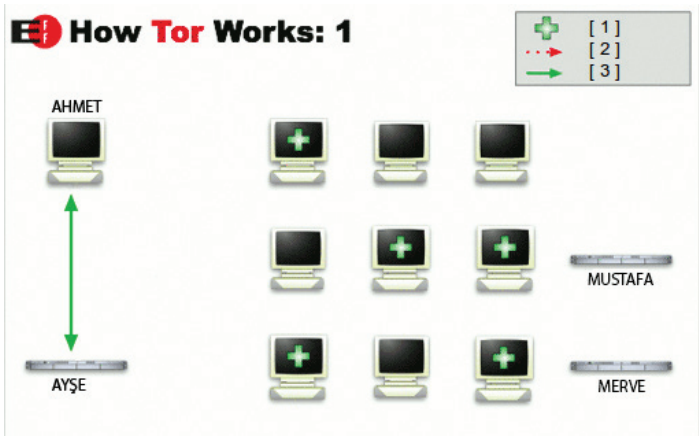
Tor ağı, dünyanın dört bir yanındaki gönüllüler tarafından işletilen binlerce sunucudan oluşmaktadır. Tor tarayıcı her yeni bağlantıda 3 röle seçer ve bunlardan internete bağlanır. Her bağlantı esnasında röleler veriyi gönderdiği ve aldığı yolu tam olarak bilmeyecek şekilde şifrelenir.

Tor tarayıcı kullanıldığında internet bağlantısını farklı bir IP adresinden, genellikle farklı bir ülkeden gelmiş gibi gösterecektir.

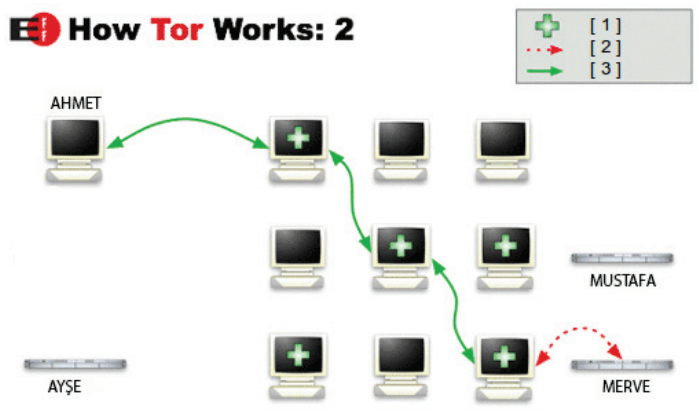
1.Tor Nasıl Çalışır?

Aşağıdaki adımlar, Ahmet'in bilgisayarının Merve'nin sunucusu ile iletişim kurmak için Tor Tarayıcı kullandığı zaman Tor ağının nasıl çalıştığını göstermektedir:

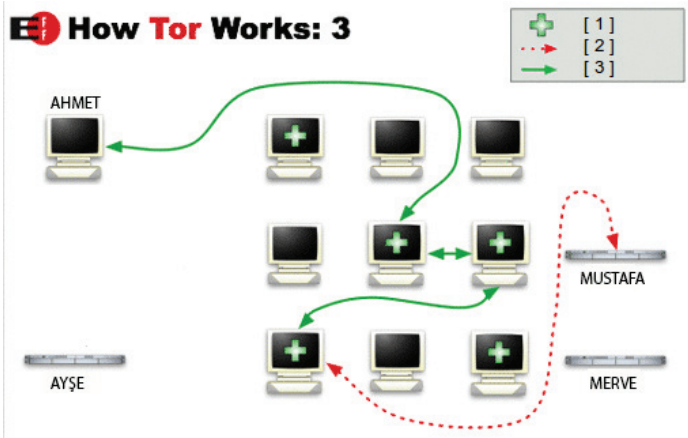
Adım 1: Ahmet'in Tor Tarayıcısı, Tor dizin sunucusundan (Ayşe) Tor röleleri [1] listesini alır.



Adım 2: Ahmet'in Tor Tarayıcısı, Tor ağından hedef sunucuya (Merve) rastgele bir yol seçer. Tor ağındaki tüm bağlantılar şifrelenmiştir (yeşil [3]). Bu örnekte, son bağlantı şifrelenmemiştir (kırmızı [2]) çünkü Merve'nin sunucusuna erişmek için HTTP kullanmaktadır. Ancak Ahmet bir web sitesini SSL/TLS yani HTTPS üzerinden ziyaret ediyorsa son bağlantı da şifrelenmiş olurdu.



Adım 3: Eğer daha sonra Ahmet başka bir sunucuyu (Mustafa) ziyaret ederse, Ahmet'in Tor Tarayıcısı bu defa farklı, rastgele bir yol seçer.

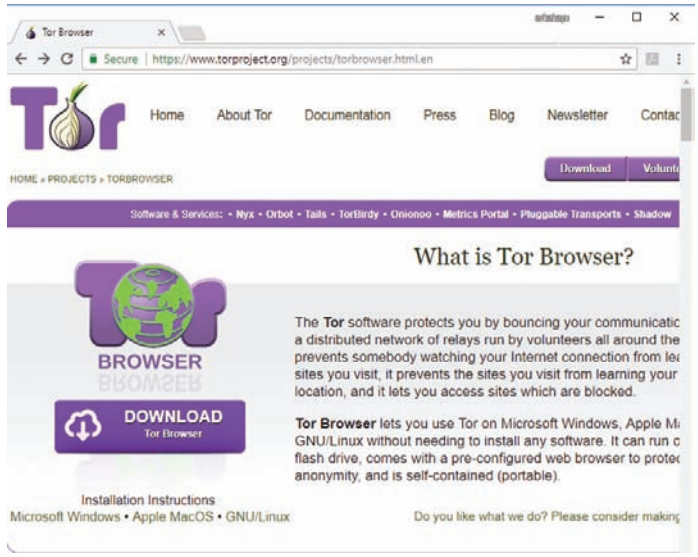


NOT: Anonimlik ve hız arasında bir ters orantı vardır. Tor, internet trafiğini dünyanın çeşitli yerlerinde bulunan gönüllü sunucular aracılığıyla yaptığı için anonimlik sağlar ancak veri akışı normal internet bağlantısından daha yavaş olacaktır.

Dikkat! 2016 yılında düzenlenen Black Hat konferansında Tor Tarayıcının çıkış düğümleri (Exit Nodes) kullanılarak bir zafiyet keşfedilmiştir.[1] Bağlantı için kullanılan Tor röleleri gönüllüler tarafından yönetilir. Bu yüzden bu röleleri kontrol etmek mümkündür. Bu durumu istismar etmek isteyen kişiler bu rölelerin içine kendi rölelerini ağ analiz teknolojileri kullanarak eklerler. Yukarıda da belirttiğim gibi mesaj rölelere şifrelenmiş katmanlar şeklinde gönderilir, rastgele bir şekilde başka röleye bağlantı sağlanır. Son röle yani Exit Node son katmanın şifresini çözebilir ve elde edilen mesaj açık metindir. Eğer bu son röle kötü niyetli bir düğüm ise bu röleye uğrayan mesaj açık bir şekilde okunabilir. Şöyle ki bu mesaj da kişinin gerçek IP adresi ve yeri görünmeyecektir ancak kullanıcı adı, parola, banka bilgisi gibi bilgiler okunabilir.

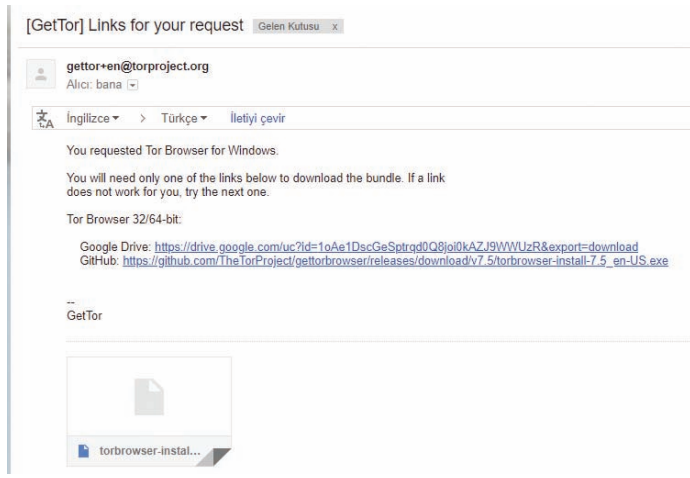
2.Tor Tarayıcısının Yüklenmesi

Adım 1: Aşağıdaki adrese gidilir ve "Download Tor Browser" butonuna basılır.



Şekil 1: Tor Tarayıcı sayfası

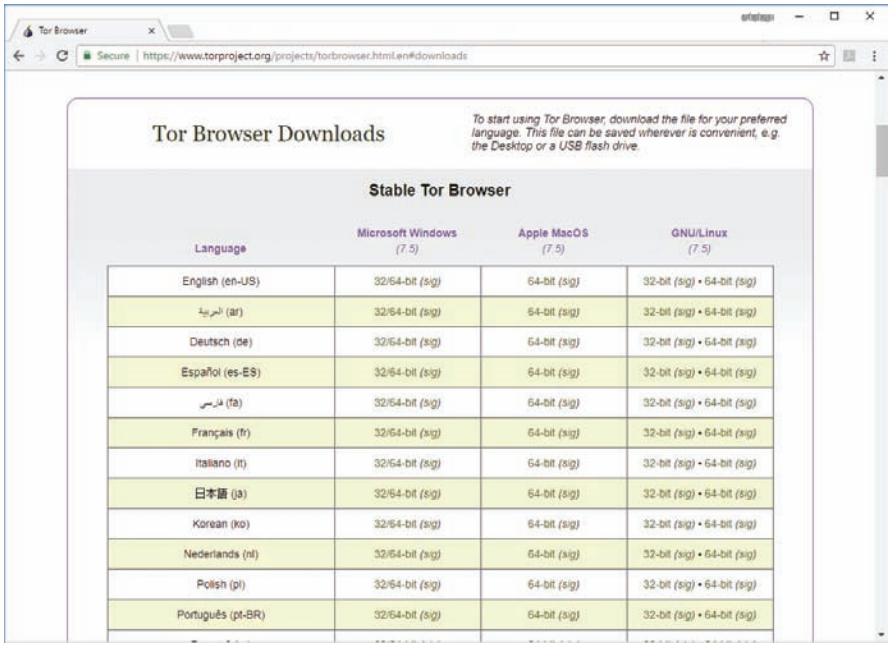
NOT: Eğer yukarıdaki adrese erişim engellendiyse başka bir adresten indirebilmek için gettor@torproject.org adresine kullandığımız işletim sisteminizi (Windows,OSx veya Linux) belirterek bir e-posta göndererek edinebiliriz.



Şekil 2: Tor e-posta cevabı

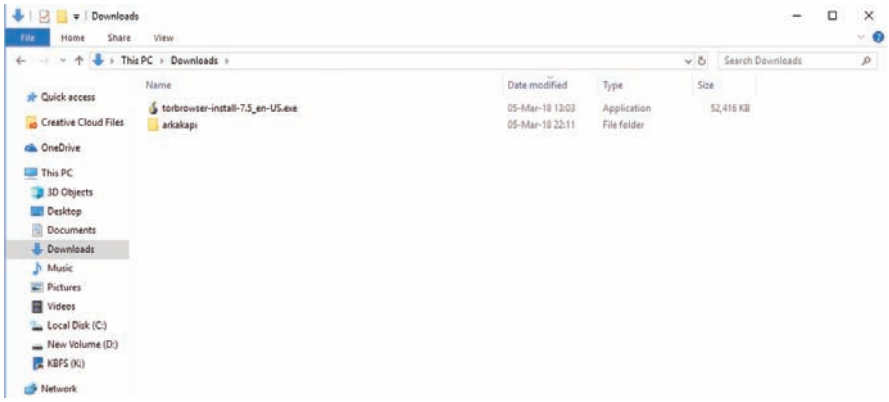
1 https://www.blackhat.com/docs/us-16/materials/us-16-Sivakorn-HTTP-Cookie-Hijacking-In-The-Wild-Security-And-Privacy-Implications.pdf

Adım 2: İndirmek istediğiniz dili ve işletim sistemini belirleyin



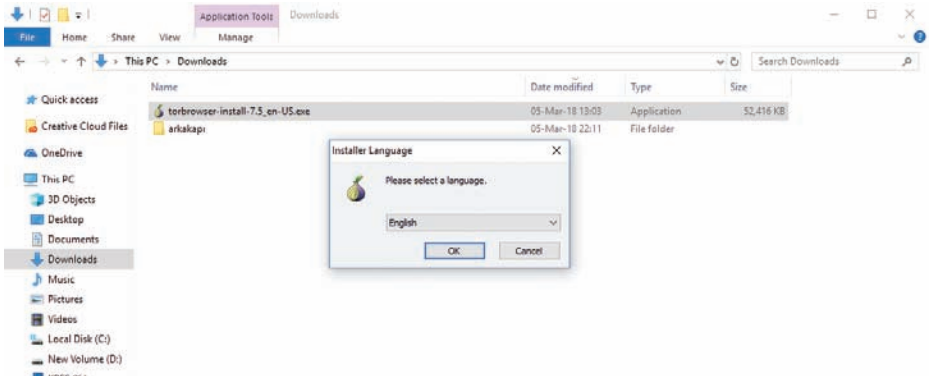
Şekil 3: Tor Tarayıcı indirme linkleri

Adım 3: Kurulum dosyasının indirildiği dizine gidilir.



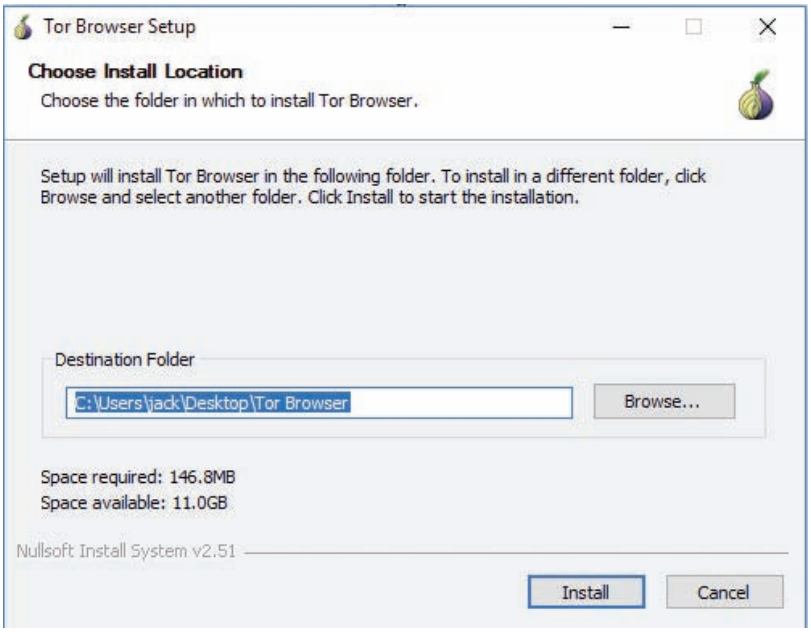
Şekil 4: Kurulum dosyasının bulunduğu dizin

Adım 4: EXE uzantılı dosya çift tıklanarak kurulum başlatılır. Kurulumun ilk adımında dil seçimi yapılır.



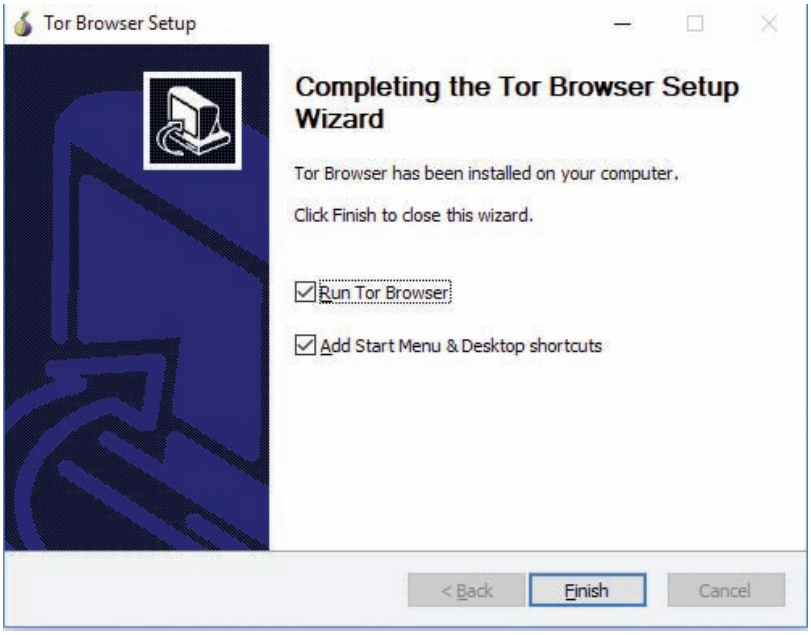
Şekil 5: Tor Tarayıcı dil paketinin kurulumu

Adım 5: Tor Tarayıcısının yüklenmek istenilen dizin belirlenir. Şekil 6'da yüklenilmek istenilen dizin olarak masaüstü seçilmiş.



Şekil 6: Tor Tarayıcının kurulum yeri

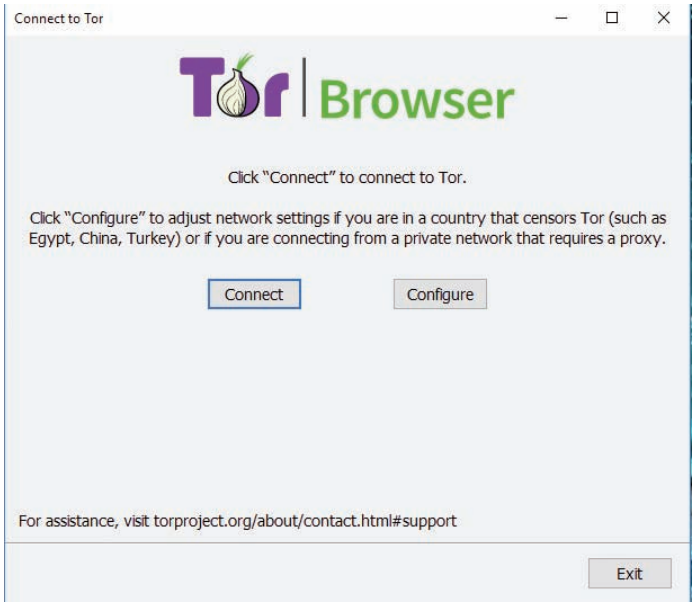
Adım 6: Kurulumu tamamlamak için aşağıdaki pencerede bitir(finish) butonuna tıklayın.



Şekil 6: Kurulumun tamamlanması

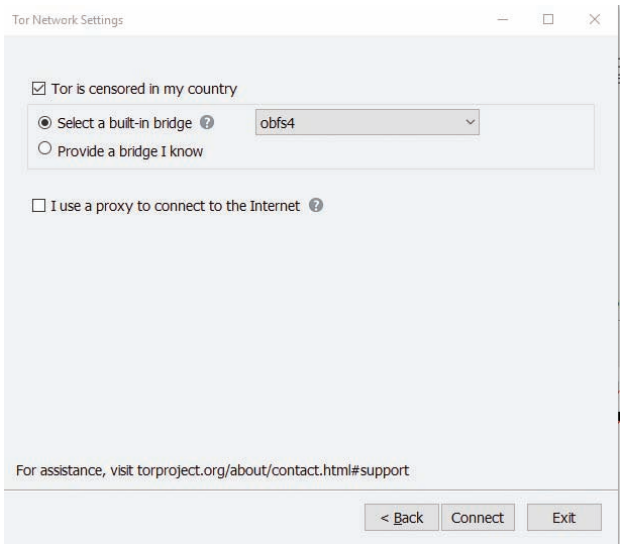
3.Tor Ağına Bağlamak İçin Gerekli Ayarlar

Adım 1: Eğer Tor internete girilen ülkede engellenmemiş ise direk bağlan (connect) butonuna basarak tarayıcı açılabilir. Fakat Tor ağına bağlanılmak istenen ülkede bu tarz servislere erişim engelli durumda ise, Tor Browser, "Configure" butonuna basılarak yapılandırılmalıdır.



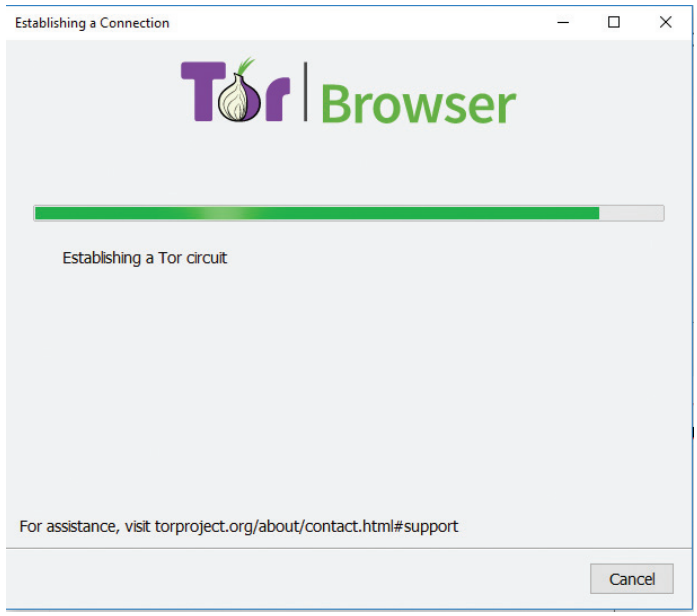
Şekil 1: Tor Tarayıcı ayarları

Adım 2: Yapılandır(Configure) butonuna basıldığında aşağıdaki pencere açılır. Burada Tor internete girilen ülkede engellendiği için köprü bağlantıları kullanılır. Köprü bağlantıları halka açık dizinde listelenmediği için engellenmesi daha zordur. Köprü olarak hazır bulunan obfs4 gibi aracılar seçilip bağlan(connect) butonuna basılır.



Şekil 2: Tor köprü yapılandırması

Adım 3: Kısa bir süre sonra Tor Tarayıcı açılacaktır



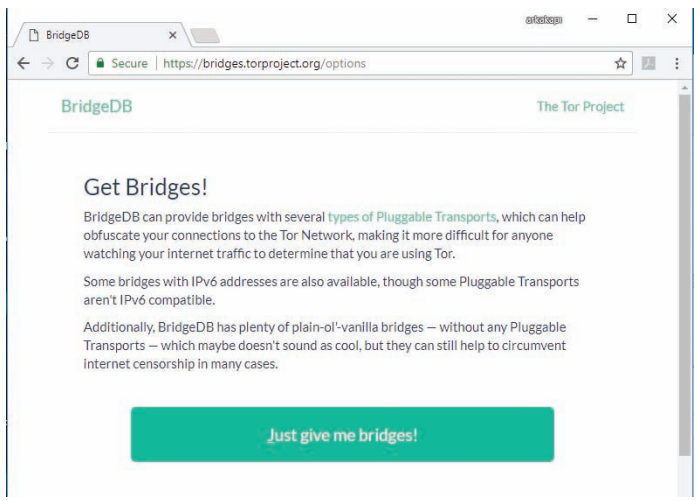
Şekil 3: Tor ağına bağlanma

4.Özel Köprüler İle Tor Ağında Bağlanma

Tor ağına bağlanmak için daha az bilinen ve bu sebeple engellenmesi daha düşük olan özel köprüler ile bağlantı yapılabilir. Tor sayfasına erişilemiyorsa "bridges@torproject.org" adresine, e-postanın body/gövde kısmına "get bridges" yazip e-mail göndererek özel köprü adresleri talep edilebilir.

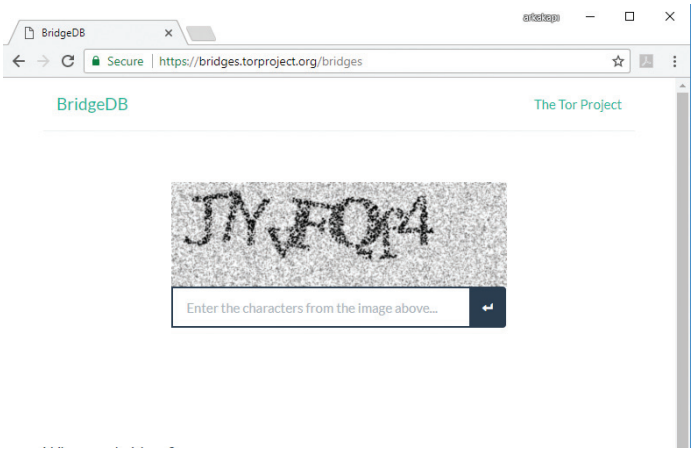
Ancak Tor sayfasına erişilebiliyorsa aşağıdaki adımlar uygulanarak özel köprüler elde edilebilir;

Adım 1: Aşağıdaki adrese gidilir ve sadece köprüleri bana ver (Just give me bridges) butonuna tıklanır.

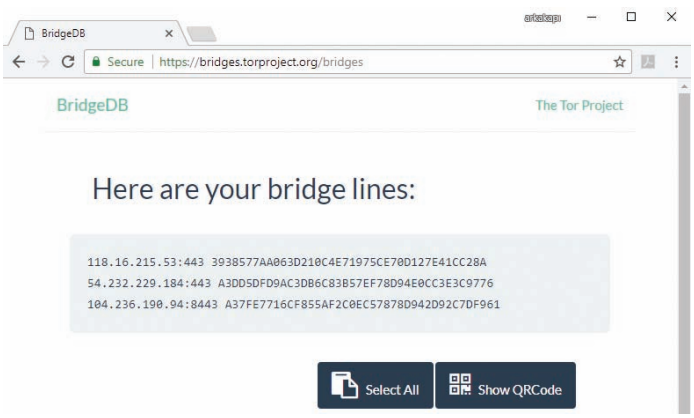


Şekil 1: Tor özel köprülerinin alınması

Adım 2: Güvenlik kodu doldurulur ve girişe basılır.

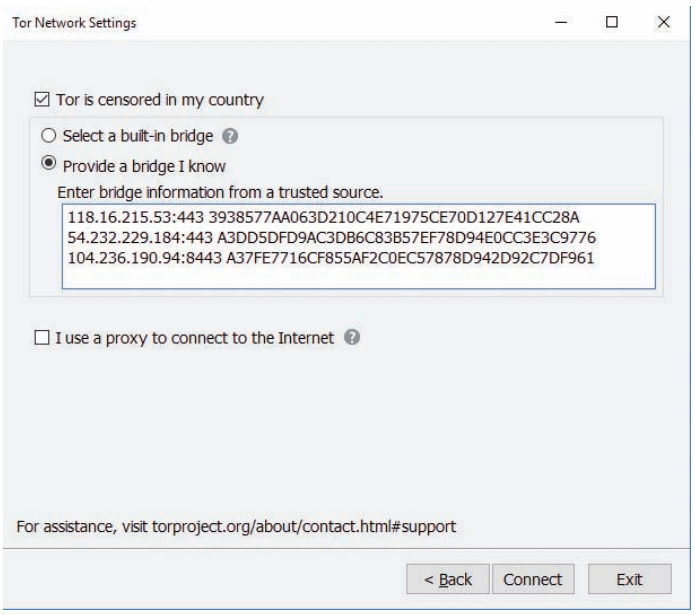


Şekil 2: Güvenlik kodu



Şekil 3: Köprü satırları

Adım 3: Aldığımız köprüler aşağıdaki bölüme kopyalanır ve bağlan (connect) butonuna tıklanır.



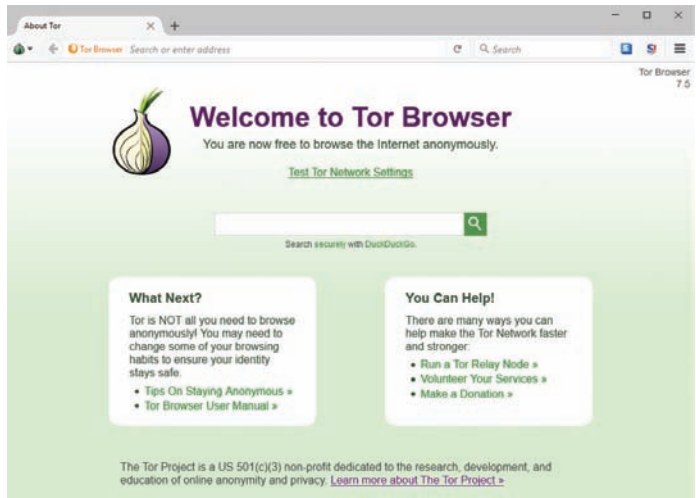
Şekil 4 : Tor Ağ Ayarları

5.Tor'u Güvenli ve Anonim Bir Şekilde Kullanmak İçin Yapılması Gerekenler

Tor Tarayıcı sadece Tor Tarayıcısı penceresinde yapılan işlemler için anonimlik sağlar. Uygulamanın çalışıyor olması diğer programların da Tor Ağını kullanıyor olduğu anlamına gelmemektedir.

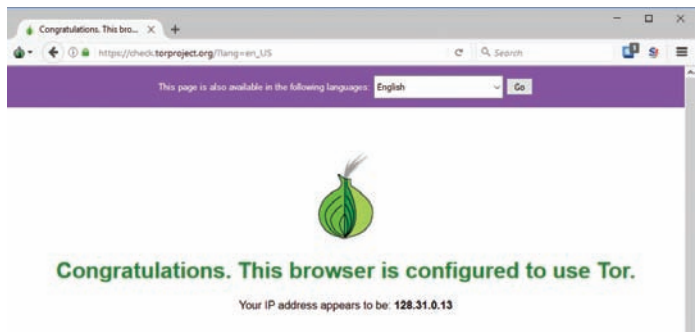
5.1.Tor Tarayıcının çalışıp çalışmadığını kontrol etme

Tor tarayıcının düzgün bir şekilde kurulup çalıştığından emin olmak için Tor Ağ Ayarlarını Test Et(Test Tor Network Settings) linkine tıklanabilir.



Şekil 1: Tor Tarayıcı Anasayfası

Eğer aşağıdaki gibi bir sayfayla karşılaşırsak Tor tarayıcının düzgün çalıştığını söyleyebiliriz.



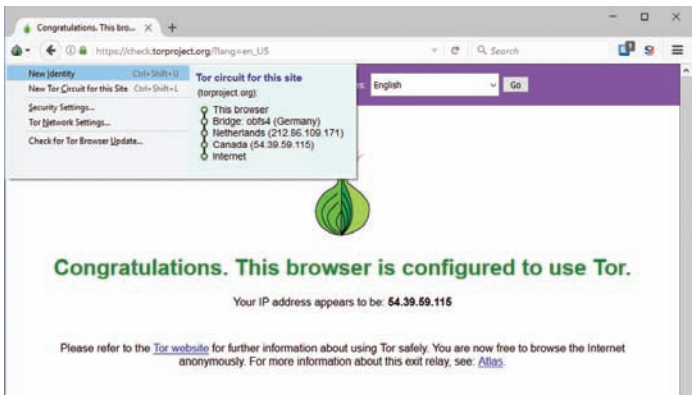
Şekil 2: Tor ağı kontrolü

Tor Projesinin kendi kontrol sistemi haricinde https://www.iplocation.net/ ve https://www.ip2location.com/ adreslerinden bağlantı bilgilerini öğrenebiliriz.

5.2.Yeni Kimlik Oluşturma

İstediğimiz zaman yeni kimlik oluşturabiliriz. Bu sayede Tor yeni bağlantı düğümleri oluşturacak ve erişilecek web sitelerine farklı bir IP adresinden ulaşıyor gibi görülecektir. Bunu yapmak için aşağıdaki adımlar uygulanabilir.

Adım 1: Tor Tarayıcısı menüsünü açmak için butonuna tıklanır.



Şekil 1: Tor Tarayıcı da yeni bir kimlik oluşturma.

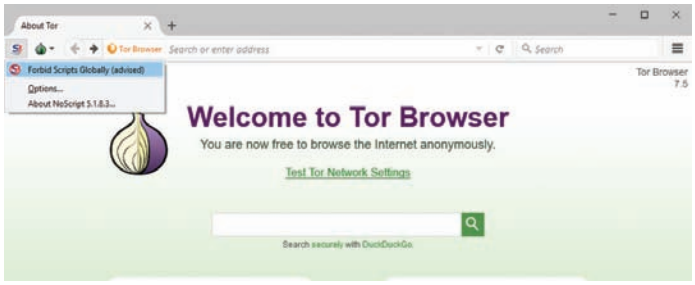
Adım 2: Açılan menüden Yeni Kimlik (New Identity) seçilir. Tor Tarayıcı tarama geçmişini temizleyecek ve yeniden başlayacaktır. Tarayıcı yeniden başladığında farklı bir IP adresinden bağlandığını görebilirsiniz.

5.3.NoScript Eklentisinin Etkinleştirilmesi

Tor Tarayıcısı NoScript eklentisi ile birlikte gelir ancak devre dışı bırakılmıştır. NoScript, zararlı web sitelerinden ve gerçek kimliğimizi Tor Tarayıcısındaki kodlar aracılığıyla ifşa edilmesine karşı ek koruma sağlar. Bu nedenle NoScript eklentisinin aktif edilmesinde fayda vardır.

Aşağıdaki adımlar izlenerek NoScript aktif edilebilir.

Adım 1: Tor Tarayıcının sol üstünde yer alan simgesine tıklanır.



Şekil 1: NoScript eklentisini etkinleştirme

Adım 2: Global Olarak Komutları Engelle (Forbid Scripts Globally) seçilir.

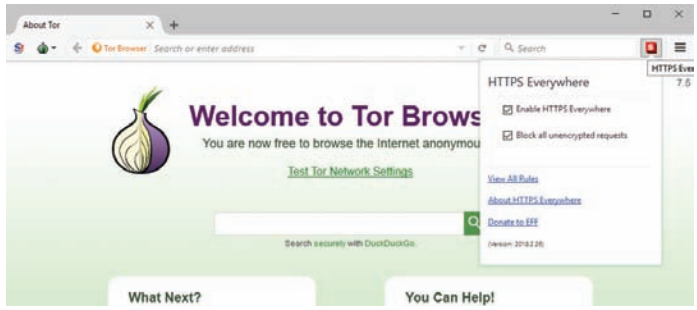
Bu ayar yapıldığında pek çok siteyi bozuk görebilirsiniz. Eğer web sitesi doğru yüklemeyi başaramaz ise şekil 1'de gösterilen tuşa tıklayarak ve geçici olarak bu sayfaya izin ver (Temporarily allow all this page) seçilerek web sitesi NoScript beyaz listesine eklenebilir.

5.4.HTTPS Everywhere Eklentisini Etkinleştirmek

HTTPS Everywhere eklentisi Tor Tarayıcı ile birlikte gelmektedir. Bu eklenti yardımıyla internette gezinirken girilen sitelerin HTTP yerine HTTPS protokolünü otomatik olarak devreye sokarak güvenli bir şekilde dolaşmamızı sağlar. Bu sayede web sitelerine gönderdiğimiz isteklerin uçtan uca şifrelendiğinden, çıkış nodları da dahil okunmadığından emin olabiliriz.

Aşağıdaki adımlar izlenerek HTTPS Everywhere eklentisi aktif edilebilir.

Adım 1: Tor Tarayıcın sağ üst köşesinde bulunan simgesine tıklanır.



Adım 2: HTTPS Everywhere'e izin ver (Enable HTTPS Everywhere) ve tüm şifrelenmemiş istekleri engelle (Block all unencrypted requests) kutucukları işaretlenir. Eğer HTTP kullanan bir siteye tekrar erişmek istersek tüm şifrelenmemiş istekleri engelle (Block all unencrypted requests) kutucuğundaki seçenek kaldırılmalıdır.

Kaynak:

https://www.torproject.org/about/overview.html.en

http://www.cs.tufts.edu/comp/116/archive/fall2016/npatel.pdf

https://boingboing.net/2016/07/01/researchers-find-over-100-spyi.html

https://en.wikipedia.org/wiki/Tor_(anonymity_network)

https://securityinabox.org/en/guide/torbrowser/windows/

Micah Lee - micah.lee@theintercept.com / Çeviri: Oğuz Aydınyılmaz - oguz@arkakapidergi.com

Haven

Edward Snowden'in yeni uygulaması laptopunuzu fiziksel olarak korumak için telefonunuzu kullanıyor![*]

Birçok gazeteci, aktivist ve yazılım geliştiricileri gibi bilgisayarımı seyahat sırasında her yere taşırım. Laptopumda doğal olarak hassas bilgileri taşımaktayım; mesajlaşma uygulaması konuşmaları, e-postalar, veritabanı parolaları, şifreleme anahtarı, yayımlanmamış çalışmalar, çeşitli hesaplara giriş yapılmış web tarayıcıları vb. Diskim şifrelenmişti fakat bunu by-pass etmek bir saldırgan için bir kaç dakika içerisinde bazı saldırı şekilleriyle (Evil Maid gibi[1]) kolayca yapılabilir. Geri dönüp güvenliği ihlal edilen bilgisayarımı kullanmaya devam etseydim, saldırgan her şeye erişebilirdi.

Edward Snowden ve arkadaşlarının bunun için bir çözümü var. Eski NSA çalışanı, bugünün itirafçısı Snowden ve ekibi, Haven adında yeni bir açık kaynaklı Android uygulaması üzerinde çalışıyor. Haven'ı yedek bir akıllı telefona yükleyip bir dizi adımdan sonra laptopunuzu uygulama üzerinden takip edebiliyorsunuz. Haven akıllı telefonun birçok sensörünü odayı gözlemlemek ve bildirilen her şeyi kayıt altına almak için kullanıyor. (Hareket sensörü, mikrofon, ışık dedektörü ve kamera) Haven'ın ilk halka açık beta sürümü resmen yayınlandı; Google Play Store'da ve Android için açık kaynaklı bir uygulama mağazası olan F-Droid üzerinden indirebilirsiniz.

Snowden, The Intercept'in ana şirketinden fon alan Basın Özgürlüğü Vakfı'nın yönettiği bir proje aracılığıyla yazılımı geliştirmeye yardımcı oluyor .Ben, Snowden ile birlikte Basın Özgürlüğü Vakfı'nın yönetim kurulundayım ve dokuz ay süren testler de dahil olmak üzere, uygulamayı geliştirmek için bazı konularda yardımcı oldum. Bununla birlikte, ürünün kusurları hakkında tam olarak bilgi sahibi olacağım ve bu makale dolayısıyla da projeye doğrudan dahil olmayan kişilerden de geri bildirim rica ediyorum.

Haven uygulaması aynı zamanda mobil cihaz güvenliği için uygulama geliştirenlerin küresel bir kolu olan Guardian Project kapsamındadır.

Haven, geleneksel olarak cihazlarında işlem yapmayı deneyen bilgisayar üreticilerinin bir problemi için harici bir çözümdür.

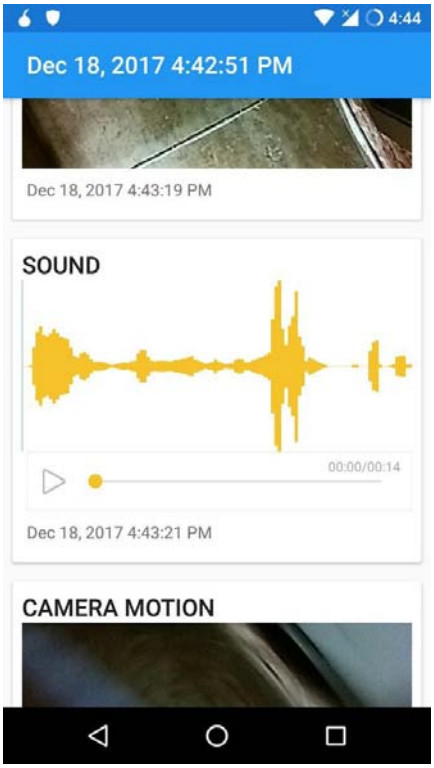
Bazı dizüstü bilgisayarlar, örneğin, bilgisayarın ön-yükleyici kodunun kötü amaçlı olarak değiştirilmediğinden emin olmaya çalışan TPM (Güvenilir Platform Modülü) adı verilen özel bir kurcalamaya dayanıklı yonga ile "güvenli önyükleme" sunar. Ama bunun yanlış sonuçlar doğuracağı çeşitli yollar bulunmaktadır: Doğrulama yapan kodda hatalar olabilir, saldırganlar kodlarını güvenilir olarak işaretlemek için bağlanabilir veya ön-yükleyiciden sonra kötü amaçlı kod eklenebilir. Bazı bilgisayar kullanıcıları kurcalama girişimi sırasında kırılacak bir çeşit mühür oluşturdular.

2009 yılında güvenlik araştırması olarak çalıştığı esnada "Evil Maid" teriminin çıkaran ve güvenli Qubes işletim sisteminin kurucusu olan Joanna Rutkowska şu sözleri konuyla alakalı dikkat çekmektedir. "Günümüz dizüstü bilgisayarlarının ve diğer bilgisayar gibi işlem yapan cihazların, günümüzde nasıl yapıldığına bağlı olarak, dizüstü bilgisayarın güvenliği ihlal edildiyse daha sonra sistematik olarak kontrol etmek neredeyse imkânsızdır. "

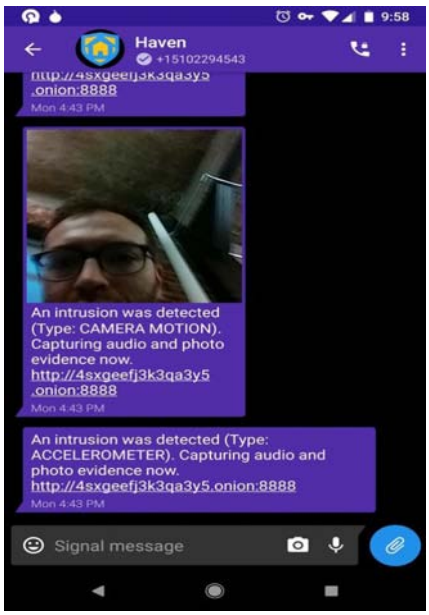
Haven'in nasıl çalıştığını bir örnekle açıklayalım: Dizüstü bilgisayarınızı bir otel kasasına kilitlediniz – kendi başına güvenli bir hareket değil – ve Haven yüklediğiniz telefonunuzu bunun üzerine yerleştirin. Birisi uzaktayken kasayı açarsa, telefonun ışık ölçeri aydınlatmada bir değişiklik tespit edebilir, mikrofonu sesi duyabilir, dizüstü bilgisayarınız hareket ettirilirse ivmeölçeri hareketi algılayabilir ve kamerası bile bu kişinin yüzünün bir fotoğrafını çekebilir. Haven uygulaması tüm bu kanıtları yüklü olduğu Android cihazına kaydeder.

1 Evil Maid Attack, Kötü Hizmetçi Saldırıs olarak çevrilebilir.Bilgisayarınızı otel odasında bırakıp, yemeğe indiğinizde odanıza otel görevlisi kılığında girebilecek birilerinin bilgisayarınıza yeni bir boot programı yüklemesi ve sizin girdiğiniz "şifreyi" çalması olarak özetlenebilecek saldırı türüdür. (e.n)

* https://theintercept.com/2017/12/22/snowdens-new-app-uses-your-smartphone-to-physically-guard-your-laptop/



Haven'ı izinsiz giriş tespit edildiği esnada, diğer telefonunuzu algıladıklarının gerçek zamanlı şifrelenmiş uyarılarını size gönderecek şekilde yapılandırabilirsiniz. Şifrelenmiş Signal bildirimleri almayı seçebilir ve ayrıca, bir Tor servis web sitesi (bir darknet sitesi) çalıştırmak için Haven'ı yapılandırabilir ve tüm uyarıları görüntülemek için başka bir cihazda Tor tarayıcısını kullanabilirsiniz. Paylaşmayı seçmedikçe, bu kaydettiğiniz kayıtlarına kimse erişemez. Haven ayrıca, ele geçirilebilen ancak bazı durumlarda daha güvenilir olabilecek SMS metin bildirimlerini de desteklemektedir.



Haven'i kullanmaktaki öncelikli amacım dizüstü bilgisayarımı Evil Maid saldırılarına karşı korumaktı ancak insanların uygulamayı kullanmakla ilgilenmesinin tek nedeni bu değildir. Electronic Frontier Vakfı'nın siber güvenlik müdürü Eva Galperin: "Haven'in tacize uğrayanlar hakkında bir şekilde casusluk yapmaktan endişe duyan ev içi taciz mağdurları için faydalı olabileceğini hayal edebiliyorum, " görüşünü bildirmektedir. Galleerin'in ana endişesi uygulamanın gerçek dışı uyarılar vermesi. Örnek olarak gerçekten hizmetçi girip eşyaları topluyorsa ve bunun için Haven uyarı veriyorsa burada bir yanlış alarm durumu olacaktır.

Haven, uzakta olduğunuzda birisi menzil içinde yürüdüğünde size fotoğraf göndermek için telefonu konumlandırarak, hırsızlık veya vandalizmi tespit etmek için ucuz bir ev veya ofis güvenlik sistemi olarak da kullanılabilir. Ya da kırsal alanlarda vahşi yaşamı izlemek ya da insan hakları ihlalleri ve kaybolmalarıyla ilgili kanıtları yakalamak için kullanabilirsiniz.

Bugüne kadar Haven'ı test etme deneyimime dayanarak, burada dikkate alınması gereken bazı şeyler var.

Haven'ı etkili bir şekilde kullanmak için kesinlikle ayrı bir Android cihazına ihtiyacınız var, ancak istemiyorsanız, bu cihazda telefon hizmeti (örneğin data ücreti, en.) için ödeme yapmanız gerekmez.

Telefon servisi olmadan Haven'ı kullanma seçeneklerini bu şekilde sıralayabiliriz:

- Bildirim almamayı seçebilirsiniz ve bunun yerine, izlediğiniz odaya geri döndüğünüzde Haven log kayıtlarını kontrol ediniz.
- Haven telefonunuzdaki bir WiFi ağına (otelin ağı gibi) bağlanabilir ve doğrudan telefondan bir Tor hizmeti web sitesini çalıştırmak için Haven'ı yapılandırabilirsiniz.
- Daha sonra bilgisayarınızda Tor tarayıcısını, Android telefonunuzda Orfox'u veya Iphone için Onion Tarayıcısını izinsiz giriş uyarılarını kontrol etmek için kullanabilirsiniz.
- Bunu yapmak için, aynı zamanda, Android için Tor olan Orbot uygulamasını da Haven telefonunuzda yüklemeniz gerekir.
- Ayrıca WiFi'ye bağlanmak ve izinsiz giriş olaylarını gerçek zamanlı Signal bildirimleri göndermek için Haven'i yapılandırabilirsiniz. Bu, uyarı bildirimlerini almanın en kullanıcı dostu yoludur. Bununla birlikte, telefon hizmeti olmadan, yeni bir Signal hesabını kaydetmek için fazladan bir telefon numarası almanız gerektiğinden, kurulum yapmak önemsizdir.

Haven'ı kullandığınız telefonunuz için telefon hizmeti (data hatta, en.) ödemesi yapmak isterseniz:

- Telefon hizmetiniz mobil veri içeriyorsa, WiFi'nin kullanılabilir olmasından endişe etmenize gerek yoktur. Aslında, WiFi'yi devre dışı bırakmanızı ve yalnızca mobil verileri kullanmanızı önermekteyiz.
- Yedek telefonun telefon numarasını kullanarak bir Signal hesabını kaydetmek için Haven uygulamasını kullanabilir, şifreli bildirimleri normal telefonunuza Signal yoluyla gönderebilirsiniz.
- Ayrıca, Haven'ın Signal hesabını kullanmak yerine izinsiz giriş olaylarında normal telefonunuza SMS bildirimleri göndermesini de seçebilirsiniz.

Eğer uzun bir süre bu takibe devam edecek olursanız, Haven telefonunuzu şarja takılı durumda tutmanız, pilin bitmemesi ve kapanmaması açısından önemlidir.

Bu, dizüstü bilgisayarınızı ve Haven telefonunuzu pilin bitmesinden çok uzun süre önce bir otelde saklayamayacağınız anlamına gelir

Dikkate alınması gereken bir başka şey de Haven'ı kurduğunuz telefonunuzun güvenliğidir.

Haven'ı kullandığınızı bilen akıllı bir saldırgan, WiFi'yi, mobil verileri ve SMS kablosuz frekanslarını engelleyerek, Haven'ın size bildirim göndermesinin önüne geçebilir. Saldırgan, local kayıtları cihazdan da silmek için telefona erişmeyi deneyebilir.

Bu nedenle, Haven'ı kullandığınız telefonunuzu kilitlemek önemlidir. Telefonunuzu güçlü bir parola ile kilitleyin ve telefonunuzun şifrelenmiş olduğundan emin olun. Kilit ekranınızı ve güvenlik ayarlarınızı Ayarlar uygulamasından değiştirebilirsiniz. Ayrıca, Android ve tüm uygulamalarınız için tüm güncellemeleri yükleyin ve Bluetooth ve NFC gibi kullanmadığınız tüm kısımları kapatın. Yapabilirseniz, mobil verileri kullanın ve WiFi'yi de kapatın. Bu, telefonun saldırı düzeyini azaltarak saldırganın odaya girdikten sonra onu hacklemesini daha da zorlaştırır.

Bir saldırgan hem Haven telefonunuzun radyo sinyallerini engelleyebilir ve hem de izinsiz giriş kayıtlarını silmek için telefonunuzu hackleyebilir, o zaman hâlâ dizüstü bilgisayarınıza yakalanmadan bir "Evil Maid" saldırısı yapmaları mümkündür.

Son olarak Haven hâlâ gelişim aşamasında. Hâlâ çözülmesi gereken pürüzler, düzeltilmesi gereken çok sayıda hata ve onu daha kullanışlı ve daha güvenilir hale getirecek birçok özellik var. Yanlış uyarılar da bulunmaktadır. Örneğin bir kullanıcı "Bir keresinde, 80'den fazla hırsız alarmı bulmaya geldim fakat bütün kayıtlar Manhattan otel odamda yüksek sesle çalışan araçların veya sirenleriyle alakalıydı. Ve bazen, gerçek olaylar gerektiğinde loglara kaydedilmiyor - Cihazımda kamera hareketlerinin hiç tetiklenmediği sorunlara rastladım, ancak bu hata şu anda benim için çözüldü." şeklinde görüş belirtmektedir. Haven uygulamasının yüksek güvenlik koşullarına güvenmeden önce olgunlaşmasını beklemek ihtiyatlı olur.

Ancak, şu haliyle bile Haven uzun bir konferansın ardından bir şeyler içmek için dışarı çıkarken dizüstü bilgisayarınızı herhangi bir gözetleme olmadan fiziksel saldırılara maruz bırakmaktan daha iyidir.

Veri Gizleme Sanatı STEGANOGRAFİ

Güvenlik deyince aklımıza ilk gelen kavramlar hiç kuşkusuz veri gizliliği (secrecy) ve mahremiyettir (privacy). Birbirine oldukça benzeyen bu iki kavram aslında bazı noktalarda farklılık gösteriyor.

Biz bir veriyi çeşitli algoritmalarla veya araçlarla şifreleyebilir yani üçüncü kişilerin anlayamayacağı bir biçime dönüştürebiliriz. Fakat bu durumda üçüncü kişiler bu verinin varlığından haberdar olur ve çeşitli yöntemler ile çözümlemeye çalışır. Veriyi bu şekilde mahrem hale getiren "Kriptografi" biliminde verimizin güvenliği, güçlü algoritmalarla etkili bir şekilde karıştırılıp anlaşılamaz hale gelmesine bağlıdır.

Bir diğer yöntem ise bu verinin varlığından bile haberdar olunmadan veriyi çeşitli yollarla gizlemek, çözümlenebilmesi için üçüncü kişilerin eline geçmesini dahi önlemektir. Bu yazımda asıl üzerinde durmak istediğim Steganografi bilimi ise bu noktada devreye giriyor.

İngilizce'de "Steganography", Yunanca'da ise "Steganos (gizli, saklı)" ve "Graphein (yazı)" kelimelerinden oluşur. Tarihi incelediğimizde yüzyıllardan beri veri gizleme ihtiyacı hep var olmuş, özellikle savaşlarda, diplomatik haberleşmelerde ve istihbarat amaçlı olarak çokça kullanılmış, çeşitli yöntemler geliştirilmiştir. Eski Yunan tarihçisi Heredot tarafından yazılmış olan Histories kitabında bulunan ilk Steganografi örneği ise Yunan ve Pers İmparatorluğu arasında geçen savaş esnasında Pers yöneticilerinden Histiaerus'ın, isyan başlatmasını istemek için kölesinin saçlarını kazıtıp gizli mesajını yazması ve saçları uzadığında bu köleyi Aristagoras'a yollaması ve mesajını iletmesi ile olmuştur.

Yine milattan önce kullanılan yöntemlerden biri olan, balmumu tabletlerin içine yazının yazılıp tekrar balmumu ile kapatılması, İkinci Dünya Savaşı'nda görünmez mürekkep kullanımı, mikro noktalama ve boş şifreleme (null cipher) teknikleri, sıradan cümleler kullanılarak gizli harflerin yerlerinden kaynaklanan yöntemler ile şifreli mesajlar iletilmesi, işkence gören bir mahkumun gözlerini açıp kapayarak mors alfabesi yoluyla iletişim kurması, sadece mor ötesi ışıkla görülebilen yazılar yazmayı sağlayan kalemler kullanılması gibi geçmişten verebileceğimiz pek çok ilginç örnek bulunmaktadır.

Peki günümüzün gelişmiş teknolojisini düşünecek olursak veri gizleme teknikleri ne kadar ilerlemiştir? Dijital dünyadaki yeni teknikler ise şu şekildedir:

- Görüntü veya ses dosyalarındaki en düşük bitlerin içerisine mesajları gizlemek
- Bir ses dosyasının yankısını değiştirmek
- Bir dosyanın görünmeyen ya da kullanılmayan alanlarına veriyi yerleştirmek

Steganografi biliminde kullanılan terminolojik bazı kavramlar ise şu şekildedir:

Taşıyıcı ya da kapak dosyası (cover): Gizli bilginin içerisine yazılacağı orijinal dosya.

Stego-medium: Bilginin saklanacağı ortam.

Gömülü (embedded/payload): Kapak dosyasında gizlenmiş veri.

Stego: Mesaj gömüldükten sonra dosyanın hali.

Steganaliz: Dosya içerisine gömülmüş veriyi tespit etme işlemi.

STEGANOGRAFİ METOTLARI

Metin Steganografi

Bu teknik oldukça basit görünmesine rağmen metin içerisine gizlenmiş veriyi bulmak oldukça zor. Öncelikle metin içerisinde cümle yapıları oluşturulur ve belirlenmiş kurallara göre harfler eklenir, boşluklar doldurulur. Metin içerisinde ifade tarzında herhangi bir hata olmaz fakat bazı kelimelerde morfolojik hatalar görülebilir. Örnek olarak, Alman bir casusun İkinci Dünya Savaşı'nda kullandığı şifreli metni inceleyelim:

"Apparently neutral's protest is thorougly discounted and ignored. Isman hard hit. Blockade issue affects Pretext for embargo on by products, ejecting suets and vegetable oils."

Her kelimenin ikinci harfini birleştirerek mesajını iletmiş:

"Pershing sails from NY June ."

Metin Staganografi'nin satır/kelime kaydırma (Line/Word shifting), açık alan (Open Spaces), karakter kodlama (encoding), semantik metotlar, kelimeler içinde özel karakter kullanımı, ilkleme (akrostiş) gibi kullanılabilecek daha birçok yöntemi vardır.

Görüntü Steganografi

En sık kullanılan yöntemlerden biri olan Görüntü Steganografi ile resmin pikselleri içerisine mesajlarımızı gizleyebiliyoruz. En az öneme sahip bite ekleme, yani "LSB (Least Significant Bit) in BMP" tekniğinde veri saklamak için ideal olan, herhangi bir sıkıştırma yapmadan resmin özelliklerini tutan 24 bitlik resim dosyası BMP (Bitmap) içerisine veriyi gizleyebiliriz. Her pikselin 24 bit olduğunu düşünürsek 2 bitlik oynamalar fark edilebilir bir değişiklik yapmayacaktır. Her pikselin renk değeri ise kırmızı yeşil ve mavi renklerini içeren 3 byte'lık alanda tutulur.

24 bitlik resmin 3 pikselinin şu şekilde olduğunu düşünürsek:

(00101101 00011101 11011100)

(10100110 11000101 00001100)

(11010010 10101100 01100011)

Her 8 bitin LSB'sini işaretlediğimizde 200 sayısının binary karşılığı olan 11001000 sayısı karşımıza çıkıyor.

(00101101 00011101 11011100)

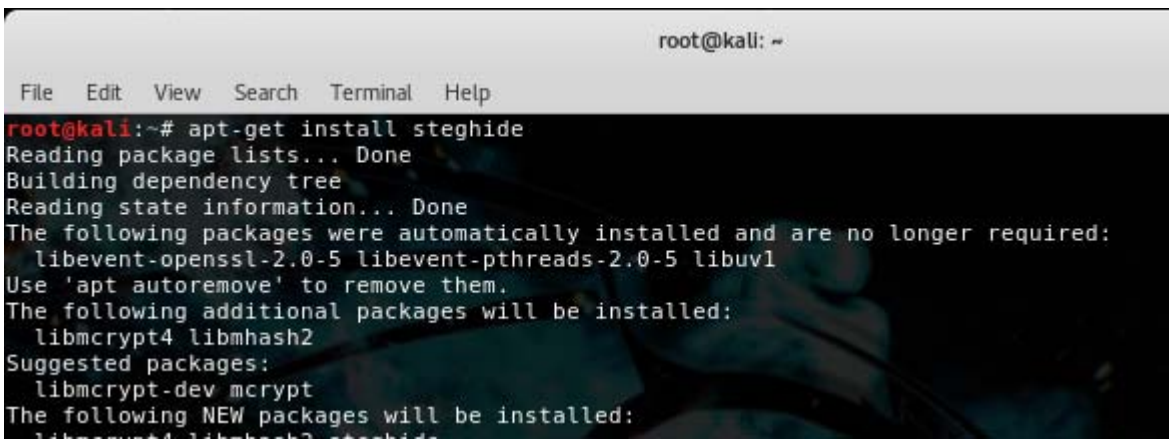
(10100110 11000101 00001100)

(11010010 10101100 01100011)

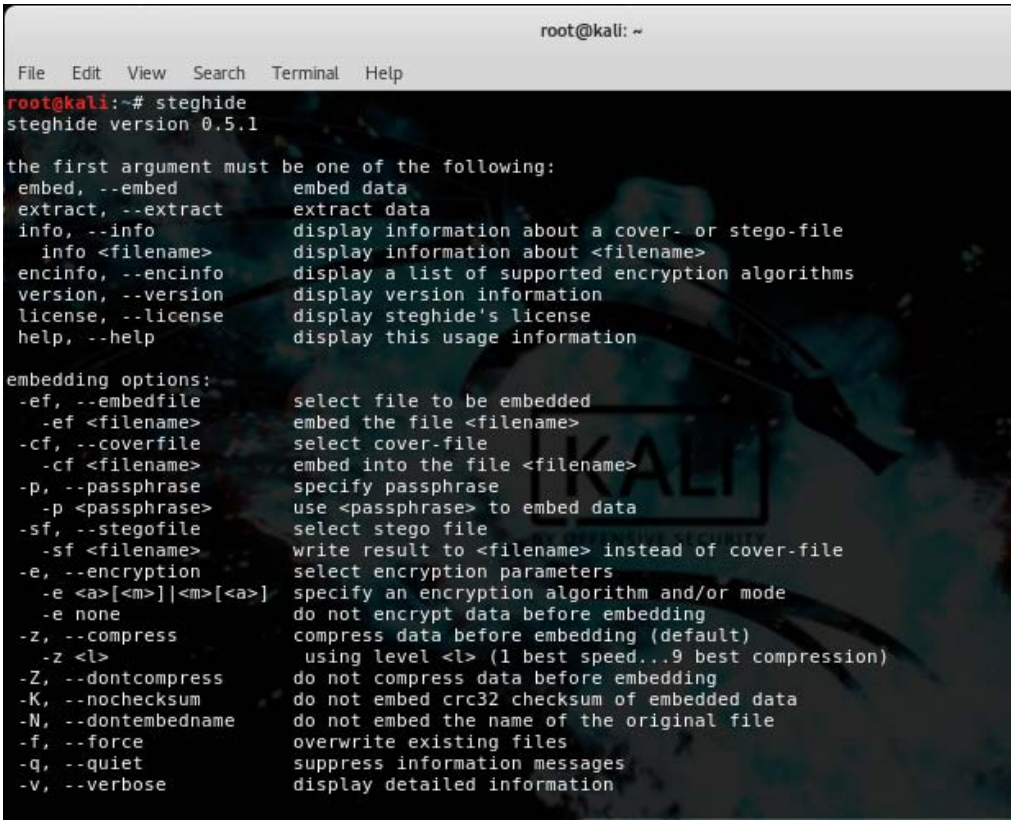
Bunun gibi LSB'ler kullanılarak harflerin binary karşılıkları ile veriler bitler içerisine kolaylıkla gizlenebilir.

Bu işlemi gerçekleştirmek için sık kullanılan Steghide aracını Linux işletim sistemimize kurarak verilerimizi nasıl gizleyeceğimizi uygulamalı olarak görelim.

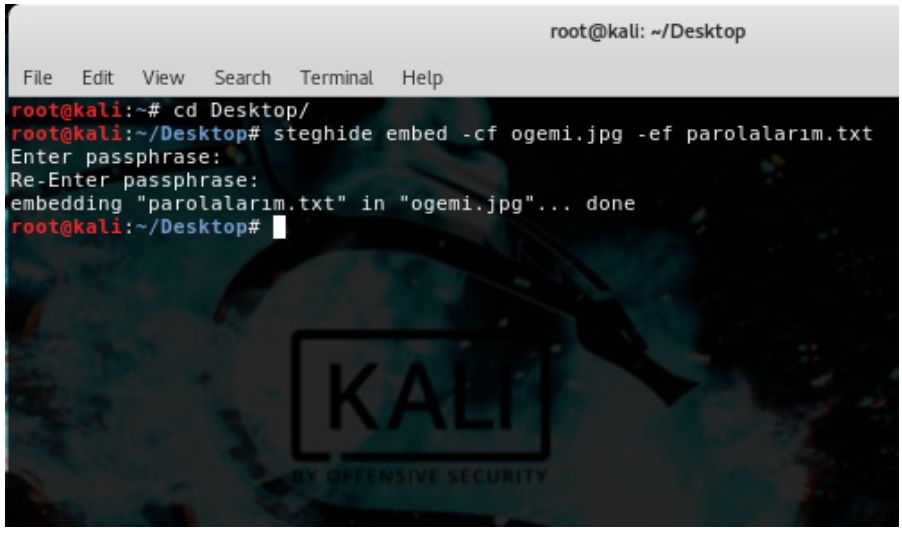
1. Öncelikle "apt-get install steghide" komutu ile aracımızın kurulumunu yapıyoruz.



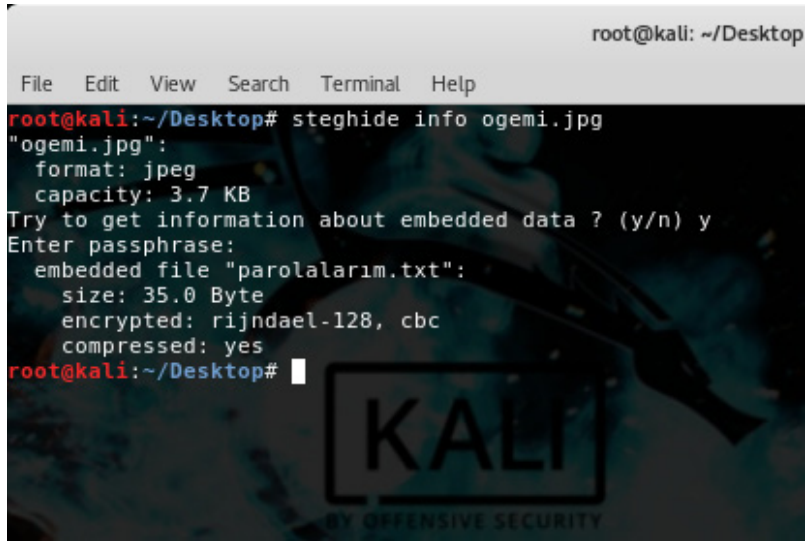
2. Kurulduktan sonra "Steghide" yazarak verimizi gizlemek için ne gibi parametreler kullanabileceğimizi görebiliriz.



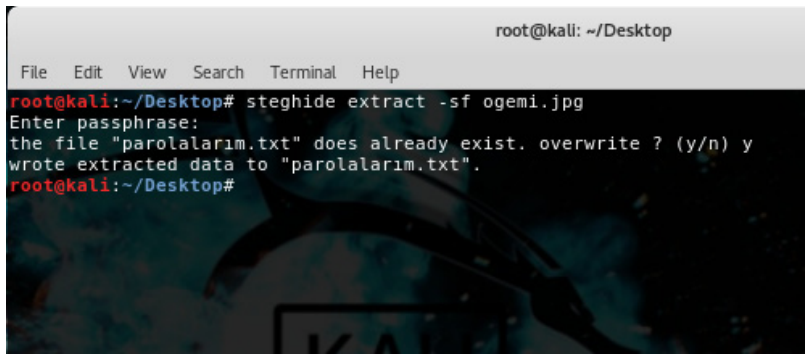
3. Ben "steghide embed -cf ogemi.jpg -ef parolalarım.txt" komutu kullanarak verilerin gizleneceği dosyayı belirtmek için -cf, hangi dosyayı gizleyeceğimizi belirtmek için ise -ef parametresini kullandım. "Embedding Options" kısmını inceleyerek eklemek istediğiniz parametreler varsa ekleyebilirsiniz. Veri gömülürken de üçüncü kişilere karşı tedbir amaçlı bir "passphrase" oluşturmamız isteniyor.



4. Text dosyamızın içeriğini o gemiye istifledikten sonra gemimizin yükünü inceleyebiliriz. Yani "steghide info ogemi.jpg" komutu ile içerik hakkında bilgi alalım.



5. Son olarak gemimizin yükünü hafifletmek ve parolalarımızı çekmek istersek de "steghide extract -sf ogemi.jpg" komutunu kullanıyoruz. Dosyayı çıkartmak için ise en başta oluşturduğumuz şifreyi giriyoruz.

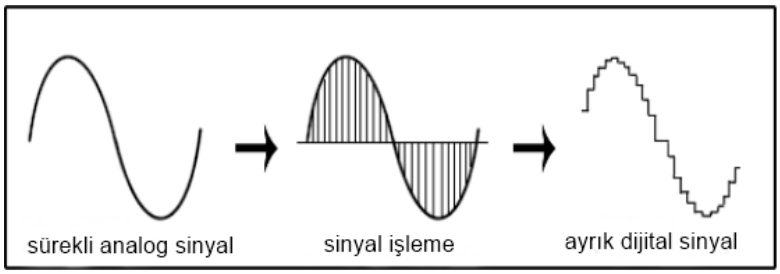


6. Son olarak resmimize baktığımızda öncesi ve sonrası arasında fark edilebilir bir değişim olmadığını görüyoruz. Yani gemimiz hâlâ kalbin derinliklerine gömülmüş bir şekilde bekliyor.

Ses Steganografi

Ses Steganografi ise bir ses dosyasında verileri gizlemeye veya güvenli ve sağlam bir şekilde işaretlemek için kullanılır. Gizli bir bilgi, ses sinyalleri kullanılarak gömülmek suretiyle gizlenmiş olur. Bu yöntem, savaş alanı iletişimi ve bankacılık işlemleri gibi bazı uygulamalarda ciddi ve hayati bir öneme sahiptir. Bu gömme işlemi de tıpkı Görüntü Steganografi'de olduğu gibi *binary* değerleri değiştirerek yapılır. Fakat görüntüden farklı olarak ses dosyası için kullanılan sinyal işleme metotları daha karmaşıktır.

Ses sinyallerini dijital ve analog olmak üzere ayırırsak dijital sesler ayrık, analog sesler ise süreklidir. Ayrık sinyaller, belirli oranlarda sürekli analog sinyalleri işlenerek üretilir. Örneğin, CD için dijital ses işleme oranı 44 kHz'dir. Aşağıdaki şekilde dijital ses sinyali dalgası oluşturmak için işlenmiş sürekli bir analog ses sinyali dalgasını göstermektedir.



Ses Steganografi Metotları

Matematik ve sinyal işleme alanındaki gelişmelerle birlikte ses dosyalarına veri gömmek için birçok metot geliştirilmiştir. Bu yüzden en sık kullanılanlar üzerinde durmak istiyorum.

LSB (Least Significant Bit) Kodlama Metodu

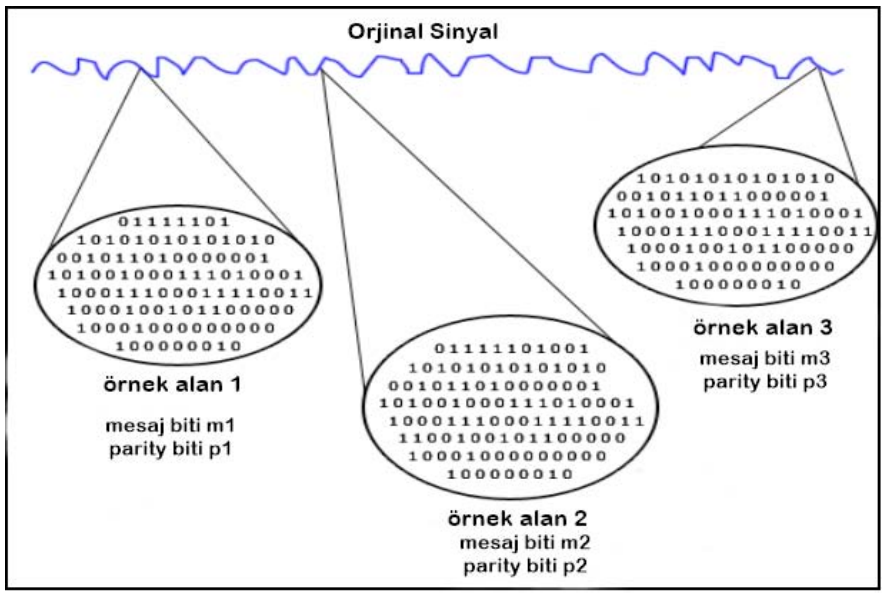
Görüntü Steganografi'de de belirtmiş olduğum gibi en sık kullanılan ve en kolay yöntemlerden biri olan LSB kodlama ses dosyaları için de şüphesiz aynı öneme sahip. Ses dosyaları için nasıl olduğunu yine bir örnekle inceleyecek olursak aşağıdaki tabloda "Hi" kelimesinin binary karşılığının LSB ile kodlandığını görüyoruz.

Audio stream sample (16-bits)	"Hi" in binary	Stego audio Stream (w embedded message)
1 1 0 1 1 1 0 1 1 1 0 0 1 0 0 1	0	1 1 0 1 1 1 0 1 1 1 0 0 1 0 0 **0**
0 0 0 1 1 0 0 0 0 1 1 0 0 1 1 0	1	0 0 0 1 1 0 0 0 0 1 1 0 0 1 1 **1**
1 1 1 0 0 1 0 1 1 1 0 1 1 0 1 0	0	1 1 1 0 0 1 0 1 1 1 0 1 1 0 1 **0**
0 0 0 1 1 0 0 0 0 1 1 0 0 0 0 0	0	0 0 0 1 1 0 0 0 0 1 1 0 0 0 0 **0**
1 1 1 0 0 0 0 1 1 1 0 1 0 1 1 0	1	1 1 1 0 0 0 0 1 1 1 0 1 0 1 1 **1**
0 0 0 0 1 0 1 1 0 0 1 0 0 0 0 0	0	0 0 0 0 1 0 1 1 0 0 1 0 0 0 0 **0**
1 1 1 1 1 0 0 0 1 1 0 0 0 1 1 1	0	1 1 1 1 1 0 0 0 1 1 0 0 0 1 1 **0**
0 1 0 0 1 1 1 1 0 1 0 1 1 0 1 0	0	0 1 0 0 1 1 1 1 0 1 0 1 1 0 1 **0**
0 1 0 0 0 0 0 0 0 1 1 0 0 0 1 1	0	0 1 0 0 0 0 0 0 0 1 1 0 0 0 1 **0**
0 0 1 1 1 0 1 1 0 1 0 0 1 1 1 0	1	0 0 1 1 1 0 1 1 0 1 0 0 1 1 1 **1**
0 1 1 0 0 0 0 0 0 0 1 1 0 0 1 0	1	0 1 1 0 0 0 0 0 0 0 1 1 0 0 1 **1**
1 0 0 0 1 1 0 1 0 1 0 1 1 1 0 0	0	1 0 0 0 1 1 0 1 0 1 0 1 1 1 0 **0**
0 1 1 0 0 0 1 0 1 0 1 0 0 0 1 0	1	0 1 1 0 0 0 1 0 1 0 1 0 0 0 1 **1**
1 1 0 0 1 0 0 0 0 1 0 0 0 0 0 0	0	1 1 0 0 1 0 0 0 0 1 0 0 0 0 0 **0**
0 0 0 0 0 0 1 0 1 1 1 1 1 1 0 1	0	0 0 0 0 0 0 1 0 1 1 1 1 1 1 0 **0**
1 1 0 1 1 1 0 0 1 1 0 0 0 1 0 1	1	1 1 0 1 1 1 0 0 1 1 0 0 0 1 0 **1**

Bu yöntem ile ses düzeyindeki değişiklikler kulağımızla algılayamayacağımız seviyededir. İnsan kulağının duyamayacağı 20.000 Hz. üzerindeki frekanslar ayarlanarak mesajlar gizlenir.

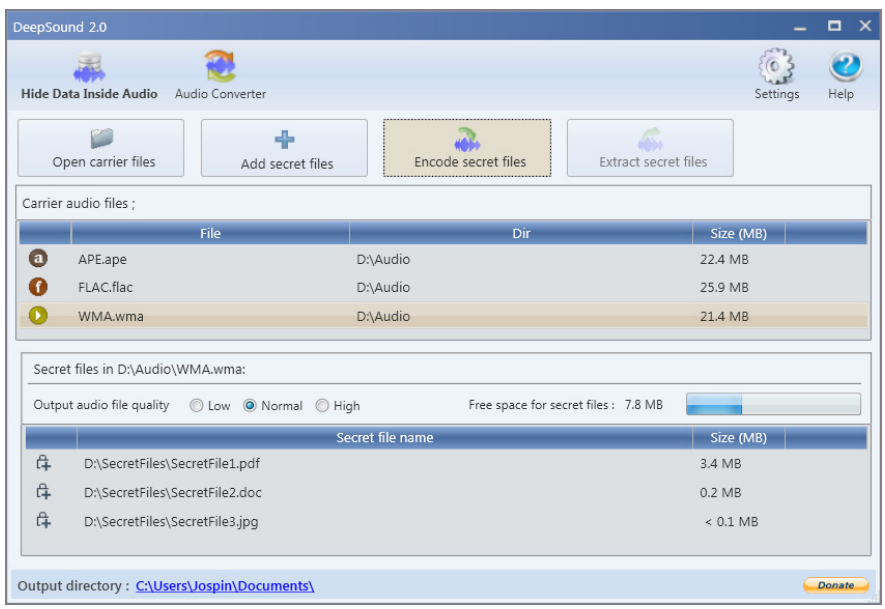
Eşlik biti (Parity) Kodlama Metodu

Parity kodlamasında ise ses sinyali ayrı örnek alanlarına ayrılır ve her mesaj bir eşlik biti içindeki alanda gizlenir. Bu nedenle, bu metot bitleri gizlemek için daha geniş bir seçenek yelpazesi sunar ve sinyaldeki değişimi daha gözlemlenemez hale getirir.



Bu tekniklerden farklı olarak faz kaymaları kullanılarak veri gizlemeye yarayan Faz Kodlama (Phase Coding) tekniği, ses sinyalinin frekans spektrumu boyunca gizli verileri mümkün olduğunca maksimum seviyede dağıtmaya çalışan Yayılı Spektrum (Spread Spectrum) tekniği ve gizli verinin ayrık bir sinyale eko eklenerek bir ses ortamına sokulmasını sağlayan Eko Gizleme Tekniği gibi yöntemler de mevcuttur fakat ayrıntıya girmeden bu işlemi hangi araçlarla nasıl yapabileceğimizden bahsedeceğim.

Teknik bilgiden biraz pratik bilgiye geçiş yapalım. Eğer Mr. Robot dizisini izliyorsanız 1. Sezon 8. bölümde Elliot'un DeepSound aracını kullanarak verileri ses dosyaları içerisine nasıl sakladığını da görmüş olmalısınız.



DeepSound aracında "*Open carrier files*" seçeneği ile ses dosyasını seçip, "*Add secret files*" seçeneği ile de saklamak istediğimiz dosyayı ekliyoruz. Ses kalitesini istediğimiz gibi ayarlayıp "*Encode secret files*" dediğimizde veriyi gömmeden önce istediğimiz formatı seçip şifre belirledikten sonra da işlem tamamlanmış oluyor. Veriyi sakladığımız ses dosyasını tekrar programda açtıktan sonra "*Extract secret files*" dediğimizde ise gizli veriye ulaşmış oluyoruz.

Steghide ve *DeepSound* dışında elbette onlarca araç geliştirilmiş durumda. *QuickStego*, *StegFS*, *StegoShare*, *Outguess*, *Stegbreak*, *Zsteg*, *OpenStego*, *Matroschka*, *AudioStegano*, *BitCrypt*, *MP3Stego*, *Xiao*, *Crypture*, *SteganographX Plus*, *rSteg*, *SSuite*, *Picsel*, Camouflage, *Hide'N'Send* bunlardan sadece bazıları. Bu saydığım araçların içerisinde hem görüntü hem de ses dosyaları için geliştirilmiş olanları da bulunuyor.

Steganografi metin, ses, resim ya da video dosyalarına telif hakkı sağlamak amacıyla damgalama (watermarking) işlemlerinde de kullanılır. Dijital damgalama görünür ve görünmez olmak üzere ikiye ayrılır. Görünen damgalama, herhangi bir resmin köşesinde bulunan logo olabilir. Görünmeyen damgalamada ise kişiye özel veriler ona sahiplik oluşturması açısından dosyaya gömülür.

Son olarak Steganaliz ise bir taşıyıcı dosya içerisinde, saklanmış bir bilgi olup olmadığını bulmayı, eğer var ise bu bilgiyi elde etmeyi amaçlayan ve steganografik sistemlere karşı yapılan analiz ve araştırmalara denir. Pasif (tarama) ve aktif (bozma/yok etme) olarak ikiye ayrılır. Steganalistler çeşitli steganografik saldırılara karşı incelemeler yaparlar. Bu saldırı tipleri ve amaçları kısaca şu şekildedir.

File only:	Saldırganın dosyaya erişimi vardır ve içeride gizlenmiş bir mesaj olup olmadığını belirlemeye çalışır.
File an Original copy:	Saldırgan şifrelenmiş mesajın bir kopyasına ve orijinalinin bir kopyasına sahip olabilir.
Reformat Attack:	Dosyanın biçimi değiştirilir.
Compression Attack:	Sıkıştırma algoritmaları ile gereksiz bilgiler bir dosyadan kaldırılmaya çalışılır.
Visual Attack	Bir insanın görsel anormallikleri aramasına izin verecek şekilde nesnenin bir kısmını saran stego-only-ataktır.
Structural Attack	Saldırgan, bitlerin istatistiksel profilini inceler bir mesajın varlığını tespit edebilir.
Statistical Attack	Potansiyel bir kapak dosyasının frekans dağılımının, kapak dosyasının teorik olarak beklenen dağılımı ile karşılaştırılmasıdır.

Geçmişten günümüze Steganografi sanatının tarihsel sürecini incelediğimizde ne kadar mesafe katettiğini açıkça görebiliyor, gelecekte de hızla ilerleyip yepyeni tekniklerle karşımıza çıkabileceğini de tahmin edebiliyoruz. İnsanlar için gizlilik ve mahremiyetin oldukça önemli olduğunu düşünürsek Steganografi ve Kriptografi bilimleri birbirlerini tamamlayarak hayatımızda önemli ve vazgeçilmez bir yer kaplıyor.

Kaynakça:

- http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.401.5678&rep=rep1&type=pdf
- http://resources.infosecinstitute.com/steganography-and-tools-to-perform-steganography/#gref
- https://www.slideshare.net/UttamJain/steganography-14902856
- http://steganography-info.blogspot.com.tr/2008/04/steganography-and-attacks.html

Saman Altından Okyanus Yürütmek

DNS Tünelleme ile Engelleri Aşın

Farz edin ki bir havaalanındasınız, ya da büyük bir kent meydanında kendinizi epey yalnız hissedip internete bağlanmak istediniz.

WiFi alıcınız civarda erişime açık onlarca modem gösteriyor. Kendinizi şanslı hissediyorsunuz.

Modemlerden birine bağlanıp, bir web adresini örneğin www.arkakapidergi.com'u ziyaret etmek istediğinizde olan oluyor! Sizi karşılayan bir ekran, üyelik bilgilerinizi girmenizi istiyor. Üyelik bilgileriniz yok, biliyorum! Ama hemen sayfanın altındaki New User (Yeni Kullanıcı) linkine tıkladığınızda, bir Arka Kapı okurunun keyfini kaçıracak bilgiler talep eden bir form sizi karşılıyor. TC kimlik numaranızdan, GSM numaranıza kadar pek çok bilgi talep ediliyor.

Kalabalıklar içinde yeniden yalnızsınız!

Hemen enseyi karartmayın. Bu yazımızın amacı, DNS Tünelleme yöntemini kullanarak bu tarz engelleri aşıp, internet gezinimine devam edebilmek.

Peşinen söyleyeyim! Yazıda anlatılanlar eğitim amaçlı olup, talimatlarla birlikte kurulacak programlardan, oluşacak zararlardan müessesemiz sorumlu değildir.

Bu sihirli yöntemi anlamanın yolu DNS'i anlamaktan geçiyor. DNS, internetin telefon defteri olarak bilinen bir protokol. Bu benzetmenin çok sıradanlaştığının farkındayım! Üstelik yazıyı okuyan 90 kuşağının sarı telefon defterlerini neredeyse hiç görmemiş olduğundan da eminim ama daha iyi benzetme buluna kadar en iyisi bu!

İnternette bir siteyi ziyaret etmek istediğimizde bu sitenin adresini, tarayıcımızın adres çubuğuna yazarız. Siz daha kahvenizi yudumlamadan ziyaret etmek istediğiniz siteyi karşınızda bulursunuz ancak, arkada muazzam hızlarda gerçekleşen bir veri alışverişi vardır. Nedir bu veri alışverişi? www.arkakapidergi.com yazıp enter'a bastığınızda tarayıcınız bu domain adresine (alan adına) karşılık gelen IP adresini bulmaya çalışır. IP adresini bulduktan sonra HTTP paketi bu adrese gönderilir. Daha fazla basitleştirmeye kalkarsam yazıyı epey uzatacağım. Arka Kapı Dergi'nin 1. Sayısında Ömer Çıtak'ın kaleme aldığı *"Güvenli Bağlantım" ile Kendi VPN Sunucunuzu Kuru*n yazısında bu detaylar var.

DNS Resolution dediğimiz bu işlem neredeyse tüm güvenlik mekanizmaları tarafından masumane görülen bir işlemdir. Çünkü hepi topu bir alan adına karşılık gelen IP adresi bilgisi sorulmakta ve cevap alınmaktadır. Aynı şekilde sizden erişim için kâh şahsi bilgilerinizi, kâh bir ücret ödemenizi isteyen bu hotspotlar, WiFi modemler de aynı varsayımı çoğunlukla tekrarlarlar. Oysa DNS protokolünde bulunan pek çok özellik, bu masumane kapıdan koca bir internet trafiğinin akmasına imkân verebilir. Deyim yerindeyse saman altından okyanuslar yürütebilirsiniz!

Haydi aşağıdaki gibi bir senaryo düşünelim.

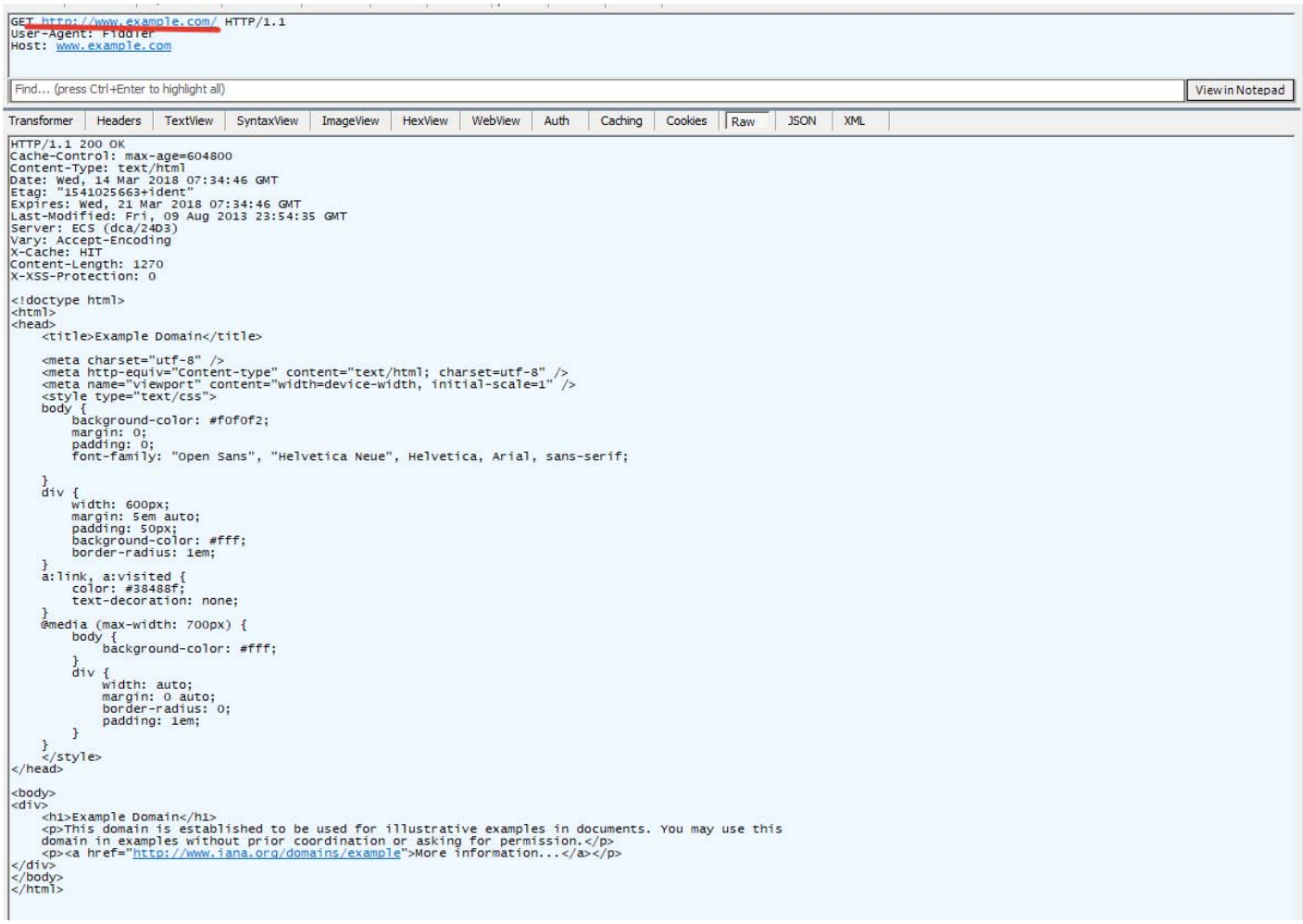
Kendi kontrolümüzde bir DNS sunucusunu kuralım. Mesela *freenet.arkakapidergi.com*'un NS kayıtları bu DNS sunucusuna işaret etsin. 53 numaralı portu dinleyelim. (DNS protokolünün varsayılan port numarası).

Yukarıda sözünü ettiğimiz bağlantı koşullarında bir web sitesi ziyaret edilmek istendiğinde öncelikle bu web adresini base64 ile encode edelim ve bir subdomain isteği olarak *freenet.arkakapidergi.com* domain'ine ekleyelim. Yani *example.com*'u ziyaret edecek isek:

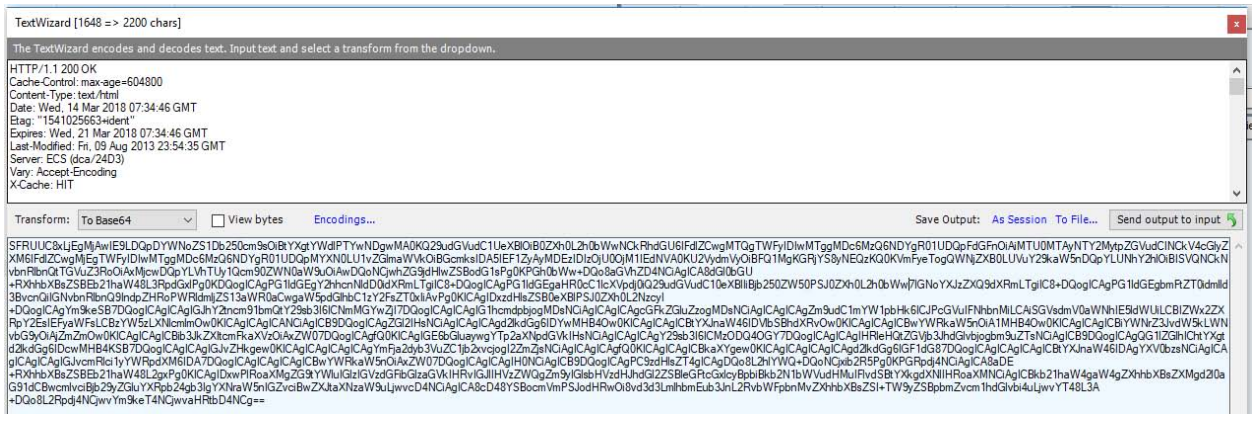
example.com'un base64 encode hali: ZXhhbXBsZS5jb20=

yani ziyaret edeceğimiz URL: *ZXhhbXBsZS5jb20=.freenet.arkakapidergi.com* olsun

freenet.arkakapidergi.com'un DNS adresi de kendisine gelen bu DNS çözümleme isteğinin maksadını biliyor. Aslında istenen *ZXhhbXBsZS5jb20=.freenet.arkakapidergi.com*'e karşılık gelen IP adresi değil example.com'un içeriği. Dolayısıyla DNS isteğini cevaplandırırken, DNS kayıtlarının arasına example.com'un içeriğini yine base64 ile encode ederek göndersin:



Bu HTTP yanıtını base64 ile encode eden sunucu aşağıdaki değere ulaşıyor:



Bu base64 encode edilmiş datayı DNS sorgu sonucu olarak gönderiyor. Client'da yani istemci taraftaki biz ise, bu gelen yanıtı derhal decode ederek *example.com* isteğine dönen sonucu elde edip, tarayıcımızda görüntüleyebiliyoruz.

Gözünüz korkmasın! Bütün bu işlemleri sizin yerinize yapan bir araç *iodine* kullanarak DNS Tünelleme gerçekleştireceğiz. Tünellemenin ardında yatan işleyiş zihinlerde billurlaşsın diye bu noktalara değinmek istedim.

Bu işlem için öncelikle bir sunucu ve bir de alan adına ihtiyacımız var. Alan adımız *arkakapidergi.com*. Ama biz *arkakapidergi.com*'un işleyişini bozmamak için *freenet.arkakapidergi.com* subdomaini üzerinden tünellemeyi gerçekleştireceğiz.

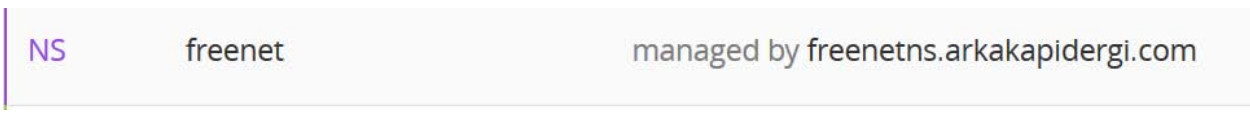
Bütün sistem DNS protokolü üzerinden yürüdüğü için öncelikle DNS ayarları ile başlıyoruz. *arkakapidergi.com*'a iki adet DNS kaydı gireceğiz. Bunlardan biri *freenet.arkakapidergi.com* için NS kaydı, yani Name Server kaydı. Bu şu demek: *freenet.arkakapidergi.com* adresine farklı subdomainler ile erişilmeye çalışıldığında bu istekler hangi nokta üzerinden yakalanacak ve yukarıda adım adım tarif ettiğimiz operasyon gerçekleşecek. Bu elbette ki *iodine* programını kurduğumuz sunucu üzerinden yakalanacak. *iodine*'i yükleyeceğimiz sunucunun IP adresi X.X.X.X olsun. Hatta bu DNS sunucumuza da bir ad verelim *freenetns.arkakapidergi.com* olsun.

Şimdi iki DNS kaydı girmek zorundayız. İlk kaydımız *freenetns.arkakapidergi.com* adresinin işaret ettiği sunucu, yani Iodine'in yüklü olduğu sunucu için. Bunun için A tipinde bir DNS kaydı giriyoruz. Domain adresi de *freenetns* olarak yazılmalı.

Ben DNS kayıtlarını Cloudflare üzerinden giriyorum.

Şimdi esas noktaya geldik. Yani subdomainler nasıl işlenecek. Elbette ki Name Server, yani DNS sunucusu yoluyla. Hangi subdomainlerin olacağını bilemeyiz. Çünkü kullanıcının ziyaret etmek istediği site adreslerinin base64 ile encode edildiğini ve subdomain'i oluşturulduğunu söyledik. Dolayısıyla statik subdomainler tanımlamak yerine, biz sadece *freenet.arkakapidergi.com* için NS kaydı yani Name Server kaydı gireceğiz. Sonrasında *freenet.arkakapidergi.com*'a yapılan tüm subdomain istekleri bu DNS sunucusuna sorulacak ve yanıt alınacak.

O zaman *freenet.arkakapidergi.com* için bir NS kaydı giriyoruz. Bu kayıt yukarıda tanımladığımız *freenetns.arkakapidergi.com*'a işaret etsin:



Şimdi operasyonun ikinci aşamasına geldik. Kendi yönetimimizde olan ve X.X.X.X IP'sine sahip sunucumuza *iodine* programını kuracağız.

Ben aşağıdaki terminal işlemlerinin tamamını Ubuntu sunucum üzerinde gerçekleştiriyorum. Paket yöneticileri (Örneğin *apt-get*, *brew* vb) farklı olabilir ancak temel işleyiş aynıdır.

Başlarken paket yöneticisini güncellemekte fayda var. Ben DigitalOcean'dan aldığım (Teşekkürler Ömer!) droplet'da kurulumu yaparken *iodine* paketinin olmadığını gördüm.

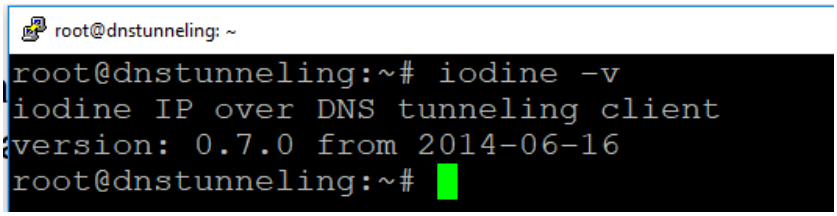
Dolayısıyla önce paket yöneticisini güncelleyelim:

```
apt-get update
```

Güncelleme sonrası *iodine*'i kurabiliriz:

```
apt-get install iodine
```

Kurulumu doğrulamak için yine komut satırından *iodine -v* yazıp versiyon bilgilerini elde edebilirsiniz:



Şimdi iodine'i başlatma zamanı. Aşağıdaki komut ile iodine'i sunucumuzda başlatıyoruz:

```
iodined -f  -P acilsusamacil 10.0.0.1 freenet.arkakapidergi.com
```

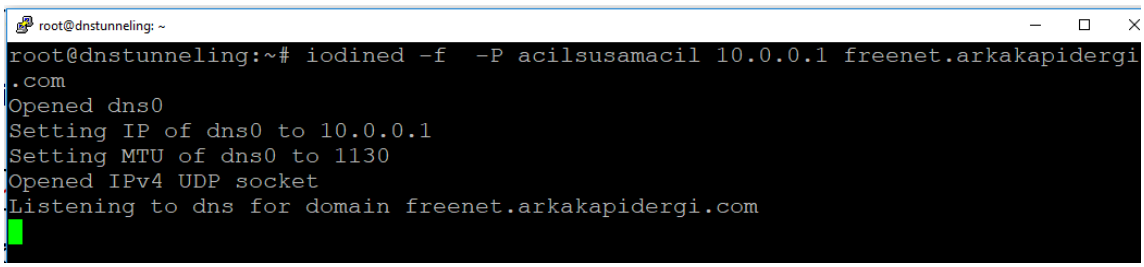
Parametreleri açıklayalım:

-f : foreground yani terminal ekranında *iodine* çalışmaya devam eder. Process'i çok kolaylıkla CTRL+C tuş kombinasyonları ile durdurabilirsiniz. Aksi halde, background modda çalışır. *iodine* komutunun çalışmasından hemen sonra terminal komut satırına düşer. Arka planda çalışmaya devam eder.

-P: Tünelimiz yol geçen hanı olmasın diye bir parola koyuyoruz: *acilsusamacil*

10.0.0.1 sunucumuzda *iodine*'in kullanacağı interface'in IP'si. *iodine* ile bizim istemci makinemiz arasında farklı bir network arayüzü üzerinden ağ kurulumu gerçekleşecek. Bizim istemci makinemiz muhtemelen 10.0.0.2 ya da 10.0.0.3 IP'sini alacak.

freenet.arkakapidergi.com: Tüm isteklerin artık kendisine bir DNS isteği olarak aktarılacağı domain.

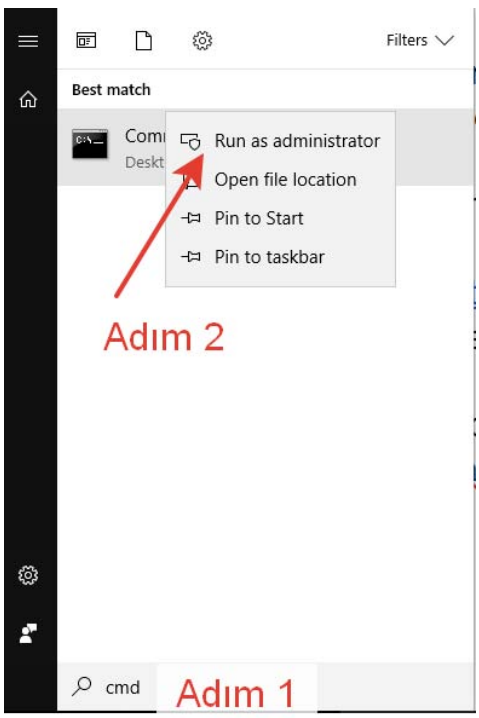


Şimdi sıra istemci, yani bizim kendi kullandığımız makinede. Herkese hitap edebilmek adına istemci makineyi bir Windows 10 makine olarak düşündüm.

Öncelikle Windows 10 makinemiz için *iodine* client'ı yükleyelim:

http://code.kryo.se/iodine/ adresine giriyoruz win32/64'ü seçiyoruz. Kurulum derhal başlıyor. Hepi topu 243 KB'lik bir dosya. Bu satır bitene kadar indi bile!

İndirdiğimiz ZIP dosyasını extract ediyoruz. Komut istemcisini Administrator yönetici olarak başlatıp, *iodine*'in yüklü olduğu dizine gidiyoruz:



Komut istemcisi açıldığında iodine'in yüklü olduğu klasöre gidiyoruz ve aşağıdaki komutu çalıştırıyoruz:

```
iodine.exe -f -P acilsusamacil freenet.arkakapidergi.com
```

-f ve -P komutları, *iodined* programında açıkladığımız fonksiyonlara sahip.

Not: IP adresini X.X.X.X olarak değiştirdim.

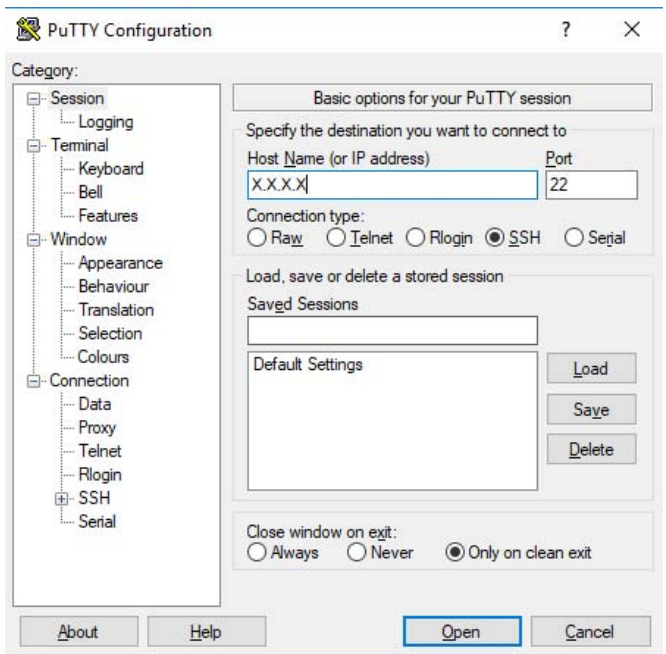
Geriye iki adımımız kaldı.

Artık istemci ve sunucu arasında bir tünel var. Şimdi örneğin tarayıcıdaki web gezinimini bu tünele aktarmamız gerekiyor. Bunu yapmanın pek çok yolu var. Ben en basit olarak Putty ile bir SSH bağlantısı kurup, bunu bir lokal bir porta bağlayarak, tarayıcı üzerinden socket bağlantısı kurmayı anlatacağım.

Makinizde Putty kurulu mu? Değilse lütfen aşağıdaki adresten Putty'nin en güncel sürümünü yükleyiniz:

https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

Putty'i açıyoruz. Konfigürasyon ekranından X.X.X.X (sizin sunucu IP'niz ne ise onu yazmalısınız.) adresine 22 numaralı porttan bir SSH bağlantısı yapacağımızı belirtiyoruz:

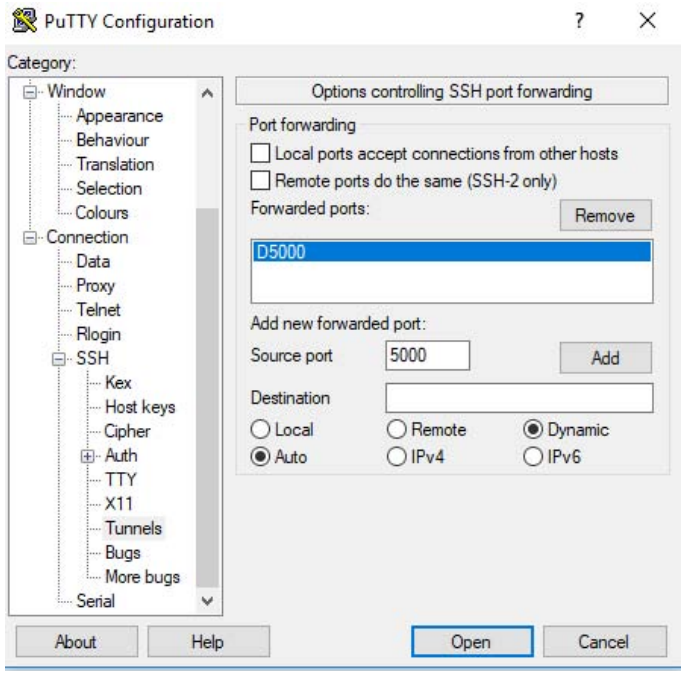


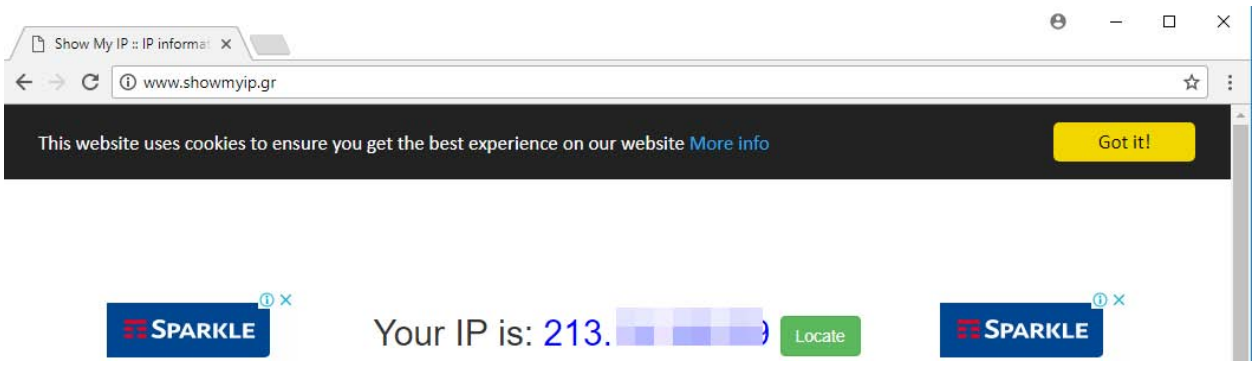
Bitmedi. *Connection->SSH->Tunnels* altından ufak birkaç ayar daha yapmamız gerekiyor:

Açılan ekrandan *Source Port*'a 5000 yazıp, *Destination* kısmından *Dynamic*'i seçip *Add* butonuna basınız. *Forwarded Ports* alanında *D5000* değerini göreceksiniz.

Open butonunu tıklayarak bağlantıyı açıyoruz. Terminal ekranından sunucumuza erişim için gerekli bilgileri giriyoruz. Her şey tamamsa, artık tarayıcı bağlantısını kendisine aktaracağımız Socket bağlantısı tamam, demektir.

Tarayıcıyı ayarlamadan önce son bir kontrol daha yapalım. Şu an bağlantımızın tünel üzerinden değil de, normal bir biçimde seyrettiğini teyit etmek için www.whatismyip.com ya da www.showmyip.gr'u ziyaret edip, IP bilgimizi kontrol edelim:



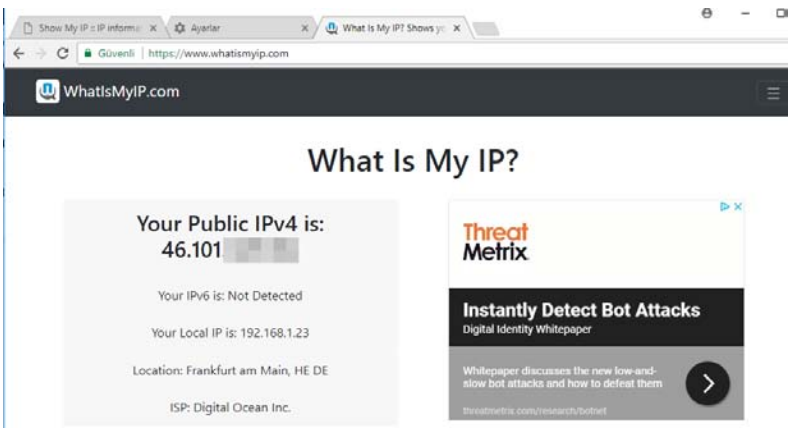


Gördüğünüz üzere IP adresimiz 213… ile başlıyor. Şimdi tarayıcımızın SOCKS ayarlarını yapalım.

Chrome adres çubuğuna *chrome://settings/* yazarak, Chrome ayarlarına ulaşabilirsiniz. Web sayfasından Gelişmiş ayarları görüntüleyerek *Proxy Ayarlarını Aç* seçeneklerini kullanınız.

SOCKS değerlerinden adres alanına 127.0.0.1, port alanına 5000 yazarak OK diyoruz. Her şey hazır!

Şimdi web üzerinden gezinim yaptığımız adresimizi tekrar kontrol edelim:



Tebrikler! Artık Chrome tarayıcıdaki tüm trafiğiniz DNS Tünel üzerinden akacak.

Andiodine tool'unu kullanarak Android mobil cihazımızı DNS Tünel sunucumuza bağlayabilir, mobil cihazınızda da DNS tünellemenin keyfini sürebilirsiniz.

Koray Peksayar - Röportaj: Şahin Solmaz - sahin@arkakapidergi.com

KEVIN MITNICK'TEN BYLOCK'A KADAR HTS, CGNAT, METADATA ve DAHA FAZLASI!

Bir zamanların ünlü hacker'ı, FBI'ın arananlar listesinde başı çeken, deyim yerindeyse FBI'la dans eden Kevin Mitnick'in, nam-ı diğer Karanlık Korsan'ın, evini basmaya gelecek FBI ajanları için yaptığı o küçük ve tatlı şakayı biliyor muydunuz?

Hükümetin Kevin'ı takip ettiği sıralarda, birgün Kevin, ajanların kendisine ne kadar yakın olduklarını merak eder ve Los Angeles'taki hücresel servis sağlayıcısına sızarak, onu izleyen FBI ajanlarının, cep telefonu numaralarını, kimleri aradıklarını ve kimlerin onları aradığını ve o an nerede olduklarını fiziksel olarak tespit eder! Akabinde, evde FBI'ın ilgilenebileceği ne varsa hepsini temizler. Tabii Karanlık Korsanımız, davetsiz misafirleri için tatlı bir şaka hazırlamayı da ihmal etmez; hemen donut satan bir mağazaya gider, çeşit çeşit donutlar alır ve bunları büyük bir kutu içinde paketler. Eve gelir, paketin üzerine "FBI Donuts!" yazar, kutuyu buzdolabına yerleştirir ve ortadan kaybolur. Ne kadar da kibar ve misafirperver değil mi? :)
Bkz: Kevin Mitnick: How to Troll the FBI - youtube.com/watch?v=Nn3O8XD1z0w

İşte biz de bu yazımızda Adli Bilişim Uzmanı Koray Peksayar ile bu güzel hikâyenin teknik tarafında neler var, yazının başlığında ByLock'un ne işi var, bu konuyla ortak paydası nedir? Balyoz ve Ergenekon davalarında benzer "teknik deliller" söz konusu muydu? Bu HTS, CGNAT, metadata etrafında ilgili hadiseleri enine boyuna ele alıyor olacağız.

Koray Peksayar, **Balyoz**, **Ergenekon** ve **ByLock** davalarındaki "dijital delillerde" rastlanan çelişkilere teknik bulgularıyla dikkat çeken ve bu davaların aydınlatılmasında aktif rol alan, mahkemelere yol gösteren yeminli bilirkişilerden!

Koray Bey, bugün sizinle Balyoz ve Ergenekon hadiselerinde yer yer duymuş olduğumuz metadata ve 15 Temmuz hadiselerinde ise pek çok kez duymuş olduğumuz HTS ve CGNAT kayıtlarının önemi, talep ve süreçleri nelerdir, bu verilere ne kadar güvenilebilir? Başlıca bu konular hakkında konuşmak istiyoruz.

Nedir bu HTS kayıtları ve neleri barındırır, diye başlayalım isterseniz.

Tabii, Historical Trafic Search (HTS), geçmiş tarihli GSM şebekesine ait kayıtlardır. Temelde iki çeşittir; birincisi, GPRS WAP denilen data şebeke kayıtlarıdır. İkincisi ise ses - arama, SMS, MMS hareketleri olduğu zaman kimin kimi, ne zaman, kaç kez, nereden aradığı, görüşmenin ne kadar sürdüğü ya da kimin kime, ne zaman ve nereden mesaj gönderdiği gibi verileri barındırır. Ancak günümüzdeki hali ile muhasebesel (faturalandırma özeti için tutulan kayıtlar) olduğunu söyleyebilirim.

--- HTS kayıtları her GSM abonesini kapsar, sabit hatlar için de görüşme kayıtları olarak tutulur. ---

Peki HTS kayıtları ne sıklıkla güncelleniyor? Örneğin bu kayıtlara göre biz şu an neredeyiz acaba?

HTS kayıtlarının güncellenmesi için bir HTS aktivitesinin gerçekleşmesi (az önce bahsettiğimiz verilerden birisinin gelmesi ya da gitmesi) gerekir. En son bu aktivite nerede gerçekleşti ise oradasınız demektir. Yani güncellenme sıklığı bu hareketlerden birisinin gerçekleştiği her andır.

Peki CGNAT nedir ve CGNAT kayıtları ne sıklıkla güncellenir?

CGNAT, Carrier-Grade NAT, yani taşıyıcı seviyesinde adres dönüştürme tekniğidir ve bunu da NAT'teki tutulan ARP tabloları vs. kullanımından ziyade insanlara atanmış internet IP'lerine ait TCP/IP portlarından 64510 tanesini teknik olarak adil olarak paylaştırmak için kullanılan tekniktir.

İnternet erişiminin ve veri alışverişinin olduğu her an güncellenir. Örneğin, akıllı cihazınızda, internet bağlantınız açık ve kullandığınız uygulamalar arka planda sürekli olarak sunucu ile haberleşiyor. Mesela Whatsapp, bir mesaj ya da çağrı var mı diye kendi sunucuları ile iletişim kurduğu anda CGNAT kayıtları da güncellenmiş olur.

--- İnternet hizmeti veren sağlayıcı, hizmetini eğer CGNAT üzerinden veriyorsa, bu kayıt ilgili sağlayıcının her abonesini kapsar. ---

Hocam şimdi de diğer önemli başlığımıza gelelim; metadata (üst-veri) nedir, hayatımızın neresinde yer alıyor, bundan biraz bahseder misiniz bize?

Metadata, veri hakkındaki veri, oluşmuş bir veri bütününün kendisi hakkında içerdiği özet veridir. Özellikle videolarda, müziklerde, fotoğraflarda, dökümanlarda; PDF'lerde, Word, Excel vs.'de karşımıza çıkıyor. Üç tip metadata var; iç metadata, dış metadata ve bir de metadata'ların metadata'sı var.

"Tanrıların Tanrısı!" der gibi oldu. :)

Tabii, veritabanlarında depolanan metadata'lar var. Şu gibi durumlarda, kendisi hakkında dosya, metadata tutmuyor ise ya da güvenilmez, dışarıdan değiştirilebilir ise bu bir dosya sistemine kaydedilirken, bir dosya metadata'sı var bir de bunun gerçekliğini, kilitli kapılar ardında, güvenliğini sağlayacak şekilde o dosya sisteminin, kaydının yapılırken ikinci bir metadata'larını tutan bir metadata veritabanı var. Mesela çeşitli kuvvet komutanlıklarında, geçmişte yaşanan kumpas davalarında yaşanan olaylar tekrar gerçekleşmesin, diye kart okutularak dosya kaydedilen sistemler var. İşte bu nokta, üçüncü faktör sayılır, çünkü; bilgisayar konsoluna erişmek için bir güvenlik faktörü aşılıyor ve ondan sonra o dosya sistemine bilgisayar sisteminden kayıt yapılma tarih, saat, kim kaydı yaptı diye üçüncü bir faktör olarak kullanılan bir sistem söz konusu.

--- HTS, CGNAT kayıtları da birer metadata'dır. ---

Peki hocam bu kayıtların kullandığımız cihazın özelliği ile herhangi bir ilgisi var mıdır? (Örnek olarak eski - tuşlu bir telefonla, yeni - akıllı bir telefonu kıyaslayabilir miyiz?)

HTS kayıtları için cihazın hiçbir önemi yok, SIM kart ve şebeke bağlantısı yeterlidir. Lakin CGNAT için bu önemli; illa ki veri paketi yollayabilmesi lazım yani GRPS-WAP ve 3G-4G diye devam ediyor ama GRPS verisi vermesi yeterli. WAP olayında malum yani aslında MMS ile de benzer, mesaj içeriğini alması için operatörün yerelinde çalışan bir veriyi alıyoruz. CGNAT sistemine dahil olduğumuz zaman da CGNAT sisteminin hatasından etkilenme olasılığına da dahil olmuş oluyorsunuz. Mesela tarafıma gelen ByLock konusundaki bir incelemede, adamın günlere yayılmış bir şekilde, yedi yüze yakın bağlantı kaydı var ve ByLock kullandığı suçlamasıyla altı aydır cezaevinde. Sahip olduğu telefon, Sony marka, eski bir telefon, telefonun bu konuda sahip olduğu tek özellik ise; fotoğraf çekip, MMS ile bunu gönderebilecek olması!

--- Maalesef bu vahim durum gibi daha birçok "hata" ve suçlama var.. --

Peki hocam biraz da anonimliğe, özgürlüğe doğru yönelelim istiyorum müsaadenizle; örneğin VPN kullanıyor olmamız HTS ya da CGNAT kaydını herhangi bir şekilde etkiler mi, öyle ise nasıl?

HTS'yi etkilemez ama CGNAT'i etkiler, yarı görünmez hale geçeriz, diyebilirim. Bundan kastım şu, eğer ben VPN bağlantısında bir filtre belirtmezsem, olası sorgulama yapıldığında VPN'e bağlandığım görülür. Ama mesela TOR kullandığında çok çılgın bir şey çıkacaktır ortaya; her tarafa bağlantı kuruluyor gözükecektir, paketleri dağıtarak çalıştığı için malum..

Aslında ses CDR'nın da kaba lokasyon bilgisi olarak kullanılması büyük bir hatadır, çünkü; ben bir konuşmaya başlayıp, 3 saat boyunca devam ettiğim takdirde, başka lokasyona geçmiş olsam dahi, konum bilgisi başka bir aktivite gerçekleşene kadar değişmeyecektir.

Peki P2P bağlantılar HTS ya da CGNAT'i herhangi bir şekilde etkiler mi?

HTS'yi etkilemez fakat CGNAT'i etkiler; CGNAT için bu bağlantılar anlamsız olacaktır yani ne işlem yapıldığına dair bir yorum yapılamayacaktır.

Bu kayıtlar anonimliğe ne kadar halel getiriyor ve bu kayıtların önemi nedir aslında?

Anonimlik tehlikeli bir konu aslında :) öte yandan anonimlik bir haktır ama işlenen suçların ya da kapalı kalmış, izleri kalan suçların tespitinde bence, hatta bence değil bütün hukukçularca bir emaredir yani bir izdir. Ancak, o izin nasıl oluştuğunun tespitinin yapıldığı, sadece ve sadece o izin bulunduğu cihazın fiziksel olarak temini, image'nın çıkarılması ve incelenmesiyle olur. Dolayısıyla, bu bağlantıların kayıt altında tutulması bir anonimlik ihlali olarak düşünülebilir.

Ancak sadece bu izlerin, suçlama konusu ya da suçun ispatı konusunda kullanılması büyük bir hata, çok çok büyük, muazzam bir hatadır! Geçmişte örneği olan olaylar (blogumda da var, hatta raporda da var bakabilirsiniz) bir deniz subayının bilgisayarında kurulu Windows sürümü ve Java sürümünün bir kötücül Java uygulaması ile arkadaşından geliyor gibi görünen bir e-posta ile linkine yönlendiriyorlar, envanter çıkartıyorlar onu. Envanter çok basit, Internet E. sürümü 8 ve Java sürümü çok emin değilim hangisi olduğuna ancak bu ikisinin birleşiminin bir sistem açığı var, CVE'de de kayıtlı ve expoloit'i

de var.[1] Bu aslında bir oyun olarak çalışıyor, koyunlar düşüyor falan.

Bunu temin ettikten sonra, muhtemelen hacking team'in kullandığı özel exploit üretme yazılımı ile bir Java uygulaması üretiliyor, yine başka bir adres çalınıyor. O oyunu beğendiysem, burada da ilgimi çekebilecek bir oyun var diye o siteye girdiğinde, bir XML, emir dosyası yüklenecek dosyanın adres listelerini içeriyor, dosyanın kendisi diskte yok, imha ediyor çünkü silmiyor sadece, imha ediyor ve Allah'tan sadece downloader olarak kullanılıyor yani dosya çalmak için de kullanılabilir.

Maalesef küçük yaştaki bireylerin istismarını içeren görüntülerin yüklenmesiyle sonuçlanıyor olay. İki gün sonra da elleriyle bulmuş gibi ihbar ediyorlar, polisler geliyor, adamın bilgisayarına el koyuyor ve götürüyor ve fezleke düzenleniyor.

Herkes birbirinden haberdar, ihbarı yapan da bulaştıran da incelemeyi yapan da(!) Tabii burada eksik tarih verisiyle, sistem üst-verileri bunlar – dosya sistemi üstverileridir. Dosyaların ilk indirildiği, son erişildiği, değiştirildiği tarih timestamp olarak birbirinin aynısı. Dolayısıyla o dosyalar indirildikten sonra hiç açılmamış, hiç de değiştirilmemiş! Bu olayı, bu raporlama sonucunda, adamın bu içeriği kendi tasarrufuyla indirmediği ortaya çıkıyor. Dolayısıyla bu sistem üstverisiyle ne yaptık? Olası CGNAT'ın oluşturduğu üstveriyle sistem üstverisini kıyasladığımızda, oluşan olayın aslında CGNAT verisine göre olmadığı, oluşmadığı ortaya çıkmış oldu...

--- Umarız burada bahsi geçenler ilgili kurum ve kişiler tarafından da biliniyor ve dikkate alınıyordur. ---

HTS ve CGNAT kayıtları neden tutuluyor, bu konuda yasal bir zorunluluk var mıdır?

Evet, 5651 sayılı kanun bu konuyla ilgili olarak, 5N1K sorularının yanıtlarının kayıt altına alınmasını emreder ama gelen örneklerde bu verilerin eksik tutulduğu görülüyor. Eksik dediğim, kayıtların tutulmuyor anlamında değil, gelen dökümlerde veri miktarı yok, ne kadar trafik oluştuğu yok? Ziyaret edilen adres yok? Oturum süresi yok, ne kadar bağlantı kurduğu? Belki "bir arkadaşa bakıp çıkacağım" dedi, böyle bir şey yok? :)

Peki bu verilerde neden eksiklik olabilir?

En başta teknik hatalardan kaynaklı olabilir. Örneğin AVEA'nın hizmet aldığı F5 Network Inc. isimli bir ABD şirketi ile ortak çalışması var CGNAT ile ilgili hatta bunu kendi sitelerinde de haber yaptılar, büyük tasarruf yaptıklarına dair.

2013 yılında açılmış bir destek talebi var[1], yapılandırmanın nasıl olabileceğini, dışarıdaki genel IP ile özel IP oranının belli bir ölçüde yapılması gerektiğini, özel IP'lerin NetMask'lerinin maksimum 22 idi sanırım, kesinlikle 16 Bit'in altına inilmemesi gerektiğini, bunun sıkıştırma oranını bozacağını, gerisin geri loglamaları bozacağına dair herkese açık bir destek bildirimi var. Hâlen de yayında bu bildirim.

Ortada bu gibi hataların kanıtları varken, bu hatalardan dolayı göz göre göre mağdurlar var. İlgili sunucuya sadece Ping isteği gitmiş olması bile suç unsuru kabul edilebiliyorken, bu konuya nasıl bir yorum yaparsınız hocam, mahkemelerin bilinci ne durumda?

Yetersiz maalesef. Şunu diyebilirim, hukuk öğretisinde, hemen hemen bütün hocaların telaffuz ettiği bir konu var -Hakim hiçbir şey bilmeyen fakat her şey hakkında karar vermek zorunda kalan kişidir.- Sorumluluğu yüksektir, ehli vukuf ile çalışması gerekir. Hakimler ehli vukufla çalışmıyorlarsa, iddia makamının ya da savunma makamının çalışması gerekir ve ortaya sunulan maddi gerçeklik parçalarının yani teknik tespitlerin mahkemeler tarafından dinlenmesi ve kendi görevlendirdikleri ehli vukuflar tarafından onanması ya da araştırılması gerekir.

Şimdi de müsaadenizle biraz da davalardan söz edelim lütfen. HTS, CGNAT, metadata kayıtlarının Balyoz, Ergenekon ve ByLock başta olmak üzere birçok davanın sürecini ve sonucunu değiştirdiğini biliyoruz artık. Bu davaların aydınlatılmasında da öncülük etmiş birisi olarak, bu kayıtların genel ve gerçek anlamda kanıt ve kıymeti nedir?

Aslında HTS kayıtları Balyoz ve Ergenekon'da yok gibiydi, onlarda daha çok teknik takip olduğu iddiası olan ses kayıtları vardı ancak az miktardalardı ve davalardan daha çok basına sızdırmalarıyla biliniyor ama bunlar usulsüz oldukları için mahkemeler tarafından değerlendirilmedi daha doğrusu usulsüz oldukları için değil mahkemelere yansımadı bunlar. Başkaları adına başkaları dinlenmiş özellikle.

Fakat Balyoz ve Ergenekon'da kayıtlı dosyaların, üstverileriyle ilgili yani kaydeden, ilk oluşturan, son kaydeden bilgisiyle suçlamalar yapılmıştı. "Dosyayı ilk kaydeden sensin!" diye, sanki üstveriler çok güvenilir bir şeymiş gibi, iddianameler bu şekildeydi.

Peki akıbetleri ne oldu?

Hepsi bozuldu! Poyrazköy tamamen beraatle sonuçlandı, Balyoz da öyle! Şu anda Ergenekon'u yargılayacak mahkeme bulunamıyor, yeniden yargılanması yapılacak.[2]

Hocam bu noktaya biraz daha değinelim istiyorum müsaadenizle, mesela bir de MS Office dosyasının versiyon uyuş-

1 Burada bahsedilen işletim sisteminin fingerprintinin çıkartılıyor olması. Sonrasında da elde edilen yazılım ve sürüm bilgileri ile Vulnerability Mapping yapılarak, bu sisteme ait bilinen zafiyetlerin elde edilmesi.

2 https://support.f5.com/csp/article/K14526 - K14526: Deterministic NAT address translations may fail for CGNAT virtual servers

mazlığı ile ilgili bir tespit vardı sanıyorum, bundan da bahseder misiniz lütfen?

Onu, sanıklardan birisi hatta yazınızda lütfen adını anın, Abdurrahman BAŞBUĞ, şu anda Çorum İl Jandarma Komutanı, kendisi hakkındaki sahteciliği bulan kişidir! Calibri-Cambria yazı tipleri 2007 Office'i ile ilk kez toplu olarak sürüme çıkan, 2005 yılında paralı olarak satılmaya başlanan, Microsoft'un da haklarını ödeyerek, pakete dahil ettiği iki tane yazı tipi; Calibri, Word'ün varsayılan yazı tipi, Cambria da Excel'in varsayılan yazı tipidir.

Halbuki bunlar genellikle Arial yazı tipi kullanmışlar, oradan seçerek Arial'i değiştirmesine rağmen, dosya kaydedilirken, içinde boşlukların font bilgisi olarak Calibri ve Cambria geçmiş kayıtlara. Word geri uyumlulukla kaydedildiği için dosya o tarihte, Calibri kullanılmış olması mümkün değildir.

Dosyaların ilk oluşturulma tarihi 2003, son kaydedilme tarihi 2004. Daha kötüsü var; Excel, Word, PowerPoint ZIP konteyner'ı içinde Power Point dökümanın içinde Fatih Camî'nin sözde bombalanması planının sözde sunumunun dosyasıdır, ZIP olarak değiştirilip açıldığında içinde XML dosyaları çıkıyor, bu XML dosyaları içinde yeni tip MS Office dosyalarının tanımları bu XML dosyası içinde, yani şu kısımda bu font kullanıldı, bu kısımda bu renk kullanıldı gibi vs. XML şemaları.

Bunların eski tip 1997 sürümünde olan ofisle kaydedilmiş olmasına rağmen bunların, 97 Office ile kaydedilmiş olması mümkün değil! İlk bulguları (2012), Abdurrahman BAŞBUĞ'a borçluyuz!

Kendisi de adli bilişim ile uğraşmış birisidir, arkasından iç denetçilik ve maliye uzmanlığı yapmıştır sonrasında da dediğim gibi, şu anda Çorum İl Jandarma Komutanı'dır.

Hocam şimdi özet hali ile Balyoz'dan ve Ergenekon'dan bahsettik peki diğer bir hazin hadisemiz olan 15 Temmuz hadiselerinde, ByLock Uygulaması'nın adını oldukça sık duyduk; peki böyle bir uygulama gerçekten var mıydı, FETÖ üyeleri bu uygulamayı iletişim amaçlı olarak gerçekten kullanmış mı? (Bunu soruyorum çünkü, bu konuda da birçok hata ve bu hatalardan dolayı binlerce insanın masum olduğu ispatlandı. (?))

ByLock sunucusunda kişilerin şahsileştirilmesinde CGNAT verileri kullanılmış ve evet, böyle bir uygulama var ve bu örgüt de iletişim amaçlı olarak kullanmış ama (istem dışı) başkaları da kullanmış.

Peki bu kayıtların talebine hangi durumlarda ve nasıl başvurabiliriz?

Bu konu kavuşturma sırasında mahkemelere taleplerle yollanıyor ancak bu durum, KYK'larla ve genelge değişiklikleriyle ya da yönetmelik değişiklikleriyle olabilecek bir durum. Yani kişinin belli durumlarda belli verileri filtreleterek istemesi, benim öğrendiğim kadarıyla bazı kişilerin kendileri hakkında bu ByLock soruşturmasıyla ilgili benim bu 9 IP adresine erişimim hangi tarih aralığında olmuş diye bir ara BTK bir cevap verdi, belli bir periyot ama sanırım başa çıkamadılar. Yani sonuçta, Hakkında ByLock kullandığı iddia edilen **219 bin kullanıcı varken, bu sayı yüz küsur binlere düştü**. Bunların bir bölümünün kullanmadıkları sağlam gerekçelerle reddedildi bu kişilerin rakamının da 30 binin üstünde olduğu iddiası var. Hatta iddia değil gerçeğe yakın. Dolayısıyla bunların oluşturacağı iş yükü çok yüksek ve bundan dolayı mahkemeler tarafından talep edilebiliyor. Sulh, ağır ve asli ceza hakimi, hukuk mahkemeleri de yapabilir herhangi bir mahkeme ya da savcı diyelim.

Peki hocam, artık ropörtajımızın sonuna geldik, son olarak eklemek istediğiniz bir şeyler varsa onları rica edeceğim sizden. Yoksa metadata'ya ve bunların önemine biraz daha dikkat çekebilmek adına bir şeyler söylemek ister misiniz? Gönderdiğimiz e-postadan, çektiğimiz fotoğrafa kadar hayatımızın her yerinde karşılaşıyoruz bu verilerle.

Irak Savaşı'na, İngiltere'yi dahil eden dökümanda üstveriden fazlası var, Word'ün kasten bırakılmış bir hatası var, -son on kullanıcı kayıtları- diye orada Tony Blair tarafından ya da danışmanları tarafından yazılmış bir rapor olmadığı, bu raporun, e-mail ile ABD Savunma Bürokratları tarafından ilk oluşturulduğu bunun ve onun sonradan Blair'ın birtakım danışmanları tarafından kendi meşreplerince değiştirilip, kaydedilerek, üstverinin göremediği kısmın Blair'a sunulduğu, bir doküman olduğu ve "Vay anasını! Saddam, kimyasal silah kullanıyormuş!" diye İngiliz Kraliyet Donanması'nın da savaşa dahil edildiğinin can alıcı bir örneğidir. Belki de dünya üzerinde görülebilecek en vahşi olaydır!

Çok dikkat çekici bir örnek oldu, teşekkür ederiz ve sizi çok yorduk hocam, çok teşekkür ederiz. Başta ülkemize ve milletimize sunduğunuz katkılar, aydınlattığınız ve aydınlatmakta olduğunuz davalar için ve sonra bu yoğunluğunuz arasında bize ayırdığınız (6 saat!) size can-ı gönülden teşekkür ederiz. İyi ki varsınız! Dergimize de bir yazar olarak sabırsızlıkla bekliyoruz. :)

Rica ederim, vakit bulduğum ilk fırsatta dergide de bir şeyler karalayacağım. :)

ARKA KAPI

Kıymetli arkadaşlar,

Koray Bey ile sohbetimiz yaklaşık 6 saat sürdü ve bunun yaklaşık olarak yarısı doğrudan röportaj için geçti. Takdir edersiniz ki bu röportajın tamamını (yaklaşık 16 sayfa kadar:) dergide yayımlayamazdık biz de bu nedenle, aşağıda röportajın tam haline ulaşabileceğiniz bir bağlantı paylaştık ve tamamını okumanızı rica ederiz.

"Başka neler var acaba?" dediğinizi duyar gibiyim, başlıca diğer konular şöyle;

- Nokia markalı eski – tuşlu bir telefonda ByLock iddiası? :)
- NAT ve CGNAT arasındaki fark nedir? Neden ihtiyaç duyuldu, nasıl tespit ve iptal edilir?
- Ülkemizde CG teknolojisinin yeri nedir, kullanıcı açısından zararları neler olabilir?
- Bu kayıtların tutulmasında, hukuksal olarak anonimlik için neler yapılabilir?
- Bu kayıtların tutulması ya da tutulmaması iletişime bir engel teşkil eder mi?
- Geçmişte BTK kaydı olmayan bazı Iphone'lar şebekeyi kullanabildi mi?

Röportajın tamamı için:

https://arkakapidergi.com/m/koray-peksayar-sahin-solmaz-roportaj.pdf

Ayrıca

- https://koray.peksayar.org/
- Av. Ali Aktaş - FETÖ'nün Kumpası ByLock Zokası kitabı

Avukat Mehmet Pehlivan - Pehlivan İlkakın Hukuk Bürosu - mehmet@pehlivanilkakin.com

Mühür Kimdeyse Süleyman O'dur

Kullanıcı Sözleşmeleri

Giriş

Biz bireysel kullanıcılar, internette bize sunulan arama motoru, e-mail, sosyal ağ gibi ücretsiz ve aynı zamanda günlük hayatımızın neredeyse tamamını kapsayan hizmetlere sonsuz güveniyoruz. Bu güvenin temelinde, "Ne kadar iyiler, böyle bir hizmeti ücretsiz sağlıyorlar bizlere. Yaşasın dünya barışı!" düşüncemiz mi yer alıyor dersiniz? Sanmıyorum. Her ne kadar bu hizmetleri görünürde para vermeden kullanıyor olsak da aslında bu hizmetlerin bedelini mahremiyetimiz ve kişisel verilerimizle ödüyoruz. Evet, yanlış okumadınız; bu şirketler tahsilatı para yerine, kişisel verilerimiz ve mahremiyetimizle yapmaktadırlar. Bu noktada işi daha da ilginç hâle getiren ise mahremiyetimizi ve kişisel verilerimizi biz kendi rızamızla paylaşıyor olmamız. Peki nasıl? Cevabı: Kullanıcı Sözleşmeleri.

Kullanıcı sözleşmeleri, ortalamada 47 sayfadan ve 3 bin 2 yüz 94 kelimeden oluşan, temelde bize ücretsiz olarak bir servisten faydalanacağımızı vadeden; ancak karşılığında bizden tam olarak ne alacağını açıklamayan, açıklamadığı bu alacağın ise mahremiyetimiz ve kişisel verilerimiz olduğu sözleşmelerdir.

Next, next, next, next, I agree…

Mahremiyetimizin ve kişisel verilerimizin kapılarını daha başlangıçta, kullanmak istediğimiz servise üye olurken açıyoruz. Bunu da *"Kullanıcı Sözleşmesini Okudum ve Onaylıyorum"* kutucuğunu işaretleyip, tamam tuşuna basarak yapıyoruz. İşte bizim için karanlık tarafa geçiş böyle başlıyor.

Saniyeler içerisinde birkaç tıkla onaylayıp geçtiğimiz bu sözleşmeler bizim için oldukça tehlikeli bir hâle gelebilir. Buz dağının görünmeyen kısmı olan kullanıcı sözleşmelerini hızlıca okuyup geçmemizin bizler için tehlikesini bir iki örnekle açıklamak gerekirse:

Bir şirket Londra'da kurdukları kamusal kablosuz internet noktası üzerinden yapılan bir deneyde, kişilerin üyelik açarken onayladıkları kullanıcı sözleşmesinde şöyle bir maddeye yer vermiştir: ***"Bu hizmeti kullanarak, doğacak ilk çocuğunuzu, şirket istediği zaman ŞİRKET'e vermeyi kabul etmiş oluyorsunuz. Eğer çocuğunuz olmazsa, en çok sevdiğiniz evcil hayvanınız alınacak. Bu anlaşma sonsuza kadar geçerlidir".*** Deney sonucunda şirket, hizmeti kullanan herkesin bu sözleşmeyi onayladığını, bunun da kimsenin sözleşmeyi okuma gereği duymadığını gösterdiğini açıkladı.

Yine başka bir şirket kullanıcı sözleşmelerinin okumamasına dikkat çekmek için, pazarlamasını yaptığı programının kullanıcı sözleşmesinin içerisine eklediği bir maddede: ***"Bahse konu olan maddeyi okuyup; firmaya başvuranlara mali bir ödül verilecektir"*** demiştir. Program 3 bin adet indirildikten ve aradan dört ay geçtikten sonra bu sözleşmeyi okuyan tek bir kişi çıkmış ve firmaya sözleşmede belirtilen e-posta adresinden başvurmuştur. Şirket de anlaşmaya uyup, bu kişiye 3 bin dolar ödül vermiştir. Belirtmek gerekir ki, bu sözleşmelerin okunmalarının tek kazanımının -bu örnekte olduğu gibi- her zaman para ödülü olmayacağı konusunda sessiz bir fikir birlikteliğimizin olduğu kanaatindeyim.

Biz bu yazımızda hiç kimsenin okumadığı, okumak istese de çarçabuk yılacağı o uzun uzadıya giden kullanıcı sözleşmelerini sizler için okuyup, bu sözleşmelerde bizden tam olarak ne için onay aldıklarını değerlendirip, siz değerli okurlara dilimizin döndüğü ve kalemimizin yettiği kadarıyla açıklamaya çalışacağız.

İncelemede bulunacağımız servisler: WhatsApp, Google, Youtube, Twitter, Facebook, Microsoft, Apple gibi markaların en çok kullanılan servisleridir. Hemen bu noktada bir yasal uyarıda bulunmak gerekir ki, bu yazıda yer alan bilgiler hukuki

tavsiye niteliğinde değildir ve maalesef her bir maddenin güncel halini de içerdiği de söylenemez. Ve yine bu yazıda sunulan bilgileri okumak, hiçbir şekilde hukuken bağlı olduğumuz sözleşmeleri okumak yerine geçmez.

WhatsApp

WhatsApp mesajlarınızı depolamasa da mesajlarınıza ilişkin meta verileri depolar. Metaveri bizce bir kelime oyunu olup, kısaca veri hakkındaki veri olarak tarif edilir. Burada verinin içeriğinden ziyade nereden geldiği, nereye gittiği ve buna ilişkin zaman ile tarihten bahsedilir. Zararsız görünse de aslında biraz evvel belirttiğim gibi tamamıyla kelime oyunudur. Örneğin, ünlü hacker Kevin Mitnick, FBI ajanları tarafından evine yapılacak baskını bu ajanların telefonlarından ele geçirdiği meta veri sayesinde önceden haber almıştır. Kurt Opsahl meta veriyi anlattığı bir yazısında şirketlerin ve devletlerin meta veriden neler öğrenilebildiğini örneklendirmiştir: Şirketler ve Devletler gece saat 02:24' de telefonda seks hizmeti veren bir numarayı arayıp 18 dakika konuştuğunuzu bilirler. Fakat ne hakkında konuştuğunuzu bilmezler. Onlar sizin Golden Gate Köprüsü'nden intiharı önleme hattını aradığınızı bilirler. Fakat konuşmanın konusu gizli kalır. Onlar sizin HIV testi yapan bir şirketle, ardından doktorunuzla, ardından hayat sigortası şirketinizle aynı saatte konuştuğunuzu bilirler. Fakat ne hakkında tartıştığınızı bilmezler diyerek aslında meta verinin ne kadar önemli olduğunu gözler önüne sermiştir.

WhatsApp üzerinden gönderilen DOSYALAR (fotoğraf, ses kaydı, doküman, konum) bir süre sunucularda saklanır, sonra silinir. Normal mesajların sunucularda depolanmadığı, uçtan uca şifrelemeyle doğrudan alıcıya gönderildiği olağan iş akışının aksine gönderilen dosyaların sunucuda saklanması üstüne üstlük bu saklamanın "ne kadar süreyle" sınırlı olacağının bilinmemesi kullanıcı dostu bir hüküm değildir.

Durum paylaşımlarınız telefon numaranıza sahip herkese açıktır. Profil fotoğrafınız, durum yazınız, son görüldü bilginizden oluşan "durum paylaşımlarınız", siz aksini belirtmedikçe, cep telefonu numaranıza sahip (engellemediğiniz) herkes tarafından görüntülenebilir. Asıl olanın gizlilik, istisna olan açıklık olduğu düşünüldüğünde bu maddenin de kullanıcı dostu olmadığı açıktır. **Yine anılan durum paylaşımlarınız üzerindeki telif haklarınıza sahipliğiniz devam eder ancak WhatsApp'ın bu durum paylaşımları üzerindeki lisansı oldukça geniştir.**

WhatsApp, hakkınızda depoladığı verileri Facebook ile paylaşır. WhatsApp, Gizlilik Politikası, 2014 yılında Facebook tarafından satın alındığını belirttikten sonra, Facebook ve onun sahip olduğu diğer şirketler ile verilerinizin paylaşılabileceğini belirtmektedir. Hemen belirtmek gerekir ki, WhatsApp'a, WhatsApp numaralarını Facebook hesapları ile eşleştirmekten dolayı Avrupa Komisyonu tarafından 122 milyon dolar ceza kesilmişti.

WhatsApp, verilerinizi kişisel olmaktan çıkarmak suretiyle üçüncü şahıslarla paylaşabilir. Ayrıca kanunun gerektirdiği veya böyle olduğuna dair iyi niyetli bir inanca sahip olduğu durumlarda WhatsApp verilerinizi toplayabilir, paylaşabilir. Bu iyi niyetli inancın da muğlaklığı yine sözleşmede buz dağının görünmeyen kısmı olarak tanımlanmaktadır.

Gizlilik Politikasında gerçekleştirilebilecek değişikliklerde kullanıcının görüşü alınmaz ve kullanıcı doğrudan bilgilendirilmez. WhatsApp, Gizlilik Politikasını belirli aralıklarla revize edebileceğini belirtmekte ancak bu durumlarda sizi bilgilendireceğini veya bu değişikliklerle ilgili görüşünüzü alacağını taahhüt etmemektedir. WhatsApp'ı bu değişikliklerden sonra kullanmaya devam etmeniz "bu yeni politikayı kabul ettiğiniz anlamına gelir". Bu madde başlangıçta kullanıcı dostu olarak görünen bir sözleşmenin bir anda nasıl balkabağına dönüşebileceğinin işareti!

Büyük Birader değil; Google bizi izliyor!

Google bünyesinde barındırdığı AdSense, Analytics, Arama, Blogger, Çeviri, Drive, Gmail, Google+, Hangouts, Haritalar, YouTube servisleri aracılığıyla medeniyet namına, yaşıyan her bireyin günlük hayatının neredeyse tümüne sirayet etmektedir. Haliyle bizlerden topladığı veriler de bir hayli büyük olmaktadır. Öyle ki, pek çok alanda ücretsiz hizmet sağlayan Google, milyarlarca dolara kendi sunucularını üretiyor. Bu da ilk etapta kulağa biraz garip geliyor çünkü bir dükkâna gidip Google Sunucularından bir tane satın alamazsınız. Peki, Google satmadığı halde neden bu kadar çok sunucu üretiyor? Çünkü Google'ın, rıza göstererek onlara açtığımız mahremiyetimizi ve kişisel bilgilerimizi depoladığı veri merkezleri için o kadar çok sunucuya ihtiyacı var ki bu onu dünyanın 4. büyük sunucu üreticisi haline getirdi.

Google, kullandığınız hizmetlerinden birçok verinizi toplar ve inceler, buna e-posta içeriklerimizin analizi de dahildir. Google hizmetlerinin oldukça geniş ve popüler olması sonucu Google'ın hakkımızda topladığı veri miktarı oldukça fazladır. Bu verilere şunlar girer: Arama sorgularımız, konum bilgilerimiz, harita aramalarımız, izlediğimiz videolar, reklamlarla etkileşimlerimiz, Google hizmetleri kullanan siteleri ziyaretimiz, kullandığınız Google hizmetleri dolayısıyla

Google'ın sahip olduğu diğer veriler. Ki bu da Gmail gibi servisleri düşündüğümüzde hatırı sayılır bir veriyi ifade ediyor.

Google bununla beraber "otomatikleştirilmiş sistemi" aracılığıyla e-posta içeriklerimiz de dahil olmak üzere içeriklerimizin tamamını analiz eder. Örneğin, tatil hakkında bir mail aldığımızda mailin sağında ve solunda uçak bileti reklamı görmemiz Google'ın bir "marifeti" dir![1]

Google, reklam servisleri ile verilerimizi paylaşmaz. Her ne kadar verilerimizi reklam servisleriyle paylaşmasa da sunduğu hizmetler dolayısıyla Google zaten kendisi bir reklam şirketidir.

Google, bizi diğer internet sitelerinde de takip eder ve bu sitelere erişimimize ilişkin verileri toplar. Google Gizlilik Politikası'na göre, AdSense gibi reklamcılık ürünlerini, +1 düğmesi gibi sosyal ürünlerini veya Google Analytics gibi analiz araçlarını kullanan bir internet sitesini ziyaret ettiğimizde, tarayıcımız belirli bilgileri Google'a otomatik olarak gönderir. Bu bilgiler arasında, ziyaret ettiğimiz sayfanın web adresi ve IP adresiniz de bulunur. Böylece internet geçmişimizle ilgili bilgi edinen Google, size ilgi alanlarınıza göre kişiselleştirilmiş reklamlar sunmayı amaçlar! Belirtmek gerekir ki, Google reklamlarını kullanmayan internet sayfası neredeyse hiç yok!

Google, bizden topladığı verileri birleştirerek hakkımızda "reklam amaçlı" profiller oluşturur. Google'da oturum açarsak hakkımızda toplanan veriler Google hesabımızla ilişkilendirilir. Oturum açmasak dahi Google, "belirli hizmetlerdeki kişisel bilgilerinizi birleştirebilir". Bu her iki ihtimalde de hakkımızda toplanan verilerle bir nevi profil oluşturulmuş olur. Google bunun amacının "istenmeyen e-postaların ve kötü amaçlı yazılımların tespit edilmesi ile özelleştirilmiş arama sonuçları ve reklamlar gibi size kişisel olarak uygun ürünlerin sağlanması" olduğunu belirtmektedir. Google'a bu konuda güvenmeli miyiz?!

Google, kesinlikle kişisel verilerimizi üçüncü şahıslarla paylaşmaz… Demek isterdik ki mümkün değildir. Google, verilerimizin harici olarak işlenmeleri amacının bulunması ve yasal nedenler nedeniyle verilerimizi üçüncü kişilerle paylaşır.

Hesabımızı ve içeriklerini silsek dahi Google, verilerimizi saklamaya devam edebilir. Belalı bir eski sevgili gibisin Google! Google, internet geçmişimizi, yarattığımız bir blogu, YouTube kanalımızı, Google+ profilimizi veya hepsini kapsayan Google hesabımızı silmemize imkân sağlar. Ancak tek başına belirli hizmetlerdeki verilerimizi silsek veya hesabımızı kapatsak dahi Google, "bilgilerinizi silmenizin ardından kalan kopyaları etkin sunuculardan hemen silmeyebilir ve bu bilgileri

yedek sistemlerinden kaldırmayabilir". **Yine bu kapsamda bir diğer madde de, Google'a içeriğimiz üzerinde tanıdığımız lisans, hizmetleri kullanmayı bıraksak dahi devam eder.** Bu yönüyle geri alınamaz nitelikte bir lisanstır.

Google, Kullanım Şartlarındaki değişikliklerde bizi doğrudan bilgilendirmez ancak değişiklikler en az 14 gün sonra yürürlüğe girer. Google, Kullanım Şartlarını belirli aralıklarla revize edebilir. Bu sözleşmede yapılacak değişiklikler ilgili sayfada yayınlanır ancak sözleşmede kullanıcının doğrudan bilgilendirileceğine ilişkin bir madde görünmemektedir. Buna karşın yeni yayınlanan değişiklikler, "yeni eklenen işlevlere yönelik veya yasal sebeplere" dayanmadığı sürece, en az 14 gün sonra yürürlüğe girer.

Google bünyesinde faaliyet gösteren YouTube'un kendine özel bir gizlilik politikası bulunmamaktadır. Google Gizlilik Politikası, diğer Google ürünlerinde olduğu gibi YouTube Gizlilik Politikasını da kapsamaktadır. Ancak YouTube Kullanım Şartları, kullanıcı içerikleri üzerindeki telif haklarının düzenlenmesi noktasında Google Genel Kullanım Şartlarından ayrılmaktadır. Google tarafından da belirtildiği üzere genel ve özel şartların farklı olması halinde bu örnekte olduğu gibi özel şart geçerli kabul edilir.

YouTube'da paylaştığımız videolar üzerinde eser sahipliği-

1 Google, Gmail ürününde artık bu hizmeti vermemektedir. Ancak özellikle de e-posta uygulamalarında e-posta içeriğine uygun yanıtlar önermesi, e-posta ile gelen tatil ve bilet rezervasyonlarını takvime ekleyip silebilmesi, hâlâ epostalarımız üzerinde bir "göz" olduğunu gösteriyor.

miz devam etse de servise tanıdığımız lisans oldukça geniştir. YouTube üzerinden yapmış olduğumuz paylaşımlar üzerinde Google, herhangi bir hak iddia etmez. Ancak servise paylaşımlarımız üzerinde tanımış olduğumuz lisans alt lisanslama hakkını da içeren devredilebilir nitelikte oldukça geniş bir lisanstır. Bu da yılların bitmek bilmeyen bir telif problemini gündeme getirir. **Yine metin şeklinde yaptığımız yorumlarımız üzerinde tanıdığımız lisans geri alınamaz nitelikte ve süreklidir.** YouTube'a metin şeklinde yaptığınız yorumlarınız üzerinde tanıdığımız lisans, geri alınamaz nitelikte ve sürekli (sonsuz süreli) bir lisanstır. Bu da akla yorumlardan çıkarılacak bir şarkı sözü ihtimalini ve bu sözlerin kime ait olacağını sorusunu getiriyor...

YouTube, dilediği zaman herhangi bir sebep göstermeksizin ve bize bildirim yapmaksızın paylaşımlarınızı silebilir YouTube'un inisiyatifinde olmak üzere Kullanım Şartları sözleşmesi veya telif hakkı ihlalleri söz konusu olduğu takdirde paylaşımlarımız bir sebep gösterilmeksizin ve bize bildirim yapılmaksızın silinebilir. Son zamanlarda milyonlarca tıklanması olan şarkılar "asılsız" şikayetler sonucunda silinmiş, sanatçısı mağdur edilmiştir.

Twitter

Twitter, bizi diğer internet sitelerinde de takip eder ve bu sitelere erişimimize ilişkin verileri toplar. Twitter Gizlilik Sözleşmesine göre "bileşen verileri" (widget data) adı verilen bir başlık altında, Twitter bileşenleri kullanan herhangi bir internet sitesini ziyaret ettiğimizde bu ziyarete ilişkin verileri çerezler kullanarak toplar. Twitter, bu sayede sizinle ilgili edindiği bilgiler ile bize özel reklamlar sunmayı amaçlar!

Twitter servisleri ile etkileşimlerimiz "günlük veriler" olarak toplanır ve kaydedilir, bu veriler en fazla 18 ay sonra silinir veya kişisel olmaktan çıkarılır. Twitter servisleri ile girdiğimiz herhangi bir etkileşim sonucunda kaynak internet sayfası, ziyaret edilen sayfalar, konum, arama kelimeleri ve çerez bilgiler, IP adresimiz, kullanıcı adımız ve e-posta adresimiz gibi verilerle eşlenerek toplanır ve sunuculara kaydedilir. Bu günlük verileri en fazla 18 ay sonrasında "silinir veya kişisel olmaktan çıkarılır".

Twitter, üçüncü taraf çerezlerin kullanılmasına izin verir. Yine Twitter, kişisel verilerimizi üçüncü şahıslarla tam olarak paylaşmaz ancak bunun istisnaları vardır. Kural olarak Twitter, kişisel verilerimizi üçüncü şahıslarla paylaşmaz ancak servis sağlayıcılar ile veya kanunun gerektirdiği durumlarda üçüncü şahıslarla verilerimiz paylaşılabilir. Ayrıca Twitter, "bağlı şirketleri" ile bilgilerimizi paylaşabilir.

Twitter, kişisel olmaktan çıkarılmış veya gizli olmayan verilerimizi üçüncü şahıslar ile paylaşabilir. Twitter, kişisel veri statüsünde olmayan verilerimizi veya gizli olarak nitelendirilemeyecek olan herkesin erişimine açık olan verilerimizi reklam şirketleriyle paylaşabilir. Örneğin, profiliniz gizli değilse tweetlerimiz, takip ettiğimiz ve bizi takip eden kişiler, tıkladığımız bağlantılar gibi. Ancak bunu yaparken adımız veya iletişim bilgilerimizi paylaşmaz.

Paylaşımlarımız üzerindeki telif haklarınıza sahipliğimiz devam eder ancak Twitter'a bu içerik üzerinde verdiğimiz lisans geniştir. Twitter üzerinden yapmış olduğumuz paylaşımlar üzerinde Twitter herhangi bir hak iddia etmez. Ancak Twitter'a, paylaşımlarınız üzerinde tanımış olduğumuz lisans alt lisanslama hakkını da içeren geniş bir lisanstır. Bu lisans, hesabımızı silsek dahi içeriğimiz üzerinde devam eder.

Facebook

Facebook, kendisine sağladığımız ve başkalarının bizim hakkınızda sağladığı her türlü veriyi toplamaktadır. Buna, hesap açmamız, içerik oluşturmamız veya paylaşmamız, başkalarıyla mesajlaşmamız, Facebook'a koyduğumuz bir fotoğrafın yeri veya bir dosyanın oluşturulduğu tarih ve hatta görüntülediğimiz içerikler bile dahildir. Öte yandan, başkalarının bizim hakkımızda paylaştığı veriler de Facebook tarafından toplanmaktadır.

Ayrıca Facebook'a erişim sağladığımız cihazın iletişim sistemi, donanım versiyonu, cihaz ayarları, pil ve sinyal gücü, cihaz konumları (GPS, WiFi sinyalleri yoluyla), cep telefonu operatörümüzün ve internet servis sağlayıcımızın adı, tarayıcımızın türü, cep telefonu numaramız da kaydedilir.

Facebook, kendi tespit ettiği gerekçelerle mahkeme kararı olmaksızın verilerimizi üçüncü kişilerle paylaşabilir. Neyse ki, Facebook, kişisel verilerimizi işlemesi nedeniyle bugüne kadar milyonlarca dolar ceza yememiş, verilerimizin hassasiyeti konusunda oldukça hassas bir şirket!

Facebook, hizmetlerini kullanan uygulamalarla, elindeki verilerimizi paylaşmaktadır. Örneğin, Facebook'ta arkadaşlarımızla bir oyun oynadığımızda veya bir internet sitesin-

de Facebook Yorum Yap ya da Paylaş düğmesini kullandığımızda, oyunun geliştiricisi veya internet sitesi oyundaki hareketlerimizle ilgili bilgi toplayabilir veya internet sitesinden Facebook'ta paylaşım yaptığımıza dair bir yorum veya bağlantı alabilir. Bu maddeyi Facebook'tan Okey oyununu oynayan babama anlattığımda babam, oyun stili ve hünerlerinin Facebook tarafından karşı komşumuz olan Emekli Astsubay Ali Bey amcaya anlatıldığını iddia etti. Ali Amca ve Facebook arasındaki bu ilişkinin kaynağını merak etmiyor değilim!

Neyse, devam edelim… Bu üçüncü şahıs hizmetlerini indirdiğimizde ya da kullandığımızda, kullanıcı adımız ya da kullanıcı kimliğimiz, yaş aralığımız, ülkemiz/dilimiz ve arkadaş listemizin yanı sıra, onlarla paylaştığımız bilgileri içeren "Herkese Açık Profilinize" erişebilirler. Bu uygulamalar, internet siteleri veya entegre uygulamalar tarafından toplanan bilgiler, onların kendi koşul ve ilkelerine tabidir.

Facebook, münferit olarak sadece bir paylaşımımızı sildiğimizde bunu veritabanından silip silmediği hakkında bilgi vermemektedir. Ancak biz biliyoruz ki, silmiyor! Facebook, "zaman tüneli" sistemine geçtiğinde önceden silinen gönderiler sayfalarda gözükmekteydi, bu da Facebook'un aslında o gönderileri veritabanından silmediğini göstermektedir.

Microsoft

Microsoft, birçok verimizi toplar ve depolar. Buna, adımız ve iletişim verilerimiz, kimlik bilgilerimiz, demografik veriler, ilgi alanlarımız ve tercihlerimiz, ödeme verileri, kişilerimiz ve ilişkilerimiz, konum verimiz, sağladığımız içerikler, müşteri destek hattıyla yaptığımız görüşmeler, ve hatta Microsoft'un perakende mağazalarına girdiğimizde güvenlik kamerası tarafından kaydedilen görüntümüz de dahildir.

Microsoft, kendisinin topladığı yetmezmiş gibi üçüncü kişilerden de verilerimizi toplamaktadır. Örneğin farklı şirketlerden demografik bilgiler satın alarak diğer verilere eklenmektedir. Ayrıca Microsoft, bazı ürünleri coğrafi konumumuza bağlı olarak özelleştirebilmek için, diğer şirketlerin IP adresimize bağlı olarak sizin konumumuzu tespit etmeye yardımcı olan hizmetlerini kullanarak, verilerimizi bu şirketlerle paylaşmış olmaktadır.

Microsoft, bizden topladığı verileri birleştirerek hakkımızda bir profil oluşturmamayı vaat etmemektedir. Microsoft'un gizlilik politikasında, servislerin geneli hakkında, bu servisleri kullanırken hakkımızda toplanan verilerin bir araya getirilerek bir reklam profili oluşturup oluşturmadığı hakkında doğrudan bir hüküm bulunmamaktadır. Bu hükmün ifade ediliş biçiminden ve servislerin geneli için böyle bir hükme yer verilmemesinden, Microsoft'un diğer servislerdeki verileri birleştirerek kullanıcıları için bir profil oluşturduğu anlaşılabilir. Ne zalimsin Microsoft!

Microsoft, kişisel verilerimizi bize reklam sunmak amaçlı olarak kullanmakta olduğunu iddia etmektedir. Microsoft, topladığı verileri, kendi hizmetleri veya üçüncü taraflarca sağlanan hizmetler üzerinden Microsoft'un sunduğu reklamların seçilmesine yardımcı olmak için kullanmaktadır. Seçilen reklamlar, mevcut konumumuz, arama sorgumuz ve görüntülediğimiz içeriğe bağlı olabilir. Bu bildirimde "ilgi alanına dayalı reklamlar" olarak belirtilen diğer reklamlar ise olası ilgi alanlarımız ve zaman içerisinde demografik verileri, arama sorguları, ilgi alanları ve tercihler, kullanım verileri ve konum verilerinden bizimle ilgili edinilen diğer bilgilere dayanarak hedeflenir.

Microsoft, mahkeme kararı olmaksızın, kişisel verilerimizi devlet kurumlarıyla paylaşabilir. Microsoft Gizlilik Politikası, yürürlükteki yasalara uymak veya kolluk güçleri ya da diğer devlet kurumlarından gelenler dahil olmak üzere geçerli yasal sürece cevap vermek için, e-postalarımızın içeriği, özel klasörlerdeki diğer özel iletişim veya dosyalar dahil olmak üzere tüm özel içeriğimizi paylaşabileceğini belirtmektedir.

Microsoft, kişisel verilerimizi üçüncü kişi reklam şirketleriyle paylaşmaktadır. Bazı durumlara Microsoft, reklam veren şirketlerin siteleri veya reklamlarında topladığı verilerle ilgili raporları onlarla paylaşmaktadır. Ayrıca verileri de doğrudan hizmet sağlayıcıları ile paylaşabilir ve bu sağlayıcıların, Microsoft adına hizmet vermelerine veya reklam ortakları için reklam seçimi ve hizmeti konusunda Microsoft'la ortak çalışmalarına izin verebilir. Kullanıcılarının verilerini başka reklam şirketleriyle paylaşan bir şirketin, iş ortaklarının güvenilirliği hakkında taahhüt vermesi düşündürücü bir husustur.

Microsoft, servisleri ile birlikte verdiği reklamları sunan reklam şirketlerinin, internet işaretçileri ile bizden. veri toplamasına izin vermektedir. Reklam veren şirketler, bazen kendi tanımlama bilgilerini oluşturmak ve okumak için, kendilerine ait internet işaretçilerini görüntülediği reklamlara koyabilir.

Microsoft, yazılımlarını satmayıp lisans verdiğini belirtmektedir ve bunun kullanıcı için bazı olumsuz sonuçları vardır. Örneğin, yazılımları, yazılım lisanslarını veya Hizmetlere erişme ya da Hizmetleri kullanma haklarını devredemezsiniz.

Apple

Apple, birtakım kişisel bilgilerimizi toplar. Bir Apple Kimliği oluşturduğumuzda, bir ürün satın aldığımızda, bir yazılım güncellemesi indirdiğimizde, bir Apple Perakende Mağazası'nda kursa kaydolduğumuzda, Apple ile irtibat kurduğumuzda veya çevrimiçi bir ankete katıldığımızda adımızı, yazışma adresimizi, telefon numaramızı, e-posta adresimizi, iletişim tercihlerimizi ve kredi kartı bilgilerimizi içeren çeşitli bilgiler Apple tarafından toplanabilir. **Apple, topladığı bu kişisel bilgilerimizi reklam amaçlı olarak kullanmakta olduğunu iddia etmektedir.**

Öyle ki, yine topladığı ve reklam amaçlı olarak kullandığı bu bilgileri, uluslararası kuruluşlara aktarabilir ya da bunlar tarafından bu bilgilere erişilebilir. Fakat Apple'ın gizlilik politikasında, "Uluslararası Kullanıcılar"'ın ne olduğu konusunda ayrıntılı bilgi verilmemiş, başka konuya geçilmiştir.

Apple, mahkeme kararına, hatta kimi durumlarda bir devlet kurumunun talebine gerek kalmaksızın kişisel verilerimizi ifşa edebilir. Apple Gizlilik Politikası, kanunun icrası ya da kamu ile ilgili diğer önemli sorunlar için ifşanın gerekli ya da uygun olduğunu tespit etmesi halinde ve hatta Apple'ın koşul ve şartlarını uygulamak ya da işlemlerini ya da kullanıcılarını korumak üzere ifşanın makul surette gerekli olduğuna karar verirse hakkımızdaki bilgileri ifşa edebileceğini belirtmektedir.

Apple, varsayılan politika olarak konum bilgimizi toplar ve paylaşır. Apple ürünlerinde konuma dayalı hizmetler sağlamak için Apple, ortakları ve lisans sahipleri, Apple bilgisayarımızın ya da aygıtımızın gerçek zamanlı coğrafi konumu dahil tam konum verilerini toplayabilir, kullanabilir ve paylaşabilir. Ancak rızamız olmaması halinde, konum verileri kimliğimizi tanımlamayacak şekilde isimsiz olarak toplanır ve Apple, ortakları ve lisans sahipleri tarafından konuma dayalı ürünleri ve hizmetleri sağlamak ve iyileştirmek için kullanılır.

Sonuç

Nasıl ki, bankaların bitmek bilmeyen uzun sözleşmelerinde yer alan ve müzakere etmemizin mümkün olmadığı "tüketici aleyhine" hükümler bankaları denetleyici kuruluşlar ve tüketicinin korunmasına ilişkin kanunlar sayesinde geçersiz sayılıyorsa, servislere ilişkin kullanıcı sözleşmeleri bakımından tam anlamıyla bu korumanın varlığından bahsedemeyiz. Fakat sivil inisiyatifler ve devletler kullanıcıların gizlilik ihtiyacına karşılık bir çözüm bulmaya çalışmaktadır. Bu kapsamda da kişisel verilerin korunmasına yönelik kanunlar ve yönetmelikler yayımlayarak servislere karşı denetim getirmeye çalışmaktadır. Ülkemizde de son zamanlarda kişisel verilere yönelik çok ciddi çalışmalar yapılmış olup, bu çalışmalara hâlen devam edilmektedir. Örneğin, 6698 sayılı Kişisel Verileri Koruma Kanunu ve bu kanun uyarınca çıkarılmış yönetmelikler, kişisel verileri koruma kurulu bu yönde atılmış çok büyük bir adımdır. Umuyoruz ki, bu servislerin biz kullanıcılar üzerindeki bu denli "hakimiyetine" ve biz kullanıcıların şeffaflık ve mahremiyet taleplerine bu düzenleyici kuruluşlar tarafından son verilecektir.

Kriptoloji'nin Altın Çağı

Telsiz, mektup, telgraf gibi anonim araçlar ile haberleşmiş hangi nesil diktatörlere, meraklı gözlere, hassas kulaklara karşı fikrinin, aşkının, ailesinin mahremiyetini korumak için şifreli haberleşmemiştir?

Bu yazımı bitirdiğimde *www.wikipedia.org* özgür kütüphanesi hâlâ bilmediğimiz sebep(ler)den ötürü **BTK** tarafından engelleniyordu. **BTK**'nın son açıklaması *www.wikipedia.org* sunucuları Türkiye'de olmalı şeklindeydi. Bilgiye yasak koyan tek ülkeyiz…

Scytale

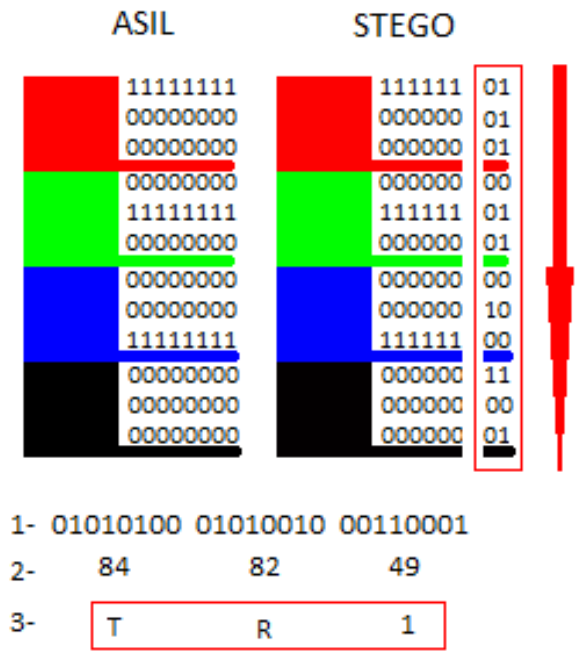
Bilinçli ve yöntemli olarak kullanılan bildiğimiz ilk kripto Scytale'dir. Antik Yunanda Ispartalıların uzak görevlere gönderilen askerler ve yöneticilerle bu yöntem ile haberleştiklerine dair M.Ö. 5. yüzyıla varan kayıtlar vardır. Boyları ve çapı aynı olan iki adet sopa hazırlanırdı. Bir tanesi göreve gönderilen askerler veya yöneticilere yanlarında taşımaları için verilirdi. Diğeri de merkez de tutulurdu. Gizli bir mesaj göndermek gerektiğinde papirüsten veya deriden eni çok dar uzunca bir şerit hazırlanırdı. Şerit sopanın etrafına boşluk kalmayacak şekilde özenle sarılır, mesaj sopa boyunca şeridin üzerine yazılırdı. Sonra şerit çözülür, anlamsız sıralı harflere dönüşmüş mesaj diğer sopanın bulunduğu görevli ya da merkeze gönderilirdi. Şerit tekrar aynı özenle diğer ikiz sopaya sarılarak şifre çözülürdü. Sopa yerine denizcilerin fıçı da kullandığı olurmuş.

Şekil 1 Temsili Scytale Sopası ve Şeridi

Steganografi

"Gizlenmiş yazı" anlamına gelen Steganografi tam anlamıyla bir kriptoloji yöntemi değildir. Mesajı şifrelemeden; aşina olduğumuz, dikkatimizi çekmeyecek ve bize doğal gelen nesne veya yöntemler ile katıştırmaktır. Tarihçi Heredot'un aktardığına göre M.Ö. 440 yıllarında İran'da bulunan bir Yunanlı, Pers istilasını bu yolla anavatanına haber vermiştir. Önce kölesinin saçını kazıtmış, dövme ile mesajı çıplak kafa derisine yazdırmıştır. Saçları uzayan kölesini haberci olarak Yunanistan'a göndermiştir. Mesaj kölenin saçı yeniden kazınarak okunmuştur.

11 Eylül saldırısının ardından radikal terör örgütlerinin fotoğrafta Steganografi yöntemini kullanarak haberleştikleri iddia edilmişti. İnsan gözü sandığımızın aksine küçük değişikliklere karşı çok duyarlı değildir. Küçük renk değişikliklerini ayırt edemez. 24 bit renk kalitesine sahip sayısal (dijital) bir fotoğrafın her noktasının (piksel) en düşük bir-iki bitini değiştirirsek fotoğrafta hissedilir bir farklılık oluşmaz.



Şekil 2 Fotoğrafta Steganorafi uygulaması

Şekil 2'deki asıl ve stego renkleri arasındaki farkı algılamaya çalışın. TR1 metni renk değerlerinin en düşük iki biti değiştirilerek resim içine yazılmıştır. Bu stego çalışmasını Windows Paint aracı ile özel renklere sayısal değerleri girerek hazırladım. Siz de kendinizi sınayabilirsiniz. Steganografinin güzel bir örneği de sayısal uydulardan önceki VHF, UHF frekansında yayınlanan teletekst sayfalarıdır. VHF, UHF frekansında yayın yapan TV formatında ekranda görünmeyen tarama boşlukları vardır. Sonradan bu boşluklar kodlanmış sayısal teletekst verileri eklenerek bilgilendirme sayfaları şeklinde değerlendirilmiştir. Televizyonda teletekst kipini seçmediğimiz müddetçe bu sayfalar görünmezler.

Şekil 3 TRT Teleteks sayfası

Akıllı telefonlara ücretsiz yüklenen onlarca uygulamanın ortamdaki sesleri telefonun mikrofonu aracılığıyla dinlediği ortaya çıkarılmıştı. O an izlediğiniz TV ya da radyo kanalı veya bulunduğunuz mekân bu uygulamalar tarafından sese kodlanmış stego ile tespit edilebiliyor. Telefon ekranına veya internette sörf yaptığınız sayfalarda takip ettiğiniz yayına, bulunduğunuz mekâna göre özelleştirilmiş reklamlar gösterilebiliyor. Shazam gibi bazı uygulamalara sesi içine özel sayısal kod yerleştirilmiş reklamları dinlettiğinizde size özel avantajlar sunabiliyor.

Sezar Şifresi

Kullanımında herhangi bir alet ya da matematik bilgisine ihtiyaç duyulmaz. Kolaylıkla kullanılabilmesinden midir, yoksa M.Ö. 100 yılında doğan ünlü Roma İmparatoru Julius Caesar tarafından geliştirilip kullanılmasından mıdır bilinmez oldukça ünlüdür. Alfabeyi ezbere bilmeniz şifrelerken ya da çözerken size kolaylık sağlar. Sezar alfabedeki her harfi kendisinden sonra gelen üçüncü harf ile değiştiriyordu. Her dilin alfabesine uygulanabilir ve isteğe göre harf değiştirme aralığı belirlenebilir.

Örneğin Julius Caesar'ın adını Sezar şifresine göre kendi alfabemiz ile kodlayalım. Önce ***ABCÇDEFGĞ HIİJKLMNOÖPRSŞTUÜVYZ*** şeklindeki alfabemizin sıralamasını her harfi 3 sağa öteleyerek değiştiriyoruz. ***Z*** harfine ulaşınca tekrar başa dönerek şöyle ***ÇDEFGĞHIİJKLMNOÖPRSŞTUÜVYZABC*** bir alfabe dizilimi elde ediyoruz. Yeni sıralamaya göre ***A*** yazmamız gereken yere ***Ç*** yazacağız. Bu kuralı diğer tüm harfler için de uygulayacağız. Bir kripto bundan daha basit daha masrafsız olamazdı. Sıralaması değiştirilmiş alfabemiz ile ***Julius*** kelimesini şifrelediğimde şu kodu ***MYOLYU*** elde ettim. Siz de ***Caesa***r kelimesi ile kendinizi deneyin. Sezar şifresi kriptoanalizin bilinmediği bir dönemde Roma ordusunun ihtiyaçlarını karşılıyordu. Günümüzde ise kriptoanalizin temel saldırı araçlarından olan dilin harf kullanım sıklığı istatistiklerinden yararlanmak suretiyle bu şifreli metni çözmek bir kahve içimi zamanınızı alır.

Şekil 4 Roma İmparatoru Julius Caesar

İslam Coğrafyasında Kriptoanaliz

Kriptoanaliz çalışmaları ilk olarak İslam'ın bilimsel araştırmalara teşvik ettiği Müslümanlar tarafından yapılmıştır. Arka Kapı dergisinin ilk sayısında yayınlanan bir önceki yazımda bahsettiğim "şifre" kelimesinin kökenini hatırlayınız. Hindistan'dan matematik, eski Yunan coğrafyasından doğa bilimleri, mantık ve felsefe öğrenen İslam dünyası bilimde kendi özgün katkılarını sunacak kadar ilerlemişti.

Ortaçağ'da kilise baskısıyla bilim ve bilimsel düşünce araçlarından yoksun kalan Avrupa'nın kriptoanaliz çalışmaları yapması elbette imkânsızdı. İslam coğrafyası matematik, istatistik, dilbilim gibi gerekli donanıma sahipti. Kriptoanaliz üzerine çalışmaları bulunan bazı bilim insanlarının bir listesi aşağıda verilmiştir. Şu an bu listeyi batılı internet sitelerinden derlemek Ortaçağ'daki rollerin yer değiştirdiğinin bir göstergesidir. Çok üzücü gerçekten…

Abdurraahman el-Halil İbn-i Ahmet (718-786) ***Kitab-ül Muamma*** (Kriptografik Mesajlar Kitabı)

Yunanca yazılmış bir şifreli mektubun çözümünü verir. Olası kelimeler yöntemini kullanır.

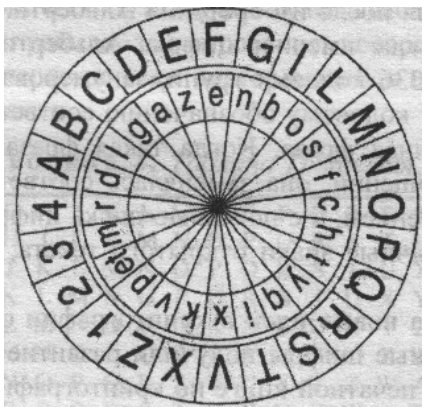
Al Kindi (801-873) ***Risāla fī Istikhrāj al-Kutub al-Mu'amāh*** (Kriptografik Mesajları Çözmek Üzerine İnceleme)

İstatistiğin babası sayılan Al Kindi temel kriptoanaliz yöntemlerinden olan Frekans Analizi'ni tanıttı.

- İbn Adlan (1187-1229) ***Al Mu'allaf lil-Malik el-Eşref***
- ibn ad-Duraihim (1312-1361) ***Miftah al-Kunuz fi Idah al-Marmuz*** (Gizli Yazıların Açığa Çıkmasının Anahtarı) Şifrelerin sınıflandırılması, frekans analizi gibi çok çeşitli konuları işler.
- Kalkaşandi (1355-1418) ***14 ciltlik Subh al-asha*** kriptoanaliz bölümü içerir. Kriptoanaliz için ilgili dili çok iyi bilmek gerektiğini vurgular.

Alberti Şifreleme Diski

İtalyan Leon Battista Alberti (1404-1472) tarafından 1466 yılında ***De Cifris*** başlıklı tezinde duyurulmuştur. Alberti batı dünyasında Kriptolojinin öncülerinden sayılırken, Alberti Diski kriptolojide bir mihenk taşıdır. *İslam Coğrafyasında Kriptoanaliz* başlıklı bölümünde bahsettiğimiz üzere müslümanlar tarafından Scaytale, Sezar Şifresi gibi yer değiştirme ve yerine koyma yöntemlerine karşı kapsamlı analizler yapılmıştı. Kriptoloji tarihi zaman dizgesini dikkate aldığımızda Alberti Diski'ni bu çalışmalara karşı geliştirilmiş bir araç olarak değerlendirebiliriz. Alberti Şifreleme Diski frekans analizi gibi yerine koyma, yer değiştirme şifreleme yöntemlerine karşı geliştirilen atakları boşa çıkartıyordu.



Şekil 5 Alberti Şifreleme Diski

Alberti Diski iç içe geçmiş iki diskten oluşuyordu. Her disk 24 hücreye bölünmüş ve aynı merkez noktasından sabitlenmişti. Şifreleme esnasında dıştaki disk sabit tutuluyor iken içteki disk döndürülüyordu. Dış disk üzerindeki büyük harfler alfabeyi temsil ediyorken iç disk üstündeki küçük harfler şifreleme indeksini belirliyordu.

Julius Ceasar'a atfedilen Latince "*veni vidi vici*" ünlü sözünü gelin beraber Alberti Diski ile şifreleyelim:

Şekilde görüldüğü üzere kolaylık olsun diye şifreli mesajı göndereceğimiz yer ile önceden şifre indeksi olarak ***g*** harfi üzerinde sözleşelim ve gizli tutalım. Metni şifrelemeye başlarken iç diski çevirerek ***g*** harfini dış diskteki büyük ***C*** harfi ile rastgele çakıştırdığımızı varsayalım. Şifreli metnimizin ilk harfi büyük ***C*** olur. Açık metnimizin ilk harfi olan ***v'***yi dıştaki diskten bulur ve iç diskteki karşılığını şifreli metnin ikinci harfi olarak küçük harfle yazarız. Şimdi şifreli metnimiz ***Cx*** oldu. Böylece devam ederiz. Metnin "veni vidi" kısmını bitirdiğimizde şifreli mesaj ***Cxzfbxbab*** olarak üretildi. Bu kadar yeter diyerek istediğimiz anda içteki diski yeniden rastgele çevirirriz. Yine kolaylık olsun diye bir adım saat yönünde çevirdim. Şifreleme indeksimiz olan ***g*** harfi artık ***D*** harfi ile çakışık hale geldi. Bu değişikliği çözümü yapacak görevliye bildirmek üzere şifreli metnimize büyük '***D' CxzfbxbabD*** ekleriz. Açık metnimizin kalan "..vici" kısmını indeksin yeni konumuna göre şifrelemeye devam ederiz. Dikkat ettiyseniz ilk bölümde örneğin ***i*** harfini ***b*** ile eşlemişken ikinci bölümde ***i*** harfini artık ***o*** harfi ile eşleşti. İndeksi her değiştirdiğimizde harf karşılıkları da değişmiş oluyor. Alberti Diski'nin kriptoanaliz saldırılarına karşı başarısı şifreli metinde çok fazla alfabe değişikliği olmasındadır. İşlemi bitirdiğimizde şifreli metnimizin tamamı ***CxzfbxbabD-koao*** olacaktır.

Şifreli mesaj karşı tarafa ulaştığında görevli önceden belirlendiği gibi iç diskteki ***g*** indeks harfini şifreli metnin başında gördüğü büyük ***C*** harfi ile çakıştırarak çözme işlemine başlar. Her büyük harfe geldiğinde indeks diskini yeniden ayarlayarak şifreyi çözmeye devam eder. İndeksi belirtmek üzere büyük harf kullanmak zorunluluk değildir. İndeksi değiştirme kuralları önceden de belirlenebilir. Alberti Şifreleme Diski'nin dış halkasında 1,2,3,4 rakamları da bulunur. Bu rakamlar ile daha önceden tablo halinde hazırlanmış ve her birine bir sayı verilmiş ön tanımlı işleri, emirleri karşı tarafa şifreli bildirmeye yarar. Bu kadar ayrıntılı açıklamayı hak ediyor değil mi?

Digraphic Şifreleme

Digraphic Şifreleme Giovanni Battista Porta (1535-1615) tarafından geliştirilmiştir. Porta henüz 28 yaşında iken 1563 yılında kriptoloji üzerine yazdığı *De Furtivis Literarum Notis* isimli eserini yayımladı.

Digraphic Şifreleme'de her harfi bir harf çifti temsil eder. Porta Kriptoloji yöntemlerini harflerin yerlerinin değiştirildiği ***yer değiştirme*** ve harflerin birbirinin yerini aldığı ***yerine koyma*** olarak iki sınıfa ayırmıştır. Bu sınıflandırma bugün de kullanılmaktadır.

Charles Wheatsone 1854 yılında daha gelişmiş bir Digraphic

Şifreleme duyurdu. Wheatsone sistemin kullanımını teşvik etmek için Lord Playfair ismini verdi. Playfair herhangi bir araç gerektirmediğinden kuralları ve anahtar kelimeyi bilmek kullanmak için yeterliydi. İngiliz alfabesinde 26 harf vardır. I ve J harfi birbirine eşitlenip anahtar kelimeyi kullanarak 5x5 bir tablo oluşturulur.

Biz 29 harflik alfabemiz için 5X6'lık bir tablo oluşturacağız. Anahtar kelimemizi de CUMHURİYET seçelim. Anahtar kelimemizi tablonun sol üst köşesinden başlayarak her harfini bir hücreye yazıyoruz. Anahtar içerisinde tekrarlayan harfleri atlıyoruz, yazmıyoruz. Örneğin anahtar kelimemizde U harfi iki defa kullanıldığı için ikincisini yazmıyoruz. Tablonun kalanını alfabenin diğer harfleri ile dolduruyoruz. En son boş hücreye beş(5) yazdım.

C	U	M	H	R
İ	Y	E	T	A
B	Ç	D	F	G
Ğ	I	J	K	L
N	O	Ö	P	S
Ş	Ü	V	Z	5

Şifrelenecek metnimiz de "***ORDULAR İLK HEDEFİNİZ AKDENİZDİR, İLERİ***" olsun. Önce açık mesajı ikili gruplara ayırıyoruz. Örnek mesajımız artık "***OR DU LA Rİ LK HE DE Fİ Nİ ZA KD EN İZ Dİ Rİ LE Rİ***" formatında olur.

Şifreleme esnasında **4** basit kural uygulanır:

1-Eğer harf çiftinde her iki harf aynı ise veya en sonda tek harf kalırsa ilk harfin sağına (Playfair'de X) 5 (beş) yazacağız.

2-Harfler tablonuzun aynı satırında görünüyorsa hemen sağındaki harfle değiştirin. Eğer harfleriniz satırın en sağındaysa satırın başından itibaren değiştirmeye başlayın. Örnek harf çiftimiz **TR** olsun

*	*	*	*	*
*	T	Y	R	Z
*	*	*	*	*
*	*	*	*	*
*	*	*	*	*
*	*	*	*	*

TR -> YZ

	*	*	*	*
	*	*	*	*
	*	*	*	*
	T	R	C	*
	*	*	*	*
	*	*	*	*

TR -> RC

3-Harfler tablonuz aynı sütunda görünüyorsa hemen sağındaki harfle değiştirin. Eğer harfleriniz sütunun en altındaysa sütunun başından itibaren değiştirmeye başlayın. Örnek harf çiftimiz **TR** olsun

*	*	T	*	*
*	*	B	*	*
*	*	*	*	*
*	*	*	*	*
*	*	R	*	*
*	*	Y	*	*

TR -> BY

*	*	*	*	*
*	*	*	*	*
*	*	R	*	*
*	*	T	*	*
*	*	L	*	*
*	*	*	*	*

TR -> IT

4-Harfler tablonuzun aynı sütununda veya aynı satırında görünmüyorsa orijinal harf çiftinin oluşturacağı dörtgenin aynı satırındaki köşeye gelen harfle değiştirin. Örnek harf çiftimiz **TR** olsun.

Z	*	*	T	*
*	*	*	*	*
*	*	*	*	*
*	*	*	*	*
R	*	*	F	*
*	*	*	*	*

TR -> ZF

Her şey hazır olduğuna göre kuralları uygulayarak metnimizi şifreleyebiliriz. Açık metnin ilk "**OR**" harf çifti ile başlıyoruz

C	U	M	H	R
İ	Y	E	T	A
B	Ç	D	F	G
Ğ	I	J	K	L
N	O	Ö	P	S
Ş	Ü	V	Z	5

Harf çiftimiz 4. kurala uyan bir konumda yerleşmiş. Kuralı uyguladığımızda **OR->SU** dönüşümünü elde ederiz. Şifreli metnimizin ilk çifti **SU** oldu. Açık metnin ikinci harf çifti **DU**' da 4. kurala uyar**, DU->ÇM** dönüşümünü verir. Yeni harf çiftini şifreli metnimize "**SUÇM**" ekliyoruz. Açık metnin sıradaki harf çifti **LA**' ya 3.kurala uyguluyoruz. **LA->GR** dönüşümünü elde edip şifreli metnimize "**SUÇMGR**" ekliyoruz.

C	U	M	H	R
İ	Y	E	T	A
B	Ç	D	E	G
Ğ	I	I	K	L
N	O	Ö	P	S
Ş	Ü	V	Z	5

Açık metnin kalan çiftlerini tablodan işaretleyip ilgili kuralları uyguladıktan sonra "***SUÇMGRCALGMTJDBTĞC5TJFİÖTŞBECAJACA"*** şifreli metni elde ederiz. İşlemin devamını ve benim kodlamamın sağlamasını dikkatli okuyucularımıza bırakıyorum.

Kodun çözümü için kodlama yaparken kullandığımız tabloyu yeniden oluşturmak ve şifreli metne sanki açık metin şifreliyormuş gibi kuralları uygulamak yeterli. Şifrelenmiş metnin ilk çiftinin çözümü **SU->OR**

C	U	M	H	R
İ	Y	E	T	A
B	Ç	D	E	G
Ğ	I	I	K	L
N	O	Ö	P	S
Ş	Ü	V	Z	5

Vigenère Şifresi

Fransız Vigenère'in (1523-?) geliştirdiği ve tarihte ilk defa bir kelime ya da cümleyi anahtar kullanan şifreleme yöntemidir. Anahtar kullanımında sonradan geliştirilen sistemlere ilham olmuştur. Şifreleme işlemi Vigenère Karesi yardımı ile yapılır. Tablonun en üst satırı şifrelenecek açık metnin harflerini temsil eder. En solda bulunan sütun ise anahtar harflerini gösterir. Açık metne ait bir harfi üstteki satırda bulup sırası gelen anahtar harfi en sol sütundaki ile çakışan hücreyi şifrelenmiş harf olarak kullanırız.

Örnek şifreleme göstermek amacıyla anahtar kelimemizi **ANITKABİRTÜRKİYEDİR** olarak belirleyip işe koyuluyoruz. Çok önemli atlatma bir haberi şifreleyip ajansımıza geçiyoruz "***Arka Kapı Dergi tanıtımı 17 Şubat'ta Abaküs Çırak Atölye'de yapıldı***"

Tabloda açık metnin ilk harfi **A**'yı en üst satırda ve anahtar kelimenin ilk harfi **A**'yı en sol sütunda çakıştırıyoruz. Çakışan hücredeki **A** şifrelenmiş ilk harfimiz**,** açık metnin ikinci harfi **r** ve anahtar kelimenin ikinci harfi **N**'yi çakıştırıyoruz. Sonuç **G** ve şifreli metnimiz şu an **AG** oldu. İşlemi açık metnimiz bitinceye kadar tekrar ediyoruz. Anahtarın en sonuna gelindiğinde tekrar anahtarın en başındaki harften itibaren şifreleme işlemine devam ediyoruz.

Sonunda elde ettiğimiz şifreli metin şöyle "**AGTTV ARSUZ NYUEY SLEBM VYIEE LŞPNR SKESE DJRKJ CVTRB UROLE İNCIC İIIBL D**" oluyor. Okunması kolay olsun diye 5'li gruplara ayırdım.

Çözümü ise gayet kolay. Anahtarın ilk harfini en soldaki sütunda bulup şifreli metnin ilk harfi ile çakışan hücreye kadar yatay sağa ilerliyoruz. Çakışan hücre ile en üst satırdaki harfi eşliyoruz. Açık metnin ilk harfine ulaşmış oluyoruz. Anahtar kelime bitince anahtarın en başındaki harften tekrar başlayarak şifreli metni bitirinceye kadar devam ediyoruz.

	a	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r	s	ş	t	u	ü	v	y	z
A	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
B	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A
C	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B
Ç	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C
D	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç
E	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D
F	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E
G	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F
Ğ	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G
H	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ
I	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H
İ	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I
J	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ
K	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J
L	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K
M	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
N	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M
O	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N
Ö	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O
P	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö
R	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P
S	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R
Ş	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S
T	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş
U	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T
Ü	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U
V	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü
Y	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V
Z	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y

Şekil 6 Vigenère Karesi

Sonraki sayıda görüşmek üzere hoşça kalın.

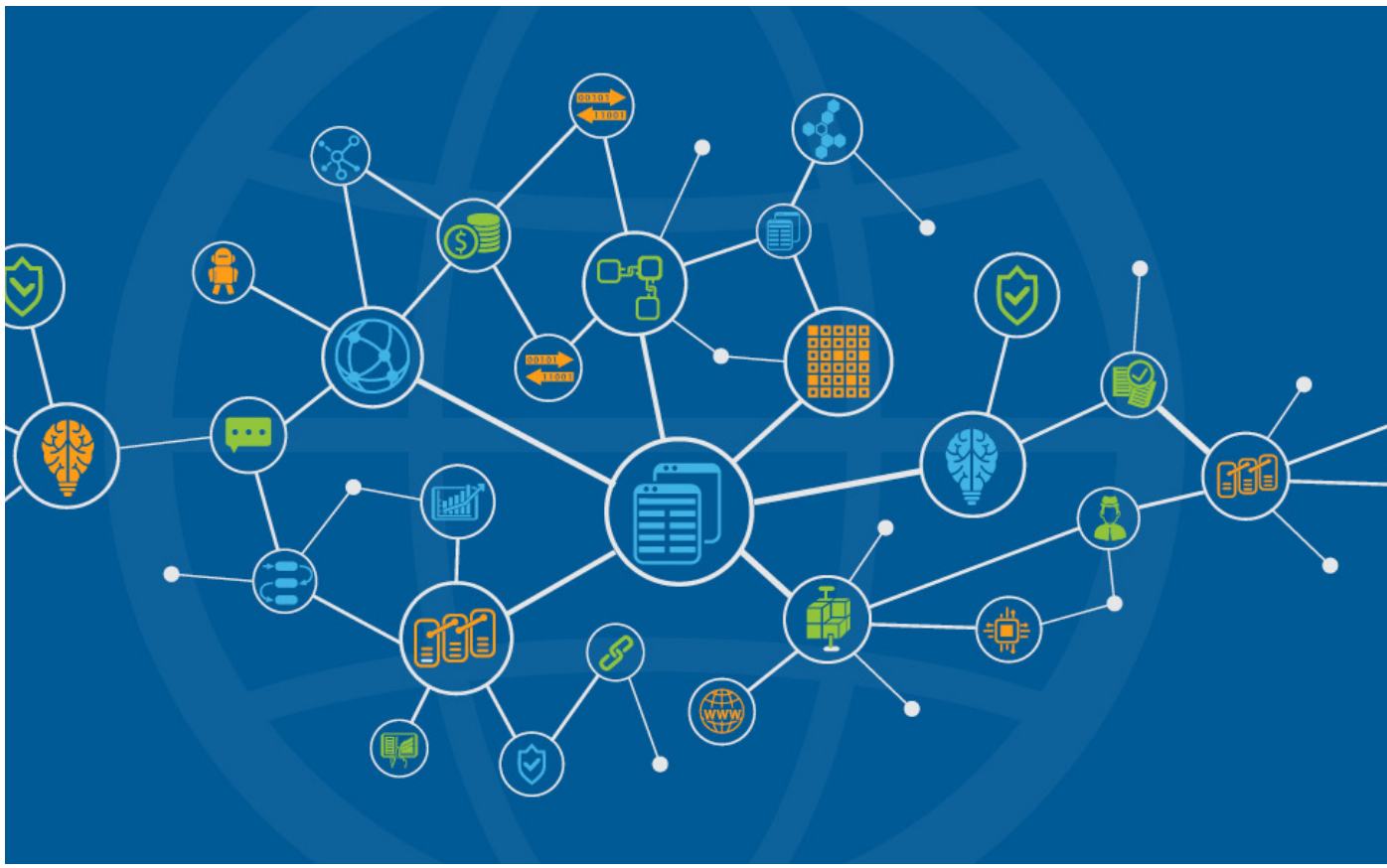
Mert Susur - mail@mertsusur.com

Kral Çıplak Diyebilmek Blokzincirinin Kısıtları

Veri Saklama Sorunları ve Çözümleri

Blokzinciri teknolojileri Türkiye'de olduğu gibi dünyada da geniş bir şekilde tartışılıyor. Geçtiğimiz 10 ay boyunca en popüler olduğu zamanları yaşadık dersem sanırım pek de yanılmış sayılmam. Bunun en büyük nedeni şüphesiz ki birçok farklı teknolojinin ortaya çıkması ve bu popülerlikten beslenerek borsalarda işlem gören kripto paraların değerlerinin bir anda artıp azalmasıydı. Yani tüketim amaçlı birçok kişinin bu işe para yatırması ve bazen kazanıp bazen kaybetmesi de bu popülerliği peşinden getirdi diyebiliriz.

Şu anda yüzlerce kişi, grup ya da firma bu teknolojinin kullanım alanlarını arıyor ve uygulamaya çalışıyor. Hatta birçok konferans ya da toplantıya gittiğinizde, özellikle ülkemizde, herkes bunun ne kadar da harika bir teknoloji olduğundan ve bu teknolojinin dünyaya nasıl fayda getireceğinden bahsediyor. Peki düşündüğünüzde şu anda günlük hayatınızda kaç tane blokzinciri uygulaması kullanıyorsunuz? Ya da bu kadar çok kullanım alanı olan bu harika teknolojinin hiç mi bir problemi ya da derdi yok? Yani demek istediğim, neden şu anda birçok firma bu alanda geliştirmeler yapıp sizlere hazır ürünler sunamıyorlar?



Evet ben de bu yazımda tam olarak bu teknolojinin '**kötü özelliklerinden**' bahsediyor olacağım. Çünkü bir yazılımcı olarak biliyorum ki eğer elinizde sadece çekiç varsa her şeyi çivi olarak görmeye başlayabilirsiniz ve bunun önüne geçmek için o çekiç ile neler yapamayacağınızı çok iyi anlamanız potansiyel olarak ileride yaratabileceğiniz sorunları önlemek açısından çok önemlidir. Tam da bu noktada Javascript Guru'su olan Douglas Crockford'ı anmadan geçemeyeceğim. Kitaplarında bahsettiği gibi '*her yazılım teknolojisi iyi ve kötü taraflarını kendi içinde barındırır, eğer o yazılım dilini çok iyi kullanmak istiyorsanız iyi yönlerini kullanıp kötü yönlerinden kaçınmanız gerekmektedir*'. Bunun için ne yazık ki günlerinizi hatta belki de gecelerinizi ayırıp bu teknolojiyi çok iyi bir şekilde öğrenmeniz gerekir. İsterseniz lafı çok da uzatmadan Türkiye'de herkesin konuşmaktan çekindiği bu kötü detaylara girelim. Bu yazıda öncelikle veri saklama sorunlarına odaklanmaya ve gelecek yazılarda da farklı sorunları ve bunların çözümlerini anlatmaya çalışacağım.

Veri saklama sorunları

Blokzinciri temelinde bir veri tabanı gibi tasarlanmıştır ve ilk tasarım amacı kısıtlı bir boyuta sahip olan işlem ve transfer bilgilerini güven ihtiyacı olmadan saklamayı hedeflemektedir. Hatta ilk tasarımı Satoshi Nakamoto'nun makalesi olarak kabul edersek hiçbir veri barındırmayan bir blok başlığının 80 Byte yer tutacağı ve her 10 dakikada bir blok üretileceği kabul edilirse bir yılda 4.2MB veri saklayacağı hesaplanmıştır.1 Tabi şu anda Bitcoin'in veri tabanı boyutu 2008 yılından itibaren yaklaşık olarak 160,124 MB civarına ulaşmış durumda. Bunun yanında Bitcoin de veri saklamak için tasarlanmamıştır dersem yanlış bir şey söylemiş olmam. Çünkü adından da anlaşılacağı gibi bir elektronik para sistemi olarak tasarlanan bu teknolojinin asıl amacı değer transferlerini gerçekleştirebilmektir.

Diğer taraftan Ethereum'u ele alırsak teknik olarak çok ciddi farklılıklar göreceğiz, detaylarına girmeden çok kısaca hatırlatmak gerekirse Ethereum da akıllı kontratlar kurup geliştirdiğiniz merkezi olmayan uygulamalarını geliştirebileceğiniz bir blokzinciri platformu. Bu platform içerisinde yazılımlarınızı kurup kullanıma açmak istiyorsanız ya da benzer şekilde başkaları tarafından kurulan uygulamaları kullanmak ve değer transferi yapmak istiyorsanız her yaptığınız işlem için bir bedel ödemeniz gerekiyor. Bu bedelin maddi özellikten bağımsız adına gas deniyor. Bu gas değeri gas price adı verilen bir birimle çarpılıyor ve madencilere ödül olarak dağıtılıyor. Örneğin 5 gas ödemeniz gerekiyorsa bu durumda eğer gas price değeri 10 Ether ise bu işlem için ödemeniz gereken tutar 50 Ether oluyor. Bu durumda gas en basit haliyle madencilerin zahmetinin karşılığı olarak tanımlanabilir. Peki madenciler ne gibi bir zahmete giriyorlar?

Madencilerin blokzinciri teknolojisindeki önemini biliyoruz, Ethereum özelinde konuşursak eğer madencilerin bir başka yaptıkları şey de blok içerisindeki akıllı kontrat çağrılarını gerçekleştirmek. Eğer bu sırada akıllı kontratlar veri saklama işlemleri yapıyorlarsa bu durumda madenciler bu veriyi de kontratın son durumuna işleyecekler ve karşılığında ödüllerini alacaklardır.

Gavin Wood'un yazdığı 38 sayfalık Ethereum Yellow Paper dokümanında bu gas konusu matematiksel modeliyle ciddi bir şekilde ele alınıyor.2 Şimdi bu dokümana göre veri saklamanın maliyetini çıkartalım. Dokümanda, 256 bit'lik bir word değerini saklamanın bedelinin 20 gas olduğu söyleniyor. Yani basit bir hesapla 1 KB veri saklamanın bedeli aşağı yukarı 640,000 gas olacak ve bugün ortalama gas price değeri 80 gwei (0.00000002 Ether) olarak kabul edersek 1 KB veri saklamak için 0.512 Ether gibi bir ücret ödemem gerektiğini görebiliriz. Tabii ki bu durum sürdürülebilir değil.

Dolayısıyla eğer hayalini kurduğum projemde Ethereum ağını kullanarak uygulamalar geliştireceksem ve merkezi olmamak adına tüm verilerimi blokzinciri içinde tutmayı hayal ediyorsam ciddi bir miktar yatırımı gözden çıkartmam gerektiği aşikar.

Blokzinciri veri depolama çözümleri

Yukarıda sizlere çok kötü bir tablo çizdiğimin farkındayım, ama azıcık daha sabredin. Sizlere bir iyi bir de kötü haberim var. İyi haber, merak etmeyin veri depolama sorunları için çok güzel bir kaç tane çözüm var. Kötü haber ise bu yazının yazıldığı tarih itibariyle hiçbiri canlı sistemlerde çalışacak kadar olgunlaşmış değil.

Bunlardan bazıları; Filecoin, Sia, StorJ ve Swarm. Bu yazının devamında en yakından inceleyip yakında üzerinde proje geliştirmeye başlayacağım için en hakim olduğum Swarm hakkında size detaylar vermeye çalışacağım.

Nedir bu Swarm?

Ethereum topluluğunun birçok farklı blokzinciri projeleri mevcut. Bunlara *Web 3 Stack* deniyor. Bazılarına örnek vermem gerekirse, merkeziyetsiz ve uçtan uca şifreli bir mesajlaşma platformu olan *Whisper*, anlık değer transferlerine izin veren blokzincirinin üzerinde çalışan Raiden bunlardan bazıları. Bunları başka bir zaman tekrar konuşuruz, ama şu anda Swarm üzerine tartışmaya devam etmek istiyorum.

1 Bitcoin: A Peer-to-Peer Electronic Cash System - https://bitcoin.org/bitcoin.pdf

2 Dr. Gavin Wood - Ethereum: A Secure Decentralised Generalised Transaction Ledger Byzantium Version - https://ethereum.github.io/yellowpaper/paper.pdf

Swarm projesinin amacı yeni dünya düzeninde merkezi olmayan bir veri depolama çözümü sunmak. Bu proje kapsamında birçok güvenlik sorunu da var, örneğin DDoS saldırıları ve erişim kısıtlamalarının doğru çalışması bizim için en önemli sorunlar. Farklı saldırı vektörlerinin gerçekleşmesi durumunda ağın dosya sağlamaya devam etmesi ve sorunsuz bir şekilde hizmet verebiliyor olması çok önemli. Swarm ekibi de bu özellikleri sağlayabildiklerini düzenli iterasyonlarla ispat edebilmek için PoC (Proof of Concept) çalışmaları yapıyorlar. 2018 yılının ikinci çeyreğinde dördüncü PoC'lerini yayınlayacaklar ve bu versiyonda birçok ilginç özelliği hayata geçirecekler.

Nasıl çalışır diye sorduğunuzu duyar gibiyim. Birazdan bunu anlatmaya başlayacağım ancak bundan önce söylemem gereken çok önemli bir şey var. Bu yazının yazıldığı sırada yani 2018 yılının ilk çeyreğinde var olan özellikler okuduğunuz zamana bağlı olarak olabilir ya da olmayabilir. Hatta çalışma yöntemi tamamen değişmiş olabilir. Dolayısıyla bu ürünü kullanmaya başlamadan önce dokümantasyonunu okuyarak başlamanız çok ama çok önemli.

Ağ üzerinde çalışan her düğümün (Node) kendisine özel bir adresi bulunur. Bu adresleri kullanarak farklı örneklere (instance) erişmek mümkün olabilir. Yani adresini bildiğiniz bir istemciye ulaşabilirsiniz ve P2P bir bağlantı kurabilirsiniz böylelikle dosyalarınıza ulaşabilirsiniz. Swarm ağına gönderdiğiniz dosyalar bzz protokolü adı verilen bir alt protokol sayesinde diğer istemcilere ulaşır. Bu protokol de bildiğimiz Ethereum protokolü olan Devp2p protokolünü kullandığı için herhangi bir Ethereum istemcisi üzerinden (örneğin; ethereum geth) çalışabilir şekilde tasarlanmıştır. Zaten PoC 0.2 versiyonu halihazırda elinizde yüklü olan geth içerisinde de mevcuttur.

Diyelim ki ben bir dosya göndermek istiyorum, bu dosyayı göndermek için seçtiğimde istemciler bu dosyayı en fazla 4K olmak olacak şekilde küçük parçalara ayırırlar ve bunların her birini bir hash fonksiyonundan geçirerek hash değerlerini üretirler. Böylelikle ellerinde bir Merkle İspatı oluşturabilecekleri bir ağaç elde etmiş olurlar. Böylece ağacın herhangi bir dalına rastgele bir şekilde erişmeniz de önlenmiş olur. Yani başka bir deyişle, ağacın tamamını bilmeden dosyayı anlamlı bir şekilde yeniden oluşturamazsınız. Ancak eğer küçük parçalara hangi sırayla erişebileceğinizi bilirseniz o zaman bunların arasında atlamalar yapabilirsiniz. Bu özellik sayesinde video yayını yapmak ya da video kareleri arasında atlamak da tabii ki nispeten kolaylaşacaktır. Ancak burada hangi video codec'ini kullandığınız da ayrı bir önem kazanır.

Ancak dikkat etmemiz gereken bir nokta daha bu verilerin asla değiştirilemez ve silinemez oluşu. Yani Swarm sizin diskiniz gibi veri saklayıp sürekli düzenleme yapabileceğiniz bir ortam değil. Bunun yerine verilerinizi yükleyip sonsuza kadar saklayacağınız bir platform.

En iyi kullanım alanları bana kalırsa video, resim ya da belgelerin saklanması olabilir. Ancak yine ufak bir uyarıda bulunmakta fayda görüyorum: şu andaki versiyonu itibariyle Swarm henüz verileri şifrelemiyor. Dolayısıyla özel ya da hassas bilgilerin bu platformda saklanması henüz doğru değil. Ekibin gelecek planları özel ya da genel bir şekilde veri saklamaya izin verileceğini gösteriyor ancak platform henüz bunun için hazır değil.

Burada veri saklamanın henüz bir ekonomik modeli yok. Çünkü platform henüz tamamlanmış değil. Ancak iki tane olası gelir modelinden bahsediliyor, verilerin geçebilmesi için taşıma görevini üstlenecek servisler taşıdıkları veriye oranla bir ödül alabilirler ya da veri saklayanlar sakladıkları kadar bir ödül alabilirler. Ama bunların hepsi tabii ki tahmin. Henüz netleşmiş bir şey yok. Fakat ileride madencilik yerine kenara attığınız USB disklerinizi çıkartıp veri saklayarak da Ether kazanabileceksiniz gibi duruyor.

Şimdilik yazımı bitirirken bir kaç konuya daha değinmek istiyorum. Türkiye'de blokzinciri alanı gerçekten gelişmeye çok açık. Ancak bir şey bildiğini iddia eden fakat derinlemesine konuşmaya başladığınızda aslında konuya giriş seviyesinde hakim olduğunu anladığınız çok fazla kişi var. Bu yüzden artık Blokzinciri nedir? Nasıl çalışır? Konularından çok işin teknik detaylarına girmemizin zamanı geldi de geçiyor. Bu yüzden bu konuyla ilgili birçok kaynak üretmeye çalışıyoruz ve yardım isteyen herkese yardımcı olmaya çalışıyoruz. Yazılım geliştirme topluluğundaki herkesin böyle bir ödevi olduğuna inanıyorum ve elimden geleni yapmaya hazırım. Umarım daha fazla kişiye ulaşıp Türkiye'de bu alanın gelişmesine katkı sağlayabiliriz.

Esen Kalın.

Musa Baş - sabloninsanlar@gmail.com

Derinlemesine Ethereum I. Bölüm

Bir önceki yazımda Bitcoin, Blockchain, akıllı sözleşmelere değinmiştim. Bu yazı serisinde ise Ethereum'u biraz daha derinlemesine incelemeye çalışacağım.

Ether Birimleri

Bitcoin'in alt birimi olan Satoshi'yi hepimiz az çok duymuşuzdur ya da Türk Lirasının alt birimi olan kuruşu hepimiz biliriz. Ether de bu şekilde birden fazla birime sahiptir. Kwei, Gwei'yi transfer yaparken ya da akıllı sözleşme imzalarken işlem bedeli olarak (gas) öderken görmüşsünüzdür.

Şimdi 1 Ether'in diğer birimlere karşılık olan değerlerine bakalım.

Wei	1000000000000000000
Kwei, Ada, Femtoether	1000000000000000
Mwei, Babbage, Picoether	1000000000000
Gwei, Shannon, Nanoether, Nano	1000000000
Szabo, Microether,Micro	1000000
Finney, Milliether,Milli	1000
Ether	1
Kether, Grand,Einstein	0.001
Mether	0.000001
Gether	0.000000001
Tether	0.000000000001

Elinizde bulunan Ether'in birimlere karşılık gelen değerlerini https://etherconverter.online adresinden öğrenebilir ya da Google üzerinden arama yaparak farklı dönüştürücü sitelerden karşılıklarını elde edebilirsiniz.

Gas Price ve İşlem Maliyetleri

Ethereum ağında yapılan işlemler için ödediğimiz masrafları *gas* olarak isimlendiriyoruz. Bu masraflar en kaba tabiriyle Ethereum ağında yapacağımız transfer ya da akıllı sözleşmelerin çalışmasında, madencilerin harcadığı eforun karşılığıdır. Bu kısma çok detaylı değinmeyeceğim, dergimizin bu sayısında Mert Susur bu konuya biraz daha derinlemesine giriyor, tekrara düşmemek adına kısa tutuyorum.

Ethereum Sürümleri

Ethereum sürekli güncellenen ve geliştirilmeye açık bir yapı. Şu an bildiğimiz 4 adet sürüm var, bu sürümler Frontier, Homestead, Metropolis, Serenity.

Bu sürümler ilerleyen dönemlerde ihtiyaca göre artabilir, bu konuda bir kesinlik yok tabii ki.

Bu sürümler kendi içlerinde de belirli aşamalarla Ethereum ağına dahil edilecek.

Frontier: Ethereum'un ilk defa hayatımıza girdiğinde kullanılan sürümüdür.

Homestead: Yakın zamana kadar kullandığımız Ethereum'un kararlı sürümlerinden biridir.

Metropolis: Byzantium ve Constantinople olarak iki aşamayla tamamlanacak olan sürümdür. Metropolis sürümünün ilk ayağı olan **Byzantium** şu an aktif olarak Ethereum ağında çalışmaktadır.

Serenity: Gelecekte kullanacağımız ve an itibariyle bilinen son sürüm olacaktır.

Yukarıda belirtmiş olduğumuz ve aktif olarak kullandığımız Metropolis sürümünün Ethereum ağına neler katacağını ayrıntıları ile inceleyelim.

İki aşamadan oluşan Metropolis sürümünün ilk ayağı Byzantium başarılı şekilde çalışmaktadır.

Metropolis Sürümü Bize Neler Getirecek?

ZK-Snarks: Zero-Knowledge Succinct Non-Interactive Argument of Knowledge kısaltmasıdır. Türkçeye ise *sıfır-bilgi interaktif olmayan bilgi argümanları* olarak çevirilmiştir.

Bu özellik Zcash'de de karşımıza çıkmaktadır. En kısa tabiriyle elimizdeki bilginin tamamını göstermeden, o bilgiye sahip olduğumuzu göstermektir. Sıfır bilgi ispatı üzerine kuruludur bu yapı. Sıfır bilgi ispatıyla ilgili daha detaylı bilgiyi "Sıfır Bilgi Ispatı" olarak Google'da aratırsanız ulaşabilirsiniz.[1]

Peki Zk-Snarks akıllı sözleşmelerde nasıl kullanılır ve bizim ne işimize yarayacak?

Ziyahan ile Mert'in bir anlaşma yaptığını ve bu anlaşma karşılığında Ziyahan'ın 10 Ether alacağını varsayalım. Ziyahan 3 adımdan oluşan bir işlemler dizisini gerçekleştirdiğinde 10 Ether'i alacaktı ve bu yapacağı işlemlerin de bir takım ticari sırlar olduğunu varsayalım bu durumda Mert'e bu işlemleri yaptığını göstermesi gerekecek ve gösterirse ticari sırları açığa çıkacaktır. İşte tam da bu durumda Ziyahan'ın imdadına Zk-Snarks yetişiyor: Gerçekte tam olarak ne yaptığını göstermeden, işlemin sadece bir parçasını göstererek kendisini kanıtlamış ve Mert'e karşı dürüst olduğunu göstermiş oluyor.

Revert, Return Data: Bir sözleşmenin çalıştırılması için belirli bir maliyetimizin olduğunu belirtmiştik daha önce, bu maliyet içerdiği operasyonlara göre sözleşmeden sözleşmeye göre değişmektedir.

Bir sözleşmenin eski haline dönmek istediğimizde ya da hata fırlatmak istediğimizde, sözleşme üzerindeki tüm gas'ı tüketiyordu. Bu da maliyet demekti. Bu güncellemeyle birlikte throw (fırlatma) işlemini gerçekleştirdiğimizde, kullanılmayan gas miktarı sözleşme sahibine iade edilecektir.

Return Data ise dönen verinin bir kopyasının bize sunulmasıdır.

Zorluk Bombası: Madenciliğin git gide zorlaşması için devreye alınacak olan geliştirmedir. Bu geliştirme POW'dan POS'a geçişin ara bağlantısı olacaktır. Madencilik oldukça zorlaşacağı için, POS'a geçmek zorunda kalacak madenciler.

Casper Algoritması

POS'u uygulamak için Casper Algoritması[2] kullanılacaktır. Casper Algoritması dürüst madencileri teşvik edip, sahtekar madencilerin cezalandırılması üzerine kurulmuştur. POW'dan POS'a geçişi kolaylaştırmak için her 100. blokta POS kullanılacak, geçiş süreci boyunca POW kullanılmaya devam edecek. Bir madenci olarak varlığınızı kötü yönde kullanırsanız, varlığınız elinizden alınacaktır. Konunun detaylarını ve teknik olarak nasıl uygulanacağını ileride daha detaylı göreceğiz.

Şimdilik yazıma burada son veriyorum, bir sonraki yazıda görüşmek üzere.

1 http://bilgisayarkavramlari.sadievrenseker.com/2009/06/22/sifir-bilgi-ispati-zero-knowledge-proof/

2 https://github.com/ethereum/research/wiki/Casper-Version-1-Implementation-Guide

Mihraç Cerrahoğlu - mihrac.cerrahoglu@gmail.com

Blockchain Tabanlı Telif Hakları Projeleri

Türkiye'de Blockchain'e Bakış ve Projesizlik

Türkiye'de Blockchain anlayışı maalesef Bitcoin'in borsa fiyatı üzerinden yapılan geyiklerden öteye gidemiyor. Bitcoin, Smart Contract ve Ethereum üzerine dikkate değer çalışmalar elbette var ama ülkemiz sınırları içinde bunu ciddiye alıp üzerine eğilen insan sayısı çok az.

Bununla ilgili araştırma yaptığımızda Mert Susur ve Onur Aykaç gibi bu konuda bilgi paylaşımında bulunup hatta bunun ötesine geçip eğitim modelleri geliştiren isimleri de es geçmek haksızlık olur. Inoix ve Codefiction çatısı altında toplanan bu grup, toplu adım atmak ve topluma değer katmak adına takip ve taktir ettiğim girişimlerde bulunuyorlar. Bu bilgi, konuyu araştırmak isteyen okurlarımız için bir kenarda dursun.

Bunun dışında sosyal medya üzerinde Blockchain teknolojisi altında üretilen projeleri tanıtıp ne kadar güvenilir veya ütopik olduğunu vurgulayan isimler de mevcut. Bu isimleri çıldırtan örneklerden bahsedersem, yurttaşlarımızın Blockchain penceresinden dünyaya nasıl baktığını özetlemiş olurum sanırım.

Açıklama: X Coin projesi cihazlar arası iletişimi X yöntemiyle sağlayıp, araçların kendi aralarında otomasyon yöntemiyle iletişimini sağlayacak. Bu proje içinde ödeme yöntemi olarak da kendi X coinlerini kullanmayı planlıyorlar ve gelecek için heyecan verici.

Gelen birinci yorum: Usta ay sonuna X100 yapar mı sence alalım mı?

İkinci yorum: Yok ya hu! Marketcap'ına baksana, yerlerde sürünüyor.

Bunun gibi onlarca yorumu tek paylaşım altında görmemiz mümkün ve bu bizim resmimiz.

Ülkemizde ilk Blockhain proje örneklerine de bakalım diyeceğim ama içim el vermiyor. Sadece Bitcoin gibi para özelliği olan ve elde tutulur bir cüzdan bile paylaşıma sunamayan ünlü projelerden bahsediyorum.

- Biz bir coin çıkardık alın!
- Projeniz nedir?
- İşte kripto parayız biz. Aynı Bitcoin gibi.
- Dediğin gibi, Bitcoin başta olmak üzere bir sürü kripto para var zaten. Farkınız yani projeniz nedir?
- Biz ondan daha iyi olacağız. Şöyle değerleneceğiz, böyle zengin edeceğiz…
- ...

Unutmayın Blockchain projelerinin coinleri şirket hisseleri gibidir. Hatta devlet paraları gibi düşünebilirsiniz. Coin alıyorum demek, "Bu projeye yatırım yapıyorum. Hisse alıyorum" demektir. Her coin üretiyorum diyen ICO'lara yatırım yapılmaz. Elle tutulur aktif projeleri veya ürünleri olması daha samimi değil mi? O halde bu sayıdaki tematik projelere göz atalım:

Telif Haklarını Koruma ve Ödeme Yöntemleri Üzerine Geliştirilen Blockchain Projeleri

Günümüzde internetin yaygınlığına paralel olarak içerik paylaşımı ve bunun tüketimi de aynı hızda artmaktadır. Bu toplumsal gelişim ve içeriğe ulaşma konusunda hız kadar kolaylık da kazandırmıştır. Tüketici açısından bu kolaylık üretici açısından kâbusa dönüşebiliyor. Paylaşılan bir makale, sanat eseri ya da dijital ürünün internet üzerinde kopyalanıp başka kâr simsarları tarafından kullanılması oldukça popülerleşti. Müzik ve video eserleri için Youtube önlemler alsa da, kendisinin

izlenim oranlarına göre ödeme politikasının ne kadar adil olduğu hâlâ tartışılmaktadır. Üstelik merkezi sistemler olması da sizi gelir ve ürün güvenliği konusunda bir firmaya güvenmeye zorluyor. Şu an için çok büyük problem gibi görünmese de Blockchain teknolojisinin her alana girmesiyle bu konuyu tartışmak gayet doğal olacak. Peki bu mevzuyu düşünüp, kafa yorup proje geliştiren topluluklar yok mu? Elbet de var. O zaman doğrudan Blockchain üzerine kurulu ya da kısmen onunla ilişkilendirilmiş projelere bir göz atalım.

Peertrack: Müzik eserleri servisi. Tıpkı Spotify ya da Audio Jungle gibi. Fakat ödeme işlemini direkt olarak kripto paralar ile yapabilirsiniz ve banka bilgilerinizi vermenize gerek yok. İyi tarafı ise eser üreticilerine (author) ödemelerin %95'ini alma garantisi veriyor. Yani Audiojungle'ın % 50 ile 70 arası verdiğini düşünürsek alkışlanması gereken bir girişim.

Copytrack: İçerik haklarını korumak için 140 ülkede hukuksal koruma garantisi veriyorlar ve mali risk (vergilendirme vs.) içermediğini belirtiyorlar. Sadece satış anında komisyon alıyorlar ve anında işleme geçiyorlar. (Smart Contract bunu otomatik olarak gerçekleştirdiği için firmaya bağlılığınız olmuyor.) Hâlihazırda borsada işlem de görüyorlar ve roadmap (yol haritası) şaşmaz ise bu yılın ikinci çeyreğinde küresel anlamda kullanıcı kayıtlarına başlayacaklar.

Binded: Eski adı Blockai olan Binded, daha çok makale ve diğer yazı türleri için geliştirilmiş bir sistem. Yazar makalesini yükler yüklemez timestamp (oluşturulduğu zamana ait damga) ile Blockchain üzerinde kayıt oluşturur ve o andan itibaren takip etmeye başlar. Herhangi bir kopya yayımlama/çalma söz konusu olduğunda eser sahibine bildirir.

Bu saydığım üç isim dışında bu tema üzerine koşturan diğer projeleri yazıyı çok uzatmamak adına isim olarak paylaşıyorum:

- Mediachain Lab:
- Ascribe:
- Ujo Music

Tüm bu projelerin global anlamda kullanıcı ya da içerik oluşturucuya faydası nedir?
Envato ve Istockphoto gibi oluşumlar üzerinde eser satan üreticiler iyi bilir ki Türkiye'de ödeme yöntemi olarak PayPal faaliyetlerine son verdiğinde iş işkenceye dönmeye başladı.

Ödeme yapmak isteyen kullanıcı için de satıcı için de aynı işkence söz konusu. Tüm üreticiler diğer ödeme yöntemleri ya da banka aracılıklarıyla boğuşmaya başladılar. Aracılara verilen paralar, resmi işlem zorlukları ve yığınla mevzuat... Kur farklarıyla buharlaşan miktarları da unutmamak lazım.

Tüm bu saydığım projelere göz attığımda eseri direkt olarak koruma altına almak adına aslında çok iddialı yöntemler görmedim. Hukuki koruma ve üretim zamanının saklanması gibi durumları bugün videohive (envato) de yapabilir. Burada firmaya ne kadar güvenilmeli sorusu tartışılabilir. Tekele mahkum olmamak ise konu, eserlerin Blockchain üzerinde saklanmadığını da söylemek mümkün. Yani kısmen yine merkezi bir fileserver ve database üzerindesiniz. Tabii ben gözden bir şey kaçırmadıysam. Bana ümit veren tarafı yukarıda bahsi geçen ödeme yöntemleri ile çektiğim zorlukların son bulacak olması ve Binded gibi bir projenin yazılan eserin kopyasını takip etmesi. Genel olarak ise tüm ciddi Blockchain projelerinden dolayı ümitliyim. Hatta Ethereum Smart Contract konusu için Solidity öğrenmeye başladım. Parlak fikrimi faaliyete geçirmek için. Yani Coin üretip insanları kandırmak için değil.

Chris Stephenson - cs@chrisstephenson.com

Meltdown

Bilgisayarın Yapısı ve Tarihi

Bilgisayar Bilimleri açısından Meltdown sıradan bir güvenlik sorunundan çok daha ilginç bir konu.

Bilgisayar tarihine ve çağdaş bilgisayar mimarisine de ışık tutuyor.

Önbelleğin gelişmesinden başlayalım.

Bilgisayarların Hızı

Hikayemiz aşırı hız merakının yol açtığı bir kazanın hikayesi olduğu için, önce bilgisayarları hızlandırmak için bugüne kadar yapılan işleri mercek altına almak lazım.

Bilgisayarların hızını sınırlayan faktörlerden biri ışığın hızı. Işığın hızını 300 bin kilometre/saniye olarak biliyoruz. Yani 3 x 10^8 metre/saniye. Yani 0,3 metre/nanosaniye. Eskiden "1 foot / saniye" derdik. "Foot" hâlâ ABD'de kullanılan ve yaklaşık 30 cm'e denk düşen Ortaçağ'dan kalma bir uzunluk ölçüsü. 30 cm / nanosaniye ciddi bir hız sınırı oluşturuyor.

Çağdaş bir bilgisayarın devir frekansı 1 GHz ise, bu 1 devir/nanosaniye anlamına geliyor. Ya da 2.5 GHz ise, 4 devir/nanosaniye'ye denk düşüyor. Bu hızda 1 işlemci devrinde ışık sadece 7,5 cm gidebilir. Ve tabii ki, ışık hızı bilgisayar içindeki sinyaller için sadece bir üst sınırdır. Bilgisayar içindeki elektrik sinyalleri bundan daha yavaş hareket etmektedir. Devrelerin kapasitansı hem sinyallerin yayılmasını yavaşlatmakta, hem de sinyalleri, yüksek frekanslarını azaltarak, çürütmektedir. Her iki durum açısından mesafeler hız için önemli bir engel teşkil ediyor.

İşlemcinin küçülmesi sadece bilgisayarın daha küçük olmasını sağlamıyor, ayrıca hem mesafe hem de devrelerin kapasitansını azaltarak, bilgisayarın hızını artırıyor.

Önbellek (Cache)

Bir zamanlar bilgisayarlarda ön bellek yoktu. Örneğin 1965 yılında üretime giren, ilk aşkım olan IBM 1130 bilgisayarının hiçbir yerinde önbellek kullanılmıyordu. Aynı şekilde 1981 yılında üretime giren IBM PC'nin ilk modellerinde de önbellek yoktu.

Maksimum 32 kbyte hafıza (RAM olarak düşünmeyin, mıknatıslı core hafıza), işlemcinin ve hafızanın temel devir periyodu 3,6 mikrosaniye idi.

Bu bilgisayar işlemcisi yüzlerce entegre devreden yapılıp boyutları 45 x 60 x 10 cm civarında idi. Herhangi bir işlem için yüzlerce sinyalin bu işlemcinin bir tarafından öbür tarafına geçmesi gerekmekte fakat tek bir geçiş 2 nanosaniyeden fazla olamamakta idi.

Yani işlemcinin fiziksel boyutu 300 kHz frekansının sebeplerinden biriydi.

Daha da önemlisi, işlemci ve ana-hafıza aşağı yukarı aynı hızda çalışıyordu. İkisinin de 3,6 mikrosaniye deviri vardı. Bazen işlemci hafızadan daha yavaş çalışıyordu. Shift, çarpma gibi "zor" komutlar 40 mikrosaniye kadar uzayabiliyordu, hele hele en zor olan bölme komutunun zamanı 100 mikrosaniye üstünde çıkabiliyordu.

Bundan saydıklarımızdan ötürü, bilgisayarın hızı hafızadan gelen bilgilerin hızına bağlı değildi. Bilgisayarın en yavaş elemanı işlemciydi. Onun hızı belirleyiciydi.

Aynı durum orijinal IBM PC için de geçerliydi. 1981'e kadar işlemci bir çip kadar küçülüp hızlanmıştı, hafıza artık DRAM idi ve o da hızlı çalışıyordu. Bilgisayarın ana frekansı 4,77 MHz, yani 1 devir yaklaşık 0,2 mikrosaniye ya da bundan sonra kullanacağımız ünite 200 nanosaniye.

İlk işlemci Intel 8088 idi. Bu modelde de hafıza, işlemci ve RAM'dan daha hızlıydı. RAM'ın hızı 200 nanosaniye idi. Yani ortalama bir işlem için işlemci 1-2 mikrosaniye (yani 1000-2000 nanosaniye). Her işlem için ortalama 4-5 byte gerekli olup veri yolu 8 bitlik olunca, yine de işlemcinin hafızadan biraz daha yavaş gittiğini görebiliriz.

Ancak bilgisayarın bundan sonraki gelişmesi bu rakamları altüst edecekti. Çipteki devreler küçüldüğü için işlemciler hızlandı. Sinyal yollarının kısaltılması, kapasitansların azaltılması ve devrelerin çoğaltılması mümkün olunca işlerin eş zamanlı yapılabilmesinde işlemcilerin hızı tabir-i caizse bir füze gibi yükseliyordu.

Tabii ki aynı elektronik malzemelerden yapılan RAM çipler de hızlanıyordu. Ancak RAM'ın hızı kadar RAM çiplerinin kapasitesi de artıyordu. DRAM'dan daha hızlı teknikleri vardı ancak bu yöntemlerle yapılan çiplerin hızı fazla olunca, kapasiteleri ve dolayısıyla byte başına fiyatları daha yüksektiler.

Bugünkü PC durumuna bakınca dramatik bir fark görüyoruz. Çağdaş bir bilgisayarda (çağdaş bir cep telefonunda bile) 2,5 GHz hızı olan 4 adet işlemci var. İşlemler ortalama 1 devir tutuyorlar. İşlemcilerin işlevi çok karışık olduğu için bu rakamlar aşağı yukarı tahmini rakamlar. Yani toplam olarak her 1 nanosaniyede 10 işlem yapılır, ve her işlem için 0,1 nanosaniye gerekmektedir. DDR3 DRAM için latency (yani getir komutunun verilmesinden, verinin elde edilmesine kadar geçen süre) 10 nanosaniye. Bu latency RAM hızı için her şey demek değil. Bir komutla 1 byte değil, epey bir veri getirmek mümkün. Aşağıda bu konuya değineceğiz.

Yine de kaba bir gerçek var. Artık çağdaş PC mimarisinden olan bilgisayarda ana hafızamız işlemcimizden 100(!) kat daha hızlı. RAM işlem için 10 nanosaniye gereksinirken, işlemci 0,1 nanosaniye gereksinmektedir.

Önbellek Prensibi

Mühendislik meşhur tabirle "Bir ahmağın 1 dolara üretebildiğini 10 sente üretmek" ise, bu bahiste de konumuz mühendislik.

Elimizde ucuz, büyük ama görece yavaş hafızalar ve pahalı küçük ama hızlı hafızalar varken yapabileceğimiz şey mühendisliktir.

Henry Ford mühendislerini hurdalıklara gönderiyordu. Atılan arabaların yıpranmamış parçalarını bulup yeni arabalara daha ucuz ve kalitesiz parçalarla yapabilmek amacıyla gidiyorlardı. Yani arabanın kullanımına göre arabayı tasarlıyorlardı.

Bilgisayarlar program değerlendirmek ve verileri işlemek için kullanılıyorlar. Program ve veri yapısı rastlantısal değil. Programlar aşağı yukarı lineer yani doğrusal yapılar. Genellikle veri yapılarımız için de aynı şey geçerli. Bir hafıza (herhangi bir hafıza) böyle kullanılıyorsa, önbellek prensibini kullanabiliriz.

Önbellek prensibi şu iki maddeden ibaret:

(a) Bir veriye ulaştıysak, bir süre sonra aynı veriye tekrar ulaşmak istememiz yüksek bir ihtimal.

(b) Yine bir veriye ulaştıysak bu verinin komşularına, ulaşmak istememiz yüksek bir olasılık.

Mühendis olarak bu prensibi böyle kullanabiliriz. Hem pahalı hızlı ve küçük bellek, hem ucuz büyük yavaş bellek kullanırız. Yavaş bellekten bir veriye ulaşıldığında o veri ve komşuları hızlı belleğe kaydediliyor. Ondan sonra o veri ya da komşuları tekrar istendiğinde bu verilere hızlı bellekten erişebiliriz.

Önbellek prensibindeki "yüksek olasılık" yeterince yüksekse bu karmaşık yapıyı kullanarak hızlı belleğin hızına yaklaşabiliriz. Ve kritik nokta bu. "hit rate" yani istediğimiz veriyi önbellekte bulmak olasılığı yüksek olacak. Bunun hesaplayabiliriz:

Hızlı belleğe erişim, H vakit alıyorsa, yavaş belleğe erişim Y vakit alıyorsa, ve "hit rate"in yüzdesi r oluyorsa, ortalama erişim vaktimiz $\frac{(Hr + Y(100-r))}{100}$ olacak.

Diyelim ki önbellek arka bellekten 100 kat daha hızlıysa, ve "hit rate" %99 ise, ortalama olarak hafızaya erişim hızımız hızlı belleğin yarısı, yavaş belleğin 50 katı olur. Ama dikkat edelim. "hit rate" sadece %95 ise, ortalama hızımız hızlı belleğin sadece %16'sı olur, yani yavaş belleğinin 6 katı olur. Eğer bu yöntem işe yarayacaksa "hit rate" gerçekten yüksek tutmak lazım. Bu hesaba katılmayan şey hafızanın pahalılığı. Hızlı bellek ucuzsa hafızanın tümünü hızlı maldan yaparak çözeriz.

Çağdaş PC'de işlemci RAM arasındaki hız uyumsuzluğunu çözmek için en az üç katmanlı (L1, L2, L3) bir önbellek kullanılıyor. İlk katmanlarda veri/komut önbellekleri olarak ayrı olabiliyor.

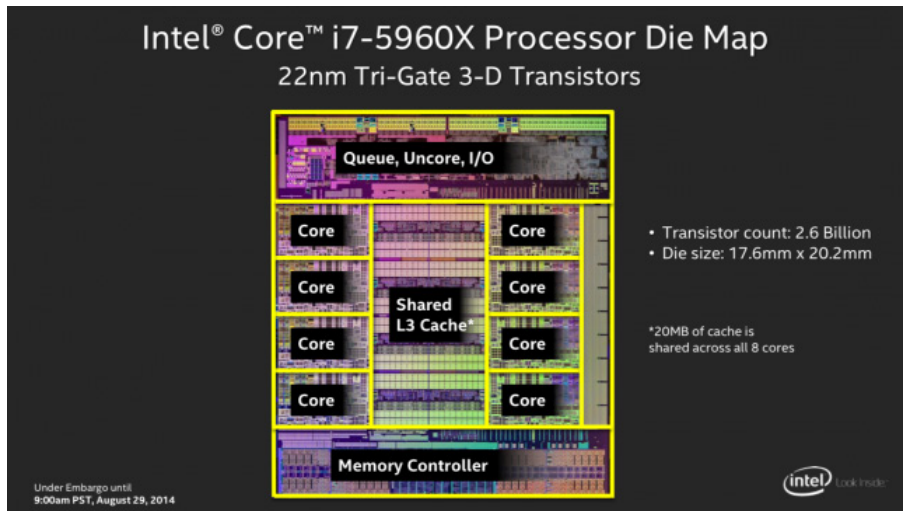
Bilgisayar çiplerindeki çoklu işlemciler için her işlemcinin ayrı önbelleği olabilir. Genellikle en son katman (bu da genellikle L3 olur) bütün işlemcilerde ortaktır. Bu nokta Meltdown hikayemiz için önemli olacak.

Önbellek prensibi sadece işlemci RAM arasında değil, bilgisayarın neredeyse her yerinde kullanılıyor. Küçükten büyüğe sayarsak. İşlemci pipeline (komut değerlendirme borusu) önbellek prensibi kullanılır. Çoğu işlemci ayrıca gelen komutları işlemcinin iç mikro komutlarına çeviriyor, Bunun için "Just In Time" değerlendirme yaparak tekrar önbellek prensibi kullanılıyor. İşlemcinin sanal hafıza ünitesi, "Translation Lookaside Buffer", ismine rağmen, sadece bir sayfa tablosuna yönelik önbellek.

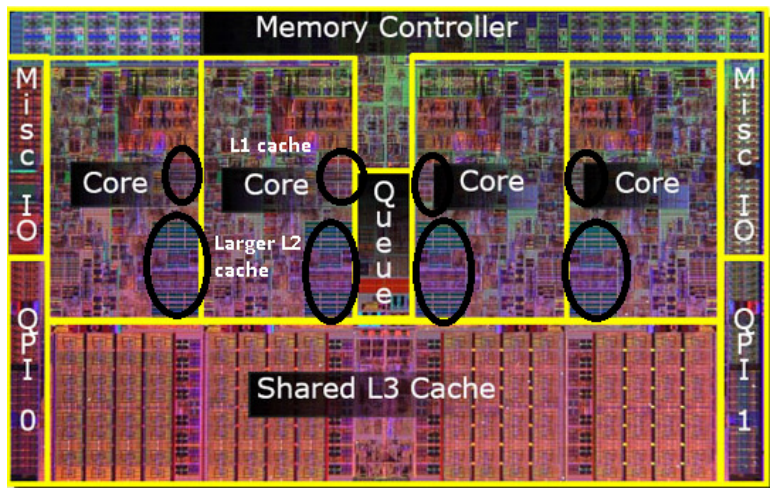
Bu önbellek olmadan, sanal hafıza, hafızanın process arasında korunması ve dolayısıyla çağdaş işletim sistemleri imkânsız olurdu. Java, C# gibi sanal makineyle çalışan yüksek düzey dillerin sanal makineleri hep, önbellek prensibini kullanarak, "Just In Time" yöntemiyle sanal makine komutlarını işlemci komutlarına çeviriyorlar. Hard disk erişimimizde, tekrar en az iki katman önbellek var. Disk yavaş ama bilgisayara göre çok daha yavaş. Disk donanımında önbellek var, ayrıca işletim sistemi RAM kullanarak, disk için başka bir önbellek oluşturuyor. Chrome, Firefox gibi tarayıcılar eriştiğimiz (ve erişeceğimizi tahmin ettikleri) web sayfalarını başka bir önbellekte tutuyor. İnternete çıktığımızda, proxyler de istemci ve sunucu arasında önbellek oluşturuyorlar.

Sunucuların kendileri oluşturdukları sayfaları tekrar tekrar oluşturmamak için önbellek kullanıyorlar. Bulut veri depolamada hızlı bir veri erişimi sağlamak için önbellek prensibi kullanarak hızlı ve yavaş depolama yöntemleri beraber kullanılıyor. En sonunda internetteki adresleri bulabilmek için kullandığımız Domain Name System (DNS); koca, bütün dünyayı kapsayan bir önbellekten ibaret.

Son kuşak Intel (ya da AMD) çiplerinin fotoğraflarına bakarsak, bilgisayardaki önbelleğin önemini kavrayabiliriz. Çipin yarısı önbellekten ibaret. Bir örnek Haswell çip fotosu, coreler arasında ortadaki kocaman ortak kullanılan L3 önbelleği gösteriyor:



Bir önceki kuşaktaki Nehalem çipinin bu fotoğrafı ayrıca core'lara ait L1 ve L2 önbelleklerini de gösteriyor.



Çip yüzeyinin neredeyse yarısı önbellek.

Bu tablodan Intel Haswell çipin L1/L2/L3 önbelleklerinin ve DRAM'ın hızları anlaşılabilir.

Intel Haswell

Intel i7-4770 (Haswell), 3.4 GHz (Turbo Boost off), 22 nm. RAM: 32 GB (PC3-12800 cl11 cr2).

- L1 Data cache = 32 KB, 64 B/line, 8-WAY.
- L1 Instruction cache = 32 KB, 64 B/line, 8-WAY.
- L2 cache = 256 KB, 64 B/line, 8-WAY
- L3 cache = 8 MB, 64 B/line

- L1 Data Cache Latency = 4 cycles for simple access via pointer
- L1 Data Cache Latency = 5 cycles for access with complex address calculation (size_t n, *p; n = p[n]).

- L2 Cache Latency = 12 cycles

- L3 Cache Latency = 36 cycles (3.4 GHz i7-4770)
- L3 Cache Latency = 43 cycles (1.6 GHz E5-2603 v3)
- L3 Cache Latency = 58 cycles (core9) - 66 cycles (core5) (3.6 GHz E5-2699 v3 - 18 cores)

- RAM Latency = 36 cycles + 57 ns (3.4 GHz i7-4770)
- RAM Latency = 62 cycles + 100 ns (3.6 GHz E5-2699 v3 dual)

Önbellekleri olmadan bugünkü normal saydığımız bilgisayar kullanımımız imkânsız olurdu. Elimizdeki bilgisayar ya da istemci beklediğimizden bin kat daha yavaş çalışırdı.

Önbellek Sorunları

Bütün bu önbellek uygulamalarının ortak yanları ve ortak sorunları var.

(a) Önbellekten çıkartma sorunu. Verilerin önbelleğe nasıl girdiklerini gördük. Ancak önbellek, doğası gereği arka bellekten küçüktür. Bazen verileri önbellekten çıkartmak zorunda olacağız.

Bunun stratejisini dikkatle oluşturmak zorundayız. Yoksa "hit rate" ve dolayısıyla önbelleğin verimliliği düşer. Yine de mühendislik yapılmak zorunda. Mükemmel bir çözüm yok. Ortalama en ekonomik, işe yarayacak olan çözümü bulmak lazım.

(b) Şeffaflık sorunu. Amacımız bilgisayarı hızlandırmak. Hesapların sonuçlarını değiştirmek değil. Yanlış fakat hızlı hesap yapmak iyi bir sonuç sayılmaz. Dolayısıyla önbelleğin çalışmasında **şeffaflık** istiyoruz. Daha hızlı çalışmalı, ancak bunun dışında başka bir değişiklik olmamalı. DNS bu sorunun örneklerinden biri. Bazen saatler boyunca bazen günler boyunca eski bir adres verebilir. Veri işlemci tarafından değiştirilince başka bir sorun oluyor. Bu veriyi arka belleğe geri yazmak gerekir. Yoksa önbellek ve arka bellek arasında tutarsızlık oluşacak. Bu da büyük bir sorun. Çok şükür ki okuma işlemleri yazma işlemlerinden daha fazladır.

Side Channel

Yan kanal (side channel) dediğimiz olay gayri resmi bir iletişim kanalıdır. Hükümetler arasında örneğin, resmi diplomatik kanallardan değil inkar edilebilir başka insanlar aracıyla hassas ön görüşmeler yapılabilir ve yapılmaktadır. Bilgisayarlarımızın başındaki en büyük dert "resmi kanal" olan internet bağlantımız. Ancak internete bağlı olmayan bir bilgisayardan bilgi sızdırmak mümkün. Örneğin bilgisayar internete bağlı değil ama mecburen elektriğe bağlıdır. Güç kablosundan yaptığı hesaplardan sinyal okunabilir. Ya da bilgisayardan sızan ısı, dolayısıyla vantilatörünün çıkarttığı ses düzeyi, yaptığı hesabın zorluğuyla değişebilir. Bu verilerden güvenlik tehdidi oluşturacak bir veri çıkartmak zor görünebilir. Ancak bilgisayar (ve dolayısıyla bir saldırıda kullanılacak bir bilgisayar) yorulmaz. Bir işlem dizisinden sadece bir bit, bir evet/hayır cevap öğrenilebilirse, bir milyon işlemden bir milyon bit öğrenilebilir. O milyon bit arasında hedef bilgisayarın kök şifresi varsa, bütün bilgisayarın kapıları açılmış oluyor.

Bilgisayar internete bağlıysa yan kanal olasılıkları çoğalıyor. Zaman bazlı bigli edinme yöntemleri kullanmak mümkün oluyor. Hedef bilgisayarın hangi zaman dilimi içinde cevap verdiği bilgisinden hareketle bir sonuç çıkartmak mümkün olabilir. Yine de bir denemeden (ya da bin denemeden) bir bitlik bilgi öğrenilebilirse bu yeter. Bit bit biriktirilir. Sisteme girilir.

Pratik bir örnek verelim. RSA kriptografide şifreleme ve deşifreleme mesajın büyük bir üs ile çarparak yapılıyor. Bu üstü değeri 10^{500} gibi olabilir. Yani $(\text{mesaj})^{(10^{500})}$ hesabı yapılıyor.

İlk düşünülen yöntemle bu hesap, tabii ki, yapılamaz. 10^{500} defa bir rakam kendisiyle çarpmak evrenin ömründen çooook daha fazla vakit alır. Böyle yapılır. m^2 hesaplamak için bir çarpma işlemi lazım, m^3 için iki çarpma, ancak m^4 hesaplamak için sadece iki çarpma lazım. Önce m^2 hesaplıyoruz, sonra onun karesini alıyoruz. Bu kare alma yöntemiyle mesajların üstlerini çoook daha hızlı hesaplayabiliriz.

Ufak bir program:

```
#lang racket
; fast-exp num num num -> num
; takes a modulo, base and exponent to calculate a fast modularised exponent modulo p
(define (fast-exp p x n)
  (let*
    ((* (lambda (x y) (modulo (* x y) p)))
    (kare (lambda (x) (* x x))))
    (cond
      ((= n 0) 1)
      ((even? n) (kare (fast-exp p x (/ n 2))))
      (else (* x (fast-exp p x (- n 1)))))))
```

Bu gerçek Racket program gerçek iş yapar. Olduğu gibi çalışır.

Racket (henüz) öğrenmemiş okuyucular için bunun (çalışamayan) C syntax versiyonunu yazalım:

```
#include <stdio.h>
#include <stdlib.h>

int sq (int p, int x) {
      return (x * x) % p ;}

int fastExp(int p, int x, int n) {
      if (n == 1) {
            return 1;
      } else if (n % 2 == 0)  {
            return sq(p, fastExp (p, x , n / 2));
      } else {
            return (x * fastExp (p, x, n - 1)) % p;
      }
}

int main(int argc, char** argv) {

      if (argc < 4){
            return 0;
      } else {
            printf ("\nResult = %d\n\n", fastExp(atoi(argv[1]),atoi(argv[2]),atoi(argv[3])));
            fflush(stdout);
            return 1;
      }
}
```

Bu C kodun dezavantajı, C int limitleri yüzünden gerçekçi sayılarla çalışamaması, çalışsaydı, stack overflow yüzünden çökerdi.

Bu iki program örneğine bakarken ortaya olasılıklı bir yan kanal çıkıyor. Kare alma hızlı üstü hesaplama algoritmasının özelliklerinden birini kullanabiliriz. m^e *modulo p* hesaplıyoruz, m, e ve p büyük sayılar. RSA kullanıyorsak bu aynı zamanda şifreleme için kullandığımız gizli değer. "Büyük rakam" dediğimizde *~500* hanelik, yani 10^{500} cıvarında, bir sayı.

Diyelim ki bir n var ki $e = 2^n$. O zaman algoritmamız çarpım yaparak m^e hesaplar. Diyelim ki $e = 2^{n-1}$. O zaman algoritmamız $(2n - 2)$ çarpım yaparak m^e hesaplar. Yani algoritmanın kullandığı zaman e değerindeki "1" olan bit sayısına göre değişir. Bir mesaj şifreleme için bu üs işlemi tekrar tekrar yapılır. Sistemi dışarıdan zaman açısından gözleyebilirsek, gizli şifrenin "1" olan bit sayısı tahmin etme şansımız olur. Tabii ki şifrenin bit sayısı bize şifrenin kendisini doğrudan vermiyor. Ancak böyle bir bilgi, şifreyi öğrenme yolunda olan bilgi hırsızı için önemli bir kazanç olabilir.

Bu side channel-yan kanal örneğini hatırda tutarak Meltdown'a doğru ilerleyebiliriz

İlk Zafiyet Tespitleri – Çoook Önceden

Güvenlik uzmanları çok önceden Intel önbellek mimarisindeki sorunları tespit etmişlerdi. Bu konuda iki önemli makale yayımlandı, biri 19911 yılında, ikincisi 199[52]. İkinci makale birincisine atıfta bulunuyor ve sonuç olarak x86 işlemcilerin bazıları "güvenli sistemlerin inşasında istenmeyen niteliklere sahip". Maalesef IEEE üyesi olmama rağmen bu iki makalenin tam metinlerine (henüz) ulaşamadım. Her iki makalenin özetinden anladığım kadarıyla, x86 işlemci mimarisinde zaman ölçme yöntemleriyle yan kanalın oluşturulabileceğine dair tespitler var.

Çağdaş Önbelleklerin Yapısı

Bu yan kanalların oluşturulabilmesini anlayabilmek için işlemci(ler) ve DRAM arasında duran L3 önbelleğin tipik yapısını incelemek gerek.

Tarihsel olarak iki tip DRAM önbelleği mimarisi vardı: "Associative" ve "Direct Mapped".

Önbellekte saklanacak veriler iki parçadan oluşuyor. Biri verinin kendisi, diğeri arka belleğinin hangi kısmına ait olduğunu dair bir adres.

"Komşu veri" önbellek prensibinden yararlanabilmek için önbelleklerde saklanan verilerin tek hafıza hücreleri değil, yan yana duran arka bellekten gelen bir hafıza satırı olarak saklanması gerekiyor. Tipik bir satır 64 byte'lıktır. Intel Haswell işlemciler bütün önbellek satır uzunlukları 64 byte. Dolayısıyla bu satırların ilk hücrelerin son 6 adres bitinin hepsi sıfır olur. Ve bu yüzden adresin bu kısmını saklanmasına gerek yok. Diğer adres bitleri bir "tag" ya da etiket olarak önbellekte saklanıyor.

Dolayısıyla işlemciden gelen hafıza adresi böyle kullanılıyor. Sağdaki 6 bit satır içindeki adres olacak, üstündeki adres bitleri önbellekte olup olmadığını tespit etmek ve, varsa, hangi satırda olduğunu tespit etmek için kullanılıyor.

Önbellekte istenen verinin tutulduğu yeri bulmak için farklı yöntemeler kullanılabilir. Bunlardan biri "associative". Aynı anda istenen adresin üst bitleri önbellekteki bütün taglarla karşılaştırılıyor. Bu silikon açısından pahalı bir yöntem ve artık çok fazla kullanılmıyor.

Çok daha kolay bir önbellek sistemine erişim yöntemi "Direct Mapped"dır.

Bu yöntemle önbellek satırları numaralandırılıyor ve doğrudan arka belleğin adreslerinin alt bitleriyle birbirine bağlanıyor. Tipik L3 önbellekleri böyle çalışıyor. Örneğin Intel Haswell[3] L3 önbelleği 8 Mbyte ve 64 bytelik satırlardan oluşuyor. Yani 128k satırı var. Gelen arka bellek adresi 36 bitlik bir adres ise, en alt 6 bit satır içi adres oluyor, bunların üstündeki 17 bit satır numarası oluyor, en üst 13 bit tag oluyor. Önbelleğe olan erişim hızlı çalışan, basit ve sade devrelerle yapılabilir.

İşlemciye daha yakın L2 ve L1 önbellekler için daha karmaşık, direct mapped ve associative yöntemlerini birleştiren bir yapıya sahip. Yine Intel Haswell işlemcilerde L2, L1 önbellekleri direct mapped artı 8 way associative.

Ancak hikayemiz için L3 önbellek ile ilgileniyoruz. Bu sadece, saf, direct mapped oluyor, ve yapacağımız işler bu olaya bağlı.

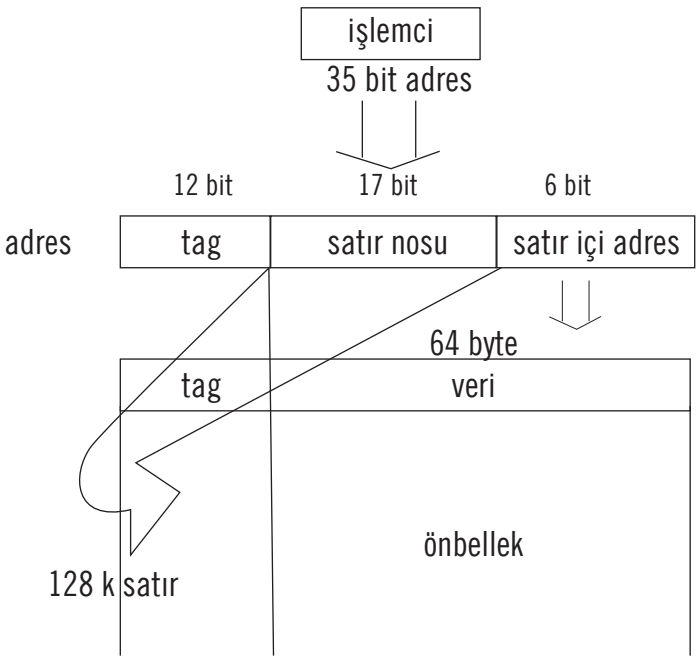
Buradan çıkan önemli sonuç şu: işlemcinin bir komutla hangi önbellek satırına ulaşmış olduğunu öğrenebilirsek o adresin ortadaki 17 bitini bilebiliriz. İspiyonculuk burada başlar! Ancak bunun önbelleğe erişimini öğrenmemiz lazım.

1 J. C. Wray, "An Analysis of Covert Timing Channels," Proceedings. 1991 IEEE Computer Society Symposium on Research in Security and Privacy(SP), Oakland, CA, 1991, pp. 2.

2 O. Sibert, R. Lindell and P. Porras, "The Intel 80x86 Processor Architecture: Pitfalls for Secure Systems," Proceedings 1995 IEEE Symposium on Security and Privacy(SP), Oakland, CA, 1995, pp. 0211.

3 Bu veriler buradan alındı: https://www.7-cpu.com/cpu/Haswell.html

Önbellek örneği: Intel Haswell L3 önbelleğin çalışması:



"Flush and Reload"un Kullanılması

2013 yılında Flush and Reload tekniğiyle yan kanal yaratmak için önbelleğin istismar edilmesini gösteren bir makale[4] yayınlandı.

Ayrıntıları öğrenmek isteyen okuyucu rahatlıkla orijinal makaleyi okuyabilir.

Yöntemin esas çalışma şekli işlemcinin tehlikeli bir komutunu kötüye kullanmak. Clflush komutuyla önbellekteki bir satırın içeriğini iptal etmek mümkün. Ondan sonra saldıran program bu önbellek satırının kapsamındaki bir adresin işlemciye hafızadan yükleme vaktini ölçer. Hızlı gelirse, demek ki aynı önbelleği kullanan başka bir program bu satırı tekrar önbelleğe yüklemiş. Unutmayalım DRAM hızı ve önbellek hızı arasında 100 kat fark var. Yani bu farkı ölçmek zor değil.

Burada yaptığımız iş işlemci çipinin bir thread'de çalıştırılan program üzerinden aynı işlemci çipindeki başka thread'de çalıştırılan başka bir programı takip etmek. Yani "hızlı" ve "yavaş" haritası çıkartarak hedef programının nereden derlendiğini görmek mümkün.

Makalede gösterilen yöntemle okumakta olduğunuz makalede bahsedilen hızlı üstü algoritma takip ediliyor. Hızlı üstü algoritmanın ana döngüsü Flush+Reload tekniğiyle takip edildiğinde hangi dönüşte sadece kare alındığını hangi dönüşte kare ve tek çarpımın yapıldığını tespit ediliyor. Böylece alınan üstü bit bit ortaya çıkıyor. Makalede takip edilen hedef programı GPG şifreleme programı olunca, bit bit ortaya çıkan üstü, şifrelemede kullanılan gizli anahtar.

Bu makale yayınlanınca, bu saldırıyı önlemek amacıyla, GPG programın yazarları programın şifreleme ana döngüsünün yapısı değiştirdiler. Ancak Flush ve Reload tekniğinin gücü gösterilmişti ve başka kullanımlarının ortaya çıkması sadece zaman meselesiydi.

Meltdown

Ve nihayet Meltdown[5]. Meltdown için Flush and Reload tekniğiyle işlemcideki iki önbellek yapılarını daha yoğun kullanarak çok daha güçlü bir saldırı oluştu.

Bu iki önbelleğin biri page table, diğeri işlemcinin komut değerlendirme boru hattı.

Hedefimiz bütün bilgisayarın fiziksel arka belleğin içeriklerini okumak. Şu ana kadar öğrendiklerimizin hepsini kullanacağız.

İşlemciyi böyle bir şeye zorlamak istiyoruz: dolaylı bir komutla fiziksel hafızanın bir hücresi adres olarak kullanmak. Dolaylı bir komut bir hafıza hücrenin içeriğini adres olarak kullanır. Böyle bir şey yaptırabilirsek, Flush & Reload tekniğiyle hangi adrese ulaştıysa o adresin önbellek satır numarasını, yani ortadaki 17 bitini öğreniriz.

Ancak bir sorunumuz var. O adreslerin programımız tarafından erişilmesi yasak. Kontrolümüzde olan bir program oradan okuyamaz. Okumaya çalıştığında işlemci "exception" ilan edip alarm zillerini çalar.

Meltdown bu engelleri aşmak için işlemcinin başka niteliklerini kullanır.

İşlemci programın nereye gideceğini tahmin ederek henüz ulaşılmamış komutları boru hattına alıp değerlendirilir. Program o yöne gitmezse ya da o komut "exception" yaratırsa, değerlendirilmiş olan komutların etkisi iptal edilir. Bir etkisi hariç: önbellekteki etkisi kalır.

Meltdown'un kurnaz planı bu: yasak hafıza bölgelerine erişen komutlar boru hattına girip değerlendiriliyor. "Biraz" sonra komutların yasak olduğu fark edilecek ve komutlar iptal edilecek. Ancak önbelleğe olan oldu. Ve bunun etkisi ölçülebilir.

İşletim sistemlerinde, hız kazanmak için işletim sistemin erişebildiği hafıza (yani arka belleğin hepsi) her programın sanal hafızada görünüyor. Ancak programların bu sanal hafıza sayfalarına ulaşması yasaklanıyor. Ama gördüğümüz gibi bu yasak ancak önbellekteki satırları etkilendikten sonra uygulanıyor.

4 Yuval Yarom, Katrina Falkner "FLUSH+RELOAD: a High Resolution, Low Noise, L3 Cache Side-Channel Attack" https://eprint.iacr.org/2013/448.pdf

5 Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, Mike Hamburg "Meltdown" https://arxiv.org/abs/1801.01207

Nihai hilemiz bizi yavaşlatan "exception"u önlemek. İşlemci tahmin programın gidişatına göre komutlarını boru hattına alıyor. İşlemcinin tahmini yanıltabilirsek hiç değerlendirilmeyecek bir komut boru hattına sokabiliriz. Yani yasak bölgeye erişip önbellekte iz bırakan komut öncesi bir koşulu dallandırma (conditional branch) komutu koyacağız. İşlemci programın bu dalına gidilmeyeceğini tahmin ettiği için dallandırma komutundan sonraki yasak komutu boru hattına koyup ön değerlendirilmesi yapar. Bu arada önbelleğe olan olur. Bu mevzu bahis dala gelince o komuta ulaşılamaz, "exception" bile fırlatılmaz.

Son bir şey kaldı. Verinin sadece 17 bitini öğrenebildik. Geri kalanı nasıl öğreneceğiz? Dolaylı komutumuzu oluşmadan o veriyi biraz sağa sola sallandırırsak diğer bitlerini rahatlıkla öğrenebiliriz.

Bu yöntemlerle Meltdown makalesi yazan araştırmacılar bilgisayar arka belleğini saniyede yarım Mbyte hızıyla okuyabildiler. Bir okuyucu bana "Bu zafiyet dolayısıyla sadece bellekteki verileri okuyor, değil mi, yani zararı olmaz?" sorusunu sordu. O "sadece" okunan bilgiler arasında SSL için kullanılan gizli anahtarlar da olabilir. Şayet durum buysa, ön kapınız da açık, arka kapınız da!

Sonuç

25 yıldan daha fazla bir süredir yayımlanan uyarıları görmezlikten gelen işlemci üreticileri büyük bir sorumsuzluk yaptılar. Meltdown şimdilik önlenmiş görünüyor. Meltdown'u önleme yöntemleri başka bir yazımızın konusu olsun. Keza Spectre[6]'yi, onu da daha sonra tartışırız...

Son olarak tüm okuyuculara referans olarak paylaştığım makalelere de göz atmalarını salık veririm. Bu makaleleri okuyarak sadece Flush and Reload, Meltdown ve Spectre hakkında bilgi elde etmeyeceksiniz. Ayrıca çağdaş işlemcinin yapısı, algoritma, programlama dillerinin nasıl çalıştığına dair bir dizi güncel ve etkileyici bilgiye de ulaşabileceksiniz.

6 Paul Kocher, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, Yuval Yarom "Spectre Attacks: Exploiting Speculative Execution" https://arxiv.org/abs/1801.01203

Murat ŞİŞMAN - info@muratsisman.com

Sinyal İstihbaratı

Sinyal Dinleme ve Analiz Yöntemleri

Kablosuz iletişimin hayatımızın her alanını kapladığı günümüzde, birçok cihaz tarafından yayılan sinyaller etrafımızı çevrelemektedir. Telsizler, cep telefonları, kablosuz modemler, Bluetooth aygıtlar, iletişim uyduları, GPS uyduları ve daha birçok cihaz farklı frekanslarda sürekli olarak sinyal yaymaktadır. Etrafımızı çevreleyen bu sinyalleri gerekli donanım ve yazılımlarla dinlemek, analiz etmek ve hatta şifreli olanları çözmek mümkündür.

Bilgisayarlar yardımıyla sinyallerin dinlenmesi için birçok farklı donanım kullanılabilmektedir. Profesyonel ekipmanlardan mini USB aygıtlara kadar birçok farklı seçeneklerde donanımlar piyasada bulunmaktadır. Realtek RTL2823U chipseti kullanan RTL-SDR donanımı 20 dolarlık fiyatı ile en ucuz ve etkili donanım çözümlerinin başında gelmektedir. Karasal TV yayınlarını bilgisayarlar üzerinden izlenmesi maksadıyla piyasada satılan bu donanım aynı zamanda 24 ile 1766 Mhz arasındaki tüm frekanslarda çalışabilme özelliğine sahiptir. Bu özelliği sayesinde karasal TV yayınlarının yanı sıra FM-AM radyo kanalları, polis, can kurtaran, itfaiye, sahil güvenlik telsizleri, amatör radyo frekansları, GSM sinyalleri ve birçok uydu sinyalini dinleyebilmektedir.

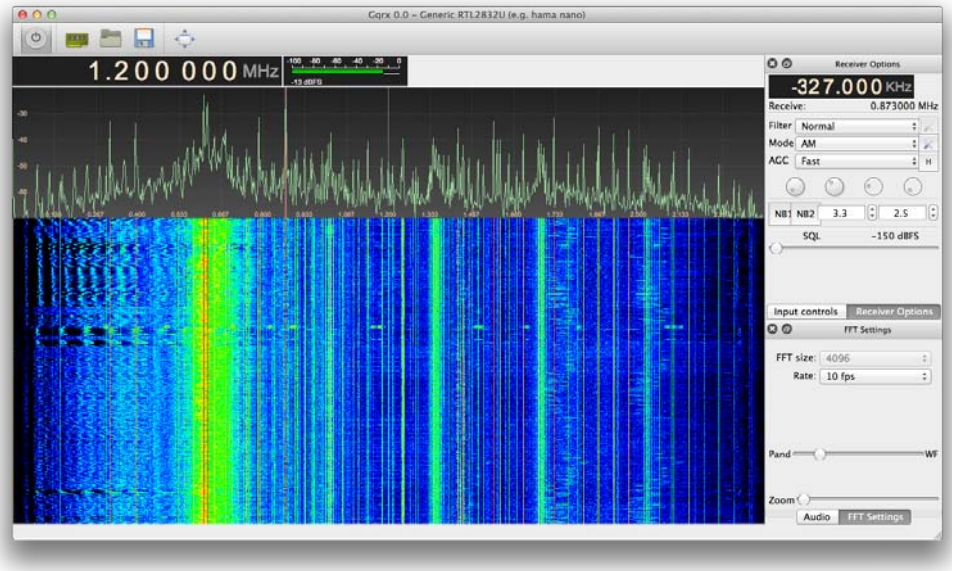
Kuşkusuz bu donanımdan verimli bir şekilde faydalanabilmek için antenin alınacak veriye uygun olması gerekmektedir. RTL-SDR donanımı yalnızca sinyal dinleyebilmektedir, sinyal gönderme işlemi gerçekleştirmemektedir. HackRF ve BladeRF gibi daha pahalı alternatif donanımlar ise hem alma *(Rx)* hem de gönderme *(Tx)* işlemlerini gerçekleştirebilmektedir.

RTL-SDR Donanımı ile yapılabileceklerden bazıları

- Polis, Ambulans, itfaiye telsizleri ve EMS iletişimi dinlenebilir *(Yasal olarak halka açık frekanslar)*
- Hava trafik kontrol konuşmaları dinlenebilir.
- Havada bulunan uçakların konumları, hızları ve yön bilgileri *(ACARS)* dinlenip harita üzerinde görüntülenebilir.
- Deniz trafiği dinlenerek gemi isim bilgisi, yön ve konum bilgileri harita üzerinde işlenebilir.
- Amatör telsizcilerin konuşmaları dinlenebilir.
- Dijital ses iletişimi dinlenebilir ve şifresi çözülebilir. *(DMR dijital telsizler)*
- Kablosuz güvenlik kamerası, bebek monitörü, bluetooth gibi cihazların sinyalleri izlenebilir.
- POCSAG/FLEX Pager sistemleri dinlenip text olarak görüntülenebilir.
- Meteoroloji uydularından uydu görüntüleri ve hava durumu bilgileri alınabilir. *(NOAA Uyduları)*
- Analog karasal TV yayınları izlenebilir.
- FM ve AM radyo kanalları dinlenebilir.
- GSM sinyalleri dinlenip analiz edilebilir.
- RF sinyalleri dinlenip analiz edilebilir.

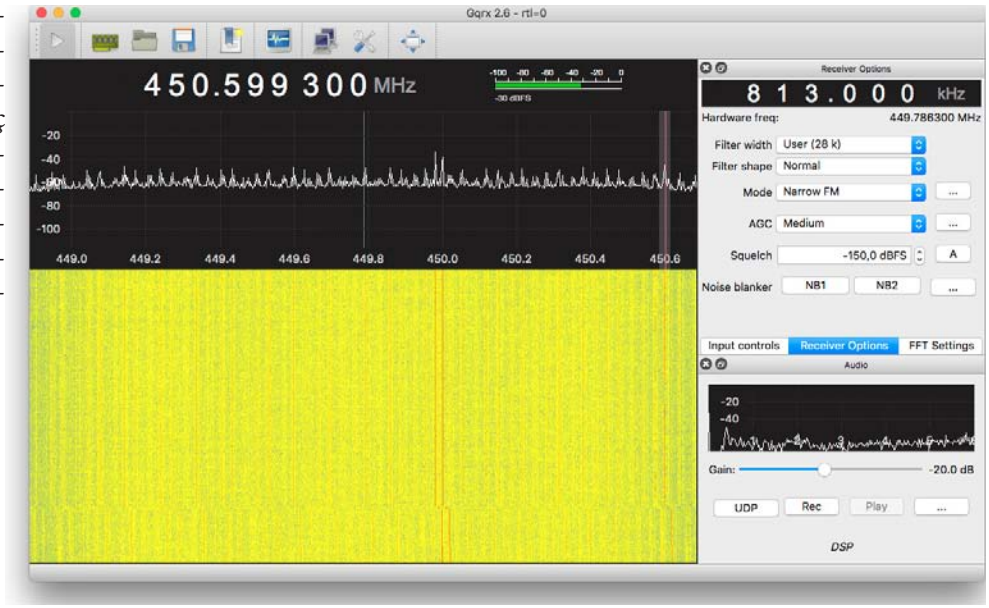
Yazılımlar ile sinyallerin dinlenmesi

RTL-SDR donanımı tüm işletim sistemlerinde çalışabilmektedir. Basit şekilde sinyalleri dinleyebilmek için SDRSharp veya Gqrx yazılımları kullanılabilir. Linux ve MacOS işletim sistemlerinde en yaygın kullanılan Gqrx yazılımıdır. İstenilen frekansın üzerine gelindiğinde eğer bir sesli iletişim var ise dinleme yapılabilir veya Gqrx bir UDP sunucuya dönüştürülüp belirli frekansın dataları UDP portundan diğer uygulamalar ile paylaşılabilir.



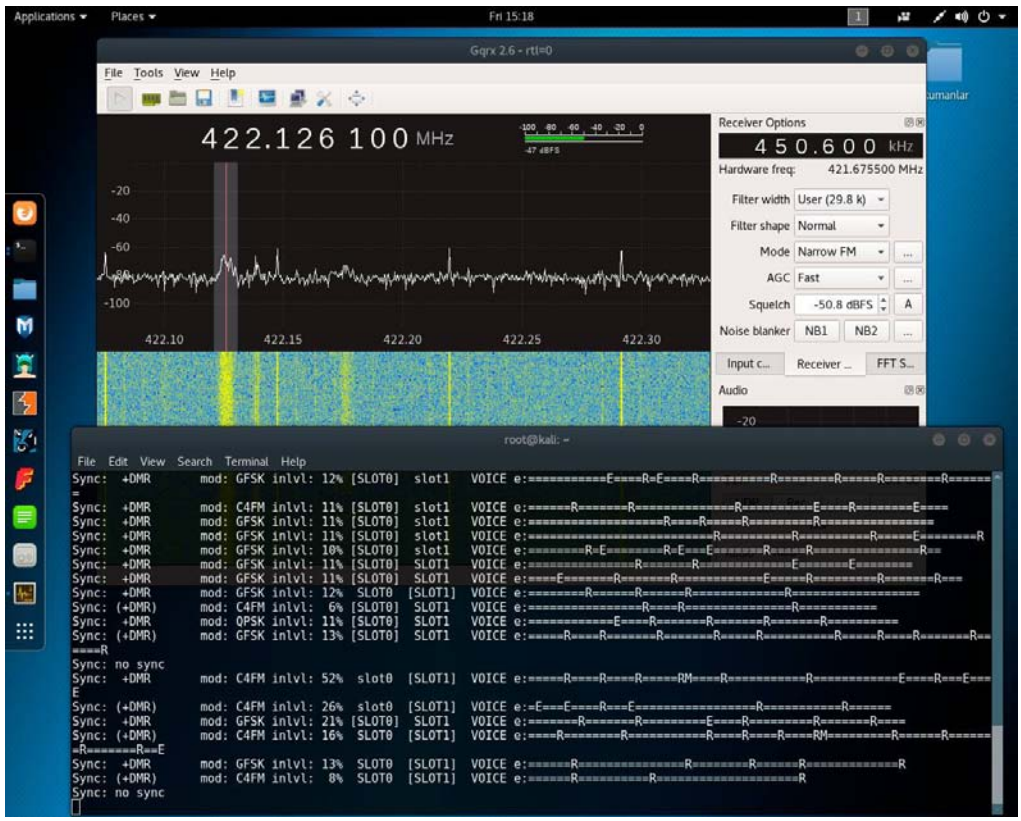
Polis Telsizlerini Dinlemek

Trafik veya asayiş polislerinin kullanmış oldukları bazı telsiz frekansları halka açık şekilde yayın yapmaktadır ve dinlenmesi yasal olarak suç teşkil etmemektedir. Genellikle gazeteciler bu frekansları dinleyerek trafik kazaları veya hırsızlık gibi suçlardan haberdar olup olay yerlerine intikal ederler. Polis telsiz frekansları internet üzerinden bulunabilmektedir.



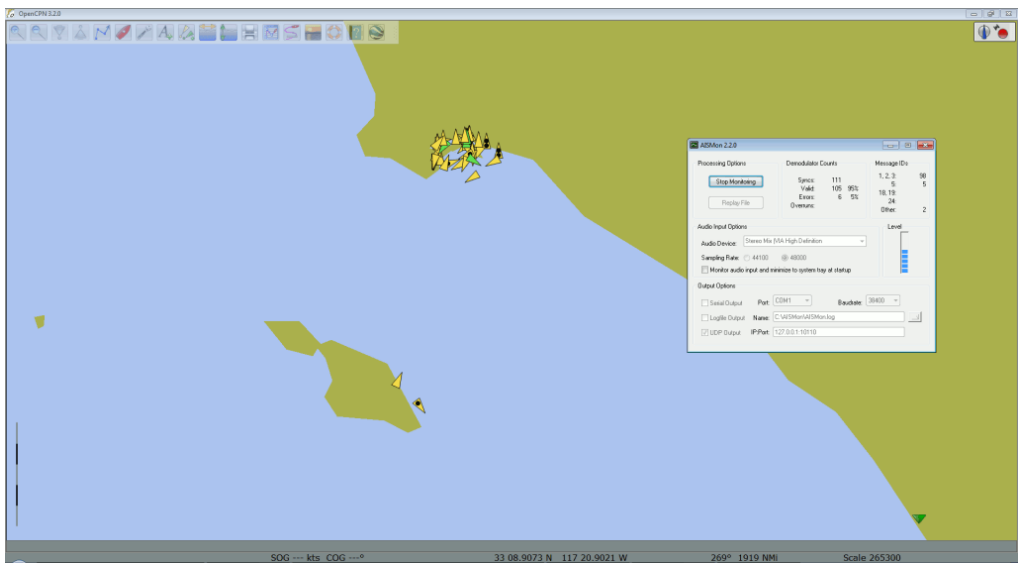
Dijital Telsizlerin Dinlenmesi

Polis, itfaiye, ambulans veya alışveriş merkezlerindeki güvenlik görevlileri dahil artık birçok kurum/kuruluş güvenlik ve başka konular nedeniyle dijital telsizler kullanmaya başlamıştır. Ancak DMR diye tabir edilen bu dijital görüşmeler birtakım yazılımlar ile çözülebilmektedir.



Gemi Trafiğini İzleme ve Analiz Etme

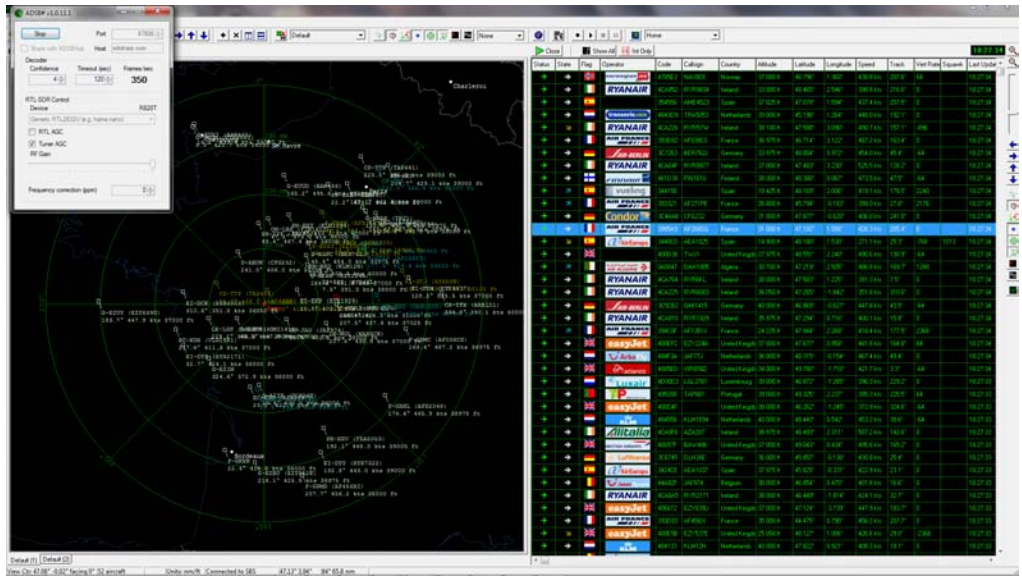
Belirli bir büyüklüğün üzerindeki ve yolcu taşıyan her bir gemi AIS (Automatic Identification System) adlı takip sistemini kullanmaktadır. VHF 161.975Mhz ile 162.025Mhz kanallarından GMSK modülasyonu ile sürekli yayın yapmaktadırlar. Bu sinyal yayınlarında geminin adı, çağrı kodu, koordinatları, rotası, hızı, gemi boyutu, gidilecek liman ve varış zamanı gibi bilgiler gönderilmektedir. Bu sinyalleri dinlemek veya bilgisayarlar yardımı ile analiz etmek suç teşkil etmemektedir ancak gemiler harici bu frekanslarda yayın yapmak yasaktır.



Sinyallerin kolayca manipüle edilebilmesi, yüksek tonajlı bir geminin radarında sahte AIS sinyalleri ile başka bir gemi varmış gibi gösterilebilmesi nedeniyle bu alan zafiyetlerle doludur. AISMON ve OpenCPN yazılımları, alınan sinyaller ile harita üzerinde gemilerin işaretlenmesine yardımcı olmaktadır.

Hava Trafiğini İzleme ve Analiz Etme

Kalkış için hazır olan veya havada aktif olan tüm uçaklar mutlaka kendilerine ait olan bilgileri sinyaller aracılığı ile yerde bulunan istasyonlara iletmek zorundadırlar. Bu bilgiler tıpkı deniz trafiğinde olduğu gibi hız, yükseklik, konum, gidilecek alan ve gidilmekte olan yön gibi birçok veriyi kapsamaktadır ve ADS-B olarak adlandırılır. Bu veriler Transponder denilen aygıt tarafından yayılmaktadır. 1090Mhz frekansı dinlenip analiz edilerek o sırada üzerimizde olan tüm uçaklar görüntülenebilir.



Uydu Sinyallerini Dinleme ve Analiz Etme

Her gün üzerimizden yüzlerce farklı uydu gelip geçmekte ve birçoğu da üzerimizden geçtiği sırada sinyaller aracılığıyla yeryüzüne veri iletmektedir. Meteoroloji alanında kullanılmak üzere tasarlanan NOAA uyduları bu sinyalleri tüm dünyaya açık şekilde yayınlamaktadır. Birçok NOAA uydusu yörüngede farklı konumlarda sürekli olarak dolaşmaktadır ve internet üzerinden anlık olarak hangi konumda oldukları görüntülenebilmektedir. http://www.n2yo.com adresinden hemen hemen tüm uyduların anlık konumları görüntülenebilmektedir.

NOAA uydularından verimli bir şekilde sinyal alabilmek için Turnstile, Quadrifilar Helix, V-Dipole veya Double Cross tipi anten kullanılmalıdır. RTL-SDR donanımı ile birlikte gelen anten bu konuda yetersiz kalmaktadır.

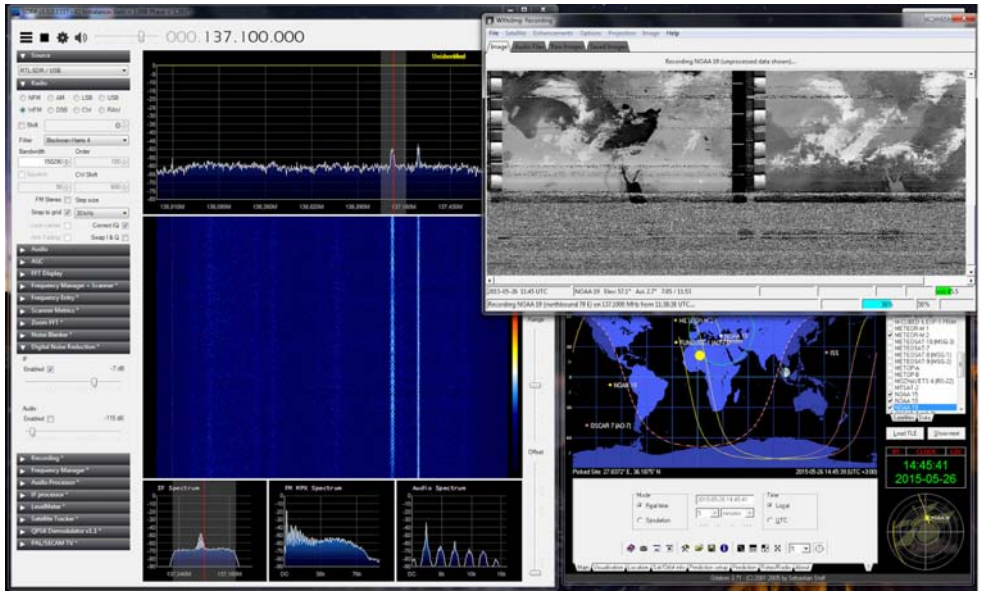
Turnstile

Quadrifilar Helix (QFH)

V-Dipole

Double Cross Antenna (DCA)

NOAA-19 uydusu üzerimizden geçerken 137.100Mhz frekansından gönderdiği sinyalleri SDRSharp yazılımı ile dinleyip, gelen sinyalleri WXtoImg yazılımına aktararak fotoğrafa dönüştürülmesi sağlanmaktadır.



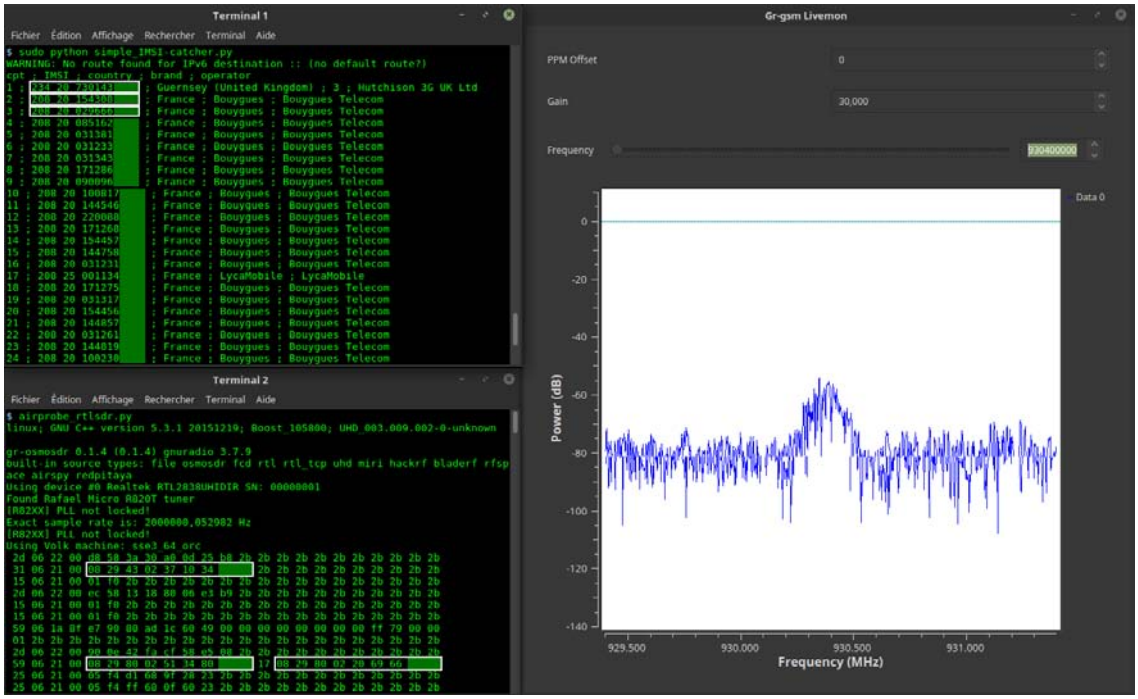
GSM Baz İstasyonları Dinleme ve Analiz Etme

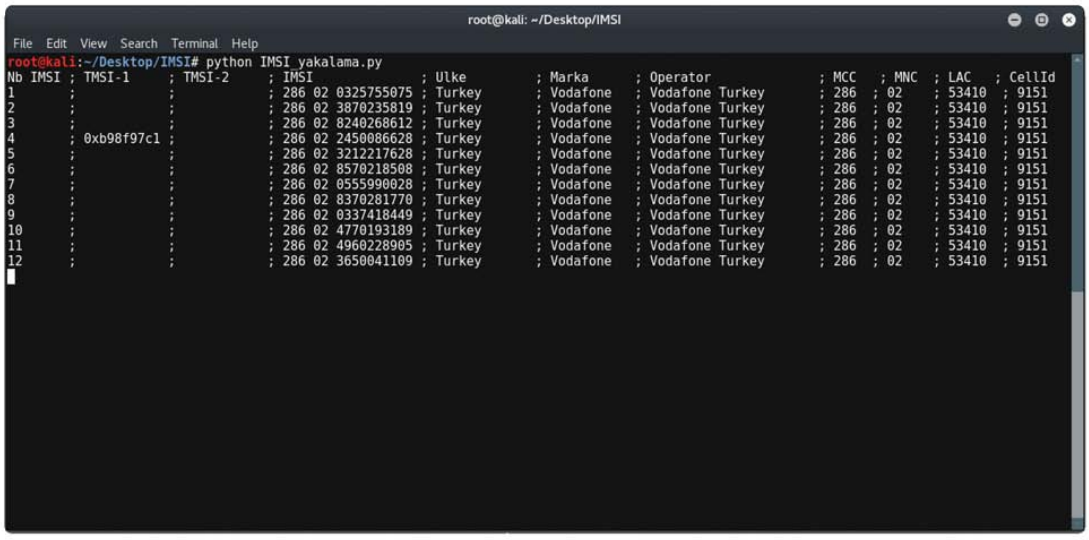
RTL-SDR donanımı ile tıpkı cep telefonlarının yaptığı gibi GSM sinyalleri dinlenip analiz edilebilir. Her kablosuz iletişim sisteminin kendisine ait bir standardı bulunmaktadır. GSM iletişimi için kullanılan sistemler hâlen oldukça eski ve birçok zafiyet içermektedir. Sinyallerin rahatlıkla dinlenebilmesi ve birtakım yazılımlar ile bu sinyallerin analiz edilmesi ile tehditler oluşabilmektedir.

GSM iletişiminde konuşmaları veya yazışmaları okuyabilmek yerine sadece sinyallerini dinlemek ve IMSI diye tabir edilen her cep telefonu kullanıcısına ait olan kodları öğrenmek bile başlı başına büyük bir zafiyet oluşturuyor. Hakkında onlarca kitap yazılan ve filmi çekilen meşhur hacker Kevin Mitnick'in bu yöntemle uzun süre FBI'den kaçmayı başarmıştı. Mitnick; sosyal mühendislik dehasını kullanarak FBI personellerine ait IMSI kodlarının tamamına sahip olmuştu. Bilgisayarına kurduğu donanım ve yazılım ile sürekli olarak çevresindeki baz istasyonlarını dinleyip o istasyonlara giriş yapan IMSI numaralarını kontrol etti. Eğer çevresindeki baz istasyonuna FBI çalışanlarından birisine ait IMSI kodu girdiyse bilgisayarı ona uyarı veriyordu ve hemen oradan uzaklaşıp kaçmayı başarıyordu. 1990'ların başında kullanılan bu yöntem hâlen kullanılabilmektedir. GSM sinyallerini dinleyen Mitnick yine buna benzer bir yöntem ile yakayı ele verdi. Tsutomu Shimomura adlı bilgisayar güvenliği uzmanı, Mitnick'i yakalayabilmek için sahte GSM baz istasyonu kurarak Mitnick'in tüm iletişimini kendisi üzerinden geçmesini ve kayıt altına alarak yakalanmasını sağladı.

Sosyal mühendislik ile GSM zafiyetleri birleştirildiğinde ucu oldukça açık ve engellenmesi neredeyse imkânsız tehditler ortaya çıkmaktadır. GSM teknolojileri yeniden elden geçirilmediği taktirde bu zafiyetler büyük tehditler oluşturmaya devam edecektir.

RTL-SDR ve Gr-GSM yazılımı ile GSM baz istasyonlarından yayın yapan sinyaller analiz edilerek IMSI numaraları görüntülenebilmektedir.





Google'a Ortak Olmak
Google AdSense Gelirinizi Bine Katlayın!

Bu yazımızda internet sitelerinin en temel yapı taşı olan çerezlerden (cookie) ve bunların oluşturduğu çok ciddi bir zafiyetten, yine bundan faydalanarak ne derece dehşet verici sonuçlar olabileceğinden bahsedeceğim. Bildiğimiz üzere çerezler, tarayıcı aracılığıyla sitelerin bizden veri toplamasına izin veren küçük dosyalardır. Örneğin sitede geçirdiğimiz süreden gezindiğimiz sayfalara, parolalarımızın ya da ayarlarımızın hatırlanmasından hangi yolla siteye ulaştığımıza, kullandığımız tarayıcıdan işletim sistemimize, hangi sıklıkla siteyi ziyaret ettiğimize kadar daha sayamadığımız birçok bilgiyi bu dosyalar aracılığıyla karşı tarafa ulaştırırız.

Hepinizin şimdiden nedir bu dehşet verici sonuçlar dediğinizi duyar gibiyim. Uzatmadan testlerini gerçekleştirdiğim ve yine aldığım sonuçlardan dolayı hayrete düştüğüm birini sizlerle paylaşacağım. İnternet reklamcılığının en büyüğü olan Google AdSense ve Adwords'u bilmeyeniniz yoktur zannediyorum. İster inanın ister inanmayın ama 2013-2015 yılları arasında 3 senede 168 Lira para kazandığım AdSense hesabımdan bu zafiyeti kullanarak bir ayda 1.200 TL ödeme aldım. 4 ay gibi bir süre zarfında yaptığım testlerde 8.800 Lira tahmini kazancın yaklaşık 5000 lirasını Google amca bana ödedi. Site aynı site reklam aynı reklam günlük 30-40 ziyaretçi alan bir site nasıl olur da bu kadar gelir elde eder. Üstelik bir bilgisayar ve Visual Basic Script ile son derece acemice hazırlanmış sanal ziyaretler üreten bir botla.

Sonuç olarak durumun ne kadar ciddi olduğunu birkaç uzman dostumla istişare ettikten, onlarında teyidini aldıktan sonra Google amcaya rapor etmeye karar verdim. Bu durum benim dürüstlük anlayışıma ahlaki değerlerime aykırı olduğu için de botu çalıştırmayı durdurdum.

Tüm ayrıntılarıyla birlikte günlerce Google Security Team ile mailleştim. Son olarak gelen *"Gönderiminize bir göz attık ve bunun bir güvenlik açığı olmadığını doğrulayabiliriz, ancak keşiflerinizle ilgili ayrıntılı bilgi göndermenizi memnuniyetle karşılıyoruz."* gibi bir cevapla yazışma sonlandı.

İnanır mısınız hiç şaşırmadım. Çünkü zaten bende bir yazılım açığıdır diye rapor etmemiştim ve bu durumu telafi edecek kısa vadede hiçbir çözümleri olmadığını çok iyi biliyordum.

Aslında çok kolay birkaç radikal çözüm var ama hiçbiri kullanıcı haklarını ihlal etmeden bunu aşamaz. Silinemeyen çerezler veya her tarayıcıya bir değişemeyen ID vermeleri falan filan.

Ama bunların hepsi hak ihlali olur. Çünkü kimse izni olmadan takip edilmek istemez. Aradan geçen 3 seneden sonra botu yeniden çalıştırdım. Birde ne göreyim kral hâlâ çıplak aynı durum devam ediyor. Zaten ben bu raporladığım sorunun, sadece Google ile ilgili bir sorun olmadığını Youtube, Yandex, Bing, Facebook'dan tutun da en küçüğüne kadar tüm internet sitelerinin bundan etkilendiğini anlatmaya çalışmıştım. Ama Google amca bunu neden önemsesin ki? Ben AdSense reklamlarını oynatarak sahte ziyaretlerle 1.000 lira kazanırken onlara 10.000-20.000 lira kazandırıyorum. Kaybeden reklam verenler oluyor.

Her neyse şimdi gelelim zurnanın zırt dediği yere. Nasıl oluyor bu sahte ziyaretler. Ben ilk önce konunun çok daha net anlaşılması için botsuz manuel olarak nasıl yapacağımızı anlatmaya çalışacağım.

Bildiğimiz gibi bütün tarayıcıların ayarlarında gizlilik diye bir bölüm var. Her ne kadar küçük farklılıklar olsa da hepsi aynı. Ben önce en çok tercih edilen Google Chrome tarayıcısı ile ilgili ayarları anlatacağım.

TARAYICI AYARLARI

Şimdi ayarlara giriyoruz.

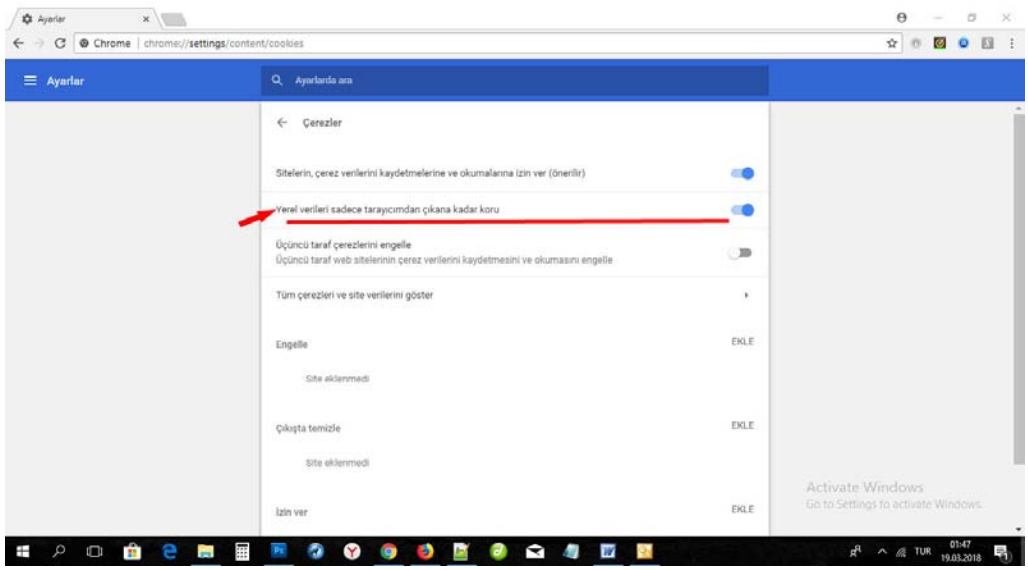
Ayarların en altında "Gelişmiş ayarları göster" seçeneğini tıklıyoruz.

Daha sonra Gizlilik ana başlığı altında "İçerik ayarlarına" giriyoruz.

Çerezlerin tarayıcıda nasıl kullanılacağı ile ilgili ayarları burada yapacağız.

Burada tek yapmamız gereken "*Yerel verileri sadece tarayıcımdan çıkana kadar koru*" seçeneğini aktif ediyoruz. Bu durumda tarayıcımızı kapattığımız anda çerezlerde silinmiş olacak.

Eğer değiştirmediysek default ayarlarında "*Sitelerin, çerez verilerini kaydetmelerine ve okumalarına izin ver (önerilir)*" seçeneği açık, "*Üçüncü taraf çerezlerini engelle*" seçeneği ise kapalıdır. Ne olur ne olmaz diye de konum ayarlarından "*Erişmeden önce sor (önerilir)*" olan seçeneği de kontrol ediyoruz. Eğer konumlara izin verilmişse mutlaka engellemek yerine "*Erişmeden önce sor (önerilir)*" seçeneğini seçiyoruz. Ayarların hepsi bu kadar. Bilgisayarımızda kurmuş olduğumuz diğer tarayıcılarda da bu ayarları yapıyoruz.



Bildiğimiz gibi trafiğimiz sadece masaüstü bilgisayarlardan olursa Google amca yemez. Çoğu tıklamayı geçersiz sayar. Onun için mobil ve biraz da tabletten girmeliyiz ki ağımız geniş olsun. Yukarıda bahsettiğim ayarlar aynı şekilde mobil tarayıcılarda da var ama bir farkla. Tarayıcıyı kapattığımızda otomatik silme işlemi yerine mobil cihazımızdan ayarlara girip elle çerezleri sileceğiz. Tabletlerde de tarayıcı ayarlarından gizlilik başlığı altında "*Tarayıcı verilerini sil*" diyerek elle sileceğiz.

Tarayıcı ayarlarımızın hepsi bu. Şimdi son olarak geldik IP adresimizi değiştirmeye. Bu işlem de en az çerezleri silmek kadar kolay. Dinamik IP ile çalışan modemimizin fişini çekip yeniden taktığımız anda yepyeni bir IP adresimiz olmuştur. Mobilde de telefonumuzu uçak moduna alıp bir süre bekleyip açıyoruz. Bu kadar.

Artık AdSense reklamlarının yayınlandığı sitemize gidip reklamlarımıza tıklayarak para kazanmaya başlayabiliriz. Yine "*bu kadar kolay olamaz çok saçma*" dediğinizi duyar gibiyim. Ama inanın bu kadar kolay. Deneyin görün. Direk, arama motoru ya da backlink ile sitenize gelin bir iki sayfa gezdikten sonra reklamı tıklayın gittiğiniz sayfada da biraz dolaştıktan sonra tarayıcıyı kapatın. Modeminizi kapatıp açın. Cihazınız mobil ise paranızı kazandıktan sonra uçak moduna alın tarayıcınızın ayarlarından çerezleri sizin. Sonra uçak modundan çıkarın. Yeniden aynı döngüye devam edin.

DİKKAT EDİLECEK ÖNEMLİ NOKTALAR

1. En öncelikli konu sakın ola sahte tıklama yaptığınız cihazınızdan ya da aynı IP'den Google hesabınıza giriş yapmayın. Anında banlanırsınız.
2. Tıklama yaparken reklam gösterim oranını tıklama oranını en doğal sayıda tutun. Yani tıklamayı artırırken sitenize ziyaretçi sayısını da aynı oranda artırın. Mesela ben siteme 30-40 olan hitimi organik hit programlarıyla 1000-1500'e çıkarttım. Bu şekilde reklam gösterimini şişirdim. Örneğin 100 olan gösterim sayısı bir anda 2000-3000 oldu. Bu durumda "Tıklama Oranını" TO değeri Google amcaya aykırı sinyal gönderemeden %1-%2 bandında kalarak tıklama şansımı 20-30 kat artırdı.
3. Sitenizin raporlarına uygun hareket edin. Google Analytics size tüm detayları veriyor zaten. Buradaki raporları inceleyip ona sadık kalmaya özen gösterin. Örneğin sitenize gelen trafiğin %60 ı mobil ise siz de sahte tıklamalarınızın %60'ını mobilden yapın. Trafiğin %40 Chrome ise siz de tıklamalarınızı %40 oranında Chrome'dan yapın. Eğer sahte tıklama yapacağınız bölge kısıtlıysa o bölgeye özgü bir site yapın ve trafiğinizi o bölgeden alın. Örneğin sahte tıklamaları sadece İstanbul içindeki ağınızdan yapacaksanız İstanbul ile ilgili bir sitede reklamlarınızı yayınlayın. istanbularakadasariyorum.com gibi bir siteden gelen trafik ve tıklama Google amcaya aykırı bir sinyal olamayacaktır.
4. Eğer sitenizin arama motorlarından çok fazla bir trafiği yoksa direk ya da Javascript yardımıyla başka bir siteden backlinkle gelen yoğun trafik oluşturabilirsiniz. Google amca trafiğinizin %90'ı neden başka bir siteden geliyor diyemez. Çünkü siz reklam da vermiş olabilirsiniz sizinle ilgili bir haber de olmuş olabilir.
5. Sitenize ulaştıktan sonra doğal davranmaya özen gösterin. Bir iki sayfa gezdikten sonra reklama tıklayıp gittiğiniz sitede gezinin. Header'daki reklam yerine footer'daki reklamı daha çok seçmeyin. Her zaman oranları koruyun.
6. Çerezleri silmek yerine bir havuzda toplayıp random olarak eski çerezlerden de bazen giriş yapmamız Google amcanın uyanmaması için iyi olur. Örneğin bir ay önceki ziyaretçi de ara sıra sitemizi yeniden ziyaret edebilmeli ve reklamımıza tıklayabilmeli.
7. Sitenizin içeriğini iyi seçin. Ona göre trafik ve tıklamayı ayarlayın. Yani kişisel bir blog ile bir haber sitesinin potansiyel trafiği bir değildir.
8. Aynı yöntem ile sitenizdeki diğer özel reklamları aldatabileceğinizi, Youtube'daki videonuzun izlenme oranını artırabileceğinizi, sizi banlayan ya da yasaklayan sitelere de yeniden giriş yapabileceğinizi veya SEO için gerekli birçok kriteri gerçekleştirebileceğinizi unutmayın. Adwords reklamlarını da aynı yöntemle tıklayarak rakip firmaların kredilerini de sömürebilirsiniz.

Şimdi bir de bu işlemi manuel yapmak yerine bir bot ile yaptığınızı düşünün. Artık sizde Google amcaya %10 ortaksınız. Saygılar.

WEB GÜVENLİĞİ VE SIZMA TEKNİKLERİ EĞİTİMİ

İLK EĞİTİME ÖZEL
750TL

Eğitim kimlere hitap ediyor?

- Siber güvenlik araştırmacısı olmak isteyenler
- Güvenli web siteleri oluşturmak isteyen web yazılımcıları
- Güvenli web hizmeti sağlamak isteyen sunucu/DC çalışanları
- Bilgi güvenliği uzmanları
- Kurum içi sızma testi gerçekleştirmek isteyenler
- IT uzman ve junior çalışanları
- Network uzman ve junior çalışanları

Eğitimin İçeriği:

- HTTP 101
- Cookies
- Same Origin Policy (SOP) & Document Object Model (DOM)
- Web Application Penetration Testing
- Why Penetration Testing For Web Applications
- Survive In the Web
- The Types of Pentesting
- Stages of Pentesting
- Passive Reconnaissance
- Active Reconnaissance
- Vulnerability Mapping
- Attacking to Web Applications
- Information Leakage
- Insecure Object Reference / Path Traversal
- Filters
- Injection Based Flaws
- Command Injection
- SQL Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Local File Inclusion (LFI) / Remote File Inclusion (RFI)
- CRLF Injection
- File Upload Vulnerabilities
- Open Redirection - Unvalidated Forward & Redirects
- Reporting Vulnerabilities
- Bonus: Gamification

Gereksinimler:

- Web / HTTP protokolü işleyişine dair temel düzeyde bilgi sahibi olmak ve
- En az bir web programlama dili için temel düzeyde bilgi sahibi olmaK

Eğitmenlerimiz:

- **Ziyahan ALBENİZ** - Security Researcher
- **Ömer ÇITAK** - Security Researcher

Eğitim sonunda elde edilecek kazanımlar?

Katılımcılar;

- Güvenli bir web uygulamasının unsurları
- Web uygulamasında zafiyet tespitine giriş
- 1 yıllık ücretsiz mentörlük hizmeti!

Kimler Katılabilir?

16 yaş ve üstü herkese hitap ediyor.
Eğitimimiz 2 gün / 16 saat'den oluşmaktadır.
Minimum katılım 15 kişi olarak belirlenmiştir.

Ne Zaman?

12 - 13 Mayıs tarihlerinde 09.30 – 18.30 saat aralığında verilecektir.

Araçlar:

- Dizüstü bilgisayar,
- Kali Linux

HEDİYELERİMİZ:

- 1 yıllık ücretsiz mentörlük hizmeti,
- Eğitmenlerimizden **Ömer ÇITAK**'ın "**Ethical Hacking**" kitabı ve
- Arka Kapı Siber Güvenlik Dergisi'nin 1 yıllık dijital ya da basılı aboneliği hediye edilecektir!

SECHOOL - İstanbul Çırak Atölye

2 Gün Web Güvenliği Eğitimi & Sızma Teknikleri **16 Saat**

www.sechool.com.tr

SECHOOL
SİBER GÜVENLİK EĞİTİM DANIŞMANLIK

Yusuf Yaltırık - yusuf.yaltirik@gmail.com

Hacker Palas

Bir Hacking Hikâyesi

Hacker kelimesinin TDK Yabancı Sözlere Karşılıklar Kılavuzu'ndaki anlamı: *Bilgisayar korsanı - Bilgisayar ve haberleşme teknolojileri konusundaki bilgisini gizli verilere ulaşmak, ağlar üzerinde yasal olmayan, zarar verici işler yapmak için kullanan kimse.*[1]

Peki bütün hackerlar zararlı mı? Ya da suçlu mu? Tabii ki hayır. Kimimiz işin "siyah", kimimiz "beyaz", kimimiz ise "gri" tarafında. Bana sorarsanız ya iyi tarafı seçersiniz ya da kötü. Bir hacker için iyi ve kötünün tanımı gayet açıktır. Siyah ve beyaz kadar. Ben de naçizane beyaz tarafında yer alıyorum.

Aslında hiçbir zaman hacker olmak istemedim. Kariyerime daha çok web ve mobil platformlarda projeler, uygulamalar geliştirerek devam etmek istedim. Çünkü insanlara "Bir açığınız var" deyince açığı sanki siz oluşturmuşsunuz, hata size aitmiş gibi, "bizim açığımızdan sana ne" vs. gibi dönüşler alınabileceğini biliyordum.

Hâlbuki amacınız sadece bulduğunuz sorunları bildirerek iyilik yapmaya çalışmak olabilir. Özellikle yazılımsal açıkları bulmak profesyonel insanlar için zor bir iş değil. Ancak açıkların mal olabileceği zararları telafi etmek bazen çok zor hatta imkânsız.

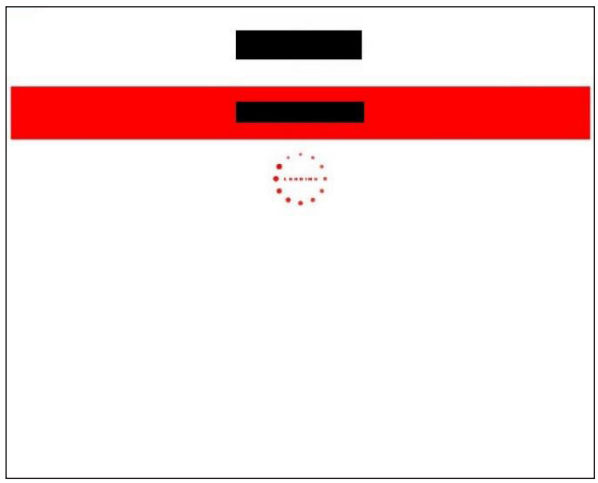
Beyaz şapkalı bile olsanız her zaman anlayışla karşılanmıyorsunuz maalesef.

Baştan söylemekte fayda var. İyi niyetli yaklaşımınız bile bazen suistimal edilebiliyor. Bazen yaptığınıza, yapacağınıza pişman olabiliyorsunuz. Bazen de iyi ki bu yolu seçmişim diyorsunuz. Bu, muhatap olduğunuz insanların siber güvenlik konusuna nasıl baktığına, ne kadar önem verdiğine paralel olarak değişiyor. Eğer siber güvenlik konusunda duyarlı ve bilgili biriyle muhatapsanız herhangi bir olumsuzlukla karşılaşmadan günü bitirebiliyorsunuz.

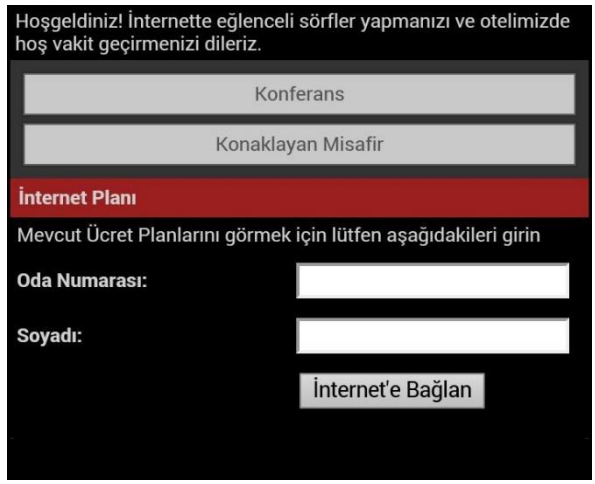
Bir gün bulunduğum bölgedeki internet erişimim kesildi ve internete erişebilmek için yapabileceğim tek şey Wifi ile başka bir ağa bağlanmaktı. Çevremdeki ağları aradım ve alıcımın ulaşabildiği, şifresiz tek ağ olan 5 yıldızlı bir otele ait Wifi ağına bağlandım. Otel ile bulunduğum mekân arasında onlarca metre olmasına rağmen alıcım neredeyse tam çekiyordu. Bulunduğum yer 4. ya da 5. kattaydı. Sanırım Wifi antenini otelin en tepesine yerleştirmişlerdi. Galiba buradaki amaç otelin reklamını yapmaktı. Dolayısıyla güçlü bir cihaz kullanıyorlardı. Şifresiz olduğu için ağa bağlandım. Doğal olarak benden oda numarası, soyisim gibi bilgilerin istendiği giriş ekranına (Bk: Giriş Ekranı) yönlendirildim. Otelin bir müşterisi değildim sonuçta.

İnternete erişimim olmadan da işlerimi nasıl halledebilirim, günü nasıl geçiririm diye düşünüyordum bir yandan. Giriş ekranını atlayıp internete bağlanmanın doğru olmadığının da farkındaydım. Bir seçim yapmam gerekiyordu. Ya işlerimi yarım bırakıp, uğraşacak başka şeyler bulacaktım ya da küçük bir yaramazlık yapıp giriş ekranını atlamak için çözüm arayacaktım. Sonunda programın açığını aramaya, eğer bulursam bildirmeye karar verdim. Bunun karşılığında interneti kullanmanın affedilebileceğini düşündüm. Açıkları aramaya başladım. Derken yazılımsal bir hatadan kaynaklanan zafiyetten yararlanarak internet erişimini sağladım. Açık çok basit bir hatadan kaynaklıydı. Program, herhangi bir sayfaya giriş yapılmaya çalışıldığında eğer oturum başlatılmamışsa giriş ekranına (Bk: Giriş Ekranı) yönlendiriyordu.

1 http://www.tdk.gov.tr/?option=com_karsilik&view=karsilik&kategori1=abecesel&kelime2=H ċ



Yönlendirme Ekranı



Giriş Ekranı

Ancak yönlendirme yapılırken (Bk: Yönlendirme Ekranı) bir takım veriler GET methodu ile gönderilerek sunucu tarafında işleniyordu. Verilerden bir tanesi de (aşağıda gördüğünüz gibi) port numarasıydı.

http://xxx.xxx.xxx.xxx/redirect.php?UI=xxxx&NI=xxxx&UIP=xxx.xxx.xxx.xxx&MA=xxxxxxxxx&RN=Guest Wireless&PORT=90&RAD=yes&CC=no&PMS=no&SIP=xxx.xxx.xxx.xxx&OS=http://www.google.com%2Fm%3Fclient%3Dms-android-htc%26source%3Dandroid-home…

Port numarası varsayılan değerini değiştirdiğimizde (Örn. 800) aktif olan, açık portlara bağlanarak herhangi birinin odasına bağlanır gibi kullanıcı ekranına (Bk: Kullanıcı Ekranı) dışarıdan erişim sağlanabiliyordu.

Kullanıcı Ekranı

Üstelik otelin kullandığı bu program otele özel yazılan bir program da değildi. Yani dünyanın birçok yerinden hatırı sayılır sayıda otel kullanıyor. Merak ettim, biraz daha ileri gittim ve oteldeki herhangi biri adına faturayı kabartabilecek işlemler yapılabildiğini fark ettim. Biraz daha ileri giderek ağdaki cihazları taradım.

Aralarında otelin sunucusunun, otel müşterilerinin kullandığı onlarca bilgisayarın, onlarca mobil cihazın da aynı ağa bağlı olduğunu gördüm. Ayrıca ağ güvenliğini sağlayan herhangi bir güvenlik duvarına da denk gelmedim. Kötü niyetli bir insanın bu açıklardan faydalanarak hem oteli hem de otelin müşterilerini ciddi zararlara uğratabileceğini düşünerek durumu ilgili kişilere aktardım. Gayet güzel bir dille teşekkür ettiler ve açığı kapatacaklarını söylediler. Tabii tüm bu işlerle uğraşırken interneti kullanmaya fırsatım olmadı. Benim için ilk hacking denebilecek olay böylece yaşanmış oldu.

Zaman geçtikçe çok güvenilir olduğunu düşündüğüm sistemlerin bile aslında pek de güvenilir olmadığını fark ettim.

Projman'ın Kaleminden TR Scene ve TCG Dergileri'nin Hikâyesi

İletişimi seven bir toplumuz. Bugün Türkiye'de her 100 kişiden yaklaşık 60'ı internet kullanıcısı[1]. 25 sene öncesine döndüğümüzde ülkemizde internet kullanıcısı henüz iki elin parmakları kadardı.

İnternetin babası sayılabilecek BBS'ler telefon hatları üzerinden modemler yardımı ile yapılan bir bağlantı ile kullanıcıların sunucu sistemine girerek, çevrimiçi olanlarla yazışabildikleri, çevrimiçi olmayanlara mesaj bırakabildikleri bir sistemdi. Ülkemizde Softcom BBS (Boğaziçi) ile Buces BBS (Bilkent Üniversitesi) dışında, dosya paylaşımları gibi çeşitli yer altı paylaşımlarının yapıldığı Neverland BBS gibi sistemler de vardı. Sonraki yıllarda SLIP türü bağlantılarla internet sistemi içerisinde bir süre daha kullanılmaya devam edilseler de zaman içerisinde kayboldular. ***telnet 139.179.11.11 3000*** komutunu hatırlayanların yüzünde bugün dahi bir gülümseme belirecektir. O günlerde 2400bps'lik modemlerin kullanıldığını da not edelim.

1993 yılında 64Kbps'lik bir kiralık hat ile ODTÜ'ye yapılan internet bağlantı hızı BBS camiasında büyük yankı uyandırmış ve hızın ne kadar yüksek olduğu konuşulmuştu. (Bugün ortalama bir 4G bağlantısının 12 Mbit olduğu düşünüldüğünde, Türkiye'nin tüm internet çıkışından 192 kat daha fazla olduğu ortaya çıkacaktır.)

1 https://www.slideshare.net/wearesocialsg/digital-in-2017-western-asia/139

Türkiye

Türkiye İnternet bilgisayar ağına bağlandı

ANKARA, (Tercüman)- Bilimin doğrudan bir üretici güç haline dönüşmesi, sanayide teknoloji içeriğinin hızla artması bağlamında bilgiye etkin ulaşımın hayati önemini dikkate alarak ODTÜ ve TÜBİTAK tarafından birlikte yürütülen uluslararası Internet bilgisayar ağına bağlanma projesi sonuca bağlandı.

Daha önce Devlet Bakanı ve Başbakan Yardımcısı Erdal İnönü'nün de katıldığı bir törenle, Hollanda'nın Nikhef araştırma merkezine X.25 kullanarak sağlanan Internet bağlantısı X.25 kullanımının çok pahalı olması nedeniyle genel kullanıma sunulamamıştı.

Internet'in genel kullanıma sunulmasını sağlayan bağlantı 64 Kbit'lik kiralık hat üzerinden Washington'da bulunan National Science Foundation (NSF) ile ODTÜ arasında gerçekleştirildi. Bağlantının PTT tarafından sağlandığı İnternet şu anda sadece ODTÜ, TÜBİTAK ve Bilkent Üniversitesi tarafından kullanılıyor.

Türkiye'de... araştırma kurumları ve üniversitelerin yanısıra kamu, özel sektör ve ordu, dünya çapında binlerce yerel ağı ve yaklaşık 750 bin çok ve tek kullanıcılı bilgisayarı birbirine bağlayan Internet'e ulaşabilecek.

1995 yılına kadar, ülkemizin önde gelen üniversiteleri ile TÜBİTAK online bağlantılarını kurarak akademik camiaya internet hizmeti sunmaya başlamışlardı bile. TÜBİTAK bünyesindeki BİTAV, isteyen bireysel kullanıcılara da kendi bünyelerindeki VAX terminallerle internet erişimi vermeye başlamıştı. Siyah ekran üzerinde yeşil yazılara saatlerce bakılan, dışarıdan izleyenlerin "bu adam bu ekranda ne görüyor?" sorusunu sordukları zamanlardı.

1996 yılında milli internet omurgamız TURNET faaliyete girdiğinde, Compuserve ve AOL isimli iki dünya devi internet servis sağlayıcı firması Amerika Birleşik Devletleri'nde on binlerce kullanıcıya hizmet veriyordu bile. TURNET'in devreye alınması ile birlikte ülkemizde de internet servis sağlayıcılar türemeye başladı. Sektör öncüleri Superonline, Raksnet, Alnet gibi kurumlar, 800'lü hatlar üzerinden önce 14.4Kbps sonra 28.8Kbps hizmet vermeye başladılar. Dijital santrallerin yaygınlaşması ile 56 Kbps hızlara çıkması 90'ların sonlarını bulacaktı. 800'lü hatların ücretli hale getirilerek belli periyotlarla faturalandırılması, internet kullanımını azaltsa da kullanıcı sayısının artmasını engelleyemedi.

Henüz Google hayatımızda yoktu o yıllarda, sosyal medya da. IRC sunucularında kurulan sohbet odalarında sosyalleşiyordu tüm dünya kullanıcıları, "asl?" sormanın ve özelden yazmanın meşhur olduğu zamanlardı.

2000'ler önce ISDN sonra DSL bağlantıları ile geniş bant kavramı ile kullanıcıları tanıştırırken, artık hem telefon hatları meşgule düşmüyor hem de internet hızı Mbit değerlerine doğru tırmanıyordu.

Internet baş döndürücü bir hızla gelişirken, büyük firmalar web mecrasında yerlerini alıyor ve kurumsal internet, ağların birbirine internet üzerinden bağlanması kavramları gelişiyor ve dünya hızla dijitalleşme sürecine giriyordu.

Bütün bu dönüşümler devam ederken, internet dünyasının arka sokağında, adına kimilerinin korsan, kimilerinin hacker adını verdiği, kişiler ve gruplar ortaya çıkıyor ve çoğu zaman maddi hasarlara yol açan aktivitelerde bulunuyorlardı. İnternet ve ağlar ile ülkemizden çok önceden tanışan Amerika Birleşik Devletleri'nde Kevin Mitnick adında henüz 16 yaşındaki bir çocuk 1979 yılında, DEC firmasının geliştirdiği PDP-X serisi bilgisayarların RSTS/E işletim sistemini yasa dışı yollarla çoğaltarak bir yıllık hapse mahkûm ediliyordu.

1996 yılında, bir Ankara gecesinde Kevin Mitnick'le ilgili bir makaleyi okuyordum:

"Kevin 1994 noelinde TCP Sequence Prediction adı verilen bir yöntem ile Shimomura'ya karşı planlı saldırısını başlattı. Böyle bir saldırıyı gerçekleştirmek için Kevin, Shimomura'nın web sunucusu ve X-terminali arasında kullanılan TCP dizi numaralarını doğru bir şekilde tahmin etmeyi denedi. TCP handshake mekanizmasının doğası gereği, TCP Sequence / Acknowledge numaraları tahmin edilebilir. Kevin bu numaraları taklit edebilirse gönderici olarak Shimomura'nın web sunucusunu taklit edebilir onunla iletişim kurabilirdi. Orijinal gönderenin ek paketler göndermesini engellemek için, Kevin gerçek göndericiye karşı SYN-Flood saldırılarını kullandı. Bu, o tarihte cesur bir saldırıydı.

Çünkü 30 yaşındaki Shimomura, haklı olarak Mitnick'inki kadar karmaşık olan bir hacker / bilimsel kişiliğe sahip olarak çok saygı duyulan bir Japon güvenlik uzmanıydı. Bununla birlikte, Mitnick ve Shimomura arasındaki en büyük fark, Shimomura'nın güvenlik açıklarını ortaya çıkardığında, onları doğrudan yetkililere bildirmesiydi, ama Mitnick onları yasa dışı kazanç için kullandı. Shimomura'nın güvenlik duvarı Mitnick'le hedef arasında meydana gelen tüm aktiviteyi kaydetti. Ertesi gün, 26 Aralık'ta, Shimomura, sis-

teminin Mitnick'in saldırısı yoluyla tehlikeye atıldığını farketti. Mitnick, Shimomura'nın bilgisayarından çoktan özel e-postalarını, çeşitli güvenlik araçlarını, cep telefonlarını kontrol etmek için kullanılan bir yazılımı ele geçirmişti bile…

Hikaye Shimomura ile Mitnick'in kovalamacasıyla devam ediyordu..."

Bu hikâye benim için bir dönüm noktası oluşturdu, o günden itibaren, bir ağ görevlisi olarak kullandığım TCP/IP, Unix (sonrasında Linux), Windows, C++, Softice vs. benim için daha özel bilgiler anlatmaya başlamıştı.

Adına TCG (Türk Crackerları Gazetesi) adını verdiğim ve 8 sayı çıkarttığım dergide, yazılımların kırılması, tersine mühendislik mecrasından çıkıp yavaş yavaş işletim sistemlerinin ve bilgisayar ağlarına yetkisiz giriş yöntemlerine doğru uzanıyordu. 8 sayılık bu online mecmua, döneminin ilk ve ciddi bir okur kitlesi toplayan bir denemesi idi.

Üniversite öğrenciliği sürerken, aynı zaman bir ISS'de çalışıyor ve sonrasının nereye varacağını hesap bile etmediğim bir yola giriyordum. TCG deki 3-5 makale ile başlayan yolculuk, çıktı alındığında 40-50 sayfalara varan bir yoğunluğu buluyor ve bu yükü sadece kendim omuzluyordum. Bu arada forumlardan ve ICQ ile bir ekip oluşmaya başlamıştım bile.

1997'ye geldiğimizde hararetle yeni bir e-dergi çıkartmayı planlıyorduk. Scene'den gelen 4K ile intro yazan arkadaşlar dergi ismini koydular, TR-Scene olacaktı yeni ekibin ismi. Kök kadroda, ana editör olarak ben (Projman), Darkapocalypse, Intruder, Meliksah, Misoskian, Bogac, Bigfoot, Mrstop gibi arkadaşlar vardı. Sizden gelenler, misafir yazarlar gibi katılımcılarla ekibin zaman zaman 20 kişiye kadar çıktığı oluyordu. Artık TR-Scene bir okul olmuş ve sadece HPVC konularında değil, bilgisayar genel kültürü ile ilgili konulara da girmeye başlamıştı. Zaman içerisinde ben artık yazar değil, daha çok koordinatör durumuna gelmiştim.

1998 sonlarında artık okul bitmiş, profesyonel çalışma hayatının zorlukları başlamıştı. İşim ve "hobim" birbirinden farklı kulvarlarda olduğundan, hobime zaman ayıramıyordum ve ekibi bir arada tutan, sürekli diyalog ortamı kaybolmuş, benim gibi diğer arkadaşların da işleri, hobilerini bastırır olmuştu. 12. Sayının birkaç ay gecikmeli de olsa yayınlanmasının ardından, hobi olarak ilerleyen bir çalışmanın da sonuna gelinmiş oldu.

Ekipten hâlâ görüştüğüm birkaç kişi dışında, o zamanlar tatlı bir hatıra olarak kaldı. Bir daha çeşitli platformlarda yazmaya çalıştıysam da çeşitli sebepler hep buna engel oldu.

Agis isminde bir firma, kabiliyetli gençleri toplamış, çeşitli exploit araçlarını bir araya getirmiş, ağ testleri yapabilen bir yazılım geliştirmiş, bunun üzerine ağ izleme ve güvenlik duvarı eklenmiş ve Mindwall isimli ürün belirli bir düzeye getirilmişti. 1999 Ağustosu'nda İstanbul'da, Metropol Bilgisayar'ın çatı katında, Mindwall programının sağını solunu kurcalayıp pazarlamaya hazır hale getirmeye çalışırken marmara depremiyle sarsıldık. Bu hem Aggressor Team'in sonu hem de Türk ekonomisinin uzunca bir süre çıkmaza gireceği bir süreci de beraberinde getiriyordu. Artık ekonominin derdi ne .com idi ne de internet, kurumların ayakta kalmaya çalıştığı bir dönemde IT sektöründe iş bulmanın da en zor olduğu zamanlardı. Bu süreç IT alanındaki birçok çalışmayı ve çalışanı da baltalamıştı.

2001 yılında, şu anda faaliyette olmayan bir bankanın internet üzerinden dolandırılması ile ilgili bir dava dosyasında adım yer alıp, hukuki bir süreç başlayınca, artık bir daha ne Projman olarak anılmaya, ne de hack ile ilgili hiçbir aktivite içerisinde olmama sözü verdim kendi kendime.

Yönümü programcılığa döndüğümde, elimde çeşitli zamanlarda yazdığım yüzlerce küçük araçtan başka bir şey yoktu. Ağ izlemenin (sniffing) en popüler olduğu dönemlerde Nexeye isimli bir ürünle yeniden IT dünyasındaydım. 2009 yılına kadar, geliştirilmesi, pazarlanması devam eden bir ürün olan Nexeye, network monitor programının yanında, dünyanın ilk Windows tabanlı ARP spoof programını da yazmış ve SwitchSnarf'ı uzunca bir süre sektörde var etmiştim.

2009 sonrasında, artık çoluk çocuk ile ilgilenmek, düzenli bir aile hayatı yaşamak gibi, orta yaş rutinleri ağır basıyor ve sabah gidip akşam geldiğim işimin tadını çıkarmaya çalışıyordum.

Her biri ayrı birer hikâye olan bu süreçleri belki de ileriki yazılarda anlatır, tecrübelerimi genç okurlarla paylaşırım. Ancak, şunu iyi biliyorum ki, 90'lı yıllarda bu işlerle ilgilenip, Projman, TR-Scene gibi isimleri duyan herkesin yüzünde bir gülücük belirecektir. Kimseyi kırmamak, ayırıcı olmamak, bilgileri birleştirip paylaşmak felsefesi üzerinden yürüyen sivil bir inisiyatif idi TR-Scene. Umarım bundan sonraki grup çalışmaları için iyi bir başlangıç noktası olur.

Çağatay Çalı - cagataycali@icloud.com

Esir Yeni Dünya
Bugünün Hikâyesi

Web kelimesi İngilizce'de kumaş dokusu kelimesinden esinlenilerek bilgisayar ağını temsilen türetilmiş bir kelime. Bir teknoloji olarak sonsuz bir bilgi deryası olmak, herkesin dilediği bilgiye dilediği zaman ortak bir protokol aracılığı ile ulaşmasını sağlamak gibi amaçlar ile ortaya çıkmıştır. Peki her zaman dilediğimiz verilere mi ulaşıyoruz?

Sıradan internet kullanıcıları olarak sosyal medya hesaplarına, arama motorlarına, tarayıcılara belli başlı bilgilerimizi teslim ediyoruz. Bu bilgiler sisteme girdi olarak alınıp bize ilgili sonuçlar, öneriler, tavsiyeler olarak geri dönüş yapıyor. Bu döngüde ücretsiz olarak kullandığımız bu servislerin kazanç sağladığı ürünler haline geliyoruz. Aramalarımız, sitelerdeki hareketlerimiz, tıklamalarımız ve hatta es geçtiğimiz içerikler dahi sistemin bir girdisi durumunda. Ücretsiz servislerin bu şekilde para kazandığını hemen hepimiz biliyoruz.

İnternetin büyük çocukları (Google, Facebook, Twitter ve benzeri) bizim tarayıcılarımızı değil kişiliklerimizi tekilleştirmeye başladı. Şeytanın dahi aklına gelmeyecek hinlikler şu an bu servislerin kemik yapılarında yer almakta, gelin bunlardan bu Ali Cengiz Oyunlarına birlikte göz atalım...

Öncelikle herkesin bildiği üzere, web siteleri ve mobil uygulamalarda geliştiricilerin ve proje yöneticilerinin ihtiyaç duyduğu metrikleri *ücretsiz* bir şekilde sağlayan servislerin yarattığı gözetle - tespit et - aksiyon al kısır döngüsünü ele almayacağız. Sizlerle gerçek hayatımıza bir şekilde girmiş, teknolojinin somut tehlikelerinden bahsediyor olacağız. Bir senaryo üzerinden gidelim, hangi kör noktalardan nelerin çıkabileceğini görelim.

Bir kafeye gittiniz ve arkadaşlarınızla hoş bir sohbet içerisindesiniz telefonunuza bir bildirim geliyor, "Hey X mekânındasın, burası insan kaynıyor!". Swarm / Facebook / Twitter / Snapchat / Uber gibi uygulamalar arka planda lokasyonunuzu alenen dinleyip birbirlerine haber verdiler ve size bu bildirimi sundular. Bu uygulamardan bir tanesi dahi analitik servislerini kullanıyorsa artık nerede olduğunuzu internetin büyük ağabeyleri de biliyor.

Hikaye bu ya, arkadaşınız size geçen yaz tatilde gezdiği Y mekânındaki fotoğraflarını gösteriyor. Siz bu fotoğrafları hangi kamerayla çektiğini soruyorsunuz, Z marka kamera ile çektiğini öğreniyorsunuz fakat yalnız değilsiniz. Acele etmeyin, ertesi gün size o kamera ve o mekân hakkında öneriler gelmeye başlayacak. Cep telefonunuz sizi oturduğunuz mekândayken dinledi ve sizi daha da tanımaya başladı. Arkadaşınız size Instagram üzerinden güzel bir kedi videosu izletmeye başladı, siz dalgınlıkla Facebook hesabınızdan "kedi vi" yazdınız fakat yanlış yere yazdığınızı fark edip hemen uygulamayı kapatıp Instagram'ı açtınız. Keşfet sekmesinde komik kedi videoları görmenize şaşırdınız mı peki?

Sosyal medya hesaplarınızın beslenmesi gerek, içtiğiniz içeceğin fotoğrafını yüklediniz. Yüklediğiniz fotoğrafta bulunan EXIF(1) datası cihazınıza dair bilgileri, cihazınızın gerçek konumunu ve bunlarla beraber uygulamanın dilediği zaman cihazınızın kamerası kullanmasının yetkisini çoktan verdiniz. (2) Hikâye bu ya, akşam eve giderken ansızın anneniz sizden kediniz için mama almanızı istedi fakat en yakın marketi geçeli çok olmuş, tüm gün verilerinizi aşırmaktan yorulan cep telefonunuzun bataryası can çekişiyor ve %5 şarja sahipsiniz. En sevdiğiniz çevrimiçi sipariş sitesine / uygulamasına girdiniz ve yoldayken eve sipariş vermek istiyorsunuz o da nesi, akşamüstü konuştuğunuz Z marka kameranın o sitede / uygulamada %25 indirimi var ve indirimin bitmesine sadece 15 dakika var.

Bu nasıl olur, bu fırsatı kaçırmamanız gerek öyle değil mi? Yoksa bunların hepsi bir kurmaca mı? Alacağınız cihazın gerçek piyasasını dakika dakika takip edebiliyorsanız ne ala. Peki o kadar şarjınız varken bu fırsatı kaçırmak yerine fiyat araştırması yapabilir misiniz, hem de yürürken? Peki bu kadar rastlantı olur mu?

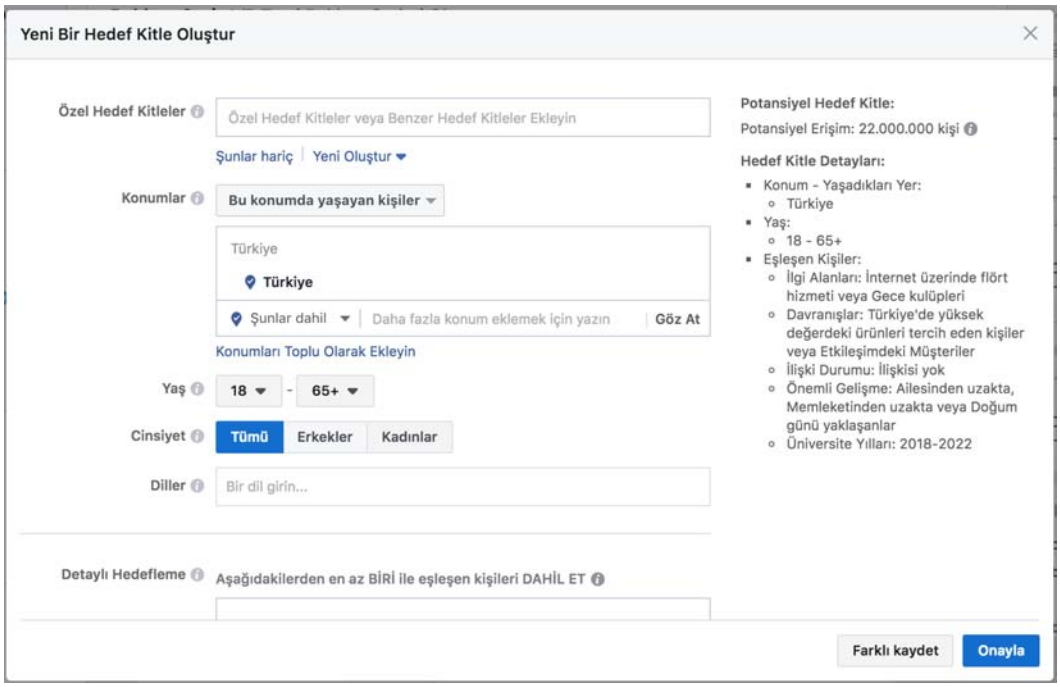
Şimdi senaryoya bir geliştirici açısından bakalım...

Kasten eskitilmiş telefonunuzun bataryasının bitmek üzere olduğu bilgisi siteler / uygulamalar tarafından kolaylıkla bulunabilir (3). Aynı zamanda yürüyor / oturuyor / uzanıyor / öz-çekim yapıyor olduğunuzun bilgisi de sizin izniniz, bilginiz dışında kolaylıkla işlenebilir. (4)

O kamerayı almak istediğinizi arkadaşınızın sesinden dinleyen uygulamanız (5), aynı zamanda sosyal medyada arkadaş olduğunuzu kişinin daha önce yüklediği Y mekânındaki fotoğrafların EXIF bilgisinden eşleştirerek doğruladı. Konum bilgilerinizden de sizi eşleştirerek sizi net bir hedef olarak belirledi. Kaçışınız yok, siz alıcısınız ve onlar da satıcı.

Bu hikayedeki konu mankeni olan bizler, bize sağlanan ücretsiz servislere verdiğimiz veriler ile kendimizi ifşa ediyoruz. Bu durumu sadece para kazanmak adına kullanacaklarını düşünmek fazla iyimser bir yaklaşım olur.

Yukarıda detaylıca incelemeye çalıştığımız konuda bir kör nokta daha var, bu bulgular ışığında kendi benliğimiz çalınıyor. Düşüncelerimiz, davranışlarımız, yaşayış tarzımız…



ARKA KAPI

Yukarıdaki görselden de anlaşılacağı üzere, Türkiye'de yaşayan, 18-65+ yaş arasında olan, ailesinden uzak, ilişkisi olmayan, gece kulüplerinde takılan ve zengin olan üniversite öğrencilerini hedefleyen bir reklam verebilir ve bu reklamla 22 milyon kişiye ulaşabilirsiniz.

Sadece bununla kalmayıp kişinin beslenme alışkanlıklarına kadar özelleştirebildiğiniz bir satış yelpazesinin ürünüyüz. Bu veri ile kötü amaçlı insanların ne tür işler yapabileceğini hayal gücünüze bırakıyorum. (6)

İnterneti kullanırken arkamızda bıraktığımız ayak izlerimiz gerçek hayatta bıraktığımıza nazaran çok daha efektif bir şekilde işleniyor ve karşımıza çıkartılıyor. Kullandığımız sitelerde / uygulamalarda çalışmayı bekleyen ufak gözlemci kardeşlerin olduğu gerçeğini unutmamak, yaptığımız her hareketin bir göz tarafından izlendiğini es geçmemek gerek.

Hikayemizde kullanıcı olarak icraat anlamında elimizle bir veriyi sistemlere yazmadık. Yazıp vazgeçtiğimiz oldu fakat o formu göndermedik.

Sevgiler,

Kaynaklar:

https://tr.wikipedia.org/wiki/Exchangeable_image_file_format

https://github.com/KrauseFx/watch.user

https://www.sitepoint.com/html5-battery-status-api/

https://krausefx.github.io/user.activity/

https://www.youtube.com/watch?v=U0SOxb_Lfps

http://www.iha.com.tr/haber-reklamlar-ile-adim-adim-takip-ediliyoruz-703132/

Erhan ALTINDAŞ- erhan.altindas@btsis.com

Ubuntu Kurulumu ve Meraklısına Notlar

Ubuntu 17.10 Artful Aardvark Kurulumu

Ubuntu:
Son kullanıcının dilinden anlayan Linux dağıtımı

Linux bilindiği üzere çeşitli dağıtımlarla son kullanıcılar ile buluşmaktadır. Bu kullanıcılar bu dağıtımlar içerisinden kendi kullanım tarzlarına uygun olanı seçebilmekte ve bilgisayarlarına kurabilmektedirler.

Bu dağıtımlar arasında diğerlerine göre son kullanıcıya en çok yaklaşmayı başarmış dağıtımlardan biri de Ubuntu'dur. Ubuntu, bir Linux çekirdeği temel alınarak geliştirilmiş açık kaynak kodlu, özgür ve ücretsiz bir Linux dağıtımıdır. İnternetten indirilebilir ve bir medya (USB veya DVD) yardımıyla kolayca bilgisayara kurulabilir.

2004 yılında ilk sürümü yayınlanmış olan Ubuntu'nun her altı ayda bir yeni sürümü yayınlanır. Ubuntu kelimesi Zulu dilinde "insanlık" anlamına gelir.

Ubuntu ilk olarak; Linux ve özgür yazılımın bilgisayar kullanıcıları için bir seçenek sunması amacıyla Güney Afrikalı girişimci Mark Shuttleworth liderliğinde, bu amaç için kurduğu Canonical Ltd. firması bünyesinde 2004 yılında başlatılmıştır. Günümüzde yine Mark Shuttleworth yönetiminde Canonical ve gönüllü Ubuntu topluluğu tarafından geliştirilmektedir.

Genellikle en çok sorulan sorulardan biri "Ubuntu ücretli midir?". Buna net bir cevap vermek gerekirse "Hayır" denilebilir çünkü, Ubuntu hem ev hem de iş kullanımı için tamamen ücretsiz olarak indirilebilir ve kullanılabilir. Ubuntu'yu, herhangi bir lisans kısıtlaması olmaksızın dilediğiniz sayıda bilgisayara kurabilir ve kullanabilirsiniz. Buna ek olarak yayınlanan güncellemeler için ve sürüm yükseltmek için de hiçbir ücret ödemezsiniz.

İşin kaynağına bakıldığında Canonical Limited, Ubuntu'yu daima ücretsiz tutacağına dair söz vermektedir. Ayrıca Ubuntu bünyesinde geliştirilen kodlar GNU Genel Kamu Lisansı isimli bir özgür yazılım lisansı ile lisanslanmıştır.

Ubuntu sürümlerindeki en belirgin özellik bir LTS (Long Term Support) sürüme seçeneğine sahip olmasıdır. Normal şartlar altında hem masaüstü hem de sunucu tarafı için altı ayda bir sürüm yayınlanırken her yirmi dört ayda bir de LTS sürüm yayınlanır. LTS sürümlerinin en önemli özelliği beş yıl boyunca güncelleme sağlanırken normal sürümlere dokuz ay kadar güncelleme sağlanır.

Ubuntu'unun diğer sürümleri

- Kubuntu: KDE masaüstü ortamını kullanan türevi.
- Lubuntu: Düşük sistem kaynağı tüketen LXDE masaüstü ortamını kullanan türevi
- Xubuntu: Düşük sistem kaynağı tüketen Xfce masaüstü ortamını kullanan türevi.
- Ubuntu MATE: MATE masaüstü ortamını kullanan türevi.
- Ubuntu Budgie: GNOME üzerine Budgie kabuğunu kullanan türevi.
- Ubuntu Studio: Profesyonel video, ses ve grafik düzenleme işlerine yönelik hazırlanan türevi.
- Mythbuntu: MythTV yayınlarını Ubuntu ile birleştirmeyi amaçlayan türevi.

şeklinde sayılabilir.

Bir diğer merak konusu Ubuntu tarafına virüs bulaşıp bulaşmadığıdır. Zararlı yazılım güvenliği Ubuntu gibi tüm Linux tabanlı bir işletim sistemlerinin en güçlü yanlarından biridir. Zararlı yazılımların Unix ve Linux sistemlerin mimarisinden kaynaklanan nedenlere sistemler içinde yayılması ya da bir zarara neden olması bir hayli zordur, ancak imkânsız değildir. Teorik olarak mümkün gözüken bu duruma pratikte kapalı kaynak kodlu sistemlere nazaran hemen hemen hiç rastlanmamıştır.

Kaç tane Linux var?:

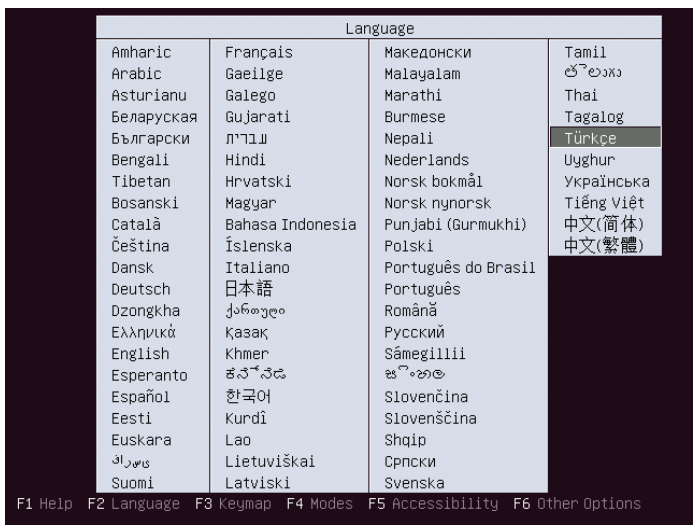
Bilinen Linux dağıtımlarını takip etmek için https://distrowatch.com/ adresini takip edebilirsiniz.

Ubuntu Kurulumu

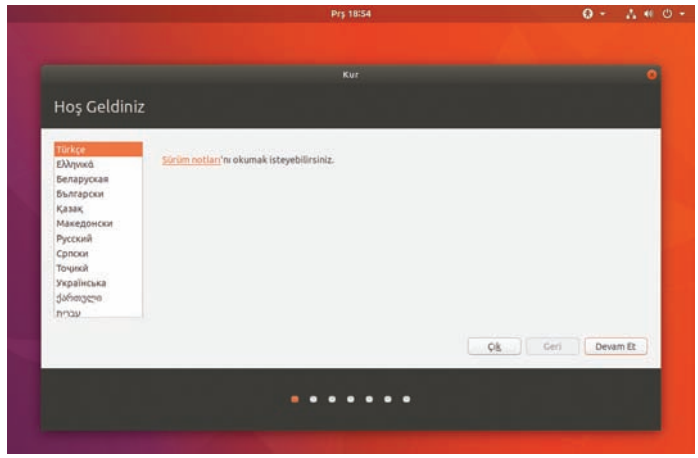
Ubuntu ilk kurulumda bu ekran ile sizi karşılar. Bu kısımda yapabileceğiniz diğer kurulum dışı işlemler

- Ubuntu'yu kurmadan denemek
- Sabit diski bozuk sektörler için denetlemek
- RAM adres bloklarındaki olası arızalara karşı denetlemek
- Hiçbir işlem yapmadan bilgisayarınızı açmak

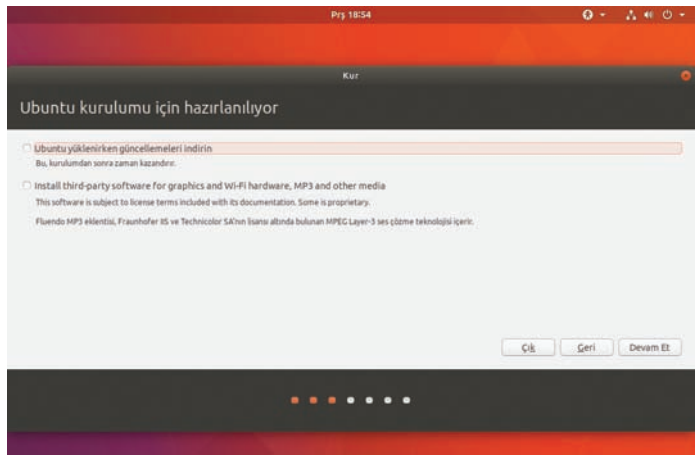
olarak sıralanabilir.



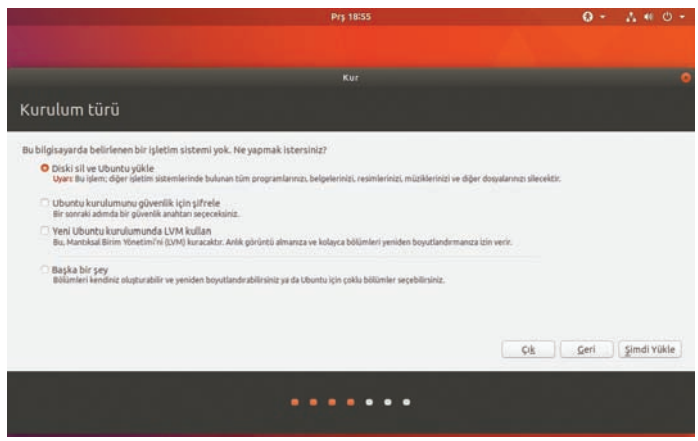
Biz bu ekran için klavyeden F2 düğmesine basarak Türkçe Dil seçeneğini işaretliyoruz.



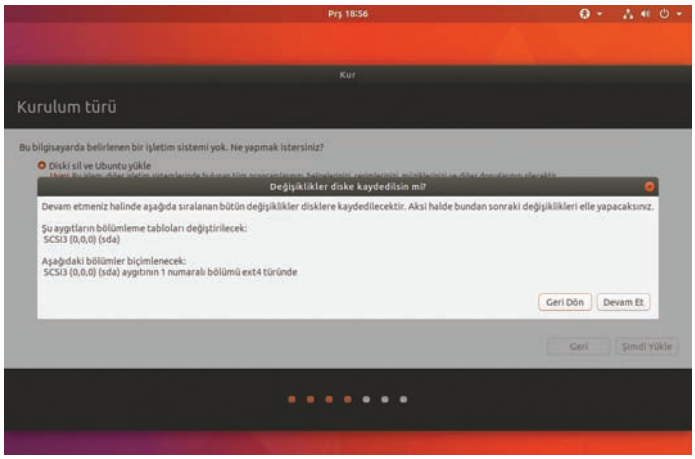
Otomatik olarak grafik ekrana geldiğimizde bizi kurulum başlangıç ekranı karşılar. Burada Türkçe dil seçeneği ile ilerlemek için "Devam Et" düğmesine basarak ilerliyoruz.



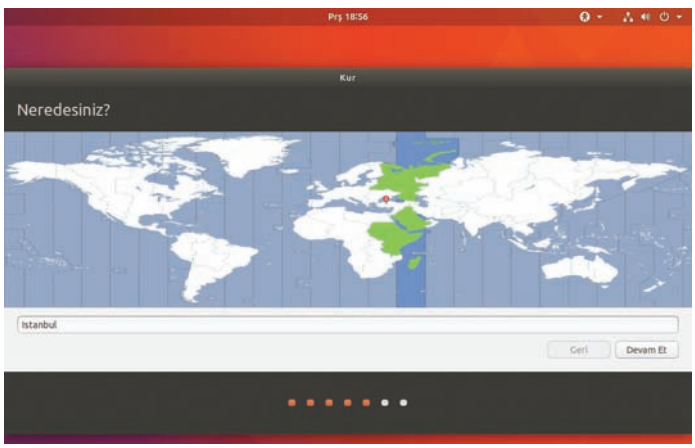
Bir sonraki ekranda güncellemeler ve üçüncü parti program desteklerinin kurulumda yükleyip yüklemeyeceğimiz sorulur. Bu yüklemeler için internet gereksinimi şarttır. Bunlar daha sonra da yüklenebilen parçalar olduğu için bu kısmı boş bırakarak devam ediyoruz.



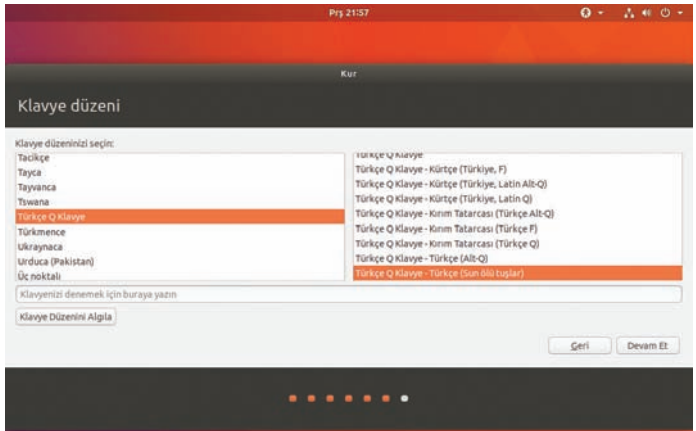
Bu bölümde disk bölümleme işlemleri yapılır. Eğer sistemimizde başka bir işletim sistemi daha kullanılacaksa "Başka bir şey" seçeneğinden gitmemiz gerekir. Örnek kurulumumuzda yalnızca Ubuntu yüklü bir bilgisayar üzerinden işlem yaptığımız için "Diski sil ve Ubuntu yükle" seçeneği ile ilerliyoruz.



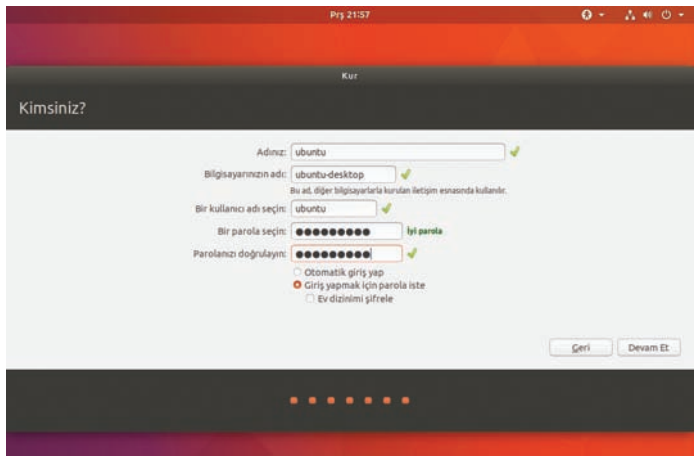
Bir sonraki ekranda Ubuntu bize yaptığımız disk bölümlendirme işlemini onaylamamızı isteyecektir. Bu onaydan sonra diskte yapılan bölümlendirme işlemleri geri alınamaz. Bu bakımdan emin olmamız gerekmektedir. Bu kısımda da emin olduktan sonra "Devam Et" düğmesine basarak ilerliyoruz.



Bu bölümde bulunduğumuz bölgeyi işaretliyoruz. Sistem saatimiz ve diğer yerel ayarlarımız buna göre ayarlanıyor. Türkiye'nin hangi ilinde olduğunuzun bir önemi olmadan doğrudan Türkiye'yi seçmeniz yeterlidir.

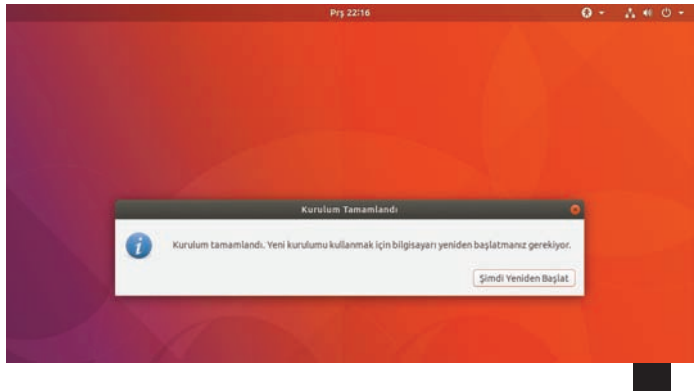


Klavye ayarlarını yaptığımız bu bölüm kullandığınız klavyeye göre farklılık gösterebilir. Biz "Türkçe Q" klavye düzeni içinde yer alan "Türkçe Q Klavye – Sun ölü Tuşlar" seçeneği ile ilerliyoruz.

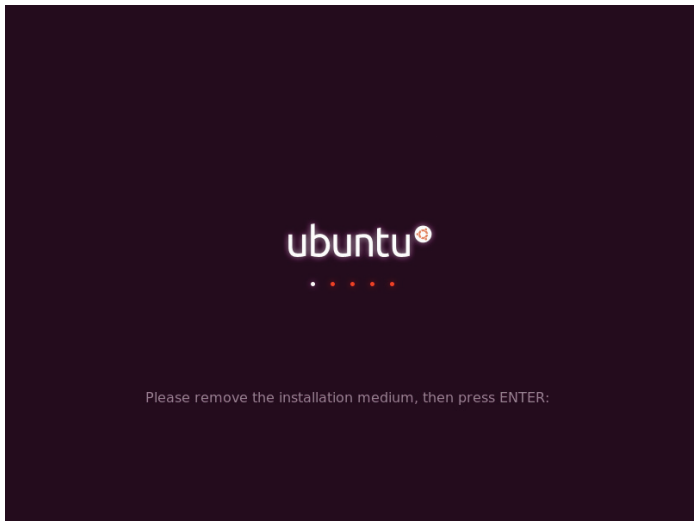


Bu kısımda bilgisayar adı, kullanıcı adı ve parola gibi bilgileri giriyoruz. Ayrıca tercih edildiği taktirde parolasız giriş seçeneği de kullanılabilir ancak bu seçenek sadece bilgisayarın ilk açılışı ile ilgili olup sistem ile ilgili işlemlerde (güncelleme, program kurulumu gibi) parolaya ihtiyaç duyulmaktadır. Bir diğer önemli seçenek ise isteğe bağlı Ev dizininin şifrelenmesi bu bölümde tercih edilebilir ancak bu seçenek ile sabit diskin başka bir Ubuntu sistemine ikincil olarak bağlanması halinde dosyalara doğrudan erişimin de mümkün olmayacağı unutulmamalıdır.

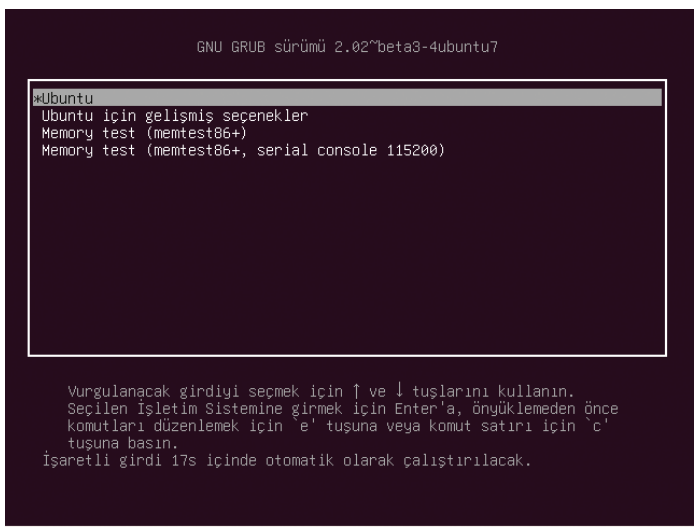
Bu işlemlerden sonra Ubuntu kurulumu başlar. Bu işlem bilgisayarın ve diskin hızına göre biraz zaman alabilir.



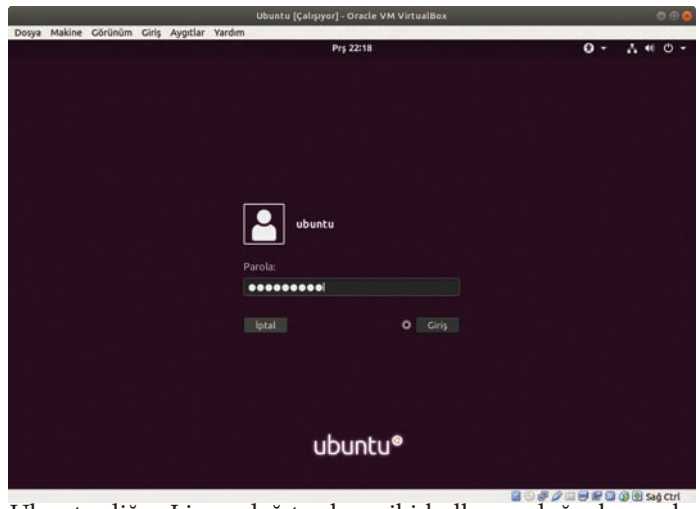
Kurulum işlemi tamamlandığında "Enter" düğmesine basarak sistemi yeniden başlatmamız gerekir.



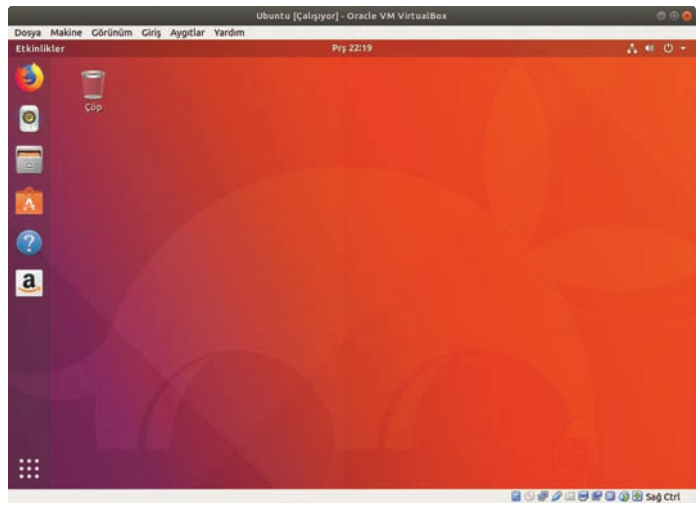
Bu işlemi yaparken USB'den kurulum yapılıyorsa USB diskin yerinden çıkarılması, DVD'den kurulum yapılıyor kurulum DVD'sinin sürücüsünden çıkarılması gerektiği unutulmamalıdır.



Ubuntu ilk açıldığında Grub ekranı gelir. Bu ekran daha çok birden fazla işletim sistemi bulunan sistemlerde istenilen işletim sisteminin seçilebilir.



Ubuntu diğer Linux dağıtımları gibi kullanıcı doğrulama ekranı ile bizi karşılar. Bu ekranda kullanıcı adı ve parolamızı girmemiz gerekir.



Kurulum ve doğrulama işlemi doğru bir şekilde tamamlandıktan sonra Ubuntu işletim sistemimiz kullanımımıza hazırdır.

Eskiden bu vardı; şimdi Linux'ta ne var?

Birebir aynı özellikleri bulunmasa da https://www.linuxalt.com/ adresinden kapalı kaynak kodlu sistemlerdeki uygulamaların Linux karşılıkları hakkında fikir edinilebilir.

Biraz da komut satırı

Komut satırı Linux tarafında pek çok işlemin yapılabildiği bir kullanıcı arabirimidir. Buradan sonra bahsedilenler yalnızca Ubuntu için değil ilgili paketlerin yüklü olduğu ve kendi paket yönetici sistemlerine göre yüklenebildiği ve kullanılabilen uygulamalardır

Stress: Sistemi biraz yoralım?

Bazen kullanıcılar sisteme yük bindirmek ve sistemlerinin ağır yük altındaki tepkilerini görmek isteyebilirler. Bu tip ihtiyaçlar için stress isimli komut bulunur. Yüklemek için

```
sudo apt-get install stress
```

komutu giriniz. Stres oldukça zengin parametrelere sahip bir komuttur. Basit ornek kullanım için dört çekirdekli bir işlemcinin 4 çekirdeğini yormak için

```
stress -c 4
```

komutunu veriniz. Siz Ctrl+C tuş kombinasyonuna basmadıkça işlemcideki 4 çekirdeğiniz en son noktada çalışacaktır.

Htop: Sistemi çok mu yorduk?

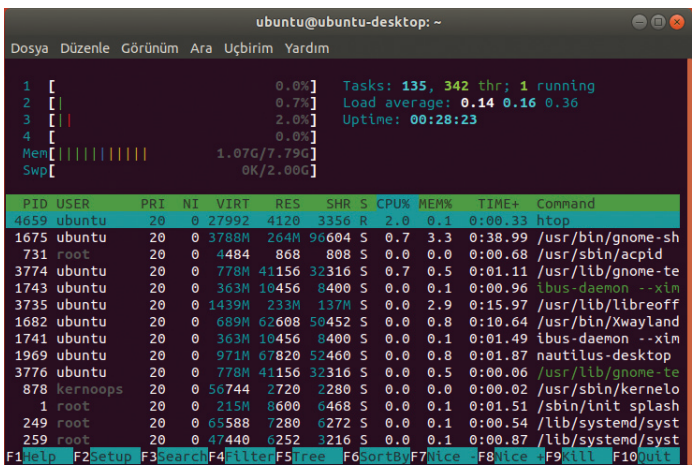
Kullanıcılar bazen sistemkaynaklarının ne kadar tüketildiğini görmek ya da kontrol etmek isterler. Htop uygulamasını kurmak için

```
sudo apt-get install htop
```

komutunu giriniz ve yükleme tamamlandıktan sonra

```
htop
```

komutu ile uygulamayı açabilir, Q düğmesi ile uygulamadan çıkabilirsiniz.



Bu komut ile kaç işlemci çekirdeği olduğu, bunlardan kaçının aktif olarak kullanıldığı, takas alanın ne kadarının kullanıldığını aktif olarak görebilirsiniz. Ayrıca sonlandırmak istediğiniz uygulamayı da ok tuşları ile belirleyip F9 a basarak sonlandırabilirsiniz.

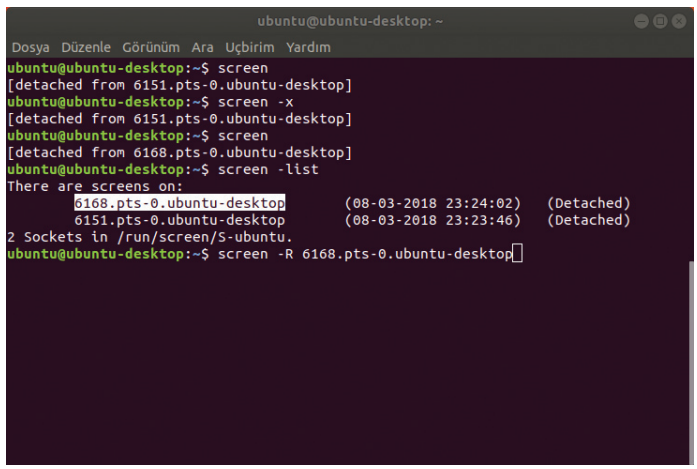
Screen: Biz yokken işimizi yapan biri

Linux kullanıcıları komut satırında uzun sürecek bir iş verdiklerinde genellikle komut ekranını *login* olarak açık bırakıp giderler. Ancak her ortamda bilgisayarın *login* ekranı açık bırakıp gitmek mümkün olmaz. Bunun açık olan *login* ekranını arka planda açarak kullanabilme seçeneği vardır. Bu işlem için

```
sudo apt-get install screen
```

komutu ile ilgili paketi yükleyebilirsiniz. Komut satırındayken

```
screen
```



komutu ile arka planda çalışacak terminal ekranına girersiniz. İşlemi başlattıktan sonra CTRL düğmesine basılı tutarak A ve D düğmelerine sırayla basar ve ana terminal ekranına düşersiniz. Bu ekranı kapatıp ya da logout olup çıksanız bile *screen* ekranı arkada işlemlerinizi yapmaya devam eder.

Tekrar bir önceki screen ekranına dönmek için

```
screen -x
```

Komutunu verebilirsiniz. Birden fazla screen ekranı acarsanız

```
screen -list
```

ile açık screen oturumlarının listesini alabilirsiniz. Bunlardan erişmek istediğinize almış olduğunuz liste bilgisinde olduğu ID bilgisi ile erişebilirisiniz örnek olarak

```
screen -R 6168.pts-0.ubuntu-desktop
```

gibi düşünülebilir ancak "6168.pts-0.ubuntu-desktop" gibi bir ID bilgisi sizin oturumunuza göre değişiklik gösterebilir.

Ccrypt: Dosyalarımızı şifreleyelim

Bazı kullanıcılar gerek bulundurdukları, gerekse internet yoluyla paylaştıkları dosyaları hatta klasörleri şifrelemek isterler. Bu tip durumlarda belki de en belirgin yöntem bir sıkıştırma yöntemi ile dosya şifrelemektir.

Linux depolarında oldukça başarılı bir dosya şifreleme paketi ile gelir. Bu program ile anahtar kelime parametresine göre

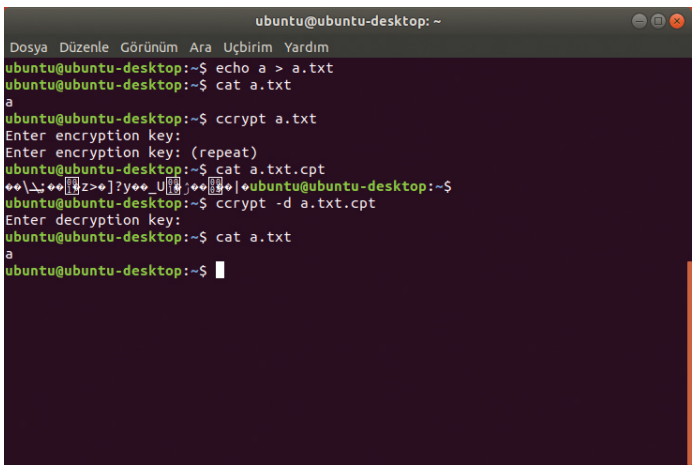
dosyaları şifreleyebilir ve tekrar açabilirsiniz. *Ccrypt* paketini yüklemek için

```
sudo apt-get install ccrypt
```

komutu veriniz. Örnek olarak içinde *a* harfi bulunan bir dosya oluşturup, *a* anahtar kelimesi işe şifrelemek ve çözmek için

```
echo a > a.txt
cat a.txt
ccrypt a.txt
(burada şifre olarak a harfini girin)
(burada şifre olarak a harfini tekrarlayın)
cat a.txt.cpt
ccrypt -d a.txt.cpt
(burada şifre olarak a harfini girin)
cat a.txt
```

adımlarını izleyebilirsiniz.



Bu tabi bir klasör içine girip * ile komutu verdiğinizde klasör içindeki tüm dosyaları bir komut işe şifreleyebilir ya da bir komut ile şifreleri çözebilirsiniz.

Secure Delete: Dosyalarınızı Güvenle Silebiliriz

Genellikle dosyalar disk uzerinden silinirken yalnızca isimleri silinir. Dosya sistemi üzerinde ismi silinen alanlar boş gözükür ve bu alanlara yeni dosyalar yazılır. Yeni dosya yazılma işlemi gerçekleşmediyse bu alanlardan veri kurtarılabilir.

Profesyonel dosya silme işlemleri genellikle dosyaların belirli bir metot ile parçalanarak disk yüzeyinde başka noktalara yazılması ve silinmesi ya da aynı yüzeye yazılarak silinmesi gibi şekillerde olabilir.

Linux tarafında güvenli bir dosya silme aracı bulunur. Unutulmamalıdır ki bu işlem dosya boyutu ve disk hızı ile orantılıdır. Kısacası dosya boyutu arttıkça işlem silme algoritmasının karışıklığı ile işlem süresi uzayabilir.

Bunun için birincisi komut satırı, ikincisi arayüz için iki paket kurulması gerekir.

```
sudo apt-get install secure-delete
```

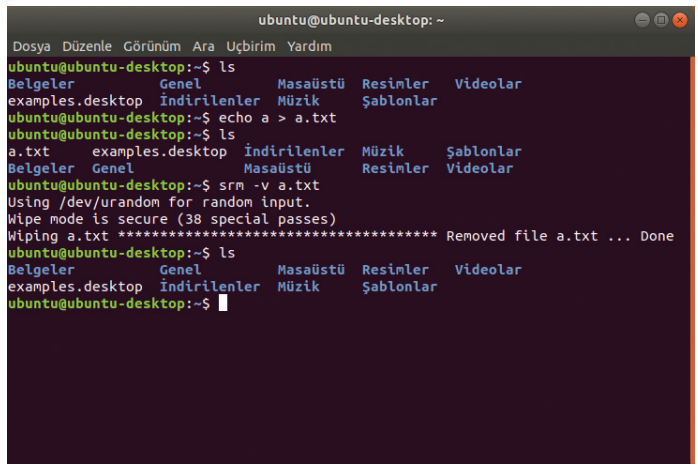
komutu ile ana dosya silme aracı kurulur. Grafik arayüzdeki kısa yol için

```
sudo apt-get install nautilus-wipe
```

grafik dosya yöneticisine de gerekli sağ tuş menüsü eklenir. Örnek olarak ismi a.txt olan bir dosyayı silmek için

```
srm -v a.txt
```

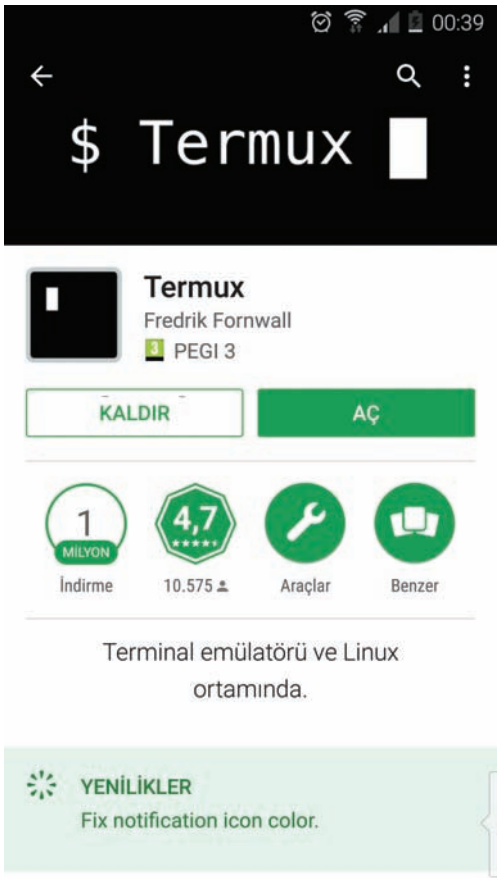
komutu verilebilir. Buradaki *-v* parametresi işlemi görsel olarak takip etmek ve hangi aşamada olduğunu belirlemek için kullanılan bir seçenektir.



Dosya yöneticisinde de istenilen bir dosya sağ tuş ile tıklanarak "*Wipe*" menüsünden silme işlemi çeşitli parametreler ile yapılabilir. Buna ek olarak kaynağı belli olmayan ikinci el bir sabit disk sahibi olduğunuzda bunu işletim sistemine bağlayıp "*Wipe available disk space*" yapmanız önerilir. Özellikle sizden önce nelerin yazılıp silindiğini bilmediğiniz bir sabit disk söz konusu ise normalde boş bile görünse, bir defa güvenli silme yöntemleri ile olası dataların üzerinden geçerek yok etmeniz önerilir.

Termux: Cep Telefonunuzdan Linux erişimi

Android telefonunuzdan Linux komut ekranına erişim seçeneğini sunan pek çok program bulunmaktadır. Android marketten yükleyebileceğiniz Termux uygulaması ile kolaylıkla IP uzerinden Linux bilgisayarınıza erişebilirsiniz.



Termux komut isteminin en önemli özelliği içinde hâlihazırda bulunmayan SSH istemcisi gibi komut setlerini, telefona kolaylıkla yüklemenize imkân sunmasıdır.

Bunun için herhangi bir root işlemi gerekmez. Sadece cep telefonu içindeki Termux programı içinden komutla yükleyebilirsiniz. Yapmak istediğiniz işleme göre Termux uygun komut setlerini otomatik olarak tavsiye etmektedir.

Buna ek olarak *screen* gibi işlemlerde gerekli tuş kombinasyonlarını varsayılan klavye ile uygulamak pek mümkün olmamaktadır. Bunun için Hacker's Keyboard seçeneği kullanılabilir. F düğmeleri ve yatay modda gelen ok düğmeleri ile komut geri çağırma gibi özellikleri ile oldukça pratik bir uygulamadır.

Siber Güvenlik Sektörü Hacktrick ‘18 ile BTK’da Buluşuyor!

Hacktrick 18; Octosec - BTK işbirliği ile düzenlenen Siber Güvenlik Konferansıdır. Octosec ekibi, 2014 yılında Ankara Üniversitesi ev sahipliğinde “Üniversiteler Arası Siber Güvenlik Zirvesi” sloganıyla başladığı Hacktrick Siber Güvenlik Konferansı ile, siber güvenlik sektöründe önde gelen isimleri, kurumları ve şirketleri sektör ile buluşturmayı hedeflemektedir. Geçmiş yıllarda Ankara Üniversitesi, Sabancı Üniversitesi, Anadolu Üniversitesi ve BTK ev sahipliğinde düzenlenen Hacktrick, binlerce kişinin katılımıyla özel sektörün, devlet kurumlarının ve üniversitelerin siber güvenlik çerçevesinde buluşmasını sağlamaktadır. Hacktrick 2018’i zeka, eğlence, heyecan ve biraz da mücadele ortamı oluşturan bir hack festivali olarak tanımlayan ekip, pratik ve teorik güvenlik çalışmalarını katılımcılarla paylaşmak üzere organize edilmiş bir etkinliktir. İlgililere faydalı eğitimler, teknik sunumlar ve birbirinden eğlenceli yarışmalarla, bilgi dolu ve eğlenceli zaman geçirmeyi hedeflemektedir. BTK’nın destekleriyle Octosec ekibi tarafından bu sene 5.sini düzenlenecek olan Hacktrick ‘18 etkinliği geçen yıllarda olduğu gibi yine katlanan bir ilgiyle karşılaştı. Gönüllülük esaslı olan etkinlikte bu sene eğitmen başvuruları da dışarıya açılmasıyla birlikte 40’tan fazla gönüllü kişiden eğitmenlik başvurusu geldi. Blockchain, Web Uygulama Güvenliği, Ağ Güvenliği, Siber İstihbarat, Ters Kod Mühendisliği, Adli Bilişim gibi birbirinden değerli konuların bulunduğu 20’den fazla eğitim sınıfı ve yaklaşık 1000 kontenjan ile birçok kişi eğitim alarak kendini hem teknik hem de sosyal anlamda geliştirme fırsatı bulacak.

Etkinliğin ilk gününde katılımcılar Konferanslara katılarak güncel konularla ilgili alanında uzman kişiler tarafından hazırlanan sunumları dinleyebilecek. Bunun yanı sıra Demo Roomlar sayesinde kendi ürünlerini geliştiren kişilerin ürünlerini yakından inceleyebilecekler. Etkinliğin ikinci günü Eğitimlere başlanacak olup aynı anda Game of Pwners bayrağı yakala(CTF) yarışması başlayacak. Game Of Pwners yarışmasında beyaz şapkalı hackerlar yarışacaklar. 4’er kişilik takımlardan olaşacak ekiplerden birinci olan takımın her bir üyesi Macbook Pro kazanma şansı elde edecek. Etkinliğin üçüncü gününde ise devam eden eğitimlerin yanı sıra Bug Miner Ödül avcılığı programında beyaz şapkalı hackerlar, önlerine gelen sistemler üzerinde zafiyet arayarak ödüller kazanmaya çalışacak.

Hacktrick Siber Güvenlik Konferansı 2018 yılı itibariyle Siber Güvenlik Ödüllerini organize ediyor. Belirlenen 10 farklı kategoride, sektörün önde gelen isimlerinin yer aldığı 50+ kişilik jürinin adayları oylaması sonucu, ödüller sahibini buluyor olacak. Hacktrick ekibi tarafından 2018 yılı için belirlenen ödül kategorileri aşağıda belirtilmiştir ve tüm kategoriler siber güvenlik alanı için özelleştirilecektir.

- Yılın En Başarılı Şirketi
- Yılın En Başarılı Ar-Ge Şirketi
- Yılın En Başarılı Yerli Yazılımı
- Yılın En Başarılı Üniversite Kulübü
- Yılın En Başarılı Akademik Personeli
- Yılın En Başarılı Akademik Araştırması
- Yılın En Başarılı Araştırmacısı
- Yılın Gelecek Vaad Eden Genç Araştırmacı Ödülü
- Yılın En Başarılı Blogu
- Yılın En Başarılı Bloggerı

Peki bu etkinliği düzenleyen Octosec kimdir? Nedir?
Octosec ekibi firmalardan tamamen bağımsız, hiçbir şekilde ticari ve kâr amacı gütmeyen, ülkemize, bu alanda çalışmak isteyen ülkemizin gençlerine ve güvenlik sektörüne hizmet etmeyi hedef edinmiş bir ekiptir. Ülkemizdeki bilgi güvenliği farkındalığını arttırmak en temel hedef olup bu doğrultuda çeşitli etkinlikler düzenlemektedir. Hacktrick Siber Güvenlik Konferansı ve HackerKamp, Octosec ekibinin düzenlediği, en çok bilinen, takip edilen ve ilgi odağı haline gelmiş etkinliklerdir. Detaylı bilgi için octosec.net adresini ziyaret edebilirsiniz.

Etkinlik Programı

4 Mayıs 2018

Konferanslar/Sunumlar, Demo Odası Sunumları

5 Mayıs 2018

Eğitimler - 1. gün, Game of Pwners Offline CTF

6 Mayıs 2018

Eğitimler - 2. gün BugMiner Ödül Avcılığı Programı

TA1IHE Murat KAYGISIZ - ta1ihe@arkakapidergi.com*

Nedir Bu Amatör Telsizcilik Dedikleri?

Yayın hayatına yeni başlamış olan dergimizde, öncelikle tüm emeği geçenlere bu hobinin tanıtımı üzerine bir yayın alanı ayırdıkları için sonsuz teşekkürlerimi sunuyorum. İlk sayıda yer alan bu bölümde, hobimize ait genel bilgilendirmeler için emek veren Erhan Altındaş arkadaşımıza da ayrıca teşekkürler etmek isterim. Bu sayıdan itibaren artık sizlere bu hobi hakkında detaylı bilgiler vermeye ve her şeyden önce bu hobinin ülkemizde yeterince anlaşılabilmesi hususuna dikkat çekmeye çalışacağım.

Bu sahada yaklaşık beş yıllık geçmişe sahip, amatör telsiz operatörü olma yolunda ilerlemeye çaba gösteren biri olarak, yazıda irdelemek üzere -Telsiz haberleşmesi nedir, telsiz haberleşmesine neden ihtiyaç duyulur ve neler yapılabilir?- gibi konu başlıkları belirledim.

Temeline inildiğinde, tanımı içerisinde bulunan ve üzerinde oldukça detaylı düşünülmesi gereken "AMATÖR" kelimesi, bu uğraşın tamamen gönülden ve aşk ile ilgi duyulan, hiçbir maddi kazanç düşünülmeyen ve aynı zamanda AR-GE bakışından ödün vermeyerek ilerletilmesi gereken bir elektronik altyapı ve aynı oranda elektronik bilgisi gerektiren bir hobi olduğunu ifade etmektedir. Bu uğraş içerisinde aynı zamanda yasaların da Amatör Telsiz Haberleşmesi ile şart koştuğu, kamuya yararlı olma ve gerekli hallerde yetişmiş haberleşme uzmanı personeli değerinde yardım etme zorunluluğu da yer almaktadır.

"Amatör Telsiz Operatörü" ehliyetine sahip olmayı isteyen her birey öncelikle tüm bunlardan sorumlu olacağını unutmamalıdır. İcrası için pek çok hobi dalında mecburiyet teşkil etmeyen yukarıdaki hususlara ilaveten, olmazsa olmaz olarak nitelendirebileceğimiz insan hayatına ve tüm canlı hayatına karşı yaşam desteği verecek gönül birliğine ve hissiyatına sahip olmak da bu hobiyi değerli kılan unsurlardır.

TELSİZ HABERLEŞMESİ NEDİR?

Günümüzde teknolojik gelişmeler, insanoğlunun sonsuz taleplerine cevap vermeye uğraşmaktadır. Neredeyse hepimiz her isteğimize en hızlı cevap verebilecek teknolojik cihazlar peşindeyiz. Her seferinde de temel isteğimiz, bu teknolojik cihazların bizim hızımıza yetişecek kapasitede çalışmalarını beklemek. Buraya kadar esasen pek de büyük bir yanlış içinde olduğumuz söylenemez. Tabii ki teknoloji ile uyumlu bir hayat sürmek zorundayız. Yaşadığımız bu sürat çağı içerisinde isteğimiz, geri gelmeyeceğini bildiğimiz zamandan olabildiğince tasarruf etmek!

Şimdi tüm bu doğrular içerisinde kendimize şunu soralım isterim; bu hızlı tempo içerisinde olmazsa olmazlarımız nelerdir? Cevap olarak iletişim desem herhalde itiraz eden olmayacaktır. Araç kullanırken, yolda yürürken, yemekte, sohbette vb. durumların neredeyse hepsinde artık hayatımız sadece bir değil, birçok toplumsal iletişim ile paralel yürümek zorunda.

Dikkat çekmek istediğim nokta ise tüm bunların temelinde yer alan elektronik altyapı veya diğer bir dille, servis sağlayıcı yapılarıdır. Her birimiz altyapı üzerinde yer alırız ve altyapı içeriğinde olabilecek bir kopma veya benzeri bir sorun geliştiği anda tüm bunların tamamını, çözümlenme sürecini dahi bilemeyeceğimiz bir anda kaybetme riski ile karşı karşıyayızdır. İşte bu noktada şu ayrımı yapmak gerek: ihtiyacımız olan şey esasında, her koşulda iletişim kurabilmek!

İşte tam bu noktada o çok güvendiğimiz internet altyapılı sistemler ve aracı yapılar bir anda ortadan yok olmakta ve bizler kullanıcı olarak maalesef isteklerimize cevap alamaz duruma düşme riski ile karşı karşıya kalmaktayız. Telsiz haberleşmesi konusuna baktığımızda ise karşımıza, herhangi bir altyapı ihtiyacının zaruri olmadığı, gerektiğinde çok hızlı şekilde oluşturulabilecek ve her koşulda iletişim sağlayabilecek bir yapı çıkmaktadır. Telsiz haberleşmesi adından da belli olduğu gibi kablo veya uydu gerektirmeden, radyo frekansları aracılığı ile bu irtibatın sağlanabildiği bir iletişim şeklidir. Yine bu iletişim şekli yukarıda özetlediğimiz tüm teknolojik altyapılar ile koordine olabilen, mevcut ise internet aracılığı ile de birçok geliştirici faktörü beraberinde taşıyabilen, en iyi ve en garantili iletişim yolu olmuş bir tekniktir. Teknoloji ile bütünleşmiş, hiçbir servis sağlayıcı gereksinimi duymayan, mesafe sınırı tanımayan, **gerektiğinde data haberleşmesinde dahi çok rahat kullanılabilen bir iletişim yoludur.**

TELSİZ HABERLEŞMESİNE NEDEN İHTİYAÇ DUYULUR?

Neden ihtiyaç duyulur sorusu esasen yukarıda da ifade edilmesine karşın, bu konuya birkaç hayati ilavelerde bulunmak

* TAMAD Tüm Telsiz Amatörleri Derneği Başkanı

gerekir. Şimdi hepimiz kendimize şu soruyu yöneltsek cevabımız ne olurdu merak etmekteyim, "beklenmeyen ve olağandışı anlarda öncelikle kim veya kimlerle irtibat kurmak isteriz?"

Burada cevap neredeyse hepimiz için "Aile" ve sonrasında "Dostlar"dır. Hâl böyle iken bu senaryo üzerinde hızlıca bir düşünelim ve detaylandıralım ister misiniz? Küçük bir senaryo ile bunca teknoloji altında konforlu bir yaşam sürerken ne kadar çaresiz kalabileceğimiz gerçeğini görelim isterim.

Rutin bir günde, iş yerindesiniz. Eşiniz çalışmıyor ve kendisi de arkadaşları ile alışveriş yapacağını size iletiyor ve hatta arada size internet altyapısı kullanan, yakın zamanda, kadınlar gününde kendisine hediye ettiğiniz son model akıllı telefonu ile AVM veya mağazalarda ya da bir fast-food restoranından çekildiği fotoğrafları sizinle paylaşıyor. Çocuğunuz veya çocuklarınız okulda dersteler ve o kadar ince hesaplanmış ki çocuklarınızın konum bilgilerini size iletmesi için onların da akıllı telefonlarında veya bileklerindeki SIM kart ile çalışan konum bilgisi atan cihazlar düşünülmüş. Çocuklarınızı bu cihazlar aracılığı ile sürekli takip etmektesiniz. Buraya kadar aile iletişim ve güvenliğiniz için gerekli her türlü tedbiri almanın rahatlığı içerisindesiniz, tebrikler! Amatör telsiz operatörü olan ve bu hobiyi gereği gibi icra etme yolunda uğraş gösteren biri dışında buraya kadar her şey mükemmel.

Tam da bu anda birdenbire bir yer sarsıntısı yaşanmaya başlar, yaklaşık on beş saniye süren bu sarsıntı sonucu nedendir bilinmez ama GSM altyapıları duruverir. Aksilik bu ya elektrik kesintisi de başlar ve o en güvendiğimiz iletişim olan internet altyapısı da yok oluverir. Bir anda ne eşinize ne çocuklarınıza ulaşamaz hale gelirsiniz. Sarsıntı bulunduğunuz yerde sorunsuz ve kayıpsız atlatılmış olsa dahi ilk iş akıllı telefonunuza sarılmak olacak ama "Şebeke bulunamadı" cevabı veya "bağlantı hatası" mesajı alacaksınız. Eşiniz ne durumda, çocuklarınız nerede ve nasıl soruları maalesef içinizi kemirecek ve onlara ulaşmak için en son baktığınızda çocuklarınızın yaklaşık 3 dakika önce veya en iyi ihtimalle 30 saniye önce nerede olduğunu belki görme imkânınız olacak.

Sevdiklerinizin sesini duymak, sonrasında dışarıya çıkarak onlara ulaşmak isteyeceksiniz. Genel durum nedir, yollar açık mı, araçla ulaşabilecek misiniz, hasar var mı, kendilerine hangi yoldan gidersem daha çabuk ulaşırım gibi birçok cevapsız soru ile baş başa kalmış bir toplumun bir bireyi olduğunuzu anlamanız oldukça kısa sürecek size garanti veririm! İşte tam da bu durumda dahi tüm yukarıdaki cevap alamadıklarınız için hiçbir şebeke ve altyapı desteğine ihtiyaç duymayan telsiz haberleşmesi en güzel yardımcınız olacaktır. Böylesi anlarda kesintisiz çalışan tek haberleşme sistemi, bizlere nasıl destek olmuş gerçek görüntülerle görmek isterseniz, hazır şu an çalışırken teknolojik desteğimiz olan YouTube üzerinde afet anlarında telsiz haberleşmesine dair videoları seyretme şansınızı değerlendirin derim.

NELER YAPILABİLİR?

Her koşulda kesintisiz iletişim için telsiz operatörleri sizlere cevap vermeye her an hazır beklemektedir. Telsiz sistemleri ve yapıları bazılarınızın tahminlerinden çok daha fazlasını sunabilmektedir. Bu tip bir durumda bilmelisiniz ki amatör telsiz haberleşmesi içerisinde doğru ve bilinçli yapılanmış, gereken teknik bilgiye sahip birçok kişi siz o dakikaları çaresizce yaşarken, çoktan görevlerine başlamış ve irtibatın kesildiği, ihtiyaç duyulan noktaların neredeyse tamamında, belki de bir arama kurtarma ekibi yanında, belki bir kayıp çocuk arayışında yardıma başlamak için evinden ve ailesinden yanlarına gitmeye bile gerek kalmadan gayet iyi durumda olduklarını öğrenmiş, kendileri ile çoktan ilk bir iki dakika içinde bilgi almış, sizlere ve kamu kurumlarına yardım için yola çıkmış olacaklardır. Bir kıtadan diğer kıtalara, ülkelerden başka ülkelere, hatta bunlar yetmezmiş gibi uzaydaki astronotlara, bazen de bir sokaktan diğerine, topluluklara aynı anda veya bireysel şekilde, bilgi almış ve aktarmış, acil içerikli yazılım dosyalarını gereken yerlere data olarak göndermiş veya almış, olay yerlerinden fotoğrafları aynı şekli ile almış veya göndermiş ama işin en ilginç yanı tüm bunları, bağlantı hatası mesajı almadan, oldukça güvenli olabilen radyo frekansları ile bir tel parçası veya benzeri ufacık bir anten ile havadan sinyaller ile başarmış olurlar.

Burada önemle şunu belirtmek isterim ki, burada verdiğimiz örnekleme acil durum içerikli bir örneklemedir ancak bu demek değildir ki amatör telsiz kullanmak sadece "Afet Haberleşmesi" anında gereklidir! Bu sadece ve sadece hayatımızın en önemli anlarında, neden bizlerin sürekli telsiz cihazlarımızı yanımızda, aracımızda, evimizde sürekli faal tuttuğumuzun en iyi anlaşılabilir şekli olduğuna bir vurgu için örneklenmiştir.

Yeri geldiğinde av veya tırmanışta, kampta, kayakta, yolda, canınız sıkıldığında, sohbete bir dost aradığınız anlarda, düğün doğum vb. keyifli anları paylaştığınızda, acil kan ihtiyacı olduğunda, ülkeler arası yarışmalara katıldığınızda ve benzeri inanılmaz keyifli etkinlikler içerisinde de bu hobinin hayatınıza neler neler katabileceğini bilmenizi, öğrenmenizi ve lezzetini yaşamanızı isterim!

Tüm bunlar nasıl yapılır sorularının cevapları ve gereken bilgileri ilerideki yazılarımızda paylaşmak dileklerimizle. Keyifli ve iletişim garantili günler dilerim. Değerli katkılarından ötürü TA1LKK Kemal KULA, TA1OEE Emrah ECİROĞLU ve TA1MHP HAKAN ŞAKRAK kardeşlerime de teşekkürler ile ilk yazımızı sonlandırmak istiyorum. 73! (Bu rakamın anlamını yakında yazacağım.)

Esra Serttaş - esraserttas93@gmail.com

KUANTUM BİLGİSAYAR

Nedir bu kuantum? Son zamanlarda her şeyin başına bir 'kuantum' getirip durdular. Kuantum yoga, kuantum terapi, kuantum yaşam koçluğu… Ne kadar da entelektüel duruyor değil mi? Ama ne demek bu kuantum? Bir eylemin başına kuantum getirince neden merak uyandırıyor? Bilim neden kuantumla ilgileniyor? Çünkü kuantum, klasiklere karşı! Ezber bozuyor… Bize getirileri ne, bizden götürdükleri ne? Nasıl keşfedildi? Bilgisayar bilimiyle nasıl bağlantı kuruldu? Egemenlik alanı nereler? Kuantumun ötesi var mı? Kuantum kontrol edilebilir mi? Peki, kuantum bir sistemse bunu yapan kuantum kriptografiyi de yaptı mı? Sağlık, eğitim, savunma, ekonomi daha birçok alanda güçlü reformlara imza atacak olan kuantum bilgisayarlar; bakalım, nasıl doğmuş, nasıl gelişiyor?

Kuantum Fizik Nedir?

Kısaca; klasik fiziğin yetersiz kaldığı yerde devreye giren fizik, kuantum fiziğidir.

Daha uzun olan kısaca; 19. yüzyıl sonlarına doğru klasik fiziğin tüm fiziksel olayları açıklayacağını inanılırdı. Mekanik olaylar 'Newton Yasaları'ndan, elektrik ve optik olaylar Maxwell Denkleminden sorulurdu. Termodinamik olayları da çiçeği burnunda İstatistik Mekanik Teorisi açıklayabiliyordu.

Derken; ışığın tane özelliği, şu meşhur; siyah cismin yansıması, fotoelektrik olayı, hareketli maddenin dalga özelliği, Compton saçılması ve elektron kırınımı, atomların kesikli enerji dağılımı gibi yapılan bir dizi deneye klasik fizik artık yanıt vermiyordu.

1900-1927 yılları arasında süren bir arayışın sonunda 'KUANTUM TEORİSİ' denen madde ve enerjinin temel birimlerini ele alan mikroskobik sistemleri (atom, çekirdek vs.) matematiksel nesnelerle tanımlayan ve matematiksel nesneleri fiziksel içeriğe dönüştüren bir dizi kuralları olan bilimsel yöntem doğdu.

Fizik ve Bilgisayar Bağlantısı Nedir?

Aslında bu konuyu iki alt başlıkta incelemek daha verimli olacaktır.

Fiziksel Bağlantı: Tek kelime ile iletkenliktir. Bu konu donanım bilgisi gerektirdiği için donanımcı arkadaşlara karşı hadsizlikte bulunmak istemem.

Bilimsel Bağlantı: Bu alt başlığı açıklarken de öncelikli olarak bilimler arası bağlantıdan söz etmek gerekir.

Carl Friedrich Gauss'un 'Bilimlerin Kraliçesi' diye adlandırdığı matematik; magmadan çıkın uzaya gidene kadar aklın ve mantığın erişebileceği hatta erişemeyeceği her şeyin temel aracıdır. Matematiğin 'fizik' bulmuş hali ise fizik bilimidir. Esasında bu bir kısır döngüdür. Matematik-fizik, fizik-matematik. Matematik; fiziğin izahını basitleştirirken, fizik, matematiğin ispatıdır. Bu iki bilim dalını birbirinden ayırmak 'Newton'a büyük haksızlık olur. Çünkü ilk kez fiziksel olaylara bir anlatım getirmek için diferansiyel hesabı Newton kullanmıştır ve Newton mekaniği incelenirken integral hesabı kullanılır.

Matematik, fizik, kimya gibi bilimler teorik alt yapıyı oluştururken mühendislik bu alt yapının pratiğe dönüştürülmesidir.

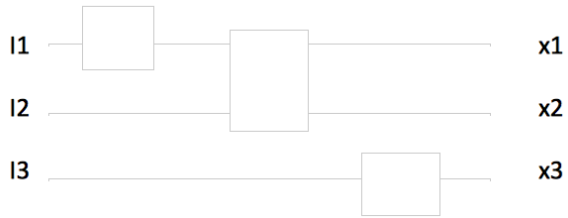
Ne demiştik? Matematiğin fizik bulmuş hali fiziktir ve bu bir kısır döngüdür, öyleyse; bilgisayar bilimi de matematik- fizik ikilisinin tasarlanmış halidir.

Kuantum Bilgisayar Nedir?

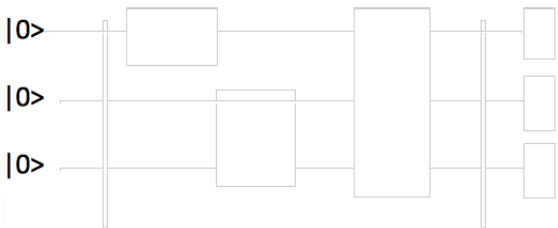
Kısaca; klasik bilgisayardan daha zeki, daha hızlı ve daha karmaşıktır. Klasik bilgisayarlar tüm verilerde '0' ve'1' değerini alan klasik bitleri kullanırken; kuantum bilgisayarlarda q-bitleri (kuantum bitleri) kullanılır. Bu da şu demek oluyor; yani, kuantum bilgisayarlar aynı anda hem '0' hem '1' değerini alabiliyor. Kuantum bilgisayarlar işlem gücünü bu q-bitlerden alır. Foton, atom çekirdeği, elektron fiziksel nesneler q-bit olarak kullanılabilir.

Kuantum bilgisayarların gücünden bahsetmek için şunu söyleyebiliriz; 128 q-bitlik bir kuantum bilgisayar mevcut en yüksek işlemciye sahip klasik bilgisayardan daha hızlı işlem yapabiliyor. Elektroniğin teorik sınırı keskin bir biçimde tanımlanamaz; çünkü başka bir unsur daha vardır. Atomik seviyede, işlemler kuantum mekaniğinin dinamik kurallarını takip eder. Bu, çeşitli komplikasyonlarla sonuçlanır. Örneğin; elektronlar aşmaları beklenmeyen bariyerleri aşarak daha düzensizce hareket eder. Öte yandan, kuantum mekaniği çok özeldir ve belki de bu komplikasyonlardan faydalanabileceğiz. Tek ve aynı bilgisayar öğesi tarafından sınırlı sayıda hesaplamanın aynı anda gerçekleştirilebileceği 'kuantum bilgisayar' teorik olarak artık yapılıyor. Kuantum bilgisayar artık aramıza katıldığında karmaşık teknik argümanlar olmaksızın da gösterilebilir. Belki, kuantum

bilgisayarlar, denklem olarak hesaplanması son derece zor durumlar yaratabilir. Nitekim bu durumu tersine çevirerek işimize yarar hale getirebiliriz ki terslenebilir hesaplama yöntemiyle bu başarılmıştır. Terslenebilir hesaplama yöntemi kullanılarak karmaşık kuantum işleminin ilk hali olarak tanımlanan bir düzenleme oluşturarak, bu işlemlerinin denklemlerini oluşturabiliriz ve denklemin, gerçekleştirmek istediğimiz karmaşık hesaplamaya denk düşeceği şekilde bir düzenleme seçebiliriz. Böylelikle doğa, minimum enerji kaybıyla, istediğimiz hesaplamayı büyük bir hızla gerçekleştirecektir.



Şekilde; klasik bilgisayar için devre diyagramını göstermeye çalıştım. Yatay çizgiler bitleri taşıyan kablolardır. Soldan sağa doğru, soldan I1,I2,I3 girdi bitleri ve çıktı bitleri x1,x2,x3 sağdan okunur.



$|\psi_i> = |0>|0>|0>$ $|\psi_F>$

Bu şekilde de bir kuantum devre diyagramını göstermeye çalıştım. |0>|0>|0> q-bitler devreye soldan girer. D1,D2,D3 ise q-bitlere uygulanan kuantum kapıları olarak düşünelim. Devrenin en sağındaki küçük üçgenler, devrenin çıktısını elde etmek için son durumdaki q-bitlerin her birinin hesaplama bazlarında ölçüldüğünü gösterir.

Kuantum Bilgisayar Nasıl Doğmuştur?

Richardo P. Feynman, California Teknoloji Enstitüsü'ndeki Amerikan Fizik Derneği'ne "Aşağıda Daha Çok Şey Var" başlıklı bir konferans vermiştir. Bana göre; kuantum bilgisayarın doğuşu o konferanstır. Çünkü Feynman yan yana bir kaç atomu ölçerek bellek hücreleri üretirsek muazzam miktarda bilgi depolayabileceğimizi düşünmüş hatta daha da ileri giderek maddeyi atomların temelinde kontrol edebilseydik neler olabileceğini hayal etmiştir.

Atom başına birden fazla bellek öğesi! Düşünsenize mucizeyi! Ama ne yazık ki elektronik hâlâ teorik limitine katiyen ulaşamamıştır.

Kuantum bilgisayarın işleyiş şeklinden bahsedelim. Q-bitler de klasik bitler gibi "0" ve "1" den oluşur. Lakin süperpozisyon dediğimiz olayla q-bitler "0" ve "1"i birleştirerek değer elde eder ve aynı anda bütün hallere girebilir. $|0> + |1> /\sqrt{2}$. Çünkü kuantum hesaplama paralel bir yapıya sahiptir yani sistemin tüm durumlarını değiştiremez.

Kuramsal fizikçi Feynman'ın kuramını teorik açıdan ele alan teorik fizikçi David Deutsch; bir şema oluşturdu. Bir q-bit topluluğu aldı ve ilk parametrelerini kaydetti, gerekli dönüşümleri mantıksal işlemlerle gerçekleştirdi. Q-bitler burada iletimi mantıksal, bloklar ise dönüşümü başardı. Yani, kuantum seviyesinde hesaplama yapabilen bir zincir oluşturdu.

Genel Kuantum İşlemleri

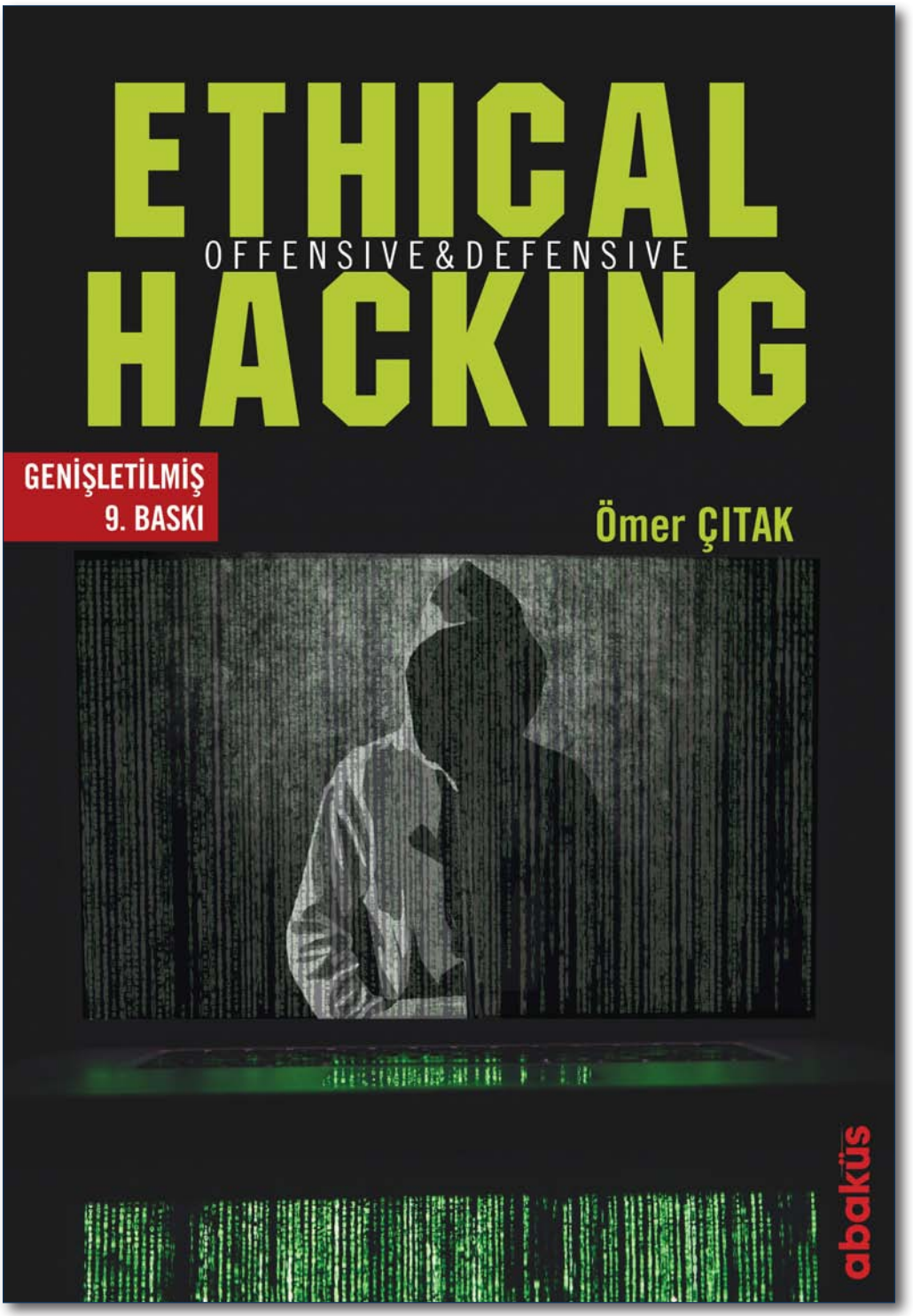
Kuantum bilgisayarların standart formülüzasyonuna doğrudan geçiş sağlamak için vektörler ve matrisler kullanılır. Kuantum bilgi, kuantum çatısında bilgi teorisinin yeniden formüle edilmesinin bir sonucudur.

Sonlu boyutlu kompleks Hilbert uzayındaki bir vektör ile tanımlı durumun serbestlik derecelerini kuantum hesaplamanın gerçekçi modellerini tanımlamak için kullanacağız. Klasik bilgi işlemede de olduğu gibi kuantum bilgi işlemede de fiziksel modellemeyi gerçekleştirmek için sonsuz boyutlu durum uzayları da kullanılabilir. İki seviyeli sistemlerinin birleşmesinde meydana gelen birleşik sistemleri iki boyutlu Hilbert uzayındaki vektörlerle tanıtacağız. İki boyutlu Hilbert uzayı için baz kümesi seçmek gerekir. Bu bazlar |0> ve |1>'den oluşur. Klasik bilgisayarlar için bu iki seviyeli sistem bir kablo üzerindeki voltaj seviyesi olabilir. Voltaj seviyesi sıfır olabileceği gibi +5mV gibi pozitif değer de olabilir. Kablodaki voltajın sıfır olma durumu klasik bit de '0' , +5mV olması da '1' olarak kodlanabilir. Bu noktada bir q-bitin durumunu gösteren { |0> , |1> } bazlarına hesaplama bazları denir. Hilbert uzayı için uygun bazlar foton yokluğundaki durum için birim vektörden, foton varlığındaki durum için dik vektörden oluşur. Genel durumun ise birim vektör ile tanımlanması $|\alpha 0|^2+|\alpha 1|^2= 1$ anlamına gelir ki buna normalizasyon denir ve kuantum ölçme işlemlerinin tutarlığı için şarttır.

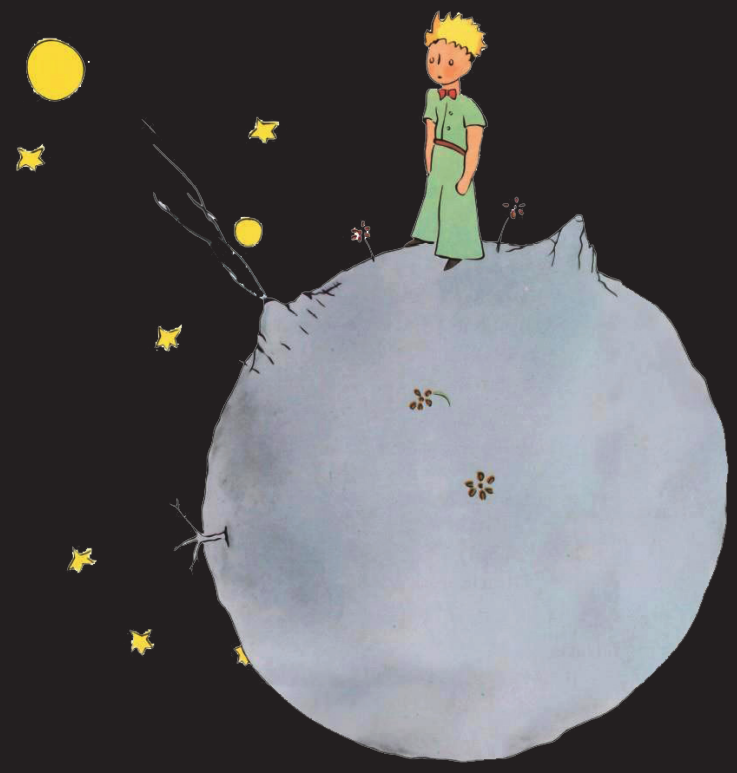
Foton var olması ve yokluğu ise sistemin genel durumunun süperpozisyonudur. $|0> + |1>$ durumu $e^{i\theta}|0> + e^{i\theta}$ vektörle tanımlı duruma denktir. Süperpozisyondaki iki dik durum arasındaki görece faz çarpanları fiziksel olarak önem arz eder ve $|0> + |1>$ durumu $|0> + e^{i\theta}|1>$ vektörleri ile tanımlanan durum fiziksel olarak farklıdır. Yani tek bir q-bitin genel durumu $|\psi|$

$|\psi|= \cos(\theta/2)\,|0>+ e^{i\alpha}\sin(\theta/2)|1>$ şeklindeki vektörle tanımlanır.

GENİŞLETİLMİŞ 9. BASKI TÜM KİTAPÇILARDA



abaküs



Büyükler sayılardan hoşlanır. Onlara yeni bir dostunuzdan söz açtınız mı, hiçbir zaman size önemli şeyler sormazlar. Hiçbir zaman: "Sesi nasıl? Hangi oyunu sever? Kelebek toplar mı?" diye sormazlar. "Kaç yaşındadır? Kaç kardeşi var? Kaç kilodur? Babası kaç para kazanır?" diye sorarlar. Ancak o zaman tanıdıklarını sanırlar onu. Büyüklere: "Pembe kiremitten bir ev gördüm, pencerelerinde sardunyalar, damında güvercinler vardı" derseniz, o evi bir türlü gözlerinin önüne getiremezler. Onlara: "Yüz bin franklık bir ev gördüm" demeniz gerek. O zaman: "Aman ne güzel!" diye bağırırlar.
Antoine de Saint-Exupéry *Küçük Prens*