ARKA KAPI

www.arkakapidergi.com

2 Aylık Siber Güvenlik Dergisi • 10 TL • 1. SAYI
2018

Meltdown ve Spectre Zafiyetlerinin Düşündürdükleri • Chris Stephenson

Devrim Niteliğindeki Blockchain Teknolojisi Güvenli mi? • Mustafa Yalçın

Web 2014'te Ölmeye Başladı • André Staltz

Ağ Tarafsızlığı • Mehmet Pehlivan

Her 8 Kişiden 1'inin Parolası Biliniyor! • Mustafa Altınkaynak

"Kendi Bağlantım" ile VPN Sunucunuzu Kurun • Ömer Çıtak

ISSN 2618-6373
01
9 772618 637008

EDİTÖRDEN

Yeni bir dergi, yeni bir heyecan ve yeni umutlar.

Konfiçyus'un harikulade bir sözü var, "Karanlığa söveceğine bir mum da sen yak!"

Bu dergi Siber Güvenlik alanında teknik bir dergi ihtiyacı için kıymetli dostların sıcacık kalpleriyle tutuşturduğu bir mumdan fazlası değil.

İnanıyoruz ki bu çalışma hem kalpleri ısıtacak, hem dimağları aydınlatacak.

Bir mumun, başka bir mumu tutuşturmakla kendinden kaybetmeyeceği hepimizin malumu.

Bizleri de zenginleştiren böyle bir çalışma için hem sevinçli, hem de affınıza ilticalen biraz da gururluyuz.

Böylesi bir çalışmanın tüm maddi yükünü omuzlayan Abaküs Yayınları'ndan Cevahir Demiryakan'a, Cem Demirezen'e ve Abaküs Kitabevi'nin basın-yayın emekçilerine.

Çalışmamıza teveccühü ile bizleri heyecanlandıran Chris Stephenson Hocamıza.

Derginin bir nevi isim babası olan Siberbulten.com'un yöneticisi Minhaç Çelik'e,

Yazıları ile bu dergiyi var eden kıymetli yazar dostlarımıza müteşekkiriz.

Dergi toplantıları esnasında vefat haberini aldığımız Mustafa Akgül Hoca'mızı da rahmet ve ülkemize kattıklarından ötürü şükran ile anıyoruz.

Yeni bir sayıda görüşmek dileği ile...

Ziyahan Albeniz

editor@arkakapidergi.com

KÜNYE

YIL: 1 Sayı: 1 - 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

Reklam ve Abonelik: abone@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

Web: www.arkakapidergi.com

Twitter.com/arkakapidergi

abone@arkakapidergi.com

editor@arkakapidergi.com

etkinlik@arkakapidergi.com

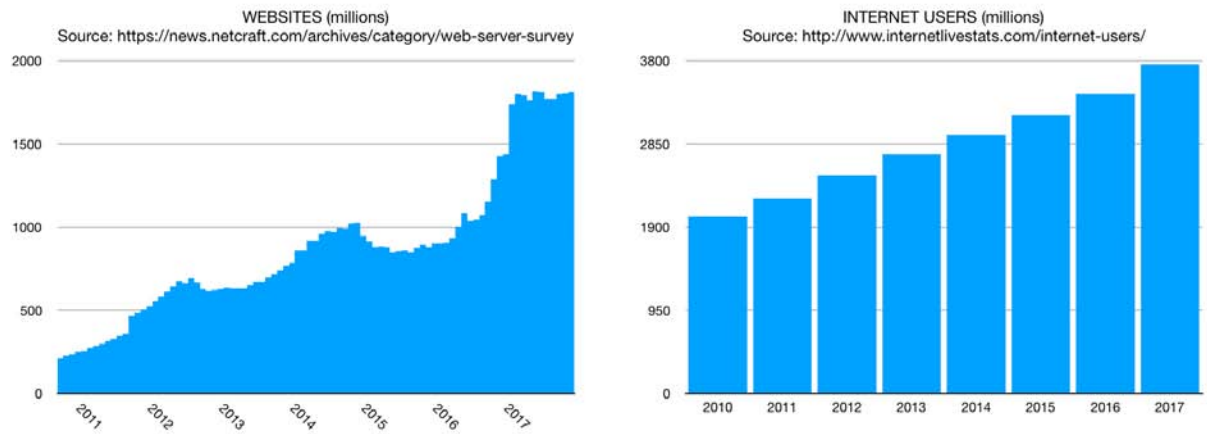
İÇİNDEKİLER

André Staltz - andre@staltz.com*

Web 2014'te Ölmeye Başladı

2014 yılından önce Google'ı, Facebook'u ve Amazon'u kullanan pek çok insan vardı. Bugün de durum bundan farksız değil. (Yazı boyunca GOOG, FB, AMZN kısaltmaları kullanılacaktır.) Bu web sitelerine bakacak olursak kelimenin gerçek anlamıyla kullanıcı arayüzleri de dâhil önemli bir değişiklikten söz edemeyiz. Ancak web'i güçlü kılan temel dinamikler önemli ölçüde değişti ve bu üç şirket web'in temelden değişiminin merkezinde yer alıyor.

Veriler internet kullanımının azalmadığını gösteriyor. Bilakis hem kullanıcı sayısı hem de web sitesi sayısı olarak istikrarlı bir büyüme görülüyor.



(Kaynak: https://news.netcraft.com/archives/category/web-server-survey and http://www.internetlivestats.com/internet-users/)

Son 4 yılda değişen ise web trafiği üzerindeki pazar payları. Verilere göre 2014'ten bu yana hiçbir şey değişmedi, fakat GOOG ve FB bugün internet trafiğinin yüzde 70'inden fazlası üzerinde etkiye sahip. Mobil internet trafiği web trafiğinin önemli bir kısmını oluşturuyor. 2015 yılında tek başına Latin Amerika'da GOOG ve FB servisleri mobil trafiğin yüzde 60'ına sahip ve 2016'nın sonlarına doğru bu artış yüzde 70'lere doğru seyrediyor. Kalan yüzde 30'luk trafik ise diğer mobil uygulama ve web sayfaları tarafından paylaşılıyor. Mobil cihazlar, GOOG ve FB ağlarına ulaşmak için kullanılan cihazların başında geliyor.

Kaynak: https://staltz.com/the-web-began-dying-in-2014-heres-how.html

Çev: Ziyahan Albeniz - ziyahan@arkakapidergi.com

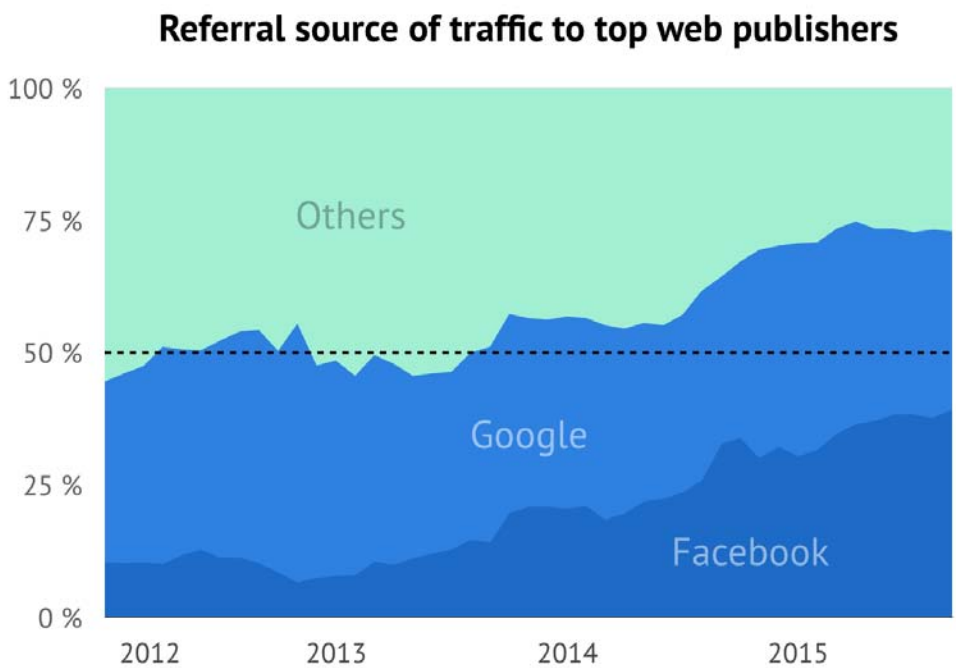
Upstream		Downstream		Aggregate	
Facebook	30.49%	YouTube	26.09%	YouTube	23.91%
WhatsApp	15.76%	Facebook	22.92%	Facebook	23.55%
Google Cloud	11.96%	HTTP - OTHER	8.00%	HTTP - OTHER	7.70%
YouTube	6.18%	WhatsApp	7.98%	WhatsApp	7.43%
SSL - OTHER	5.94%	Instagram	4.91%	Google Market	5.85%
HTTP - OTHER	5.26%	Google Market	4.64%	Instagram	4.65%
Instagram	2.55%	MPEG - OTHER	4.46%	Google Cloud	4.41%
Google Market	1.57%	Google	3.50%	MPEG - OTHER	4.05%
MPEG - OTHER	0.94%	SSL - OTHER	2.95%	SSL - OTHER	3.27%
Snapchat	0.79%	Snapchat	1.02%	Snapchat	0.98%
	81.44%		86.28%		85.51%

sandvine

(Kaynak: https://www.sandvine.com/resources/global-internet-phenomena/2016/north-america-and-latin-america.html)

GOOG ve FB hâkimiyetinin bir başka tezahürü medya siteleri üzerinde görülebilir. GOOG ve FB'ye ait olmayan popüler web siteleri genellikle basın sektöründen. Örneğin Amerika'da Top 10 arasında yer alan 6 medya sitesi var[1]. Yine Brezilya'da Top 10'da, 6 medya sitesi bulunuyor.[2] İngiltere'de ise Top 10'nun 5'i medya sektörüne ait.[3]

Peki bu medya siteleri ziyaretçilerini nereden alıyorlar? 2014 öncesinde Arama Motoru Optimizasyonu (SEO) web geliştiricileri arasında, Google arama sonuçlarındaki sıralamada pozisyonlarını iyileştiren yaygın bir çözümdü. Çünkü bu yaklaşık olarak trafiğin yüzde 35'ini temsil ediyordu. Trafiğin yüzde 50'den fazlası ise diğer kaynaklardan geliyordu. Facebook'ta bir sayfanızın, bir grubunuzun olması iyi sayılabilirdi ama esas önemli olan SEO'ydu. Sonraki üç yıl boyunca Facebook'tan gelen trafik yaklaşık olarak yüzde 45 artarak, arama trafiklerden gelen rakamı ezdi geçti. 2017 yılında medya, sayfa gösterimleri konusunda trafiğin çoğunluğunu temsil ettiği için hem Facebook'a hem de Google'a bağımlıydı.



(Kaynak: https://blog.parse.ly/post/2855/facebook-continues-to-beat-google-in-sending-traffic-to-top-publishers/)

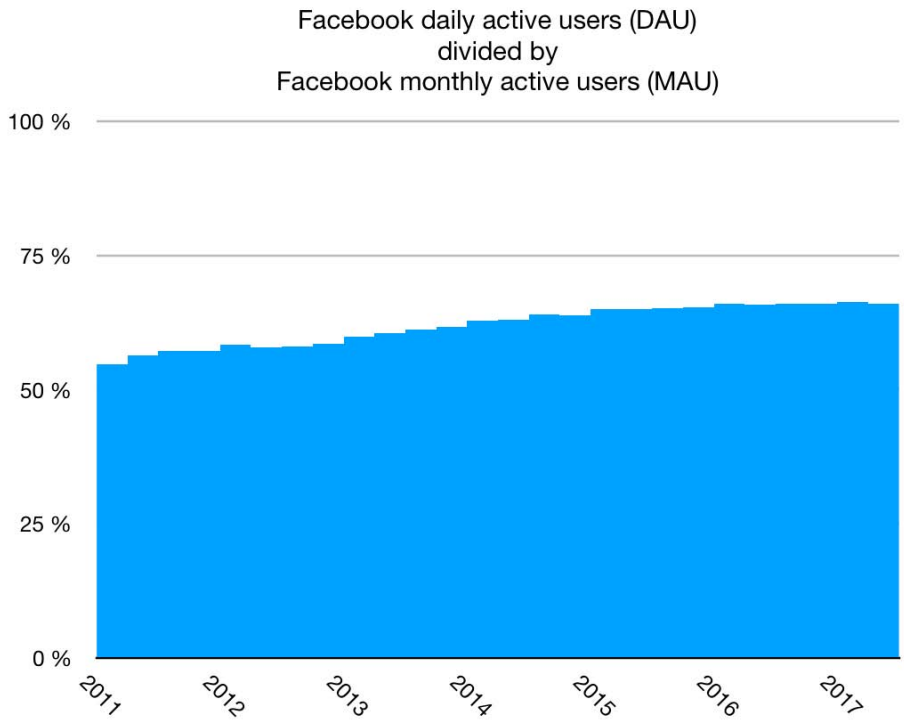
1 https://www.statista.com/statistics/271412/most-visited-us-web-properties-based-on-number-of-visitors/
2 https://www.statista.com/statistics/254727/most-visited-web-properties-in-brazil/
3 https://www.statista.com/statistics/272871/leading-internet-properties-in-the-uk-by-unique-visitors/

Medya siteleri ve bu iki teknoloji devi arasındaki ilişki durumu biraz karışık. 2014'te FB, Facebook Paper adını verdiği ve reklam tüketimleri üzerinde kendisine geniş kontrol sağlayan bir hizmete girişti. Bu taktik başarılı olmadı fakat stratejileri Facebook Instant Articles gibi farklı araçlarla devam etti. Sosyal platformlardan gelen trafiğe bağımlı olan ve bu sosyal devler tarafından tehdit edilen medya nihayet karşılık vererek Instant Articles'a sundukları desteği geri çektiler.

Facebook işin kaymağını yerken, GOOG kendi arama trafiğinin artmadığını fark etti, bu yüzden de Accelerated Mobile Pages (AMP) adını verdiği alternatif bir hizmet başlatarak medya sitelerine trafik yönlendirmesi yapmaksızın, makaleleri kendi sunucularından servis etme hizmetini başlattı. Basın, FB'ye gösterdiği tepkinin benzerini GOOG'a da gösterdi: arama devlerinin haber tüketimini kontrol etmek için gösterdikleri aç gözlülüğü kamuoyu ile paylaştılar.

Veriler gösteriyor ki Google Search önemli ölçüde değişmezken, FB web üzerindeki hâkimiyetini önemli ölçüde arttırdı. FB bunu tam olarak nasıl başardı ve bu ilerlemenin anahtarı durumundaki hadiseler nelerdi? 2014 öncesinde, her iki şirket de pek çok web servisinden oluşan bir ürün yelpazesine sahipti. Google henüz Alphabet firması olarak biçim değiştirmemişken odak noktası biraz dağınıktı. Google ilk olarak Google Wave ile ardından Google Buzz, Orkut ve Google+ ile sosyal platformlarda kendine yer edinmeye çalışıyordu. Google, sosyal medya kategorisinde biri 2014 sonrasında, 5'i ise tek başına 2010 yılında olmak üzere toplamda 18 şirkete sahip oldu.[4] FB ise arama dünyasında MSFT (Microsoft. Hisse senedi borsasında şirketi temsilen kullanılan kısaltma, çn) ortaklığında Bing vasıtasıyla rekabet ediyordu.

Görünen o ki 2014 yılı boyunca FB, sadece sosyal alana yoğunlaşmak için kendini re-organize etti. Şubat ayında Google'ın Youtube'u satın almak için ödediği fiyatın 11 katını ödeyerek WhatsApp'ı satın aldı. Aralık ayında MSFT ile Bing ortaklığını sona erdirdi. Kullanıcıların Facebook platformuna bağlılıkları istikrarlı bir biçimde devam etti. (Yandaki görseli inceleyiniz.). FB, dört basit ürünü Facebook, WhatsApp, Messenger ve Instagram vasıtası ile, sosyal paylaşım kategorisinin süper gücü haline geldi.



(Kaynak: https://www.statista.com/statistics/346167/facebook-global-dau/ and https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/)

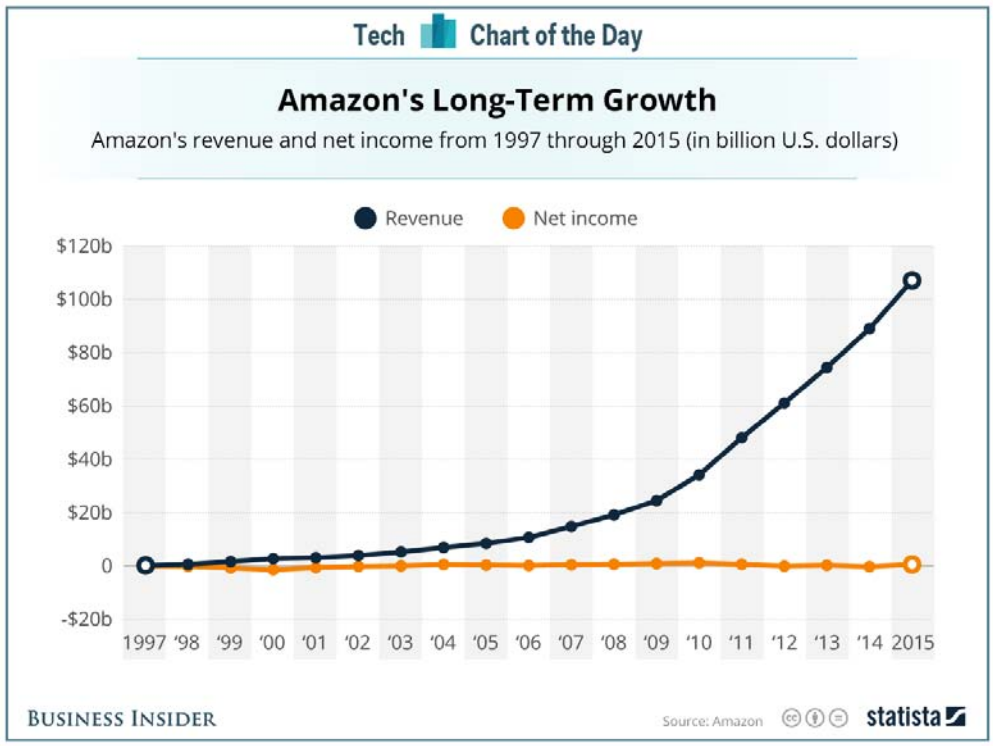
Aynı şekilde Google, 2014 yılında sadece yapay zekâya odaklanacak şekilde kendini re-organize etti. Ocak 2014'te, DeepMind'ı satın aldı ve aynı yılın Eylül ayında Orkut'u kapattı. (Orkut, Google'ın bazı ülkelerde maddi başarı sağlayan birkaç sosyal medya ürününden biri idi.)

Ağustos 2015'te The Alphabet Inc adı ile yeniden yapılanma anons edildi, muhtemelen bu aşamaya gelinmesi bürokrasi ve toplantılarla birkaç ayı bulmuştur. Bu yeniden yapılanma Google'ın web yönelimli departmanlara, basit bir misyonla odaklanması açısından önemli idi. Google basit arama pazarında gelecek görmedi ve Eric Schmidt'in sözleri ile aramadan öneriye "*From Search to Suggest*" geçişini duyurdu ve Sundar Pichai'nin sözleriyle ilk yapay zekâ şirketi oldu. Web'i kısa zamanda etkisi alma açısından bakarsak Google şimdilerde FB'nin gerisinde ancak teknik tecrübesi, dev bütçesi, etki ve vizyonu ile uzun vadede yapay zekâ ürünleri sayesinde internet üzerinde büyük bir yol oynayacak. Google ne yaptığını biliyor!

4 https://www.geckoboard.com/tech-acquisitions/

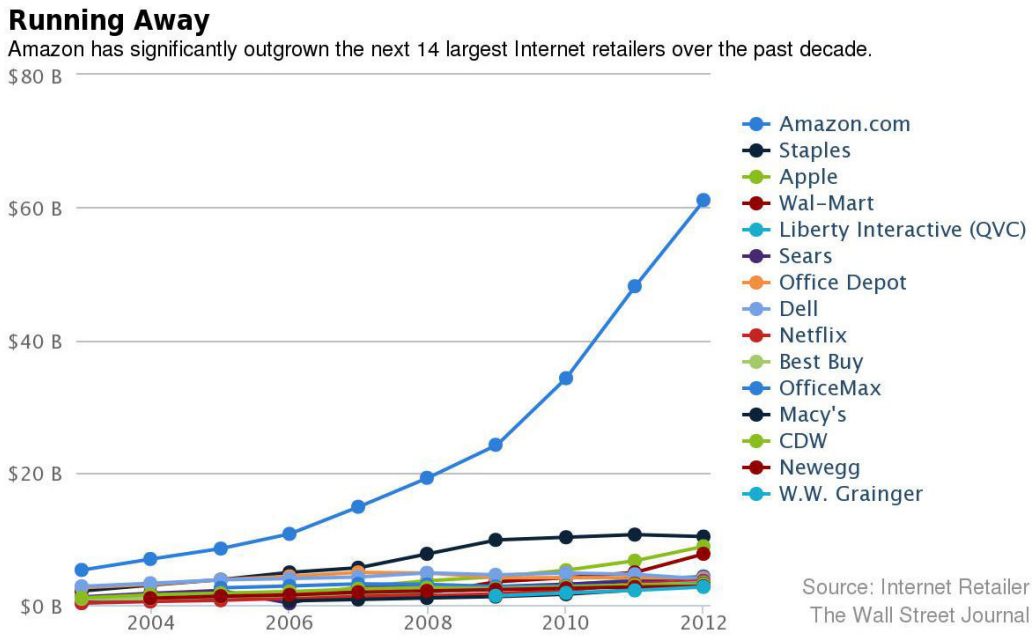
Bu firmalar, 4 yıl önceki firmalar değil. Google artık bir internet şirketi değil. O artık bir bilgi interneti şirketi. FB, aynı şekilde bir internet şirketi değil, bir sosyal internet şirketidir. Önceleri aralarında bir rekabete giriştiler. Bu rekabet internette, kullanıcılar açısından çeşitliliğe sebep oldu. Fakat bugün onlar, web'te kendilerine biçtikleri görev ile ziyadesiyle memnun görünüyorlar ve bizler bize sunulan ürün ve hizmet çeşitliliğini kaybettik. Şimdi tartışmanın başka bir veçhesine, e-ticaret ve Amazon'a bakalım.

Veriler gösteriyor ki Amazon kâr etmeye odaklanmıyor.



(Kaynak: https://www.statista.com/chart/4298/amazons-long-term-growth/)

Kâr yerine, kendisine biçtiği misyon ABD'deki rakiplerini alt ederek, sektör liderliğini yakalamak.



Amazon'un nasıl bir e-ticaret şirketi olduğunu detaylandırabilirdim ancak bu Scott Galloway'ın bu konudaki görüşlerinin tekrarından fazlası olmayacak. Gerçekten de izlenmeye değer bir konuşma için, dinlemenizi tavsiye ederim.[5]

Web Ne idi, Ne oldu...

Yukarıda zikrettiğimiz olay ve bilgiler üç internet şirketinin nasıl böylesine büyük bir etkiye sahip olduklarını açıklıyor. Fakat bu saydıklarımız nasıl oluyor da web'in ölümünün başlangıcı anlamına geliyor? Bunu açıklamak için web'in ne olduğunu tekrar düşünmeliyiz.

Web'in mucidi Tim Berners-Lee'ye göre web'in gerçek misyonu çok yönlü bir yayın ve paylaşım platformu olması idi. Bugün ise Tim'in kendisi dahi Web'in ölmek üzere olduğunu itiraf ediyor[6]: Onun istediği web ile, şimdilerde sahip olduğu web arasında dağlar kadar fark var!

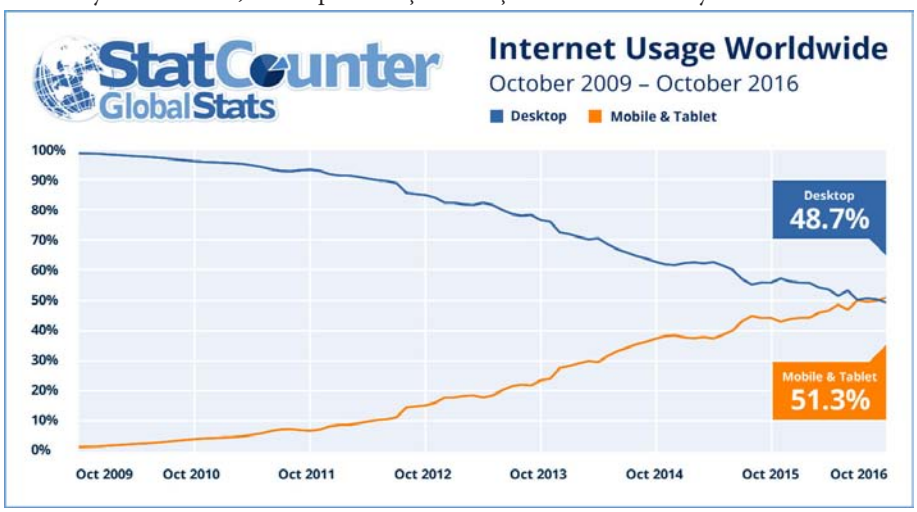
Google, Open Web'i Savunmuyor mu?

Google web'te doğan bir firma olarak, web'in hem teknik olarak ilerlemesine, hem de (ç.n: kitlelerce) benimsenmesine yardım etmiştir. Bu reddedilemez. Hâlâ open native mobil uygulamaları savunuculuğu üzerinden Progressive Web Apps (PWAs)'ı savunarak[7], web'in gelişmesi çabalarına öncülük ediyor.

Google open web'in hayatta kalmasını garanti altına almaya çalışmıyor mu? Tam olarak değil. Google'ın amacı mümkün oldukça fazla data toplamak ve AI'yi (yapay zekâ) inşaa etmek.

Onların misyonu bizlere zamanında ve kişiselleştirilmiş bilgiler sunacak yapay zekâya sahip olmak, özellikle bilgiler sağlayacak web sitelerine değil. Google tarafından gösterilen tüm çabalar bu yüce AI ülküsüne hizmet ediyor.

Mobil kullanımı yükselişte, daha şimdiden masaüstünü geçerek internet kullanımında ilk tercih haline geldi ve mobil uygulamalar bugüne kadar iyi bir kullanıcı deneyimi için ilk tercih oldu. Google native uygulamalardan, Android için bir nebze olsa da, özellikle iOS cihazlardan ya çok az bilgi toplayabiliyor, ya da hiç toplayamıyor. PWA'lar doğal ve open web'de vücut bulduğunda kullanıcılara bekledikleri deneyimi sunarken, data toplamak için elverişli bir zemin hazırlayacaklar.



Google open PWA'ları savunduğu kadar Firebase ve Google bağımlı AMP yüklemeleri de teşvik etmektedir. Google Open Web'i tutarlı bir biçimde savunmuyor. GTalk'da XMPP'yi (nam-ı diğer Jabber, çn.) kullanmaktan vazgeçti[8] ve açık bir protokol kullanmayan Google Hangouts'u destekleyerek GTalk'ın kullanımını durdurdu. Chrome Web Store tıpkı App Store gibi bir arka bahçe. Google, yine açık bir standart olan RSS'i kullanan Google Readers'ı kapattı.[9] Google Cloud TPU ise kendi veri merkezlerinde mevcut olan kendi açık kaynak framework'ü TensorFlow'u destekleyen tescilli bir donanımdır.[10] Google Inbox, kapalı iş modellerinin temel bileşeni, standart dışı kapalı bir algoritma ile tüm yaşantınızı organize etmeyi vaad ediyor.

Google, çalışanların özerkliğe ve çeşitli projelere sahip olduğu büyük bir şirket. Büyük gayretler, fikirler ilk yapay zekâ şirketi olma misyonu ile fevkalade uyumlu ve tutarlıdır. Kapalı ve bulut sunucularında yaşayan bir yapay zekâ!

5 https://www.youtube.com/watch?v=GWBjUsmO-Lw
6 https://www.theguardian.com/technology/2017/mar/11/tim-berners-lee-web-inventor-save-internet
7 https://developers.google.com/web/progressive-web-apps/
8 https://www.eff.org/deeplinks/2013/05/google-abandons-open-standards-instant-messaging
9 http://edition.cnn.com/2013/03/14/tech/web/google-reader-discontinued/index.html
10 https://www.forbes.com/sites/moorinsights/2017/05/22/google-cloud-tpu-strategic-implications-for-google-nvidia-and-the-machine-learning-industry/3/#60053cf7513d

90'lardan 2010'lara kadar kullandığımız web mükemmel olmasa da orijinal amacına sadıktı. Web'in bu çeşitliliği birçok firmanın işlerini yapmasına, sıradan ve bağımsız hobi gruplarının büyümesine, kişisel sitelerin kendilerini fiziksel olarak barındırabilecek herhangi bir sunucudan yayın yapmasına imkan sağladı. İnternetin yapısal çeşitliği, web'deki işletmelerin ve topluluklarının başarılarına doğrudan bağlıdır. Web'in herkese açık olması onun güvenliği, erişilebilirliği, yenilikçi ve rekabetçi olması açısından hayatidir.

2014'ten sonra, internetin sunduğu bu yapısal ve ekonomik çeşitliliğin kazanımları kaybedilmeye başlandı. Amazon ve devasa oranlarda siteler barındıran Google'ın Cloud Servisleri ile rekabet etmek zor. Yoğun bir ziyaretçi trafiğine talip olan herhangi bir site arama motorları ve sosyal ağlara bağımlı halde.

Amazon, Facebook ve Google'ın Gölgesinde Ne Olacak Bu Web'in Hali

Takip eden analiz, web'in bugünkü durumunu baz alan ve Google, Amazon ve Facebook yönetimlerinin kamuoyu ile paylaştığı stratejilerden hareketle bir gelecek kurgusuna dayanmaktadır.

ABD'deki Ağ Tarafsızlığı savaşı 2014'te kazanıldı[11], fakat 2017'de muhtemelen kaybedilecek ikinci bir savaş görmekteyiz.[12] Internet Servis Sağlayıcıları (ISP) muhtemelen yakında kullanıcıların hangi sitelere erişip, erişemeyeceğine karar verebilecekler. Google, Facebook ve Amazon siteleri internet kullanıcıları nazarındaki popülariteleri nedeniyle erişime açık olan siteler arasında olacaklar. Pazar bunu istediği için ISP'ler muhtemelen Google, Facebook ve Amazon'a ulaşmak için daha ucuz planlar sunarken, full internet erişimi için daha yüksek fiyatlar talep edecekler. Portekiz'de daha şimdiden böyle bir vakıa söz konusu.[13] Bu, üç teknoloji devinin sahip olduğu egemenliğin giderek artması demek. Küçük işletmelerin bağımsız web sitesi sahibi olmasının hiçbir özendirici tarafı kalmayacak ve daha mantıklı bir seçenek olarak görülen Facebook sayfalarına yönelecekler. Daha küçük e-ticaret siteleri ya Amazon tarafından satın alınacak ya da iflas edecek. Kullanıcıların çoğu tüm sitelere erişemeyeceği için Google, kullanıcı ve siteler arasında sadece bir köprü olarak eski cazibesini yitirecek.

Google'ın aramadan uzaklaşması aslında web için nasıl bir strateji güttüklerinin göstergesi. Yıllarca Google, web'i indexleyerek web'e yardımcı olan önemli bir araç olarak kullanıldı. Fakat son zamanlarda sadece bir arama motoru olmak Google için çekici değil. Gelecek projeksiyonuyla ilgili beyanlarında ifade ettikleri amaçlar için, "Dünyanın bilgisini organize etmek ve evrensel olarak erişebilir ve kullanışlı kılmak", arama motoru yaklaşımının pabucu dama atıldı. Google'a göre arama sorgusundan, arama sonuçlarına, oradan web sitesine, bilgiye giden birkaç saniyelik yol, ideal bir kullanıcı deneyimi sunmak için oldukça uzun. Amaçları, bu yoldaki aracıları, engelleri kaldırmak. Arama sonuçlarını kırpmak için "Kendimi Şanslı Hissediyorum" butonunu denediler, fakat akıllı bir analiz olmadan bunlar güvenilir bir kestirme yol sunamazlardı. Yapay zekâ ile, "bilgiyi getir" gibi tek bir adım ile, arama dahi yapmadan istenen sonuçları getirebileceklerine inanıyorlar. Suggest olarak tabir ettikleri tam olarak bu.

Bir index olarak, insanlar arama sonuçlarının tarafsızlığı ile ilgili olarak farklı beklentilere sahiptirler. Bazıları Google'dan tamamen tarafsız olmasını beklerken, bazıları bazı sonuçların kaldırılarak aramanın hemen sonuçlandırılmasını isterler. Avrupa Birliği Google'dan arama sonuçlarından kaldırılma taleplerine uymasını istedi (Unutulma hakkı, çn)[14] ve alışveriş ile ilgili sonuçlarda tarafsız olmadığı gerekçesiyle Google'ı cezalandırdı.[15] İş modeliyle uyumlu olmadığı için, içeriklere dair tarafsız bir pozisyonda olmanın Google için hiçbir kazançlı tarafı yok. Üstüne üstlük birden fazla hükümet tarafından izleniyor ve potansiyel olarak firma itibarlarını riske atıyorlar.

Suggest stratejisi ise Google Now, Google Assistant, Android bildirimleri ve Google Home servisleri üzerinden hizmet vermek. Bunların hiçbirisi web'in sözü edilen parçaları değil, diğer bir deyişle web sitelerinden müteşekkil browser dünyasının dışındalar. İnternet, sadece Google'ın bulutundaki datanın, son kullanıcı cihazına aktarılması işlevini görüyor, web'in kendisi ise bypass edilmiş durumda. Google'ın başkanı Schmidt'in vizyonu ise masaüstü bilgisayarlarda browser üzerinden deneyimlenenin aksine, her yerde olan ve kişiselleştirilmiş bir internet.[16]

Benzer şekilde Amazon iş modeli hâlâ web portallarına dayanıyor. (yüzde 33'lük bir satışı temsil ediyor, yüzde 25 gibi büyük bir oran ise mobil uygulamaları üzerinden gerçekleşiyor. Amazon Echo'dan söz etmeye gerek bile yok.) Google Home gibi, Amazon Echo da web'i bypass ederek interneti sadece cloud sunucuları ve son kullanıcı arasında bir iletişim için kullanıyorlar. Web harici olan bu yeni trafikte, teknoloji devleri data trafiği üzerinde daha fazla söz hakkına sahip. Hatta bu

11 https://www.theverge.com/2014/2/25/5431382/the-internet-is-fucked
12 https://www.theverge.com/2017/7/12/15715030/what-is-net-neutrality-fcc-ajit-pai-bill-rules-repealed
13 https://www.reddit.com/r/technology/comments/79770i/in_portugal_with_no_net_neutrality_internet/
14 https://www.cnet.com/news/google-must-delete-search-results-rules-european-court/
15 https://www.bloomberg.com/news/articles/2017-06-27/google-gets-record-2-7-billion-eu-fine-for-skewing-searches
16 https://www.hollywoodreporter.com/news/google-chairman-eric-schmidt-internet-765989

devler, Google'ın Amazon Echo cihazlardan Youtube erişimini engellediği gibi birbirlerini dahi bloklayabiliyorlar.[17]

Teknoloji Devlerinin Apple'laşması

Google, MSFT, Facebook ve Amazon, Apple'ın yüksek kalitedeki ürünler etrafında marka sadakati oluşturma stratejisini taklit ediyorlar. Benim Apple'laşma adını verdiğim süreç boyunca bu şirketler; 1) Kendi arka bahçelerini, korunaklı alanlarını oluşturuyorlar. (Play Store vb. çn.), 2) donanım şirketleri olmaya başlıyorlar, 3) pazar için tasarım yaparken, tasarımın kendisini pazarlıyorlar. Bu Apple'ın kendisi için bir tehdit, çünkü bu saydığımız firmalar konu big datanın toplanması ve kullanılmasına geldiğinde, bu işin ağa babaları. Apple'ın App Store'ı erken ve gözüpek sunuşu, baskın yazılım dağıtım platformu olan web'i şok ederken, web'in yerini alacak derecede bir tehdit arz etmiyordu. Fakat bu yeni dalga daha farklı görünüyor: daha az dikkat çekiyor fakat, web'i yerinden edecek gibi.

Google, Facebook ve Amazon'un tarayıcıları ortadan kaldırmaya yönelik spesifik bir amaçları olmasa da, web'i etrafından dolaşmaya yönelik bir meyilleri var. Bilgi ve ticaret internetinde, kullanıcılara istediklerini sunmada etkili olmak amaçtır. Oysa sosyal internette hedef, insanlar arasındaki iletişim için etkili bir kanal sunmaktır. Bu, Facebook'un gelecekteki sosyal etkileşim ortamı olarak Arttırılmış Gerçeklik (AR) ve Sanal Gerçeklik (VR) ile ilgili 10 yıllık stratejisini açıklıyor. Bu strateji sosyal arttırılmış gerçekliğin (AR) tarayıcılardaki gerçek zamanlı stratejiden nasıl daha doğal olduğunu kanıtlayarak web'i bypass edecek. Bugün dahi pek çok kişi, diğerleri ile mobil uygulamalar vasıtası ile iletişim kuruyor, tarayıcılar yolu ile değil.

Bu üç internet devinin ortak noktası, datanın üretildiği ve paylaşıldığı yeni sanal kontekstler yaratarak tarayıcıların dışında büyümeleri. Web tıpkı diğer teknolojiler gibi yeni teknolojilere karşı cazibesini yitirerek ölecek. Ve bugün tarih olan pek çok teknoloji gibi ne aniden yok olacak, ne de bütünüyle ortadan kaybolacak. Bugün bir Walkman satın alabilir ve bu Walkman ile bir kaset dinleyebilirsiniz, buna rağmen bu teknolojinin kolektif yaygınlığını yitirdiği gerçeğini değiştirmez. Web'in ölümü, ona olan ihtiyacın adım adım ortadan kalkması ile gelecek, dramatik bir yok oluş ile değil.

Trinet

İnternet web'den daha çok yaşayacak. Google, Facebook ve Amazon hâlâ deniz altlarından geçen internet kablolarına (Backbone, internet omurgası çn.) bağımlı. Bununla birlikte, pek çok açıdan internet yaygınlığını kaybedecek ve temel altyapı sadece Google, Facebook ve Amazon trafiği için optimize edilecek. Artık bildiğimiz manada o bir "ağların ağı" (network of networks" yerine, sadece "network of three networks" yani Trinet olacak. İnternet altyapısının doğuşuna zemin hazırlayan Workplace konsepti daha soyut bir seviyeye taşınacak: Facebook Grupları, Google Hangouts, G Suite ve bu devlerin sahip olduğu rekabet halindeki servisler. Workplace ağları bugün zaten yerel ağlarda değil, SaaS'larda hayat buluyor. Kullanıcı deneyimini geliştirmek için, Trinet internetin teknik bir gelişimi olacak. Bugün bu çabalar Google'da gerçekleşiyor.[18] Uzun vadede, eski internetin routing mekanizmasını ve web'i desteklemek yük olarak addedilecek, farklı donanım ve protokol seviyelerinde internete verilen destek kesilecek. Eski internete erişmek, nasıl ki bugün Windows 95 browser'ınızda emüle edilebiliyorsa[19], Trinet aracılığı ile erişilen Google'ın bulut servisleri yolu ile gerçekleşecek. ISP'ler de internetin eskidiğini kabul edecek ve Google, Facebook ve Amazon kullanıcı deneyiminden kaynaklanan pazar talebi nedeniyle Trinet'i destekleyecek.

Belki AR ve VR'ın yarattığı kullanıcı deneyimleri, temassız ticaret ve bilgi paylaşımı devlerin inşa ettiği gelecek hakkında iyimser bir kanı uyandırıyor. Fakat web'in 25 yılı bize çantada keklik olarak gördüğümüz temel özgürlüklerimizi kanıksattı. Anonim olmanın ne kadar faydalı olduğunu unuttuk, paylaşımlarımız üzerinde kontrol sahibi olmayı ve Google ile aynı haklara sahip olarak nasıl bağımsız bir start-up başlatabileceğimizi unuttuk. Trinet'te, şayet Google'dan ya da Facebook'tan banlanırsanız, herhangi bir alternatifiniz olmayacak. Yeni bir hesap oluşturmaktan bile men edilebilirsiniz. Özel kuruluşlar olarak, Google, Facebook ve Amazon size her zaman ağlarına erişebileceğinizi garanti etmek zorunda değil. Bu devlerin sunucularında hesap sahibi olmak gibi yasal bir hakka sahip değilsiniz. Toplumlar olarak böyle bir hakkın peşinde de değiliz ve var gücümüzle önümüze koydukları bu stratejiye karşı çıkıyoruz.

Web ve internet, özgürlüğü temsil ediyor: tüm uluslardan insanlar arasında bilginin etkili ve denetimsiz paylaşımı. Trinet'te daha canlı paylaşımlara sahip olabileceğiz belki ama özgürlüğümüzü feda etmiş olacağız. Pek çoğumuz ise verdiğimiz bu ödünün yarattığı trajedinin sadece gerçekleştiğinde farkına varacağız!

17 https://www.reuters.com/article/us-amazon-com-google/amazon-says-google-has-pulled-youtube-from-echo-show-device-in-tech-face-off-idUSKCN1C20A8

18 https://www.nextplatform.com/2017/07/17/google-wants-rewire-internet/

19 https://win95.ajf.me/

Avukat Mehmet Pehlivan • **PEHLİVAN I İLKAKIN HUKUK BÜROSU** • mehmet@pehlivanilkakin.com

Ağ Tarafsızlığı

Giriş

Geçtiğimiz günlerde ABD'de internetten sorumlu düzenleyici kuruluş olan Federal Communications Commision'da (FCC) yapılan bir oylama ile 2015 yılında internete tarafsız erişimi garanti altında tutan ağ tarafsızlığını korumak için getirilen düzenlemenin kaldırılmasına karar verildi. Bu karar henüz kesinleşmiş bir karar değil. Kesinleşmesi için Temsilciler Meclisi'ne ve Senato'ya gidecek. Eğer bu karar Senato'dan geçerse, sırada Anayasa Mahkemesi var. Yani henüz tam anlamıyla "Ağ Tarafsızlığı"na veda etmiş değiliz. Bu nedenle bu süreçte bu kavramın ne olduğu ve bizim için neden önemli olduğunu bilmek yalnızca profesyonel anlamda web kullanıcılarının değil sıradan web kullanıcıları için de hayati önem taşımaktadır.

Peki, ağ tarafsızlığı ne demek ve önemi nedir?

Ağ Tarafsızlığı (Net Neutrality), ilk olarak 2003 yılında Columbia Üniversitesi'nde iletişim hukuku profesörü olan Tim Wu tarafından kavramlaştırılmıştır. Ağ tarafsızlığı kavramı, internet erişim sağlayıcıları veya devletlerin internet üzerindeki veri veya hizmetlere eşit davranması gerektiğini ortaya koyan bir kavramdır. İnternet üzerindeki hiçbir verinin, hizmetin veya platformun özel olarak bir politikayla, kanunla, düzenlemeyle kontrol edilmemesi ve trafiğinin engellenmemesi bu kavramın özünü oluşturmaktadır.

Ağ tarafsızlığı, internetteki tüm veri akışının, örneğin elektronik postaların, müzik ve videoların ya da internet aramalarının ve internet üzerinden yapılan telefon görüşmelerinin, internet sağlayıcıları tarafından birbirinden farksız ve eşit hızda mümkün kılınmasına verilen isimdir. **Daha basit bir ifadeyle belirtmek gerekirse, Ağ tarafsızlığı, internet erişim sağlayıcıları veya devletlerin veri niteliğine göre biz kullanıcılardan ayrı bir hizmet bedeli alamayacağı gibi internet hızı ve ulaşım izni gibi konularda da söz sahibi olmamasını ve her kullanıcının aynı kalitede hizmet almasını amaçlamaktadır.** Ağ tarafsızlığı birçok ülkede yasalar ile korunan ve düzenlenen bir hususdur.

Dünya'daki ve Türkiye'deki Düzenlemeler

Avrupa Birliği ve Amerika'da 2015 yılında uygulamaya geçirilen, ağ tarafsızlığını da içerisinde barındıran, açık internet kuralları Avrupa Birliği'nde hâlen yürürlükte olup; tüm üye ülkelerdeki erişim sağlayıcıları bağlayan bir düzenlemedir.

Amerika'daki olumsuz gelişmelerin hemen peşinden Avrupa Birliği üye ülkesi olan Almanya'da Federal Hükümet, açık ve eşit bir internetin "vazgeçilemez" olduğunu vurguladı. Almanya'da Federal Ağ Ajansı, bir internet sağlayıcısına "veri akışını yasak bir şekilde kısıtladığı" takdirde, ağ tarafsızlığını ihlal ettiği gerekçesiyle 500 bin Euro'ya kadar para cezası verebiliyor. Avrupa Birliği'ndeki düzenlemeye ek olarak Federal Hükümet, Telekomünikasyon Yasası'nda konuyla ilgili değişiklik yapmış ve bu değişiklik geçen Mayıs ayında Federal Konsey'den geçerek yürürlüğe girmiştir.

Amerika'da ise yukarıda değinildiği gibi Federal İletişim Komisyonu (FCC) 14 Aralık 2017'de tartışmalı bir karara imza atarak açık internet uygulamasının kaldırılmasına karar vermiştir. Karar, Temsilciler Meclisi'ne ve Senato'ya gidecek. Eğer bu karar Senato'dan geçerse, sırada Anayasa Mahkemesi var. Yani henüz devam eden bir süreç söz konusu. Yine kararın

peşinden tepkilere Washington Başsavcısı Bob Ferguson sessiz kalmayarak ve konuyla ilgili, *"Ülke çapındaki diğer başsavcılarla beraber, FCC'nin ağ tarafsızlığına karşı bu yasadışı tutumunu dava edeceğim*" açıklamasını yaptı. Anlaşılacağı üzere Ağ Tarafsızlığına ilişkin tartışmalar ABD'de uzun süre devam edecek.

Türkiye'de ise ağ tarafsızlığı konusunda çalışmalar sürmekte olsa da henüz yasal bir düzenleme söz konusu değil. Bu da kimi servis sağlayıcıların gri bölgede gezinmesine ve tartışmalı kimi uygulamalar gerçekleştirmesine sebep olmakta. Örneğin kimi servis sağlayıcıların mobil internet kullanıcılarına belirli servisleri paket dışı tutmasını sağlayan hizmetler satması ya da kendi hizmetlerine bu tarz bir imtiyaz sağlaması, ağ tarafsızlığı ihlalinin sınırlarında gezen uygulamalardır. Bu konuda maalesef henüz bir düzenlemeye sahip olmadığımız için bu uygulamalar serbest bir şekilde devam etmektedir.

Ancak bu noktada tam bir serbestlikten bahsedilemez. Öyle ki, her ne kadar yasal bir düzenleme söz konusu olmasa da Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından TTNET aleyhine verilen 18.01.2012 tarihli ve 2012/DK-59/19 sayılı kararın Türkiye'de ağ tarafsızlığını ihlal konusunda verilen ilk ceza olduğu ileri sürülüyor. Bu kararda, TTNET'in YouTube, İzlesene, Vimeo ve Rapidshare gibi servisleri mahkeme kararı olmaksızın yavaşlattığı veya engellediği vurgulanarak yüklü miktarda para cezasına hükmedildi. Ağ tarafsızlığının ihlali olan bu durum için BTK, yasal dayanak olmadığı halde mevcut yönetmeliklerde var olan erişim sağlayıcı yükümlülüklerinin ihlal edildiği olgusuna dayanıyor.

Ağ Tarafsızlığına Veda Etmenin Sonuçları

Bu düzenlemenin tartışılmaya açılmasından önce ve sonra konu hakkında düzenleme bulunmayan ülkelerde yaşanan birçok ağ tarafsızlığı ihlali bulunmaktadır. Bu ihlallere örnek vermek gerekirse; bazı ülkelerde, yerli içeriklerin yabancı içeriklere nazaran daha güçlü olabilmesi için yabancı sitelerin trafiği yavaşlatılırken, bazı ülkelerde ise müzik endüstrisi baskısıyla peer-to-peer bağlantı sağlayan yazılımlar veya bu iletişimi kullanan protokoller engelleniyor. Bazen güvenlik gerekçesiyle VPN bağlantılar engellenirken, bazen de hâkim durumdaki erişim sağlayıcı şirketler, kendi ürettikleri içerik veya servisleri ön plana çıkarma peşine düşüyor. Bazı ülkelerde erişim sağlayıcılar, diğer içerik sağlayıcılara taşıdıkları içeriğin veya verinin niteliğine göre farklı fiyat uygulama yoluna giderken, içinde Türkiye'nin de bulunduğu bazı devletler, internette zararlı olabileceğini düşündüğü içeriklere erişimin engellenmesinin kamusal bir hak olduğu görüşünde ısrar ediyor.

Nihayet internete tarafsız erişimi garanti altında tutan ağ tarafsızlığının saf dışı bırakılması, internet servis sağlayıcılarının ve devletlerin internetteki belirli içeriklere veya hizmetlere erişimi ücretlendirmelerine ya da engellemelerine sınırsız olanak tanımaktadır. Özellikle erişim sağlayıcıları bakımından belirli içeriklerin ücretlendirilmesi, kısıtlanması ya da tamamen engellenmesi erişim sağlayıcısı şirketlerin ticari ve siyasi çıkarları doğrultusunda olabileceğinden keyfilik söz konusu olacaktır. Diğer bir deyişle, erişim sağlayıcı şirket internet hızımızı keyfi olarak yavaşlatabilir, internette belirli sitelere girmek için bizden ek ücret talep edebilir, belirli konudaki içeriklere ya da hizmetlere erişimimizi tamamen engelleyebilir. Böyle bir durumda, şirket yönetiminin dünya görüşü ve ticari planları ve devlet politikaları bizim internette nelere erişebileceğimizin temel belirleyicisi hâline gelir.

Ağ tarafsızlığının ihlali birçok şekilde örneklendirilebilir. Mesela internet erişim sağlayıcısı şirketin aynı zamanda kendi televizyon servisini tam hızla ve ek ücret talep etmeden verirken; dünyanın en zengin içeriklerini barındıran ve en çok kullanılan televizyon servisleri hızlarını yavaşlatması ya da onları kullanmak isterseniz sizden ek paket ücreti talep etmesi ya da sansürlemesi kaçınılmaz olacaktır.

Benzer şekilde ağ tarafsızlığının olmaması, erişim sağlayıcısı şirketin internet servisini paket servis mantığıyla verebilmesi anlamına da geliyor. Yani size temel paketle belirli bir grup siteye girme hakkı verip, geri kalan diğer servisler için ayrı paketler ve ek ücret talep edebilmesinin de önünü açıyor. Örneğin size sosyal medya paketi almadan Facebook, Twitter ve İnstagram'a giremezsiniz, ya da video paketi almadan Youtube, Periscope izleyemezsiniz diyebilmesi işten bile değildir.

Facebook'un Free Basics projesi bunun en somut örneklerinden biri olarak düşünülebilir. Şöyle ki, Facebook gelişmekte olan ülkelerde pazarlamaya çalıştığı Free Basics projesi ile birlikte gelir durumu düşük insanlara, o ülkelerdeki erişim sağlayıcıları ile anlaşarak ücretsiz olarak 'internet erişimi' sağlamaktadır. Ancak yalnızca Facebook'a ve onlar tarafından seçilmiş belirli sitelere ücretsiz olarak girilebilmektedir. Şayet internet paketi alabilecek gelir durumunuz yoksa, internet sizin için yalnızca Facebook ve bunun izin verdiği sitelerden ibaret olarak kalacaktır.

Söz konusu tasarının tehlikesi ve ağ tarafsızlığının kaldırılmasının neden olacağı tehlikeleri anlamak için web'in nam-ı diğer HTTP protokolünün yaratıcısı Tim Berners Lee'nin ***"Ağ tarafsızlığını kaybetmek, bildiğimiz interneti kaybetmek"*** sözlerine kulak vermek gerekiyor. Hele ki, bu karar internetin icat edildiği, dünyaya yayılmaya başladığı yer olan Amerika'da alınmışsa. Zira Amerika aynı zamanda dünyanın başat kültür merkezi niteliğindedir. Amerika'da yürürlükte olan böylesi bir uygulamanın diğer ülkelerde uygulanması kolay ve hızlı oluyor. Saydığımız bütün bu nedenlerden ötürü sonuna kadar açık internet kuralları ve ağ tarafsızlığının savunulması hayatîdir.

HER 8 KİŞİDEN 1'İNİN PAROLASI BİLİNİYOR!

Geçtiğimiz ay Reddit başta olmak üzere birçok platform üzerinde milyarlarca kişiye ait e-posta adresi ve parola bilgileri yayınlandı.

Artık siber suçluların yanı sıra bu işe yeni başlamış kişiler bile yer altı olarak tabir edilen platformlar üzerinden hassas bilgilere rahatlıkla erişebiliyor. Siber suç salgını katlanarak devam ediyor. Sızdırılan veriler bugüne kadarki en büyük sızıntı olarak kabul edilebilecek cinsten. Toplamda 1 milyarın üzerinde kişinin e-posta adresi ve parola bilgisi yayınlanmış görünüyor. Tehlikenin farkında mısınız?

Yaptığımız inceleme sonrasında bu parola bilgilerinin gerçek sızıntılar olduğunu ve doğru bilgiler içerdiğini onayladık.

Sızıntı hakkında

41 GB boyutuna sahip liste, 5 Aralık 2017 tarihinde bir forum sitesinde yayınlandı. Listenin son olarak 29 Kasım 2017 tarihinde güncellendiği gözlemlenirken toplamda yayımlanan kullanıcı adı ve parola bilgisi sayısının 1 milyar 400 milyon 553 bin 869 olduğu görülmektedir.

Veriler daha hızlı aratılabilmesi amacıyla parçalanmış ve alfabetik olarak ağaç yapısına dönüştürülmüştür.

Bugüne dek yaşanan veri sızıntıları arasında bu sonuncunun en büyük veri sızıntısı olduğunu rahatlıkla söyleyebiliriz. Şöyle ki bundan önce gerçekleştirilen en büyük sızıntı yaklaşık 797 milyon olan Exploit.in Combo listesine aitti. Yeni gerçekleşen sızıntı ise neredeyse bu sızıntının iki katı büyüklüğündedir.

Bu sızıntı Anti Public, Exploit.in gibi bilinen listeleri içerdiği gibi LinkedIn, Pastebin örnekleri gibi daha da küçük sızıntıları içeren toplam 252 listeden harmanlanmıştır. Yayınlanan bu listede Anti Public ve Exploit.in sızıntılarına 385 milyon yeni kullanıcı adı ve parola bilgisinin eklendiğini görülüyor.

Önemli sızıntı listelerini sizler için derledik.

```
2017-08-09: d4a0359bdb8b5f65119a6d1561c0d636ca64e19ffa9371ad797bd7086ee3927b  ./inputbreach/330k.txt     11M
2017-08-09: ab11e98ec937160da094cfb5211dad4b75a73727f0dfaad29410462fa4244f1c  ./inputbreach/500k+ComboList[Netflix,Paypal.Origin.Amazon].txt     3.1M
2017-08-09: 74be21c25cfa46e6ba82c5cd04dc64b03937deb554c61843dbbd80d92df3186f  ./inputbreach/accounts.txt     9.9M
2017-08-09: 52548fdf7cc735bf1bdad8b3448ccef864b60e384e63eaa59c4d7f8a30d71a43  ./inputbreach/FRESHOVER1,2+M.txt   40M
2017-08-09: f7c1579e5fe77dfc4c92264727c99e969a923e815d1793d3e6d0e6d17a8cbb19  ./inputbreach/gmail.com    23M
2017-10-02: 52f640e95015bb060eb075fe2ac88776395e2e38cd13972ad251f3d81ae89296  ./inputbreach/000webhost_13mil_plain_Oct_2015_filtered.txt     484M
2017-10-02: 2852052b0636cb590eb00b6d6808e0c1a4660b9473931e59b92b212d2a825d0e  ./inputbreach/surgeryu.com-641009_surgeryu.users_30.10.2016.txt    36K
2017-11-08: ea499b03d11cb000c97cc6d19c55c48e0dded56e59f41a2fcf80d2c4239cb950  ./inputbreach/10workingminecraftaccounts.txt  4.0K
2017-11-08: 27426d4e35547a54514a404a5c18bbfb8e05e44d42bb7c5fe8767d4f41ee517a  ./inputbreach/1394store.com_LEAKED_DATABASE_filtered.txt  612K
2017-11-08: d4014c9281d74f2b3853fc2398a8fbf6cod447919d3a0d44e1287a20e5e1f415  ./inputbreach/36kmember_filtered  1.1M
2017-11-08: 5a5f58c957935642422255abd9e26b318f921f47b4093d2eaf8f57ff44c6ae22  ./inputbreach/7k7k     201M
2017-11-08: 56e2fa4a0708b83b3bd9506e31ea698e3ad1f37065a34661f7c8819d1617e087  ./inputbreach/99fame.com_filtered.txt 36K
2017-11-08: 716e7b552c9cc14f90b6cf74067a9adc5faa6144288be0688dd262b98e201ad6  ./inputbreach/Alancristea.txt 8.0K
2017-11-08: 5fb0135d6a98a54c61fa08341960bbc943601a3c9cfb0372b1185bc9557b632a  ./inputbreach/Balancek.txt     168K
2017-11-08: bdc490aabd0c10ea711b67b0a4b9038723ebd89eec5c3ac2346bc21b2bb0c4f8  ./inputbreach/Barbelith_Users_credentials_filtered     208K
2017-11-08: cfd492442dc17b2587436383b1bf8bcb780b3112106b958979995735d656be07  ./inputbreach/BitcoinLixter_filtered.txt  92K
2017-11-08: 4f50ace9bfa563f50bf2c14e799e6cb1ac0ab46a2c29e093657a2afafda27226  ./inputbreach/CSGameServs.Com.txt 504K
2017-11-08: 44d94d26841ccceb6d0ee03d4863b6e6079fce4d18ac389b416e29d72367cc53  ./inputbreach/DBDBDB_filtered 760K
2017-11-08: f62e7922a1b71f26ebd6176748e3f6bdb9bf7a10dee5bca587915d08c2bd72fd  ./inputbreach/Delicious_Takoyaki_filtered.txt 2.8M
2017-11-08: 833b2b89425399187a064a4d3d439c5c702a5c2faba057d8bfaee56943bc916e  ./inputbreach/Fling_filtered  1.3G
2017-11-08: f149ebd26038acc1e892d45fda51806f36e18143ac694648a9d65a66961b52c4  ./inputbreach/LulzSecDelivers_filtered.txt     760K
2017-11-08: e2611cf0657b29476a306dd571180dd947be6c3df086bd243456920ff2ddf068  ./inputbreach/RuneScape2k15_filtered  2.8M
2017-11-08: cf83b090996e37fcdb1861b1f2f98dccbdcca7a729885beba561e976809af460  ./inputbreach/WEBS_filtered   328K
2017-11-08: b75a42d0dc01c1a9a839a179b8d05867f0624195b69dd58480bfad14e592e581  ./inputbreach/myspace.sorted1 1.1G
2017-11-08: 495d7bc8ab6d49cb298cd031cbac9fe82d959f5e3503a8781371b91683434349  ./inputbreach/myspace.sorted10    1.1G
2017-11-08: b5536c830b3171ec7e1041eba4a4064ee9a4fc6daa3d9982761f14ad17532242  ./inputbreach/myspace.sorted2 1.1G
2017-11-08: ec8b6c21b2dc1657f205b111675de9d61913f20c786ec1059ae2607cf559361a  ./inputbreach/myspace.sorted3 1.1G
2017-11-08: ef67ecc976b4248c2ab941757c6a45fec324d0788300ccddb6eae1b87bcc9899  ./inputbreach/myspace.sorted4 1.1G
2017-11-08: 5fe59f766c61a4583546771871fa7c2c49ac671b64ca4fc89102f85522ace4aa  ./inputbreach/myspace.sorted5 1.1G
2017-11-08: fb8bbbfc625860852f9daac0f6667c3391414a0475aa9037f9b05c6bcb0e9261  ./inputbreach/myspace.sorted6 1.1G
2017-11-08: dc23bd7a1f70b7352d15518d68c095a27d4c4524fa36a3031155d5eed11de8fa  ./inputbreach/myspace.sorted7 1.1G
2017-11-08: b8c9de47be886e584ee74b0d9c1dd00a8ca59e423faeed02c16a8ea8012abc42  ./inputbreach/myspace.sorted8 1.1G
2017-11-08: 5a7b01a4e58a8366c29544b61d0e8cd16e98f0bbee49d535ce9a121850984710  ./inputbreach/myspace.sorted9 1.1G
2017-11-08: 0399b86ace44f91608c6499790c8a01ffd43260f61b2801cf80cbad3b32f0283  ./inputbreach/plaintxt_yahoo_voices_filtered.txt  14M
2017-11-09: 0c0daf85728a36601f20fee06da376e93d411d932540e9944df3bcf9cf0b3402  ./inputbreach/badoo.sorted1   896M
2017-11-09: 8f77ce122d8df9de1cb05d9ef9aa1e6b22727b6f763a95fbec179a00396678f0  ./inputbreach/badoo.sorted2   896M
2017-11-09: f1ece7b51a01e71f7d6d4a6d8093978882d03b2e0e7fa407981b8491843c7075  ./inputbreach/badoo.sorted3   896M
2017-11-09: 8d35ade99d5ca947f15a2116f0b270a7545e5d0fa61dff233decb791a9ab4129  ./inputbreach/badoo.sorted4   896M
2017-11-18: c030f1caac244304b4eda17b2771cb38f5ad4cdd64157d4426c9e230edd2edf3  ./inputbreach/linkedin110M_1  865M
2017-11-18: 6925d41d3d5bcbc796687af3e7f46cbcc6f4192299883770b25ddbedc739013f  ./inputbreach/linkedin110M_2  865M
2017-11-18: ca9737346546549999df7315ad5d2c4696d1372ce88dcf47bd955cc07f942637e  ./inputbreach/linkedin110M_3  865M
2017-11-18: 577163f674f8b4e192329dbe3ac2fceff342a72b6a17a5c864824688761c5ace  ./inputbreach/linkedin110M_4  865M
2017-11-19: 484ab8696224a7b5780e107d872f8203c656d81b241ca6aa594027db9e6eb920  ./inputbreach/taobao  409M
2017-11-19: 14423bb83eb099b859756ae1c56eff58497db33bd805a386c08d2ae8fb3a5213  ./inputbreach/xsplit_sorted   91M
2017-11-19: f409e63a064e0dd241a9e8d9228f1538fb3cc443f0f2aeb1e20f2d1f4371d6ba  ./inputbreach/zoosk_sorted1   811M
2017-11-19: 2b767c72a259ccf35596788a1846e1dd586fd66b6bb56a3cafd097d1f520cce0  ./inputbreach/zoosk_sorted2   811M
```

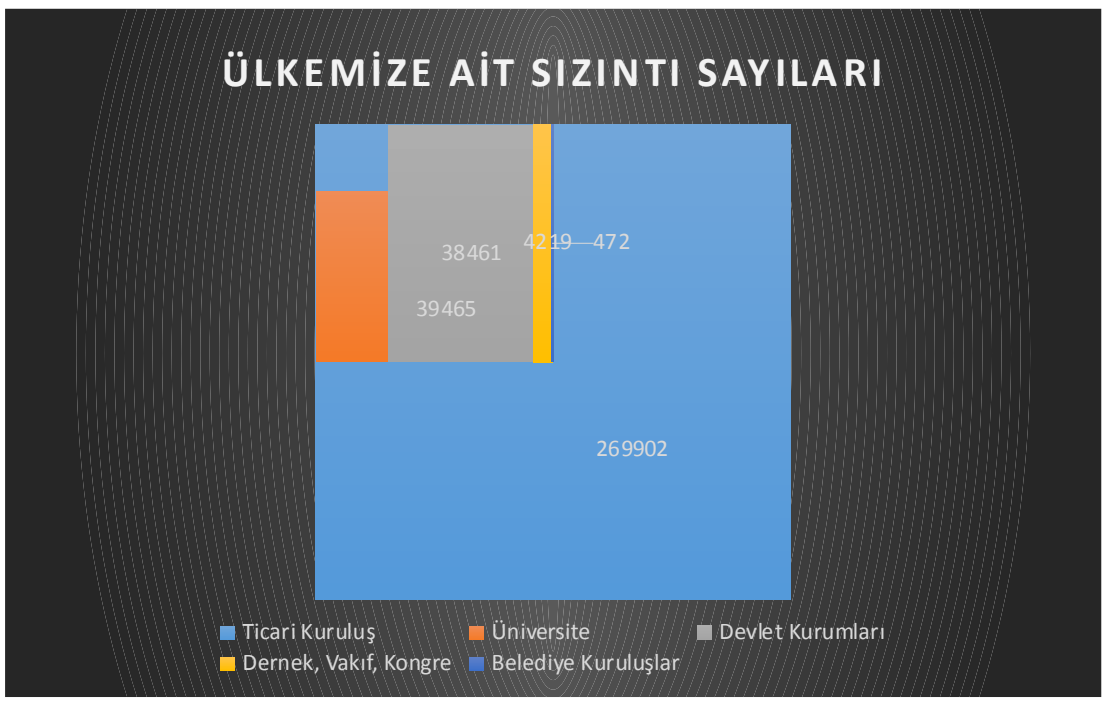
DOSYA	BOYUT
VK_100M_EMAILpass.txt	2,8 GB
1000000yandex.txt	100 GB
linkedin110_1.txt	865 MB
linkedin110_2.txt	865 MB
linkedin110_3.txt	865 MB
linkedin110_4.txt	865 MB
myspace.txt	11 GB

En Çok Kullanılan Parolalar

#	ADET	PAROLA
1	9.218.720	123456
2	3.103.503	123456789
3	1.651.385	Qwerty
4	1.313.464	password
5	1.273.179	111111
6	1.126.222	12345678
7	1.085.144	abc123
8	969.909	1234567
9	952.446	password1
10	879.924	1234567890

Sızdırılan veriler içerisinden ülkemize ait görünen adresleri incelediğimizde hatırı sayılır bir rakam ile karşılaşıyoruz. Tüm ülke vatandaşlarımızın bu anlamda parola bilgilerini güncellemelerini tavsiye ediyoruz.

Ülkemiz alan adlarına yönelik ".TR" yaptığımız çalışma sonrasında **1,112.197** adrese ulaştık. Bu kayıtlara ilişkin istatistikleri aşağıdaki şema ve tablolarda görebilirsiniz.



Ülkemize ait sızıntı sayıları

EN ÇOK KULLANILAN PAROLA BİLGİSİ (METİN)	
1	ankara
2	zeynep
3	istanbul
4	sanane
5	fenerbahce
6	mustafa
7	mehmet
8	cimbom
9	galatasaray
10	fenerbahce

EN ÇOK KULLANILAN PAROLA BİLGİSİ (ALFA NUMERİK)			
1	abc123	9	1234qwer
2	1q2w3e4r	10	q1w2e3r4
3	1q2w3e4r5t	11	a123456
4	123qwe	12	zxcvbnm
5	qwerty123	13	123456789a
6	qwe123	14	1234we
7	qwerty1	15	asd123
8	qazwsx	16	12345a

EN ÇOK KULLANILAN PAROLA BİLGİSİ (SAYISAL)					
1	123456	11	987654321	21	212121
2	123456789	12	666666	22	19071907
3	12346789	13	123321	23	987654
4	12345	14	159753	24	159357
5	111111	15	555555	25	102030
6	123123	16	123654	26	131313
7	1234567890	17	14531453	27	999999
8	654321	18	123123123	28	11111111
9	112233	19	7777777	29	333333
10	121212	20	222222	30	777777

Sonuç olarak sızdırılan listeyi kontrol amaçlı rastgele kişilerden aldığımız e-posta adresleriyle yaptığım inceleme sonrasında %90 oranında doğruluk sağladığı, çıkan sonuçlar içerisinde yer alan parola bilgisinin daha önce kullandığı/kullanmakta olduğu sonuçlarını elde ettik.

ÖNEMLİ: Bu sızıntı bizlere bir kez daha aynı parolanın farklı platformlarda kullanılmaması, parola serileri oluşturulmaması ve farklı platformlar için farklı parola tanımlamalarının ne kadar elzem olduğunu hatırlatıyor. Parola bilginizin sızdırılma ihtimaline karşın 2FA olarak bilinen iki aşamalı kimlik doğrulamayı etkinleştirmenizi öneririz.

SANAL DÜNYA, GERÇEK TEHDİTLER

abaküs

UYGULAMALI
Siber Güvenlik ve Hacking

Mustafa ALTINKAYNAK

- Siber Güvenliğe Giriş
- GNU/Linux Temelleri
- Kriptoloji
- Web Uygulama Güvenliği
- OWASP
- Burp Suite
- Sistem Güvenliği
- Ağ Güvenliği
- WEP/WPA/WPA2 Cracking
- Tersine Mühendislik
- Cracking
- BadUSB

abaküs

Parolalarınızı Tek Bir Yerden Yönetin: KeePassXC

İmparatorluğun Anahtarı: Parolalar!

Dijital varlıklarımız çok önemli. Fotoğraflarımız, videolarımız ve bunun gibi hassas verilerimizi sakladığımız servisler, Kırk Haramiler'in altınlarını sakladıkları mağara misali, kapılarını ardına kadar açmaya hazır: Açıl susam açıl!

İbretlik bir hikâye olduğunun farkındasınız. Ama gerçek bundan farklı değil. Dijital varlıklarımız söz konusu olduğunda, "açıl susam açıl" parolasından daha basit parolalar seçebiliyoruz. Maalesef, **123456** hâlâ en çok kullanılan parola. Sadece 2017 yılı için değil, 2016, 2015, 2014 yıllarında da en çok tercih edilen parola 123456 idi. Uzun yıllardır listedeki yerini şaşırtıcı bir biçimde kuruyor.

Peki güçlü parolaları nasıl seçeceğiz. Bunun bir kıstası var mı?

Güçlü bir parola seçseniz dahi, muhtemelen güç bela seçtiğiniz ve akılda tutmak için bin bir yola başvurduğunuz parolalarınızı, farklı servislerde / sitelerde de aynı biçimde kullanacaksınız. Dolayısıyla kullanmış olduğunuz servislerden biri şayet hacklenirse, burada kullandığınız parolayı elde eden saldırganlar, "password reuse attack" denilen yöntem ile, kullanıcısı olabileceğiniz / olduğunuz diğer sistemlerde de aynı parolaları deneyeceklerdir. Evet, maalesef bu olay kırk yılda bir vuku bulabilecek ender bir olay değil, bugünün dijital dünyasında bir vaka-ı adiye! Facebook CEO'su Mark Zukenberg'in hesaplarının çalınması hadisesi, aynen bu biçimde gerçekleşti. Linkedin'in hacklenmesi ile ifşa olan hesaplar arasında Mark'ın da hesabı vardı. Mark 25 saniye içersinde hacklenebilecek "dadada" gibi basit bir parola kullanmaya ek olarak, Pinterest, Twitter gibi servislerde de aynı parolayı kullanıyordu.

Geldiğimiz noktada servisler, üyelik esnasında güçlü parolalar seçilmesi konusunda kullanıcılara yönergeler sunuyor. Hatta bu parola politikalarını üyelik aşamasında dayatan servisler dahi mevcut. Fakat bu en iyi ihtimalle kullanıcının bu "güçlü" parolayı, güvensiz yöntemlerle saklamasına, örneğin bir post-iti ile monitörüne yapıştırmasına, bir ajandaya kaydetmesine neden oluyor. Bunun için icat edilen ajandalar dahi var.

Yazımızın konusu ise hem güçlü parololar seçmek hem de bunları güvenli bir biçimde saklamamıza yardımcı olacak, multi platform bir uygulama: KeePassXC. Bu yazıda KeePassXC'yi tanıyacak, kurulum ve kullanımının ayrıntılarına değineceğiz.

KeePassX tüm parolalarımızı tek bir yerde saklayıp yönetmemize yarayan, Windows, Linux, MacOS X gibi farklı platformlarda kullanabileceğimiz bir parola yöneticisi.

Parola yöneticileri farklı site ve servisler için, farklı parolalar oluşturabileceğimiz, bunları ezberlemek zorunda bırakmaksızın, saklayıp ulaşılabilir kılan harika programlardır. Siz sadece master password denilen, ana parolayı hatırda tutmakla mükellefsiniz. Ana parolanın girilmesinden itibaren parola yöneticisi, şifreli bir biçimde sakladığı diğer servislere ait parolalarınıza ulaşmanızı sağlar. Kullanışlı arayüzleri sayesinde sadece tuş kombinasyonları ile parolalarınızı parola yöneticisiden alıp, hedef site/servise girmenizi kolaylaştırır.

Muhtemelen KeePassX, KeePassXC, KeePass, KeePass2 gibi birbirine benzeyen pek çok program ismine rastladınız. Bunların bazıları aynı kod üzerine bina edilen programlarken, diğerleri de sadece aynı veritabanı formatını kullanmaktadır. Biz bu yazı ile birlikte çoklu platform desteği ve alternatiflerine göre daha aktif bir geliştirme grafiği olduğundan KeePassXC'ye hususi bir yer ayırdık.

Bir parola yöneticisi kullanmak sadece sizin değil, saldırganların da dikkatlerini tek bir yöne çekecektir. Nitekim Kevin Mitnick son kitabı Görünmezlik Sanatı (The Art Of Invisibility) 'nda girdiği bilgisayarlarda nasıl KeePassX programını, kendi derlediği binary ile değiştirerek master passworde eriştiğinin ayrıntılarını paylaşıyor. Araştırmaların da ortaya koyduğu şekilde, yaygın olarak kullanılan parola yöneticileri zafiyetler içerebiliyor. Bu sebeple doğru aracı seçerken, titiz davranmakta fayda var.

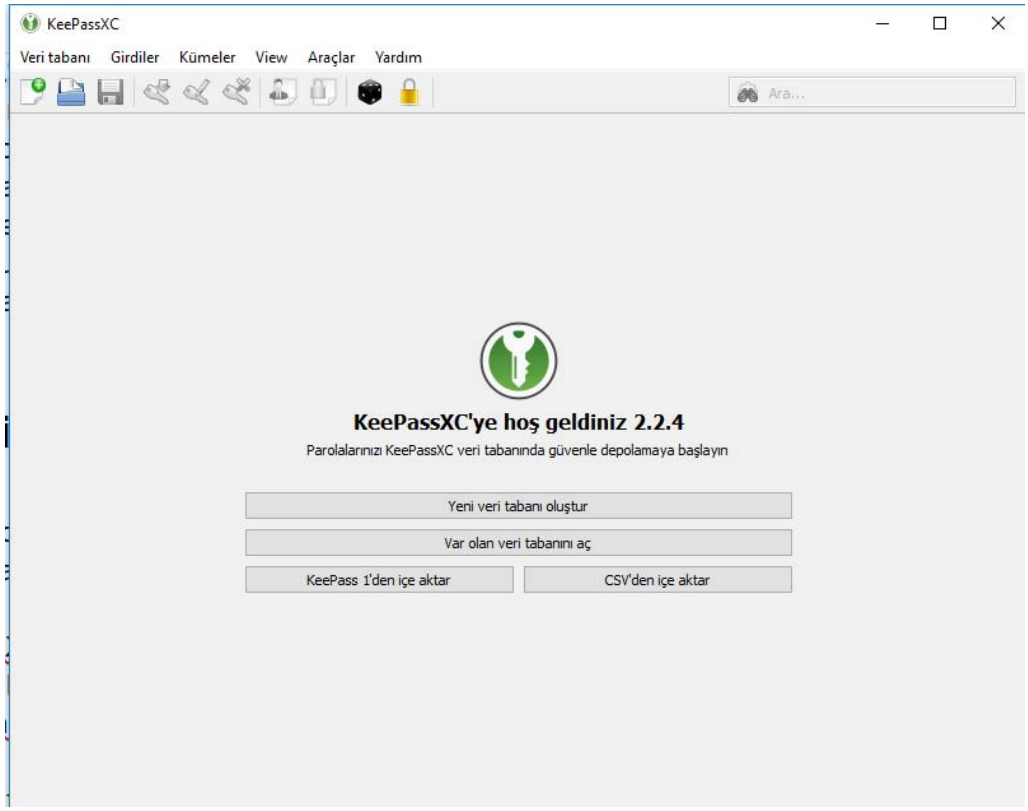
KeePassXC'nin Windows, Mac ya da Linux işletim sistemleri için kurulum dosyasını https://keepassxc.org/download adresinden indirebilirsiniz. KeePassXC, Windows 7 ve üzeri işletim sistemlerinde, MacOS x 10.7 ve üzeri sistemlerde ve pek çok Linux dağıtımında sorunsuz çalışmaktadır.

KeePassXC Nasıl Çalışıyor?

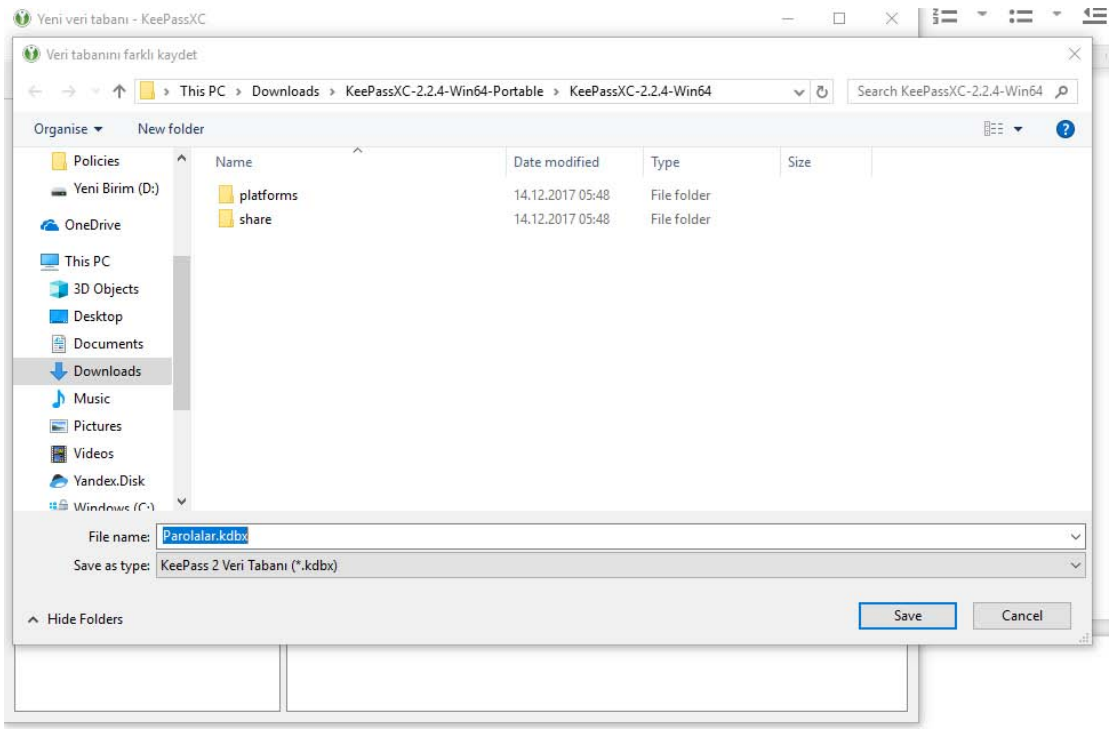
KeePassXC, tüm parolaları saklayan bir veritabanı dosyası ile birlikte çalışmaktadır. Bu veritabanı bilgisayarınızda şifreli bir biçimde saklanmaktadır. Şayet bilgisayarınız çalınırsa, bu veritabanındaki bilgiler okunamayacaktır. Yukarıda bahsettiğimiz master password, ana parola bu veritabanının şifrelenmesinde kullanılmaktadır. Omuzlarınızdaki yegâne görev imparatorluğun anahtarı demek olan bu master password'u seçerken, olabildiğince titiz davranmak ve güçlü bir parola seçmek. Bunun dışındaki tüm operasyonu KeePassXC yönetecek. Tersinden ifade edersek, master password 'ü yani imparatorluğun anahtarını ele geçiren biri, bu veritabanında saklanan diğer tüm passwordlerinizi de elde edecektir.

Haydi Başlayalım!

Yukarıda indirme bağlantısını verdiğimiz adresten KeePassXC dosyasını indirdikten sonra kurulum dosyasını çalıştırıyoruz. Yönergeler takip edilip, kurulum bittikten sonra da KeePassXC uygulamasını çalıştırıyoruz.

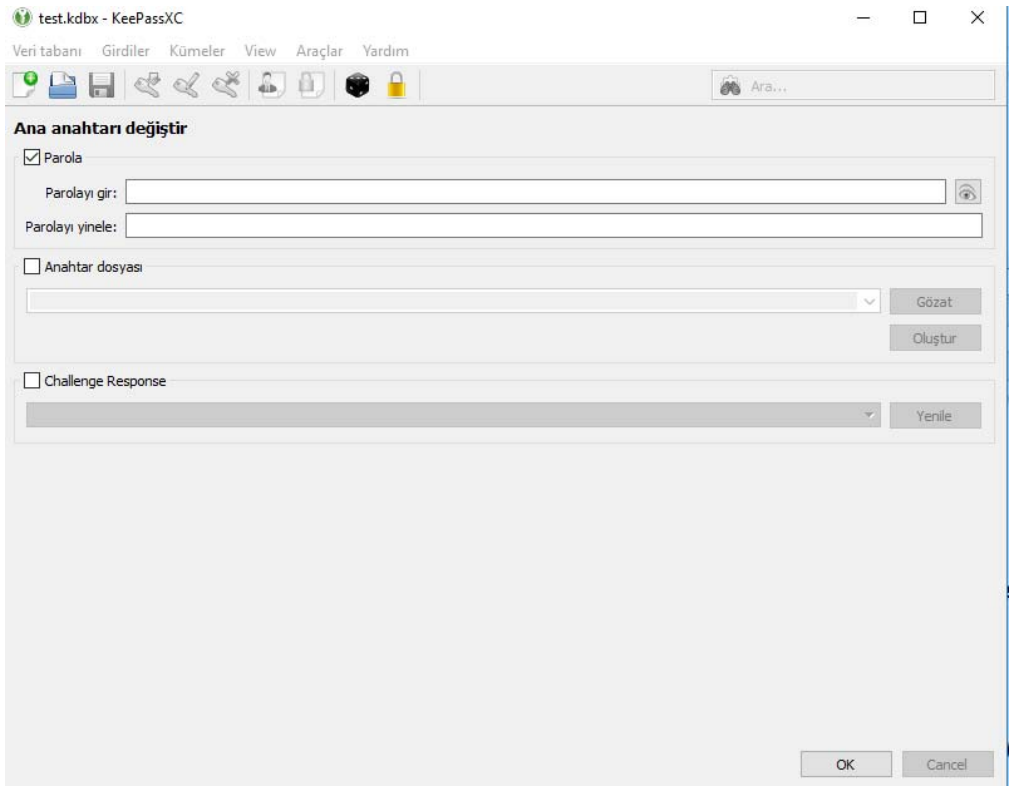


KeePassXC'yi ilk kez kullandığınızı varsayıyoruz. Dolayısı ile bir parola veritabanı oluşturacağız. Bizi karşılayan ekranda "Create new Database" butonu tıklandığında, kaydedeceğimiz parola veritabanının adını ve kaydedileceği dizin yolunu soran bir ekran ile karşılaşacağız.



Parola veritabanımıza uygun bir isim verip, kaydedileceği dizini de seçtikten sonra Save butonuna tıklayabiliriz. Parola veritabanınızı daha sonra HDD'nizde herhangi bir yere, hatta başka bir PC'ye bile taşıyabilirsiniz.

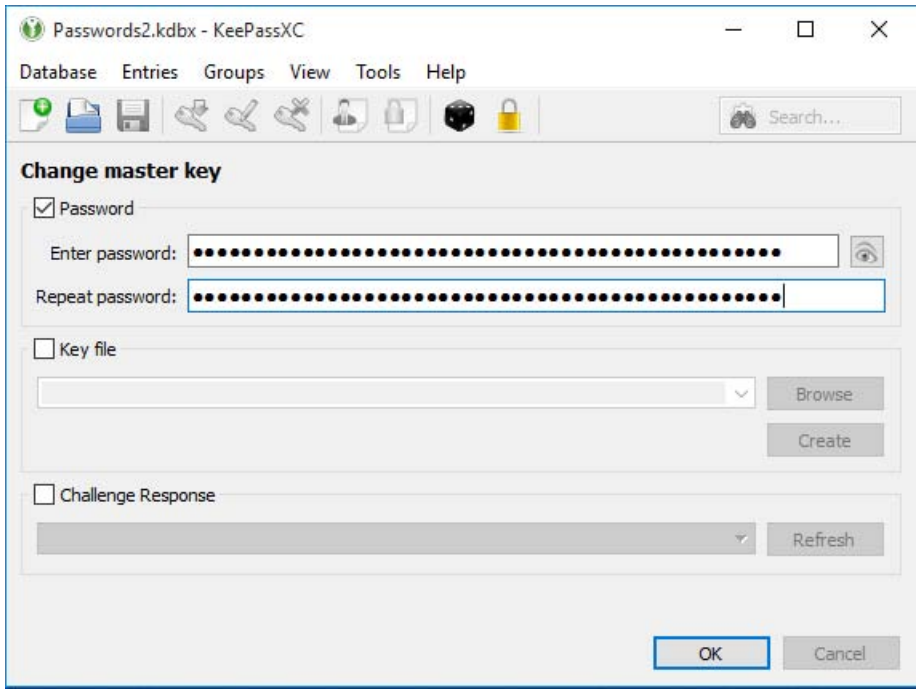
Save butonunu tıkladıktan sonra sizi yeni girdiler bekleyen bir ekran karşılayacak:



Parola alanı, yukarıda bahsettiğimiz, parola veritabanını koruyacak olan masster password'ün belirtildiği alan. Parola kutusuna seçtiğiniz parolayı girdikten hemen sonra Parola Yenile kutusuna da aynı parolayı tekrarlamalısınız. Girdiğiniz parolayı görüntülemek için parola kutusunun sağında yer alan göz ikonuna tıklayabilirsiniz.

Anahtar Dosyası (Keyfile) Nedir?

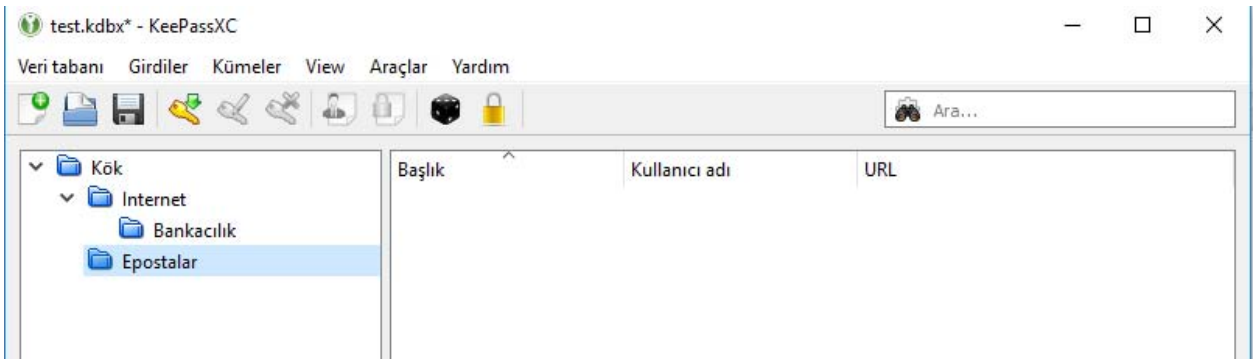
Master password ile birlikte bir de Anahtar Dosyası kullanmak, parola veritabanının ele geçirilmesi durumunda deşifre etmek isteyen kişinin işini iyice zorlaştıracaktır. Var olan bir dosyayı anahtar dosyası olarak kullanabilirsiniz. Örneğin sevimli bir kedinin fotoğrafının bulunduğu image tipinde bir dosyayı anahtar dosyası olarak kullanabilirsiniz. Anahtar dosyası seçerken dikkat etmeniz gereken en önemli husus, bu dosyanın üzerinde kesinlikle değişiklik yapılmaması gerektiği. Şayet dosya içeriği değişirse, parola veritabanınıza bir daha erişemezsiniz. Unutmayın! Keyfile olarak herhangi bir dosyayı kullanabilirisiniz demiştik. Dosya değişikliği uyarısı ile birlikte şunu da hatırlatmakta fayda var. Bu söz konusu anahtar dosyasını, şirin bir kedinin fotoğraf dosyası örneğin, bir image görüntüleyici ile açmak dahi dosyayı modifiye edebilir. Dolayısıyla anahtar dosyası (keyfile) olarak kullanacağınız dosyanın ismini değiştirerek, bir yedeğini alıp ancak bu şekilde kullanmanızı öneririz.



Parola veritabanımızı oluşturduk. Şimdi KeePassXC'nin sunduğu imkanlara bakalım.

Parolalarınızı Organize Edin / Gruplayın

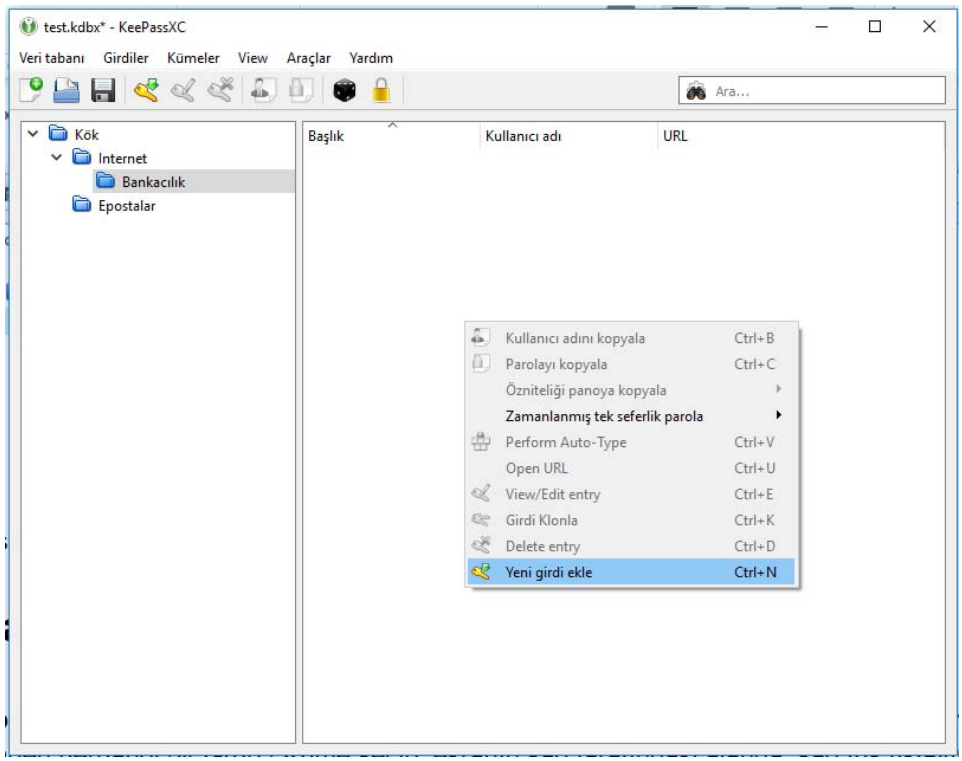
KeePassXC, parolarınızı Groups altında (Türkçe çeviride Kümeler olarak göreceksiniz) gruplamanıza imkân vermektedir. KeePassXC ile parola grupları oluşturabilir, silebilir, düzenleyebilir, gruplara alt gruplar ekleyebilirsiniz. Bunu yapmak için ekranın üstünde yer alan Kümeler (Groups) menüsünü kullanabilir ya da sol taraftan ilgili grubun / kümenin üzerini sağ tuşla tıklayarak, açılan context menüden seçebilirsiniz.

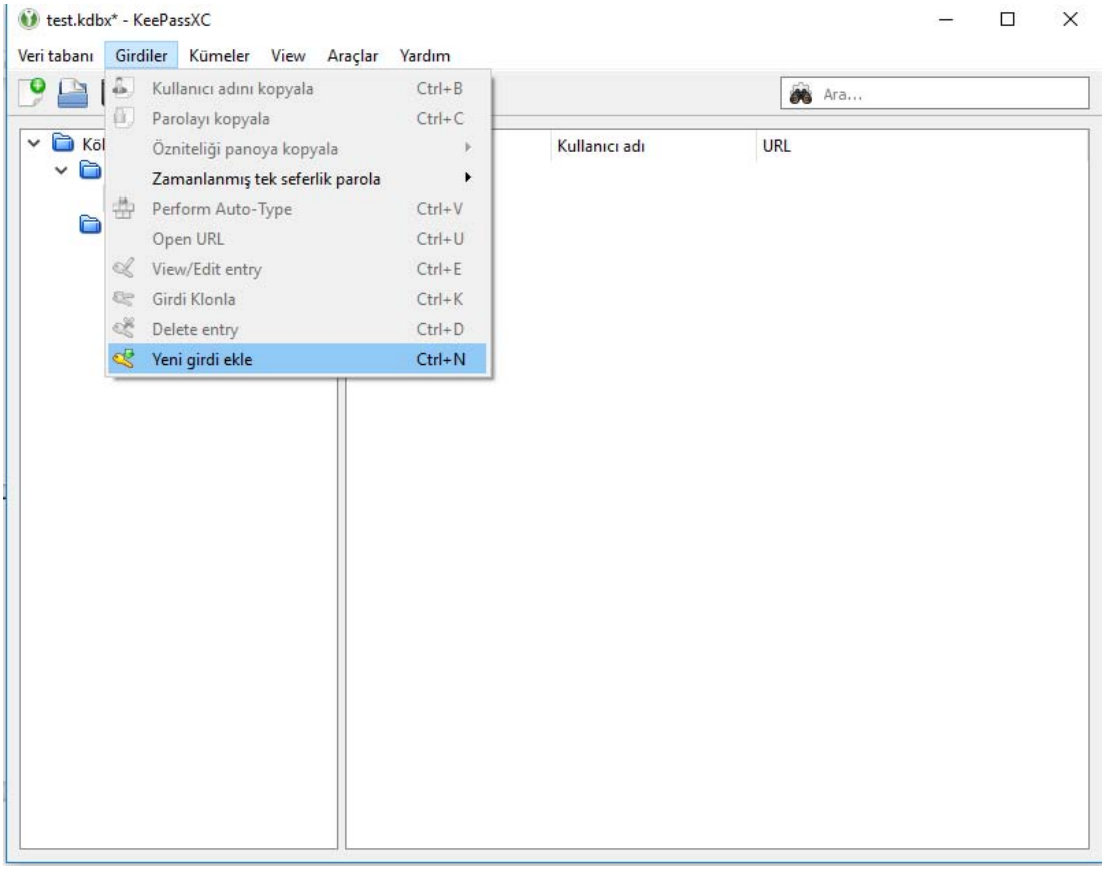


Groups / Kümeler özelliği, KeePassXC 'nin işleyişini etkilememektedir. Yalnızca kullanıcıya kolaylık sunmak açısından parolaları görsel olarak gruplamayı sağlamaktadır.

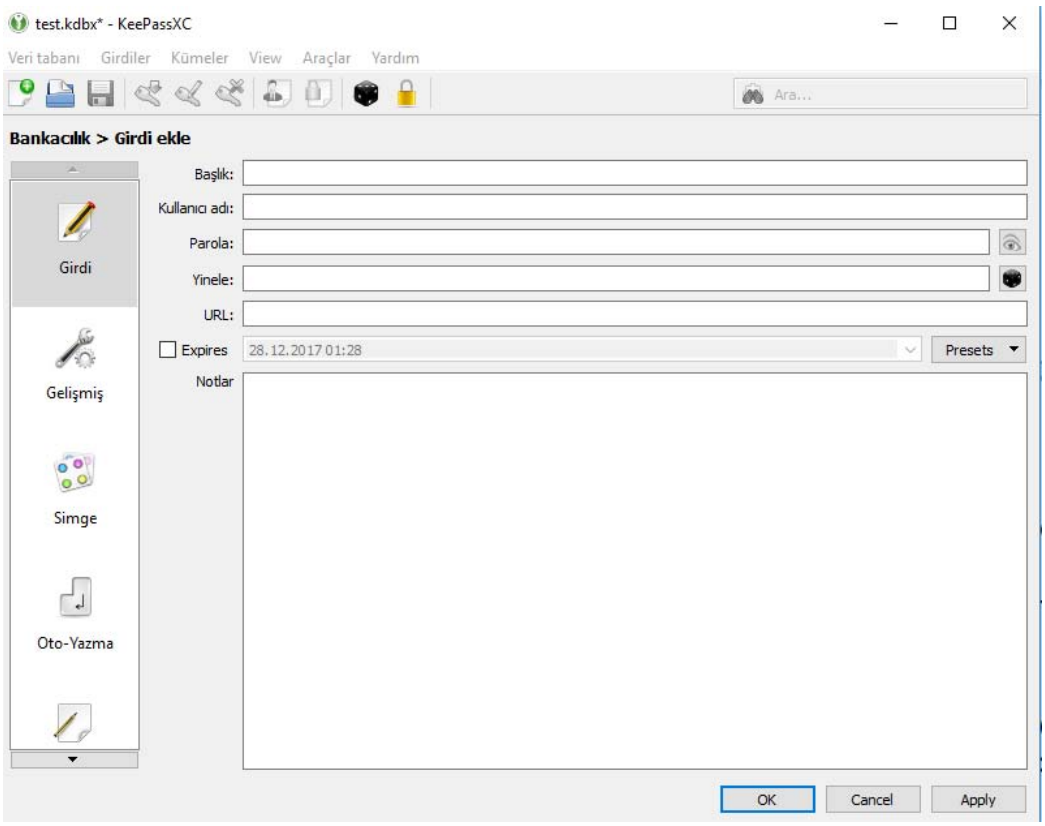
Parolaları Oluşturmak, Düzenlemek ve Saklamak

Yeni bir parola oluşturmak, ya da hâlihazırda var olan bir parolayı saklamak için Group / Küme menüsünden herhangi bir Grup / Küme seçip, ekranın sağ tarafındaki alanda sağ tuş tıklayıp, açılan menüden Add New Entry / Yeni Girdi Ekle'yi seçebilir ya da ekranın üst kısmında bulunan Entries / Girdiler menüsünden Add New Entry / Yeni Girdi Ekle'i seçebiliriz.

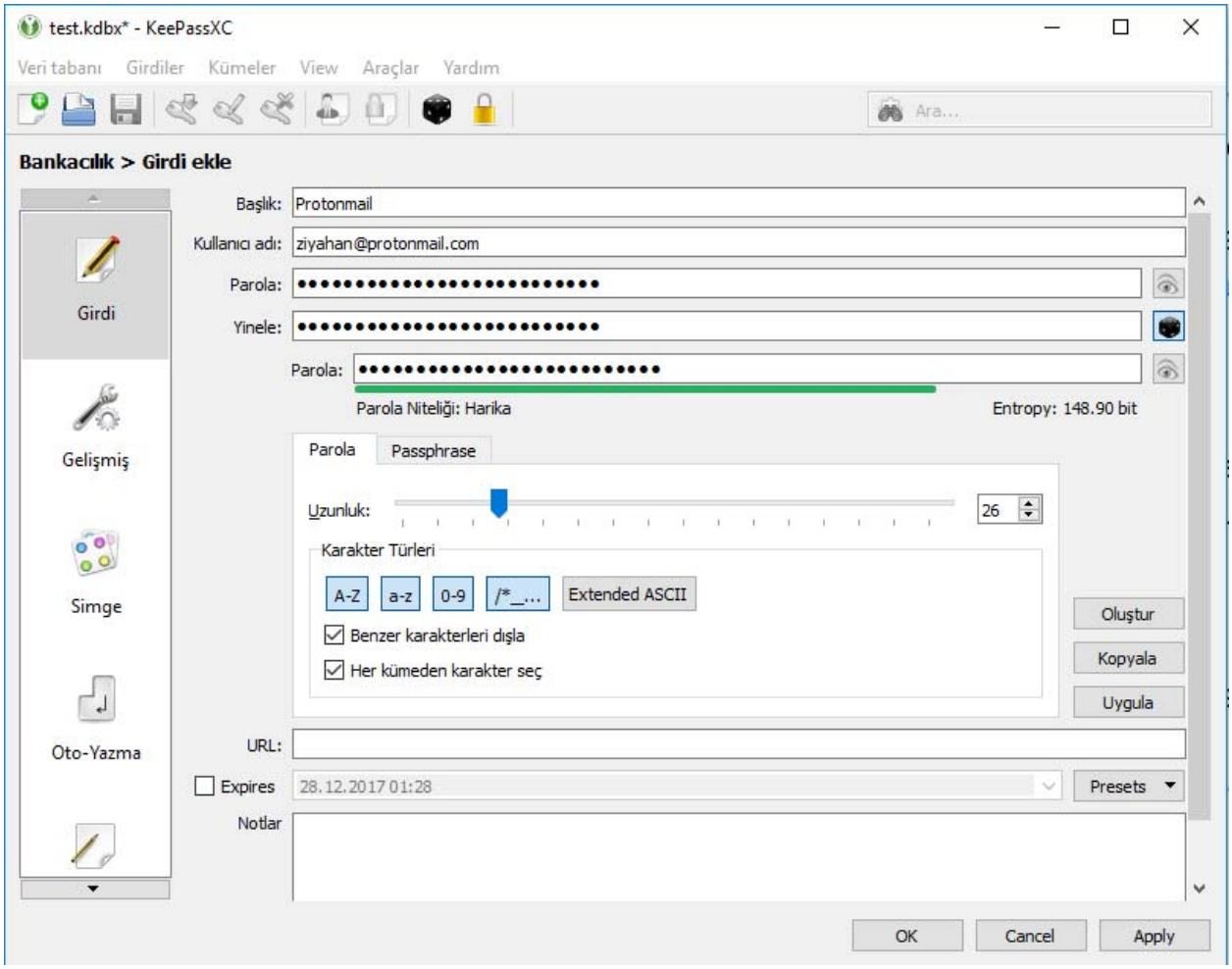




Aşağıdaki gibi bir ekran bizi karşılayacak:



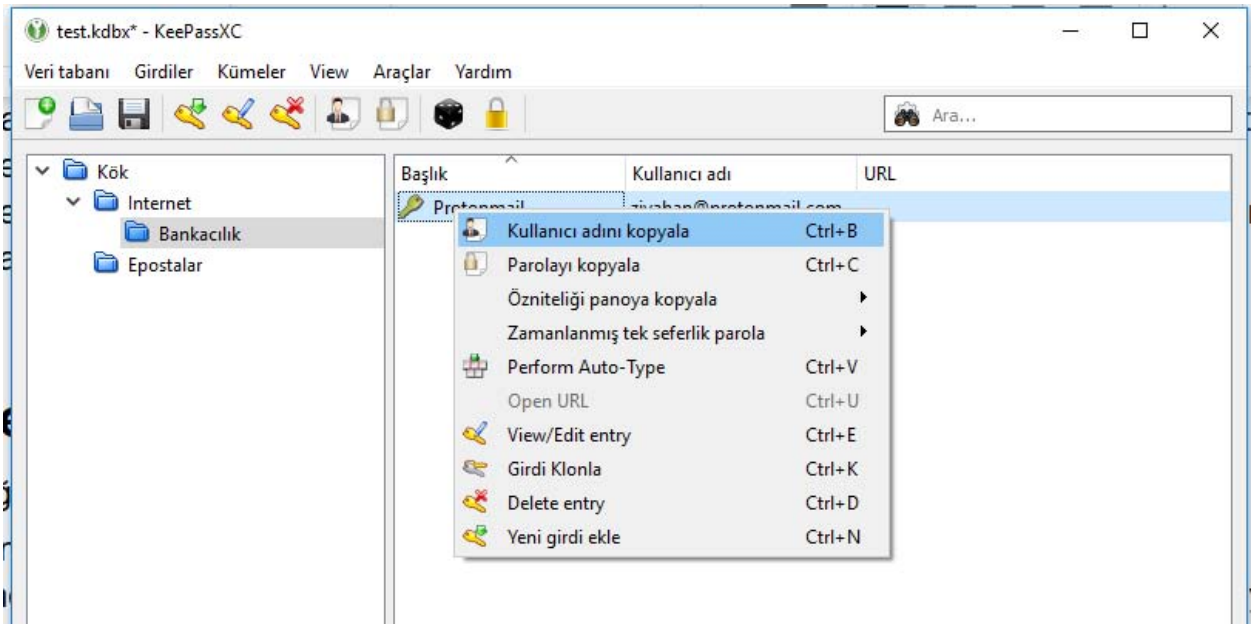
- Title / Başlık alanına bu parolayı sizin için tanımlayan bir değer girebilirsiniz. Örneğin *ProtonMail Hesabım* gibi parolayı kullanacağınız servis ya da web sitesinin adı olabilir.
- Kullanıcı Adı / Username alanına bu parola ile ilişkili kullanıcı adı bilgisini girebilirsiniz. Şayet bir kullanıcı adı yok ise, bu alanı boş bırakabilirsiniz.
- Parolanızı Parola / Password alanına girerek, hemen altındaki kutuya parolanın aynısını yazmalısınız. Şayet bu servis için hâlihazırda bir parolanız yoksa ve KeePassXC'yi kullanarak bir parola oluşturmak istiyorsanız sağdaki zar ikonunu tıklayarak, yeni parola oluşturma sihirbazını açabilirsiniz.



- Genellikle yeni bir servise/siteye kayıt olurken bu özelliği kullanacaksınız. Böylece bu servis ve siteler için istenilen formatta ve güçlükte şifreleri kolaylıkla oluşturabileceksiniz. Üstelik KeePassXC'in sunduğu en önemli avantaj ile bunları akılda tutmak ya da bir yere not etmek zorunda kalmayacaksınız. Parola oluştururken, uzunluk, parolanın içereceği karakter tipleri (harf, sayı, özel karakter) belirtebilirsiniz. Şayet KeePassXC'nin oluşturduğu parola gözünüze hoş görünmezse Generate / Oluştur butonuna tıklayarak belirttiğiniz kriterlere sahip başka bir parola oluşturulmasını sağlayabilirsiniz. Oluşturulan parola Uygula butonuna bastığınızda hem parola kutusuna hem de parola yenileme kutusuna KeePassX tarafından yazılacaktır.
- Girdi alanları uygun değerlerle doldurulduğunda OK butouna basabilirsiniz. OK tuşuna basmanız ile birlikte bu oluşturulan yeni parola, parola veritabanına yazılacaktır. Değişikliklerin kaydedildiğinden emin olmak için File > Save Database ya da Veritabanı / Veritabanına Kaydet seçeneklerini kullanabilirsiniz. Kayıt esnasında bir yanlışlık yaptığınızı düşünüyorsanız parola veritabanın kapatıp tekrar açabilirsiniz. (Veritabanı -> Veritabanını Kapat) değişiklikler kaydedilmeden silinecektir.

Kaydettiğimiz Parolayı Kullanalım

Kaydettiğimiz parolayı kullanmak için, ilgili girdi üzerinde sağ tuş tıklayıp Kullanıcı Adını Kopyala (CTRL+B tuş kombinasyonları kullanılabilir) ya da Parolayı Kopyala (CTRL+C tuş kombinasyonları kullanılabilir.) seçenekleri kullanılabilir:



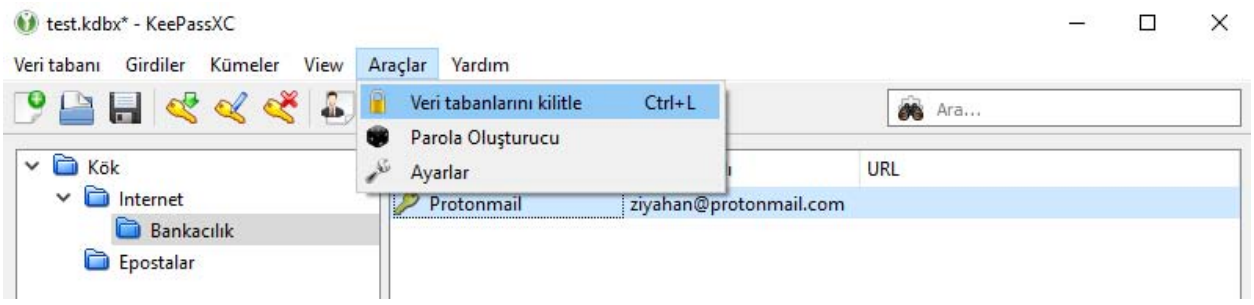
Kopyalanan değerlerden hemen sonra (kullanıcı adı ya da parola) hedef web sitesi ya da servisteki ilgili alana CTRL+V ile bu değerler yapıştırılabilir.

Diğer Özellikler Nelerdir?

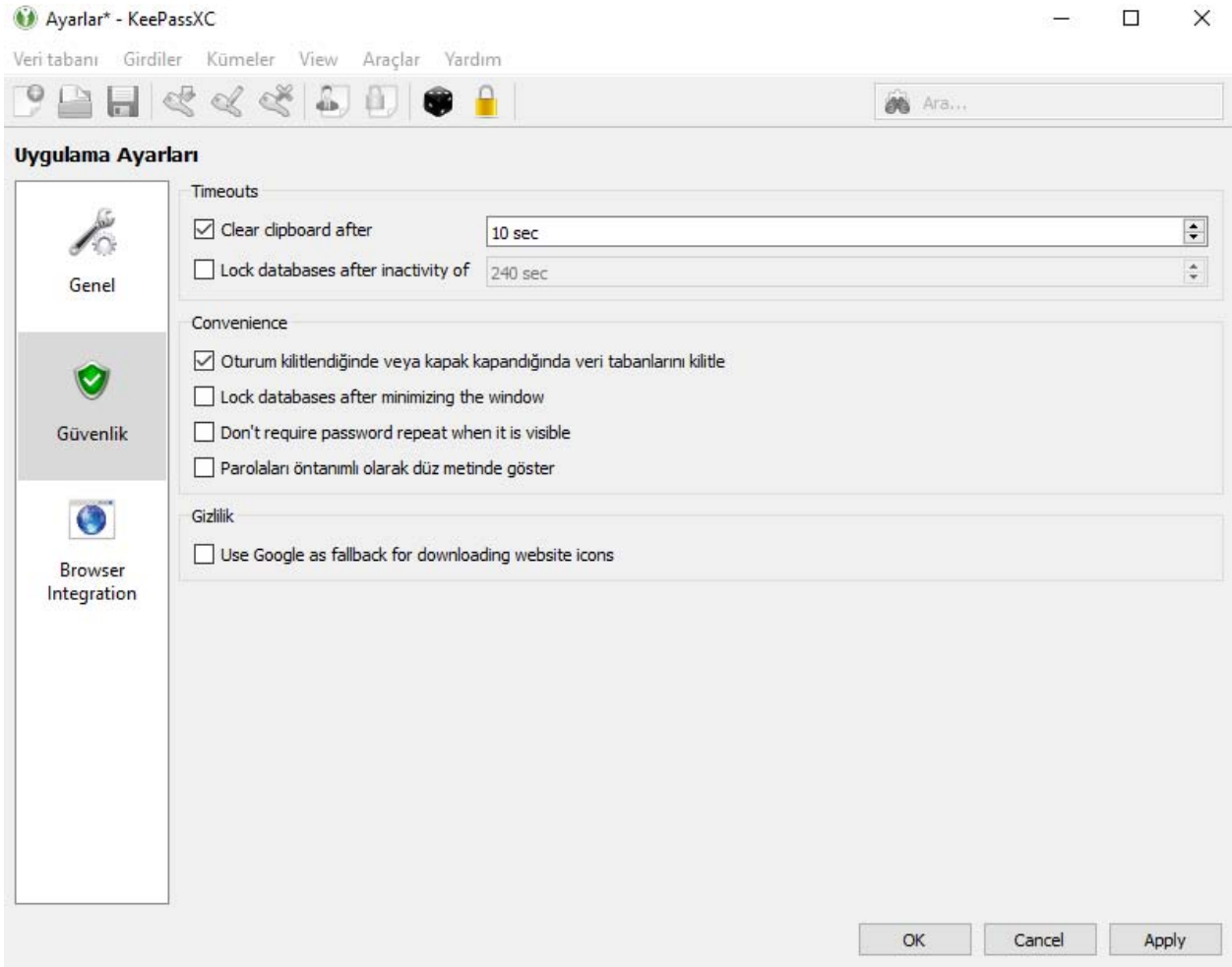
Elbette KeePassXC'nin sunduğu özellikler yukarıda anlatılanlarla sınırlı değil.

KeePassXC ile ayrıca;

- Ana ekranda bulunan arama kutusu vasıtası ile tüm girdilerde arama yapabilir.
- Ekranda bulunan grid'in kolonları vasıtası ile entry'leri / girdileri sıralayabilir.
- Araçlar > Veritabanını Kitle vasıtası ile KeePassXC açık olsa dahi parolara ulaşmak için tekrar master password'u (ve şayet başlangıçta belirtildi ise keyfile'ı da) sormasını sağlayabiliriz.



- Ayrıca, Araçlar->Ayarlar menüsü altında yer alan Güvenlik sekmesinden,KeePassXC belirli bir süre hareketsiz kaldığında, yani kullanıcı etkileşimi olmadığında kendini kilitlemesini ve ancak master parola girildiği takdirde tekrar parolalara erişim sağlamasını sağlayabiliriz:

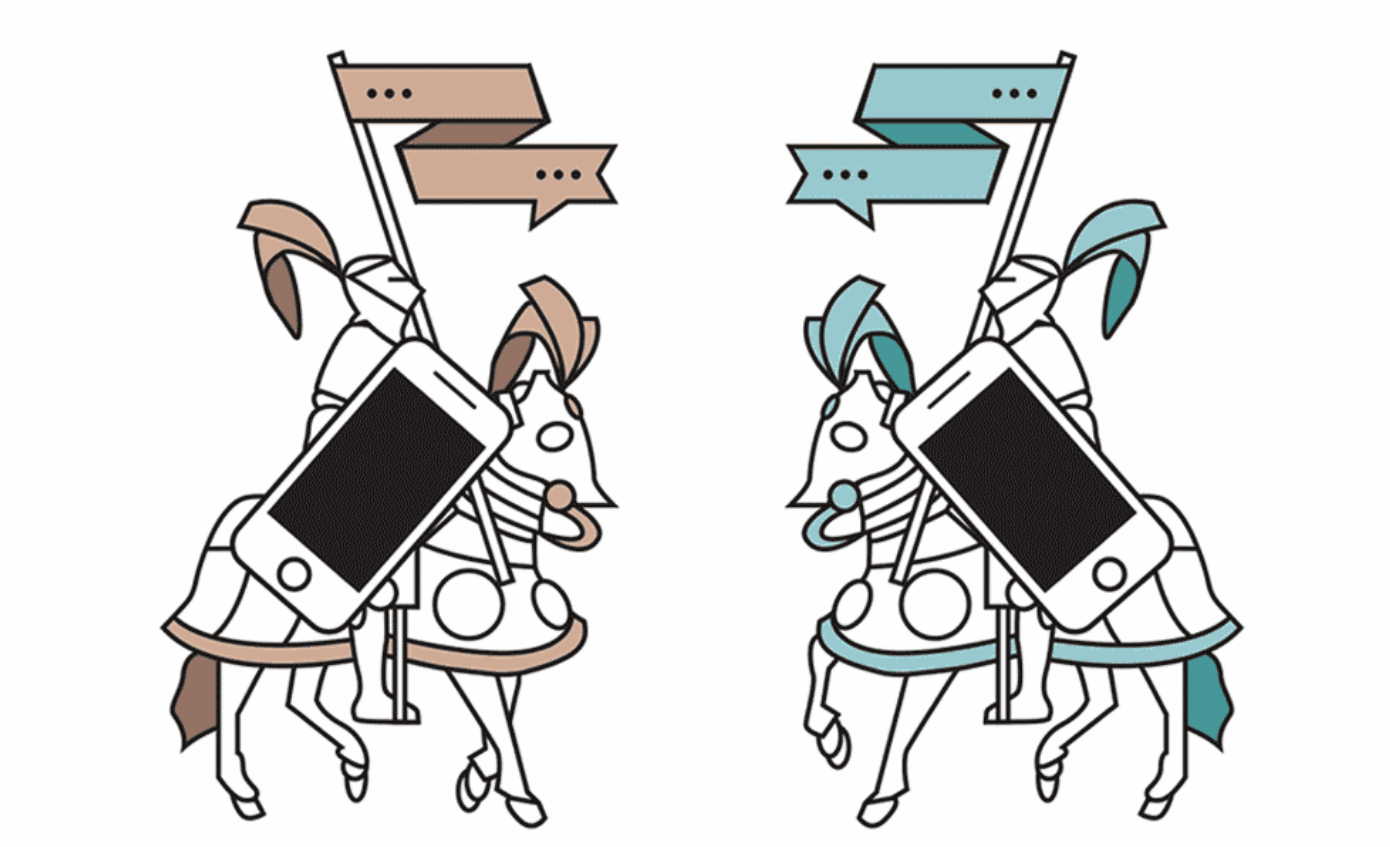


KeePassXC sadece kullanıcı adı ve parolalarınızı değil, hesaplarla ilgili dosya, resim vb belgelerinizi de bu entry / girdiler içerisinde saklamanızı sağlar. Örneğin son zamanlarda coin cüzdanlarının KeePassXC'de saklandığı görülüyor.

Artık süresi dolan parolarınız için kaygılanmaya son. Farklı servislerde aynı parolayı kullanmak zorunda da değilsiniz. Master parolanızı yeterli güçlükte belirleyerek, diğer tüm işlemleri KeePassXC'ye bırakabilirsiniz.

Micah Lee • micah.lee@theintercept.com • Çeviri: Ziyahan Albeniz

Güvenli Mesajlaşma Programlarının Savaşı ve Signal'in Tartışmasız Galibiyeti[1]



1 https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp/ Çeviri The Intercept'den alınan izin ile gerçekleşmiştir.

Geçtiğimiz bahar aylarında, mesajlaşma uygulamaları gizliliğe dair pek çok özellik kazandı. Nisan ayında dünyanın en popüler mesajlaşma programlarından WhatsApp, tüm kullanıcıları için uçtan uça şifrelemeyi kullanacağını duyurdu. Bu, mesajların WhatsApp'ın kendisi de dahil olmak üzere, herhangi bir Facebook çalışanından dünyanın en güçlü elektronik casusluk teşkilatı NSA'ye kadar tüm üçüncü kişiler tarafından okunamayacak olması demekti.

Akabinde, Mayıs ayında teknoloji devi Google, uçtan uca şifrelemeyi destekleyen Allo isimli anlık mesajlaşma programı ile bu furyaya katıldı.

Gizlilik açısından meseleyi önemli kılan nokta ise her iki uygulamanın da -WhatsApp ve Allo- Signal'in mimarı Open Whisper Systems tarafından geliştirilen güvenli mesajlaşma protokolünü kullanıyor oluşu.

Özetleyecek olursak **şu an güvenli şifreleme mekanizmasını kullanan en az üç uygulama var: Whatsapp, Allo ve Signal. Peki gizlilik konusunda titiz davranmayı sevenler bu üçü arasında nasıl tercih yapacaklar?**

Bu yazıda WhatsApp, Allo ve Signal uygulamalarını gizlilik perspektifinden mukayese edeceğiz.

Her üç uygulama da aynı güvenli mesaj protokolünü kullanırken, hangi bilgilerin şifreleneceği, metadata'ların toplanıp toplanmayacağı ve bulut servislerinde hangi bilgilerin saklanacağı konusunda -bir başka deyişle hangi bilgilere hükümetler erişebilecek, hangi bilgiler hackerlar tarafından potansiyel erişime açık olacak- konularında farklılaşmaktalar.

What's Up, WhatsApp?

1 milyardan fazla kullanıcı ile WhatsApp şüphesiz dünyanın en popüler mesajlaşma uygulaması. Bu yüzden bir buçuk yıl önce firmanın güvenli mesajlaşmayı entegre etmek için Open Whisper Systems ile iş birliği yaptığını duyurması şifreleme savunucuları arasında bomba etkisi yarattı.

Bu yeni özelliğin görücüye çıkması kademe kademe gerçekleşti. İlk olarak sadece uygulamanın Android versiyonunda, bire bir mesaj gönderiminde kullanılan özellik, geçtiğimiz Nisan ayında iOS kullanıcıları da dahil tüm kullanıcılar için, tüm mesaj gönderimlerinde (grup mesajları ve multi medya mesajları) devreye alındı. Mesajların Signal protokolü ile şifreleneceği duyuruldu.

İyi haber: Eğer resmi bir kanaldan bir şekilde WhatsApp mesajları istenecek olursa -tıpkı Brezilya'da vuku bulan son hadisede olduğu gibi[1]- WhatsApp bu uçtan uça şifreli mesajları deşifre edebilecek anahtarlara sahip olmadığı için, bu isteği karşılayamayacak.

Fakat akılda tutulması gereken önemli nokta şu, Signal protokolünün varlığına rağmen WhatsApp sunucuları üzerinden aktarılan veriler sayesinde -mesajın içeriğini göremese de- mesajın kim tarafından kime gönderildiği, ne zaman gönderildiğini görebilecek. Ayrıca Whatsapp'ın gizlilik sözleşmesine göre firma metadata olarak adlandırılan bu bilgileri saklama hakkını saklı tutuyor ve hükümetler ile paylaşıyor:

"WhatsApp başarıyla teslim edilen mesajlarla ilgili tarih ve zaman damgası bilgilerini, mesajdaki telefon numaralarını ve yasal olarak toplamakla mükellef olduğu bilgileri saklayabilir."[2] [3]

WhatsApp'dan bir kaynağın Gazetecileri Koruma Komitesine (Committee to Protect Journalists) verdiği bilgiye göre, "WhatsApp Normal şartlarda işlemlere ait bir günlük tutmuyor." Fakat firma tutmayacağına dair bir teminatta da bulunmuyor. Firma bu dataları kolaylıkla saklayabilir ve hizmet sözleşmesi ile çelişmeksizin talep halinde resmi kanallar ile paylaşabilir.

WhatsApp'ı ilk kez kurduğunuzda telefonunuzdaki kişi listenizi uygulama ile paylaşmanız konusunda bir seçenekle karşılaşırsınız, ancak paylaşmanız zaruri değildir. Bu özellik hâlihazırda listenizde WhatsApp kullanan kişilerden kolaylıkla haberdar olmanızı sağlar. Yine WhatsApp'dan bir kaynağın bildirdiğine göre şirket kişi listesine ait dataları tutuyor. Bu aynı zamanda gelen resmi bir talep doğrultusunda bu dataların paylaşılabileceği anlamına geliyor.

Son olarak **online yedekleme WhatsApp mesajlarının güvenliğinde koca bir delik açıyor. Uçtan uça şifreleme yalnızca mesajların internet üzerinden nasıl gönderileceğini belirliyor, fakat mesajların telefonunuzda hangi biçimle saklanacağını belirlemiyor.**

Mesajlar telefonda tutulduğunda, telefonun hâlihazırdaki güvenlik sistemi ile korunmaktadır. (Bu yüzden telefonun güçlü bir parolaya sahip olmasını önemli buluyoruz.) **Şayet telefonunuzu, bulut'a (cloud'a) kopyalamayı seçerseniz, mesela Android kullanıcılarının Google account'a ya da şayet iPhone kullanıcısı iseniz iCloud'a olabildiği gibi, mesajlarınızı yedekleme servis sağlayıcınıza teslim etmiş olursunuz.**

1 Nisan 2016'da verilen bir kararla WhatsApp mahkemelerin veri talebine, uçtan uça şifrelemeden ötürü "Elimizde olmaya datayı paylaşamayız" yanıtı verdiği için 3 gün süre ile tüm ulusta erişim dışı kaldı. https://theintercept.com/2016/05/02/whatsapp-used-by-100-million-brazilians-was-shut-down-nationwide-today-by-a-single-judge/

2 "WhatsApp may retain date and time stamp information associated with successfully delivered messages and the mobile phone numbers involved in the messages, as well as any other information which WhatsApp is legally compelled to collect."

3 WhatsApp kullanıcı sözleşmesinin güncel halinde bu kısım yer almamaktadır. Ancak yine de WhatsApp bu dataları tutmayacağı hususunda bir taahhütte bulunmamaktadır. ç.nc

WhatsApp varsayılan olarak mesajları iOS ve Android tarafından cloud'a yedeklenebilecek şekilde saklamaktadır.[4] Fakat aynı zamanda cloud'da yedeklenen chat mesajlarınızı kaldırmayı da destekler. Şayet WhatsApp'ı önemli mesajların iletiminde kullanıyorsanız bu önerdiğimiz bir yöntemdir.

Allo, World

Google'ın yayınlanmak üzere olan Allo uygulaması[5] ile ilgili anlaşılması gereken ilk nokta, varsayılan olarak Google'ın bu mesajları okuma yeteneğine sahip olduğu. Şayet Signal protokolü ile uçtan uca şifreleme kullanmak isterseniz, uygulama içerisinden "incognito mode"'a geçmeniz gerekiyor.

2016 yılında[6], **telefonlarımızdaki görüşmelerin varsayılan olarak güvenli olması gereken bir çağda, Allo'nun varsayılan olarak şifrelemeyi dayatmıyor oluşu, geçmişe olan garip bir bağlılık. Google'ın uçtan uca şifrelemenin varsayılan olarak etkin olmadığı bir uygulama yayınlıyor oluşu, Tesla'nın hava yastıklarının yalnız oto eğlence aksesurlarının devre dışı bırakılması ile çalıştığı bir arabayı piyasaya sürmesine benziyor. NSA hakkında ifşaatları ile tanınan Edward Snowden, Allo'nun bu varsayılan davranışını hem tehlikeli ve hem de güvensiz olarak addediyor.**

Diğer yandan Google makine öğrenmesinin görüşmelerinize uygulanacağı yeni bir yöntem deniyor: Bu yönteme göre Allo, Google Assistant olarak bilinen bir yapay zekâ ile bağlantı kuracak. Google Assistant tüm mesajlarınızı okuyarak sizin kendi ifadelerinizden edindiği tarzınızla bir dizi yanıt önerecek. Aynı zamanda Google arama da doğrudan görüşmelerinizle entegre hale gelecek. Örneğin siz ve arkadaşınız bir restorant aratabilecek, sunulan seçeneklerden birini tercih ederek uygulama üzerinden rezervasyon yaptırabileceksiniz.

Allo'nun makine öğrenme özelliği -Google tüm mesajların içeriklerini okumaya ihtiyaç duyacağı için- mesajlar için uçtan uça şifrelemeyi varsayılan olarak devreye almaktan alıkoyan bir özellik. Google'dan görüş belirten bir yetkiliye göre, Google makine öğrenmesini çalışır kılabilmek için mesajların içeriklerine erişmek zorunda. Görüşüne başvurulan kaynak ayrıca Google'ın kullanıcı datalarının nerede ve ne kadar süre ile saklanacağı konusunda bir vaatte bulunmaya Allo'nun yayınlanacağı yaz sonuna kadar hazır olmadığını belirtiyor.[7]

Allo'nun ardındaki teknoloji oldukça havalı olmasına rağmen, gizlilik endişeleri açısından yanlış bir yolda seyrediyor. Şayet gizlilik sizin için önemli ise, uçtan uca şifrelemeyi varsayılan bir seçenek olarak kullanan uygulamaları tercih etmelisiniz.

Allo ile beraber, Google ayrıca yeni bir görüntülü arama uygulaması olan Duo'yu yayınladı. Allo'dan farklı olarak, Duo'daki tüm görüntülü aramalar varsayılan olarak uçtan uça şifrelenecek. Google şifrelemenin nasıl çalışacağı, aramalara ait metadataların Google sunucularında saklanıp saklanmayacağına dair ayrıntıları henüz açıklamadı.

Allo ve Duo, her iki uygulama da Google'ın gizlilik politikaları şemsiyesi altında. Maalesef bu gizlilik sözleşmesi Google ürünleri ile ilgili ayrıntılardan söz etmiyor.

Signal

Daha ilk bakışta Signal'i WhatsApp ve Allo'dan ayıran özellik, Signal'in açık kaynak kodlu bir uygulama oluşu. Uygulamanın kaynak kodları güvenlik ve arka kapılar için araştırma yapmak isteyen tüm uzmanlara açık. Signal'i benzersiz kılan diğer bir özellik de Signal'in iş modeli: Signal'in herhangi bir ticari kaygısı yok. Reklam gelirleri ile fonlanan Facebook ve Google'ın aksine Open Whisper Systems tamamen bağış ve yardımlar ile desteklenmekte ve firma mümkün olduğu kadar az kullanıcı datası saklamakta.

WhatsApp'ta olduğu gibi Signal'de de mesajlar varsayılan olarak uçtan uça şifreli gönderilmektedir. Yani Open Whisper Systems'ın kendisi dahil herhangi bir üçüncü kişi/kuruluş bu mesajları okuyamamaktadır. Peki ya mesajlara dair metadatalar, telefonunuzun kişi listesi ve cloud backup'ları?

Signal'in gizlilik sözleşmesi olabildiğince kısa ve nettir. WhatsApp'dan farklı olarak Signal mesaja ait herhangi bir metadata saklamamaktadır. Kendisi de bir kriptograf olan Open Whisper Systems'in kurucusu Moxie Marlinspike'nin ifadesi ile, Signal sunucularında saklanan metadataya en yakın bilgi her bir kullanıcının sunucuya bağlantı kurduğu son zamana ait bilgidir -ki bu bilgi saat, dakika ve saniye bilgisinden son bağlanılan gün bilgisine kadar azaltılmıştır.

Signal kullanıcıları kişi listelerini, listelerindeki diğer kullanıcıları bulmak için paylaşmak zorundadır. Oysa Whatsapp'ta

4 Örneğin Android telefonunuzda sohbetleriniz Google Drive'a yedeklenmektedir. ç.n.
5 Eylül 2016'da uygulamanın ilk sürümü yayınlandı. ç.n.
6 Yazının yayınlandığı tarih, ç.n.
7 Allo'nun ilk sürümü Eylül 2016'da yayınlandı. ç.n.

bu tercihe bağlıdır fakat aynı zamanda yine WhatsApp tarafından önerilmektedir. Signal kişi listenizi doğrudan sunucuya göndermemektedir. Bunun yerine kriptoprafik hash olarak bilinen bir fonksiyon vasıtası ile telefon numaralarını gizleyerek sunucuya göndermektedir. Eğer bu konuda titizsek, hashlenerek saklanan telefon numaralarını truncate olarak bilinen bir işlem ile kısaltmaktadır. Marlinspike'a göre hashlenmiş telefon numaralarının gönderildiği sunucu Signal kullanan kullanıcıları belirten bir liste ile yanıt vermekte ve ardından sorguyu silmektedir.

Şayet telefonunuzu Google ya da iCloud hesabınıza yedeklerseniz, Signal sizin hiçbir mesajınızı bu yedeklemeye dahil etmeyecektir. WhatsApp'ın backup konusundaki uçtan uça şifrelemeyi gölgeleyen özelliği[8] Signal'de yoktur, kazara dahi olsa özel mesajlarınızın üçüncü bir tarafa teslim edilme riski yoktur.

Elbette bu aynı zamanda Signal verilerinizin cloud'da saklanması ile ilgili bir yöntem olmadığı anlamına gelmektedir. Şayet telefonunuzu kaybeder ya da bir yedeklemeyi restore ederseniz, bu en yalın anlamıyla tüm görüşme geçmişinizi kaybedeceğiniz anlamına gelmektedir. Signal'in Android versiyonu kullanıcılara lokal olarak uygulama datalarını içeri ve dışarı aktarma imkanı vermektedir. Şayet yeni bir telefon aldı iseniz, bu özelliği kullanabilirsiniz. Fakat Signal'in iOS versiyonu bu özelliği desteklememektedir.

Özetle, şayet resmi bir kurum Open Whisper Systems'dan mesaj içeriklerini ya da metadataları, yahut kullanıcının kişi listesini vermesini isterse, Open Whisper Systems'ın elinde teslim edecek hiçbir data olmadığı açık. Talep sahibi resmi kurum sadece (mobil işletim sistemi üreticisi olan, ç.n) Google ve Apple'dan Signal mesajlarının yedeklemelerini istemek için küçük bir şansa sahip olacak.

Kullanıcı gizliliği perspektifinden mukayesenin açık ara galibinin -bazı dezavantajlarına rağmen- Signal olduğu net.

WhatsApp'ın 1 milyarlık kullanıcı sayısı ile karşılaştırıldığında[9] Signal'in kullanıcı tabanı oldukça az. Marlinspike, kaç kullanıcıya sahip olduklarına dair bir istatistik yayınlamadıklarını belirtiyor. Fakat Google Play Store raporlarına göre Signal 1 ile 5 milyon arasında bir indirme oranına sahip[10]. App Store ise bu datayı yayımlamadı.

Yukarıdaki veriden anlaşılacağı üzere, **şayet Signal'i telefonunuza yüklerseniz, tek seçeneğiniz arkadaşlarınızı, ailenizi ve meslektaşlarınızı da Signal kullanmaya ikna etmek. Şayet WhatsApp yüklediyseniz, kişi listenizdeki pek çok kişinin hâlihazırda WhatsApp'ı kullanıyor olması kuvvetle muhtemel. WhatsApp ile doğrudan uçtan uca şifrelemenin etkin olacağı bir görüşmeye zahmetsizce başlayabilirsiniz.**

Signal ayrıca rakiplerine oranla daha az özelliğe sahip, ilerlemesi de yine diğerlerine nazaran daha küçük adımlarla gerçekleşiyor. Örneğin Signal Desktop'un ilk versiyonu 2015'in sonlarından beri kullanılabilir olmasına rağmen sadece Android kullanıcıları için mevcut. iPhone desteği henüz geliştirilmedi ve ne zaman nihayete ereceği maalesef belli değil. WhatsApp'ın desktop kullanımı ise telefon tipinden bağımsız olarak tüm kullanıcılar için mevcut.

Marlinspike 'in aktardığı bilgilere göre Open Whisper Systems sadece üç tam zamanlı personel[11] çalıştırıyor. Bunlardan ikisi yazılım geliştirici, biri ise kullanıcı desteği ve proje yönetimi ile ilgileniyor. Böylesine kısıtlı imkanlarla, sahip olduklarının çoğunu başarmaları gerçekten şaşırtıcı.

8 Örneğin Whatsapp mesajlarınız Android telefonda varsayılan olarak Google Drive hesabınızda yedeklenmektedir. ç.n.

9 Yazı yazıldığı anda. ç.n.

10 Son verilere göre Signal 5 ile 10 milyon kullanıcı tarafından indirilmiştir. Kasım/2017, ç.n.

11 Veri güncel değildir. ç.n.

Ömer ÇITAK • omer@omercitak.com

"Kendi Bağlantım" ile VPN Sunucunuzu Kurun

Bildiğiniz üzere Wikipedia gibi faydalı birçok siteye erişim engelli. Bunun gibi ülkemizde engellenmiş sitelere erişebilmek için birden fazla yöntem mevcut. Bu yöntemlerden biri de VPN.

Ancak ülkemizde VPN'ler doğru bir biçimde kullanılmıyor. VPN'nin ne olduğu, nasıl çalıştığı bilinmiyor. Durum böyle olunca internette yasaklı sitelere erişelim derken tüm trafiğimizi güvenmediğimiz kişi veya kuruluşlara teslim etmiş oluyoruz.

O yüzden bu yazımızda "VPN nedir?", "Nasıl çalışır?" gibi soruları yanıtlamakla birlikte çok kolay bir şekilde kendi VPN'inizi kurup internette nasıl güvende olacağınızı anlatacağım.

VPN Nedir?

VPN'nin açılımı Virtual Private Network, yani "Sanal Özel Ağ"dır. VPN'ler; kişi veya kuruluşlar tarafından kurulan bir iç ağdır. Bazı durumlarda bu iç ağa, dışardan dahil olunmasına izin verilir.

Daha net anlaşılması için bir örnek vereyim. Gidip herhangi bir İnternet Servis Sağlayıcısı (ISP) ile anlaşıp evinize internet bağlattınız. ISP'nin sizin için tahsis ettiği IP adresi X.X.X.X olsun. Bu IP adresi, sizin hattınıza atanmış IP adresidir. Dolayısı ile sizin evinizden herhangi bir cihaz ile internete çıkıldığında IP adresiniz X.X.X.X olarak gözükecektir.

Ama aynı zamanda modeminizin broadcast (yayın yapan cihaz) olduğu, evinizdeki akıllı telefonların, bilgisayarların, akıllı televizyonların kısacası internete ihtiyaç duyan tüm cihazların bağlandığı bir iç ağınız var. Bu iç ağınızın broadcast cihazı modeminiz olduğundan modeminiz; ağa bağlanan tüm cihazlara sadece iç ağınızda geçerli olacak birer IP adresi tahsis eder. Bu IP adresleri, broadcast'iniz yani modeminiz ile aynı aralıkta olmalıdır. Genelde modemin IP adresi 192.168.1.1 olur ve ağa bağlı cihazlara sırası ile 192.168.1.2, 1.3, 1.4 gibi IP adreslerini verir. Burada modemin birden fazla rolü var. Router, DHCP server gibi. Broadcast kısmı aslında tüm cihazların eşit olduğu bir iletişim modeli. Yani soru sorulup yanıt alınan bir protokol. Modemi burada kural koyucu yapan onun Router ve DHCP sunucusu olması aynı zamanda.

Modemin iç ağda cihazlara atadığı bu IP adresleri, cihazınızın sadece yerel ağda kullandığı IP adresleridir. Cihazınız internete çıkmak istediğinde gönderdiği TCP/IP paketi internete çıkarken önce modeme uğrar sonrasında da ISP'nin size tahsis ettiği IP adresi paketin kaynağı olacak şekilde alıcısına teslim edilir. Yani evinizdeki ağa bağlı akıllı telefonunuzun da bilgisayarınızın da IP adresi internet üzerinde aynıdır.

Buraya kadar özet bir biçimde evinizdeki ağın nasıl çalıştığını anlatmaya çalıştım. Dikkat ederseniz daha VPN'e gelmedik.

Şimdi, evinizdeki bir bilgisayara bir web sunucusu (Örneğin Apache) kurup, HTTP taleplerine yanıt verecek hale getirdiğinizi varsayalım. Bu bilgisayarınız artık hem bir "istemci", hem de bir "sunucu" oldu. Sunucu oldu çünkü artık taleplere yanıt verebilir hale geldi. Üzerine bir web sunucusu kurulmadan önce taleplere yanıt verebilecek bir mekanizması olmadığından sadece "istemci" pozisyonunda idi.

Web sunucunuza gel zaman git zaman birçok dosyanızı koydunuz ve sizin eliniz ayağınız oldu. Hatta bununla yetinmediniz, yerel ağınıza 2-3 sunucu daha kurdunuz. Daha net anlaşılsın diye yerel ağınızdaki sunucularınıza IP tahsis edelim:

- 1. sunucu: 192.168.1.21
- 2. sunucu: 192.168.1.22
- 3. sunucu: 192.168.1.23

Artık yerel ağınızda bilgisayarınızın tarayıcısında adres çubuğuna cihazlarınızın IP adreslerini yazarak sunucularınıza ve istediğiniz bilgiye rahatça erişebiliyorsunuz.

Zamanla 3 adet olan sunucularınız 5, 10, 15 oldu. Artık hangi sunucu hangi bilgileri tutuyordu sorusunu unutmaya başlıyorsunuz. Hop! Kafanızda yanan bir ampül ile bu sunuculara birer "domain" yani alan adı tahsis ettiniz.

Artık tarayıcınızın adres çubuğuna IP adresi yazmak yerine, "okul", "aile", "oyun" gibi alan adları yazarak sunucularınıza erişebiliyorsunuz. Ne kadar güzel bir sistem kurduk değil mi? Tıpkı internet gibi! İnternet de aslında sunucuların birbirine bağlı olduğu, her bir sunucunun ve istemcinin birer IP adre-

si sahibi olduğu bir ağ. Siz de evinizde tıpkı internet gibi bir ağ oluşturdunuz. Bu ağ, size ait olduğundan mütevellit "size özel ağ", yani VPN olmuş oldu.

Bunların üzerine bir gol de iş yerinizden geldi. Size dediler ki; "ey falanca, biz senin için iş dosyalarının olduğu bir sunucu kurduk. IP adresi şudur. Ancak unutma, sadece senin IP adresinden gelen taleplere yanıt verecek". Yani iş yeriniz, sadece ISP'nin size tahsis ettiği IP adresinden ziyaret edebileceğiniz bir sunucu kurdu.

Yukarıdaki örnekten devam edecek olursak, işiniz gereği uzun süre yurt dışına çıkmak zorunda kaldığınızı varsayalım. Hayda, e ama sizin okul, aile, oyun dosyalarınız hep yerel ağınızdaki sunuculardaydı. Bu sunucular yerel ağda olduğundan uzaktan erişim yetkiniz de yok. Ne yapacaksınız?

Sunuculara modemden port yönlendirmesi ile (NAT yöntemi) internete mi açacaksınız? Yok yok hayır bu olmaz, böyle yaparsanız tüm dosyalarınızı internete açmış olursunuz. Sizin erişebildiğinize herkes erişir.

Her sunucuya uzaktan erişim için ek yazılımlar mı kuracaksınız? Yok bu da olmaz. Okul, aile oyun sunucularına erişebilirsiniz ancak iş yerinizden sadece sizin IP adresiniz ile erişebileceğiniz uzak sunucuya erişemezsiniz.

Yapmanız gereken şey şudur: uzaktan kendi yerel ağınıza dahil olmak. Bunun için kullanabileceğiniz özgür yazılımlar mevcut. Örneğin en popüler özgür VPN yazılımı olan OpenVPN'nin sunucu uygulamasını yerel ağınızdaki cihaza kurduğunuz vakit, uzaktan yerel ağınıza bağlanabileceksiniz. Bu şekilde yerel ağdaki sunucularınıza erişebileceksiniz.

Aynı zamanda uzaktan yerel ağa bağlanmak için gönderdiğiniz her talep internete çıkmadan önce bu yerel ağa gelecek, bu yerel ağdan internete çıkacak. Böylelikle iş yerinden sizin için açılan sunucuya talepte bulunduğunuzda talebiniz sizin VPN'inizden çıkacağı için iş yerindeki sunucunuza da erişebileceksiniz.

VPN dediğimiz olayın aslı budur. Yerelde bir ağ kurarsınız, o ağdan yapılabilecek işleri yapabilmek için o ağa dahil olursunuz. Böylelikle o ağa dahil olduğunuzda internete çıkması gereken her talep bağlı olduğunuz uzak yerel ağ (VPN) üzerinden internete çıkar.

Yasaklı sitelere girmek için de bu mimariyi birebir kullanıyoruz. Öncelikle Wikipedia veya girmek istediğimiz sitenin yasaklı olmadığı bir ülkede çok cüzi miktarlara sunucu kiralıyoruz, kiraladığımız sunucuya gerekli yazılımlarını kuruyoruz ve ağımıza bağlanıyoruz. Sonrasında Wikipedia'ya erişmek istediğimizde talebimiz öncelikle bağlı olduğumuz VPN'e gidip oradan Wikipedia'ya gideceğinden herhangi bir yasak olmadan Wikipedia'ya erişmiş oluyoruz.

"Güvenli Bağlantım" Nedir?

Güvenli Bağlantım, internet erişiminize müdahaleleri engellemek, hız kaybı yaşamadan güvenli bir şekilde şifreli bağlantı sağlamak için kendi VPN kurulumunuzu yapmanızı size öğreten bir web sitesidir. Tamamen özgür yazılımları kullanarak bir VPN kurup, kurduğunuz VPN'e bağlanıp internette güvenli ve özgürce gezinmenize yardımcı olmaktadır.

Şimdi ise Kendi Bağlantım üzerinden kendi VPN'inizi nasıl kuracağınızı anlatacağım. Bu bölüm üç ayrı başlıktan oluşacak. Bu başlıklar aşağıdaki gibi olacak:

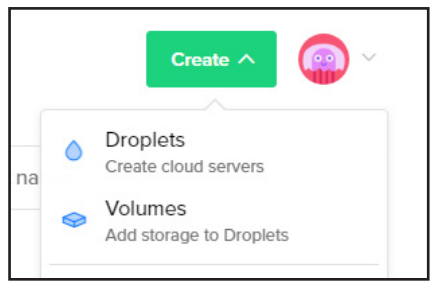
1. Sunucu kiralama
2. Sunucu ve OpenVPN kurulumu
3. Bilgisayarlar için bağlantı ve program ayarları

Bu adımların sonunda internette özgür ve güvenli şekilde dolaşıyor olacaksınız. Wikipedia gibi bir ansiklopedinin bile engellendiği bir coğrafyada yaşıyoruz. Yarın uyandığımızda yeni bir bilgi kaynağının daha engellendiğini öğrenmemiz çok yüksek bir ihtimal. İşte bu tarz engellemelere ve internette sansüre karşı VPN kullanın, kullandırın.

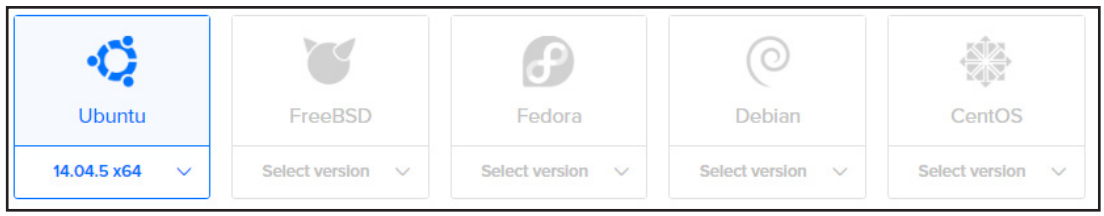
1. Sunucu Kiralama

Bu bölümde basitçe, bir sunucu nasıl kiralanır onu anlatacağım. Hem kolaylığı hem güvenilirliği açısından sunucuyu DigitalOcean sitesinden kiralayacağız.

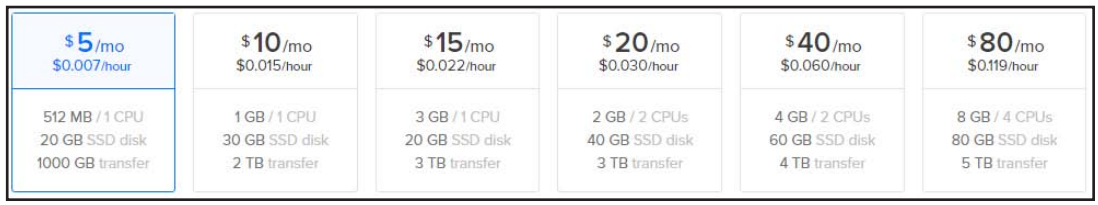
Öncelikle ilk adım olarak digitalocean.com'a kaydolup, kredi kartınızı tanımlamanız gerekiyor. Tavsiyem limitini sürekli 0TL tuttuğunuz, sadece alışveriş yapacağınız zaman limitini güncellediğiniz bir sanal kredi kartı bağlamanız.



Öncelikle yukarıdaki görseldeki göründüğü üzere sitenin sağ üst tarafında bulunan arka planı yeşil olan "Create" butonuna tıklıyoruz. Açılan alt menüden "Droplets" seçeneğini seçiyoruz. Aslında Droplets'in Türkçe'si "damlacık"tır ancak DigitalOcean literatüründe "sunucu"ya karşılık gelmektedir. Hosting sağlayıcının adı okyanus olunca (ocean), bizim de payımıza bu okyanusta damla olmak düşüyor.

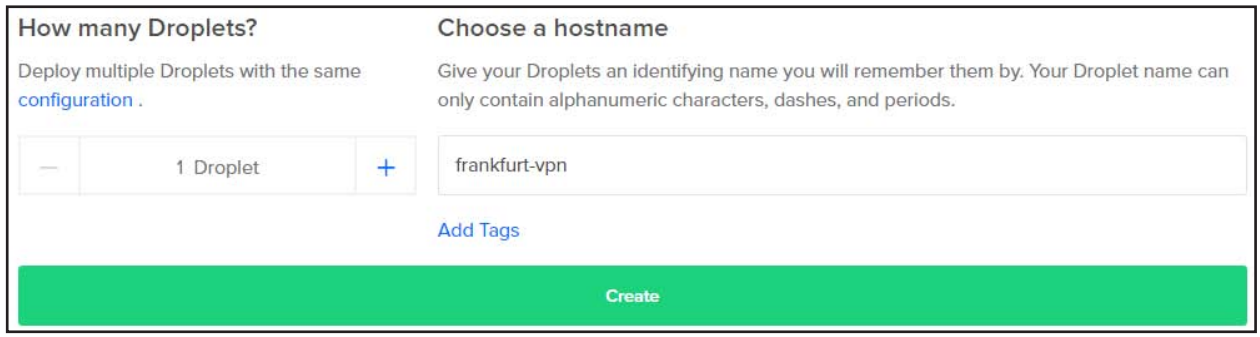


Yeni droplet oluşturma sayfasında ilk adım olarak sunucuya kurulucak Linux dağıtımını seçmemiz gerekiyor. En solda bulunan Ubuntu'nun 14.04.5 x64 sürümünü seçin.

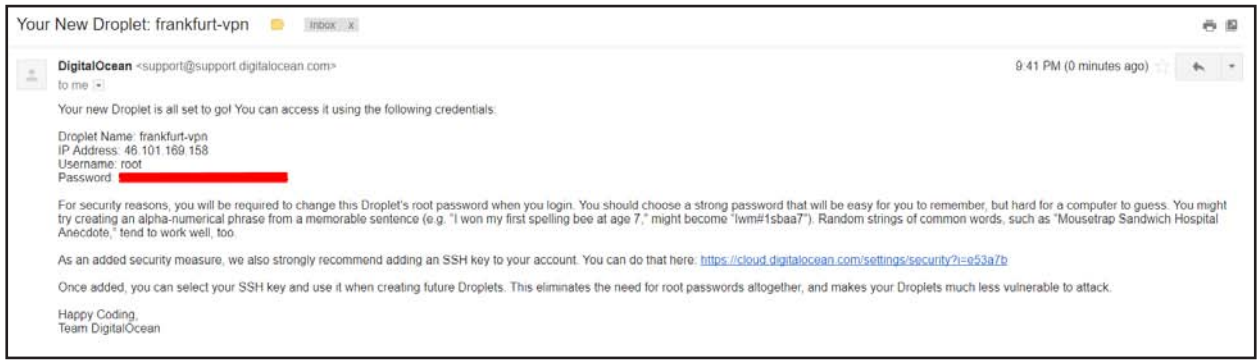


Ardından sunucunun kapasitesine ait paketi seçeceğiz. Ayda 5 dolar olan, en solda bulunan paket bizim işimizi görecektir.

Bu adımda ise sunucunun lokasyonunu seçeceğiz. Seçenekler arasında Frankfurt bizim için en mantıklı olan lokasyon. Zira fiziksel olarak Türkiye'ye en yakın lokasyon olduğundan diğer lokasyonlara göre daha hızlı internette gezinebileceksiniz.



Son olarak en aşağıdaki bölümde sol tarafı "1 Droplet" olacak şekilde bırakarak 1 tane sunucu açmak istediğimizi belirtiyor ve sağ tarafta sunucumuzun ismini yazıyoruz. Ben isim olarak "frankfurt-vpn"i seçtim.



Ve sunucu saniyeler içerisinde oluşturulup, erişim bilgileri bize mail olarak geldi!

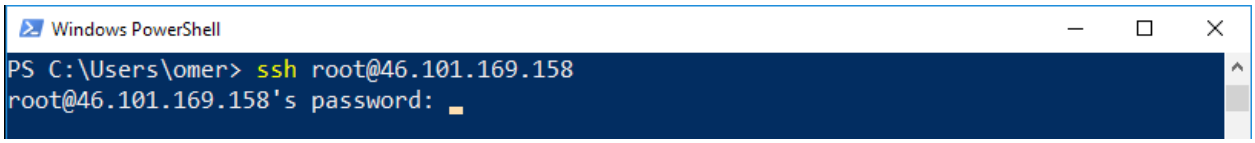
Bu bölüm bu kadardı. Sıradaki bölüme geçelim.

2. Sunucu ve OpenVPN Kurulumu

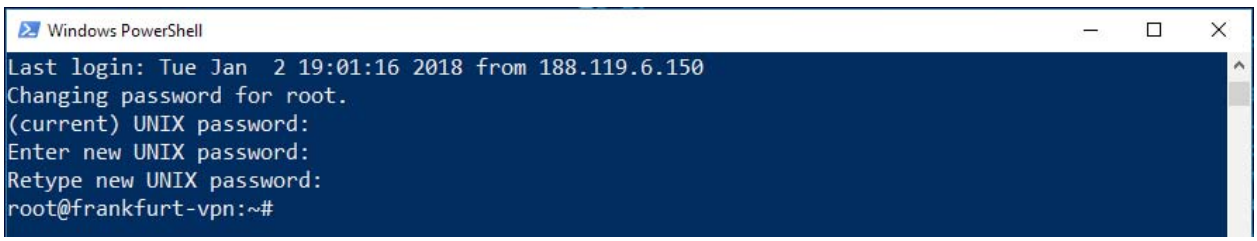
Öncelikle DigitalOcean'dan bize gelen maildeki bilgiler ile sunucumuza uzaktan SSH bağlantısı yapmamız gerekiyor. Bunun için bilgisayarımızda kullanmamız gereken bir terminal ve SSH yazılımına ihtiyacımız var. Linux ve MacOS kullanıcıları doğrudan terminallerini kullanabilirler ancak Windows kullanıcıları, Windows ile birlikte gelen "Powershell"i kullanmalıdırlar.

Windows arama çubuğuna "Powershell" yazarsanız Powershell karşınıza gelecektir. Powershell'i açtıktan sonra aşağıdaki komutu yazıp Enter'a basın.

```
ssh root@{mailde_gelen_ip_adresi}
```

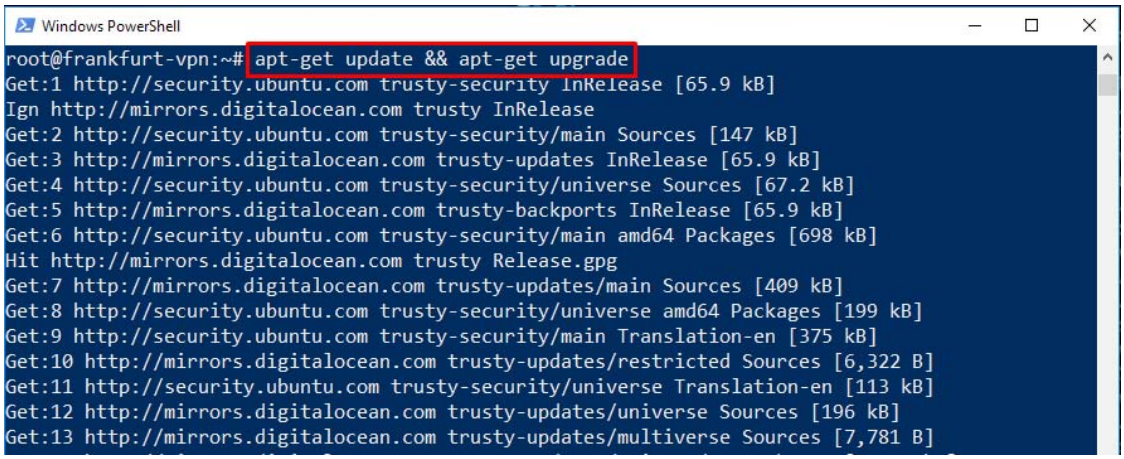


Yukarıdaki komut ile sunucumuza SSH bağlantısı yapacağız. Komutu yazıp uyguladıktan sonra bizden parola isteyecektir. Parolanız yine DigitalOcean tarafından gönderilen mailde mevcut. Parolayı mailden kopyalayıp, Powershell üzerinde farenin sağ düğmesine bir tık yaparsanız parolanız Powershell'e yapıştırılmış olacaktır. Ancak dikkat edin, bu ve sonraki parola adımlarında yazdığınız parola görünmez. O yüzden bir kere sağ tık yapmanız yeterli. Yapışmadı hissiyatına kapılarak iki üç kere yapıştırmaya çalışmayın :)



İlk adımda bizden sunucuya erişim parolamızı istiyordu. Sonraki iki adımda ise ilk girişimiz olduğundan yeni bir parola belirlememizi istiyor. Zor, kimselerin tahmin edemeyeceği bir parola koyun. (Güvenli bir parola oluşturmak ve saklamak için dergimizin bu sayısında yayınlanan *Parolalarınızı Tek Bir Yerden Yönetin: KeePassXC* yazısını tavsiye ederiz.)

Ve ardından nihayet sunucumuza bağlanmış olduk.

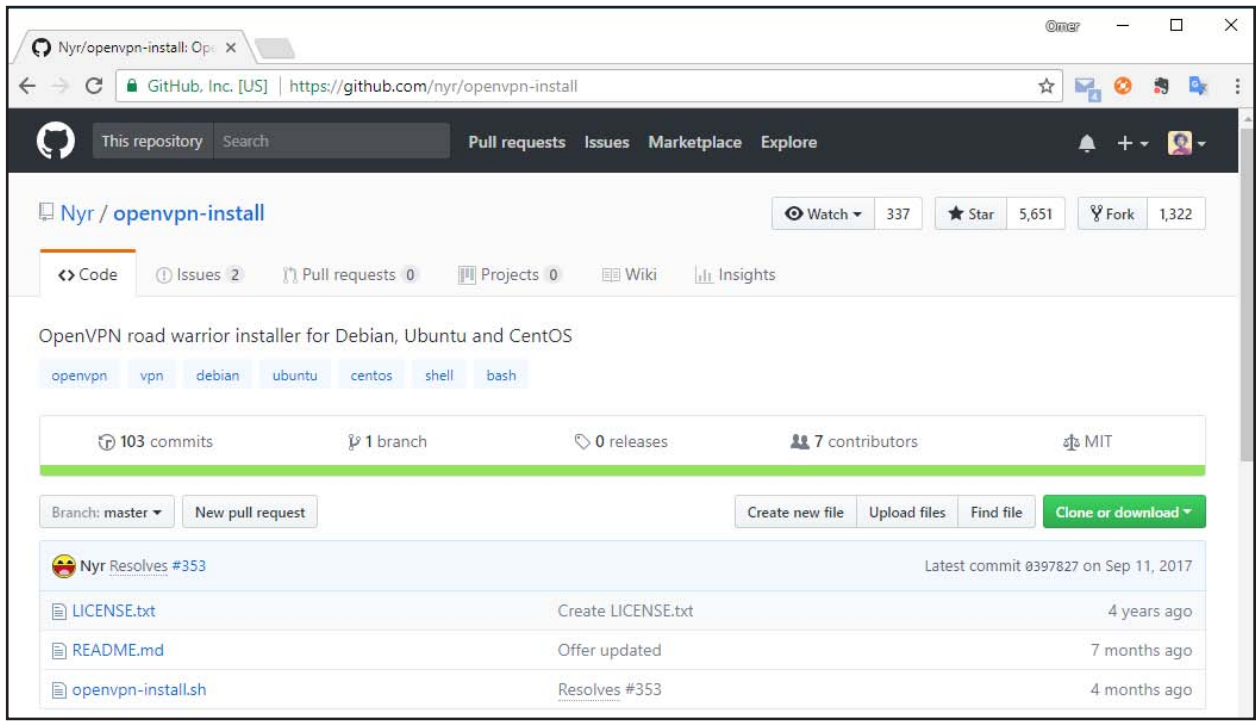


Şimdi ise ilk iş olarak sunucuda depo ve yazılımları güncelleyeceğiz.

```
apt-get update && apt-get upgrade
```

Yukarıdaki komutu yazıp uyguladığınızda bir süre beklemeniz gerekecek. Bu bekleme sonunda tüm uygulamalar ve depolar güncellenmiş olacak.

Gelelim OpenVPN'in kurulumuna.



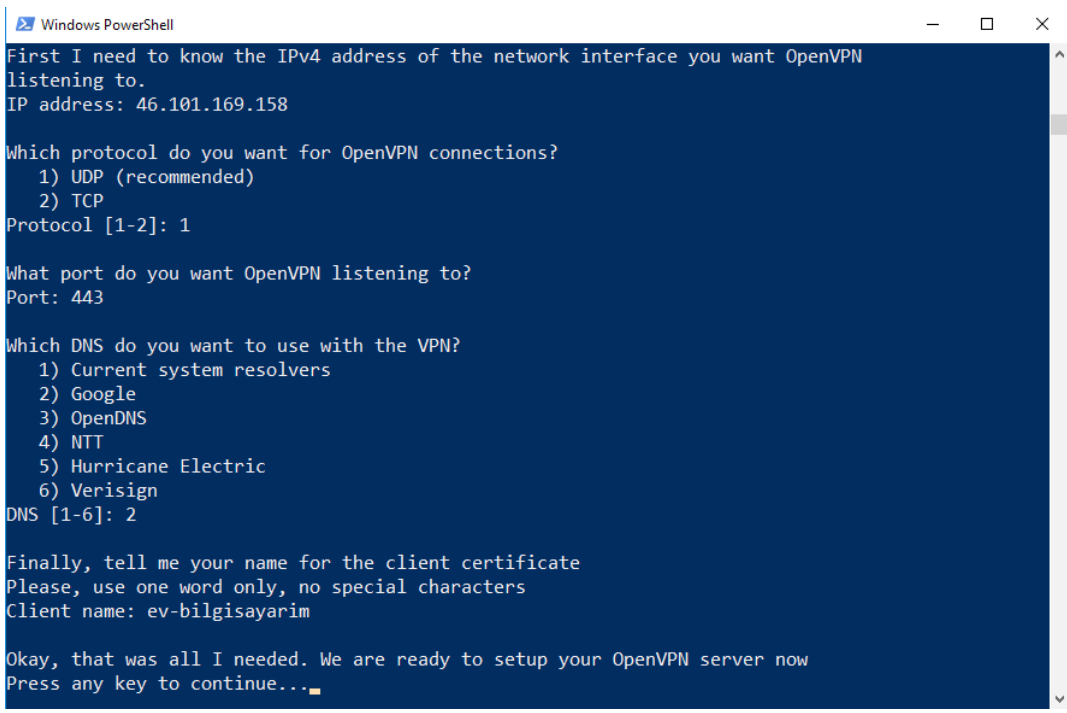
Normalde OpenVPN'in kurulumu biraz karmaşık ama bir Özgür Yazılım gönüllüsü bu adımları kolaylaştıracak bir kod yazıp bunu GitHub'da paylaşmış. Biz de bu arkadaşın yazdığı araçtan faydalanacağız.

GitHub adresi: https://github.com/nyr/openvpn-install

GitHub sayfasında da bulunan bu aracı kullanmak için çalıştırmamız gereken bir komut var.

```
wget https://git.io/vpn -O openvpn-install.sh && bash openvpn-install.sh
```

Bu komutu terminale yazıp uyguladığımız vakit yandaki görseldeki gibi bir çıktı ile karşılaşacağız.



1. IP Adress: Sunumuzun IP adresini soruyor. Otomatik olarak doldurulmuş geldiğinden Enter'a basın.
2. Protocol: UDP'yi seçin.
3. Port: VPN'e bağlanmaya çalıştığınız ağda VPN portu engellenmiş olabilme ihtimaline karşın 443 yazın. 443'ü kimse engellemek istemez.
4. DNS: Google DNS'i seçin.
5. Client Name: Sunucuya bağlanacağınız cihazın ismini girin. Örneğin "ev-bilgisayarim"

Bu adımlar sonucunda aşağıdaki gibi bir çıktı ile karşılaşacaksınız.

```
Finished!

Your client configuration is available at /root/ev-bilgisayarim.ovpn
If you want to add more clients, you simply need to run this script again!
root@frankfurt-vpn:~#
```

Yukarıdaki görselde de göründüğü üzere ev bilgisayarınızdan VPN'inize bağlanmanız için gerekli dosyayı "/root" dizini altında "ev-bilgisayarim.ovpn" adı ile oluşturdu.

Birden fazla cihazdan VPN'inize bağlanmak istiyorsanız yukarıdaki komutu tekrar çalıştırıp, istediğiniz kadar cihaz için "ovpn" uzantılı bağlantı dosyası oluşturabilirsiniz.

Şimdi ise oluşturduğumuz ".ovpn" uzantılı bağlantı dosyasını bilgisayarınıza aktarmanız gerekiyor. Bunun için "PuTTY SCP Client" yazılımını kullanacağız.

Yazılımı putty.org sitesindeki "Download" sayfasından indirebilirsiniz. Dikkat edin, aşağıdaki görseldeki gibi "pscp.exe" nin size uygun olan versiyonunu indirmelisiniz.

pscp.exe (an SCP client, i.e. command-line secure file copy)

32-bit:	pscp.exe	(or by FTP)	(signature)
64-bit:	pscp.exe	(or by FTP)	(signature)

İndirdikten sonra Powershell üzerinden Windows'un "Downloads" dizinine geçip, sunucudan dosyayı kopyalamak için ihtiyacımız olan komutu yazacağız.

```
Windows PowerShell
PS C:\Users\omer> cd .\Downloads\
PS C:\Users\omer\Downloads> .\pscp.exe root@46.101.169.158:ev-bilgisayarim.ovpn C:\Users\omer\De
sktop\ev-bilgisayarim.ovpn
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 256 49:ef:42:83:6b:f4:c3:7c:13:bc:e4:86:79:58:26:e7
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n) y
root@46.101.169.158's password:
ev-bilgisayarim.ovpn      | 8 kB |   8.0 kB/s | ETA: 00:00:00 | 100%
PS C:\Users\omer\Downloads>
```

```
cd .\Downloads\
```

Komutu ile "Downloads" dizinine geçtik.

```
.\pscp.exe  root@46.101.169.158:ev-bilgisayarim.ovpn  C:\Users\omer\Desktop\ev-bilgisayarim.ovpn
```

Komutu ile sunucudaki "ev-bilgisayarim.ovpn" dosyasını bilgisayarımızın Desktop dizinine indirmiş olduk.

Bu komutu yazdıktan sonra size anahtarı cache'de saklamak isteyip istemediğinizi soracak, "y" harfine basıp onaylayın.

Hemen ardından sizden sunucu parolanızı isteyecek, parolayı girip uyguladığınız vakit "ev-bilgisayarim.ovpn" dosyası bilgisayarınıza inmiş olacak.

DİKKAT: Yukarıdaki komutu ben kendi bilgisayarıma göre yazdım. Sizin bilgisayarınızın dili farklı ise dizin isimleri farklılık gösterebilir. Ayrıca yine komutta ben kendi sunucumun IP adresini yazdım. Siz, sizin sunucunuzun IP adresini yazmalısınız.

3. Bilgisayarlar için Bağlantı ve Program Ayarları

Windows cihazımızdan, kurduğumuz VPN'e bağlanmak için OpenVPN istemcisine ihtiyacımız var. OpenVPN istemcisini indirmek için openvpn.net'in "Downloads" sayfasına gitmeliyiz (https://openvpn.net/index.php/open-source/downloads.html).

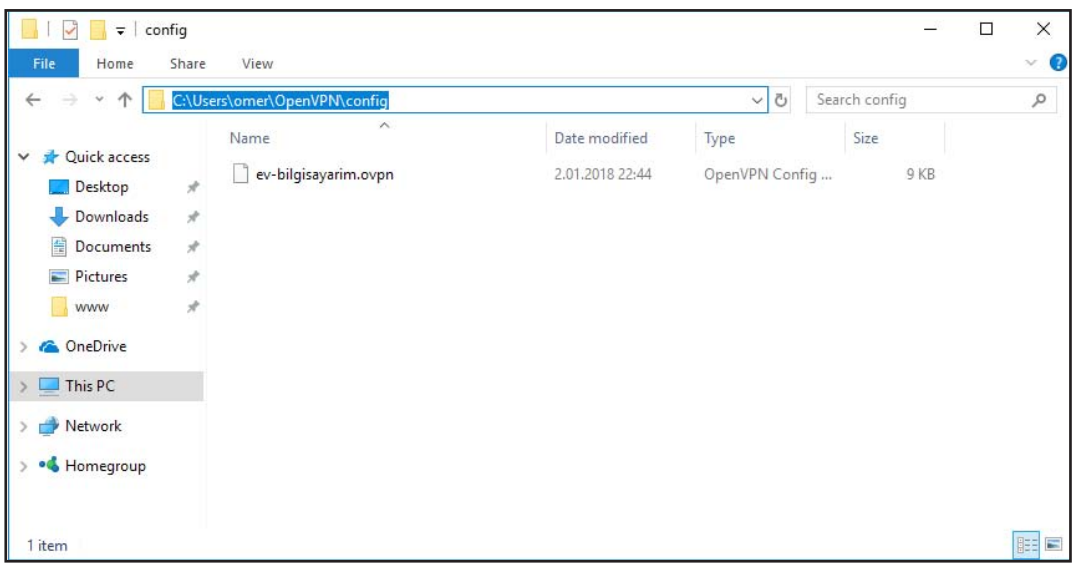
Source Tarball (gzip)	openvpn-2.4.4.tar.gz	GnuPG Signature
Source Tarball (xz)	openvpn-2.4.4.tar.xz	GnuPG Signature
Source Zip	openvpn-2.4.4.zip	GnuPG Signature
Installer, Windows Vista and later	openvpn-install-2.4.4-I601.exe	GnuPG Signature

Sitedeki indirme sayfasına gittiğinizde yukarıdaki gibi bir görsel ile karşılaşacaksınız. İstemcinin en güncel sürümü olan 2.4.4'ün "Windows Installer"ını yani yukarıdaki görseldeki 4. sıradakini indiriyoruz.

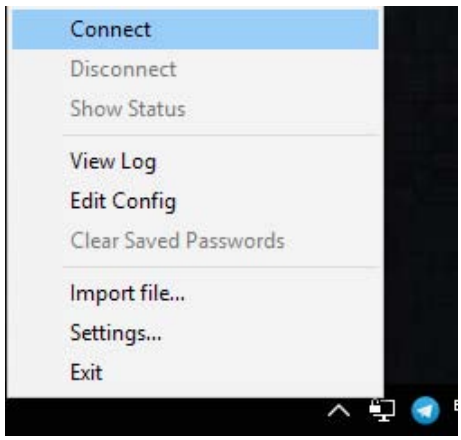
Ardından indirdiğiniz Installer'ı çalıştırın ve kurulum aşamasında herhangi bir konfigürasyon yapmadan sırası ile "Next", "I Agree", "Next", "Install" ve "Finish" butonlarına basın.

İstemci kurulumu bu kadar. Şimdi ise oluşturduğumuz VPN'e bağlanabilmek için, VPN sunucumuzdan kişisel bilgisayarımız için oluşturduğumuz "ev-bilgisayarim.ovpn" dosyasını OpenVPN istemcisine tanıtmamız gerekiyor.

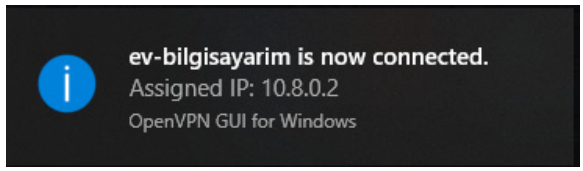
Bunun için "ev-bilgisayarim.ovpn" dosyanızı bilgisayarınızdaki "C:\Users\{kullanici_adiniz}\OpenVPN\config" dizinine kopyalamalısınız. Misal benim bilgisayarımdaki kullanıcı adı "omer" ve "C:\Users\omer\OpenVPN\config" dizini şu şekilde görünüyor:



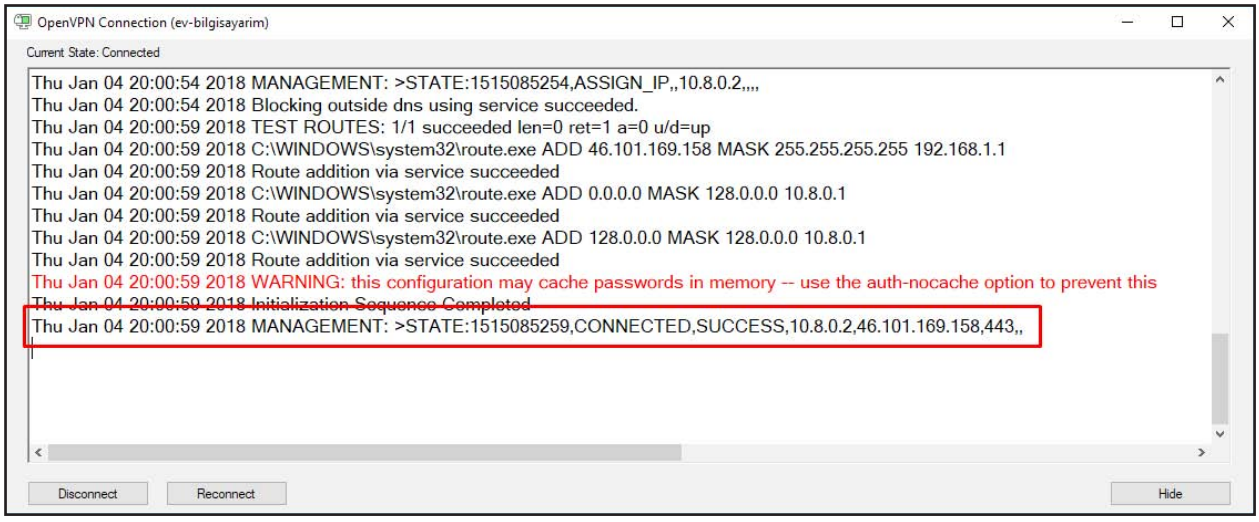
Bu adımı da gerçekleştirdikten sonra masaüstümüzde oluşturulmuş olan "OpenVPN GUI" adlı kısayolu çalıştırıyoruz. Çalıştırdıktan sonra bilgisayarımızın sağ altında, OpenVPN ikonu yer alacak. Aşağıdaki görseldeki gibi ikona sağ tıklayıp "Connect" demeniz gerekiyor.



Ve ardından Windows tarafından VPN'e bağlandığımıza dair bir bildirim alıyoruz.



Son kez kontrol edelim isterseniz, bilgisayarınızın görev çubuğun sağ tarafında bulunan OpenVPN ikonuna sağ tıklayarak "Show Status" seçeneğine tıkladığınızda aşağıdaki görselde işaretlediğim alandaki gibi "CONNECTED, SUCCESS" mesajını almış olmamız gerekiyor.



İşte VPN kurmak bu kadar basit! Kendi Bağlantım ve Arka Kapı dergisi, size yeni yılda internette bol bol özgür ve güvenli dolaşmanızı diler!

Bayram Gök • bayram@arkakapidergi.com

Kriptoloji'ye Giriş

Bilişim teknolojileri alanında yetkin dostlar ile hasbihâl ederken, sektörün gündemini konu edinecek, her okura hitap edebilecek içerikte bir dergi çıkarma fikri ortaya atıldı. Söyleşideki herkes kısa süre önce yayın hayatına başlayan başka bir dergi için yazı hazırlayıp katkıda bulunmuştu. Ancak daha ilk sayıda yazı içeriğinden bağımsız olarak kişiler sansüre uğramış, eser ve kişi bağı koparılmış ve bu talihsiz tecrübe herkeste hayal kırıklığı yaratmıştı. Herkes üzgündü, hevesimiz kırılmıştı. Dergi içeriği ile uyumlu, eserlerin özgürlüğünün kişiden bağımsız olacağı bir ilke üzerinde anlaşarak yeni bir dergi çıkarmak için yola çıkıldı.

Ben de kendime bir yazı konusu düşünürken editörümüz Ziyahan Bey "Kriptoloji üzerine yazar mısın?" diye sordu. Sıradan insanlardan tutun da devletin zirvesindeki görevlilere kadar herkesin gündemine yerleşmiş kripto paraların, daha özel olarak Bitcoin'in üzerine bina edildiği şu gizemli kriptoloji hakkında yazacak olmak bana da cazip geldi. Böylece birkaç sayıya yayılacak, geçmişten günümüze kriptoloji serüvenini konu edinecek popüler bilim tadında bir yazı dizisi kaleme almaya karar verdim.

GİRİŞ

Cryptography veya cryptology sözcükleri dilimize kriptografi ve kriptoloji şeklinde yerleşmiştir. Yunanca κρυπτός kryptós "saklı, gizli" ve γράφειν graphein "yazma" veya -λογία -logia "çalışma" kelimelerinin birleşimiyle oluşmuştur. Basitçe ifade edersek kriptografi veya kriptoloji bilimi kişiye, kuruma, devlete özel verilerin şifrelenerek gizlenmesi, rakiplerden korunması, güvenli şekilde taşınması, doğru adrese teslim edilmesi ya da özetle tüm bu sürecin analiz edilip açık noktaların tespit edilmesi ile ilgilenir. Çoğu tanımda kriptolojinin matematik ile tanımlanmış kuramlar ile çalıştığına vurgu yapılır. İkinci Dünya Savaşı'ndan sonra gelişen açık anahtar temelli matematik algoritmalarına dayanan bu atıf anlaşılabilir ancak, bir yanıyla eksiktir. Bu binlerce yıldır gizlilik sağlamak için kullanılan işaretlere, şekil veya yer değiştirmelere dayanan yöntemleri yok saymak olur.

1978 yılı kriptoloji için bir milat olarak kabul edilebilir. 1977-78 yılına kadar anahtar ve şifreleme yöntemi dahil her şey gizli tutulurdu. Çünkü o güne kadar kullanılan kriptoloji yöntemlerinde bir metni şifrelemek için kullanılan anahtar aynı zamanda şifrelenmiş metni deşifresinde de kullanılıyordu. O güne kadar kriptoloji için gizlilik en önemli ve yegâne hayati unsurdu, bu değişmek üzereydi. Ron Rivest, Adi Shamir, Leonard Adleman isimli üç araştırmacı, adlarının baş harfleri ile anılacak olan ilk açık anahtarlı şifreleme algoritması RSA'yı yayımladılar. O güne kadar devletlerin büyük bütçeler ayırarak geliştirdikleri ve en mahrem sırları olarak özenle sakladıkları gizli anahtar ve gizli şifreleme yöntemi artık anlamsızdı, hemen terk edildi. İşler şaşırtıcı derecede değişmişti. Anahtar ve şifreleme yöntemi en ince ayrıntısına kadar açık açık herkese anlatılıyordu.

RSA'nın matematik temeli ilkokul seviyesi basitliğindeydi. Korkutucu yüzüyle ise onu kırmak isteyenler karşılaşıyordu. Çünkü her şifrelenen harf veya rakamı çözen, devasa basamaklarla ifade edilen doğru anahtar sayısının çarpanlarına ayrılması işlemi süper bilgisayarlar için bile yüzlerce yıl sürmekteydi. Yazı dizimizin gelecek bölümlerinde bu algoritmanın ayrıntılarına değineceğiz.

Kriptolojide yöntem

Kriptoloji yöntemleri daha iyisi keşfedilene ya da algoritması çözülene, açığa çıkartılana kadar yaşarlar. Bir defa çözüldüklerinde terk edilir ve bir daha kullanılmazlar. Şifreleme yöntemleri tasarım esnasında kusursuzdurlar. Uygulamada ise yöntemlerin en zayıf noktasını dikkatsiz, sistem işleyişi hakkında yeterli bilgiye sahip olmayan, yönergeleri tam uygulamayan kullanıcılar oluşturur. Diğer bir deyişle insan faktörü kriptolojinin zincirinin en zayıf halkasıdır.

Yöntemler kullanıma sunulmadan önce iyice sınanmalı, kullanıcıdan kaynaklanabilecek hatalar olabildiğince göz önüne alınmalıdır. Kullanıcıyı belirli kalıplar içinde davranmaya zorlayacak önlemler geliştirilmelidir.

İnsanımız ve Kriptoloji

Bireysel ya da kurumsal olarak bilgiye, veriye gerekli değeri ve özeni göstermeyen bir toplum olduğumuz su götürmez bir gerçek. Bilişim sektöründe çalıştığım yıllar boyunca parolanın önemini kavramış kullanıcı ile karşılaşmam nadir bir durumdur. 123456, doğum tarihi, çocuğunun adı gibi seçimlerin ne kadar basit olduğunu anlatmaya çalıştığımda "Basit olduğu için seçtim" cevabını almam, bu işin en şaşırtıcı kısmıdır.

Burada şifre kelimesinin kökenine değinmek de bilgi güvenliği kültürümüzün gelişmesinde faydalı olacaktır.

Şifre kelimesi dilimize Fransızca chiffrer "rakamlaştırmak, bir yazıyı anlaşılmaması için kodlayarak yazmak" fiilinden girmiştir. Fransızca olan bu fiil, Fransızca chiffre "sayı, rakam" sözcüğünden türetilmiştir. Fransızca'ya ise İtalyanca "sıfır veya Arap rakamları" anlamına gelen ciffra sözcüğünden geçmiştir. İtalyancaya ise Arapça şifr صفر "sıfır" sözcüğünden girmiştir. Avrupalılar M.S. 1000'li yıllara kadar çok zaman isteyen ve hatalı işlem yapmaya açık Roma ve Eski Yunan sayılama sistemleri ile hesap yapmaya çalışıyorlardı. Bu insanlar Endülüs Müslümanlarının Hint kökenli 10 tabanını esas alan, konumlu ve sıfır içeren sayı sistemi ile hesap yapmayı kolayca ve çabucak yapabildiklerini görünce şaşırıp kalmışlardı. Öyle ki halk arasında sıfırın (Arapça şifr صفر) büyülü, gizem içeren bir rakam olduğu kanısı yerleşmişti. Sonradan bu karışıklığı gidermek, sıfırı nitelemek için "null", "zero" gibi yeni kelimeler türetilmek zorunda kalınmıştı.

Türkiye'de Kriptoloji Çalışmaları

Yazıyı hazırlamadan önce internette kriptoloji ile ilgili Türkçe kaynakları taradım. Bir elin parmaklarını geçmeyecek yerli yazara ait kitap, bir bu kadar çeviri ve bölük pörçük tez çalışmaları, ders notlarından başka bir kaynak bulamadım. En zengin Türkçe kaynağın bulunduğu www.wikipedia.org sitesine erişim ise hâlâ öğrenemediğimiz sebep(ler)den ötürü BTK tarafından engellenmiş durumda.

Türkiye'de ilk kriptoloji çalışmaları 1972 yılında ODTÜ bünyesinde küçük bir çalışma grubu ile başladı. Kamunun ve TSK'nin artan güvenlik ihtiyaçları ile beraber kriptoloji çalışmaları da gelişti. Bu çalışma grubuna 1995 yılında TÜBİTAK bünyesinde kurumsal bir kimlik kazandırılarak ULUSAL ELEKTRONİK VE KRİPTOLOJİ ARAŞTIRMA ENSTİTÜSÜ kuruldu. Kısa adıyla UEKAE olan bu kuruluşumuz çeşitli askeri projeler yanında AKİS elektronik sertifika (e-imza) gibi sivil kullanıma yönelik güvenlik ürünleri de geliştirmektedir. Üniversitelerimizde ise doğrudan kripto analist yetiştiren bölümler bulunmuyor. Üniversite mezunları için TÜBİTAK yaz okulları düzenlerken; İTÜ, ODTÜ, Ankara Üniversitesi dahil bazı üniversitelerimiz sertifika programları düzenliyorlar.

AKİS kart

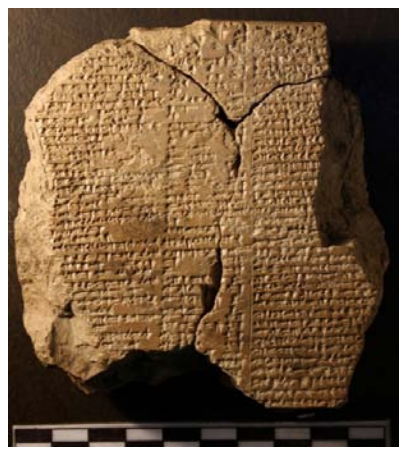
Kamu son yıllarda e-devlet projesi kapsamında büyük bir dönüşüm geçiriyor. Ne yazık ki vatandaşların e-devlet parolalarını diğer kişilerle paylaştığına şahit oluyorum.

Vatandaşın kendi kişisel gizliliğini önemsemediği bir devletin de gizliliği olamaz. Çünkü o vatandaş bir gün o devletin yönetici makamlarından birisine geçtiğinde aynı anlayışla devlet işlerini yürütecektir. Devlet kademelerinde yapılanan bir grubun devlete ait olduğunu iddia ettiği kriptolu telefon konuşmalarını nasıl yayınladığına şahit olduk. Gerçi bu konuşma kayıtlarının ortam dinlemesinden mi yoksa kriptonun çözülerek doğrudan elde edildiğini tam bilemiyoruz. Devletin ileri gelenleri bu konuşma içeriklerinin uydurma olduğunu beyan etseler de yeni kriptolu telefon geliştirme çalışması başlatmaktan da geri durmadılar.

Bu yazı dizimizde kadim zamanlardan bugüne, kişisel bilgilerden ticarete, devlet sırlarından askeri stratejilere kadar gizlilik sağlamak için kullanılan yöntemlere genel bir bakış atacağız. Enigma ve RSA dahil yazının geliştirilmesinden bu zamana dek geçen süre içerisinde kullanılan en basitinden en karmaşığına bazı sistem ve yöntemleri inceleyeceğiz.

Dil, Yazı ve Alfabe

M.Ö. 4000 yıllarında yazının geliştirilmesi insanlık tarihimizin en önemli keşfidir. Mağara duvarlarında, kayalar üzerinde önce insan, hayvan veya sahneleri betimleyen basit çizimler zamanla soyut anlamlar kazanarak sembollere evrildiler. Duvarlardan, kaya yüzeylerinden; kil tablet, deri, papirüs üzerinde anlam ifade eden cümle yapılarına, sayılara dönüştüler.



Süleymaniye Müzesi, Irak- Gılgamış Destanı dizeleri, Çivi yazılı bir tablet

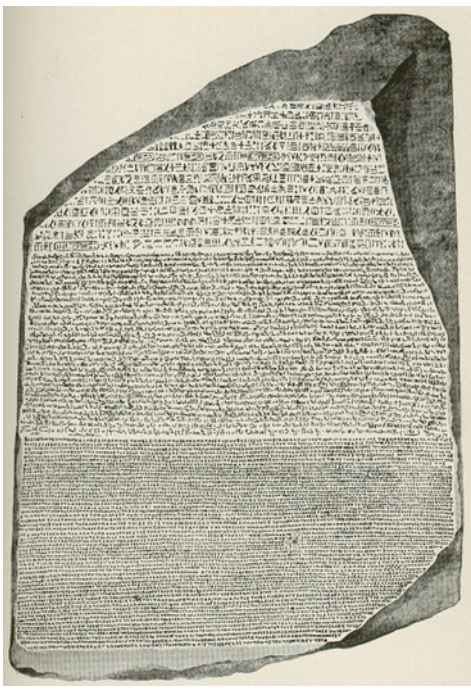
Yazı malzemelerinin pahalı olması, az bulunması ve eğitim kurumlarının yaygın olmadığı bu dönemde okuryazar olmak gerçek bir üstünlük, özel bir ayrıcalıktı. Yazı yazmayı, okumayı ve hesabı bilen az sayıdaki yazman, hesap uzmanı, vergi memuru ellerindeki bu imkânı kıskançlıkla korurlardı. Yanları-

na alıp eğitecekleri az sayıdaki çırakları dahi özenle seçerlerdi. Durum böyle olunca tablet ve kemik parçası üzerinde gördükleri karmaşık şekiller halk için gizemden, sırdan başka bir şey ifade etmezdi. Bilgi sınırlı sayıdaki bir yazman kitlesinin tekelinde dolaşırdı. İlk okuryazar insanları ilk kriptograflar, yazıyı da -kullanımdan amaç bu olmasa da- ilk kriptoloji yöntemi olarak tanımlamamızda hiçbir sakınca ve aykırılık yoktur.

Kripto analiz yaparken çözülmeye çalışılan metnin dilini, yazısını ve alfabesi iyi tanımak, hâkim olmak önemlidir.

Dil, yazı ve alfabe; diğer diller, yazılar ve alfabeler ile sürekli bir etkileşim halindedirler. Onları kullanan insanlara bağlı olarak süreklilik arz ederler. Baskın ve daha gelişmiş türdeşleri karşısında kullanımları giderek azalır ve unutulur giderler. Sonraki yazılarımızda işleyeceğimiz alfabe temelli saklı yazı analizlerine örnek olarak iki güzel hikâyeye değinelim.

Tüm Mısır coğrafyasına serpilmiş mimari yapıların üzerinde ve papirüs yapraklarında bolca bulunan hiyeroglif yazısı son okuryazarı yaşamını yitirdiğinden çözülmesi gereken bir gizem olarak bilim insanlarını meşgul ediyordu. Herkes bu yazıları okuyabilmek ve Mısır tarihini gün yüzüne çıkarmak istiyordu.

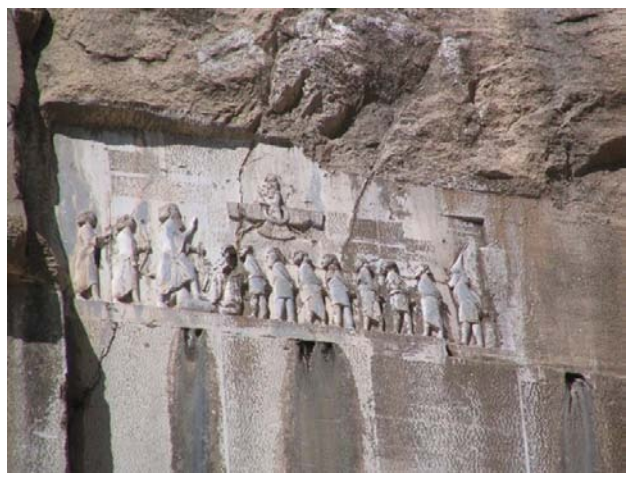


Rosetta Taşı ya da Reşid Taşı

Napolyon'un 1878 Mısır seferi esnasında yıkılan bir kale duvarının altında bir metnin Demotik, Hiyeroglif ve Antik Yunanca üç ayrı dilde yazıldığı granitten büyükçe bir taş bulundu. Fransız dilbilimci, ileride Mısırbilim Profesörü de olacak olan Jean-François Champollion, Antik Yunanca metindeki Ptolemaios ve Cleopatra özel isimlerinin hiyeroglif metin üzerinde çerçeve içinde yazıldığını fark etti. Eşleştirme yaparak metni çözdü. Hiyeroglif'in resim yazısı değil ses üreten bir alfabe olduğunu ortaya koydu. Hâlâ konuşulan Kıpti dilinin yardımıyla eski Mısır yazısı okunur hale geldi ve Mısır tarihi araştırmaları büyük bir hız kazandı.

Henry Creswicke Rawlinson Hindistan doğu Şirketi ordusunda subay olarak görev yapan amatör bir arkeologdu. 1838 yılında İran'a atandı. İşi dışında İran'da arkeolojik eserleri incelemeye başladı. Yerel rehberler bir gün onu yerden 50 metre yükseğe dik bir kayanın yamacına M.Ö. 5. Yüzyılda Pers İmparatoru Büyük Darius tarafından yaptırılmış Behistun yazıtına götürdüler.

Binlerce yıldır herkesin görebildiği bu yazıtta hiç kimse ne anlatıldığını bilmiyordu. Okuyabilen, çözebilen olmamıştı. İranlı yetkililerden bin bir güçlükle izin alıp palanga sistemi yardımıyla kayaya asılı durarak yazıyı kopyaladı. Uzun süre bu anlamsız görünen sembolleri yorumlamaya çalıştı. Rawlinson nihayet Eski Farsça, Elamca ve Babil dilinde yazılmış üç dilli bu yazıtın şifresini kırdı. Tüm Mezopotamya yazıtlarının incelenmesinin önündeki aşılmaz engeli kaldırmış oldu.



Behistun Yazıtı

Son olarak sizlere ülkemizde Rüzgarla Konuşanlar (Windtalkers) adıyla gösterilen filmden bahsetmek istiyorum. Amerikalılar İkinci Dünya Savaşı sırasında Japonların Purple şifresini kırarken Japoncanın kendilerine yaşattığı zorluğun intikamını Japonlardan almak istercesine bir grup Navajo yerlisini telsiz operatörü olarak orduya alırlar. Alın çözün bakalım Navajo dilini, derler. Kriptoloji ilgililerine izlemelerini tavsiye ederim

Sonraki sayımızda görüşmek üzere...

Musa BAŞ - sabloninsanlar@gmail.com

Özgürleştiren Bir Zincir: Blockchain Teknolojisi ve Akıllı (Smart) Kontratlar

Son zamanlarda maddi değeri oldukça artan ve insanların zenginleşme hayaliyle "Merhaba" dedikleri kripto para dünyası gündemimizi oldukça meşgul ediyor.

Kripto para dünyasının adını en çok duyuran Bitcoin'in aynı zamanda bir mihenk taşı olduğunu söylersem, sanırım yanılmış olmam.

Bitcoin'i değerli kılanın ne olduğunu anlatabilmek için arkasındaki teknolojiye ve felsefeye biraz değinmek istiyorum.

Bitcoin Nedir?

2008 yılında yaşanan küresel finans krizi sonrası insanlarda finans kurumlarına ve bu mekanizmaları düzenleyen, denetleyen kurumlara karşı bir güvensizlik ortaya çıkmaya başladı. Bu olaylardan bir süre sonra Satoshi Nakamoto takma adlı kişi ya da grup tarafından "Bitcoin: Eşten Eşe Elektronik Nakit Ödeme Sistemi" başlıklı bir makale yayınlandı. Yukarıda belirttiğim başlık ile Google üzerinde arama yaparsanız siz de bu makaleyi okuyabilirsiniz.

Bitcoin bir merkezi sisteme bağlı olmadan, kimsenin müdahalesine ve manipülasyona izin vermeyen yapısı ile dijital bir para birimi olarak doğdu.

Sadece para birimi mi idi Bitcoin? Tabii ki hayır! Finans dünyasına ve merkezi kurumlara karşı başkaldıran, kişilerin merkezi kurumlara bağlı olmadan eşten eşe dijital varlığını transfer etmesini sağlayan asi bir çocuk olarak da tanımlıyorum ben kendisini.

Şimdi bu asi çocuğun elinin bu kadar güçlü olmasını sağlayan teknolojiden bahsetmenin tam sırası: Blokchain Teknolojisi.

Sahne şimdi Blockchain'in.

Blockchain Nedir?

Blockchain'i Türkçeye kayıt zinciri ya da blok zinciri olarak çevirebiliriz. Blockchain ağını tüm işlemlerin veya dijital varlıkların kayıt edildiği bir deftere benzetebiliriz.

Bu defterin en büyük özelliği verilerin tek bir noktada tutulmasından ziyade ağın tamamında dağıtık bir şekilde tutulmasıdır. Verilerin tutulduğu noktalardan bir tanesi kaybolsa dahi, veriler ve sistem işleyişi diğer noktalar üzerinden devam etmektedir.

Blockchain zincirinde her zincir özel bir şifreleme sayesinde kendinden önce gelen zincir ile ilişkilidir. Defter örneğimize dönecek olursak defterin her sayfası kendinden önceki sayfa ile şifreleme sayesinde birbiriyle ilişkilidir.

Defter içinde bir sayfanın değişmiş olması kendisinden önceki sayfaları da uyumsuz hale getirir. Defter içindeki değişiklikler anında gün yüzüne çıkacaktır.

Defterin bu şekilde tutulması ve çalışma mekanizması; güvenlik ve şeffaflık konusunda Blockchain'e tam not vermemizi sağlıyor.

Blockchain'i hepimiz Bitcoin ile duyduk, kimimiz belki de Blockchain ile Bitcoin'i aynı bile zannediyor olabilir.

Ben artık Blockchain teknolojisini, bir protokol olarak tanımlamayı ya da bir programlama diline benzetmeyi yanlış görmüyorum. Nasıl bir programlama diliyle farklı problemler için çözüm geliştirebiliyorsak, Blockchain ile de farklı problemler için çözüm üretebiliriz. Bu sebeplerden dolayı Blockchain'i tanımlarken sadece Bitcoin transferlerinin tutulduğu bir defterden ziyade dijital varlıkların ve verilerin tutulduğu bir defter olarak tanımladım.

Blockchain hayatımızda ne gibi problemlere çözümler getirmiş ve getirebilir biraz da bunlara değinelim.

Bir hususa daha değinmeden geçemeyeceğim. Blockchain ağlarında bir madenci olması zorunluluğu yok, aşağıda değineceğim örnekler üzerinde de bunu göreceksiniz.

Blockchain Uygulamaları;

Bitcoin

Bitcoin hepimizin aşina olduğu, son yıllarda artan maddi değeriyle gündemimizi oldukça meşgul eden ilk kripto para birimi, tabir-i caiz ise dijital altın. İlk kripto para birimi olmasının yanı sıra ilk defa Blockchain teknolojisini kullanan bir uygulama olarak da tanımlayabiliriz.

Eşler arası para transferleri, bu transferlerin geçmişleri madenci adı verdiğimiz kişi ya da gruplar tarafından özel problemin çözülmesiyle elde edilen block içerisinde yazılır.

Ethereum

Vitalik Buterin tarafından 2015 yılında tanıtılan Ethereum; açık kaynak kodlu, Blockchain tabanlı akıllı sözleşmeler tasarlamanızı sağlayan ilk kripto para birimidir. Oluşturulan akıllı sözleşmeler kimsenin müdahalesine gerek kalmadan, sözleşmenin şartları yerine geldiği zaman anında gerçekleşiyor. Bir örnek vermemiz gerekir ise; A ve B olarak iki kişinin Ethereum tabanlı bir akıllı sözleşme yaptıklarını varsayalım. Sözleşme gereği A kişisi ile B kişisi 31.12.2018 tarihindeki dolar kuruna göre bir tahmin yaptıklarını ve bu tahminin sonucunda kimin tahmini gerçekleşirse bir miktar para gönderileceğine dair sözleşmeyi yaptılar. 31.12.2018 tarihi geldiğinde ilgili şartlar oluştuğunda kazanan kim ise sözleşme tarafından kazanan kişiye, kazandığı miktar otomatik olarak gönderilecektir.

Açık kaynak kodlu olmasıyla ve Solidity adlı scipt dili ile sizler de kendi sözleşmelerinizi yazabilirsiniz.

IOTA

Nesnelerin internetiyle ilgili problemleri çözmeye odaklı, açık kaynak kodlu dağıtık bir defter. Bitcoin'e nazaran çok kısa sürelerde doğrulama yapılabilen, madencilik ve bloklar yerine, sistem tarafından belirlenen sizden önceki iki işlemi doğrulama modeline dayanan bir uygulama.

Bithealth

Sağlık hizmetlerinin daha hızlı ve güvenli olmasını amaçlayan bir girişim. Blockchain üzerinde kişilerin sağlık verilerini tutan bu girişimin faydalarını şöyle sıralayabiliriz;

Hastaların sağlık verilerinin private key (özel anahtar) ile korunması.

İstenildiği zaman dünyanın dört bir tarafına anlık olarak gönderilebilmesi.

Geleneksel veri saklama modelleri yerine kişisel verilerin şifrelenerek daha güvenli şekilde saklanması.

Hastanın sağlık durumlarında herhangi bir değişiklik gerçekleştiğinde doktorun zaman damgası ile bu değişikliği onaylaması. İlgili kişilere bildirilmesi.

Copyrobo

Blockchain tabanlı yerli bir girişim olan Copyrobo, herhangi bir görseli ya da yazılı bir belgeyi zaman damgası ile kayıt altına alan bir uygulamadır. Bu uygulama ile size ait bir görseli ya da yazılı belgeyi kayıt altına alıp, sizin olduğunu kanıtlayıp, delil olarak gösterebilirsiniz.

Örnekler ve yapılabilecek olanlar tabii ki bunlarla sınırlı değil çok daha fazlası mevcut. Yakın gelecekte Blockchain teknolojisi hangi problemlerimize çözümler sunacak hep beraber göreceğiz.

Smart Contract (Akıllı Sözleşmeler)

Bir sözleşmenin şartlarını programlayarak, bu şartların kimsenin müdahalesine gerek duymadan takibini ve gerçekleşmesini sağlayan protokole "akıllı sözleşmeler" diyoruz.

Programlanabilen her akış bir akıllı sözleşme haline getirilebilir.

Akıllı sözleşmeler kripto para dünyasında ilk olarak Ethereum ile karşımıza çıkıyor.

Biraz daha akılda kalıcı olması için bir örnek ile daha da perçinlemek istiyorum;

Örnek: Sözleşme gereği bir araç kiraladınız ve bu aracı kiralarken aylık taksitini arka arkaya iki defa geciktirdiğinizde aracınızı bir daha çalıştıramayacağınızı taahhüt ettiniz.

Olanlar oldu iki defa arka arkaya taksitinizi geciktirdiniz, sözleşme gereği aracınızı bir daha çalıştıramayacaksınız, arabanın da programlanabilir olduğunu düşündüğümüzde bu sözleşme şartı yerine geldiğinde, otomatik olarak kimseye ihtiyaç duymadan arabanın kontağı kapatılacaktır. Bu gibi örnekleri çoğaltabiliriz. Yukarıda da belirttiğim gibi programlayabildiğiniz bir akışa sahip olan tüm işlemlerinizi akıllı sözleşmeler haline getirebilirsiniz.

Örnek 2: Geleneksel ev kiralama ya da otelde konaklama yapmak istediğimiz zaman insan faktörüne ihtiyaç duyuyoruz genellikle. Bir görevli tarafından konaklayacağımız ev ya da otel odasının giriş anahtarının bize teslim edilmesi gerekiyor. Kimsenin bizimle muhatap olmadığı bir yerde, konaklayacağımız yere giriş şansımız olabilir mi? Nesnelerin interneti (IOT) ile

birlikte programlanabilir kapı kilitleri, programlanabilir eşyalarımız oldu: kahve makineleri, lambalarımız vs. Akıllı sözleşme aracılığı ile bir günlüğüne konaklamak için bir ev kiraladığımızı düşünelim, sözleşmeyi yaptık. Sözleşme sonucunda bizim belirtilen tarih boyunca bize tahsis edilen evin kapısının, bizim özel anahtarımız ile açıldığını düşünün. Tarih geçtiğinde ise tekrar açılmadığını düşünün. Bu senaryo şu anda **slock.it** Blockchain tabanında gerçekleştiriyor, Youtube ya da Google üzerinde arama yaparsanız göreceksiniz.

Örnekleri çoğaltabiliriz, hayal gücünün ve teknolojinin sınırı yok.

Akıllı sözleşmelerin nasıl çalıştığına teorik olarak değinelim;

- Sözleşmenin konusu oluşturulur.
- Sözleşmenin şartları belirlenir.
- Sözleşme blok zinciri ortamında oluşturulur.
- Sözleşme, sözleşme taraflarının özel (private) anahtarları ile imzalanır.
- Sözleşmenin şartlarının yerine gelip gelmediğini blok zinciri kontrol eder.
- Sözleşme şartları sonucunda uygulanacak hükümler blok zinciri tarafından uygulanır.

Teknik olarak detayına değinmiyorum. Derginin gelecek sayılarında çalışma prensibine de değineceğimizi umuyorum.

Akıllı sözleşmelerin avantajları nelerdir?

- Güvenlik
- Hız
- Maliyet
- Yedekleme
- Standartlaşma

Yazıma bu noktada son veriyorum. Yazılacak konuşulacak çok şey var. Blockchain ve akıllı sözleşmeler hakkında, naçizane bir giriş yaptığımı düşünüyorum. İlerleyen yazılarda görüşmek üzere.

Blockchain'le kalın.

Mustafa Yalçın – iletisim@sahvemat.com

Devrim Niteliğindeki

Blockchain Teknolojisi Güvenli mi?

Blockchain son zamanlarda sıklıkla adını duyduğumuz bir teknoloji. Sadece Blockchain'in kendisiden değil, hemen her gün Blockchain teknolojisi üzerine inşa edilmiş yeni bir fikir, yeni bir teknolojiden haberdar olmaktayız.

Blockchain'in avantajlarından siz de faydalanmak, dağıtık mimari kullanarak yeni bir fikir ortaya çıkartmak isteyebilirsiniz. Sadece yeni fikirler değil, hâlihazırda mevcut olan, yürürlükte olan bir fikri, bir iş modelini bu dağıtık mimariye uyarlayarak, yeni bir biçimde kullanıcılarla buluşturabilirsiniz.

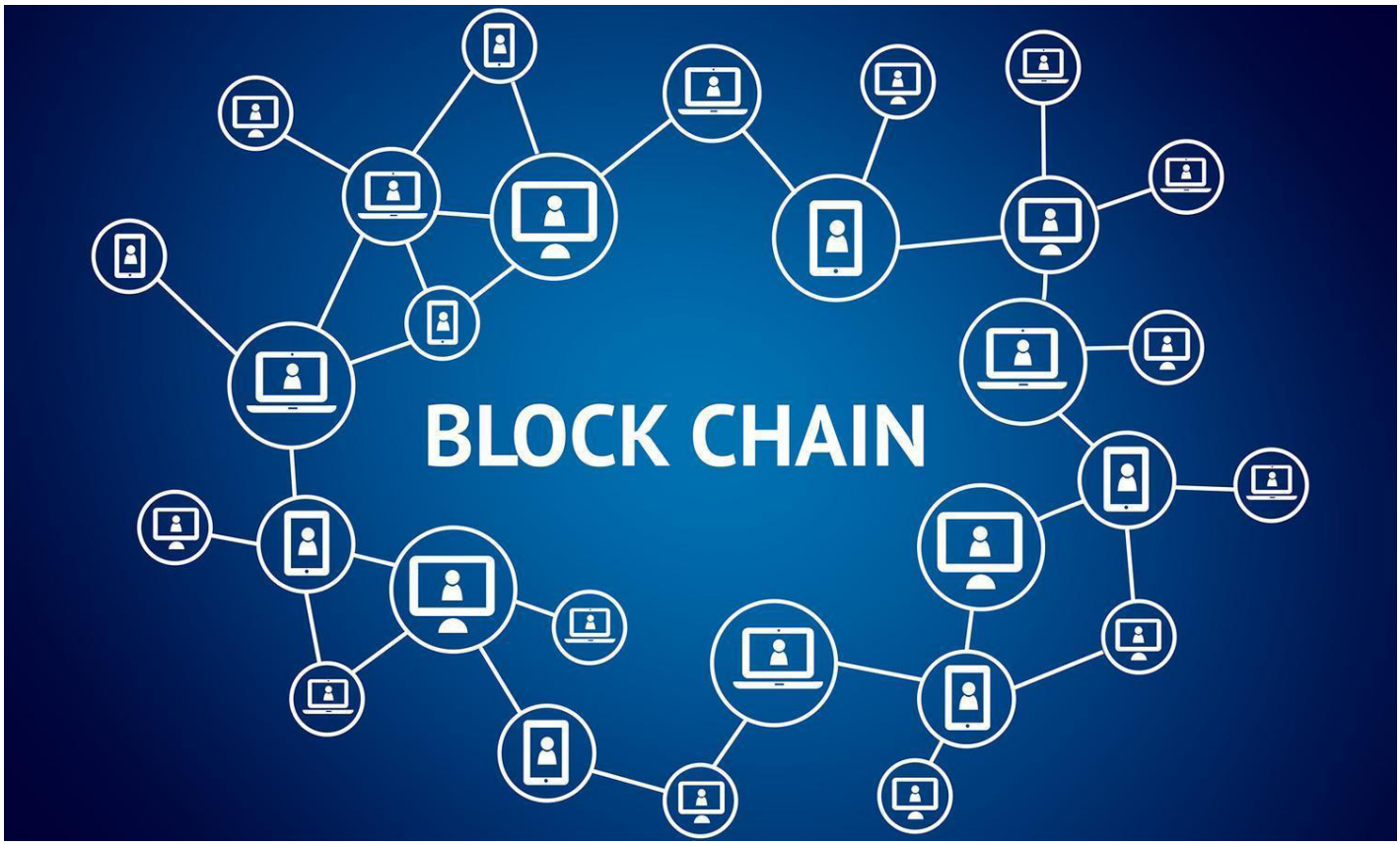
Peki oluşturulan bu Blockchain tabanlı projelerin değerini nasıl ve ne ile ölçeriz? Projeyi kullanan insanlarla ve proje yardımı ile çözdüğümüz sorunlarla ölçebiliriz.

Kullanan insanlarla, çözdüğünüz sorunlarla ölçebiliriz. Blockchain tabanlı sistemleri kolayca tasarlayabilmenizi ve öğrenebilmenizi sağlayacak onlarca makale yayınlanmaya başladı. Fakat çoğu insan "güvenli Blockchain tasarımı" ile ilgili makale bulamamaktadır.

Bu yazımızda gerek teorik bilgilerden gerek yaşanmış örneklerden hareketle güvenli bir Blockchain tasarımı üzerinde beyin fırtınası yapmaya ne dersiniz?

Blockchain üzerine uyarlanabilecek örnekleri defalarca bir yerlerde konuştuk ya da bir yerlerden okudunuz. Hemen bu örneklerden birini hatırlayalım:

Ahmet, Blockchain teknolojisine merak salan ve bu teknolojinin önemli olduğuna inanan bir yazılımcıdır. Her yazılımcı



gibi içindeki girişimci ruhu ile Blockchain teknolojisini nerede kullanabileceğine dair beyin fırtınası yapmaktadır. Beynindeki bu amansız fırtınayı Spotify'da şarkı dinleyerek dindirmeye çalışıyor ve kendine şu soruları soruyordu:

"Acaba ben bu yazılımı Blockchain teknolojisini kullanarak geliştirsem, dinleyici ile şarkıcı arasında Spotify gibi aracı kuruluşları çıkarıp herkesin kendi şarkısını yükleyip satabilmesini sağlasam hem maliyeti düşürmüş hem de insanlara yeni bir hizmet sunmuş olur muyum?" diyor.

Bu yazılımın gerçekleştirilebilmesi için iki yol vardır;

Bitcoin gibi orijinal bir Blockchain tasarımı ile baştan sona şarkı yüklenebilmesini ve bu verilerin dağıtılabilmesini sağlayacak bir yapı kurması gerekir.

Ya da Ethereum üzerinde akıllı kontratlar (smart contracts) ile uygun altyapıyı sunan bir "coin" geliştirerek yapabilir.

Her iki yolda da güvenli tasarım yapılmadığı takdirde felaketlere neden olabilecek sonuçlar doğabilecektir. Maalesef bu sonuçların bazıları geçmişte de yaşanmıştır.

Ahmet'in güvenli tasarım için sorması gereken sorular ve koyması gereken kurallar vardır. Kabaca örnekleyelim;

Eserlerin ücretinin ödenmeden dinlenemiyor olması.

Kullanıcıların yaptığı ödemelerin doğrulandığından ve ödemenin eser sahibine ulaştığından emin olunması.

Kullanıcıların ödeme yapmadığı halde hesabındaki paranın izinsiz gönderilmesini önlemek gibi temel finansal işlemlerin doğru yapılması.

Bu ve benzeri örnekler verilebilir.Temel para gönderme ve alma işlemleri güvenli ve doğru bir şekilde yerine getirilse bile buna bağlı kütüphanelerdeki ya da diğer bileşenlerdeki mantıksal hatalar sebebiyle art niyetli kişilerin saldırısına maruz kalınabilir. Bunların sonucunda izinsiz ödeme alınıp, gönderilebilir. Yeterli kontroller yazılsa bile hâlen risk olabilir mi? Cevap: Evet!

Nasıl başka riskler olabilir? Ahmet'in Bitcoin alt yapısından faydalanarak bu sistemi geliştirdiğini varsayalım.

Bitcoin'in kullandığı Blockchain alt yapısında PoW (Proof-of-Work) adını verdiğimiz işe dayalı bir kanıt modeli kullanılmaktadır. Bu da yapılan para transferlerinin biriktiği havuzdan her 10 dakikada bir, madencilerin hesaplama gücünü kullanarak bulduğu bloklara yazması ile gerçekleşir. Bitcoin'de bazen transferlerin 10 dakikada onaylanmadığını görüyoruz, sebebi ise madencilerin en yüksek işlem ücreti ödeyenleri ilk sırada tercih etmeleridir. Burada şu çıkarımı yapmak faydalı olacaktır: Bitcoin'de madencilik yapanlar havuzdan para transferi işlemlerini seçerek yapabiliyorlar. İşte bu noktada şimdiye kadar yaşanmamış ama teorik olarak yaşanması mümkün olan bir saldırıdan bahsedebiliriz: %51 Saldırısı.

Satoshi Nakamoto daha Bitcoin tasarımını açıkladığı ilk makalede bizlere bu saldırıdan bahsediyor. Eğer %51 art niyetli kişilerin eline geçerse siz ödemenizi aldığınızı sanırsınız ama art niyetli %51'i oluşturan madenci çoğunluğu o işlemleri onaylamayabilir. Bu da en yalın haliyle sizin ticaretini yaptığınız ürün için paranızı tahsil edememeniz ama ürünü adama vermiş olmanız anlamına gelmektedir. Bu yüzden yapılan para transferlerinin her birinde "Onay / Confirmation" denilen bir bekleme süresi vardır. Gerçekleştirilen para transferi Bitcoin alt yapısı kullanılan sistemlerde ortalama 3 blok onayı alarak güvenilir kabul edilmektedir. Bu değer blok üretmenin zorluğuna göre zamanla değişkenlik gösterebilir. Mevcut blok üretme zorluğunun derecesine bakılarak 3 onay yeterli görülmektedir. Her bulunan yeni blokla yapılan para transferine güven artar ve geri çevrilmesi zorlaşır.

Bu anlattıklarım şu an için yaşanmış bir saldırı değildir, çoğu insan da yaşanacağına inanmamaktadır. Çünkü Bitcoin'in ulaştığı yüksek işlem gücü şu an yüklü bir yatırım, yüklü bir elektrik harcanmasını gerektiriyor. Böyle bir saldırı haberinin yayılması sonucu ile Bitcoin fiyatlarında yaşanılacak olan düşüş kaçınılmaz olacaktır. Bu durum yapılan yatırımın yüksekliği karşısında, saldırganın elde edeceği kârı otomatik olarak düşüreceği için potansiyel saldırganları / kötüye kullanımları psikolojik olarak engellemektedir. Ama böylesi bir tehdit modelinin teknik olarak mümkün olduğunu aklımızdan çıkarmamakta fayda bulunmaktadır.

Peki Ahmet, Ethereum tabanında akıllı kontrat yazarak bu işi yapsaydı nasıl olurdu? O zaman güvenli olur muydu?

Aynı şekilde Bitcoin'in maruz kalabileceği %51 saldırısına Ethereum da maruz kalabilir. Bu saldırıyı göz ardı ettiğimizde, bu noktada da ortaya üzerinde düşünülmesi gereken farklı sorular ortaya çıkıyor. Bitcoin yaklaşık 10 yıldır piyasada olmasına rağmen hâlâ "DENEYSEL" bir çalışmadır. Versiyon bilgisine baktığınızda hâlâ 0.15.1, 0.13.3 gibi "0" ile başlayan versiyon bilgisi görmekteyiz, çünkü hâlâ yüzde yüz hazır olduğundan kimse emin değil. Evet yıllardır bir problem çıkmıyor ama önümüzdeki sene çıkmayacağının garantisini kimse veremiyor. Aynı bankanın sürekli güvenlik testlerine tabi tutulması gibi gönüllü araştırmacılarca bulunan sorunlar yamalanarak piyasaya sürülmektedir.

Ethereum'a baktığımızda ise düşünülmesi gereken bir konu daha var. Bitcoin'e göre finansal işlemlerin ötesinde daha karmaşık işlemler içeriyor, blokların üzerine her gün daha fazla kod yazılıyor ve her geçen gün daha çok geliştiriliyor. Yazılımın yaşam döngüsü göz önüne alındığında her zaman yeni bir güvenlik zafiyetinin ortaya çıkma ihtimalini göz önünde

bulundurmalısınız. Bunun yanı sıra da sizin yazdığınız akıllı kontrat kodunun yüzde yüz güvenli olup olmayacağı konusu da gündeme geliyor.

Tarihte ilk en büyük akıllı kontratlar üzerine hack vakası Ethereum'da "The DAO" adı verilen projede yaşandı.

The DAO (Decentralized Autonomous Organization) yani dağıtık otonom organizasyon adı verilen bu projede 2016 yılında 150 milyon Dolar civarında yatırım toplandı ve kimseye ait olmayan aynı zamanda herkese ait olabilecek bir şirket fikri ile ortaya çıktı. The DAO adı verilen token'ı satın alabilir ve satın aldığınız kadar şirkette söz hakkınız olacağı bir yapı hayal edin. Yatırımları yine oylamalar ile farklı projelerde değerlendirerek, yatırımcılara geri dönüşün kâr paylaşımı olarak yapılması hedefleniyordu.

Projeye yatırım yapanlara sunulan bir diğer özellik de aldığınız "DAO Token"'ı projenin ana hesabına geri göndererek 3 hafta bekleme sonrasında yatırıma karşılık gelen miktar da "Ethereum"u cüzdanınıza yüklüyor olmasıydı. Yatırım toplama süresi bittikten birkaç hafta sonra yatırılan 150 milyon doların 30 milyon doları, bu özelliği farklı bir şekilde kullanmayı başaran bir hacker tarafından birkaç saat içerisinde çalındı.

Saldırı sonrası proje tasarım kodu incelendiğinde para çekme, yatırma, oy verme gibi seçeneklerin sırasını farklı şekilde tetikleyerek izinsiz para çekmeye sebep olan bir mantıksal hata tespit edildi.[1] Saldırı sonucunu özetlersek Ethereum ve The DAO projesi ekibi çalışanları ile para çekme işlemindeki üç haftalık zorunlu bekleme süresi sayesinde DAO Hard Fork adı verdikleri yeni güncelleme ile üç hafta içerisinde (tabii ki tüm madencilerin desteğini alarak) yazılımı güncellediler ve hacker'ın çaldığı Ethereum'ları kilitleyerek hacker'ın bu Ethereum'lara ulaşmasını engellediler.

Bir diğer örnek ise "Edgeless" adı verilen dağıtık mimari üzerine kurulmuş bir casino projesi. Bu proje yapılan yatırımından, 2017 Haziran ayında "Parity" (cüzdandaki bakiyenin belirli kişilerce onaylanarak ortak kontrol edilmesini sağlayan bir çeşit akıllı kontrat kodu) kodunda yer alan güvenlik açığı sebebi ile 5,6 milyon dolar çalındı.

Daha yakın bir tarihte Parity akıllı sözleşme (smart contract) üzerinde bulunan başka bir güvenlik açığı sebebi ile milyonlarca dolar değerindeki Ethereum cüzdanlarda kilitli kaldı. Bu güvenlik açığını anlamak için Parity kodunun çalışma mantığını biraz aydınlatmakta fayda var. Parity akıllı kontratının yaptığı işi fiziki olarak günümüz bankalarındaki ortak yönetilen hesaplara benzetebiliriz. Örneğin eşinizle birlikte ortak birikim hesabı açtınız ve düzenli yatırım yapıyorsunuz. Buradaki bakiyeyi kullanabilmek için hesap sahiplerinin ikisinin de imzası / onayı gereklidir. Ethereum üzerinde de bu işlemi yapabilmemizi sağlayan akıllı kontratların en popüleri Parity'dir.

Parity sözleşmesi kullanılarak ortak yönetilen Ethereum cüzdanları üzerinde anahtar sahiplerinin imzası olmadan bakiyelerin dışarı transferi mümkün olmamaktadır. Tüm tarafların imzası gereklidir. Saldırganın bulduğu güvenlik açığı ise anahtar sahiplerinin imzalarını geçersiz kılıp hesap sahiplerinin tüm onaylarını alarak yapmak istedikleri transferleri geri döndürülemez olarak geçersiz kılmaktı. Bu güvenlik açığı nedeni ile yüksek miktarda Ethereum bakiyesine sahip cüzdanlar saldırıya uğramış ve yaklaşık 150 milyon dolar değerindeki bakiyelerin kilitli kalmasına sebep olmuştur.

Ahmet yazdığı projeye MuzikaCoin adını verdi ve maalesef güvenlik üzerine bu konuştuklarımızdan habersiz. Ahmet'in yakın gelecekte "Blockchain Security Researcher" kavramıyla karşılaşmasına sebep olacak bir hack vakası yaşamamasını diliyoruz. (Gerçekten böyle bir proje yok tabii, yaparsanız payımı isterim :))

Blockchain Security Researcher... Kulağa hoş geliyor değil mi?

Güvenli zincirler tasarlamanız dileğiyle.

1 https://www.coindesk.com/understanding-dao-hack-journalists/

Chris Stephenson - cs@chrisstephenson.com

Meltdown ve Spectre Zafiyetlerinin Düşündürdükleri

Meltdown ve Spectre gibi korkunç güvenlik zafiyetlerinin yayınlandığı bir ayda derginizin ilk sayısının yayınlanıyor olması zamanlama açısından harika.

Öncelikle derginize ve bu konularla ilgilenen herkese bir merhaba demek isterim.

Ben de derginiz vesilesi ile Meltdown ve Spectre zafiyetlerinin aklıma getirdiği birkaç sorun hakkında düşüncelerimi aktarma fırsatı buldum.

Niçin güvenlik sorunları?

Güvenlik sorunlarıyla ilgileniliyor. Ticari önemi de çok. Ancak bu sorunların altında yatan sebepler nelerdir? Niçin sistemlerimiz güvenli değil?

İnternetin varlığı yüzünden bütün sistemlerimiz neredeyse bütün dünyaya açık. Bir sunucunuz varsa, en basitinden SSH için 22 numaralı portunuz açıksa[1], sistem loglarına göz attığınızda her saniye birkaç basit login denemesi görmeniz kuvvetle muhtemel. Devamlı saldırı altındayız. Yani devamlı programlarımıza kötü amaçlı giriş denemeleri gerçekleştiriliyor. Peki ama bu saldırılar niçin başarılı oluyor?

Temel sebeplerden biri C diline bağlı. Aslında C dilinin suçu yok. Ve C++ dili de C dilinin bu niteliklerini miras olarak alıyor. Problemlere neden olarak C dilinin şu iki özelliği aslında kâfi; (a) dizi erişiminin sınırları otomatik olarak kontrol edilmiyor (b) dizi hafıza içinde tipi belli olmayan bir pointer. Bu iki nedenden ötürü dizi sınırlarının taşmasını tetikleyen bir girdi, stack üzerinde veriler yazıp saldırı kodunun çalıştırılmasına yol açabilir.[2] (Buffer overrun zafiyeti)

İddia ettiğim güvenlik meselesi büyük ölçüde programlama dilinin yapısal sorunu. C dilinde, Pascal'da olduğu gibi, dizi sınırları her erişimde kontrol edilmekte olsaydı ve referansların tipleri belli olsaydı böylesi bir zafiyetin varlığı mümkün olmayacaktı. Bunu önlemek amacıyla iOS, MS Windows, GNU-Linux işletim sistemlerinde, çalışma zamanında kontroller yapılsa idi, doğal olarak işletim sistemlerimiz bir miktar daha yavaş çalışacaktı. Peki bugün Meltdown'u önlemek için zaten sistemlerimizi yavaşlatmayacak mıyız?

Tabii ki her güvenlik açığı böylesi bir zafiyetten kaynaklanmıyor. Örneğin SQL injection programlama dillerinin başka bir zaafına, tip sistemlerinin zayıf olmasına, bağlıdır. Sorun şu; bir kullanıcı girdisi de SQL sorgusu da aynı tipte, String tipinde oluyor. Aslında bu iki şey farklı tipte olmalı idi. Burada programlama dilinin tip sisteminin bir zaafı söz konusu. Metin bir şeydir, SQL komutu başka bir veri tipidir. Bu ikisinin aynı biçimde yorumlanması bu güvenlik zafiyetine sebep oluyor.

Meltdown ve Spectre açıkları eskilerden biraz farklı olarak doğrudan bir dil sorununa bağlı değil. Spectre zafiyeti, Javascript dilinde yazılan bir kod ile browser üzerinden bile istismar edilebiliyor.

Yine de Meltdown ve Spectre'ye gelirsek ilginç bir şekilde çözümler de programlama dili, yani derleyici aracılığı ile çözülmeye çalışılıyor. Derleyiciler, Meltdown ya da Spectre'ye sebep olabilecek makine kodu işlem dizileri üretmemeye çalışacak. Onlarca milyar işlemciyi hemen değiştiremeyeceğimize göre başka çare de yok. LLVM ve GCC C dili derleyicileri ürettikleri makine kodlarında "retpoline"[3] tekniğiyle Spectre/Meltdown açıklarını kapatmaya çalışıyorlar.[4]

"Legacy" sorunu

"Bütün ölmüş kuşakların geleneği, büyük bir ağırlıkla, yaşayanların beyinleri üzerine kâbus gibi çöker." Karl Marx, *Louis Bonaparte'ın 18 Brumaire'i*.

1 Tabii ki SSH'i başka porta bağladınız değil mi? 22'yi kapatıp başka porta bağlamadıysan elinizi çabuk tutun, makalenin sonunu beklemeden.

2 Tabii ki C dilini yaratanların suçu yok. C dili zamanında önemli bir adımı, ileri bir adımı temsil ediyordu. Ancak nihayetinde C dili, PDP-11 makinesine taşınabilir işletim sistemi (Unix) yazmak için icat edilen bir dil. PDP-11'in temel hafızası 64kbyte. PDP-11'de virtual memory yoktu, ayrı bir kernel state de yoktu. Yani küçük ve hızlı kod önemliydi, bugün bildiğimiz anlamda bir güvenlik imkansızdı. C dili 1973 yılının koşullarına göre tasarlanmış. Sorun aslında 45 sene sonra hâlâ aynı dili kullanmakta olmamızdan kaynaklanıyor.

3 Ayrıntılar Google Project Zero Blogu (https://googleprojectzero.blogspot.com.tr/2018/01/reading-privileged-memory-with-side.html), llvm.org sitesi ve lkml.org sitesinden okunabilir.

4 Google tarafından bu teknik, indirect jump yerine işlemcinin "ret" yani return komutu kullanıyor. "Trampoline" kavramı hem makine seviyesinde interrupt, exception ve case programlamasında hem fonksiyonel dillerde "continuation passing style" ile tail call elimination için kullanılıyor. "Retpoline" kelimesi "ret" ve "trampoline" kelimelerin birleşmesinden geliyor.

45 senelik bir programlama diliyle yazılan en az 30 senelik işletim sistemleriyle[5] bilgisayar sistemlerimizi yönetmeye çalışıyoruz. Bugünkü bilgisayarların sayısı o zamankinden en az bin kat fazla, hızları, hafızaları binlerce kat artmış durumda. Sözünü ettiğimiz sistemler geliştirildiğinde çok az cihaz internete bağlıydı; şimdi neredeyse hepsi internete bağlı. Durum değişti, donanım değişti ama yazılım teknolojimiz yeteri kadar değişmedi.

Yazılımı değiştirmek donanımı değiştirmek kadar kolay değil.

Gelecek için çözüm yolları

Bilgisayar olarak Raspberry Pi kullanıyorsanız, Meltdown/Spectre açıklarından endişe etmenize gerek yok. Pi'deki ARM işlemcisi bu açıklara izin vermiyor. Raspberry Pi'deki ARM basit bir RISC (Reduced Instruction Set Computer) işlemcisi olduğu için speculative execution yapmayıp bu saldırıdan kurtuluyor.

Donanımımızda da bir kâbusumuz var: CISC. x86 işlemci mimarisi geçmişten kalma bir kâbus. Karışık ama güçlü komutlarıyla makine kodunun manuel yazılmasını kolaylaştırıyor. 1980'lerde Stanford ve Berkeley'de geliştirilen RISC mimarisi basit, tek devrede çalışan komutlar, işlemcide bol register kullandığı için aynı hesaplama işi daha az transistor ve daha az enerji tüketerek yapar. Basit komutlarıyla RISC mimarisi de işlemcinin "pipeline" boru hattı çalışmasını kolaylaştırıyor. İşlemci komutları adım adım işlemci içindeki bir boru hattından ilerliyor ve aynı anda birden fazla komut değerlendiriliyor. Bu da bazen komutların sıradışı ("out of order") değerlendirilmesine yol açıyor.

Örneğin bir atla ("Jump") komutu derleniyor, bununla beraber bir sonraki komut da derleniyor. Bu "Branch Delay Slot" olarak biliniyor. Makine dilinde yazılacak programlar için programcılık zor bir sanat oluyor. Ancak makine dilinde kim program yazıyor ki? Derleyiciler yüksek seviyeli dillerde yazılan programları derleyerek makine diline çeviriyor. Yani bu zor işi derleyiciye bırakabiliriz. Derleyiciyi yazan deha bu sorunu bir defa çözüyor, biz de faydalanıyoruz.

Intel ve müritleri uzun bir zaman CISC için direndi. Ancak RISC kazandı. RISC mimarisinin daha düşük elektrik tüketimi yüzünden dünyadaki işlemcilerin ezici çoğu (%95'i ?) RISC. Sadece iPhone ve Android telefonlarındaki (RISC mimarisi) ARM çipleri bu çoğunluğu sağlıyor. Intel'in Pentium çipleri de P6 modelinden itibaren bir RISC çekirdeği içeriyor. CISC komutları RISC'e çevrilip değerlendiriliyor.

RISC komutlarının doğrudan programlar tarafından kullanılabilmesi bir avantajı daha beraberinde getiriyor. İstersek "out of order" sorunlarının çözülmesini derleyiciye bırakabiliriz. x86 işlemcileri bu sorunları kendi kendine çözmek zorunda. AMD'nin iddialarına göre AMD çiplerinde speculative execution çip üzerindeki bir "yapay zekâ" ünitesinin yardımıyla yapılıyor.

Ancak işlemci tahminlerde bulunmak zorunda değil. Makine kodlarını üreten derleyici atlamalar ve döngüler konusunda bilgiye sahip. RISC'in başırılı mantığı buydu.

Son kuşaklarda RISC işlemcileri ve CISC işlemcileri arasında bir miktar "convergence" oldu. Yani birbirine benzemeye başladı. Bu yüzden bu en son ARM (RISC mimarisi) işlemciler da Spectre açığına kurban olabilir. Teoride ARM (ve Intelden farklı bir x86 mimarisi olan AMD) Meltdown kurbanı olabilir, ancak araştırmacılar pratikte bunu uygulamayı başaramadılar.

Gelecek için düşünceler

Galiba Spectre/Meltdown ve benzer sorunlar RISC için seçilen yoldan daha kolay çözülür. RISC yaklaşımı programlama dilleri ve onu derleyicilerini kullanarak sade tutulan bir işlemciden azami performans sağlamak. Belki bu uzun vadede daha mantıklıdır.

Spectre/Meltdown sorunu işlemcinin "speculative execution" yapmasına bağlıdır. Bu "speculative execution", "Branch Delay Slot" gibi derleyici tarafından üretilen kodun kontrolü altında olsaydı, sorun bir derleyici değişimiyle hallolurdu.

Galiba daha genel bir krize doğru gidiyoruz. İşlemciler ve bağlılık düzeyleri artıyor. Dünyada bir trilyon işlemciye doğru gidiyoruz. Bu basit bir hesapla, kişi başına 130 işlemci demek. Evinizde kaç işlemci var? Kredi kartları ve telefonun içindeki SIM kartlarının çiplerini de saymayı unutmayın. Şu anda bu yazıyı okuyan Türkiyeli bir okurun sahip olduğu tahminen 100 kadar işlemci var.

Ancak bilgisayarların artan bu gücü hiç güvenli değil. Ne sunucular ne "Internet of Things" aletleri. Aslında Blockchain içine gömülen programlar da sorunlu. Bir şey yapmalı!

"Speculative Execution" ile başımız beladayken, ben de biraz spekülasyon yapmak isterim:

Büyük değişimler hep zor görünüyor. "Backward compatibility" Karl Marx'ın 1848'de öngördüğü sorundur. x86 ve C dilinin garipliklerinden kurtulamıyoruz. Yine de bazen değişim "yandan", yani (hiç beklemediğimiz noktadan) gerçekleşiyor. Yıllarca "Ne zaman desktop'ta GNU Linux kazanacak?" sorusunu soruluyordu. En az ben soruyordum. Olmadı. Ama bu mücadele fark etmediğimiz bir şekilde bitirildi. Desktop'un önemi çok azaldı. Diğer taraftan sunucu alanında GNU Linux ve benzerleri tartışılmaz bir zafer kazandı. Bireysel kullanımda cep telefonu ve tablet masaüstü bilgisayarları gölgede bı-

5 Unix 1974, Microsoft Windows 1986, GNU Linux 1991. iOS da Unix tabanlı. Yani en genç olanı 27 yaşında.

raktı. Sadece MS Windows değil, Intel'den de vazgeçildi. Zafer kazanan taraf Unix/GNU Linux tabanlı olan iOS ve Android oldu. Ve ARM işlemcisiyle kazandılar. Daha da ilginci, ikisi de aşağı yukarı tek programlama dilli ortamlar yarattı. Android için Google maalesef Java'yı seçti, Apple önce Pascal, sonra Objective C, sonra Go. Ancak önemli olan şu ki, kullanıcıya tutarlı bir deneyim sunabilmek için geliştiriciye çok sınırlı bir programlama dili seçeneği verildi.

Maalesef Google ve Apple programlama dili meselesinde, şirketler olarak, radikal adımlar atacak kadar cesarete sahip değiller. Söylemek acı, ama programlama dilleri araştırma alanında Microsoft daha ileri. Avrupa'da Microsoft Research bir dizi iyi araştırmacıya ev sahipliği yapıyor. Tip güvenliği açısından C#, Java'dan daha sağlam bir dil; F# ve F* dillerinin benzerleri Google ve Apple'den çıkmıyor. Go, Dart ve Swift kaçırılmış fırsatlar.

Bu güvenlik sorunlarını çözecek yeni bir paradigma değişimi mümkün mü? Yani Android ile böyle bir şey oldu. Yeni işlemci tipi, (görece) yeni işletim sistemi (yozlaşmış bir GNU Linux) ve tek dilli bir ortam (ne yazık ki, Java).

Blockchain dünyasında[6] güvenli, ispat edilebilir bir biçimde çalışacak programlara ihtiyaç var. Blockchain dünyasında bu ihtiyacı karşılamak için Simplicity, Obsidian, F* gibi diller öneriliyor. Genellikle fonksiyonel, sofistike bir şekilde statically typed, ve bazen Turing incomplete. Turing incomplete, finitistic dillerde halting sorunu çözülebilir. Programların doğruluğu da ispatlanabilir.

Blockchain dünyasında bu yeni diller en temel bilgisayar bilimleri teorisine dönüyorlar. Lambda calculus, simple typed lambda calculus, SKI combinators bu diller altında yatıyor.

Bu sorunları kökten çözeceksek bence programlama meselesini tekrar gözden geçirmemiz lazım. Ve donanım yazılım ilişkisi burada önemli bir rol oynayacak. RISC atılımı ile bu küçük çaplı da olsa başarılmıştı. Yazılım donanım ilişkisinde önemli bir değişim olmuştu.

Blockchain dünyası henüz çok yeni olduğu için böylesi yeni atılımlar oralarda mümkün. Acaba göremediğimiz "geriye uyum"un olmak zorunda olmadığı bir alanda yeni, daha güvenli, bir programlama donanım ilişkisi ortaya çıkabilir mi? Programlama dili ve donanımın uyum içinde güvenliği sağladığı bir ortam. Tabii ki eski arkadaşımız GNU Linux'u da geride bırakmak zorunda oluruz.

Haskell gibi güçlü bir static type system, bir ihtimalle finitistic, yani Turing incomplete, fonksiyonel bir dil ile beraber uygun bir donanım olabilir mi? Bilmem. RISC'in zaferi icadından itibaren 25 sene sürdü. Bilgisayar dünyamız yeni teknolojiler konusunda o kadar hantal ve muhafazakâr ki hızlı gelişmeler beklemek zor.[7] Yoksa yamalara devam edeceğiz ve dünyamız gitgide bozulan sistemler sayesinde daha tehlikeli olacak.

Bilgisayar Bilimleri Eğitimi

Bu konudaki bir başka düşüncem ise şu, acaba kaç Bilgisayar Bilimleri/Mühendisliği lisans programı Spectre/Meltdown sorununu anlayacak bir teknik bilgi verebilir? 25 sene önce verilirdi. Şimdi? Türkiye'ye özgün bir sorun değil. Müfredatlarına bakıyorum uzun süre değişmemişler, ancak anladığım kadarıyla çoğu yerde eğitimin içi boşaltılmış. Lisans mezunu bilgisayar mimarisinde virtual memory, page tables, onların cache, hafıza cacheleri ve pipeline işlevinin ne demek olduğunu öğreniyor mu? Makine dilinde bir program yazabilir mi? Derleyicinin kod üretiminden anlar mı? Yüksek düzeyli dillerin rolünü kavramış mı? Ya da lambda calculus, Turing completenes ve incompleteness, type systems ne demek bilir mi? Şahsen 20 sene önce bunların çoğunu derslerimde anlatıyordum. Bence şimdilerde çoğu üniversitede verilmiyor.

Yanıldıysam, haber verin de sevineyim. Gelecekte bilgisayar alanında üniversiteler işe yarayacaksa bu konulara özel bir önem verilmeli. Yoksa bu iş başka kurumlarda yapılacak. Üniversiteler için (birkaç elit kurumu hariç) çok fazla umudum kalmadı.

Sonuç

Meltdown / Spectre sorunu beni teşvik etti. Umarım yazdıklarım da okuyucular olarak sizleri yeni düşünceler / fikirler konusunda teşvik etmiştir. Hepimize kolay gelsin.

6 Kripto paraları bir saadet zincirinden ibaret (T24'deki makaleme bakınız http://t24.com.tr/yazarlar/chris-stephenson/bilgisayar-bilimcisi-gozuyle-kripto-para-ve-yatirimciya-tavsiyeler,18768). Ancak Blockchain teknoloji ve otomatik sözleşme gibi uygulamalar önemli bir alan olabilir.

7 Fizik bilimini düşünün. 1932 yılında Neutron keşfedildi. Daha önce bilinmiyordu. 10 sene içinde nükleer reaktör, 13 sene içinde atom bombası yapıldı. İkisi Neutron'un varlığına bağlıydı. Microsoft Windows'dan legacy 16 bit kodunun çıkartılabilmesi atom bombasının gelişmesinden daha uzun sürdü.

Ulaş Fırat Özdemir - htcinian@gmail.com

KRACK
(Key Reinstallation Attack
Anahtarı Tekrar Oluşturma Saldırısı)

Bu yazımda sizlere çoğu internet arayüzünü korumakta olan ve geniş bir cihaz skalasının kablosuz iletişim güvenliğini sağlayan WPA2 protokolündeki bir zafiyetten bahsedeceğim.

KRACK Nedir?

KRACK saldırısı güvenli olarak adlandırılan ve kullanıcı cihazı ile internet sağlayıcı cihaz arasındaki kablosuz iletişimi koruyan WPA2 protokolü üzerinde bulunan bir zafiyettir. WPA2 protokolü cihazlar arasında parola değişimi yaparak güvenli bir şekilde kimlik doğrulaması yapar ve eğer paylaşılan parola doğru ise yetkilendirme yapıp internete bağlanmamıza izin verir. Bu protokol aynı zamanda iki cihaz arasındaki iletişimi şifreler ve şifreli bir bağlantı sağlar. Bu sayede dışarıdaki saldırganlar bu protokolü kullanan cihazlara saldıramazlar. En azından KRACK'e kadar bu protokolün güvenli olduğu düşünülüyordu.

KRACK saldırısı bize kablosuz bağlantı sağlayan cihazın parolasını vermez. Bu çok karıştırılsa da bu saldırı bize aradaki şifreli bağlantıyı güçsüz kılacak ve şifreleme mekanizmasını güçsüzleştirecek bir yöntem sağlar. Cihaza bağlantı parolasını bize vermez ve bilmemize de gerek yoktur. Bu saldırı sayesinde kimi cihazlarda kullanıcıya gelen paketlerin, kimilerinde kullanıcıdan giden paketlerin, kimisinde ise çift yönlü iletişimin şifresini çözmemizi sağlar. Bazı durumlarda ise şifreli iletişim olsa dahi aradaki doğrulamayı (mesaj bütünlüğünü) sağlayan hash anahtarını bularak bütünlüğü değiştirmemizi ve paketlerin içeriğinde oynama yapabilmemizi sağlar.

Parola, Şifre ve diğerleri

Olası bir kavram kargaşasına mâni olmak adına genellikle birbirine karıştırılan parola, şifre ve benzeri kavramları (gizli sözcük, kod) incelemek istiyorum. Şifre kelimesi Türkçemizde bizden bizi tanımlayacak ve/veya kimliğimizi, işlemlerimizi doğrulama amacıyla oluşturulan metin şeklinde kullanılmaktadır. Örneğin, banka şifreniz 4 haneli, resimdeki şifreyi giriniz, şifreli konuşuyor vb. Parola ise daha çok filmlerde, ajanların veya askerlerin birbiri ile iletişimde kullandıkları söz olarak hafızalara kazınmış durumda.

Aslında kelime kökenine bakılırsa şifre (ing. Cipher) İtalyanca'da sayı anlamına gelen "cifra" kelimesinden gelmektedir. Parola ise yine İtalyanca'dan gelmektedir ve anlamı sözdür. Buradan anlayabileceğiniz gibi şifreler sayılar, karakterler ve işaretler kullanılarak oluşturulmuş metinlerdir. Parolalar ise bizim bildiğimiz ve aklımızda tuttuğumuz ve belirlediğimiz salt metinlerdir. Parolada da farklı karakterleri görmek mümkündür ama bizden alınan parola alındığı gibi saklanmaz. Parola alındıktan sonra matematiksel işlemlerden geçerek şifre dediğimiz metni oluşturur ((ing.) parola:password, şifre:cipher)

WEP, WPA ve WPA2

Kablosuz iletişim teknolojilerinin güvenliğini sağlayan ve geniş ölçekte kullanılan üç protokol vardır. Bunlar WEP, WPA ve WPA2'dir.

WEP

- WEP kablosuz iletişimde kullanılan ve IEEE 802.11b'de tanımlanmış bir protokoldür.
- WEP kablosuz iletişimde tanımlanmış ve standart haline gelmiş ilk protokoldür.
- WEP kablolu ağlar kadar güvenli bir iletişimi amaçlamaktadır.
- WEP'de bir sürü güvenlik açığı vardır ve yeni yöntemlere göre ayarlaması daha zordur.
- 24 bit IV kullanır ve bu nedenle güçsüzdür.
- RC4 akan şifreleme ile birlikte 64/128 bit anahtar kullanır ve ana anahtar el ile girilmelidir.

WPA

- WPA, WEP'de bulunan zafiyetleri gidermeyi amaçlamaktaydı.
- WEP cihazları ile uyumludur ve donanımda bir değişikliğe gerek kalmaz.
- Kişisel ve kurumsal adında iki modu vardır.
- RC4 şifrelemeyi kullanmaya devam eder ama anahtar boyutu 256bit'dir.
- Her bir alıcı TKIP sayesinde kendi şifresini almaktadır.
- Kurumsal modu 802.1X ve EAP kullanarak kimlik doğrulaması yapar.
- Bu nedenle kurumsal kullanımda daha güçlü olmasına rağmen bir sürü saldırı yöntemine açıktır.
- Artık kullanılması güvenli değildir.

WPA2

- Yeni donanımlar ile birlikte gelen standarttır.
- Kişisel ve kurumsal modları mevcuttur.
- RC4 ve TKIP yöntemlerini AES (blok şifreleme) ve CCMP ile değiştirir.
- WPA'ya göre daha karmaşık anahtar üretimi yöntemlerine sahiptir.
- Üretilen anahtara karşı kaba kuvvet saldırıları düzenlenebilse de anahtarı trivial/uygun bir zamanda bulmak mümkün değildir.

WPA3

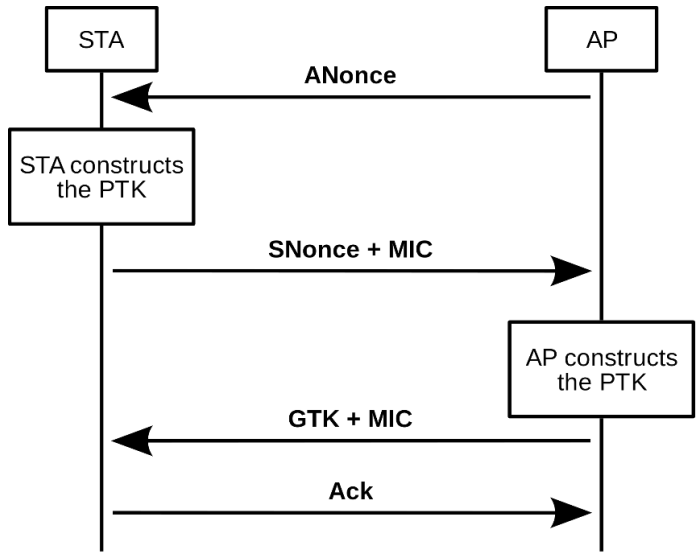
- WPA2'de bulunan zafiyetlerden sonra daha güvenli bir protokol kullanma zamanı gelmiştir.
- Protokol 8 Ocak 2018'de duyurulmuştur ve taslağı üzerinde tartışmalara başlanmıştır.
- Protokolün 2018 yılının ortalarına doğru açıklanması beklenmektedir.

Bazı özellikleri;

- IoT gibi ekranı olmayan cihazların bağlantılarını kolaylaştıracaktır.
- Kullanıcılar güvenli olmayan parolalar koysalar bile güvenliği sağlayacaktır.
- Umumi yerlerdeki kablosuz internet güvenliğini iyileştirmek için kişisel şifreleme kullanılacaktır.
- Bu yöntem her kişiye farklı bir anahtar ile şifreleme sağlayarak güvenliği arttırmayı hedeflemektedir.
- Kaba kuvvet saldırısı yapmaya çalışan cihazların bağlantılarını düşürerek kaba kuvvet saldırılarını zorlaştırmayı planlamaktadır.

Dörtlü El Sıkışması

WPA2 eski protokollerden farklı şekilde parolayı şifreli bir şekilde kablosuz kanallardan göndermez (parolayı göndermez, iki tarafta işlemler yaparak kimlik doğrular). Bunun yerine iki tarafın da aynı bilgilere sahip olduğunu doğrulamak için bir metin gönderir ve metin kullanılarak oluşturulan cevaba göre şifreleme işlemini başlatır.



Bu şemayı açıklamak gerekirse AP bizim bağlantı yapmak istediğimiz cihaz olurken STA da bizi temsil etmektedir.

Şifreleme yapılabilmesi için önce doğrulama yapılması gerekir. Bu doğrulama ve şifreleme ile şifre çözmede kullanılacak parolanın şifreli bir kanaldan gitmesi gerekmektedir. Bu şifreli kanalda şifreleme yapmak için kullanılan anahtara PTK diyeceğiz. PTK anahtarı PMK (wireless parolası ya da 802.1x ile elde edilen parolanın SHA1 hali) ile bazı bilgilerin yan yana gelmesiyle oluşur. (|| birleştirme olarak adlandırılacaktır):

PTK = PMK || ApNonce ||STaNonce ||ApMac || STaMac

Nonce değerleri rasgele üretilen değerlerdir. AP ile başlayan değerler AP tarafından, STA ile başlayan değerler ise STA tarafından sunulur.

1) İlk önce AP cihazı bize kendi ürettiği nonce değerini ve MAC adresini verir. Bu sayede STA cihazı PTK anahtarını üretmek için gereken bütün veriye sahiptir ve PTK anahtarını oluşturur.

2) STA cihazı AP cihazına kendi ürettiği rastgele değeri gönderir. Bu sayede AP cihazı da PTK anahtarını üretir. Artık aralarında konuşmaya hazırlardır.

3) AP cihazı STA cihazına geri kalan iletişimi şifrelemede kullanılacak GTK anahtarını gönderir. Bu anahtarı daha önce bildikleri PTK ile şifreleyerek gönderir. Bu sayede dışarıdan din-

leyen birisi şifreyi çözememektedir. Bu adım sayesinde STA cihazı şifre üretmek için gereken parametreleri alır ve şifre üretimine başlamak için var olan değerleri ayarlar ve şifre üretimine başlar. (Bu ayarlama esnasında var olan sayaç gibi değerleri sıfırlar.)

4) STA cihazı GTK anahtarını aldığına dair cevabı döndürür.

Bu durumda STA cihazının Ack cevabını döndürememesi ya da GTK cevabının yolda kaybolması koşulunda STA cihazı 3. Kısmı tekrar gönderebilmektedir. Bu paket, yakalamamız sayesinde paketi istediğimiz kadar tekrarlayabilmekteyiz.

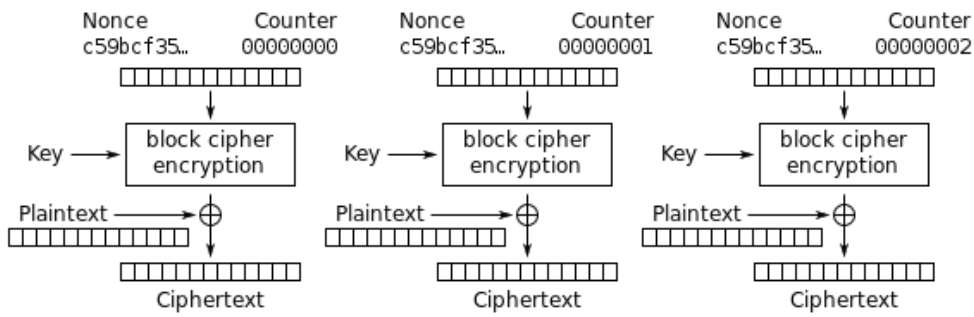
KRACK

KRACK saldırısı daha önce de bahsedildiği gibi aradaki şifrelemeyi sağlayan anahtara ihtiyaç duymaz. Bu saldırı iki cihaz arasında yapılan 4 yönlü el sıkışma protokolünde bulunan bir açıktan faydalanır. Bu protokolün 3. Adımında internet sağlayan cihaz kullanıcı cihaza el sıkışmanın gerçekleştiğine dair bir paket gönderir. Bu paketi alan kullanıcı cihaz anahtarın kurulumunu tamamlar ve verileri şifrelemeye başlar. Bu paketin havada kaybolmuş olabileceğini düşünen internet sağlayıcı cihaz bu paketi tekrar gönderir. Yani kullanıcı cihazı bu paketi birden çok defa alabilir. Her aldığında anahtara şifrelemede yardımcı olan IV (başlangıç vektörü) ve paket sayacını sıfırlar ve tekrardan anahtarın kurulumunu sağlar. Bu sayede her seferinde aynı anahtar ve başlangıç vektörü ile şifreleme yapmış olur.

Peki nedir bu başlangıç vektörü ve paket sayacı? WPA2 protokolü blok şifreleme metotlarından birisi olan AES ile şifreleme sağlar. AES blok şifrelemenin sayaç modu (CTR) ile şifreleme yapar. Bu şifreleme metodunda girdi olarak nonce/IV (başlangıç vektörü) kullanılır ve sayaç ile birleştirilir (concat.). Bu nedenle her seferinde ortaya çıkan şifre farklı olur. Paket sayacı 128 bitlik bir değer olup her paket ile değişim göstermektedir. AES şifreleme, CTR modu ve blok şifreleme nasıl yapılır?

0) Başlangıç vektörü ve şifreleme algoritması belirlenir.
1*) Veri bloklar halinde ayrılır (32 bit).
1.a*) Nonce, Counter vb. bilgileri kullanılmaya başlanır.
2*) Her blok için XOR işlemine tabii tutulacak giriş belirlenir (Counter ise counter belirlenir, yoksa XOR'lar sıralanır)
3*) Her blok XOR işlemine tabi tutulur.

Yeni bloklar sıralanır ve iletişimde kullanılır (* ile belirtilen işlemler blok şifrelemenin genel kullanımına aittir, 0 numaralı işlem blok şifrelemenin modunu belirler).



Counter (CTR) mode encryption

Görebileceğiniz gibi her bir bloğu özel kılan şey nonce değeri (IV) ile counter değeridir. Counter ve nonce birleşip blok şifrelemenin bir parçasını oluşturur. Peki counter olmasa, sadece nonce ve key ile bir şifre üretsek ve bu şifreyi metin bloklarına uygulasak ne olurdu?

Eğer her seferinde aynı şifreyi kullanırsak çıktımız her seferinde aynı olacaktır. Bu nedenle iki şifreli bloğu birbiriyle XOR işlemine tabi tutarsak şifre kısmını yok edebiliriz (m_1 x ş x m_2 x ş = m_1 x m_2) Bu sayede eğer m_1 veya m_2 mesajlarının bir kısmına sahip olursak diğer mesajı da elde etmemiz mümkündür. Aynı zamanda mesajlardan birine sahip olursak şifreyi de elde edebiliriz. Bu nedenle şifrelemede kullanılan parolaya ihtiyacımız kalmaz. KRACK saldırısı şifreyi aynı tutabilmek için tek değişen değer olan counter değerini sabit tutmaya çalışmaktadır. Dört adımlı el sıkışmanın üçüncü adımındaki paketi tekrar yollayarak counter değerini sıfırlayabilmektedir. Bu sayede her seferinde aynı şifreye sahip olup bu şifre ile metni çözebilmektedir. Bu saldırı standartlarda tanımlı olan bir noktayı kullandığı için cihaz fark etmeksizin WPA2 yöntemini kullanan bütün cihazlar için geçerlidir. Bu nedenle cihazınız için yayınlanmış güvenlik güncelleştirmesini yükleyiniz.

Burada bahsedilen matematiğin mucizesi için dergimizdeki kriptografi köşesini takip etmeyi unutmayın.

Zafiyetlerle Bluetooth: Geçmişi ve Geleceği

Birçoğumuzun hayatına telefonlar sayesinde giren Bluetooth artık hayatımızın her alanında yaygın biçimde kullanılan bir teknoloji haline gelmiştir. IoT ve Endüstri 4.0 sayesinde neredeyse bütün cihazlar internete bağlanabilecek, birbirleriyle konuşabilecek bir hale gelmekte. Sadece ev eşyaları ile sınırlı kalmayıp kapı kilitlerinden insansız hava araçları arası iletişime, kalp pili sensörlerinden kablosuz hoparlör ve kulaklıklara kadar birçok alanda Bluetooth teknolojisi kullanılmakta. Gelişmekte olan Bluetooth 5 ile gelen örgü ağı teknolojisi ile kapsama alanını 30.000 kilometreye kadar genişletebilmektedir. Peki, Bluetooth teknolojisi nasıl doğmuştur hiç merak ettiniz mi? Bu yazıda Bluetooth'tan bahsedeceğim ve bu sayede hem Bluetooth'un iç yapısı ve çalışma mantığı ile tanışırken, hem de bir kablosuz teknoloji olan Bluetooth'un aslında hayatımıza kattığı riskleri ve bu teknolojiye karşı yapılmış saldırıları inceleme şansınız olacak.[1]

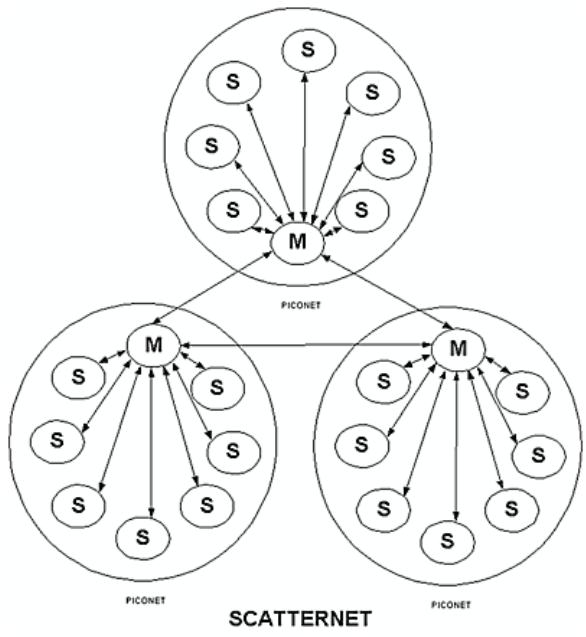
BLUETOOTH'UN DOĞUŞU

Ericsson şirketi 1989 yılında seri iletişimin (RS-232) kablosuz alternatifini oluşturmak için çalışmalara başlar. 1989 ve 1992'de Ericsson şirketinde çalışmakta olan Dr. Jaap Haartesn teknolojinin temellerini oluşturan iki adet patent alır. 1996 yılında ise Nokia ve benzeri şirketler Bluetooth gibi kısa mesafeli bir protokol arayışı içine girerler. Bu şirketler Bluetooth Special Intrests Group (SIG) adı altında toplanırlar. Günümüzde de teknolojinin markası ve lisansı SIG'e aittir. Bluetooth teknolojisi adını 10. yüzyılda yaşamış olan Danimarka ve Norveç kralı Harald Blaatand'dan almıştır. Haarald İskandinavyalı kabileleri tek bir krallık altında birleştirmeyi başarmıştır ve sayısız savaşa katılmıştır. Bluetooth ise İskandinav kralın mavi bir meyve olan yaban mersinine olan ilgisinden ilhamla bu adı almıştır. Bluetooth, taşınabilir ya da sabit elektrikli aletlerin kısa mesafede iletişimini gerçekleştiren evrensel bir standart oluşturmak amacıyla tasarlanmıştır. Genelde bahsedilen cihazlar (o devirde) seri iletişim ile haberleştiğinden bazı kaynaklarda seri iletişimi kablosuz hale getiren teknoloji şeklinde de tanımlanır.

2.4Ghz bandında çalışan Bluetooth üç güç sınıfında kablosuz iletişim kurmak için tasarlanmıştır. Bunlar kısa mesafe (10-100 cm), olağan mesafe (10m) ve uzun mesafe (100m) den oluşur (Sridhar, 2008).

Bluetooth artık hayatımızda daha aktif bir rol oynamaya başlamış olsa dahi kullanıcıların bilgisinin yetersiz kaldığı alanlar bulunmakta. Bu alanlardan birisi de teknolojide bulunan zafiyetler sayesinde oluşan güvenlik riskleridir. (Laurie, Holtmann, & Herfurt, 2006).

Bluetooth teknolojisi ana cihaz ve buna bağlı yedi köle cihazdan oluşan bir yapıdadır. Bu yapıya PictoNet adı verilir. Köleler ana cihazdan maksimum 10 metre uzakta bulunabilmektedir. Pictonetler birleşerek Scatternet'leri oluştururlar. Ana cihaz köle cihazlarla konuşur, köleler ile direkt konuşmak mümkün değildir.



1 Bluetooth Special Intrests Group 5 Temel şirketten oluşmuştur;Bu şirketler Ericsson, Nokia, Intel, Toshiba ve IBM'dir Apple ve Microsoft da sonrandan dahil olmuştur. SIG 32302 üye, 594 ortak ve 7 destekçi şirketten oluşmaktadır. SIG e dahil olmak ücretsizdir, www.bluetooth.com linki üzerinden siz de dahil olabilirsiniz. Eğer çalışma gruplarına dahil olmak ya da spesifikasyonları belirlemek istiyorsanız küçük bir ek ücret karşılığında üyeliğinizi Ortak (Associate) üyeliğe yükseltebilirsiniz. Ortak üyeliğin avantajları için web sitesini ziyaret edebilirsiniz. SIG basit üyeliği alarak Bluetooth protokolünü inceleyip blogları ve haberleri inceleyerek protokol ile ilgili gelişmelerden haberdar olabilirsiniz.

BLUETOOTH GÜVENLİĞİ

Bluetooth protokolü üç güvenlik modeli tanımlar. 1. Güvenlik Modu hiçbir güvenlik uygulamasına sahip değildir. Cihazın kendini koruması için gereken adımların hiçbirini uygulamaz. 2. Güvenlik Modu servis seviyesinde güvenlik sağlar. Yani iletişim kurarken güvenli servisi kullanan bir uygulama nispeten güvende olsa dahi cihazın güvenliği ile ilgili ekstra bir koruma eklenmemiştir. 3. Güvenlik Modu'nda ise bağlantı seviyesinde bir güvenlik tedbiri uygulandığından, bazı izinsiz giriş yöntemlerine karşı korumalıdır. Her Bluetooth servisi temelinde bir güvenlik moduna sahiptir, bu modun altında kendi güvenliğini üç seviye ile sağlayabilir. Kimi servisler yetkilendirme ve kimlik doğrulama kullanırken, diğerleri sadece kimlik doğrulamayı kullanabilir ya da her cihaza açık olabilir. Bu protokolü kullanan cihazlarda ise iki farklı güvenlik modeli vardır. Bunlar güvenilen cihazlar ve güvenilmeyen cihazlardır.

Yani kısaca özetlemek gerekirse Bluetooth üç farklı katmanda güvenlik sağlar. Protokol bazında güvenlik modları, uygulama ve servis bazında yetkilendirme ve kimlik doğrulama, cihaz bazında güven modeli.

SALDIRI YÖNTEMLERİ

Bluetooth protokolüne ve kullanan cihazlara karşı geniş bir saldırı vektörü bulunmakta. Bu vektörü kullanarak oluşturulan ve renkli isimlere sahip bir sürü saldırı vektörü bulunmaktadır. Mavi dinleme, mavi çarpma, mavi çalma, mavi öpme, mavi kandırma, mavi bıçaklama ve daha niceleri. Bütün saldırılar Bluetooth'da bulunan bir açığı kullanarak saldırganın, kurbanın telefonuna yetkisiz erişimde bulunmasını amaçlar. Bu erişim sayesinde yetki yükseltme ile veri değişiminden cihaz kontrolüne, başka cihazlara saldırmaktan delil yok etmeye kadar bir sürü saldırı oluşturmak mümkündür. Bluetooth cihazlarını genelde kısa mesafeli olarak düşünürüz, ama Bluetoone teknolojisi ile yüksek kazançlı antenler kullanılarak 1500 metreye kadar, Bluetooth 5 ile yeni gelişen ağ yapısı sayesinde ise bu saldırılar kilometrelerce mesafeye kadar çıkartabilmektedir.

Saldırganların genel yöntemi hatalı dosyaların aktarımı ile beklenmedik sonuçlar oluşturmaktır. Bir sistem beklenmedik bir hatalı dosya alınca ve belirlenen güvenlik seviyesine yetersiz ise ya dengesiz bir duruma düşer ya da sistem çöker. Bu durumlardan yararlanan saldırganlar zafiyete sahip cihazlar üzerinden bir sürü saldırı gerçekleştirebilmektedir.

Bu saldırılar sonucunda yapılabilecekler listesi bir hayli geniştir. Adınıza arama yapma ve mesaj atma. Dosyalarınızı görüntüleme, değiştirme veya güncelleme. Fotoğraf, video veya ses gibi hassas içeriğe sahip olabilecek medyaları oluşturmak suretiyle özel hayata müdahale. Veri hırsızlığı ve sonrasında bağlantılı olarak maddi değer hırsızlığı. Cihazınızı bir saldırgan cihaza dönüştürme. Kısacası protokolün bulunduğu cihazda ana yetkili (root) seviyesinde yetkiye sahip olarak gerçekleştirebileceğiniz bütün işlemlere erişim hakları bulunmakta.

Bu durum genellikle Bluetooth ve benzeri çiplerin ana çipe doğrudan bağlantılı olması ve ana çip üzerinde yetki sınırlandırılması yapılmamasından kaynaklı oluşur, yani yetki bakımından sınırlandırılmamış Bluetooth bir de zafiyete sahip olunca saldırganların hedefi haline gelmektedir.

BLUEBORNE

2017 yılının Eylül ayında yayınlanan Blueborne adındaki zafiyet Bluetooth teknolojisinin ne kadar korkutucu sonuçlara yol açabileceğini bir kere daha gözler önüne serdi. Bu saldırı sayesinde birçok cihazda uzaktan kod çalıştırmak mümkün hale geliyordu, yani sizin yapabileceğiniz etkileşimi uzaktan ulaşılabilir hale getirmekteydi. Peki Blueborne saldırısının daha önce bahsettiğimiz saldırılardan farkı ne?

Daha önce bahsettiğim saldırılar bir kullanıcı izni sayesinde gerçekleşiyordu, bir dosya transfer isteği, bağlantı isteği, cihaza güvenme isteği vb. yani son kullanıcının haberi her zaman oluyordu. Bu tarz istekleri kabul ettiklerinde ise saldırıya maruz kalabiliyorlardı. Blueborne bize uzaktan sömürülebilen zafiyetleri ve Bluetooth üzerinde benzeri zafiyetlerin etkisini gösterdi.

UZAKTAN SÖMÜRÜLEBİLEN ZAFİYETLER

Uzaktan sömürülebilen zafiyetler, hiçbir kullanıcı etkileşimi gerçekleştirmeden yararlanılabilen zafiyetlerdir. Bu türe ait üç ana temel niteliğinde kural bulunmaktadır.

1) Sömürebilmek için hiçbir insan etkileşimine ihtiyaç duymamalı.

2) Sistemin aktif durumu ile ilgili karmaşık varsayımlarda bulunmamalı.

3) Sömürüldükten sonra sistemi istikrarlı bir halde bırakmalı.

Yani anlayabileceğiniz üzere ruhunuz dahi duymadan sizin üzerinizden zafiyeti kullanarak daha önce belirttiğim bütün saldırıları gerçekleştirmek mümkün.

Blueborne konusuna tekrar değinecek olursak, bir saldırgan Bluetooth teknolojisini kullanarak kilometrelerce öteden bir Bluetooth saldırısı sayesinde bir bireyin ve hatta kitlelerin cihazlarına ulaşabilmekte, kendi planlarına göre ve gizli bir şekilde manipüle edebilmektedir.

BLUETOOTH ZAFİYETLERİ

Daha önce dilim döndüğünce Türkçeye çevirmeye çalıştığım saldırı vektörlerine bu kısımda değinmeye çalışacağım. Öncelikle kavramları açıklamak isterim.

Bluesnarf (Mavi tüketme)

Belki de bilinen en yaygın saldırı şeklidir. OBEX (obje değişimi) protokolü, Bluetooth uygulama katmanında iş kartları

ve diğer objeleri almak için geliştirilmiştir. Bluesnarf saldırısı OBEX GET isteği sayesinde bilinen dosyalara erişim sağlayabilmektedir. Eğer kurbanın Bluetooth sürücü yazılımı hatalı konfigüre edilmiş ise saldırgan GET isteği ile cihazdaki bütün dosyalara erişim hakkına sahip olur. Çoğu durumda bu servis kimlik doğrulama gerektirmez, bu nedenle herkes tarafından kullanılabilmektedir.

Bluesnarf++ (Mavi tüketme++)

Bu saldırı Bluesnarf saldırısına benzemektedir. Ana farkı ise saldırganın dosya sistemine giriş sağlanırken kullanılan yöntemdir. Eğer OBEX üzerinde bir FTP (Dosya Transfer Protokolü) sunucusu çalışıyor ise OBEX Push servisi sayesinde cihazla eşleşme olmadan bu servise bağlantı sağlanabilmektedir. Kimlik doğrulama ve eşleşme olmadan dosyaları görüntüleyip değiştirme yetkilerini ele geçirirler.

Bluebug (Mavi böcek)

Bu zafiyet saldırganın Bluetooth cihazı üzerinde yetkisiz işlemler gerçekleştirmesini sağlar. Bazı cihazlar Bluetooth teknolojisinin kullanmış olduğu AT (Ascii Terminal) komutlarını yine Bluetooth üzerinden kabul edebilmektedir. Bu sayede saldırgan istediği AT komutlarını kullanarak cihazı kontrol etmeye başlar. Bluetooth protokolünü ele geçirmeyi başaran saldırgan cihaz ile istediği yapılandırmayı kullanmakta özgürdür ve cihazı ele geçirmiştir.

BluePrinting (Mavi iz çıkarma)

Bu saldırı sayesinde Bluetooth teknolojisinin bize sağlamış olduğu verileri kullanarak cihazın markası, modeli gibi bilgileri ele geçirebilmekteyiz. Bluetooth MAC adresinin ilk üç hanesi cihazı ve üreticisi ile ilgili bilgi verir. Bunun haricinde cihazdan alabileceğimiz desteklenen uygulamalar, açık portlar vb. bilgiler ile cihazın markasını, modelini hatta Bluetooth yazılımının sürümüne erişim sağlanabilir. Bu sayede çalışan sistem ile ilgili daha detaylı bilgiye sahip olup saldırı vektörü daraltılabilir.

HelloMoto (Merhaba Moto)

Bu saldırı Motorola'nın bazı cihazlarındaki "güvenilebilir cihazların" yönetiminin hatalı bir şekilde işlenmesini kullanan zafiyeti sömürür. Saldırgan OBEX Push servisini kullanarak vCard (kişi bilgileri bulunan sanal yapı) göndermeye başlar. Saldırgan sonra gönderiyi yarıda keserek başarısız bir gönderme oluşturur. Bu başarısız gönderme saldırganı güvenilenler listesinden çıkarmaz. Bu sayede saldırgan kulaklık profiline kimlik doğrulama gerekmeden bağlanabilir. Bağlantı yapıldıktan sonra cihaz AT komutları sayesinde saldırganın eline geçmektedir.

BlueBump (Mavi Çarpma)

Bu saldırı biraz sosyal mühendislik gerektirmektedir. Asıl fikir kurban ile güvenli bir bağlantı sağlamaktır. Bu sanal bir iş kartı veya bir dosya aktarımı ile mümkündür. Bir aktarım sonrası kurban sizi güvenilir cihaz listesine eklemişse eğer saldırgan bu sefer bağlantıyı koparmadan kurbana bağlantı anahtarını silmesini talep eder. Bağlantı anahtarını silen ve saldırganın hâlâ bağlı olduğundan habersiz olan kurban olağan işlerine devam eder. Saldırgan ise halen devam eden bağlantısını kullanarak yeniden anahtar oluşturmayı talep eder. Bunun sonucunda saldırganın cihazı kurbanın güvenilenler listesine kimlik doğrulama olmaksızın tekrar girer ve kurban bu anahtarı devre dışı bırakana dek saldırgan, kurbanın telefonuna erişebilir.

BlueDump (Mavi Yığın)

Bu saldırıda saldırgan Bluetooth cihazının eşleşmiş olduğu adresleri (BDADDR) bilmek zorundadır. Saldırgan kendi adresini kurbanın bağlı olduğu bir cihazın adresiyle değiştirir ve kurbana bağlanır. Saldırganın bağlantı anahtarı olmadığından kurbanın cihazı bağlanmak istediğinde bağlantı anahtarı yok (HCI_Link_Key_Request_Negative_Reply) döndürecektir. Bazı durumlarda bu kurbanın cihazının bağlantı anahtarını silip tekrardan eşleşme moduna girmesini sağlayacaktır. Saldırgan, eşleşme moduna giren cihazın eşleşme olayını alabilir anahtar değişimini okuyabilir. Bu sayede hem güvenilen cihazı listeden çıkarmış olup hem de bağlantı yapabilme hakkına sahip olur aynı zamanda anahtar değişimine müdahil olup ortadaki adam saldırısı gerçekleştirebilmektedir.

BlueChop (Mavi kesme)

Bu saldırıda amaç Scatternet'e bağlı cihazlar için pictonet bağlantılarını koparmak, Pictonet ağını bozmaya çalışmaktır. Saldırı ana cihazın birden çok cihaza bağlanarak genişlemiş bir ağ (Scatternet) yaratabilme özelliğini kullanır. Saldırgan kendi adresini Pictonete bağlı bir cihazın adresiyle değiştirir ve ana cihaz ile bağlantı kurar. Bu sayede Pictonet bağlantısını bozar.

Kimlik Doğrulamayı Suistimal

Kimlik doğrulama Bluetooth cihazlarında bir servisi kullanacak bütün cihazlar için geçerlidir, yani bir cihaz kimlik doğrulama yapıp cihaza bağlanmadan o cihazda bulunan bir servisi kullanamaz. Servis sağlayıcı cihaza bir servis kullanmak için bağlanan cihazlar servis sağlayıcı üzerinde yetkisiz erişim sağlayan bütün servisleri kullanabilirler. Bu saldırıda saldırgan servis sağlayıcı üzerinde çalışan yetkisiz servislere bağlanmaya çalışır ve bu servisleri kendi amaçları için kullanır.

BlueSmack (Mavi Öpme)

BlueSmack bir DoS saldırısıdır ve Linux BlueZ Bluetooth katmanını kullanarak oluşturulabilir. L2CAP(uygulama/servis) seviyesinde bir başka Bluetooth cihazından yankı (Echo) isteği talep etmek mümkündür. ICMP ping mantığıyla benzer şekilde L2CAP pingin amacı bağlantıyı kontrol etmek ve gidiş geliş süresini ölçmektir. BlueZ ile gelen l2ping sayesinde saldırgan paketlerin boyutunu değiştirerek ping saldırısı yapabilir (-s parametresi ile 600 bayt boyutu idealdir).

BlueBorne (Mavi Bulaşma)

Bluetooth yığıtında bulunan zafiyetleri kullanan Blueborne, cihazların haberi olmadan onlara bağlanıp, cihazın içerisinde maksimum yetkiyle komut çalıştırabilmektedir. Bunun sonucunda çalışan komutlar sayesinde cihaz üzerinde bütün işlemler yapılabilmektedir. (Dinleme, veri değiştirme, okuma, takip.) Bu sorun Bluetooth çipinin ana çipe güvenlik kontro-

lüne maruz kalmadan bağlanabilmesi ve maksimum yetkiye sahip olmasından kaynaklanır.

Car Whisperer (Araçlara Fısıldayan)

Bu saldırıda saldırganlar arabalardaki Bluetooth radyolarında varsayılan olarak gelen PIN kodlarını kullanırlar. Cihazlar bir telefonu taklit ederek araçlara bağlanırlar. Bağlandıktan sonra araçlarda bulunan müzik sistemlerinden ses çalabilir, mikrofondan ses dinleyebilirler. Saldırı yönlü bir anten ile 500 metre öteden 120 ile giden bir araca karşı uygulanmış ve araç 15 saniye boyunca saldırıya maruz kalmıştır.

Bluestabbing (Mavi Bıçaklama)

Bu saldırı da Bluesmack saldırısı gibi bir DoS saldırı türüdür. Amacı Bluetooth cihazında bir hata oluşturmak veya onu çökertmektir. Bluetooth cihaz ismi UTF-8 ile encode edilmiştir, Bluetooth bağlantısı yapan bütün cihazlar UTF-8 desteklemez. Bu nedenle cihaz isminde UTF-8'e ait özel karakterler içeren Bluetooth cihazlarını listelemeye çalışırken desteklemeyen cihazlar çöker ve cihaz baştan başlatılır. Saldırgan cihazlarda hataya yol açabilir ve bu sayede cihazlar istenmeyen bir duruma düşebilir.

Bluespooofing (Mavi Kopyalama)

Saldırgan kurbanın güvenilir cihazlar listesinde bulunan bir cihazı kopyalar. Cihaz adresini, servis kayıtlarını ve benzeri verileri kopyalar. Protokolleri ve profilleri simüle eder ve kopyaladığı cihazı birebir taklit eder. Şifrelemeyi kapatır ve şifresiz bir şekilde tekrar bağlanmaya çalışır. Bu sayede şifresiz bağlantıyı kabul eden kurbana başka bir cihaz gibi bağlanmak mümkündür.

Bloover (Mavi Süpürge)

Bloover daha önce bahsedilen saldırı vektörlerinin denenebileceği bir Java/Bada uygulamasıdır. Bluebug, Hellomoto, Bluesnarf ve hatalı obje yaratımı saldırılarını destekler. Bluetooth protokolünü test etmek için kullanılır.

BlueStalker (Mavi Takipçi)

Ticari takip servisidir. Bluebug SMS mesajı sayesinde telefon numarasını bulur ve doğrulama mesajında araya girer. GSM yer takibi yapar.

Bloonix

Bluetooth cihazlarını test etmek için yapılan Linux dağıtımıdır. Canlı sürümdür, 2.6 kernel'ine sahiptir, en son BlueZ protokolüne sahiptir, rapor yaratır ve Bluetooth bağlantısını ve cihaz üzerindeki konfigürasyonunu test eden araçlara sahiptir. (Bir nevi Bluetooth saldırısı test kiti.)

BlueSniping ve BlueTooone (Mavi Nişanlama ve Mavi Ton)
Bluetooth verici ve alıcılarına yönlü antenler takma suretiyle Bluetooth cihazlarının iletişim mesafesini arttırmaya verilen isimdir. Bu yönlü antenler sayesinde 4 kilometreye kadar uzaktan bir Bluetooth bağlantısı yapılabilir, bir saldırı.

Diğer Yöntemler

Burada bahsedilmeyen ama internet üzerinden incelenebilecek birkaç yöntem daha bulunur. Bunlardan bazıları aşağıda listelenmiştir.

Bluehacking (mavi saldırma), Marphing, Bluejacking (Mavi Çalma), Bluesnafting [s ic], Bluetoothing...

Saldırıların Geleceği

Bluetooth teknolojisi çok geniş bir yapıya sahiptir. Günümüzde kullanılan çoğu standart gibi temelde IEEE OSI Referans modeline benzer bir yapıyla başlar. Temelde (fizikselde) Radyo ve temelbant ile başlayan protokol yığıtı en üstte uygulama katmanını kullanır. TCP/IP yapısına da benzetilebilecek protokol yığıtının TCP/IP den farkı benzer protokollerin uygulama katmanında kullandıkları TCP/IP yığıtı yerine, yüksek seviye uygulamalar için SIG'in tanımlamış olduğu geniş protokol ve uygulama yelpazesini kullanmasıdır. Kendi tanımladığı bu uygulama yelpazesinde detaylı bir şekilde incelenmemiş bir sürü protokol bulunmaktadır, Standartlara bağlı kalmaması nedeniyle denenmesi gereken bir sürü uygulama, bir sürü protokol ve incelenebilecek bir sürü iç/ara iletişim bulunmaktadır. Bu nedenle saldırılara açıktır. Protokollerin tanımlarının bulunduğu spesifikasyon 2822 sayfadan oluşmaktadır. Bu nedenle araştırmacılar başka yüksek seviyeli protokoller üzerine detaylıca araştırma yaparken, Bluetooth protokolü üzerinde aynı derecede detaylı araştırmalar gerçekleştirilmemiştir. Diğer protokollerin (Bluetooth'a göre) daha kolay anlaşılabilir olması ve Bluetooth un daha karmaşık yapısı onu bu araştırmalardan uzak tutmuştur. Bu nedenlerden dolayı Bluetooth üzerinde daha bir sürü açığa çıkmamış saldırı yöntemi bulmak mümkündür.

Saldırılardan Korunma

Daha önce bahsettiğim saldırılardan korunabilmek için gerekmedikçe Bluetooth bağlantısını açık bırakmayın ve güvenmediğiniz Bluetooth bağlantılarını kabul etmeyin. Bluetooth yazılımınızı güncel tutun ve kullanmadığınız Bluetooth cihazlarını güvenilir cihazlar listesinden çıkartın. Bu yöntemler sizi Bluetooth üzerinden gelecek olan çoğu saldırıdan koruyacaktır, yalnız şunu unutmamak gerek. Mükemmel güvenlik yoktur ve teknoloji geliştikçe saldırı vektörleri de gelişmeye devam edecektir.

Meryem Akdoğan - mrymakdogan@gmail.com

Mobil Uygulamalar, Tehditler ve Uygulama Güvenliğinde Gerekli Yaklaşımlar

Yeni nesil bir trend olarak karşımıza çıkan mobil cihazların gelişimi ve etkisi her geçen gün artarak devam etmektedir.

Herkesin evinde bir bilgisayar olmasa da muhakkak bir mobil cihaz olması bu durumu kanıtlar nitelikte. Hem taşınabilirliğinin kolay olması hem de bilgisayarlarda kullanabileceğiniz birçok uygulamayı size sunması bu cihazları daha da vazgeçilmez kılmıştır.

Mobil cihazlar için tasarlanmış yazılımlara mobil uygulama denilmektedir. Mobil uygulamalar, dünyada genellikle Android ve iOS işletim sistemlerinde kullanılmak üzere tasarlanmaktadır.

Uygulamaların çoğunluğu işlevi gereği sürekli internet erişiminde bulunabilmektedir. Buna bağlı olarak uygulamaların hızla artması önemli bir güvenlik riski yaratmaktadır. Bu nedenle hem bu platformda yazılım geliştirenlerin hem de kullanıcıların bu konuda daha dikkatli olmaları gerekmektedir.

Mobil uygulama aracılığı ile kullanıcılara ait kişisel bilgiler, telefon kayıtları, adres defterleri ve konumları gibi birçok bilgiye erişimin sağlanması yaygın olarak kullanılan veri toplama yöntemi haline gelmiştir. Fakat bu verilerin kötü niyetli üçüncü kişilerin hedefi haline gelmesi ile önemli bir güvenlik problemi ortaya çıkmaktadır. Örneğin; masum göründüğünü düşündüğünüz bir video düzenleme uygulaması sizin konum, adres defteri veya internet erişim yetkisi gibi bilgilerinize erişmek istiyor. Peki bu uygulamanın bu bilgileri amacı dışında kullanabileceğini hiç düşündünüz mü? Veya bir çalar saat uygulamasının dahili hafıza alanını okuma yetkisi istemesi ne gibi kötü sonuçlar doğurabilir? Uygulamaları kullanma isteği uygulamaların hassas verilere erişim için talep ettikleri yetki taleplerini göz ardı etmeye sebebiyet vermektedir.

Mobil uygulamalar aracılığı ile kullanıcılara ait kritik verilere erişilebiliyor olması saldırganların iştahını kabartmış, mobil cihazlara yönelik farklı yeteneklerde zararlı yazılımların geliştirilmesinde artışa sebep olmuştur. Saldırganlar geliştirmiş oldukları zararlı yazılımları, kullanıcıların mobil cihazlarına bulaştırabilmek için bilinen klasik sosyal mühendislik yöntemlerini kullanmışlardır.

Günümüzde Android cihazlar için market görevi gören Google Play'de uygulama sayısı, insanların ilgilerine ve zevklerine yönelik sürekli artış göstermektedir. Google Play içerisinde ücretli olarak sunulan uygulamaları, ücretsiz olarak kimi web sitelerinden indiren kullanıcılar, ilgili uygulamaların içerisine enjekte edilen zararlı yazılıma maruz kalmaktadır. Hatta bazı durumlarda popüler olan ancak bulunduğumuz ülkede hizmet vermeyen uygulamalar olmasından dolayı da kullanıcılar Google Play dışından uygulama yüklemeye mecbur bırakılmakta ve siber saldırılar ile karşı karşıya getirilmektedir. (Örneğin; PokemonGo)

Zararlı yazılımları hazırlayan saldırganların kurum veya devlet çalışanlarını hedef alması yanında kişisel hedefler doğrultusunda da bu yönteme başvurdukları görülmüştür. Zararlı yazılım enjekte edilmiş bir uygulama dosyasının mobil cihaz üzerinde çalıştırılması sonrasında söz konusu zararlı yazılım ilgili mobil cihaza bulaşmakta ve cihazı saldırgana hizmet vermeye hazır duruma getirmektedir.

Soru: Peki bir uygulamanın kötü niyetli olup olmadığını nasıl anlayabiliriz?

Cevap: "Uygulamanın davranışları analiz edilerek anlaşılabilmektedir."

Mobil uygulamanın zararlı yazılım olması dışında bir de uygulamada zafiyetlerin bulunması hususu var. Bu durumda aslında gizli bir tehdit söz konusu. Bu sebeple mobil uygulama güvenliği siber güvenlik alanında önemli bir yer tutmaktadır. Dolayısıyla bu alana eğilim de gün geçtikçe artmaktadır.

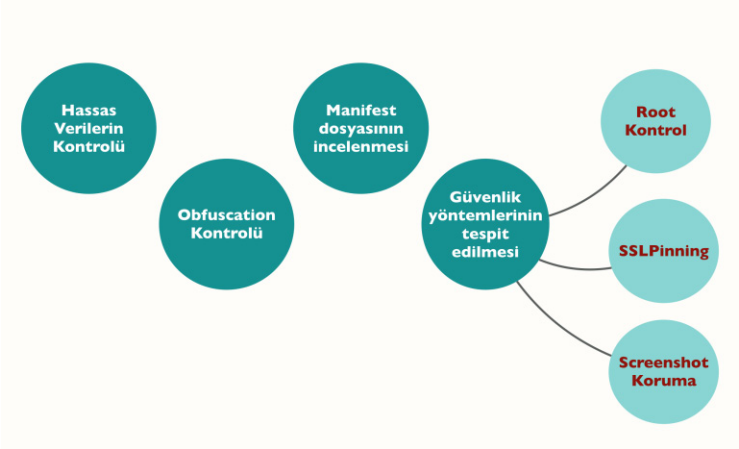
Ben de bu yazının geri kalanında bir mobil uygulamayı analiz etmek için izlenmesi gereken yaklaşımdan söz edeceğim.

Mobil Uygulama Analizinde Yaklaşımlar

Mobil uygulamaları test etmek için ilk olarak uygulama hakkında detaylı bilgi toplamamız son derecede önem taşımakta-

dır. Bu uygulama daha önce bahsedildiği üzere zararlı bir uygulama analizi olabileceği gibi, kullanıcıların faydası için geliştirilmiş bir mobil uygulama da olabilir. Bu nedenle uygulama, -kurulumdan önce ve sonra- olmak üzere, her iki durumda da analiz edilmelidir. Böylece uygulamanın her davranışı analiz edilebilir ve bir saldırgan gözüyle bakılarak saldırı senaryosu oluşturulabilir.

Uygulama Kurulmadan Önce



Öncelikle uygulamayı kurmadan önce uygulamanın paket dosyası üzerinde birtakım analizler gerçekleştirerek davranışlar hakkında bilgi sahibi olunabilir. Örneğin; Android uygulama paketi olan APK dosyası aslında bir sıkıştırılmış dosyadır. Bu dosya içerisindeki dosyaları çıkarırsanız geliştirici tarafından uygulamanın oluşturulması aşamasında kaynak kodları dahil olmak üzere tüm hazırlanan dosyalara sahip olabilirsiniz.

Bu adım sırasında izlenecek yollar:

- Hassas verilerin kontrolü
- Obfuscation (Şaşırtma kontrolü)
- AndroidManifest.xml dosyasının incelenmesi
- Güvenlik yöntemlerinin tespit edilmesi

Hassas Bilgilerin Kontrolü

Uygulamayı kurmadan önce kaynak kodda hassas verilerin olma ihtimali incelenmelidir. Böylece uygulama hakkında genel bilgi sahibi olunabilir ve bu bilgiler test sırasında kullanılabilir. Örneğin; kaynak kodlarda veritabanı dosyası bilgileri, domain/IP bilgileri, şifreleme vb. bilgiler elde edilebilmektedir. Bu analizin verimli gerçekleşebilmesi için eğer APK dosyası (Android uygulama dosyası) inceleniyor ise temel Java programlama ve Android platformları için uygulama geliştirmenin bilinmesi ya da IPA dosyası (iOS uygulama dosyası) incelemek isteniyor ise temel Swift dili bilinmesi gerekmektedir. Bu sayede resmi daha iyi görebilirsiniz.

Obfuscation (Şaşırtma) Yöntemi Kontrolü

Bu yöntem iyi niyetli uygulama geliştiricileri tarafından olduğu kadar kötü niyetli insanlar tarafından da kullanılabilmektedir. Obfuscation, uygulamanın kaynak kodunda hassas bilgilere erişmek istediğimizde geliştiricinin bu bilgileri bizi şaşırtmak amacıyla daha karmaşık halde kullanmasıdır. Geliştirici dosya veya parametre isimlerine kolay ulaşmamızı istemiyor olabilir. Örneğin; veritabanı (database) erişim dosyası ve bu bilgilerin olduğu class ismini, değişken ismini db yerine anlamsız kelimeler ile isimlendirmesi gibi. Dolayısıyla detaylı inceleme yapılması önemlidir.

Manifest Dosyasının İncelenmesi

Geliştirici tarafından hazırlanan AndroidManifest.xml dosyası uygulamanın cihazdan erişmek üzere talep ettiği yetkileri belirten dosyadır. Uygulamanın tüm temel bilgileri bu dosya içerisinde belirtilir. Dolayısıyla bu dosya uygulamanın davranışları hakkında genel bir çerçeve çizmektedir. Böylece uygulamanın erişmek istediği yerler veri olarak test sırasında değerlendirilmektedir.

Güvenlik Yöntemlerinin Tespit Edilmesi

Bazı uygulamalar kurulurken veya çalıştırılırken güvenlik önlemi almak amacıyla cihaz üzerinde birtakım kontroller gerçekleştirirler. Mobil uygulama analizi esnasında uygulamanın hangi kontrolleri gerçekleştirmek istediği tespit edilebilmektedir. Bu kontroller uygulamanın çalışma akışının devam etmesine engel olduğu için bypass etme yöntemleri de tespit edilmiştir. Bunun için örnek olarak Xposed Framework gibi bir mobil uygulama kullanılarak ve içerisindeki modülleri seçerek cihazı özelleştirmek veya bazı güvenlik önlemlerini atlatmak mümkündür.

Root Cihaz Kontrolü

Uygulama kurulurken cihazın root veya JailBreak olup olmadığını kontrol ediyor olabilir. Bu gibi güvenlik önlemlerinin kontrolünün önceden gerçekleştirilip ona uygun ortam ayarlanmalıdır.

SSLPinning

Uygulamanın SSLPinning güvenlik yöntemini kullanıp kullanmadığı test edilmelidir.

Screenshot Koruması

Uygulamanın ekran görüntüsü almanızı engelliyor olması da bir güvenlik önlemidir. Bu nedenle bu durumun da önceden bilinmesi ve atlatılmaya çalışılmasında fayda vardır.

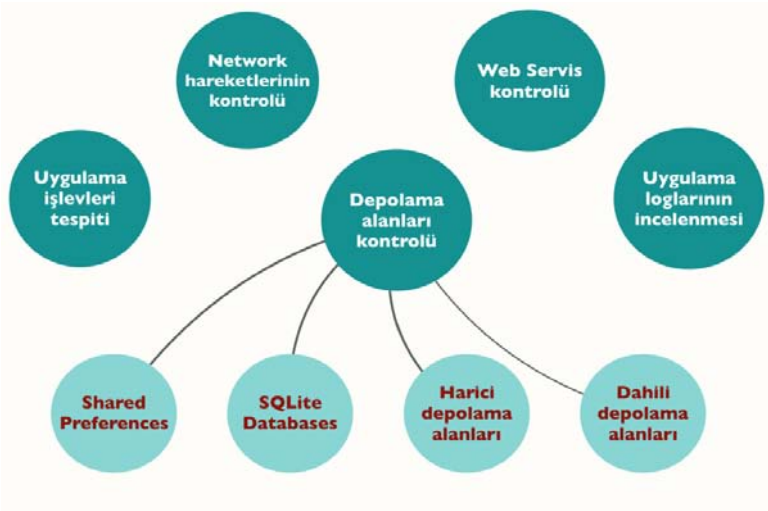
Uygulama Kurulduktan Sonra

Uygulamayı kurmadan önceki analizleri gerçekleştirdikten sonra bir de kurulum esnasında ve sonrasında yapılacak kontroller vardır. Burada tamamen sanal ortamlar ve sahte hesaplar üzerinde testlerin yapılması önemlidir. Aslında bu kı-

sım mobil uygulamaların güvenlik açısından denetlenmesinde geri kalan resmin en büyük kısmıdır. Bu nedenle aşağıdaki adımlar analiz yapan kişi tarafından titizlikle incelenmelidir.

Bu adımda izlenecek yollar;

- Uygulama işlevlerinin tespiti
- Network (ağ) hareketlerinin kontrolü
- Depolama alanları kontrolü
- Web servis kontrolü
- Uygulama loglarının incelenmesi



Uygulama İşlevlerinin Tespiti

Uygulamalar amacı doğrultusunda veya dışında birtakım işlemler gerçekleştirmenize sebep olabilmektedir.

Örneğin uygulama,

- Register (Kayıt olma)
- Login (Giriş yapma)
- Sıra numarası alma (Eğer bir banka uygulaması ise)
- Alışveriş yapma
- Mesaj gönderme vb.

Uygulamanın işlevlerinin tespit edilmesi sırasında bir proxy aracı kullanarak gezinti boyunca elde edilen verileri analiz için kaydetmek önemlidir. Bu yöntem ile uygulamadaki davranış anomalileri belirlenebileceği gibi bulunuyorsa zaafları da ortaya çıkarılabilmektedir.

Network Hareketlerinin Kontrolü

Wireshark gibi bir uygulama ile mobil uygulamanın ağ trafiğini izleyip analiz etmek gerekir. Eğer zararlı bir yazılım ise cihazdaki hassas bilgileri okuyarak veya uygulama içerisindeki işlemlerinizi düzenli olarak bir sunucuya gönderiyor olabilir. Bunların tespiti ağ hareketleri izlenerek gerçekleştirilebilmektedir.

Depolama Alanları Kontrolü

Mobil uygulama geliştiriciler, uygulama verilerini saklamak için bazı depolama yöntemleri kullanırlar. Bunlar;

- Shared Preferences
- SQLite Databases
- Harici depolama alanları
- Dahili depolama alanları

Shared Preferences

Geliştiriciler Shared Preferences klasörü altında uygulamanın ayarlarını veya verileri tutabilmektedirler. Veriler genellikle XML formatında dosya içerisinde tutulmaktadır. Bu güvensiz bir veri depolama yöntemi olduğu için saldırganların ilk bakacağı yerlerden birisidir.

SQLite Database

SQLite kullanımı ve kurulumu oldukça basit olan bir veritabanı yönetim sistemidir. Her veritabanı için sadece bir dosya vardır. Böylece veritabanı kolay yedeklenebilir ve kopyalanabilir. Dosyalar genellikle .db veya .sqlite uzantılıdır. Güvenli herhangi bir şifreleme uygulanmadığı taktirde saldırganlar tarafından da erişimi kolay olduğu için güvenli bir veri depolama yöntemi değildir.

Dahili Depolama

Dahili depolama, dosyaları doğrudan cihaza kaydedebileceğimiz başka bir yöntemdir. Kaydedilen dosyalar uygulama için özeldir ve diğer uygulamalar bunlara erişemez. Kullanıcı uygulamayı kaldırdığında ise bu dosyalar kaldırılır.

Harici Depolama

Dosyaların belirli bir konuma kaydedildiği depolama yöntemidir. Bu taşınabilir bir depolama ortamı olan SD kart alanı veya taşınabilir olmayan bir depolama alanı olabilir. Özellikle zararlı yazılım analizlerinde önem arz eden noktalardandır.

Web Servis Kontrolü

Uygulamanın herhangi bir web servis ile bağlantıya geçip geçmediği yine bir proxy aracı yardımıyla öğrenilebilmektedir. Web servislerin kullandığı metotlar tespit edildiğinde ilgili parametreler çeşitli yollarla manipüle edilmeye çalışılacaktır. Ayrıca web servis testleri yaparken meydana gelebilecek tüm web uygulama zafiyetlerinin testi yapılmalıdır. Örneğin; SQL Injection, XML Injection, oturum çalma, kaba kuvvet saldırıları gibi.

Uygulama Loglarının İncelenmesi

Uygulamada kritik bilgilerin loglara kaydedilmesi ihtimali düşünülerek loglar incelenmelidir. Böylece ayrıntılı bir analiz gerçekleştirilmiş olmaktadır.

Besim Altınok - besimaltnok@gmail.com

WiPi Hunter
Zararlı Kablosuz Ağ Aktivitelerinin Tespit Edilmesi

WiPi Hunter ilk olarak kablosuz ağ saldırı ve testleri için özelleştirilmiş bir araç olan WiFi Pineapple aktivitelerini tespit etmek için tasarlanmıştı. Ancak daha sonra proje genel anlamda "**Zararlı kablosuz ağ aktivitelerini tespit emek**" için tekrar düzenlendi.

Bu proje ile ilgili söyleyebileceğim en önemli şey WiPi Hunter projesinin sadece bir kod parçası olmadığıdır. Bu projede illegal kablosuz ağ aktiviteleri ile mücadelede kullanılabilecek bir fikir, yeni bir yöntem ve farklı bakış açıları bulabilirsiniz.

Proje tek bir script içine hapsedilmeden modül modül yazılmıştır ve süreç bu şekilde devam ettirilmektedir. Bu sayede siz de istediğiniz herhangi bir modülü veya modül içindeki fonksiyonu alıp farklı projeler yaratabilirsiniz.

Projedeki modülleri geliştirilirken izlenen yol ise,

- Saldırıyı yap, saldırı trafiğini kaydet, Wireshark ile incele, anormal paketleri ayrı olarak kaydet ve Scapy ile incele

şeklinde uygulanmıştır.

Bu sayede detaylar daha rahat görülebilmektedir.

WiPi Hunter projesi içerisinde şu an için 5 farklı modül bulunmaktadır. Projede yer alan modüller ve kısa açıklamaları aşağıdaki gibidir:

- **PiSavar:** WiFi Pineapple içinde varsayılan olarak gelen ve sahte erişim noktaları oluşturmak için kullanılan PineAP modül aktivitelerini tespit etmek ve WiFi Pineapple cihazına karşı saldırı düzenlemek amacı ile geliştirilmiştir.
- **PiFinger:** Bağlı bulunduğumuz ağlar hakkında bazı analizler yaparak, bunun sahte bir erişim noktası olup olmadığını anlamaya çalışır ve daha öce bağlandığımız kablosuz ağlar üzerinde bazı kontroller yaparak bir kablosuz ağ güvenlik skoru üretir.
- **PiDense:** Hackerların sahte erişim noktası açma stratejilerini göz önünde bulundurarak monitoring işlemleri gerçekleştirir.
- **PiKarma:** WiFi Pineapple, FruityWifi ve MANA Toolkit gibi birçok önemli ve değerli araçların saldırı amacı ile kullandığı bir modül olan KARMA modülünün aktivitelerini tespit etmek ve buna karşı bir saldırı düzenlemek amacı ile geliştirilmiştir.
- **PiNokyo**: WiFi Pineapple cihazı veya KARMA saldırısı eğer bir ortamda aktif ise, kablosuz ağ kullanıcıları bu konuda bilgilendirilir. Modül geliştirilme aşamasındadır. Gelişmeyi projenin Github hesabından takip edebilirsiniz.

PiSavar

Bu projede amacım WiFi Pineapple cihazının aktivitelerini tespit etmek ve bundan etkilenen kullanıcılara bir çözüm sunmaktı. **Pi Savar** isminde iki anlam var. **Pi**, WiFi Pineapple temsilen kullandığım bir kısaltma, Savar ise Türkçe bir kelime. Tehlikeyi savurmak anlamında kullanmak istedim. Bu nedenle adına PiSavar dedim. Bundan sonraki bütün çalışmalarda da bu yapıyı kullandım.

Uzun zamandır WiFi Pineapple cihazı ile ilgileniyordum. Ama bu ilgim saldırma odaklı değildi, sadece ne olduğunu nasıl çalıştığını ve ne tarz senaryolar ile saldırganların bunu kullanabileceğini öğrenmek ve buna çözüm sunmak istiyordum.

Yaptığım incelemelerde, sahip olduğu kullanıcı arayüzü sayesinde çokça tercih edildiğini gördüm. Sahte erişim noktaları açmak için de varsayılan olarak kurulu gelen ve ona asıl gücünü veren PineAP isimli bir modüle sahipti.

Bu modülün çalışma prensibi tam olarak şu şekilde:

- Cihazlarınızdan yayılan istekleri analiz edip parse ederek, SSID bilgilerini topluyor ve bu SSID bilgileri için bir SSID Pool oluşturuyor.
- Ve istemeniz halinde bu SSID bilgilerini kullanarak sahte erişim noktaları oluşturup, kullanıcıları tuzağa düşürüyor.

Bu oldukça kullanışlı ve kolay uygulanabilir bir özellik. Ben de bu aktiviteyi tespit etmek için neler yapabilirim, diye bir kontrol ettiğimde, bu işlevi yaparken tek bir MAC adresi üzerinden birden fazla SSID yaydığını gözlemledim.

Burada bir problem vardı. Ben de bu problemi en basit şekilde çözerek kullanılabilir ve taşınabilir bir yöntem geliştirmek istedim.

Bunun için Python kullandım. Aynı zamanda real time paketleri yakalamak ve ayrıştırmak için Scapy modülünü ekledim.

Bu kapsamda bir algoritma yazdım ve bu aktiviteyi tespit etmeye başladı.

Ek olarak PiSavar aracı iki farklı metot ile çalıştırılabiliyor. Bunlardan birini sadece aktiviteyi tespit etmek ve kayıt etmek için; diğerini de hem aktiviteyi tespit etmek, kayıt etmek hem de cihaza bir saldırı başlatarak etkilenen kullanıcıları kurtarmak için tasarladım.

En başta söylediğim gibi, taşınabilir bir fikir olması çok önemli. PiSavar aracı da tam olarak taşınabilir cihazlara uygulanabilmekte. Eğer isterseniz bir tane Raspberry Pi Zero W temin edip, yazılımın sürekli istediğiniz bir yerde sizin için çalışmasını sağlayabilirsiniz.

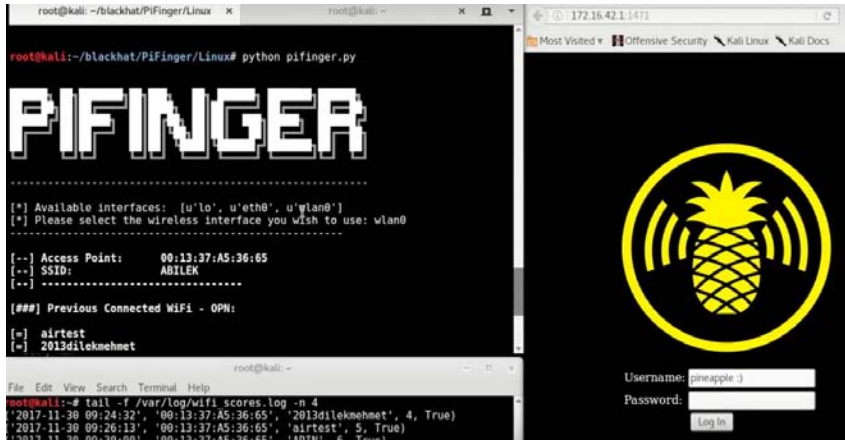
NOT: Bu yazılımı kullandığınız zamanlarda sadece kendinizi korumak ile kalmayıp, aynı zamanda çevrenizi de güvende tutabileceksiniz. (**PiSavar - Kullanışlı, Taşınabilir, Herkes için güvenlik)**

- **KAYNAK KOD:** https://github.com/WiPi-Hunter/PiSavar
- **Kullandığım modüller:** argparse, time, scapy, termcolor, logging, commands, netifaces
- **Kullandığım dil:** Python

Yakın zamanda kazandırılacak özellikler:

- PineAP modülü tarafından yayılan SSID bilgilerini kayıt altına almak
- WiFi Pineapple cihazına yakalanan istemcilerin MAC adres bilgilerini kayıt altına almak

PiFinger



PiFinger aracı da PiSavar aracı ile aynı amaç için tasarlanmış bir yazılımdır. Bu aracın ortaya çıkış hikayesi de PiSavar aracından sonra oldu.

İlk durumda PineAP modülünün aktivitelerini tespit edebiliyordum, ama eğer saldırgan sadece bir özel SSID ile yayın yapıyorsa, hatta bu OPN (Open'ın kısaltması. Parola korumalı olmayan ağlar için kullanılan bir kısaltma.) değil parola korumalı bir kablosuz ağ ise, bu durumda bir önceki modül ile bunu tespit edemeyecektim. Bu nedenle kullanıcıların bağlandığı ağı inceleyerek (bilgi toplayarak) bazı izler yakalayabileceğimi düşündüm.

Bu kapsamda WiFi Pineapple cihazını inceledim ve bazı bulgular keşfettim. İncelemeler sonucunda bu cihazın varsayılan olarak kullandığı bazı değerlere ve bu değerlerin sıkça değiştirilmediğine şahit oldum.

Bu değerler:

- MAC adresi
- Hostname bilgisi
- DHCP IP aralığı
- Default Port numarası gibi değerlerdi.

Bunları kullanarak bir test gerçekleştirdiğimde WiFi Pineapple cihazını fingerprint yöntemi ile tespit edebildiğimi gördüm ve bu modülü geliştirdim.

Ancak ortada bir problem vardı, eğer saldırgan bu varsayılan ayarları değiştirirse?

İşte tam bu noktada **HTTP Port Fingerprint** özelliği kullanılabilir. Bu biraz uzun süren bir yöntem ancak gerçekten etkili bir yöntem ve fingerprint için kullanılabilir. (Bu özelliği yakında ekleyeceğim)

Tüm bu özellikleri harmanlayıp, ek olarak kullanıcılara her analiz sonucunda bir Kablosuz Ağ Güvenlik Skoru üreticisi

geliştirdim. Bu kapsamda bazı unsurları göz önünde tutuyordum:

- İlk olarak bağlı bulunduğumuz ağ eğer bir WiFi Pineapple tarafından açıldı ise, aşağıdaki tabloda görüldüğü üzere kablosuz ağ güvenlik skorunuz **kritik** niteliği kazanıyor.
- İkinci olarak daha önce bağlandığınız kablosuz ağları analiz ediyor ve bağlandığınız her parola koruması olmayan ağ için 1 puan Kablosuz Ağ Güvenlik Skoru'nuza ekleniyor.

Puan	Kritiklik Değeri
1-3	Low (Düşük)
4-6	Medium (Orta)
7-10	High (Yüksek)
Sahte Erişim Noktası	Critical (Kritik)

Bu durumda tabloda görüldüğü üzere aldığınız puan değerinin artması ile beraber Kablosuz Ağ Güvenlik Skoru'nuz etkileniyor.

- **KAYNAK KOD:** https://github.com/WiPi-Hunter/PiFinger
- **Kullandığım modüller:** time, termcolor, sys, commands, interfaces, os
- **Kullandığım dil:** Python

Yakın zamanda kazandırılacak özellikler:

- HTTP Port fingerprint
- WiFi Pineapple dışında diğer bütün sahte erişim noktalarını da analiz edebilecek yöntemler kısa zaman içerisinde eklenecektir. Bu nedenle projenin Github hesabına da göz atmanızda fayda var.

PiDense

Bu çalışma da WiPi Hunter çalışmasının üçüncü parçasıydı. Ancak bu çalışmayı gerçekleştirirken sadece WiFi Pineapple cihazını göz önünde tutmadım. Bunu tamamen sahte erişim noktaları açma stratejilerini izlemeye ve aksiyon almaya yarayan bir araç olması için geliştirmek istedim. Çünkü saldırganlar genellikle sahte kablosuz ağ açarken:

- Bütün özellikleri aynı
- Aynı SSID, parola korumasız
- Aynı SSID, parola korumalı
- Benzer SSID, parola korumasız
- İlgi çekici SSID isimleri, parola korumasız. (FreeNet, ForGuess, Internet, OPEN) gibi durumları göz önünde tutarak aktivitelerini geliştirirler.

Bundan dolayı ilk olarak OPEN Wireless Network yoğunluklarını ölçüp benzer SSID bilgilerinin aktivitelerini bulan bir araç olarak ortaya çıkardım.

Bu aracın şu an için iki özelliği var:

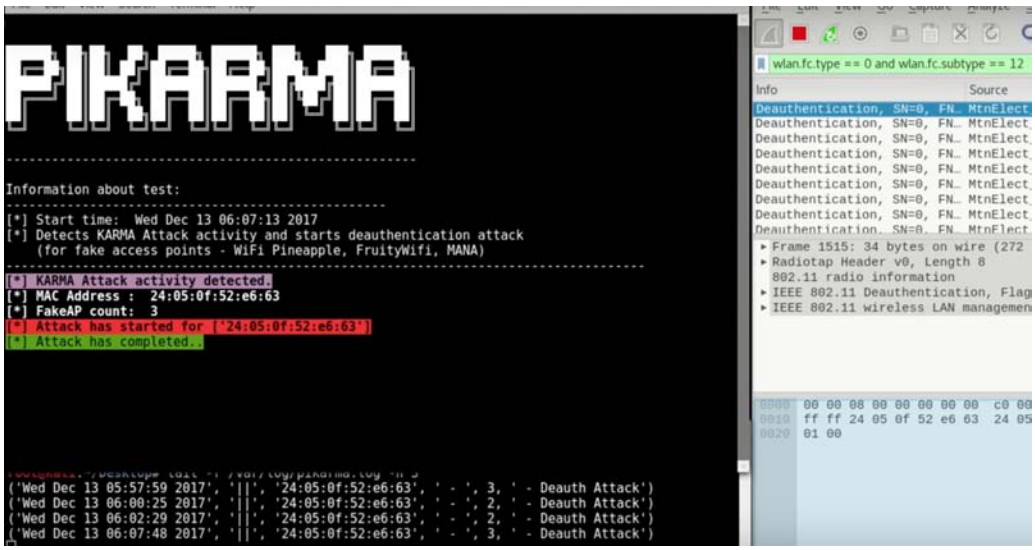
1. Sürekli etraftaki şifresiz yayın yapan kablosuz ağ yoğunluklarını ölçmek. Yani siz şirketiniz, eviniz veya herhangi bir lokasyon için OPN eşik değeri (sınır değeri) değiştirebiliyorsunuz. Bu tanımlamadan sonra eğer belirlediğiniz değer üzerinde parolasız yayın yapan kablosuz ağ sayısı artarsa sizi bilgilendiriyor.
2. İkinci olarak aynı SSID bilgileri ama farklı şifreleme tipinde yayınları yakalıyor.

- MAC Address = **MAC1** ; SSID = **Barikat** ; Enc = **Y**
- MAC Address = **MAC1** ; SSID = **Barikat** ; Enc = **N**
- **KAYNAK KOD:** https://github.com/WiPi-Hunter/PiDense
- **Kullandığım modüller:** time, termcolor, scapy, argparse
- **Kullandığım dil:** Python

Yakın zamanda kazandırılacak özellikler:

- Tanımlanan Blacklist SSID listesinin hareketlerinin izlenmesi.
- Benzer SSID bilgisine sahip yayınların izlenmesi.
- Kurum ismine göre tehditlerin izlenmesi.

PiKarma

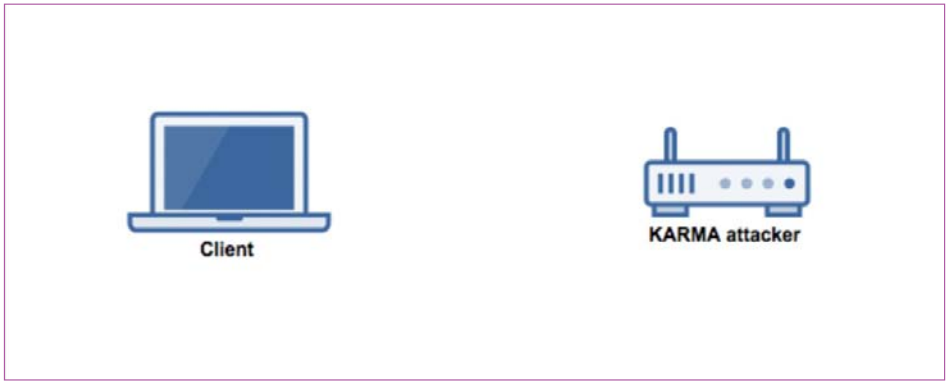


WiPi Hunter projesine ait bir diğer çalışma, PiKarma çalışmasıdır. Bu modülden bahsetmeden önce sizlere KARMA modülünün insanları nasıl tuzağa düşürdüğünden bahsetmek istiyorum. KARMA modülü, WiFi Pineapple dışında FruityWifi gibi çok değerli bir proje tarafından da kullanılmaktadır. Bunun yanında @**SensePost** tarafından bu modülün kullandığı saldırı biçimi daha da geliştirilerek MANA toolkit isimli yeni bir proje oluşturuldu ve **DEF CON**'da sunuldu.

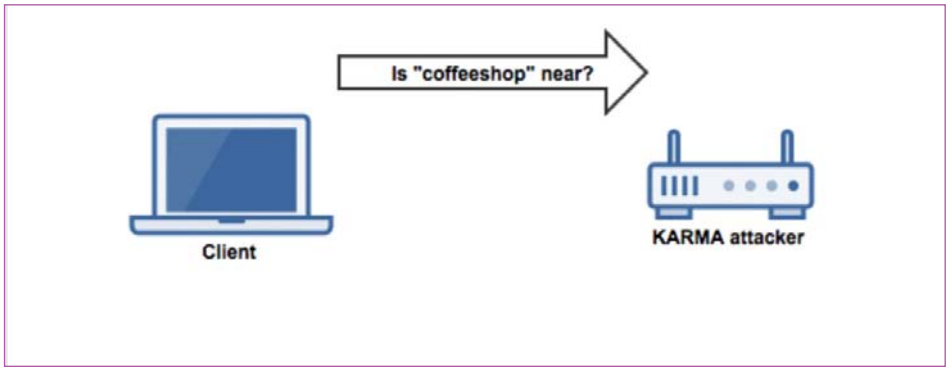
Şimdi gelelim saldırının detaylarına:

Biliyoruz ki, cihazlarımız lokasyon bazlı düşünemez ve daha önce bağlandıkları ağları bizim talebimiz ile anımsamaya çalışırlar. İşte tam bu noktada, KARMA modülü devreye giriyor.

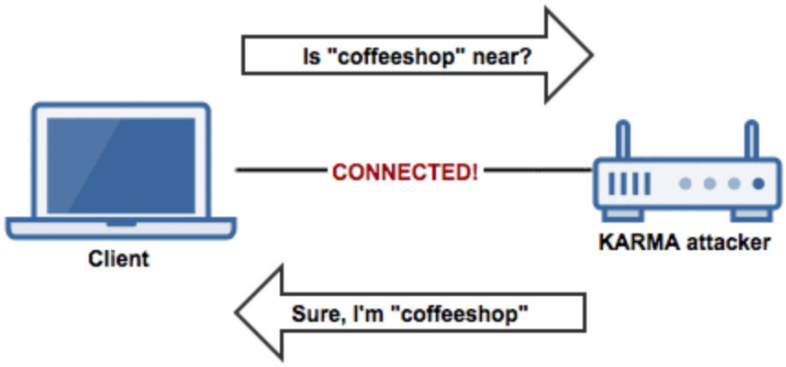
İlk durum



İlk talep



Son işlem



Bu modülün çalışma prensibi tam olarak şu şekilde:

- Cihazlarınızdan yayılan kablosuz ağa bağlanma taleplerini (Probe Request) dinliyor.
- Gelen bu bağlanma taleplerine karşı cevap üreterek (Probe Response) cihazların tuzağa düşmesini sağlamaktadır.

Bu oldukça kullanışlı ve kolay uygulanabilir bir özellik. Ben de bu aktiviteyi tespit etmek için neler yapabilirim, diye bir kontrol ettiğimde, bu işlevi yaparken tek bir MAC adresi üzerinden birden fazla **Probe Response** paketi yaydığını gözlemledim.

Burada bir problem vardı. Ben de bu problemi en basit şekilde çözerek kullanılabilir ve taşınabilir bir yöntem geliştirmek istedim.

Bunun için yine Python dilini kullandım. Aynı zamanda real time (gerçek zamanlı) paketleri yakalamak ve ayrıştırmak içinde Scapy modülünü ekledim.

Bu kapsamda bir algoritma yazdım ve bu aktiviteyi tespit etmeye başladı.

Ek olarak **PiKarma** aracı da **PiSavar** aracı gibi iki farklı metot ile çalıştırılabiliyor. Bunlardan ilkini sadece aktiviteyi tespit etmek ve kayıt etmek için, diğerini de hem aktiviteyi tespit etmek, kayıt etmek hem de cihaza bir saldırı başlatarak etkilenen kullanıcıları kurtarmak için tasarladım.

En başta söylediğim gibi, taşınabilir bir fikir olması çok önemli. PiKarma aracı da PiSavar aracı gibi taşınabilir cihazlara uygulanabilmekte. Eğer isterseniz bir tane Raspberry Pi Zero W temin edip, yazılımın sürekli istediğiniz bir yerde sizin için çalışmasını sağlayabilirsiniz.

NOT: Bu yazılımı kullandığınız zamanlarda sadece kendinizi korumak ile kalmayıp, aynı zaman da çevrenizi de güvende tutabileceksiniz. (**PiKarma - Kullanışlı, Taşınabilir, Herkes için güvenlik**)

Yetenekleri:

- KARMA saldırısını tespit etmek (MANA toolkit).
- Karşı saldırı başlatarak istemcileri kurtarmak.

Yakın zamanda kazandırılacak özellikler:

- KARMA saldırısının doğrulanması için gerekli algoritma.
- KARMA saldırısından etkilenen istemcilerin kayıt altına alınması.
- KARMA saldırısında kullanılan SSID bilgilerinin kayıt altına alınması.

WiPi Hunter:

- **Badge:** Blackhat Europe 2017
- **Youtube Oynatma Listesi:** WiPi Hunter
- **Github:** https://github.com/WiPi-Hunter
- **Twitter:** https://twitter.com/wipihunter

Ulaş Fırat ÖZDEMİR - htcnian@gmail.com

Web Application Firewall Atlatma Yöntemleri

Web servislerinde sızma testi gerçekleştirirken bazen Cloudflare, Sucuri gibi engellere takılmış olabilirsiniz. Bu yazımızda güvenlik duvarlarını atlatmak amacıyla kullanılabilecek yöntemlerden bahsedeceğim.

WAF Nedir?

WAF son kullanıcı ile istek yapılan web sunucusu arasında bulunan bir araçtır. WAF OSI'nin 7. katmanı olan uygulama katmanında görev alır ve adından da anlaşılabileceği gibi web uygulamalarını olası saldırılara karşı korumayı amaçlar. Son kullanıcı ile sunucu arasında oluşan iletişimi dinleyerek tanımlanan kurallara göre filtreleme, düzeltme veya engelleme işlemleri yapar. WAF'lar web servisi katmanında[1] giden istekleri ve gelen yanıtları incelemeleri nedeniyle çoğu zaman "Deep Packet Inspection Firewall" olarak adlandırılırlar.

Bazı WAF'lar belli saldırı imzalarını filtrelemeye çalışırken bazıları ise web servisinin normal trafiğine aykırı oluşan anormal durumları tespit etmeye çalışırlar. WAF'lar donanım veya yazılım tabanlı olabilirler ve dışarıdan gelebilecek saldırı ile beraber iç ağdan oluşabilecek saldırıları da filtrelerler. WAF'lar yaptıkları filtrelemenin yanında aynı zamanda tanımlanan kurallara göre kayıt tutarlar. Aktif modda bulunan WAF'lar hem bloklama hem de kayıt işlemi yaparken pasif moddaki WAF'lar sadece kayıt tutma işlevini gerçekleştirir.

WAF Türleri

WAF'lar çalışma şekillerine göre temelde üç kategoriye ayrılabilirler. Beyaz liste (Whitelist) ile çalışan WAF'lar sadece beyaz listede tanımlanmış durumların oluşmasına izin verirler. Bunun haricinde oluşan durumları filtreler ya da engellerler. Kara liste (Blacklist) ile çalışan WAF'lar ise kara liste içinde tanımlanan durumları tespit edip engellerler. Karma modu kullanan güvenlik duvarları ise iki filtreleme yönteminden de yararlanırlar.

WAF'lar daha önce de bahsedildiği gibi son kullanıcı ile web sunucusu arasındaki istekleri incelerler ama WAF'lar her zaman fiziksel olarak son kullanıcı ile web suncusu arasında bulunmak zorunda değildir. WAF'lar bulundukları topolojiye göre üçe ayrılırlar:

- Web sunucusu üzerinde (On premise, inline)
- Web sunucusunun bulunduğu ağda (Switch ile port mirroring[2])
- Web sunucusu ile istemci arasında (Bulut, reverse proxy)

WAF Topolojileri

WAF'ların topolojilerine uygun bilinmesi gereken birkaç temel nokta bulunmaktadır. Bu bilgiler yazımın geri kalanındaki yöntemleri ve WAF'ların yapısının anlaşılmasını kolaylaştıracaktır.

Bulut WAF: En genel kullanılan WAF türüdür. Genelde web uygulamasına kendileri ulaşırlar yani son kullanıcı ile web uygulaması arasında doğrudan bir bağlantı oluşmaz. Cloudflare örneğinden bahsetmek gerekirse bu servis alan adınızın DNS kayıtların Cloudflare DNS kayıtlarıyla değiştirmenizi ister. Bu sayede sizin sitenizi ziyaret eden bir kişi öncelikle Cloudflare servisine uğrayacaktır. Cloudflare ise sizin sitenize yapılan istekleri filtreler ve kontrollü bir şekilde yönlendirir.

Port mirroring kullanan WAF'lar iç ağda aynı switch'e bağlı bulunurlar. Tam olarak kullanıcı ile sunucu arasında bulunmadıklarından isteği direkt engelleyememektedirler. Bu nedenle istek web sunucusuna ulaşabilmektedir. Bu durumda WAF sadece kayıt tutma işlevini görebilmekte, geriye cevap dönmesi için sunucu tarafında ekstra konfigürasyonların yapılmasına ihtiyaç duyulmaktadır.

1 Web servisleri HTTP, HTTPS, REST, SOAP, XML-RPC vb. erişim yöntemlerini kullanırlar

2 Farklı markalarda Switched Port Analyzer (SPAN) veya Roving Analysis Port (RAP) şeklinde adlandırılırlar

Sunucu üzerinde bulunan WAF'lar ise uygulama ile birlikte barındığından dağıtık olamamakta, bu nedenle WAF üzerinde olası bir saldırıda DoS/DDoS ile web uygulaması devre dışı kalabilmektedir. Bu nedenle dağıtık çözümler tercih edilmektedir. Sunucu ile kullanıcı arasına kurulacak CDN veya dağıtılmış sunucular için her sunucuya özel WAF konumlandırmak gerekeceğinden bu çözümü genelde tercih etmek istemezler. Bu nedenle genellikle bulut tabanlı WAF'lar tercih edilmektedir.

WAF Algılama

Bir web uygulamasının WAF'ın arkasında olduğunu algılamanın birden çok yolu vardır. Ben bu yollardan bazılarını sizinle paylaşacağım. Bunlar;

- WAF'lar filtrelere takılmayan tarayıcılara bir cookie bırakabilmektedir,
- WAF'lar HTTP başlıklarını değiştirebilmektedir[3],
- Bazı WAF'lar engel cevaplarına farklı HTTP kodları koyabilmektedir,
- Bazı WAF'lar istenmeyen bir durum karşısında bağlantıyı koparabilmektedir,
- Bazı WAF'lar cevabın gövdesine kendi cevaplarını ekleyebilmektedir ve
- Yan kanal (Side-channel) saldırıları (cevap zamanı, güvenlik kuralları vb.)

WAF'ları algılamak için bu kuralları tek tek deneyebilirsiniz ama tahmin edeceğiniz gibi bunu otomatize yapan araçlar da mevcuttur[4].

WAF Atlatma

WAF atlatma tekniklerini temelde ben üç parçaya ayırmaktayım. Tabii yetkili bir hesaba giriş yapıp sistemde yetki elde etmek bir yöntemdir. Ama burada asıl amaç yetkisiz bir kullanıcının WAF'ı atlatmasıdır.

1. Doğrudan erişim (Web uygulamasına WAF'a uğramadan erişme)
2. Dolaylı erişim (Encoding vb. sayesinde kuralları atlatma)
3. Engel kaldırma (Robot yazılımlar ve yük altındaki durumlar için koyulan engelleri aşma)

Doğrudan erişim yöntemleri

Daha önce bulut tabanlı WAF'ların DNS üzerinden erişim sağladığını belitmiştim. Alan adının DNS kaydını WAF'ın belirttiği adres ile değiştirmek her durumda yeterli olmayabilir; çünkü web servisinin IP adresini bilirsek servise IP üzerinden erişim sağlayabilir, WAF'ı ve korumalarını devre dışı bırakabiliriz. Bu yöntemler web uygulamasını IP adresini tespit etmeye yöneliktir.

Doğrudan erişim yöntemlerini temelde 3 farklı noktada incelemek mümkündür. Bunlar;

- Tersine Atlatma (Uygulamanın saldırgana IP adresini yollaması)
- Bağlı Atlatma (Saldırganın uygulamaya erişip IP adresini temin etmesi) ve
- Zafiyetli Servislerdir (Uygulamalarda bulunan bir kod, eklenti veya temanın saldırgana IP adresi göstermesi)[6]

Not: Tersine atlatma, Bağlı atlatma ve Zafiyetli servisler kavramları bu konuda yeterince detaylı bir yazı bulamamam sonucu yazıma eklediğim terimlerdir. Proxy ve shell almada kullanılan reverse/bind analojisini kullanmaktayım. Umarım bu terimler konuya uygundur ve bu sayede siber güvenliğe bir katkı sunabilirim.

Tersine Atlatma

Tersine atlatma sırasında web sitesinde var olan bir uygulama, eklenti, betik veya dışarıya herhangi bir çıktı yaratan modül teste tabi tutulur. Bu modüllerden bazıları dışarıya sadece istenilen çıktıyı üretmez. Mesela alan adınıza kayıtlı bir mail sunucusu bu durumlardan biridir. Bir forum sitesine sahip olduğunuzu düşünün. Kayıt olan kullanıcılara aktivasyon linki, parola sıfırlama linki vb. nedenler ile sunucunuzdan e-posta gönderilecektir. Bu e-postaların başlık bilgileri sizin suncunuzun IP adresini ele verebilmektedir. Bu konuda incelenebilecek bazı noktaları belirtmek isterim. Buradaki amaç web uygulamasından dışarıya IP verisini gönderebilmek veya web uygulaması ile dışarıda bulunan bir kaynağa erişim sağlayabilmektir.

1. Web uygulamasının gönderdiği e-postalar,
2. Web uygulamasına gönderilen uzak linkler; (multimedya dosyaları, ofis dokümanları),

   a. Bu linkler web uygulamasının başka bir sunucuya doğrudan erişimini sağlayabilir ve/veya

   b. Avatar resmi, gömülü medya, web servisinin dışarıdan ulaşabileceği her türlü kaynak. (Sizin sunucunuza bağlantı atar ise log kayıtlarından, IP logger servislerinden bilgi edinebilirsiniz,)
3. XSS saldırıları (bkz. zafiyetli servisler),
4. Remote File Inclusion sayesinde dışarıdaki dosyaya erişme zafiyetleri (bkz. zafiyetli servisler) ve
5. Wordpress ve benzeri servislerde bulunan pinglerdir (pingback/xmlrpc)

3 HTTP, HTTPS, REST, SOAP, XML-RPC vb. ile yapılan isteklerde WAF'tan sonra başlık verilerinde değişiklik görülebilir

4 WafW00f, WhatWaf, Nmap http-waf-detect

6. RCE ile servisten ping yollamak (bkz. Zafiyetli servisler)

Bu tarz saldırılardan korunmak için girdi kontrolünü doğru bir şekilde sağlamanız gerekir. Kullanıcıdan alınan veriye duyulabilecek güven sonucunda sunucunuzun istenmeyen kaynaklara erişmesi mümkündür. Talep doğrultusunda sunucunuzun hangi kaynaklara ve IP bloklarına erişebileceğini sınırlandırabilirsiniz. Bu sayede bu şartları sağlamayan kaynaklara doğrudan erişimi kısıtlayıp, IP'nizi gizli tutabilirsiniz.

Bağlı Atlatma

Web uygulamalarının IP bilgisini dışarıya sızdırmalarına her zaman ihtiyacımız yoktur. Bağlı atlatma sırasında saldırgan web sitesinin var olan bir kaynağına erişim sağlayıp servisin IP adresini öğrenebilir. Cloudflare örneğinden devam edecek olursak, Cloudflare koruması alan adınızın DNS sunucusunda tutulan bütün kayıtları kapsamaz. Sadece sitenize ulaşan alan adının NS kayıtlarını düzenlemek Cloudflare konfigürasyonu için yeterlidir. Bu nedenle alan adı kayıtlarınızda (DNS) var olan mail kaydına (MX) atanan IP adresi uygulamanın çalıştığı IP adresini döndürebilmektedir. Bu konuda incelenebilecek bazı noktaları belirtmek isterim.

1. DNS kayıtları[5],
2. Web uygulamasına ait subdomain'ler[6] (subdomain.servis.tld),
3. SSL kayıtları[7] (Unique SSL kayıtları, SSL IP sızdırması), Certificate Transparency logları (crt.sh)
4. Uygulamada bulunan IP bildiren dosyalar/sayfalar

   a. Arama motorları sayesinde servisinizde bulunan log dosyaları vb. dosyaları incelemek

   b. Servisinizin gösterdiği web sayfalarında gömülü olan (eklenti sayesinde veya kullanıcı/yetkili tarafından unutulmuş) IP'leri tespit etmek.

   c. Path Traversal ile dosyalara erişim sayesinde IP bildiren dosya bulmak (statik HTML sayfalar/ web uygulamasında çalışan eklenti dosyaları, hosts vb.) (bkz. Zafiyetli servisler)

   d. Local File Inclusion ile sunucudan dosya okumak (log kayıtları vb.) (bkz. Zafiyetli Ser.)

   e. RCE ile sunucudan WhatIsMyIp gibi servislere istek göndermek. (bkz. Zafiyetli servisler)
5. Eski DNS kayıtlarını incelemek (DNS History)

   a. Bazı siteler bulut tabanlı WAF'lara geçmeden önce sunucu IP'lerini doğrudan DNS kayıtlarına koyabilmektedir. Eski kayıtları viewdns.info gibi servisler üzerinden inceleyebilirsiniz.
6. SQL injection gibi yöntemler ile web uygulamasının verebileceği hataları incelemek (bkz. Zafiyetli servisler)
7. Reverse IP ile WAF'ın IP adresine sahip başka web servisleri bulunabilmektedir.

   a. Eğer WAF'ın kayıtlarında aynı sunucuda bulunan iki web sitesi var ise ikinci site üzerinde bu yöntemler denenebilir.

   b. Reverse whois ile aynı maile kaydolmuş domainler de bulunabilir.

   c. Shodan ve Censys.io gibi sitelerden aynı SSL kaydına sahip siteler bulunabilir.
8. Sızdırılmış veri tabanları, Cloudflare gibi sitelerin veri tabanları daha önceden sızdırılmış olması nedeniyle internetten sorgulanabilmektedir.

   a. Crimeflare/Clouflare Watch vb. siteler.

   b. Bazı resolver servisleri ile Shodan / Censys.io gibi servisler aktif olarak tarama yapmaları nedeniyle ekstra kayıtlara sahip olabilmektedir.
9. Google, Archive.com ve benzeri sitelerin sizin siteniz hakkında tuttuğu eski kayıtlar.

   a. Eğer siteniz önceleri IP bazlı host ediliyorsa bu yöntem IP'nizi sızdırabilir.
10. HTTP istekleri ile IP aralığı taraması.

    a. Eğer web servisinin bulunduğu sunucuyu tahmin edebiliyorsak (bir IP aralığına sahip isek) bu IP aralığına istek yapıp gelen yanıtları inceleyebiliriz.

    b. Eğer IP yerine port bazlı bir servis kullanılıyor ise IP'ler üzerinde bize istek dönen portları tarayabiliriz.

    c. Eğer isim bazlı bir servis kullanılıyor ise her IP'ye bir başlık (genelde host header'ı) göndermek suretiyle bir istek yapabiliriz. Geriye dönen yanıtı inceleyerek doğru IP'ye istek yapıp yapmadığımızı belirleyebiliriz.

    d. Bu yöntemlerin çalışması için sunucunun dışarıdan bir IP'ye erişebilmesi gerekir. Eğer erişim sadece WAF üzerinden olması için yapılandırılmış ise TCP yerine UDP üzerinden çalışan servislere WAF iplerini spoof ederek bağlanmayı deneyebilirsiniz.

5 Bazı web servislerinin DNS kayıtları IP adresini döndürebilmektedir. Mail için MX, DNSSEC için SIG, IPv6 için AAAA; domain sertifikaları için CAA kaydına bakılabilir. Tüm kayıt türleri için Wikipedia sayfası incelenebilir. Web sitesinin DNS kayıtları DIG aracıyla veya internetten sorgulanabilir

6 Bazen sitelerin subdomainleri IP DNS kayıtlarını yapmamış olabiliyor. Bu nedenle subdomainlerine Ping v.b. araçlar ile eriştiğimizde IP adresini görüntüleyebiliriz.

7 SSL kayıtlarının özgün olması Shodan ve Censysy.io gibi servislerden web sitesinin bulunmasını kolaylaştıracaktır. Reverse domain ile alınan aynı IP ye bağlı alan adlarını bu sertifikada bulunan alan adlarıyla karşılaştırarak aynı sunucuda bulunan alan adlarını tespit etmeye çalışabiliriz. Aynı SSL sertifikasına sahip sunucuların IP adreslerinden web servisinin bulunduğu sunucu tespit edilebilir.

Bu tarz saldırılardan korunmak için web servisinin dışarıya gönderdiği ve dışarıdan aldığı istek ve kaynakların WAF tarafından sıkı bir incelemeden geçirilmesi gerekir. Eğer bir servis/uygulama dışarıya IP bilgisi döndürüyor ise bunu engellemesi gerekir. Web servisinizin ve sunucunuzda çalışan uygulamaların da bu tarz bir olası saldırıya karşı güvenli olması gerekmektedir.

Zafiyetli Servisler

Web servisleri her zaman yeterince güvenli olmayabilir. Belli zafiyetleri taşıyan web servisleri sizlere IP adreslerini kendi elleri ile sunacaklardır. Zafiyetin türüne göre size sunulan IP adresi bir istek şeklinde ya da direkt olarak size sunulabilir. Bu konuya ayrıca değinmemin nedeni bu kısımda anlatılanlar bağlı veya tersine atlatma konularına dahil olmakla birlikte web servisinde veya WAF üzerinde bulunan bir zafiyetin sömürülmesine dayanmaktadır. Bu konuda bazı incelenebilecek noktaları belirtmek isterim.

1. XSS saldırıları:

   a. Bu sayede sunucudan dışarıya bağlantı yaratabilirsiniz.

2. Remote Code Execution saldırıları:

   a. Bu sayede web uygulamasından dışarıya bağlantı yaratabilirsiniz,

   b. Eğer erişiminiz bulunuyorsa yerel dosya sistemini okuyabilirsiniz (RCE to LFI),

   c. Eğer dış ağa erişiminiz var ise WhatIsMyIP gibi bir servise sorgu atarak cevabını görebilirsiniz.

3. LFI ile servise bulunan bir dosyayı görüntülemek:

   a. Bu sayede web sitelerinde bulunan bir dosyaları görüntüleyebilirsiniz,

   b. Log dosyaları, eklenti dosyaları, hosts vb. yapılandırma dosyaları.

4. SQL injection:

   a. SQL Injection sayesinde veri tabanına erişebilirsiniz,

   b. Veri tabanı sunucusu sizin sunucunuz ile aynı yerde ise veritabanının bulunduğu IP'yi öğrenmeye çalışabilirsiniz,

   c. Eğer farklı sunuculardaki ise SQL üzerinden kod çalıştırıp RCE zafiyetini deneyebilirsiniz. Bu sayede sunucuda kod çalıştırıp gelen bağlantılardan web servisinin IP adresini tespit edebilirsiniz.

5. Path Traversal ile dosya yolunu bulmak:

   a. Bu zafiyet sayesinde web uygulamasının altındaki farklı klasörleri görüntüleyebilirsiniz,

   b. Eğer web servisinin yetkisi var ise LFI exploit'ini (lokaldeki dosyaları okumayı) kolaylaştırır. Dosya isimlerini aklınızdan/listeden/random denemenize gerek kalmaz,

   c. Full Path Disclosure zafiyeti ise size web servisinin sunucu üzerinde nerede bulunduğunu gösterir. Eğer yetkiniz var ise LFI yapmayı kolaylaştırır.

6. HTTP Enum:

   a. Bazı web servisleri (bkz. IIS 7) web adresine HTTP isteği gönderirken host header'ı boş bir şekilde gider ise cevap olarak IP adresini döndürmektedir,

   b. "curl http://sub.domain.tld -v -l --http1.0 --Header 'Host: ' " sayesinde bu zafiyeti deneyebilirsiniz.

7. XMLRPC/PingBack ve diğerleri:

   a. Bu iki fonksiyon Wordpress kullanan web sitelerine ait olup bu fonksiyonlara yapılan istek doğrultusunda verilen yere (IP /domain) istek atmaktadırlar.

8. WAF'da bulunan hatalar (bug):

   a. Cloudflare 17 Şubat 2017'de bir hata yüzünden sunucuda RAM'den okuma yapabilmekte idi. Bu sayede RAM'den bilgi çekip IP adresi/HTTP başlıkları hatta cookie verileri dahil bulunabilmekte idi,

   b. ipleak.com/full-report/ vb. web servislerinden sorgulama yapabilirsiniz. Bu ve benzer arama motorları sayesinde IP bilgisine erişmeyi deneyebilirsiniz.

9. Heartbleed vb. sunucu/web servisi zafiyetleri:

   a. Heartbleed zafiyetine sahip olan sunucunun RAM'inden belli miktarda veri okunabilmekteydi. Bu ve benzeri zafiyetler ile içeriden bilgi edinilebilir.

10. Bazı web servislerinin düzgün yapılandırılmamış panellerine erişim yaptığınızda veya bir fonksiyonu talep ettiğinizde (parolamı unuttum gibi) size IP:Port şeklinde bir adres dönebilmektedir.

Zafiyet içeren servislere sahip olmamak için servislerinizi ve eklentilerinizi daima güncel tutunuz. Web servisinizi düzenli olarak pentest ve takip eden zafiyet iyileştirme (vuln. Remediation) sürecinden geçirerek bulunabilecek zafiyetleri düzetebilirsiniz. Web servisinizin kullandığı teknolojilerde oluşabilecek sıfırıncı gün zafiyetlerini takip etmeniz size bu tarz bir saldırının yapılma riskini azaltacaktır. Sunucunuz ve web uygulama ayarlarını bu bilgiler doğrultusunda gözden geçirmeniz yararlı olacaktır.

Erişim Sağlama Konusunda Bilmeniz Gerekenler

Bazı WAF'ların erişim esnasında sizin isteğinize cookie/session gibi verileri eklediğinden bahsetmiştik. Web uygulamaları WAF'lar atlatılmak istenildiğinde bunun gibi verilere bakarak engelleme yapabilmektedir. Bazı servisler bu verilerin bir desene uyup uymadığını kontrol ederken, bazıları ise WAF ile konuşup bu kaydın gerçekliğini sorgulayabilmektedir. Bu nedenle bu parametreleri WAF'a bağlanıp elde ettikten sonra isteklerinize ekleyebilirsiniz.

Bazı web servisleri veya sunucuları sadece WAF üzerinden gelen IP aralıklarına izin vermektedir. Bu tarz bir problem ile karşı karşıya kalır iseniz UDP kullanan servisler sayesinde IP adresinizi spoof ederek doğrudan erişim sağlamaya çalışabilirsiniz. Eğer WAF üzerinden istek gönderebilecek bir yöntem tespit ettiyseniz yukarıdaki bütün saldırı yöntemlerini WAF'ı kullanarak sağlayabilirsiniz.

Erişim doğrulama

WAF'ın IP adresini tespit ettiğinizi varsayalım. Peki bu IP adresi gerçekten istenilen kaynağa mı ait? Bu IP adresine erişiminiz var mı, var ise nasıl? Bu soruları doğrulamak için yapabileceğiniz birkaç adımı belirtmek isterim.

1. IP adresini tespit etmede kullandığınız yöntemi tekrarlayarak aynı sonucu aldığınızdan emin olun:

   a. Bu sayede sahte bilgi ve hatayı minimize etmiş olursunuz.

2. *hosts* dosyanızı IP ile değiştirip web servisine ulaşmaya çalışın:

   a. Bunu yaparken cookie verilerini inceleyerek/WAF tespit yöntemlerini kullanarak WAF'ı geçip geçemediğinizi test edebilirsiniz,

   b. Wireshark ile yaptığınız isteği inceleyip WAF'a uğrayıp uğramadığını tespit edebilirsiniz,

   c. Bazı tarayıcılarda bulunan yönlendirme tespit eklentileri de Wireshark'a benzer bir sonuç verecektir.

3. Bulunan IP'ye ve sunucuda kullanılan yönteme göre direkt/host parametresi/port ile erişmeyi deneyebilirsiniz.

4. Bulunan IP karşısında uygulanacak stres testleri web sitesinin WAF/CDN tarafından cache belleğe alınmamış parçalarında yavaşlamaya sebebiyet verecektir. Eğer sunucu/web servisi sadece belli IP'lere cevap veriyor ise yavaşlama yaşanmayacaktır. Bu sayede IP'ye erişiminiz olup olmadığını test edebilirsiniz.

5. Bazı durumlarda web servisleri WAF sistemleri haricinde doğrudan erişimi kısıtlamak için WAF ile web servisi arasına tersine bir bağlantı (Reverse Proxy) konumlandırabilmektedirler. Tespit ettiğiniz IP adresinin web servisine doğrudan mı yoksa tersine bağlantı ile dolaylı bir şekilde mi ulaştığını kontrol etmeniz gerekebilir.

Bulut Tabanlı WAF'ların İncelenmesi

Bu kısımda bulut tabanlı WAF'larda kullanılan teknolojilerden bazılarını inceleyeceğim. Hepsinden bahsetmek çok zor çünkü yeterli seviyede kodlama bilen ve bir sunucuya sahip olan herkes kendi WAF'ını oluşturabilmektedir. Bu nedenle sadece belirli bir kısmını inceleyebilmekteyim.

Cloudflare

Cloudflare, Go/Python/PHP ve Javascript yazılımları ile geliştirilen bulut tabanlı bir WAF'tır. Kendisi açık kaynaklı olup kaynak kodlarına https://cloudflare.github.io/ adresinden erişilebilir. Bu WAF kullanıcılarına ülke/IP gibi birkaç farklı parametre kullanarak filtreler tanımlamalarına izin verir. Bu filtreler engelle, izin ver, CAPTCHA çözdür, Javascript çalıştır modlarından oluşmaktadır. Kullanıcılarına IP blokları ve ülke kodları (TOR çıkış IP'leri TOR adı altında bir ülke şeklinde sunulmaktadır) ile filtreleme imkanı sağlar. Filtreden geçen kullanıcıların cookielerine iki yeni değer eklerler. Bu değerler sayesinde web servisine erişim sağlanır. Web servisi saldırı altındayken filtreleme uygularlar. Size web servisinin IP adresi yerine kendi IP adresini döndürür. Ücretsiz SSL sertifikası sağlar. Web servisi ile kullanıcı arasında bir filtre görevi görerek bazı istekleri engellerler. SQL Injection, XSS, Path Traversal gibi saldırıları bir dereceye kadar engeller. Web servisinde oluşabilecek anlık çöküntü karşısında CDN görevi görerek saldırıya uğramış ve erişilemeyen sayfalar için cache'de bulunan web sitesini döndürebilirler.

Imperva SecureSphere

Impervanın geliştirdiği SecureSphere Gartner Raporu'nda en iyiler kategorisinde bulunan bir WAF'tır. Kullanıcılarının genellikle şirketler olduğunu ve WAF'ın 45 bin dolarlık fiyatını düşünürsek kaynak kodlarının yayınlanmayacağını tahmin edebiliriz. Botlara karşı güncellenen bir "Tehdit Radar"ına sahiptir. Abone olunan sistemlerden güncel olarak verileri alıp filitrelere ekleyebilmektedir. Tehdit Radarı; Kaynakları güvenilirliğine göre sırama,

- Topluluğundan ve dışarıdan topladığı bilgilere göre güncelleme,
- Botlara karşı koruma,

- Hesap ele geçirme saldırılarına karşı koruma

sağlamaktadır. Bu WAF'ı algılamak için bir saldırı sonrasında dönülen istekte bulunan HTTP versiyonunu incelemek gerekir (WAFW00F). Özelliklerine şuradan ulaşabilirsiniz: www.imperva.com/docs/DS_SecureSphere_Web_Application_Firewall.pdf

Gartner Raporu

Gartner şirketi güvenliğin belli alanlarında yıllık raporlar yayınlamaktadır. Bu raporlarda güvenlik ürünlerini belli kategorilerde sıralayıp onlara özgü bir grafik çıkartmaktadır. Bu grafik sayesinde WAF ürünlerini inceleyebilirsiniz.

WAF Tespitinde Kullanılan Otomatize Araçlar

Wafw00f

Wafw00f ve Waffun DEFCON18 konferansında tanıtılmış olup Wafw00f, Kali Linux işletim sisteminde yüklü olarak gelmektedir (WAFFUN yayınlanmamıştır). Bu araç istekler ve alınan yanıtları inceleyerek WAF'ın türünü bulmanızı sağlar. WAF'a istekler göndererek hatalı/engelli sayfalar ile engellenmemiş sayfalar yakalamayı, alınan yanıtlara göre WAF türünü tahmin etmeyi amaçlar. WAF'a karşı yaptığı denemelerde akıllı bir şekilde istek yapamaz (mesela admin klasörünü uygulamaya göre sorgulamaz veya bulunamayan bir dosyayı denerken sistemde bulunup bulunmayacağına bakmadan rastgele değer üreterek dener). Programın Github üzerinden de temini mümkündür. Bir Python betiğidir. Bazı özellikleri listelenmiştir.

- CDN'leri ve WAF'ları isteklere dönen cevaplar (HTTP Response) sayesinde belirlemeye çalışırlar,
- Bazı WAF'ları belirlerken saldırı denemeleri yapabilmektedir (WAF'dan bir hata alabilmek adına),
- Varsayılan olarak Microsoft.com'u hedef almaktadır (SSL kapalı ve port 80),
- Sırasıyla normal, bulunmayan dosya, bilinmeyen metot, Path Traversal, hatalı host, hatalı tagın encoded hali, hatalı tag, XSS, admin klasörü/korunaklı klasör, encoded XSS, cmd.exe dosyasına erişim saldırılarını dener,
- Kodu modifiye ederek bu saldırıları değiştirebilirsiniz ve bu sayede farklı saldırı vektörlerini deneyebilirsiniz,
- Admin klasörü olarak /Admin_Files/ olarak belirlemiştir,
- XSS olarak *<script>alert(1)</script>*, Path Traversal için *../../../../etc/passwd* denemektedir,
- Hatalı tag için ise *<invalid>hello* kullanılmaktadır,
- https://github.com/EnableSecurity/wafw00f

WhatWaf

WhatWaf, wafw00f gibi WAF tarama/tespit aracıdır. Proxy desteği, çoklu URL desteği, 20 farklı tamper metodu, SQL ve XSS kullanarak firewall atlatma, dosyadan veya terminal komutuyla kişisel payload oluşturma gibi bir sürü ek özelliğiyle Wafw00f'tan ayrılmaktadır. Desteklediği 40 farklı WAF konusunda minimum bir saldırı ile hata üretmeyi garantilemektedir. Wafw00f gibi HTTP isteği yapıp geri dönen yanıtı inceler ve buna göre WAF türünü belirlemeye çalışır. Bir Python betiğidir. Birkaç özelliği listelenmiştir:

- SOCKs4/5, HTTP/s ve TOR proxylerini kullanabilir,
- SQLi ve XSS ile WAF'ların filtrelerini bypass edebilir,
- Birden çok site için tarama yapabilmektedir (-l / --list parametresi),
- 40 firewall destekler,
- 20 tampering metodu bulunur,
- Kendi payload'larımızı tanımlayabiliriz,
- *User Agent* değişimine izin verir,
- Sırasıyla 20 tamper metodu şu şekilde sıralanabilir:
  - Kesme işaretini UTF Encode ile gönderme, kesme işaretinin başına *NULL* karakter ekleme, payload'ın sonuna null karakter ekleme, payload base64 kullanarak encode etme, payload'ın karakterlerine çifte URL encode uygulama, sayıları parantez içine alma, kesme ve çift tırnak işaretlerini backslash kullanarak kaçırma, payloadı küçük harfli yapma, bazı karakterleri Unicode'a çevirme, parantezlerin içindeki karakterin başına çift tırnak ekleme, payload'ı yorumun arasına alma, payloadı yorumun arasına alıp boşlukları da yoruma çevirme, payloadın karakterlerini HTML entity'leriyle değiştirme, bazı karakterleri ordinal halleriyle değiştirme, payloadın başına null ekleme, payload'ı rastgele büyük küçük harf yapma, payloada rastgele yorum ekleme, payload'a rastgele Unicode karakter ekleme, boşlukları yorum yapma, boşlukları çift forward flash (/) yapma, boşluklara yeni satır ile rastgele üretilmiş karakterler ekleme, payload'ı rastgele boşluk ve yorum ile genişletme, boşlukları null karakteriyle değiştirme, boşlukları + işaretiyle değiştirme, boşlukları ASCII boşluk karakterleriyle değiştirme, payload büyük karakterler haline getirme, noktalama işaretlerini URL encode etme, bütün karakterleri URL encode etme.

xWaf

xWaf Çinli MayIKissYou adlı kullanıcı tarafından yazılmıştır. Bu araç encoding yöntemleri ve sqlmap tamper kullanarak WAF'ı geçmeyi ve SQL Injection yapmayı amaçlamaktadır. WAF ile ilgili güzel bilgiler döndürüp encoding sayesinde sqlmap'in önüne geçmek istese de tamper yöntemleri ile

Sqlmap'a bağlı kalmaktadır. Bir Python betiğidir. Amacı IP adresini bulmak değildir, bu nedenle bu yazıda bahsedilen yöntemleri kullanmak yerine ileriki yazılarımda bahsedeceğim Dolaylı Erişim yöntemlerini kullanmayı amaçlar

bypasswaf

Bypasswaf, Burp aracının HTTP başlık verilerine birkaç eklenti yaparak WAF'ı geçmeyi planlamaktadır. İstek yerel adresten geliyormuş gibi göstermek amacıyla HTTP başlıklarını değiştirmek, ekstra başlıklar eklemektedir. Burp eklentisidir. Eklediği başlıklar ektedir.

- X-Originating-IP: 127.0.0.1
- X-Forwarded-For: 127.0.0.1
- X-Remote-IP: 127.0.0.1
- X-Remote-Addr: 127.0.0.1
- X-Client-IP: 127.0.0.1

Online Resolve Servisleri

Bu servisler genelde alt domainlere ping ile ulaşmaya çalışmaktadır. Bu domainlerin sonuçlarını size dönmektedir. Bazıları eskiden buldukları IP'leri de dönebilmektedir. Belki de eskiden bulunmuş IP adreslerinden IP çözümleyebilirsiniz.

- skypegrab.net/cf.php
- skypeipresolver.net/cloudflare.php
- webresolver.nl/tools/cloudflare
- orca.tech/web-tools/cloudflare-resolver.html
- tools.k2an.com/?page=cloudflareipresolver
- iphostinfo.com/cloudflare/
- anonymiz.com/cloudflare-resolver

Fierce Domain Scanner

Bu araç verilen IP aralığındaki web servislerine isim bazlı erişmeye çalışıp dönen yanıtlarda bir arama yapmaktadır. Bu yanıt sayesinde siteye erişim sağladığında eriştiği IP adresini kaydedebilmektedir.

Github üzerinde bulunan ve IP bulmaya çalışan Cloudflare atlatma araçlarının çoğu (Hatcloud da dahil olmak üzere) eskiden sızdırılmış Cloudflare veritabanını ve alt alan adlarını ping'lemeyi kullanır. Siz otomatize araçlar ile cevap aramak yerine bu araçların nasıl çalıştığını öğrenmiş oldunuz. Bu sayede artık o araçlara bağlı kalmak zorunda değilsiniz.

Bu yazım WAF atlatma üzerine olup üç serilik yazı planımın ilkini oluşturmaktadır. Serinin bu kısmında IP adresinin tespitinden bahsedilmiştir, IP adresi bulunamayan, IP ile erişilemeyen ya da bulut WAF kullanmayan siteler için WAF'ın filitrelerini atlatan yöntemlere ikinci yazımızda değinilecektir.

Bahar Anahmias - banahmias@gmail.com

iPhone 6 Telefonum Çalındı, Hırsızı Nasıl Buldum?

Bundan 2 sene önce telefonum çalındı. iPhone 6. O zamanlar yeni piyasaya çıkmıştı. Biz de almıştık.

Küçük kızımın mezuniyet günüydü. Ailece okul yemeğindeydik. Bizim Tepe'de. Çok güzel bir gecenin ardından eve döndük.

Sabah olunca telefonumu şarja takmam gerektiğini düşündüm. Bütün evi aradım. Yok, yok, yok. Birden telefonumun akşam yanımda olmadığını farkettim. Aceleyle aşağıya indim, arabayı araştırdım. Ardından davetin olduğu mekana gittim. Sordum, soruşturdum. Gören, bilen yoktu. Otoparkta gezindim. Düşürdüm mü diye.

O kadar üzüldüm, o kadar üzüldüm ki. Resmen hasta oldum.

Eşimin hakkını ödeyemem. Çok anlayışlıydı. Bana hiç birşey söylemedi. Dikkat etseydin vs. demedi. Ne kadar üzüldüğümü gördü.

Bir ümit iPhone'ların **"Find my iPhone" (iPhone'umu bul)** özelliğini etkinleştirdim.

Bir de mesaj yazdım. Telefon açılır açılmaz bulunsun diye. **"Lütfen iPhone'umu bulursanız şu şu telefona haber veriniz'** diye.

Telefonuyla yaşayan, dijitale bu kadar önem veren bir insan olarak telefonum gitti diye kahroldum. Tüm notlarım, mesajlarım, kişilerim, son resimlerim, her şey ama her şey oradaydı. Evet, bulutta bilgilerim vardı. Ama son bilgiler eksikti. Son resimler eksikti. Son notlar eksikti.

Ardından 1 ay geçti. Ses seda yoktu. Ben de evdeki eski bir iPhone'u kullanmaya başladım.

Kullananlar bilir, e-mailimiz, iTunes hesabımız, her şey bu telefonlarda.

İşin kötüsü tüm hesaplarımız da bu iPhone'a bağlıydı.

Bir pazar günü e-maillerime bakıyorum. 20-30 tane okunmamış e-mail var. Arada 2 tanesi okunmuş. 'Allah, allah' dedim. 'Ne zaman okudum ben bunu?'. Bir de ne göreyim, benim e-mailimden Apple hesabıma girilmiş, bir de güzel şifre değiştirilmiş, hem e-mail de değiştirilmiş. O anda kafamdan aşağı kaynar sular döküldü. Evime girilmiş, eşyalarım karıştırılmış gibi hissettim. O güne kadar belki de kaybettim, ya da bulan getirir diye düşündüğüm iPhone'umu birisi çalmıştı.

Ertesi sabah aceleyle adliyeye gittim. Suç duyurusunda bulundum. Ailece çalıştığımız sevgili avukatımız işini gücünü bırakıp yardıma geldi.

E-mail hesabıma girilip, iTunes hesabım hacklendiği için suç "Adi hırsızlık" değil, "Bilişim Suçu" sayılıyordu. Biz de o şekilde suç duyurusunda bulunduk.

Yazılarımda hiç bahsetmiş miydim bilmiyorum, en çok sevdiğim şeylerden biri dedektiflik romanlarıdır. Tüm kitap çeşitlerini okumayı çok severim ama onların yeri gerçekten ayrı.

O andan sonra adım adım, bir dedektif gibi olayı çözmeye başladım.

Sinirlenmiştim. Haneye tecavüz edilmişti. Telefonumda ailemin özel resimleri, e-maillerim, numaralarım her şeyim vardı.

Hırsızın e-mailinden yola çıktım. iTunes hesabına bir e-mail vermişti. E-mailinde isim ve soyisim olabilecek kelimeler vardı. Burada hırsızımın ismini yazmak istemem. Olası isim kombinasyonlarını sabırla araştırdım.

Google, Facebook, Instagram hepsine girdim. Bu isimlere baktım.

Birini buldum. Havalı, havalı pozlar vererek fotoğraflarını çektirmişti. Ben de okul davetinde en son fotoğrafçının önünde oyalanıp, mezuniyet resimlerine bakmıştım. Acaba o sırada mı telefonum yürümüştü? Fotoğraflara bakarken muhtemelen telefonumu elimden bırakmıştım, o sırada birinin üstüne bir iki fotoğraf koyup, saklaması ve sonra da alması muhtemeldi. Bu nedenle özellikle havalı fotoğraf çektirmiş, hem de bu fotoğrafları bir fotoğraf stüdyosu aracılığıyla çektirmiş bu genç en önemli şüphelim oldu.

1-2 hafta sonra bendeki telefona iCloud üzerinden birkaç resim geldi. Kız resimleri. Muhtemelen hırsızımın arkadaşı, kuzeni, vs.

Çektirdikleri fotoğrafları WhatsApp üzerinden yolladıkla-

rı için benim telefonuma da düşmüştü. Daha da sinirlendim. Resimler çirkin resimler değildi. Ama ya olsaydı. Çocuklarım da aynı hesaba bağlıydı.

Bilmem biliyor musunuz, resimleri çektiğiniz tarih ve konum resime işleniyor. *(Çapkınlar ve çapkınlık yapmak isteyenler, dikkat edin, derim. Dedektiflik yapmak isteyen eşlere de bir tüyo benden)* Buna da **metadata** deniyor. Resimlerin çekildiği lokasyona, eve kadar Google Earth'ten buldum.

Telefondaki resimleri bilgisayara aktardım, lokasyonu kapatmadan çektikleri için evin Yalova civarında bir ev olduğunu öğrendim. Adresi aldım.

Ardından Facebook'ta benim hırsızın tüm kız arkadaşlarının resimlerine baktım. Fotoğraftaki kızları bulamadım.

Sonra hırsızın Facebook resimlerinin yorumlarına tek tek baktım. O yorumlarda değişik isimli bir kız buldum. Kızın profiline girince, ana sayfada bir de ne göreyim. Bu kız, benim hırsızla, bir iPhone 6 ile aynaya bakarak resim çektirmiş. Muhtemelen benim telefonumla. Kızı da takibe aldım. Çalıştığı yeri, ismini, okulunu gruplarda paylaştıklarından buldum.

Hepsi için bayağı bir mesai harcadım. Kızın Facebook timeline'ında verdiği bazı haberlerden iş adresini buldum.

Şüpheli gencin paylaşımlarından ise çalıştığı yeri, yaşadığı yeri keşfettim.

Tüm bunları biraz üzüntü, biraz sinir, çokça kızgınlıkla yaptım. Bulduklarımı basarak, elimdekilerle **"Bilişim Suçları"** bölümüne gittim.

- Hırsızımın muhtemel ev adresi.
- Hırsızımın e-maili.
- Benim e-mailimde değiştirilen account
- Çektikleri resimlerin lokasyonu
- Kızlardan birinin iş adresi
- Tüm resimler
- Tüm yazışmalar

Hepsinin çıktısını aldım.

Polisimize elimdekileri anlattım. **Telefonumun çalınmasından çok, hesabıma girilmesinin evime girilmiş gibi hissettirdiğini söyledim.**

Ben resimlerin metadatasından şunu şunu buldum vs. deyince polis şaşırdı. Sonra hırsızımı isminden araştırdı. Lokasyonunu tesbit etti.

Ardından kızın ismini verdim. Ama bu isimde hiç kimse yoktu. Kızın adı da bir değişikti zaten. "Amirim acaba o isim aslında şu, şu olamaz mı?" deyince polis dayanamadı "Ne iş yapıyorsunuz?" diye sordu. Kız ismindeki harflerden yeni bir isim türetmişti. Onlara dijital medya alanında yüksek lisans yaptığımı, ama esas olarak öğrenmeye ve araştırmaya çok meraklı olduğumu söyledim. Polis de bana **"Burada çalışsanız kısa sürede amir olurdunuz."** dedi. *(Daha sonra bu eşimle benim aramda bir anekdot olarak kaldı.)*

Sözün özü:
Şu dönemde yeni teknolojileri kimse çalmasa iyi olur. **IMEI numarası** ile telefonun yeri bulunabiliyor ve tespit edilebiliyor. Bilmeyenler de bu yazıdan sonra öğrenir inşallah. Akıllı telefon bunlar malum.

Hırsızımı yakaladım. Polise tüm kanıtları verdim. Ama gönlüm hapis yatmasına izin vermedi. Gencecik çocuk, bir cahillik yapmış. Hırsızlık kötü suç ama telefon hırsızlığı sonuçta. Adam öldürmemiş ya. Mahkeme korkusu vs. ona yeter diye düşündüm.

Geçenlerde mahkemem vardı. Mahkeme öncesi avukatım onlarla konuştu. Bu suçun bilişim suçu olduğu için 5 seneden itibaren ceza alabileceğini, anlaşma yoluna gitmek isteyip, istemediklerini sordu. Tabii ki anlaştık. Zararımı tazmin ettiler ve davayı geri çektik.

Bu da bir telefon hikayesi…

Neden mi yazdım tüm bunları?

Telefonları kimse çalmasın diye.

O telefonlarda herkesin kişisel bilgisi var.

O telefonların nerede olduğu hemen bulunabiliyor.

Polisimiz ve mahkememiz, er ya da geç suçluya cezasını veriyor.

Suç cezasız kalmıyor.

Bir yerde bir telefon bulsanız bile, hemen sahibini bulmaya çalışın. Özenip de kullansam mı diye düşünmeyin.

Sevgiler,

Bahar Anahmias, the iPhone addict

www.birkahvemolasi.co

Parrot Security OS (Parrot Project)

M. Emrah ÜNSÜR (meu@Parrot Project), özel bir şirkette 'pentester/red teamer' olarak çalışıyorum. 'DEF CON' Resmi Türkiye Grubu (DC90312) kurucusuyum. 'Reddit', 'Tor Project' gibi 10+ 'open-source' projeye katkıda bulundum. Şu anda, 'Parrot Project' takım üyesi olup, 'contributor', 'ambassador' ve 'forum moderator' görevlerini yürütmekteyim.

(e-posta: meu@emrahunsur.com, telegram: @emrahunsur)

I. Nedir?

"Parrot Security OS", "Parrot Project" çatısı altında 2013 yılında farklı ülkelerde yaşayan ve tamamen gönüllülerden oluşan bir ekip[1] tarafından "pentesting/red teaming/reverse engineering/digital forensics (+*anti forensics*)/development (*software, exploit, tool*)/privacy defense, anonymity" başlıkları için tasarlanmış, aynı zamanda günlük kullanım için de ideal olan, düzenli olarak geliştirme yapılan ve yeni özellikler eklenen (*rolling releases*),'live' olarak da kullanılabilen, eski veya sınırlı kaynaklarda (*düşük donanımlarda*) verimli çalışabilen (*lightweight*)[2], hem tecrübeli hem de yeni kullanıcılar için uygun, 'stabil' bir 'GNU/Linux' dağıtımı ve topluluk projesidir.

Bunların yanı sıra,

- Özenle seçilmiş 600+ güncel araç barındıran,
- Güvenli ve şifrelenmiş ortam (*end to end encryption*, *full disk encryption*) sağlayan,
- Geliştirme (*software, exploit, tool*) için uygun ortam sağlayan,
- Güvenli derleme ortamı ve repo'lara (*gpg signed*) sahip,
- Dünyanın dört bir yanında 'mirror'[3] sunucuları bulunan,
- Geniş donanım desteği olan,
- 'ARM' desteği olan,
- 'MATE' masaüstü ortamı kullanan,
- Tamamen 'özgür' olan (*kaynak kodu istediğin gibi oku ve/veya değiştir!*),
- Tamamen ücretsiz (*ve hep ücretsiz kalacak!*) olan,
- Kurulumu ve kullanımı basit,
- 'polimorfik'[4] bir işletim sistemidir.

Ek olarak, "Parrot Security OS", DistroWatch sitesinde, kendi alanındaki en çok tıklanan dağıtımlar listesinde 2. sırada, genel dağıtımlar listesinde ise 29. sıradadır. (*Son 3 aylık veriye göre.*)

1 Ekip üyelerinin her biri, bir kurumda veya kuruluşta 'pentester/red teamer, software developer, system/network administrator' gibi görevlerde bulunmaktadır.

2 Minimum gereksinimler; CPU: 1GHz Dual Core CPU, 32-bit, 64-bit, ARMv7 & ARMv8, RAM: 256MB~512MB, HDD: 6GB~8GB (*standart*), 8GB~16GB (*full*)

3 'ParrotSec OS' imaj dosyalarını ve paketlerini indirmek (*download*) istediğiniz zaman, çeşitli ülkelerde bulunan lokasyonlardaki 'resmi mirror'ların birinden alırsınız.

4 'Parrot Security OS', 'pentest/red teaming', yazılım geliştirme ve -'güvenli' (*sandbox+şifrelenmiş ortam+anonimlik*)- günlük kullanım amaçlarının hepsini tek bir işletim sistemi içerisinde toplamaktadır.

Özellik Tablosu

"Parrot Security OS", 3 farklı versiyona sahiptir; Security, Home, IoT. Bu versiyonların özellikleri ve farkları aşağıdaki tabloda belirtilmiştir.

	Security	Home	IoT
Mimari	x86 32bit&64bit	x86 32bit&64bit	ARMv7&ARMv8 64bit
Linux Versiyonu	4.14	4.14	('board'a bağlı)
Debian Versiyonu	Debian 10 Buster	Debian 10 Buster	Debian 10 Buster
Release Model	Rolling Release	Rolling Release	Rolling Release
Masaüstü Ortamı	MATE 1.18	MATE 1.18	MATE 1.18 veya 'headless'
UEFI desteği	√	√	×
Sandbox	√	√	√
Office Suite	LibreOffice 5.4	LibreOffice 5.4	Abiword/Gnumeric
Web Suite	Firefox 57 Quantum	Firefox 57 Quantum	Epiphany (veya firefox-esr)
Adblocker ve Web koruma	Ublock Origin + NoScript + Privacy Badger	Ublock Origin + NoScript + Privacy Badger	Ublock Origin + NoScript + Privacy Badger
AnonSurf + Tor Browser	√	√	-
'Pentesting/Red Teaming' araçları	√	×	-
'Cryptography' araçları	√	√	√
'Reverse Engineering' araçları	√	×	×
'Digital Forensics' araçları	√	× ('cloning' araçları bulunmaktadır)	× ('cloning' araçları bulunmaktadır)
Geliştirme (software, exploit, tool development) araçları	√	√	√
Wine desteği	√	×	×
Bitcoin cüzdanı (electrum)	√	√	√

Download url: https://www.parrotsec.org/download.fx

II. Farklar

Topluluk

"ParrotSec OS"i benzer dağıtımlardan ayıran en önemli fark, amacından ziyade ona ulaşma yolu. Tek cümle ile özetlemek gerekirse, 'Parrot Project', bir 'güvenlik' dağıtımı geliştirmekten daha fazlası olmak istiyor ve birçok fikir için 'gateway' (köprü, en) görevi görüyor. Bu güç de topluluğumuzdan geliyor.

Altını çizmem gereken önemli noktalardan bir tanesi, güçlü teknik ekip ve altyapısının yanı sıra kendi alanındaki hiçbir dağıtımın sahip olmadığı (*'open-source' doğası gereği*) herhangi bir kâr amacı gütmeden yardımlaşma ve ortak projeler üretebilmek için kurulmuş, gönüllülük esasına dayanan ciddi bir topluluk ve organizasyon yapısına sahip olmasıdır.

Kuzey/Orta/Güney Amerika, Asya, Avrupa, Afrika olmak üzere, 20+ ülkede temsilcisi olan topluluklarımız mevcuttur ve bu topluluklarda ülkenin kendi dilinde iletişim kurabilmek mümkündür. Bu topluluklar, iletişimlerini yüz yüze, bir alana mesaj bırakarak veya anlık olarak sağlamaktadır.

Bu toplulukların amacı, sadece 'Parrot Project' (*ve *nix*) desteği ve eğitimi değil (*kullanıcılar karşılaştıkları sorunları anlık olarak sorabiliyor, cevabını ve çözümünü anlık olarak hızlıca alabiliyor!*), genel olarak -*tamamen ücretsiz olmak koşulu ile*- siber güvenlik/bilgi güvenliği başlığı altındaki her alt başlık konusunda tartışmalar/paylaşımlar/bilgilendirmeler/eğitimler/sunumlar/yayınlar yapmaktır.[5]

Teknik

Güncel versiyonumuzun (3.10/Intruder) iki major özelliği bulunmaktadır.

Bunların birincisi, 'privacy defense, anonymity' başlığı için tasarladığımız 'AnonSurf'. 'AnonSurf', sistem trafiğinin 'TOR' ve 'I2P' ağları üzerinden yapılmasını sağlayan, 'GUI' ve 'CLI' arayüzü olan 'Parrot Security OS' anonim modudur. Çalışma mantığı ise, 'firewall (iptables)' katmanında çalışarak, TCP/IP tespitini zorlaştırır, 'TCP' trafiğinin hepsi otomatik olarak 'TOR proxy'e yönlendirilir. Ayrıca, 'Tor Browser, TorChat' gibi standart araçlar da üzerinde yüklü gelmektedir.

İkincisi ise, 'sandbox' sistemi[6]. Farklı tekniklerin birleşimiyle tasarladığımız bu özellik, işletim sistemi bileşenlerini 'izole' ederek 'proaktif' şekilde korunmasını sağlıyor. Çalışma mantığı ise, örneğin, sistem üzerinde bulunan 'Firefox' çalıştırıldığında, 'sandbox' bileşenleri tetiklenir. Kullanıcı hesabına tanımlanmış özel bir kullanıcı alanı oluşturulur. 'root' kullanıcısı ve kullanıcı değiştirme yetenekleri pasif hale getirilir. 'Linux capabilities' (*Linux 2.2 ve POSIX 1003.1e'de tanıtılmıştır*), 'supplementary' kullanıcı grubu engellenir. 'Shell' ortamı pasif, 'seccomp' aktif hale getirilir. Buna ek olarak, tüm sistem 'salt okunur' olduğu için özel bir 'dosya ağacı' oluşturulur, '/dev' ve '/tmp' klasörlerinin özel sürümleri orijinal dosyaların yerini alır ve '/home' klasörü yalnızca beyaz listeye alınmış klasörlerin çok sıkı bir seçimini (*whitelist*) içerir, yazma izinlerine sahip olan klasörlere zararlı kodun yürütülmesini önlemek için 'noexec' bayrağı atanır. Benzer kısıtlamalar diğer hassas sistem programlarına uygulanır. Bu sistemin amacı, tehditleri 'izole' ederek, saldırganın hassas ve kritik kaynaklara ulaşmasını engellemektir.

III. Planlar

Eğitim

Sıkı kurallara ve disipline bağlı düzenli geliştirme faaliyetleriyle, var olan özelliklerin mükemmelleştirilmesi, bu faaliyetlerin yeni özelliklerle birleştirilmesi, güncel teknoloji/trend'lerin projeye dahil edilmesi, yeni yazılım/araç analizlerinin yapılması[7] ve yeni kullanıcılar için sistemin daha kolay kullanılmasını sağlamanın yanı sıra odaklanmak istediğimiz ve bizim için en önemli konu, eğitimdir.

Halihazırda yaptığımız eğitim çalışmalarının yanında hem uluslararası platformumuzda hem de bölgesel toplulukların/ülke topluluklarının kendi dillerinde verecekleri eğitimlerin arttırılması, çeşitlendirilmesi ve bu çerçevede 'pentesting/red teaming, reverse engineering, software development, system administration, networking, cryptography, malware analysis' konuları üzerinde dokümantasyon havuzu (*kitap, e-kitap, makale, kılavuz vb*) oluşturmak da üzerinde durduğumuz noktalardan bir tanesidir.

Teknik

'Sandbox' sistemimizi geliştirmeye ve mükemmelleştirmeye devam edeceğiz. Bunun yanı sıra, 'Parrot Security Mobile' yayınlamak da bir sonraki planlarımız arasında bulunmakta. Bugüne kadar yaptığımız gibi, bu da 'benzer' bir proje değil, 'özel' bir proje olacak.

İletişim

Aşağıdaki adresleri kullanarak bizlere ulaşabilir, daha ayrıntılı bilgi alabilir, soru(n)larınız ve/veya önerileriniz varsa bizlerle paylaşabilirsiniz;

- Parrot Project Resmi Web Sitesi: https://www.parrotsec.org/
- Parrot Community (*Forum*): https://community.parrotsec.org/
- Parrot Project 'Ambassador' Listesi: https://docs.parrotsec.org/community/ambassadors-list
- Parrot Project Yerel Topluluklar: https://docs.parrotsec.org/community#local-communities
- Telegram (*ParrotSec Global*): https://t.me/parrotsecgroup
- Telegram (*ParrotSec Türkiye*): https://t.me/parrotsecturkey

5 Topluluk gruplarına katılım, ilgisi ve/veya bilgisi olan herkese açıktır.

6 'Sandbox', çalışan/çalıştırılacak programları -*işletim sisteminden*- ayırmak (*izole etmek*) için kullanılan bir güvenlik mekanizmasıdır. Genellikle güvenilmeyen veya doğrulanmayan kaynaklardan alınmış, test edilmemiş veya güvenilmeyen yazılımlarla karşılaşıldığında kullanılır. (*ref: Vikipedia*)

7 Analizler, ekip üyeleri aktif olarak bir kurumda veya kuruluşta 'pentester/red teamer, software developer, system/network administrator' gibi görevlerde bulundukları için daha verimli olmaktadır.

Erhan ALTINDAS - erhan.altindas@btsis.com

Amatör Telsizcilik

Amatör Telsizcilik:
Her şeyden önce bir hobidir.

Bu hobi herhangi bir ticari, siyasi yayın amacı olmaksızın tamamıyla bireysel çabalar ile ulusal ve uluslararası radyo haberleşmesini bünyesinde barındıran bir aktivitedir. Bu aktivite ulusal ve uluslararası yönetmenliklere bağlı kalmak şartıyla kişinin kendisini geliştirmeye yönelik olarak ülkesinde ve dünyanın çeşitli yerlerinde yer alan amatör telsizcilerle haberleşme yapması şeklinde tanımlanabilir. Sözü geçen bu faaliyetlerin tümü "RADYO AMATÖRLÜĞÜ" ya da "AMATÖR TELSİZCİLİK" şeklinde anılır.

Bu tanım kanunen "" Hiçbir maddi ve siyasi çıkar gözetmeksizin ve milli güvenlik gereklerine mutlaka bağlı kalmak şartıyla sadece kişisel istek ve çaba ile radyo tekniği alanında kendisini yetiştirmek amacıyla çalışan gerçek kişiler" 7 Nisan 1983 gün ve 2813 sayılı Telsiz Kanunu Madde 12) "Radyo Amatörü" olarak belirtilmiştir. Dünyada günümüzde yaklaşık 4.2 milyon olmasına karşın, Türkiye'de ise sayısı her yıl artmakla birlikte yaklaşık 15 bin 346 civarında Amatör Telsizci vardır (Türkiye'deki sayı 12/2016 tarihi itibari ile Kıyı Emniyeti Genel Müdürlüğü'nden alınmıştır.). Bu sayının ülkemizde az olmasının en temel nedeni ise Amatör Telsizciliğin 1983 yılına kadar ülkemizde yasak olmasıdır.

Nedir bu RÖLE dedikleri?

Röle bir bakıma cep telefonu şebekelerindeki baz istasyonları gibidir. İki telsizin birbiri ile doğrudan iletişim kuramadığı noktalarda merkezi ve yüksek bir noktada bulunan röle sistemi ile iletişim kurulur. Bir frekanstan aldığı sesi gerçek zamanlı olarak başka bir frekanstan yayınlamak sureti ile kapsama alanında bulunan diğer amatör telsizcilere iletir.

Neden Amatör Telsizcilik?

Bu kişilere göre cevabı farklılık içeren bir soru olabilir. Bazı kişiler için bu sorunun cevabı afet gibi durumlara bir ön hazırlık olurken, bazıları için sadece bir hobi olabilir. Ancak amaç ne olursa olsun tüm amatör telsizcilerin en önemli buluşma noktası havadır. "Havadan duyuşmak" tabiri de buradan gelir. Amatör telsizci olmanız halinde çevreniz ile bir frekans üzerinden veya tekrarlayıcı istasyonlar (Röle) sayesinde diğer amatörlerle iletişim kurabilirsiniz. Bu yolla sadece dünyamız üzerinde bir noktayla değil yörüngedeki uzay istasyonları ile dahi iletişim kurmanız mümkün.

Amatör telsizcilik sizinle aynı ilgi alanları olan dünyanın bir başka yerindeki radyo amatörleri ile bağlantı kurmanızı sağlayacak deneysel ve sosyal bir hobidir.

Amatör Telsizci Ne Yapar?

Amatör telsizciler elektronik haberleşme kapsamında ve uluslararası bir birlik olan IARU tarafından tahsis edilmiş ve devlet tarafından izin verilen frekans aralığında, satın aldıkları cihazlar veya kendi geliştirdikleri imkanlarla haberleşme sağlarlar.

Bu anlamda amatör telsizciliğin en çekici yanlarından biri herhangi bir taşıyıcı ya da operatör kuruma bağımlı kalmaksızın iletişim kurabilme yetisine sahip olmaktır. Tarihe baktığımızda elektronik ve haberleşme alanında pek çok keşfin adresi yine radyo amatörleridir. Amatör telsizcilik sürekli gelişime açık bir hobi olup kişinin kendini devamlı olarak güncelleme ve öğrendikleri ile bir sonraki adıma geçme amacı içerisinde olduğu, elindeki bilgilerle yetinemediği bir aktivitedir.

Amatör Telsizcilerin
Temel ve Gereçleri Nelerdir?

- **Telsiz alıcı-verici cihazlar.**
- **Mors kullanan alıcı ve verici cihazlar.**
- **Amatör amaçlı dijital ve analog yapılmış her çeşit cihaz.**
- **Amatörlerin kendi imkanları ile imal ettikleri cihazlar.**
- **El yapımı ve hazır üretim antenler.**

AMATÖR TELSİZCİLERE AYRILMIŞ ÖZEL FREKANSLAR VAR MIDIR?

Bu sorunun cevabı kısaca "Evet"tir. Belirli ve sınırlı olan frekans bandını herkes kontrolsüzce yayın yapsaydı telsiz muhaberesinde karışıklıklar meydana gelecek ve örneğin bir ambulans ya da itfaiyenin haberleşmesi engellenebilecekti. Bu tüm amatör telsizciler tarafından uyulması gereken en önemli kurallardan biridir.

Ülkemizde ve dünyada birçok istasyon aralarında muhabere yapmaktadır ve her kurumun kullanacağı frekans aralıkları önceden kanunla belirlenmiştir. Aynı şekilde yalnızca amatör telsizcilere ayrılmış olan HF, VHF, UHF, FM ve SHF olarak adlandırılan bandlarda belirlenmiş frekanslar vardır. Bu frekanslar tüm dünyada kurallar ve uygulamalar çerçevesinde ortak olarak belirlenmiştir.

Amatörlerin; kanunların, yönetmeliklerin ve protokollerin belirlediği özel durumların dışında başka frekans üzerinden haberleşme yapmaları yasak olmakla birlikte kendilerine tanımlı frekansta bile olsalar anlaşılamayacak şekilde şifreli haberleşmeleri aynı şekilde yasaktır.

73 NEDİR?

Amatör telsizcilikte "Selamlar" anlamına gelen bir kısaltmadır. Bu kısaltmanın kaynağı eski telgraf uygulamalarıdır.

DOĞAL AFETLERDE AMATOR TELSİZCİLİĞİN ÖNEMİ NEDİR?

Özellikle doğal afet durumlarında, ilkyardım kadar haberleşme de hayati önem arz etmektedir. Yaşanan deneyimler göstermiştir ki olağanüstü durumlarda mevcut sabit, mobil ve benzeri haberleşme sistemleri gerek yaşanan yoğunluktan gerekse farklı teknik nedenlerde dolayı hizmet veremez duruma gelebilmektedir. Sadece ülkemizde değil tüm dünyada benzer iletişim sorunları yaşanabilmektedir. Benzer olağanüstü durumlarda kamu kurum ve kuruluşları arasında, ayrıca dünya yüzündeki diğer istasyonlarla haberleşmeye en iyi amatör telsizciler aracılık edebilmektedir. Kullanılan tüm sistemler bu gibi durumlarda maksimum seviyede kullanılmakta ve tüm amatör telsizciler bu haberleşmeyi tamamen gönüllü olarak yürütmektedirler.

NE KADAR UZAK MESAFE İLE GÖRÜŞME SAĞLANABİLİR?

Bu amatör telsizciler için sıkça sorulan soruların en başında yer almaktadır. Normal şartlar altında bir el cihazının menzili sınırlıyken, doğru cihazlar ve doğru anten kurulumu ile mesafede sınırlar kalkabilir.

Uzak mesafe haberleşmeleri genellikle HF (Yüksek Frekans-High Frequencies) olarak anılan telsizler ile yapılır. Bu telsizlerin haberleşme şekli geleneksel UHF/VHF telsizlerden farklı olmakla birlikte daha farklı bir telsiz türüdür. HF haberleşmesi "**güneşin hareketlerine**", hava şartlarına, mevsimlere, tüm doğa şartlarına göre değişiklik gösterebilir. Dolayısıyla haberleşme günün saatine ve mevsimlere göre de farklılık gösterir.

AMATÖR TELSİZCİLİĞİN FAYDALARI NELERDİR?

Kanunlar çerçevesinde baktığımızda amatör telsizciler yalnızca kendilerine tahsis edilmiş frekanslarda birbirleri ile haberleşebilmektedir. Özellikle bu konudaki çalışmalarını belirli bir disipline oturtmuş afet haberleşme konusunda çalışma ve hazırlıklar yapan çok önemli derneklerimiz bulunmaktadır. Bunun haricinde ülke tanıtımına katkıda bulunmak ve uzaktaki insanlarla doğrudan haberleşebilmek de bu faydalar arasında sayılabilir.

ÇAĞRI İŞARETİ NEDİR?

Çağrı İşareti, amatör telsiz haberleşmesinin birinci disiplinidir. Örnek olarak bir istasyona seslenirken önce onun çağrı işaretini ardından kendi çağrı işaretinizi söylemeniz gerekir. Amatör telsiz haberleşmesinin başlaması buna bağlı olmakla birlikte çağrı sonlanırken de bu durum karşılıklı tekrarlanır. Çağrı işareti bulunmayan anonslar genellikle dikkate alınmaz. Çağrı işaretleri telsiz belgesi türüne göre, bulunulan bölgeye göre benzer ama kişiye tanımlı son eke göre eşsizdir. Yani bir kişiye tahsil edilen bir çağrı işareti başka bir kişiye asla tahsis edilmez.

Örnek olarak TA1OEA bir çağrı işaretidir. Yalnız bu konuda ülkemizde kendiliğinden yerleşmiş bir algı olmuştur. Normal şartlar altında TA1OEA uluslar arası fonetik alfabeye göre TANGO ALFA ONE OSCAR ECHO ALFA şeklinde telaffuz edilmesi gerekirken TANGO ALFA BİR OSCAR ECHO ALFA şeklinde telaffuz edilmektedir. Yani sadece rakam kısmı ulusal fonetik alfabeye göre anılmaktadır. Ancak yurt dışında biri ile konuşurken uluslararası fonetik alfabeye özen gösterilmemesi durumunda yanlış anlaşılmalara sebep olunabilir.

AMATÖR TELSİZCİLİK ve HALK BANDI AYNI MIDIR?

Bu soruya öncelikle "hayır" diye cevap vermek yerinde olacaktır. Tüm bu teknolojiler telsiz haberleşme teknolojileri olsa da amatör ve halk bandı kesinlikle aynı kullanım dinamikleri-

ne sahip değildir. Halk bandında yalnızca uygun bir cihaz alıp kullanmak mümkünken amatör telsizcilik tarafında belli yönetmelikler, şartlar ve geçilmesi gereken bir sınav ile yalnızca bu akreditasyonu sağlayabilen kişilerin görüşebildiği bir alan söz konusudur.

DÜNYADA TANINMIŞ KİŞİLER ARASINDA AMATÖR TELSİZCİLER VAR MIDIR?

- Yeni Ürdün Kralı Abdullah
- Aktör Marlon BRANDO
- Japonya Başbakanı Keizo OBUCHİ
- Hindistan Başbakanı Rajiv GHANDI
- Arjantin Devlet Başkanı Carlos MENEM,
- Astronot Yuri GAGARİN

NASIL AMATÖR TELSİZCİ OLUNUR?

Amatör telsizci olmak için önce gerekli şartları sağlamak ve bu şartlar sağlanıyorsa Kıyı Emniyeti Genel Müdürlüğü tarafından yapılan sınavlara girmek ve başarılı olmak gerekmektedir. Genellikle sınavlar her yıl Mayıs ve Kasım aylarında yapılmaktadır. İhtiyaç hasıl olması durumunda kurum tarafından belirlenen tarihlerde ve yerlerde de yapılabilir. Amatör Telsizcilik Sınavının yer ve zamanı sınav tarihinden ortalama 30 gün önce Kıyı Emniyeti Genel Müdürlüğü'nün internet sayfasından duyurulmaktadır.

Amatör telsizcilik sınavı için başvuruda bulunacakların on iki yaşından büyük ve temyiz kudretine sahip olması temel şarttır. Reşit olmayanlar Veli/Vasi izni ile sınava girebilirler.

İlk olarak Kıyı Emniyeti Genel Müdürlüğü internet sayfası veya T.C. E-Devlet internet sayfasından başvuru yapılır. Sonra sınav giriş ücretini yatıranlar amatör telsizcilik sınav başvurularını Kıyı Emniyeti Genel Müdürlüğü internet sayfasından elektronik ortamda takip edebilirler.

Başvuruların değerlendirilmesi neticesinde sınava girme hakkı kazanan adaylara sınav giriş belgesi verilir ancak bu belge internet üzerinden doğrudan temin edilebilir. Yapılan sınavdan sonra kazanan adayların listesi Kıyı Emniyeti Genel Müdürlüğü internet sayfasında ilan edilir.

Amatör Telsizciler belge sınıfına göre A, B ve C sınıfı olarak üçe ayrılır.

- A sınıfı belgesi: Özel Telsiz Sistemleri Yönetmeliğinin ekinde yer alan EK-4 Amatör Telsiz istasyonları'nın Tablo-1'inde belirtilen tüm frekans bantlarında, belirlenen güç sınırlarında, izin verilen emisyonları kullanabilme olanağı sağlar,
- B sınıfı belgesi: Özel Telsiz Sistemleri Yönetmeliğinin ekinde yer alan EK-4 Amatör Telsiz istasyonları'nın Tablo-1'inde B sınıfı için belirtilen frekans bantların, belirlenen güç sınırlarında, izin verilen emisyonları kullanabilme olanağı sağlar.
- C sınıfı belgesi: Özel Telsiz Sistemleri Yönetmeliğinin ekinde yer alan EK-4 Amatör Telsiz İstasyonları'nın Tablo-1'inde B sınıfı için belirlenen Spektrumun bir bölümüne düşük güç seviyelerinde kısıtlı erişimi sağlar.

Sınavda A ve B sınıfı için oluşturulan sorulardan en az 75 puan alanlar A sınıfı, 60-74 arası puan alanlar B sınıfı; C sınıfı için oluşturulan sorulardan en az 60 puan alan adaylar C sınıfı amatör telsizcilik belgesi almaya hak kazanırlar.

Sınav çoktan seçmeli olup toplam elli sorudan oluşur ve tek oturumda gerçekleşir. Engelli adaylar için sınav komisyonu gerekli önlemleri alır. Kopya çektiği tespit edilen adayların sınavı geçersiz sayılır. İşletme, Ulusal ve Uluslararası Düzenlemeler ve Teknik olmak üzere üç farklı kategori bulunur. Haberleşme, elektrik, elektronik ve fizik dallarından birinde en az lisans düzeyinde yüksek öğrenim görmüş olan adaylar, teknik konulardan sınava tabi tutulmazlar.

Amatör telsizcilik sınavında başarılı olan ve sınavdan sonra en geç bir yıl içerisinde Kıyı Emniyeti Genel Müdürlüğü internet sayfasında belirtilen evrakları Kıyı Emniyeti Genel Müdürlüğü'ne teslim etmeleri gerekmektedir.

SON SÖZ

Her şeyden önce bir hobi olarak amatör telsizcilik özellikle telsiz ve haberleşme konusuna ilgi duyan herkesin dahil olabileceği ve kendini geliştirebileceği bir aktivitedir. Lisans aldıktan sonra temin edebileceğiniz bir cihaz ile bir süre dinleme yaparak havadan konuşmanın standartlarını görmeniz tavsiye edilir. Sonrasında konuşmaya başladığınızda diğer amatör arkadaşlar size yardımcı olacaktır.

Katkılarından dolayı tüm AMATÖR TELSİZCİLERE ve Sn. Cem DAĞDEMİR'e (TA2MCD) teşekkür ederim.

AMATÖR TELSİZCİKTE EN SIK KULLANILAN Q (DURUM) KODLARI

QRM	Göndermem başka emisyonlarla, yayınlarla karıştırılıyor mu?	Göndermeniz başka emisyon – yayınlarla ..... seviyede karıştırılıyor. 1 Karıştırılmıyor. 2 Az 3 Orta seviyede 4 Güçlü 5 Çok güçlü
QRT	Göndermeyi durdurayım mı?	Göndermeyi durdurunuz.
QRX	Beni yeniden ne zaman çağıracaksınız? * Tekrar ne zaman haberleşme yapacağız.	..... (saat) de ..... KHz (MHz)'den yeniden çağrı yapacağım.
QSL	Alındığını onaylar mısınız? (İşaretlerin alındığının veya haberleşmenin tümünün işaretle veya yazılı tasdiki ya da teyidi.)	Alındığını onaylıyorum.
QTH	Enlem ve boylam derecelerine (ya da belli bir coğrafi noktaya göre) bulunduğunuz yer neresidir? * İstasyonunuzun bulunduğu yer veya ikamet ettiğiniz yerin adı nedir?	Bulunduğum yer ..... enlem ..... boylam derecesidir. (Belli bir coğrafi noktaya göre ..... dayız.) *İstasyonumun bulunduğu yer veya ikamet ettiğim yer ..... dir.

ULUSAL VE ULUSLARARASI FONETİK ALFABE

(Bunu aynı isimde Google'da bulabilirsiniz. Evrensel bir şeydir. Tablo olarak ekleyebilirsiniz)

HARF	ULUSLARARASI	TÜRKÇE
A	Alfa	Ankara
B	Bravo	Bursa
C	Charlie	Ceyhan
Ç	---	Çankırı
D	Delta	Denizli
E	Echo	Edirne
F	Foxtrot	Fatsa
G	Golf	Giresun
H	Hotel	Hopa
I	India	Isparta
İ	---	İzmir
J	Juliet	Jale
K	Kilo	Kayseri
L	Lima	Lüleburgaz
M	Mike	Manisa
N	November	Nazilli
O	Oscar	Ordu
Ö	---	Ödemiş
P	Papa	Pazar
Q	Quebec	---
R	Romeo	Rize
S	Sierra	Samsun
Ş	---	Şarköy
T	Tango	Trabzon
U	Uniform	Urfa
Ü	---	Ünye
V	Victor	Van
W	Whiskey	---
X	X ray	---
Y	Yankee	Yalova
Z	Zulu	Zonguldak

RAKAM	ULUSLARARASI
0	Nada Zero
1	Una One
2	Bisso Two
3	Terra Three
4	Karte Four
5	Panta Five
6	Soxi Six
7	Sette Seven
8	Okto Eight
9	Nove Nine

Android Cihazınız için Güvenlik Rehberi

Android işletim sistemi Google tarafından desteklenen; cep telefonlarından, televizyonlara, tabletlere kadar pek çok farklı cihazda kullanılan bir işletim sistemidir.

Aşağıdaki talimatlar kullandığınız cihazın tipine göre değişiklik gösterebilir.

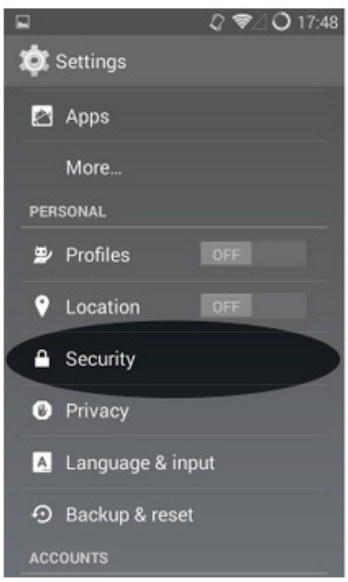
Google'ın topladığı verileri en aza indirin

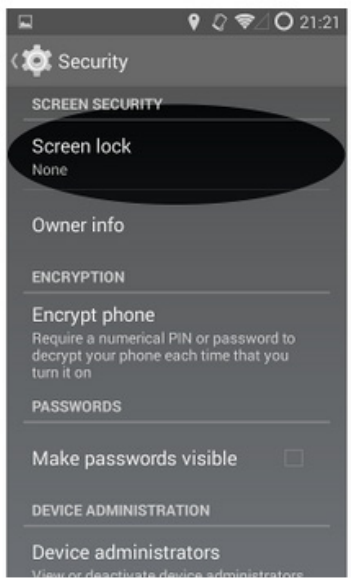
Pek çok Android cihazda, Google hesabınız ile oturum açmak zorunda değilsiniz. Kurulumda karşınıza çıkacak bu seçeneği atlayabilmek mümkün. Fakat bu bazı servisleri kısıtlı kullanmanıza neden olabilir. Ayrıca **https://myactivity.google.com/myactivity** bağlantısı üzerinden Google aktivite profilinizi düzenleyebilir, hangi verilerin saklanacağını belirleyebilir ya da etkinlik verilerinizi silebilirsiniz.

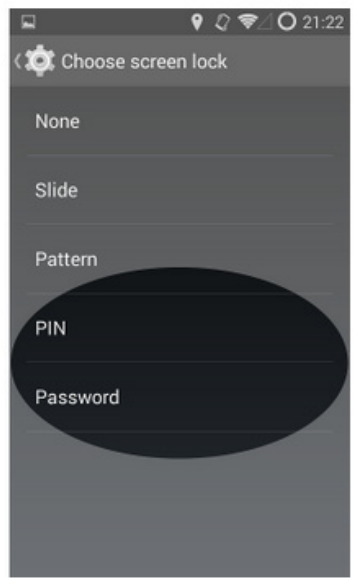
Cihazınıza bir PIN set edin.

Cihazınızı korumak için bir PIN ya da bir alfanumerik parola belirleyin.

PIN / Parola set etmek için: Settings > Security > Screen lock



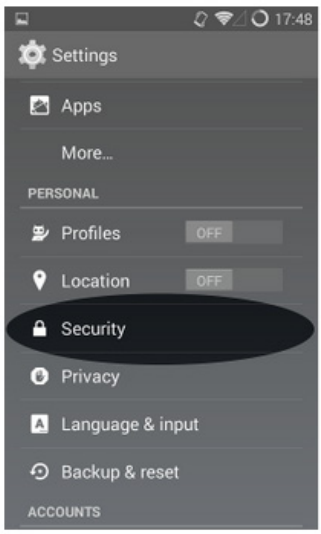


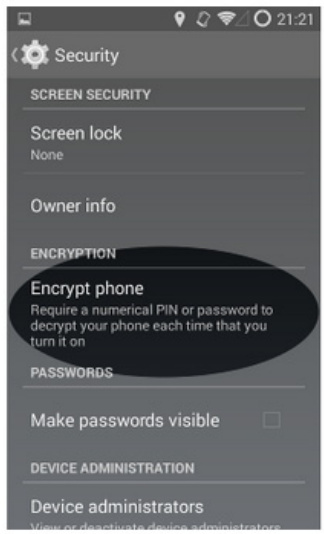


Verilerinizi Korumak için Cihazınızı Şifreleyin

PIN / Parola'dan farklı olarak bu seçenek ile cihazınızın içerisindeki dataları şifreleyebilirsiniz. Bunun için öncelikle PIN ya da parolayı etkinleştirmeniz ve her açılışta bu bilgiyi girmeniz gerekmektedir. Şifreleme işlemi yoğun enerji harcadığından cihazı şarja bağlamanız önerilir.

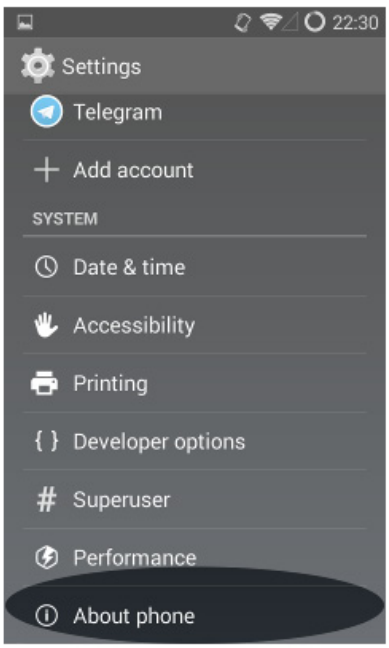
Not: Şifrelemeden sonra olası PIN / Parola unutursanız verilerinizi deşifre etmeniz mümkün olmayacaktır. Bu durumda fabrika ayarlarına dönme seçeneğini kullanabilirsiniz ancak bu da tüm datalarınızın silinmesine yol açacaktır. Cihazınızı şifrelemek için *Settings* > *Security* > *Encrypt phone/tablet* menülerini kullanabilirsiniz.

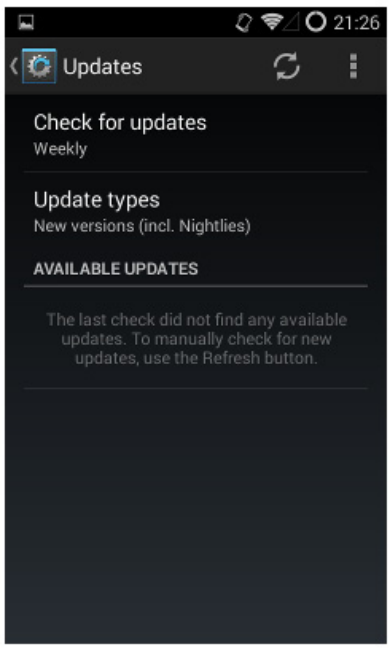




Cihazınızı ve programlarınızı güncel tutun

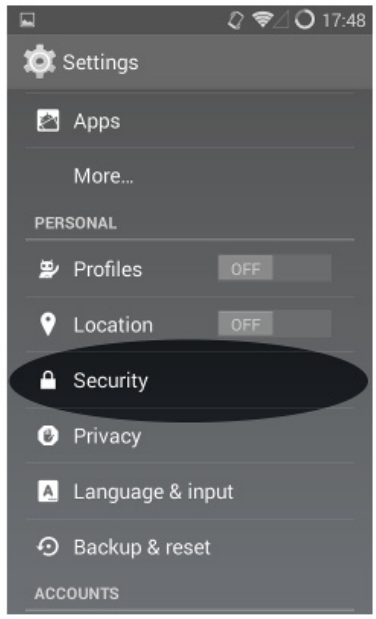
Sadece Android değil, tüm cihazlarınız için gerek cihazın işletim sistemini gerek kullandığınız programları güncel tutmanızı öneririz. Cihaz güncellemesi için: Settings > About phone/tablet > System Update menü seçeneklerini kullanabilirsiniz.

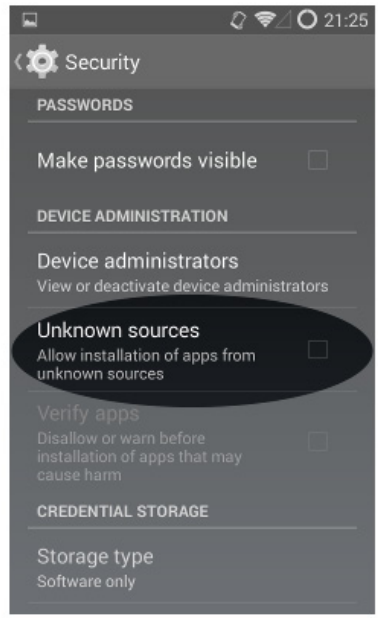




Güvenilir Olmayan Kaynaklardan Uygulama İndirmeyin

Güvenilir olmayan, bilinmeyen kaynaklardan uygulama indirmeyin. Telefonunuzu yalnız güvenilir kaynaklardan indirme yapacak şekilde ayarlayabilirsiniz. Bunun için *Settings* > *Security* > *Unknown sources* menü seçeneklerinden bilinmeyen kaynaklardan yükleme yapılmaması engellemek için seçeneği devre dışı bırakın.

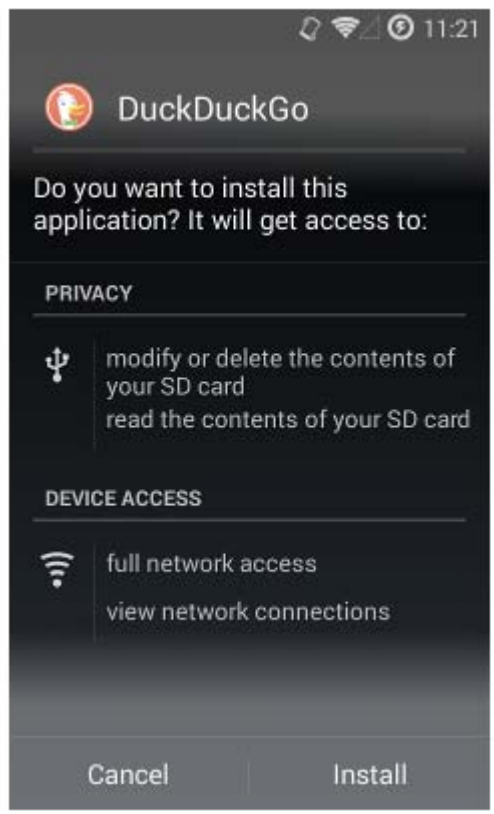


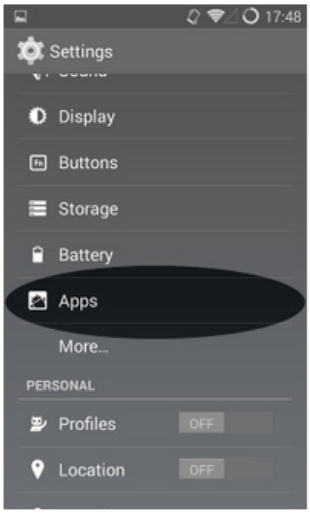


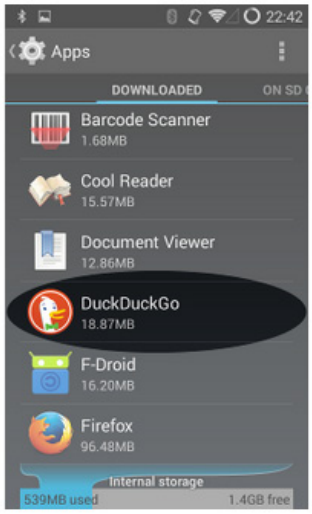
Uygulama Yetkilerini Mutlaka Gözden Geçirin

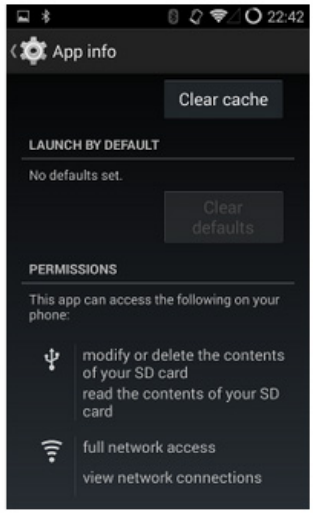
Uygulama yüklerken uygulamanın talep ettiği yetkileri mutlaka gözden geçirin. Uygulama amacı dışında bir yetki talep ediyor mu? Örneğin uygulamanın ana faaliyeti ile alakalı olmadığı halde, mikrofon, kamera, hoparlör ya da diğer sensörlere erişim talep ediyor mu?

Sadece yeni uygulamalar için değil, hâlihazırda yüklü uygulamaların da izinlerini kontrol edin. Aşırı, gereğinden fazla yetki verilmiş bir uygulama varsa nedenini sorgulayın, gerekirse cihazınızdan kaldırın. Bazı uygulamalar güncelleme esnasında yeni yetkiler talep etmiş olabilir, bazı yetkiler gözünüzden kaçmış olabilir ya da artık kullanmadığınız bir uygulama olabilir. Belki de hâlihazırda kullandığınız bir uygulamayı, aynı işi yapan fakat daha az yetki gereksinen başka bir uygulama ile değiştirmek isteyebilirsiniz:



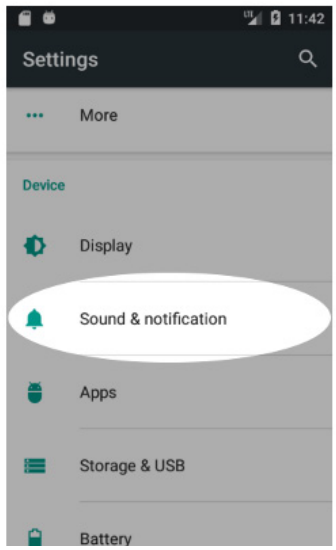


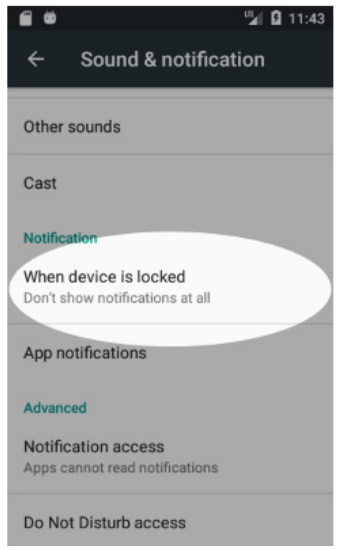




Hangi verilerin bulutta yedekleneceğini belirleyin, gözden geçirin

Uygulamaları senkronize etmemek, bulut sunucularına örneğin Google Drive'a gönderilen verileri sınırlar. Örneğin WhatsApp uygulaması varsayılan olarak yazışmaları, üstelik kendisi uçtan uça şifreleme kullanan bir uygulama olmasına rağmen, şifrelenmemiş bir halde Google Drive'da yedeklemektedir. Bu ve benzeri senkronizasyon ayarlarını gözden geçirin. Bu işlem için *Settings > Accounts section > [app name]* menülerini kullanabilirsiniz.





Özel bildirimleri gizleyin!

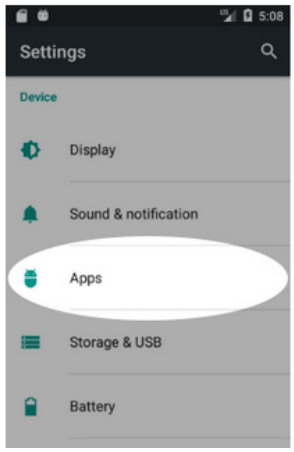
Telefonunuz kilitli fakat gelen bir mesaj ile ilgili bildirim kiminle yazıştığınızı ele mi veriyor? PIN aktif olmasına rağmen sizi arayan kişinin bilgisi ekranda mı gözüküyor? Öyle ise cihazınızın bildirim ayarlarınızı gözden geçirme vakti. Kilitli ekranlarda bildirimlerin gözükmesini engelleyebilirsiniz. (Sadece yeni versiyonlarda geçerli.)

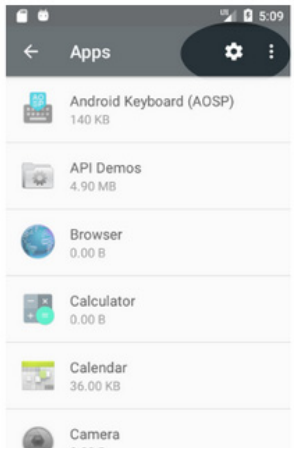
Settings > Sound & notifications

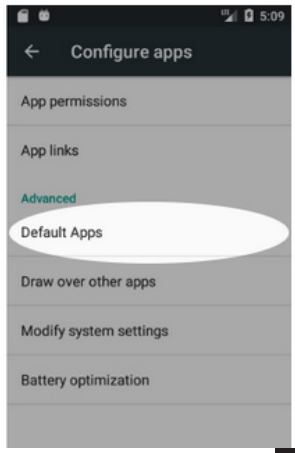
Cihazınızın varsayılan uygulamalarını gözden geçirin

Cihazınız text mesajı göndermek için varsayılan olarak hangi uygulamayı kullanıyor? Ya da bir linke tıkladığınız zaman web sitesi varsayılan olarak hangi tarayıcıda görüntülenecek? Bu ve benzeri varsayılan program ayarlarını gözden geçirin. Varsayılan uygulamaları, güvenli uygulamalar ile değiştirebilirsiniz.

Settings > Apps > ⚙ icon > Default

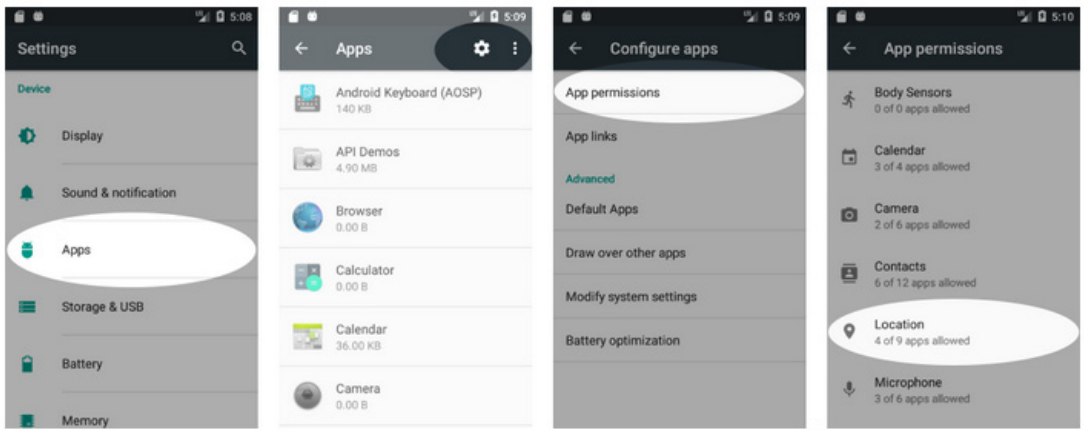






Konum bilginizi uygulamalar ile paylaşmayın!
Hangi uygulamanın konum bilginize erişebileceğini kontrol edin / ayarlayın.

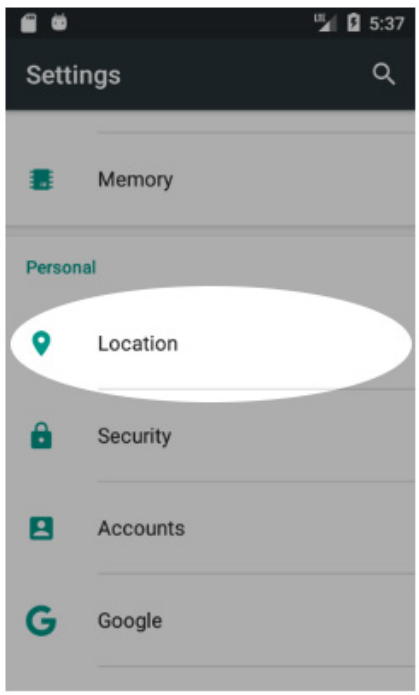
Settings > Apps > ⚙ icon > App permissions > Location

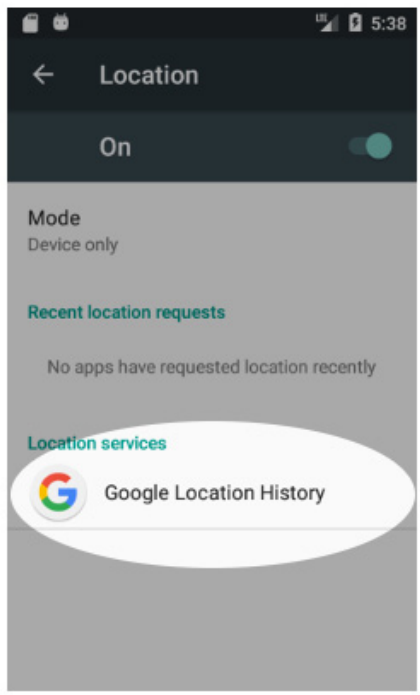


Konum bilginizi Google ile paylaşmayın!

Yukarıdaki adımda uygulamaların lokasyon bilgimize erişip erişmeyeceğini belirlemiş idik. Bu uygulamalara / servislere Google da dahil. Washington Üniversitesi tarafından yapılan ADINT araştırması, yaklaşık bin dolarlık bir bütçe ile, mobil reklamları kullanarak nasıl kişilerin adım adım izlenebileceğini ortaya koyuyor[1]. Uygulamaların lokasyon bilginize erişmesini engelleyerek buna engel olabilirsiniz. Aşağıdaki menü seçenekleri ile uygulamaların konum bilginize ulaşıp ulaşmadığını kontrol edebilirsiniz:

Settings > Location > Google Location History





1 https://adint.cs.washington.edu/

Cihazınıza Custom bir Android Versiyonu Yükleyebilirsiniz

CyanoGenmod temelli LineageOS vb bir Android versiyonunu cihazınıza yükleyebilirsiniz. Bu işlem için teknik bilgi gerekmektedir. Cihazınızın garanti kapsamı dışında kalabileceğini unutmayın.

Cihazınıza custom bir Android versiyonu yüklemeden önce, bazı cihazların yönetici (root) yetkilerine sahip olması gerekmektedir.

Bu yetkileri almak için yapılan işlemler sonrasında, bu yetkiler geri devredilmelidir! Eğer cihazınız yönetici modunda ise, bu cihaza izinsiz erişebilen bireyler, cihazınız üzerinde yetkisiz işlemler yapabilir hatta cihazınızın kontrolünü tamamen ele geçirebilir!

Bu nedenle, eğer bilinçli ve bir amaç doğrultusunda açık bırakmadıysanız yetkili modunu kapalı tutmaya özen gösteriniz. Yetkili modunu uygulama marketinde bulunan Rootchecker ve benzeri uygulamalar ile sorgulayabilirsiniz.

Varsayılan arama motoru olarak DuckDuckgo ya da Startpage'i kullanabilirsiniz.

Arama geçmişinizi tutmayan, gizliliğinize önem veren DuckDuckgo ya da Startpage gibi arama motorlarını varsayılan arama motoru olarak kullanabilirsiniz.

MAID (Mobile Advertising ID)'yi resetleyin

MAID, browserlardaki cookie benzeri, cihaza özel olarak atanan ve reklam izlemelerinde kullanılan bir değerdir. Mobil reklamcılıkta reklamlar MAID ile hedeflenebilir. Örneğin şu MAID'e sahip kişi görsün şeklinde reklamlar ayarlanabilir. Bu reklam görüntülenme bilgisi, tarih, saat ve lokasyon bilgisi ile korele edilip yeriniz tespit edilebilir. Adım adım izlenebilirsiniz.

Google Settings > Ads > Reset advertising ID'yi tıklayarak MAID değerini sıfırlayın.

Not: DuckDuckGo'nun yayınladığı Android Privacy Tips blog yazısından istifade edilmiştir.

Kaynak: https://spreadprivacy.com/android-privacy-tips/

Mustafa Akgül Anısına

Türkiye'de **internetin başlaması, yayılması** ve internet kültürünün gelişmesinde büyük katkısı olan, Doç. Dr. Mustafa Akgül, geçtiğimiz ay tedavi gördüğü hastanede, 69 yaşında hayata gözlerini yumdu. İlk Türkçe internet kitabının da yazarı olan Akgül'ü, saygıyla anarak biraz daha yakından tanıyalım.

Ülkemizde "İlk internet" bağlantısının kurulmasından, düzenlediği birçok etkinlik, eğitim, seminer ve konferansın yanı sıra, yayımladığı yazılar ve e-posta listeleriyle Türkiye'de internet ve teknoloji kültürüne paha biçilmez bir katkıda bulunmuştur. İlk Türkçe internet kitabını (İnternet: Bilgiye Erişimin Yeni Araç ve Olanakları'nı) yazmıştır. İşte bu katkılarından dolayı, ülkemizde, "**İnternet'in Babası!**" olarak anılır ki hiç şüphesiz, bu övgüyü fazlasıyla hak etmiştir!

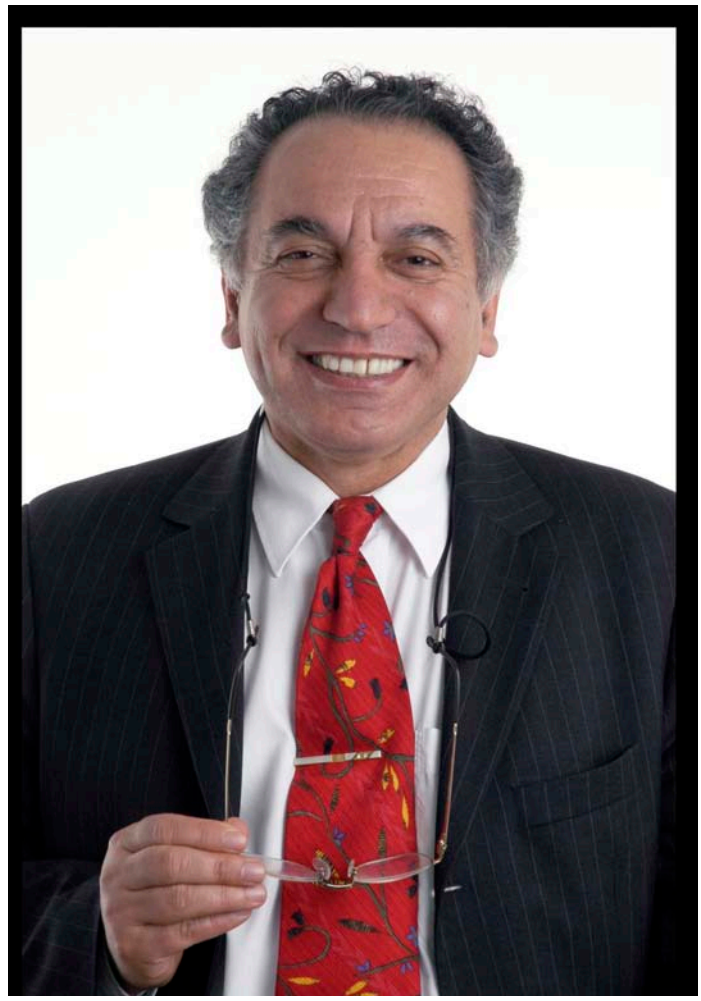
İnternetin Babası!

Akgül, GNU/Linux ve Özgür Yazılım Topluluğunun oluşmasında da öncülük etmiştir. Linux Kullanıcıları Derneği'nin kurucu başkanlığını yapmıştır. Durdurak bilmeksizin çalışmalarına devam eden Mustafa Akgül, İnternet Teknolojileri Derneği'nin başkanlığını, İnternet Kurulu, Kamunet Teknik Kurulu, TOBB Sektör Kurulu, Türkiye Bilişim Derneği Yönetim Kurulu üyeliği görevlerinde bulunmuştur. Dahası, 20 yılı aşkın bir süredir devam eden İnternet Konferansları, Akademik Bilişim Konferansları ve İnternet Haftası etkinliklerinin koordinatörü olmuştur.

Eğitim Hayatı

ODTÜ İnşaat Mühendisliği / 1970, ODTÜ Matematik/Yöneylem / 1974 mezunu olan Mustafa AKGÜL, 1981 yılında Waterloo University'de (Kanada) "Combinatorics and Optimization" üzerine doktora derecesini almıştır.

University of Delaware ve North Carolina State University'de misafir öğretim üyesi olarak görev yapmış ve 1987'den beri Bilkent Üniversitesi'nde öğretim üyesi olarak çalışmıştır.



Saygıyla Anıyoruz!

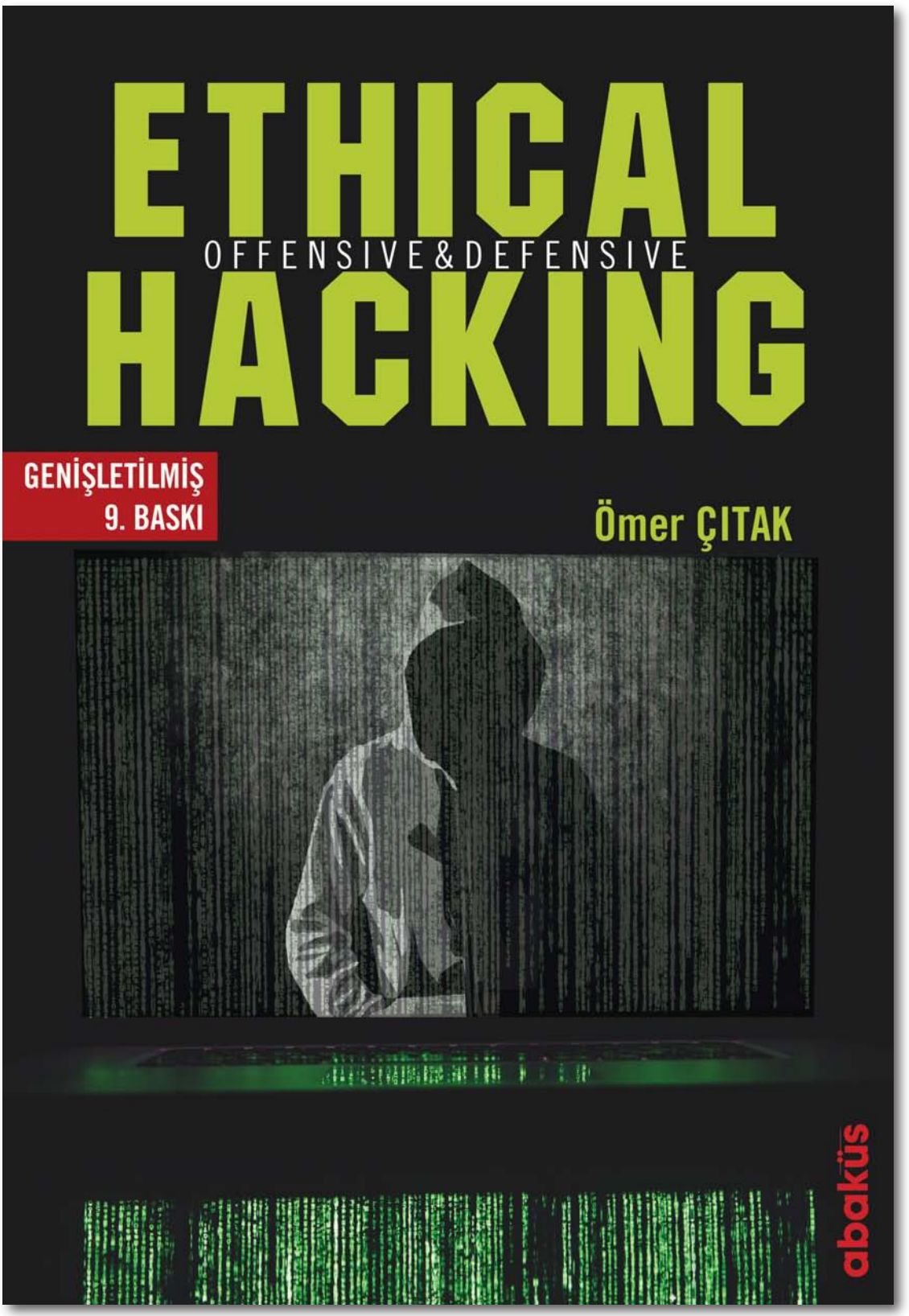
Ülkemizde internetin gelişmesi, iletişimin özgürleşmesi, özgür yazılım felsefesinin ve bilgi teknolojilerinin tüm ülkeye yaygınlaştırılması çalışmalarında her zaman en önde yer alan, Mustafa Akgül hocamızı kaybetmenin derin üzüntüsü içerisindeyiz ve onu saygıyla anıyoruz.

Başta ailesi olmak üzere, öğrencilerine, çalışma arkadaşlarına ve tüm sevenlerine başsağlığı diliyor, acılarını paylaşıyoruz.

Biliyoruz ki "Mustafa Akgül" adı, Türkiye İnterneti ile birlikte sonsuza kadar yaşayacak! Son olarak eklemek isteriz ki kıymetli hocamız, Mustafa Akgül'ün, internette sansüre karşı verdiği mücadelenin de sonuna kadar destekçisiyiz.

Saygı ve rahmetle...

GENİŞLETİLMİŞ 9. BASKI TÜM KİTAPÇILARDA



abaküs