

~ BU KİTABI ÇALIN ~

Bu Kitabı Çalın

Ocak 2014



İçindekiler

Teşekkür.....	4
Giriş.....	5
1. EXIF ve GPS.....	6
2. Sosyal Medyada Açık Hesaplar.....	13
3. Ünlü Olmak.....	17
4. Budala Son Kullanıcı.....	18
5. Twitter'ın Karanlık Yüzü.....	20
6. PGP Kullanın.....	23
7. Google Hesabı Silmek.....	31
8. Big Brother = Usta.....	36
9. Kimyasal Silah Kullanımı ve Amerika.....	39
10. Arka Kapı.....	44
11. AKP, Baskı ve Polis Devleti.....	47
12. Online Kripto Araçları.....	50
13. CV Rekabetçiliği.....	53
14. SteamOS'un Düşündürdükleri.....	56
15. Tor ve Günümüz İnterneti.....	60
16. SSL, Man In The Middle ve Turktrust.....	63
17. Tor'a Giriş.....	71
18. DNS Leak Tehlikesi.....	83
19. Ccrypt İle Şifreleme.....	92
20. Şifreler, Şifreler ve Şifreler.....	97
21. Kızılı Erkekli Gizlilik Hakkı.....	107
22. Büyük Birader'le Mücadele Etmek.....	113
23. Veriyi Unutmak ve Unutulma Hakkı.....	120
24. Casus Yazılım ve Teknoloji Kültürsüzlüğü.....	125
25. Anonim Hesapların Korunması.....	131
26. Çalışanın İzlenmesi ve İş Yerinde Gizlilik Hakkı.....	135
27. Girift Haklar.....	141
28. Arch Linux'u USB Belleğe Kurmak.....	145
İletişim.....	156

Teşekkür

Bana bugüne kadar karşılıksız destek veren herkese sonsuz teşekkürlerimi sunarım. Sizler olmadan ben daima eksik kalacağım.

Giriş

Elinizde bulunan bu kitap, Kame'nin ilk senesini içermektedir. 2013 yılı Ağustos - Aralık aylarında blogda yazılmış tüm yazıları elimden geldiği şekilde aktarmaya çalıştım. Eğer yazılarda eksiklik farkederseniz şimdiden özür dilerim.

Bu kitapta toplam 28 yazı bulunmaktadır. Yazılar içerik itibariyle Internette gizlilik ve güvenlik, gizlilik hakkı, unutulma hakkı, kriptografi, çalışan gizliliği, iş yerinde gizlilik, sosyal medya ve siyasi eleştirilerden oluşmaktadır.

Dikkat edeceğiniz üzere bolca atıflarda bulundum ve bunları dipnot olarak gösterdim. Bu bağlantıların ilerleyen zaman içerisinde kırılması, erişilememesi gibi durumlar olabilir. Bu konuda beni bilgilendirirseniz memnun olurum. Ayrıca, belirli haber sitelerinin sayıca bağlantı fazlası olması benim herhangi bir ideolojiye yakın olduğum fikri vermesin.

Son olarak, kitapla ilgili görüşlerinizi lütfen bildirmekten çekinmeyin. Kitap, Attribution-NonCommercial-ShareAlike 4.0 International License altındadır ve içeriğini kopyalama, değiştirme ve kullanma özgürlüğüne sahiptir. Bunun için referans vermenize gerek yoktur. Fakat, yazıları kesinlikle kâr getirecek herhangi bir ticari amaç için kullanamaz ve teklif dahi edemezsiniz.

1. EXIF ve GPS

Her şeyden önce söylemek istediğim birkaç şey var. Öncelikle, bu ve bundan sonraki yazıların herhangi birini tatmin etmek gibi bir amacı yok. Yazılar amatörce, bolca eksik bulacaksınız, her türlü eleştiriye açık ve eksikler doğrultusunda güncellenecek. O yüzden yorumlarda ne ekerseniz onu biçersiniz.

Telefonum çok akıllı...

Hayatınızda birçok şeyi kolaylaştıran “**akıllı telefonlar**”, medyadaki dezenformasyonu engelleyebilecek mükemmel bir “araç” haline dönüşürken diğer yandan da sizin gizliliğinizi ve güvenliğinizi tehlikeye sokabilecek bir başka araca (*silaha*) da dönüşebiliyor. Peki bu telefonlar akıllı ama kimin için akıllı? Bu telefonlarla çekilmiş fotoğraflarla sizler insanlara “**gerçeği**” anlatmaya çalışırken EXIF ve GPS madalyonun diğer yüzü, buz dağının görünmeyen kısmı ve gizliliğinize doğrultmuş bir silah. Yazıyı daha iyi anlayabilmeniz için Firefox’un Exif Viewer eklentisini kurabilirsiniz. Kullanımı gayet basit, sağ tık menünüze de yerleşecektir. Basit olması açısından örnek üzerinde anlatırken bunu tercih edeceğim.

Acele işe...

Mazur görülebilecek bir davranış, o anın getirdiği korku, heyecan, gerilim vs. ile aceleci davranmak, elindeki görüntüleri hemen, en kolay yoldan paylaşmak. Siz bu telefonların yardımıyla basitçe o anı kaydebiliyorsunuz ve sizin için akıllı bir araç haline dönüşüyor. Diğer yandan telefonun kamera ayarlarını kontrol etmediniz, GPS açık, arka planda bir sürü servis çalışıyor. Peki siz bu durumda kendinizi büyük bir tehlike içine de sokmuş olmuyor

musunuz? Bana gönderilen bir Gezi fotoğrafı üzerinden gidelim:



Fotoğrafın üzerine tıklayıp gerçek boyutunda açtığınız zaman

(ön izlemede EXIF yok!) sağ tıklayıp View Image EXIF Data dediğinizde aşağıdaki görüntü ile karşılaşacaksınız:

Exif Viewer
Please select your image and set the desired options, then click on the "Display EXIF Data" button.

Local File:

Remote URL:

Basic information only
 Display Maker Note (if available)
 Suppress image display
 Use tables rather than lists
 Display EXIF tag ID

http://network23.org/kame/files/2013/08/gps-1.jpg

• Embedded thumbnail image:



EXIF Interoperability IFD

- Interoperability Index = R98
- Interoperability Version = 0100

EXIF GPS IFD

- GPS Version ID = 0x02,0x02,0x00,0x00
- GPS Latitude Reference = north latitude (N)
- GPS Latitude = 41/1,1/1,5619/100 [degrees, minutes, seconds] ==> 41° 1' 56.19" == 41.032275°
- GPS Longitude Reference = east longitude (E)
- GPS Longitude = 28/1,58/1,3497/100 [degrees, minutes, seconds] ==> 28° 58' 34.97" == 28.976381°
- Links to online mapping websites:
 - [Google™ Maps](#)
 - [Yahoo!® Maps](#)
 - [Bing® Maps](#)
 - [Mapquest®](#)

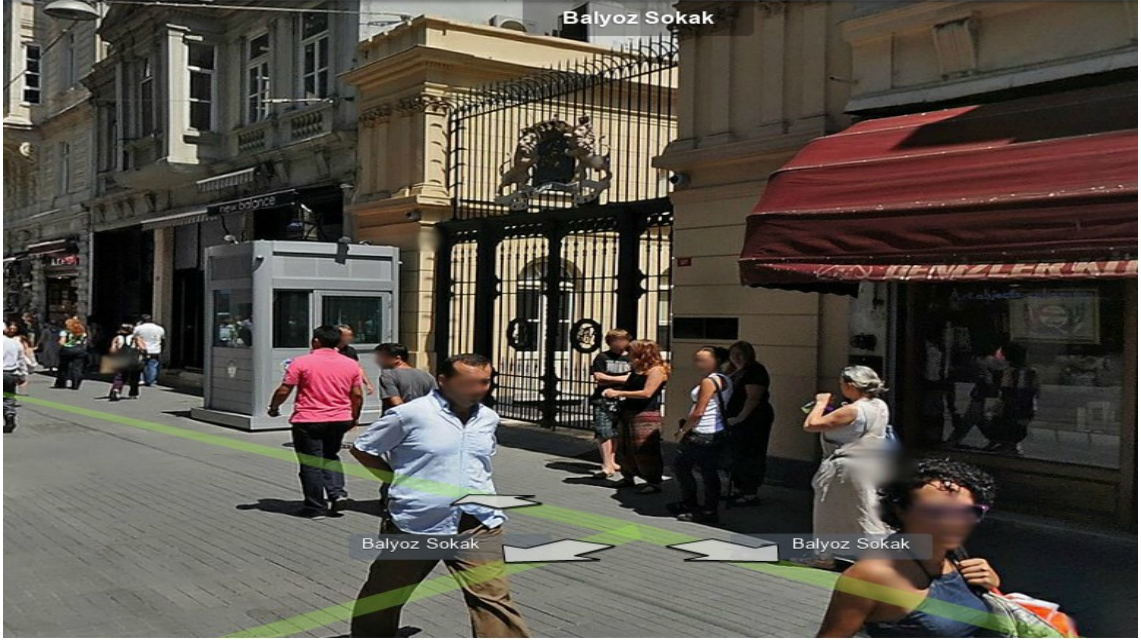
Karşınızda akıllı telefonunuz ve marifeti. Fotoğrafa konum bilgileriniz girilmiş! Enleminiz 41.032275 ve boylamınız 28.976381. Tabi siz bunun farkında değildiniz, çünkü içinde bulunduğunuz durum buna müsait değildi. Küçük bir hata, telefonun modelinden,

çekildięe yere kadar her Őeyi ieren bir bilgiye sahip. Bir de enlem ve boylam bilgilerinize haritadan ([Google](#)) bakalım:



Bir insan “**bakin ben buradayım**” diye ne kadar baęrabilir, cevabı bu kck ayrıntıda gizli. Hayatınızı kolaylařtıran bu akıllı telefon artık bařka insanların iřini de kolaylařtıracak.

İstanbul’u hi bilmeyen biri olarak panoramadan ([Yandex](#)) tam konumunuza bakalım:



Burayı bulabilmek benim birkaç dakikamı aldı. Fotoğrafın konumla ilgili görsel olarak pek fazla bir şey içermemesine rağmen GPS bilgileri üzerinden %100 olarak yeri basit bir Internet kullanıcısı tarafından bile tespit edilebiliyor. Elinizde ise bir harita, varsa panorama ve EXIF bilgilerini görebileceğiniz basit bir eklenti.

Korkuyorum...

Fotoğrafları farkında olmadan bu şekilde çekseniz bile daha sonra yüklerken fotoğrafların EXIF bilgilerini açık kaynak, özgür bir yazılım olan Gimp (*Windows, Linux, Mac OS sürümleri mevcut*) ile silebilirsiniz. Tek yapmanız gereken farklı kaydederken EXIF ve XMP verilerini seçmemek. Bu arada ben de bahaneyle sizlere Gimp kullandırmış oluyorum.

Komplo teorisi kuralım...

Kafanızda bir şeyler canlandırmak adına; düşünün ki imaj yüklediğiniz bir servis var ve EXIF bilgilerini silmiyor, mahkeme

kararı ile (*hiçbir zaman kullanıcı sözleşmesini okumadığınız için farkında değilsiniz*) anında T.C. devletine de verebilecek. Ben de bu tarz gösterilere katılmış insanlar hakkında bilgi toplamaya ve onları “**fişlemeye**” çalışan biriyim. Gezi ile ilgili araştırma yaparken bir şekilde bu servisi buluyor ve sizin hesabınıza ve yüklediğiniz fotoğraflara ulaşıyorum (*fotoğraflar ziyaretçiler tarafından görülebiliyor diyelim*). Bir yanda Gezi fotoğraflarınız, diğer yanda evde kediniz ile çektiğiniz Caturday fotoğrafları. Hepsinin ortak noktası ise gözünüzden kaçan bu konum bilgisi. Sonucu sizin için “**akıllı**” telefon bir kabus olurken ben yüce devletim ve gizli servisim adına bu akıllı telefondan faydalanıp büyük bir başarı elde etmiş oluyorum. Yani bu telefon artık benim için “**akıllı**”.

Ama birçok imaj paylaşım sitesi EXIF bilgilerini siliyor/blokluyor...

Kullanıcılar veya ziyaretçiler için geçerli bir durum. Ama orjinal fotoğrafı ya da fotoğrafın sahip olduğu EXIF bilgilerini ne yaptığını kimse bilmiyor. Bir örnekle anlatalım; Facebook’un Instagram’ı satın almasını¹ geçtim, kendisi Amazon servisleri ve sunucuları kullanıyor². Amazon ise CIA ile 600 milyon \$’lık kontrat imzalamış olduğu ortaya çıktı³ ve artık sunucuları konusunda birçok aktivisti rahatsız etmekte. Buna örnek olarak joindiaspora.com’un⁴ imajlar için Amazon’u kullanması⁵ kullanıcıların bazılarını diğer POD’lara kaçırdı. Ucuz bir komplo teorisi gibi bakmaktansa Instagram’ı tercih etmemeyi bu çerçevede kabul etmek daha mantıklı. Bu tarz servisleri en azından bu tarz fotoğraflar için kullanmamak hayatınızdan hiçbir şey

1 <http://mashable.com/2012/04/09/facebook-instagram-buy/>

2 <http://instagram-engineering.tumblr.com/post/13649370142/what-powers-instagram-hundreds-of-instances-dozens-of>

3 <http://www.information-management.com/news/be-the-cloud-making-the-case-for-copying-amazon-and-the-cia-10024744-1.html>

4 <https://joindiaspora.com/>

5 <https://joindiaspora.com/posts/2945881>

götürmeyecektir.

Sonuç...

Bu tarz durumlar insanın başına her zaman gelebilir. Önemli olan böyle bir tehlikenin farkında olabilmek. Telefonların kamera için konum ayarı kapatılabilir, yüklemeye önce fotoğrafların EXIF bilgileri silinebilir, en önemlisi aceleci davranmadan, önlemini baştan alarak, İnternet'te bulunan her servise güvenmeden, sağlam adımlar atıp ne yaptığının bilincinde olmak. Yoksa, Instagram vs. kullanmanız veya gözü kapalı bu tarz servisleri, API'sini savunmanız kimsenin umrunda değil. Çünkü kendi düşen ağlamaz.

2. Sosyal Medyada Açık Hesaplar

Yazının temel amacı sosyal medyayı bir korkuluk gibi göstermek değil. Sadece sosyal medyadaki açık hesapların içeriğinin çok basit bir şekilde birileri tarafından cachelenmesi, arama motorları ile bu sayfalara rahatça erişilebilmesi, ve siz sosyal medya hesaplarını kapatsanız dahi bu sitelerde verilerinizin kalması.

Sosyal medyanın çok hızlı gelişimiyle beraber aynı hızda sosyal medya ajanslarının gelir arttırma yolları da gelişti. Örneğin, sosyal medya üzerindeki açık hesapları bir havuza aktaran monitoring sitelerinin, girdileri inceleyerek firmalara ürünleri hakkında insanların ne düşündüğü üzerine bilgi satması. Bir nevi +, - ve nötr olarak girdileri tasnif edip ayrıntılı rapor hazırlamak. Bazı siteler de arama ile site üzerine gelen ziyaretçilerden gelir kazanmak derdinde. Yani sizin girdilerinizi cacheleyerek kendi sitesine koyuyor, böylece arama yapıldığında sonuç olarak bu site de çıkıyor. Bu bir nevi veri madenciliğidir ve en kötüsü ise açık hesapların bu şekilde sömürülmesini engelleyecek yasal bir kısıtlama yok. Örnekler üzerinden devam edelim.

Twitter için birkaç örnek (*test etmek için kendi kullanıcı adınızla bakabilirsiniz*):

- Twtrland: <http://twtrland.com>
- Twicsy: <http://twicsy.com>
- Topsy: <http://topsy.com>
- Favstar: <http://favstar.fm>

- Loviv: <http://loviv.com>

Twitter'daki tweetlerinizden paylaştığınız fotoğraflara ve hatta video'lara kadar her şey bu "**arama**" siteleri tarafından cachelemiş durumda ve hepsi de sizin insiyatifiniz dışında gerçekleşti. Çünkü kurallar buna müsaade ediyor, bu sitelerin açık hesaba sahip olduğunuz için size sormak ya da izin istemek gibi bir dertleri yok. Diyelim ki Twitter hesabınızı sildiniz, bu siteleri bilmiyordunuz ve bazıları sizden profilinizin silinmesi için Twitter hesabınızla giriş yapmanızı istedi, alın size bir dert daha!

Hesabınız açıktı fakat sonradan kapattınız (*korumaya aldınız*), Twitter diyor ki; profilinizi kapatsanız bile bir zamanlar açık profile gönderdiğiniz tweetler hala açık ve aranabilir. Sadece profili kapattıktan sonra gönderdiğiniz tweetleriniz kapalı olacaktır. Bir diğer deyişle, açık hesaba gönderdiğiniz tweetler bu siteler tarafından cachelemişse, hesabı kapatsanız bile sadece hesabı kapattıktan sonraki tweetleriniz cachelemeyecek.

G+ için benzerlik açısından birkaç örnek (*yoksa bir sürü site var*):

- GooglePlusDirectory: <http://googleplusfriends.com>
- PlusArkadaşArama: <http://www.plusarkadasarama.com>
- Psd2wp: <http://gplus.psd2wp.pl>
- Google-plus: <http://google-plus.pl>

Farkettiğiniz gibi bu G+ arama sitelerin hepsi aynı yazılıma sahipler. Domainlere whois çekebilir, sunucuları nerede veya kim

bunlar araştırabilirsiniz. Belki aynı kişi, kuruluş veya herneyse onundur ya da bu yazılım herkesin serbestçe indirip istediği gibi kullanılabildiği bir şeydir. Yani, birileri açık sosyal medya hesaplarını ve içeriğini “**arama**” adı altında öyle ya da böyle istediği gibi kendi veritabanına aktarabiliyor, cacheleyebiliyor. Peki herkes böyle basit bir yazılımla bile açık hesapları bu kadar ayrıntılı cacheleyebilirken, devletler, gizli servisler kim bilir neler yapıyordur değil mi?

Hesabımı kapattım ama...

Açık hesabınızı kapattınız/sildiniz diyelim. Fakat bu sitelerin farkında değildiniz ve rastgele adınızla ilgili bir arama yaptığınızda bugüne kadar gönderdiğiniz tweetlerden, G+ girdilerine her şey tekrar karşınıza çıktı. Hem de çok basit bir arama ile! Kabus sizin için yeniden başlıyor. Bu sefer de sitelerin iletişim sayfalarından profilinizin kaldırılması talebinde bulundunuz. Bu sitelerin birçoğunun e-postasının çalışmadığını, bazılarının yaptıkları şeyin herhangi bir yasal ihlal içermediğini anlatan otomatik cevap gönderdiğini, çok azı da silinmesi için gerekçe istediğini göreceksiniz.

Açık hesap mı kapalı (korunan) hesap mı?

Açık hesabın daha çok kişiye ulaşması kapalı hesapla kıyaslanmaz bile. Fakat sosyal medya sitelerinin politikaları böyle şeylere izin verdiğinden dolayı, ileride özellikle kendi adı ve soyadıyla yazanlar için büyük bir risk teşkil edecektir. Twitter veya G+ (*diğer micro blogging siteleri vs.*) üzerinde yazdığınız bir şey bir sürü farklı site tarafından cacheleniyor, herhangi bir arama sayesinde de bunlara rahatça ulaşılabilir. Kapalı hesaplar bu konuda güvenli, ama paylaştığınız bir bilginin açık hesap gibi yayılma olasılığı da bir o

kadar düşük. Burada ısrarla üzerinde durmak istediğim şey siz hesapları kapatsanız bile ileride yazdıklarınızın durup dururken başınıza iş açabilme olasılığı. Ne yapmalıyım diyorsanız, hafif paranoyak olarak diyebileceğim şey kendi adınız ve soyadınızla açık hesap kullanmayın. Kimse sizin gerçek kimliğinizi Internet üzerinde bilmek zorunda değil, açıkçası kimsenin (*bazıları hariç*) bunu merak ettiği de yok. Yeterki siz paylaştığınız şeylerin güvenilebilir olduğunu en azından belirli bir oranda sağlayın.

Son olarak, sosyal medya ajanslarının bazıları için diyebileceğim tek bir şey var; **“...yüzde 300 kâr ile, sahibini astırma olasılığı bile olsa, işlemeyeceği cinayet, atılmayacağı tehlike yoktur.”**

3. Ünlü Olmak

Hiç adını bile duymadığım biri saçma sapan bir televizyon programına çıkıyor ve diyor ki; **“mp3 indirenler tespit edilmeli ve cezalandırılmalı. devletimiz bu konuda lütfen gereğini yapsın.”** Sonra devam ediyor; **“bizim cemiyet...”**

Kendilerini sıradan bir insandan farklı gören sıradan bir insanın karşılığı ünlü olabilir. Çoğul olunca bu kelime, kendilerini farklı gören sıradan insanlar, yani ünlüler şeklinde devam ettirilebilir. Bu cemiyet -kendileri öyle diyor- matah özelliklerinin süslenip püslenip insanlara her türlü iletişim aracıyla dikte edilmesi ile bir konum kazanmışlardır. Yani senden benden farklı, üreten, vergisini veren, devletine ve milletine faydalı bu muhterem zatlar, elde ettikleri bu **“ünlü konumu”** ile toplumun tepesinde bir yerlerde, Maslow piramitinin ucuna oturmuşlardır. Girdikleri ünlü halet-i ruhiyesi ise nerden geldiği belli olmayan ve **“sıradan insanlara”** dayatılan konumları ile **“farklılık”**, diğerlerini **“ötekileştirme”** ve **“dokunulmazlık”** şekline bürünmektedir.

Özellike magazin kısmı kendi konumlarındaki çıkmazın ve hatta ünlü kelimesinin adeta bir sembolü/karşılığıdır. Kendileri hem üst-beni yaratıp hem de magazine karşı olduklarında ise genel tepkileri **“biz de normal vatandaş gibi dışarıda hareket edemeyecek miyiz?”** noktasındadır. Evet, edemeyeceksiniz. Çünkü kendinizi metalaştırıp **“birey”** yerine **“ünlü”** olmaktan, her zaman yürüdüğünüz yolları normal bir vatandaşla paylaştığınız için **“dışarı”** yapmaktan ve size sağlayacağı konumdan vazgeçemeyeceğiniz için asla normal bir vatandaş ol-a-mayacaksınız.

4. Budala Son Kullanıcı

Sevgili dostum Ahmet, blogunda [İnternet Notları] İnternetin de Özel Hayatın da Sonu Gelmedi⁶ başlıklı bir yazı yayımlamış. Ahmet'in de affına sığınarak yazıya ufak tefek eleştiriler getirmek isterim.

Bazı insanların tabiri caizse “**budala**” olduğunu herkes söyleyebilir. Aslında buna tüm insanlar budaladır desek daha doğru olacak. Ben de budalayım, sen de budalasın, o da budala. Bunu şöyle örneklendireyim, bir şeye küçüktür diyorsanız; onun başka bir şeyden küçük ama aynı şekilde başka bir şeyden de büyük olduğunu söylüyorsunuz. Bir şeyi ne kadar iyi bildiğinizi düşünürseniz düşünün, muhakkak bir hata yapıyorsunuz. Burada sıkıntı kullanıcının herhangi bir servisin hesabına sahip olup her şeyi ondan beklemesinden de kaynaklanıyor. Bir diğer deyişle de sermaye olsun, bazı geliştiriciler olsun, bazı yazarlar olsun, bazı “**budalalar**” olsun, sürekli bir ürünün kolay kullanıma sahip olması için o kadar çok yaygara kopardılar ki ve insanları o kadar çok rahata alıştırdılar ki, artık sermaye, güvenlik konusunda da kullanıcıların “**budala**” olmasını beklemeye başladı. Kimse kullanıcıda çok basit bir bilgi düzeyinden başka bir şey istemiyor. O yüzden reklamlar “**tek tıkla işinizi halledin**” noktasına kaydı. Bu ayrıca bir pazarlama yöntemidir. Sermaye, hedef pazarını seçerken öncelikle bu rahata alıştırmış ve kendini üreticiye emanet etmiş kullanıcıları seçiyor ve onlardan da istediği gibi faydalanabiliyor. Kim ne derse desin, bu rahatlık, kolay kullanım herkesin işine geliyor.

6 <http://ahmetasabanci.com/internet-notlari-internetin-de-ozel-hayatin-da-sonu-gelmedi/>

Hepimiz budala olduğumuza göre bunun sorumlusu bir anlamda da bizleriz. Steam, GNU/Linux'a gelirken -ben de dahil- heyecanlanmış ve desteklemiştim (*alın size bir hata*). Peşinden DRM'yi oyunlarla sokmaya başladı⁷, Stallman'ın deyimiyle bir sürü kapalı kaynak kodu açık kaynak bir sisteme soktu. Şimdi birileri çıkıp **“o zaman kullanma kardeşim, seçim senin”** diyebilir. Seçim benim ama bu sadece benim bilgisayar kullanmayı bilip bilmememle alakalı değil. Başında düştüğüm bir hata var. Karşımda art niyetli bir sermaye var. Onu da geçtim bunu destekleyen bir sürü ileri düzey kullanıcı da var. Bu, ayrıca, sermayenin kullanıcılara zoraki bir dayatmasıdır.

Duckduckgo mu Duckduckdon't mu?⁸ Startpage⁹ daha bir alternatif olarak gözüküyor ve Avrupa lokasyonlu. Amerikan mahkemelerinin kapsama alanı dışında. Madem bir seçim yapacağız, o zaman neden Startpage değil? Başka biri de neden YaCy¹⁰ değil diyebilir. Tor¹¹, %100 güvenli değil. Bazı Exit nodlarından veri örnekleri toplayan servisler var. Bu dediklerim güvensizler anlamına gelmesin. Peki bunların sizin iyi bir bilgisayar kullanıcısı olmanız veya olmamanızla ilişkisi var mı? Sermaye, istediği gibi hareket ettiği sürece, siz sadece belirli bir oranda kendinizi koruyabilirsiniz. Yazının hedef kitlesi budala son kullanıcının **“gizliliğimiz elden gidiyor vay vay”** diye ağlaması ve insanları ümitsizliğe itmesi olabilir. Unutulmamalı ki teknoloji de tek bir tarafa hizmet etmiyor. Siz ne kadar gizlilik ve güvenlik üzerine kendinizi geliştirirseniz geliştirin, sermaye de onu bertaraf etmek için elinden geleni yapacaktır.

7 <https://www.gnu.org/philosophy/nonfree-games.html>

8 <http://www.alexanderhanff.com/duckduckgone>

9 <http://startpage.com/>

10 <http://yacy.net/>

11 <https://torproject.org/>

5. Twitter'ın Karanlık Yüzü

PRISM konusu patladıktan sonra Twitter nasıl oluyor da bu kadar temiz ve dokunulmamış kalabilir hep şüpheli yaklaşmıştım. Bu hizmetin elbet bir karanlık yüzü olmalıydı. Aradan geçen süre içerisinde bilin bakalım ne oldu?

Polonyalı bir aktivist olan Alexander Hanff¹² kendi gizlilik temelli projelerini yayımlamak için bir site hazırlarken ziyaretçi istatistikleri üzerine Apache'nin GeoIP modülünü kullanmak istiyor. Bu konudaki temel düşüncesi ziyaretçilerin IP bilgilerini -daha doğrusu gizliliklerini ihlal etmeden- kaydetmeden onlar hakkında ülke ve IP bilgisi almaya çalışıyor. Ne oluyorsa da tam bu noktada oluyor. Birden fazla Twitter hesabı olduğu için (*kendi diyor*) birinden kendi hesabına Tweetdeck¹³ üzerinden bir DM (*özel mesaj*) atıyor;

<http://mydomain.com/stats.php?ref=twitter>

ref dizisinin amacını veri tabanına kaydedilmek üzere test amaçlı kullandığını çünkü sponsorlarıyla ilişkili bazı kayıtları geri yüklemek istemesi olduğunu belirtiyor. Şöyle bir sonuçla karşılaşılıyor;

8 » 2013-08-25 19:44:07 » stats.php?ref=twitter » US

9 » 2013-08-25 19:44:07 » stats.php?ref=twitter » US

10 » 2013-08-25 19:44:07 » stats.php?ref=twitter » US

11 » 2013-08-25 19:44:14 » stats.php?ref=twitter » PL

¹² <http://alexanderhanff.com/>

¹³ <http://tweetdeck.com/>

12 » 2013-08-25 19:44:14 » stats.php?ref=twitter » US

13 » 2013-08-25 19:45:06 » stats.php?ref=twitter » PL

Sonuç beklendiği gibi pek gizliliğe zarar verici gibi gözükmemekte. Fakat 8, 9, 10 ve 12. satırlara bakarsanız ülke kodunun Amerika olduğunu göreceksiniz. Özellikle 8 ve 10 özel mesaj gönderildikten hemen sonra oluşmuş. İşin ilginç bu bir özel mesaj ve URL'sinin gizli olması, yani teorik olarak "US" girdilerine sahip olmaması gerektiği. Hanff, Apache'nin erişim kayıtlarına baktığı zaman US satırlarında Twitter'ın kendisini Twitterbot/1.0 olarak tanıtmak ve URL'ye GET isteği göndermek için 199.16.156.126 IP'sini kullandığını görüyor. Bunun bir özel mesaj olduğu düşünülecek olursa Twitter'ın aslında bunu görmemesi ve kendine GET isteği üzerinden bir kopya oluşturmaması gerekmektedir.

Buna kısaca Twitter'ın özel mesajları taraması demek daha doğru olacaktır. Bu açık bir gizlilik ihlalidir. Twitter bu konuda iyi niyetli olduklarını, kullanıcıyı düşündüklerini söylese de GET ve kopya oluşturması niyetleri ile tamamen çelişmektedir. Yazının tamamını buradan¹⁴ okuyabilirsiniz.

Twitter'la ilgili başka bir haber¹⁵ de Glendale okul yetkilileri Hermosa Beach adlı bir sosyal medya şirketi ile anlaşarak öğrencilerinin Twitter, Facebook, Youtube ve Instagram paylaşımlarını takip ettirdiği ortaya çıktı. Günlük raporlar, öğrencilerin şiddet, nefret, saldırganlık vs. üzerine olan eğilim frekanslarından oluşuyor. Geçen sene Hermosa Beach şirketine

14 <http://www.alexanderhanff.com/twitter-surveillance>

15 <http://www.glendalenewspress.com/news/tn-gnp-me-monitoring-20130824,0,4640365.story>

40,500\$ ödenmiş, toplam 13,000 orta ve lise öğrencisi monitörlenmiş. Okul yetkililerinin “**niyeti**” ise öğrencilerinin kendilerine ve başkalarına zarar vermeden önceden tespit edilebilmesiymiş. İnsanın aklına Minority Report¹⁶ gelmiyor değil. Tabii öğrencilerin hesaplarının nasıl tespit edildiği ise başka bir konu. Monitörlene kadar bu hesapların tespitinin nasıl yapıldığı da bilinmeli ve paylaşılmaya değer olduğunu düşünüyorum.

Görüldüğü üzere, bazı sosyal medya şirketleri zaten çok uzun bir süredir monitörlene işini yapmaktaydılar. Bunlar firmalar için ürün, marka değerlendirmeleri içerirken bazıları da Glendale okulu gibi “**öğrencilerinin iyiliği**” altında paylaşımlarının incelenmesini içermekte. Her ne olursa olsun, yapılan paylaşımların birilerinin süzgeçinden geçtiği ve bunların sadece iyi niyetli olmadıklarıdır. Twitter, T.C. devleti ile kullanıcı bilgisi paylaşımına yanaşmamış olabilir¹⁷, belki hiç yanaşmayacak da olabilir ama dikkat edilmesi gereken şey gizliliğiniz ve güvenliğiniz için özel şirketlere bel bağlamamanız gerekliliğidir. Gizlilik bir insan hakkıdır. Bunun seçimi, bu hakkın birilerine devredilmesi söz konusu bile olamaz.

16 <http://www.imdb.com/title/tt0181689/>

17 <http://www.hurriyet.com.tr/teknoloji/23545191.asp>

6. PGP Kullanım

Bir uygulamayı nasıl kullanabileceğinize dair rehberler hazırlanırken, hazırlayan kişi -kaçınsa da- kendisi nasıl kullanıyorsa öyle anlatır. Bu bir hata değildir, bunda yanlış bir şey yoktur. Az bildiği anlamına da gelmez. Aynı şekilde alışkanlıklarının dışına çıkması onu anlatacağı şeyde hata yapmaya da götürebilir.

Böyle bir giriş yaptıktan sonra PGP üzerine hazırlanan bu rehberin, yazan kişinin kullanım çerçevesinde ilerleyeceği için “**eksik**” olduğu düşünülen noktalar aslında bilerek boş bırakılmıştır. Adım adım ilerleyecek olursak:

- PGP, e-posta ve dosyaların güvenliği için bir kriptolama ve doğrulama (*matematiksel kısmı için aramaya inanın*) aracıdır. Sizlere gönderdiğiniz dosyanın ya da e-postanın şifrelenmesini ve başkaları tarafından okunmamasını (*ya da sadece gönderdiğiniz kişi tarafından okunabilmesini*), gönderen kişinin kimliğini doğrulamayı ve gönderilen dosya ya da e-postanın yapısının bozulmadan size ulaşmasını (*ya da bozulup bozulmadığını anlamanızı*) sağlar.
- Kullandığınız e-posta sağlayıcı ne kadar güvenli olursa olsun e-posta mahremiyeti artık ayaklar altına alındığı için gönderdiğiniz e-postaları bu yöntemle göndermeniz güvenliğinizi kat kat arttıracak, e-posta içeriğiniz üçüncü şahıslar tarafından okunamayacaktır.
- PGP anahtarları oluşturmak için açık kaynak veya ticari yazılımlar mevcuttur. GNU/Linux kullanan biri olarak sadece GPG; GnuPrivacyGuard ve Terminal üzerinden gideceğim. O yüzden açık bir terminaliniz olursa hemen başlayabilirsiniz.

Çünkü her şeyi onun üzerinde yapacağız. “#” komut, “>” ise terminal çıktısıdır.

Dağıtımınızın ne olduğunu bilmediğim ve bilemeyeceğim için paket yöneticinizden gnupg'nin kurulu olup olmadığına bir bakın. Eğer kurulu değilse kurun. Her şeyin artık hazır olduğunu varsayarak;

```
# gpg --gen-key
> Please select what kind of key you want:
> (1) RSA and RSA (default)
> (2) DSA and Elgamal
> (3) DSA (sign only)
> (4) RSA (sign only)
```

Burada sizlere ne tür bir kriptolama yöntemi kullandığınızı soruluyor. Varsayılan olan 1'i seçip (*1 ve enter*) yolumuza devam ediyoruz.

```
> RSA keys may be between 1024 and 4096 bits long.
> What keysize do you want? (2048)
```

Anahtarınız ne kadar güçlü olacak burada belirleyeceğiz. En büyük olanı iyidir diyoruz. 4096 yazın ve devam edin.


```

> Please specify how long the key should be valid.
> 0 = key does not expire
> = key expires in n days
> w = key expires in n weeks
> m = key expires in n months
> y = key expires in n years
> Key is valid for? (0)

```

Burada anahtarınızın ömrünü biçeceğiz. Bir nevi son kullanım tarihi. Sınırsız olmasını pek tavsiye etmiyorum. 3-5 gün sonra dolması da bana mantıklı gelen bir şey değil (*eğer paylaşmayacaksanız*). İdeal olarak 1-2 sene seçilebilir. 1y ya da 2y yazarak devam edebilirsiniz.

```

> GnuPG needs to construct a user ID to identify your key.
> Real name:
> Email address:
> Comment:
> Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit?

```

Adınız veyahut takma adınız, kullanacağınız e-posta adresiniz, anahtarla ilgili -varsa- yorumunuz (*bu daha çok neden kullandığınızı, ne işi yaradığı ile ilgili olabilir*), son olarak O yazarak devam ediyoruz. Karşınıza şifre belirlemeniz için bir pencere açılacak. Buraya büyük, küçük harf, rakam ve işaretler kullanarak en az 10 karakterlik bir şifre yazıyorsunuz. İleride unutmayacağınız fakat

güçlü bir şifre yazmanız sizin yararınıza olacaktır.

Anahtarın oluşturulabilmesi için rastgele bytes'a ihtiyaç olacak. Bu yüzden film açın, tarayıcınızda sitelere girin, metin editörüne bir şeyler yazın. Anahtarın oluşması biraz zaman alacaktır. Oluştuğunda ise:

```
> gpg: key ***** marked as ultimately trusted  
> public and secret key created and signed
```

Şeklinde bir çıktı alacaksınız. ***** (*rakam ve harflerden oluşan 8 hane*) sizin anahtarınızın ID'si olmaktadır. Bu ID ayrıca 40 hanelik fingerprint'in son 8 hanesidir.

Sıra geldi oluşturduğumuz anahtarımızı nasıl kullanabilir, paylaşabiliriz, yedekleyebilir ve silebiliriz kısmına. Diyelim ki elinizde önemli bir dosya var ve kimsenin açık kurcalamasını istemiyorsunuz:

```
# gpg -e ***** dosya.txt
```

Dosyanızın kriptolanmış hali olan dosya..txt.gpg'nin oluştuğunu göreceksiniz. Açmak isterseniz:

```
# gpg -d dosya.txt.gpg  
# gpg --output dosya.txt --decrypt dosya.txt.gpg
```

Anahtarınızı paylaşmanın iki yolu var. Biri anahtarınızı dışa aktarıp (*ASCII-armored*) göndermek, bir diğeri de anahtar sunucularına yollamak. ASCII-armored için:

```
# gpg --output anahtarım.asc --export -a *****
```

Böyle e-postanız üzerinden anahtarım.asc'yi arkadaşlarınıza gönderebilirsiniz. Herhangi bir sunucuya göndermek için:

```
# gpg --send-key *****
```

Böylece arkadaşlarınız paylaştığınız anahtarınızı kullanarak sizlere kriptolanmış e-posta veya dosya gönderebilecekler. Şimdi size gönderilen bir anahtarı nasıl aktarabileceğinize bakalım:

```
# gpg --import arkadaşımınanahtarı.asc
```

Arkadaşınız eğer anahtarını sunuculardan birine göndermiş ve siz sadece ID'sini biliyorsanız:

```
# gpg --recv-key *****
```

Size gönderilen bir anahtarı doğrulamak isterseniz muhakkak fingerprint'ini karşılaştırın.

```
# gpg --fingerprint *****
```

Aynı şekilde anahtarınızı imzalamanız da anahtarı kullanan kişilere anahtarın sahibi olduğunuzu söyler.

```
# gpg --sign-key *****
```

Çok önemli bir adım olarak anahtarınızı nasıl yedeklersiniz? Öncelikle anahtar(larınızı) listelemek için:

```
# gpg --list-keys
```

Açık anahtarınız; pub 4096R/ ve gizli anahtarınız; sub 4096R/ 'den sonraki 8 karakterlik kısımdır. Açık anahtarınızı yedeklemek için;

```
# gpg -ao açikanaharım.key --export *****
```

Gizli anahtarınızı yedeklemek için;

```
# gpg -ao gizlianahtarım.key --export-secret-keys *****
```

Silirse geri yüklemek için;

```
# gpg --import açikanahtarım.key
```

```
# gpg --import gizlianahtarım.key
```

Bu yedekleri usb diskinizde saklayabilir, cd'ye yazdırabilirsiniz. Önemli olan bunları kaybetmemek. Bununla birlikte, anahtarı iptal etmek (*revoke*) bilmemiz gereken başka bir şeydir. Bir anahtar neden iptal edilire gelirse (*bu bilginiz olsun kısmı*):

- Şifrenizi unutmuşsunuzdur ve hatırlama ihtimaliniz yoktur.
- Anahtarınızı kaybetmişsinizdir ve geri yükleyemiyorsunuzdur.
- Birileri tarafından kullandığınız şifre bulunmuştur.

Her türlü kötü durumları bu konuda kafanızda canlandırabilirsiniz. Ama temel olarak bu üç neden kafanızın bir yerinde bulunsun. İptal edilmiş bir anahtar ile karşılaştığınızda hatırlarsınız.

Revoke anahtarı oluşturmak için:

```
# gpg --gen-revoke *****
```

Anahtarı aktarmak için:

```
# gpg --import revoke.asc
```

Eğer anahtarı bir sunucuya göndermişseniz revoke edilmiş anahtarı tekrar göndermeniz o anahtarın iptal edildiğini gösterecektir.

Son olarak, oluşturduğunuz anahtarı ve sahip olduğunuz anahtarları silmek isterseniz:

```
# gpg --delete-secret-key *****  
# gpg --delete-key 'arkadaşım@epostası'
```

O kadar uğraştık, bir e-posta göndereceğim ama nasıl diyorsanız, diyelim ki göndereceğiniz kişinin anahtarı sizde mevcut ve bir metin editörü ile (*ben vim kullanıyorum bana bakmayın*) e-postada anlatmak istediklerinizi yazdınız;

```
# gpg -e -r 'ArkadaşımınanahtarIDsi' eposta.txt
```

Eklentiye eposta.txt.gpg'yi koyun ve gönderin. Arkadaşınız yukarıda bahsettiğimiz şekilde e-posta.pgp.txt'yi açacak ve e-postayı okuyacaktır. Ben biraz eski kafalı olduğum için bu şekilde yapıyorum. Kullandığınız e-posta istemcisi (*Thunderbird, Claws vs*) ya da web tabanlı e-posta istemciniz bunu otomatik yapıyor olabilir. Onu sizin keşfetmeniz gerekecek.

Tekrar tekrar söylemeye gerek yok ama ben gene söyleyeyim. Kullandığınız e-posta servisi ne kadar güvenilir olduğunu iddaa ederse etsin, siz PGP kullanın!

7. Google Hesabı Silmek

Uzun zamandır Google ile ilgili bir yazı yazıp, açık açık suç işlediklerini duyurmak niyetindeyim. Benim ağırdan almam ve PRISM konusunun derinlik kazanmasından sonra Google bazı şeyleri değiştirmiş ve anlatmak istediğim şeyin en büyük kısmını geçersiz kılmış. Bu, sonuç olarak, hem iyi hem de kötü.

Güncelleme (30.10.2013): Google, gizlilik ve güvenlik ilkelerini değiştirerek, silinen hesabın artık tamamen silinmesini sağlamaktadır.

Google'da hesabı silseniz dahi Gmail ve diğer Google servisleri (*Blogger, Analytics vd.*) arkaplanda kalmakta, özellikle Gmail, hesap silinse de e-posta alıp, kopyalarını saklamaktaydı. Değişikliğin iyi yanı şu; en azından artık hesap silindikten sonra Gmail e-posta alma işlevini yitiriyor. Kötü yanı ise, biz öyle olduğunu biliyoruz ve diğer servisler (*Gmail için eğer gelen, spam vd. kutularda daha önceden kalan e-postalar varsa onlar da duruyor*) verileriyle birlikte durmaya devam ediyor. Peki, bir şeyi "silmekten" anladığımız nedir? "**Silmek**" bizlere ne ifade ediyor?

Sözlük anlamına (TDK¹⁸) bakarsak, "**ortadan kaldırmak, yok etmek, ilişkisini koparmak veya gidermek**" şeklinde sonuçlara ulaşabiliriz. İngilizce-ingilizce anlamına buradan bakabilirsiniz. Sonuç (*make invisible dışında*) pek de farklı değil. Başından beri anlamıyla ilgili beklentilerimiz de bu yöndeydi. Google örneğimize kelime anlamları üzerinden geri dönelim. Google hesabını sildiğiniz

18 <http://tdk.gov.tr/>

zaman hesabınız ortadan kalkmıyor. Çünkü, hesabınızı istediğiniz zaman kurtarabiliyorsunuz.

Ekran görüntüsünde de görüldüğü gibi eğer telefon bilgileriniz Google hesabınızla ilişkilendirilmişse, basit bir SMS yolu ile “**silmiş**” olduğunuz Google hesabını geri alabiliyorsunuz. Yani, hesabınız ne “**ortadan kalkmış**” ne de “**yok olmuş**”. Hesabınız kurtarıldıktan sonra “**Ürünler**” bölümüne girerek eğer daha önce Google ürünlerine sahipseniz bunların aynen durduklarını göreceksiniz.

The screenshot shows the Google account settings page (Hesaplar) in Turkish. The page is titled "Hesaplar" and features a navigation menu on the left with options: Hesap, Güvenlik, and Ürünler. The main content area is titled "Ürünleriniz" and displays a grid of Google products and services, including Analytics, Blogger, Gmail, Google Arkadaşı Bağlantısı, Google Grupları, Google Sizin Dilinizde, Hesap Özeti, Picasa Web Albümleri, Reader, Takvim, Talk, and Web Yöneticisi Araçları. A "Hesap Özeti" (Account Summary) section on the right provides information about the data stored in the account and offers a button to "Hesap Özeti'nde oturum aç" (Log in to Account Summary). Below the product grid, there is a note: "Şundan hoşlanabileceğinizi düşündük:" (We thought you might like this:).

Ekran görüntüsünün hesap silinmeden önce alınmış olabileceğini düşünen olursa, lütfen hesabını silsin ve geri kurtarsın. Bir diğer kelime anlamımıza geri dönecek olursak, Google hesabımızla ilişkili ürünlerin (*görüldüğü üzere Analytics, Blogger, Gmail vd.*) aynen durduğunu, hatta verilerinin de silinmediğini yani **"ilişkinin kopmadığını"** ve devam ettiğini görmekteyiz. Kelime anlamı olarak silmek, Google için hiçbir şey ifade etmemekte. Bir tek **"make invisible"** buna uymaktadır o kadar. Bir diğer deyişle, Google hesabınızı gizliyor.

Benim düşünceme göre (*de¹⁹*), kullanıcı hesabını silmek istiyorsa ve kullandığı ürün neyse **"hesabını sil"** seçeneği koyuyorsa, hesabı tamamen silinmeli. Bunun dolambaçlı yollara girmesine, çeşitli nedenlerle suistimal edilmesine göz yumulmamalı. Google hesap ve veri silme konusunda açık ve net olarak kullanıcılarını yanlış yönlendirmektedir. Google'ın kendini nasıl savunabileceğine

19 <https://twitter.com/alexanderhanff/status/373442725372100608>

bakacak olursak²⁰:

- Kazara silinir ya da geri kurtarmak isterseniz diye verilerinizi tutuyoruz/saklıyoruz/bir süre sonra siliyoruz.
- Hesabı silseniz dahi en fazla 6 ila 24 boyunca verileri yasal olarak saklayabiliriz²¹.
- Sunulan hizmetin daha da geliştirilebilmesi için veriler anonim olarak tutulmaktadır.

Bir süre sonra silmeye örnek olarak Gmail'de tamamen sildiğini sandığınız bir e-posta Google sunucularından 60 gün sonra silinmektedir²² ve 1. cevabımız ile tamamen örtüşmektedir. İsterseniz 2. cevap ile bunu da ilişkilendirebilirsiniz ve yasal olarak buna kimse itiraz edemez. Tracking²³ kısmı üçüncü cevap ile örtüşmektedir. Google, tüm bunları istediği gibi uydurabilir, kamuyu istedikleri doğrultuda fakat "**yasalardan sapmadan**" yönlendirebilir. Fakat tüm bunları yaparken kullanıcılarını da yanlış yönlendirmeye devam etmektedir.

Verilerin ve gizliliğin korunması adına, hesap silindikten sonra hesapla ilişkili verilerin de ortadan kalkması gerekmektedir. Verilerin unutulması (*Right to be forgotten*²⁴) şirketlerin kabul etmesi ve derhal uygulamaya koyması gereken bir zorunluluk olmalıdır. Google gibi devasa şirketler bile böyle kıvrırken küçük şirketlerin pastadan pay alabilmek için veri ve gizlilik haklarını nasıl suistimal

20 <https://www.google.com/policies/privacy/>

21 https://en.wikipedia.org/wiki/Data_Retention_Directive

22 <http://www.smartplanet.com/blog/thinking-tech/does-8220delete-forever-8221-in-gmail-really-mean-it/2149>

23 https://en.wikipedia.org/wiki/Criticism_of_Google

24 https://en.wikipedia.org/wiki/Do_Not_Track_Policy#Right_to_be_forgotten_.28EUropean_Union.29

edebileceđini düşünmek korku verici.

8. Big Brother = Usta

Hepinizin, George Orwell'in 1984 eserini okuduğunu varsayarak "**Oligarşik Kollektivizm Kuramı Ve Uygulaması**"ndan karışık bir alıntı yapacağım. Okumadıysanız da sorun etmeyin, bunu okuyun, sonra gidin kitabı okuyun. Bugünleri "**okumak**" adına epey bir yardımcı olması ve yeni fikirleri sizlerde tekrar filizlendirmesi adına.



Geçmişteki oligarşik yönetimlerin hepsi ya kemikleştiklerinden ya da yumuşadıklarından güçlerini yitirmişlerdir. Ya aptal, küstah ve kibirli hale gelip kendilerini değişen koşullara göre ayarlamayarak yıkıldılar, ya da liberalleşip yüreksizlik göstererek, zor kullanmaları gerektiği yerde teslim olup, yine yıkıldılar. Oligarşi yönetiminin esası babadan oğula geçmesi değil, yaşamayan tarafından yaşayana zorla

kabul ettirilen belirli bir dünya görüşü ve belli bir yaşam biçimidir. Egemen grup, kendisinden sonra gelecek olanları atayabildiği sürece egemendir. Parti'nin kaygısı, kendi kanından olanı değil, kendisini sürekli kılmaktır. Hiyerarşik yapının her zaman aynı kalması kaydıyla, kimin boyun eğen olduğu önemli değildir. Sistemli olarak, yavaş yavaş aile dayanışmasının altını oyar ve kendi liderine, doğrudan doğruya aile bağlılığı gibi duygular çağrıştırarak, onu sevimli gösterecek bir ad verir.

Günümüzdeki savaşın başlıca amacı, genel yaşam standardını iyileştirmeksizin, makinenin ürettiklerini tüketmektir. Mal üretilmeli, ama dağıtılmamalıydı. Uygulamada bunu gerçekleştirmenin tek yolu da sürekli devam edecek bir savaştı. Savaşın yaptığı en önemli şey yok etmektir; illa ki insan hayatından değil, insanların yaptıkları iş sonucu ürettiklerinin yok edilmesi. Savaş, ilke olarak her zaman, nüfusun ancak hayatta kalmasına yetecek kadar gereksinimi karşıladıktan sonra artakalan üretim fazlasının tümünü yiyip bitirecek şekilde planlanmıştır.

Savaş isterisi ve düşmana duyulan nefret, en çok İç Parti'de güçlüdür. Teknolojik ilerleme bile, yalnızca, ortaya koyduğu ürünler bir biçimde insanın özgürlüğünü kısıtlamaya yarayacaksa gerçekleşmektedir. Matbaanın bulunuşu kamunun görüşünün hile yapılarak, istenildiği şekilde değiştirilmesini kolaylaştırdı, sinema ve radyo ise bu yöntemi daha da geliştirdi. Televizyonun geliştirilmesi ve aynı aletin aynı anda hem alıcı, hem de verici olabilmesine olanak veren teknik ilerleme, özel hayatın sonu oldu.

Kitleler, asla kendiliklerinden ayaklanamazlar ve asla, yalnızca baskı gördükleri için ayaklanmazlar. Aslında, kıyaslama standartlarına sahip olmalarına izin verilmediği sürece, baskı altında olduklarının bilincine bile varamazlar hiçbir zaman.

Tüm dünya bugün, bundan elli yıl önce olduğundan daha ilkeldir.

9. Kimyasal Silah Kullanımı ve Amerika

Kimyasal silah kullanımıyla ilgili tarih kaynaklarına baktığınız zaman İ.Ö. 4000 yıllarına kadar geriye gidebilirsiniz. Spartalı askerler düşmanlarına karşı kükürt dumanı kullanmışlar, İ.S. 1346'da Kırım Tatarları mancınıklarla çürümüş ve virüslü cesetler fırlatmış, 1500'lerde İspanyol fatihleri yerli halklar üzerinde biyolojik savaşlar yapmıştır.

Bir iktidar partisi düşünün, meşruiyetini kaybetmiş, Nobel'e çemkiren²⁵, Olimpiyatlar'a küsen²⁶, Twitter'dan "**kına stokları tükenmiş**" diyebilen²⁷, iktidarlığını garanti altına alıp daha uzun bir süre devam ettirmek için savaş arayan, bunun için de sulandırılmaya müsait her türlü tanımdan yola çıkarak "**demokrasi**" götürmek, "**zulümden**" kurtarmak, ezilenin "**umudu**" olmak ve tüm bunlara da uygun bir kılıf olarak "**kimyasal silah kullandı**" diyerek tek bir hedef gösterebilen.

Kimyasal silahların çok fazla tarihçesine girmeden, Amerika'nın kimyasal silah kullanımına ve etkilerine tarihsel olarak bir bakalım. Amerika'nın diyorum, ve doğrudan Amerika'yı hedef alıyorum. Rus kuvvetlerin Bolşeviklere karşı İngiltere desteğiyle zehirli gaz kullanması²⁸, Almanya'nın 1. Dünya Savaşı'nda klor gazı kullanması²⁹ gibi birçok örneği kolaylıkla bulabilirsiniz. Bu yazıyla ilgili olarak, bu bir derleme yazısıdır, bolca referans göreceksiniz. Temel kaynak ise

25 <http://www.sabah.com.tr/Gundem/2013/08/08/ey-nobel-sen-nasil-baris-odulleri-dagitiyorsun>

26 <http://www.ensonhaber.com/egemen-bagis-biz-degil-olimpiyatlar-kaybetti-2013-09-08.html>

27 <https://twitter.com/suatkilic/status/376490038227652609>

28 <http://www.rawstory.com/rs/2013/09/01/winston-churchills-shocking-use-of-chemical-weapons/>

29 <http://www.history.com/this-day-in-history/second-battle-of-ypres-begins>

burasıdır³⁰.

1950-1953 Kore Savaşı

Savaş sırasında, Kuzey Kore, Sovyetler Birliği ve Çin, Amerika'nın 1947 yılında geliştirdikleri biyolojik silahları kullanmakla suçlanmıştı³¹. Daha detaylı bir bilgi için buraya³² bakabilirsiniz.

1955-1975 Vietnam Savaşı

Amerika, 1965-1972 yılları arasında Napalm³³ ve Agent Orange (*Portakal Gazı*)'ını³⁴ bu savaşta ana silahları olarak kullanmıştı. Napalm ile ilgili bir bilgi verecek olursak, su 100 derecede kaynarken, Napalm'ın etkisi 815 derecenin üzerine çıkıyor. İlk kullanımı ise 6 Mart 1944³⁵ yılına kadar gitmektedir. Deride ve vücutta ağır yanıklar oluşturur, atmosferde %20 daha fazla karbon monoksit ve ateş fırtınasına neden olur, ateş fırtınası rüzgarla birlikte saatte 110km hıza ulaşabilir. Vietnam'da yaklaşık olarak 400.000 ton Napalm kullanılmıştır³⁶.

Portakal Gazı'na gelecek olursak (*İngilizce'den çeviri olarak genelde Portakal Gazı kullanılıyor.*) aslen herbisittir. Yapararak dökücü olduğundan ve Vietcong'ların en büyük besin ve saklanma kaynağı, hatta silahı da yoğun Vietnam ormanları olduğu için, Amerika, yaklaşık 73 milyon litre bu herbisit, asit, jet yakıtı karışımını

30 <https://scriptonitedaily.wordpress.com/2013/09/04/the-shameful-and-recent-history-of-chemical-weapons-abuses-by-the-us-government/>

31 <http://www.telegraph.co.uk/news/worldnews/asia/northkorea/7811949/Did-the-US-wage-germ-warfare-in-Korea.html>

32 https://en.wikipedia.org/wiki/Allegations_of_biological_warfare_in_the_Korean_War

33 <http://vietnamawbb.weebly.com/napalm-agent-orange.html>

34 <http://vietnamawbb.weebly.com/napalm-agent-orange.html>

35 https://en.wikipedia.org/wiki/Napalm#Military_use

36 <http://science.howstuffworks.com/napalm3.htm>

dökmüştür³⁷. En popüler olanı Agent Orange olmasına rağmen Amerika, Agent Pink, Agent Green, Agent Purple, Agent Blue, Agent White, genel adıyla “**Yağmur Herbisitleri**” kullanmıştır. Yıkıcılığı ise akıl almaz boyutlardadır. Güney Vietnam’ın %24’ü, 5 milyon dönüm mangrov ormanı, 500.000 dönüm ekili arazi, 3,181 köy, ayrıca Vietnam sınırına yakın Laos ve Kambojca’daki bazı alanlara dökülen Portakal Gazı yüzünden, 4.8 milyon insan ölmüş³⁸, 400.000 sakat doğum gerçekleşmiştir³⁹. Portakal Gazı’nın ise etkileri hala devam etmektedir⁴⁰.

Güney Vietnam’ın bazı bölgelerinde dioksin seviyesi uluslararası standartların 100 katı üzerindedir⁴¹. Portakal Gazı’ndan etkilenen yetişkinlerin çocuklarında prostat kanseri, solunum kanserleri, ilik kanserleri, diyabet, lenfoma, sarkom gibi birçok ölümcül hastalık görülmektedir.

Irak

16 Mart 1988’de gerçekleştirilen Halepçe Katliamı’nda⁴² (ayrıca bir soykırımdır bu) 5.000 Kürt sivilin ölümüne neden olan hardal, sarin, sinir gazları saldırısıyla suçlanan Saddam Hüseyin’in arkasında doğrudan ve dolaylı olarak Amerika ve İngiltere bulunmaktadır. Dönemim Thatcher ve Reagan hükümetleri, Irak-İran savaşında Saddam rejimini askeri olarak desteklemekteydiler⁴³, onlar için Saddam’ın kimyasal silah kullanması görmezden gelinebilirdi.

37 <http://www.warlegacies.org/History.pdf>

38 <http://vietnamawbb.weebly.com/napalm-agent-orange.html>

39 <http://vietnamawbb.weebly.com/napalm-agent-orange.html>

40 <http://hnn.us/article/143784>

41 https://en.wikipedia.org/wiki/Vietnam_War#Chemical_defoliation

42 http://en.wikipedia.org/wiki/Halabja_poison_gas_attack

43 <http://scriptonitedaily.wordpress.com/2013/05/29/we-are-not-the-good-guys-the-compassionate-case-against-foreign-intervention/>

Zaten en büyük silah sağlayıcısı da kendileriydi. Bilindiği gibi 2004 yılında⁴⁴ Bush hükümetinde ise, bu, Irak'a karşı kullanılacak en büyük koza dönüştürüldü. Peki ne oldu? Sonuçları burada⁴⁵.

Milyonlarca ölüm, peşinden gelen doğa ve hayvan katliamları, nesilleri etkileyen kanser, sakat doğum, soykırım, arkasında dünyanın küresel jandarması Amerika! En büyük kozu ise başkalarını kimyasal silah kullanmakla suçlayıp, dünyayı kana bulayarak payidar olmak! Tarihsel sürece devam edelim:

- 1907 yılında, Lahey Kongresi'nde kimyasal silahlar yasadışı ilan edildi, fakat Amerika kongreye katılmadı⁴⁶.
- 1927 yılında, Milletler Cemiyeti'nde kimyasal/biyolojik silahları yasaklamak için Genevre Protokolü hazırlandı, fakat Amerika Milletler Cemiyeti'ne girmeyi reddetti⁴⁷.
- 1947 yılında, dönemin başbakanı Harry Truman kongre tarafından değerlendirilmesi amacıyla Genevre Protokolü'nden çekildi⁴⁸.
- 1961 yılında, dönemin başbakanı Kennedy, kimyasal silah harcamalarını 75 milyon \$'dan 330 milyon \$'a çıkarttı⁴⁹.
- Amerika, 1974 yılına kadar 1928 yılında hazırlanan Genevre Protokolü'ne onay vermedi⁵⁰. Bu süreçte yaşananları yukarıda tekrar inceleyebilirsiniz. 1985 yılında, Amerika, açık havada biyolojik silah denemelerine kaldığı yerden devam etti ve 4 yıl boyunca Irak'a kimyasal silah desteğinde bulundu.

44 <http://news.bbc.co.uk/1/hi/4440664.stm>

45 https://en.wikipedia.org/wiki/Casualties_of_the_Iraq_War

46 <http://www.icrc.org/applic/ihl/ihl.nsf/INTRO/195>

47 <http://www.un.org/disarmament/WMD/Bio/1925GenevaProtocol.shtml>

48 <http://www.fas.org/nuke/control/geneva/intro.htm>

49 <http://www.counterpunch.org/2013/09/02/a-short-history-of-bio-chemical-weapons/>

50 <http://www.state.gov/t/isn/4784.htm>

- 1989 yılında, Paris'te, 140 ülke kimyasal silah kullanımını Paris Konferansı'da kınadı⁵¹. Kınama, Irak'ın Halepçe Katliamı temelliydi. Daha sonra da ortaya çıktığı gibi Irak'ta kullanılan kimyasal gazlar Amerika'da üretilmişti⁵².
- Son Kimyasal Silahlar Kongresi, 1997 yılının Nisan ayında Amerika tarafından imzalandı ve aynı gün yürürlüğe girdi⁵³.

Yeni Şafak'tan kendine köşe yazarı diyen Sinem Köseoğlu'nun bir yazısına denk geldim⁵⁴. Yazısının sonundan küçük bir alıntı yapıyorum; **“Suriye'deki masum insanların umudunun ABD iç siyasetine bağlı olması ne acı, değil mi?”** Kendisine tavsiyem, masum insanların umudunu ABD'nin kimyasal silah geçmişine ve savaş suçları tarihine bakarak tekrar tekrar değerlendirsin. Bunu yapabilmesi elbette zordur. Çünkü kendisi gibi yazarlar sadece umut tacirleridir. Bu gibi yazarlar, Irak'taki kitle imha silahlarını da demokrasi ve umut götürmek altında insanlara köşe yazılarından aktarmışlardı. Ama hiçbiri çıkıp o silahları satanın ve kullanımını destekleyenin Amerika olduğunu söyleyemedi.

Son olarak, Winston Churchill'in kimyasal silah kullanımı için söyledikleriyle bitirelim; **“Barbar kabilelere karşı zehirli gazların kullanılmasının güçlü taraftarıyım.”** Sağlam bir mide dileğiyle!

51 <http://www.nytimes.com/1989/01/12/world/paris-conference-condemns-the-use-of-chemical-arms.html>

52 <http://www.counterpunch.org/2013/09/02/a-short-history-of-bio-chemical-weapons/>

53 <http://www.opcw.org/about-opcw/member-states/>

54 <http://yenisafak.com.tr/yazarlar/sinemkoseoglu/washingtonun-kafasi-karisik/39463>

10. Arka Kapı

Eğer işlemcinizin üreticisi (AMD, Intel, Qualcomm vd.) NSA tarafından arka kapı bırakmaya zorlanmışsa ya da herhangi bir donanımızda bu tarz gizlilik ihlalleri yapılmışsa, kendinizi nasıl korumaya çalışırsanız çalışın NSA sizinle ilgili her şeyi görebilir.

Daha ayrıntılı bir açıklama yapmam gerekirse; kullandığınız donanımın geliştirme aşamasında, Büyük Birader sizleri izleyebilmek için üreticileri arka kapı bırakması için zorlamış, çip geliştirmesinde doğrudan veya dolaylı olarak katkıda bulunmuşsa kendinizi gizleyebilmeniz pek de mümkün olmayacaktır. Buradaki izleme daha çok sizin yaptığınız her şeyi kaydetmek değil de kendilerine bir arka kapı bırakmak, zamanı geldiğinde ya da ihtiyaç duyulduğunda buna başvurarak gerekli bilgiyi temin etmektir.

Bu tarz bir veri temini her şeyi kaydedip samanlıkta iğne aramaktan çok değerli veriyi almaya yarar. Kendini mükemmel bir şekilde kamufle etmiş böyle bir yöntem, kullandığınız herhangi bir cihazın rahatça izlenmesine olanak sağlayacaktır. Bir diğer deyişle, NSA kendi işleri için hazırladığı özel çiplere sahip olacak, tüketici ise bu çiplere sahip donanımları bunun farkında bile olmadan satın alarak kullanmaya başlayacak. Her şey uzaktan bir komplo teorisi gibi durmaktadır. Fakat son sızan bilgilere göre⁵⁵ buna benzer, daha doğrusu bunu ima edecek bir çalışma 2007 yılında başlamış. Google ise⁵⁶ bu dönemde kendine ait her servis için noktadan noktaya (*man*

55 <https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html>

56 <http://yro.slashdot.org/story/13/09/09/1154209/google-speeding-up-new-encryption-project-after-latest-snowden-leaks>

*in the middle*⁵⁷ yok demek) kriptolanmış iletişim için çalışmaktaydı ve Snowden'dan sonra bu işi iyice hızlandırdı. Bu, şu işe yarayacak; eğer biri verileri bir şekilde Google'dan temin etmek isterse Google istese bile bu verileri veremeyecek.

Bu noktada, Windows ve Mac OS kullanıcıları ciddi anlamda tehlikede olduğu varsayılabilir. GNU/Linux kullanıcıları nispeten daha az, *BSD kullanıcıları ise daha da az tehlikedeler. Art niyetli bir firmware, işlemci (*donanım*) üzerindeki bu tarz arka kapıları aktive edebilir ve bundan istediği gibi faydalanabilir. Siz ise işletim sisteminizi, donanım yazılımınızı güncelleştirdiğinizi zannedebilirsiniz. Kulağa çok çılgınca geldiği doğru. Böyle bir şeyin yapılmış olabileceğini ise ancak ileri düzey bir elektron mikroskobu ve ileri düzey teknik aletlerle işlemcinizi inceleyerek görebilirsiniz. Böyle bir şeyi test etmek ise tüketicilerin boyunu aşmaktadır.

Bir Kernel hacker'ı olan Theodore Ts'o⁵⁸, Intel'in /dev/random'ı sadece RDRAND'e dayanması gerekliliğindeki ısrarını neden reddettiğini⁵⁹ de bu üstte anlattığım "**komplo teorisi**"ne dayanarak söylüyor. Diyor ki; "**Denetlenmesi kesinlikle mümkün olmayan, bir çipin içine gizlenmiş uygulama demek olan sadece donanımsal RNG'ye⁶⁰ güvenmek, KÖTÜ bir fikirdir.**" Örneğin, eğer Intel, RNG'yi⁶¹ doğrudan işlemcileri içine yerleştirirse kullanıcıların yazılımı kullanması yerine yazılımın kullanıcıları kullanmasına olanak sağlamış olacaktır. Başka bir deyişle, eğer RNG bir anahtar ile dağıtılmakta ise bunu tespit edebilmek imkansız

57 https://en.wikipedia.org/wiki/Man-in-the-middle_attack

58 <https://plus.google.com/117091380454742934025>

59 <https://plus.google.com/117091380454742934025/posts/SDcoemc9V3J>

60 https://en.wikipedia.org/wiki/Hardware_random_number_generator

61 https://en.wikipedia.org/wiki/Random_number_generation

olacak. Fakat kullanıcı yazılıma dayanarak RNG'yi gerçekleştirirse, yazılımdaki buna benzer bir arka kapı ise kolaylıkla farkedilebilecektir.

“Ne yapalım, harddiskimizi kriptoladıktan sonra bilgisayarımızın üzerine benzip döküp yakalım mı?” dediğinizi duyar gibiyim. **“NSA beni ne yapsın?”** diyerek espri yaptığınızı biliyorum. Fakat bunu her normalleştirdiğinizde size dönüşü daha kötü olacak, daha çok gizlilik ihlali içerecek, sizleri aptal yerine koyacak ve birer köleye çevirecektir. Farkında olun, uyanık olun, hakkınıza sahip çıkın!

11. AKP, Baskı ve Polis Devleti

AKP'nin iktidarlığı dönemi boyunca siyasi anlamda “**baskı**”’yı nasıl kullandığını, sistematik olarak vatandaşlarını nasıl korkuttuğunu ve şiddetle nasıl boyun eğdirmeye çalıştığını incelemeye çalışalım. Bu süreçte eksikler elbette olacaktır, eklemekten çekinmeyiniz.

Baskının ne olduğunu kısaca anlatmak istersek bir tür zulme benzese de tepkisel değil, daha çok aktiftir. Baskı, muhalefeti kontrol etmek yerine onun kökünü kazımayı amaçlar. Bu anlamda zulümden ayrılır. Kitleleri siyasetin dışına iter, ifade özgürlüklerini engeller⁶², bunu yaparken de siyasi ve psikolojik araçlara başvurur. AKP rejimine bakılırsa eğer sendikaları nasıl zayıflattığı ve ortadan kaldırmaya çalıştığını⁶³, basın özgürlüğünü⁶⁴ kendi istekleri doğrultusunda evirip çevirdiğini⁶⁵, vatandaşlarını “**dinlediğini**”⁶⁶, İnternet üzerinde “**izlediğini**”⁶⁷, her sokağa bir “**göz**”⁶⁸ diktiğini, kendince doktor kesildiğini⁶⁹, ahlak polisi olup kitap yasakladığını⁷⁰ görebiliriz. Bu, insanların üzerinde bir korku dalgası oluşturur. Etrafta sizi izleyen veya dinleyen bir mekanizmanın olması, sizi devamlı yaptığınız işlerde sorgulamaya, içinize Büyük Birader korkusu salmaya yarar. Böylece daha rahat kontrol edilebilir ve baskı

62 <http://t24.com.tr/haber/af-orgutu-2013-raporu-turkiyede-ifade-ozgurlugu-kisitli/230512>

63 <http://haber.sol.org.tr/sonuncu-kavga/mecliste-gece-yarisi-tmmob-operasyonu-haberi-76112>

64 <http://www.amerikaninsesi.com/content/rsf-turkiye-basin-ozgurlugunde-154uncu-sirada/1709213.html>

65 <http://www.yesilgazete.org/blog/2013/06/07/al-birini-vur-otekine-6-musvedde-medya-gazetesinde-tek-baslik/>

66 <http://www.evrensel.net/news.php?id=65085>

67 <http://www.enphormasyon.org/>

68 <https://tr.wikipedia.org/wiki/MOBESE>

69 <http://www.sendika.org/2013/01/kurtaj-yasasi-bir-degersizlestirme-projesi/>

70 <http://www.gazetecileronline.com/newsdetails/6037-/GazetecilerOnline/iste-akp-tipi-demokrasinin-eseri-bir-yilda-46-kita>

altında tutulabilirsiniz.

Polis, niteliği itibariyle ceza yasasını uygulamak ve iç asayışı sağlamakla görevlidir. Liberal perspektiften bakarsak, yurttaşlarını birbirlerinden korur, bireysel hak ve özgürlükleri savunur, hukuk düzenini destekler. Fakat, AKP gibi kendilerine “**muhafazakar demokrat**⁷¹” diyen rejimlerde polisin rolü, devletin otoritesini korumaya ve hakimiyetini toplumun her alanına yaymaya dönüşür. Ayrıca, AKP’ye hizmet etmesi ve bir “**baskı**” aracı olarak kullanılması da buna eklenmelidir. Türkiye’de 2013 yılı itibariyle 340,000 polis memuru var⁷². AKP’nin polise -ve özel güvenliğe- bu kadar çok yatırım yapmasının altındaki neden de polise biçtikleri “**devleti ve biz elitleri muhafaza et**”tir.

AKP rejiminde görüldüğü gibi polislik “**siyasi**” olduğu zaman toplumsal olarak otoriter ve siyaseten muhafazakar bir kültür üretme eğilimine girer. Bu yüzden de kendi geleneği için gencecik ve suçsuz insanları (*Mehmet Ayvalıtaş⁷³, Abdullah Cömert⁷⁴, Ali İsmail Korkmaz⁷⁵, Medeni Yıldırım⁷⁶, Ethem Sarısülük⁷⁷, Ahmet Atakan⁷⁸*) katletmekten geri kalmaz. Polisin halkın gözündeki tarafsızlığı, AKP’nin baskısından kaynaklanan gösterileri/protestoları kontrol etmede kullanıldığında ve kendisine AKP tarafından biçilen rolle iyice

71 <http://hurarsiv.hurriyet.com.tr/goster/ShowNew.aspx?id=314711>

72 <http://www.bianet.org/bianet/bianet/146843-devletin-polisleri-polislerin-devleti>

73 <http://haber.sol.org.tr/soldakiler/akp-saldirilari-sonucunda-genc-isci-mehmet-ayvalitas-hayatini-kaybetti-haberi-74012>

74 <http://bianet.org/bianet/insan-haklari/148263-abdullah-comert-i-kim-oldurdu>

75 <http://haber.sol.org.tr/devlet-ve-siyaset/ali-ismail-korkmaza-polis-ve-sopali-bir-grup-birlikte-saldirdi-haberi-76172>

76 <http://www.evrensel.net/news.php?id=60728>

77 <http://haber.sol.org.tr/devlet-ve-siyaset/polisin-vurdugu-ethem-sarisulukun-beyin-olumu-gerceklesti-haberi-74596>

78 <http://haber.sol.org.tr/devlet-ve-siyaset/akp-antakyada-yine-katletti-ahmet-atakani-kaybettik-haberi-79379>

tehlikeye girmiştir. Aslında, bu, tehlikeye girmenin yanı sıra frensiz olarak bayır aşağı gitmektir. Polisin, Gezi'den sonra ne mahkemelere⁷⁹ ne de halka hesap verdiğini⁸⁰, yaşananlardan dolayı özür bile dilemediğini⁸¹ gördük⁸².

AKP tarafından polise verilen bu aşırı yetki, sosyal hayatın bütün yönlerinin siyasi kontrol altına aldığı bir korku dalgası yaratmak üzerinedir. Polis gücü, bu “**elitler**” tarafından yönetildiği için Türkiye bir polis devletine dönüşmüştür. Polis, artık AKP'nin özel ordusu olarak hareket etmektedir ve bir baskı unsuru olarak kullanılmaktadır. AKP'li vekil ve bakanların, kendilerine yazar, siyasetçi, düşünür diyen yalakaların polise kahramanım dediği⁸³, polis tarafından öldürülen insanlara terörist diyerek⁸⁴ “**egemen biziz, terörü ve kimin terörist olduğunu da biz belirleriz**” rolü de bu muhafazakarlıktan kaynaklanmaktadır. Çünkü polis ondan beklenen muhafaza arzusunu yerine getirmeye çalışmaktadır. Elbette, AKP iktidarı gidip yerine başka bir iktidar geldiğinde polise biçilecek rol, hesaba çekilebilirlik ve siyasi kontrol yeni iktidara göre şekillenecektir. Burada yapılması gereken zayıf bir sorumluluk, keyfiyete ve değişken cezalara tabi olması ya da günün hükümetinin ihtiyaçlarına göre koşulmasına olanak verilmemesi olacaktır.

79 <http://haber.sol.org.tr/devlet-ve-siyaset/ethemin-katili-serbest-birakildi-haberi-75247>

80 http://www.radikal.com.tr/turkiye/bakanlik_mufettisleri_gezide_orantisiz_guc_kullanildi-1148833

81 <http://haber.sol.org.tr/devlet-ve-siyaset/ali-ismailin-katilinden-igrenc-savunma-haberi-78407>

82 <http://vagus.tv/2013/09/10/egm-sahis-yuksekte-dusmustur-dusme-ani-ve-oncesinde-mudahale-olmamistir/>

83 <http://www.ntvmsnbc.com/id/25450862/>

84 https://twitter.com/ozlemezcan_/status/377396052334112768

12. Online Kripto Araçları

Başlığa aldanıp nasıl kullanacağımızı anlatacağım bir rehber zannetmeyin. Snowden'in belgelerine dayanarak NSA tarafından bir şekilde kırıldığı söylenen⁸⁵ bu araçların neler olduğundan bahsedelim.

Amerikan İç Savaşı muharebelerinden olan Bull Run⁸⁶ ilk 21 Temmuz 1861 yılında gerçekleşti. Konfederasyon'un kazandığı bu muharebe aradan 152 yıl sonra NSA'in belirli ağ iletişim teknolojilerini kırmak için kullandığı kripto çözme programının kod adı⁸⁷ oldu. İngiltere cephesinde ise 23 Ekim 1642⁸⁸ yılında ilk İngiliz İç Savaşı muhaberesi olan Edgehill, bu kripto çözme programına isim verdi.

Bullrun Projesi ortaya çıkarttığı üzere⁸⁹, NSA ve GCHQ'nun HTTPS, VoIP, SSL gibi geniş çapta kullanılan online protokollere karşı bunu kullanmakta ve bu protokolleri kırabilmektedir.

85 https://www.nytimes.com/interactive/2013/09/05/us/unlocking-private-communications.html?_r=1&

86 https://en.wikipedia.org/wiki/First_Battle_of_Bull_Run

87 <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>

88 https://en.wikipedia.org/wiki/Battle_of_Edgehill

89 <https://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us>

Bu protokoller, programlar nelerdir, bakacak olursak:

VPN (*Virtual Private Network*⁹⁰)

Özellikle şirketlerin çalışanlarının ofise uzaktan erişim sağlayabilmesi için kullandığı VPN'ler⁹¹.

Şifreli Chat

İletim esnasında kırılması mümkün olmayan (mesaj servisi tarafından bile), Adium⁹² ve AIM⁹³ gibi noktadan noktaya şifreleme sağlayan programlar.

SSH (*Secure Shell*⁹⁴)

Güvensiz bir ağda, güvenlik kanalı üzerinden iki bilgisayar arasındaki veri aktarımının gerçekleştirilmesini sağlayan, kriptografik ağ protokolü. GNU/Linux ve Mac kullanıcıları için standart halinde gelmiş bir uygulamadır.

HTTPS (*Hypertext Transfer Protocol Secure*⁹⁵)

Özellikle kullanıcı ve sunucu arasındaki bilgilerin (*şifre, finansal bilgiler vs.*) başkaları tarafından erişimini engellemek için HTTP protokolüne SSL protokolü eklenerek oluşturulmuş ve standart haline gelmiş güvenli hiper metin aktarım iletişim kuralı. Son

90 https://en.wikipedia.org/wiki/Virtual_private_network

91 https://tr.wikipedia.org/wiki/VPN#Sanal_.C3.96zel_A.C4.9Flar_.28VPN.29

92 <https://adium.im/>

93 <http://www.aim.com/>

94 https://en.wikipedia.org/wiki/Secure_Shell

95 https://en.wikipedia.org/wiki/HTTP_Secure

dönemde Facebook⁹⁶, Twitter⁹⁷, Gmail⁹⁸ gibi servislerle daha da bilinir hale gelmiştir.

TSL/SSL (*Transport Layer Security/Secure Sockets Layer*⁹⁹)

İstemci-sunucu uygulamalarının (*tarayıcı, e-posta vs.*) ağ boyunca gizlice dinleme ya da yetki dışı erişimi engellemek için olan kriptografik protokollerdir.

Şifreli VoIP (*Voice over Internet Protocol*¹⁰⁰)

Microsoft'un Skype ya da Apple'ın FaceTime gibi servisleri kullanıcıların Internet üzerinden sesli ve görüntülü iletişim kurmalarını sağlayan uygulamalar.

96 <https://facebook.com/>

97 <https://twitter.com/>

98 <https://gmail.com/>

99 https://en.wikipedia.org/wiki/Transport_Layer_Security

100 https://en.wikipedia.org/wiki/Voice_over_IP

13. CV Rekabetçiliği

İyi bir CV nasıl olmalıdır? Başarılı CV'lerin sırrı nedir? CV'niz ile rakiplerinizin önüne nasıl geçebilirsiniz? CV yazmanın 10 altın kuralı... Fark edilin... Aykırı olun... Israrcı olun... Kendinizi övmekten çekinmeyin... Blablblah

Tüm bunları okuduğunuzda günümüzdeki iş bulma sürecinin tamamen rekabet yapma yeteneğine dayandırıldığını göreceksiniz. İş arama ve ilan siteleri, kariyer planlama merkezleri, başarı öyküleri vd. bu rekabetçiliğin birer simgesidir. Sizin mesleki ya da yüksek öğreniminiz açısından uygun bir işe yerleşip yerleşememeniz, size dayatılan pazarın bu yapısını kabul etmenizle veya pazardaki başarınızla ilişkilendirilmektedir. Peki kimler tarafından?

Bir hikaye ile devam edelim. Çok uzak bir ülkede aileler iş ortamlarından ve aldıkları ücretlerden, muktedirin altında ezilip itilmekten ve kendi kötü yaşam koşullarından dolayı, çocuklarının daha iyi bir yaşama sahip olmasını istemektedirler. Muktedirler, bir yandan **“Bu meslekler iyidir.”**, **“Bu mesleklerin parası iyidir.”** diyerek topluma öğrettikleri, zorla dayattıkları işleri ve bu düşünceleri ailelerin çocuklarına aktarabilmesi ve çocuklarını bu alanlara sokabilmesi için planlı ve programlı olarak çalışmaktadır. Aile, bu süreç içerisinde çocuğunun **“o”** mesleklerden birinin sahibi olursa, güç sahibi olacağını, para sahibi olacağını, çocuğu daha gelişirken beynine işlemekte, devamlı kendilerinden örnek vermekte **“Bizim gibi olmak/çalışmak istemiyorsan...”** diyerek sanki içinde buldukları durumun kendi suçlarıymış gibi algılayıp çocuklarına aktarmaktadır. Aynı şeyi çocuğun gittiği okullar/üniversiteler de yapmakta, bilinçli olarak eğitim sistemi de kendi rekabetçiliği ile

çocukların geleceğini tayin etmektedir. Çocuk, ailesi tarafından, toplum tarafından ve gittiği okullar tarafından zorla bir alana sokulup, tüm bunlar kabul ettirilerek, yapmak istediği şeyi veya hayalindeki işi yapamayacak olmasına rağmen bu alanlardan birinden mezun olur ve iş aramaya koyulur. Karşısında ise bu muktedirler, işverenler, kendisini tecrübesizlikle, rekabet yapma yeteneği yoksunluğuyla, **“Taşra üniversitesinden mezun olmuşsun.”** demekle, piyasadaki işsizlikten dolayı kendilerine muhtaç olduğunu söylemekle, bilinçli olarak korkutmakla ve daha çocukken ailesinin, öğretmenlerinin, okullarının kafasına vura vura soktuğu **“iyi maaşı”** vermemekle tehdit edip, çocuğu bir güzel sindirerek yıllardır ona öğretilen tüm bu şeyleri bir kalemde silmektedir. Çocuk, aslında piyasaya yön verenin bu muktedirler olduğunu ve tek dertlerinin ucuz işgücü temini olduğunu farkeder. Bu büyüyüp gelişen, hayalindeki şeyleri yapamayacak olan çocuk bunun darbesiyle bir kez daha yıkılır. Gerçekler bunlar diye, aslında gerçek diye başında kendisine yutturdukları şeyleri, şimdi, aslında öyle değil böyle diyerek bu güç budalası ahmaklar tarafından istendiği gibi kullanıldığını, manipüle edildiğini farkeder.

Hikayede anlattığım üzere, muktedirler aklın karanlık çağlarında olduğu gibi yargıladıklarına hiçbir savunma ve itiraz hakkı tanımadan keyiflerinin oyuncağına dönüştüren engizisyon kuruluna dönüşüyor. Savunma ve itiraz hakkını da mülakatlarda sizlere kendi yön verdikleri süreç doğrultusunda izin veriyor. Onda da çoğunlukla her kavramı bilinçli olarak yanlış kullanmaktadırlar ki böylece kavramların içini boşaltabilmeli ve karşısındaki bireyleri bilinçli olarak aptallaştırmaya çalışabilmelidirler.

Muktedirlerin, rekabetçilikten sonra en çok sırtını dayadıkları ve güç aldıkları şey “**tecrübesizliktir**”. Siz tecrübesizsinizdir ve size yapılması gereken ödeme “**emeğinizin**” karşılığı olan o düşük ücrettir, ayrıca hakettiğiniz ünvan da süslü “**jr.**”, “**newbie**” gibi şeylerdir, böylece işgücünüzün değil ünvanınızın hakettiği bir ücret vardır. Alın size bir kavramın içinin boşaltılması örneği. Emeğin (ve ünvanın) bir değeri var! Halbuki emeğin kendisinin değeri yoktur, sizin sattığınız kendi işgücünüzdür. İşveren sizin işgücünüzü satın alır ve ona belirli bir çalışma süresi için ödeme yapar. Siz günde 8 saat çalışıyorsanız, işverenin bu zaman içinde sizin ücretinizi ödemesi için gerekli olan süre, çalışma sürenizin küçük bir kısmıdır. İşverene kalan süre, değer, onun için artı-değerdir, yani ücretin dışında kalan değer. Bu tür basit ve zorla kabul ettirilmiş oyunlar, muktedirlerin ucuz işgücü temini politikasından başka bir şey değildir.

Kısaca bir özet geçecek ve toparlayacak olursak, piyasayı yöneten bu kudretli tanrılar kavramların içinini boşaltır, kendi yön verdikleri piyasalarda kendilerine uygun işgücü temini için bilinçli olarak fakirleştirdikleri aileleri ve eğitimi kullanır, sizin işgücünüze değil size verdikleri basit ünvanlara ücret belirler. Böylece çark her zaman onlar için döner, kavramlar onların istedikleri şekilde tanımlanır, size ise aldatılmak, “**kaderinize razı olmak**” ve bu tanrıların vereceği kırıntılar kalır.

14. SteamOS'un Düşündürdükleri

“GNU/Linux'ta oyun oynamak ya da oynayamamak, işte bütün mesele bu!” peki gerçekten bu mu? 12 yıllık bir GNU/Linux kullanıcısı olarak o kadar çok oyun oynadım ki bu işletim sisteminde, bazen kendimi zorla dayatılan “Linux'ta oyun oynanmaz.” düşüncesiyle başbaşa bulmaktan alamıyorum.

GNU/Linux'ta oyun oynamak hep ya imkansız, ya çok zor ya da birilerinin “heveslediği” veya görmek “istediği” bir şeymiş gibi aktarılmaktadır. Fakat, durum onların böyle aktarmasına rağmen hiçbir zaman öyle olmadı. GNU/Linux'ta zaten oyun oynanmaktaydı. Dahası, buna Windows oyunları da dahil. GNU/Linux'un gelişimini (kullanım artışına paralel olarak) “oyun” endeksli düşünen bu insanlar Wine¹⁰¹, Cedega'yı (malesef bitti)¹⁰², Crossover¹⁰³, ve PlayOnLinux'u¹⁰⁴ ya görmezlikten geldi, ya kullanmasını karmaşık gösterdi (yani üşendi) ya da “istedikleri” oyunların çalışmadığını iddaa etti. Bunların dışında, id Software¹⁰⁵ oyun motorlarını GPL ile lisanslayıp açarken, oyunlarına GNU/Linux desteği verirken veya GarageGames¹⁰⁶ veya Epic Games¹⁰⁷ veya Bioware¹⁰⁸ v.d. oyun(lar)ına bu desteği verirken nedense beklenen o “etki” veya “heyecan” bir türlü bu “hevesli” ve “istekli” insanlarda görülmedi. Peki bu firmalar bu konuda desteklenmedilerse -veya desteklenmezlerse- bir sonraki oyunlarında GNU/Linux desteği vermeleri olası mıdır sizce? Bu konuda sizlere biraz daha ayrıntı vereyim.

101<http://www.winehq.org/>

102<http://www.transgaming.com/>

103<http://www.codeweavers.com/>

104<http://www.playonlinux.com/>

105https://en.wikipedia.org/wiki/Id_Software

106<https://en.wikipedia.org/wiki/GarageGames>

107https://en.wikipedia.org/wiki/Epic_Games

108<https://en.wikipedia.org/wiki/Bioware>

id Software'in ioquake 3¹⁰⁹ -13 yıllık- motoru ile yapılan GNU/Linux oyunlarına bir bakacak olursak, Urban Terror¹¹⁰, Tremulous¹¹¹, Smokin' Guns¹¹², OpenArena¹¹³ ve World of Padman¹¹⁴ gibi çok büyük oyuncu kitlesine hitap eden oyunlar. Bunları örnek göstermemin nedeni bu oyunların 13 yıllık bir motora rağmen bugün bile devamlı oynanması, bağımsız geliştiricilerin bu tarz büyük yazılım firmalarının da desteği ile mükemmel modifikasyonlar hazırlayabilmesidir. Yani, "**destek**" verildikten sonra -ve görmezden gelinmezse- bağımsız olarak GNU/Linux için de çok iyi oyunlar hazırlanabilir, bu oyunlarla GNU/Linux kullanıcılara cazip gösterilebilir -eğer masaüstü kullanıcısının "**oyun**" mantıklı olduğunda ısrarcıysanız-. Bir diğer nokta da üzerinden bir on yıl daha geçse iyi bir oyun -ya da mod- "**kalitesinden**" bir şey kaybeder mi? Kalite elbette anlam olarak sizin ondan ne aldığınız, yani beklentinizin karşılanma derecesidir. Bir diğer deyişle, Mercedes kullanmayan biri için Mercedes kaliteli olmaz. Bu oyunlara da bir örnek vermem gerekirse; Starcraft¹¹⁵ oynamaktan ya da Fallout 2¹¹⁶ v.s. oynamaktan bir "**oyuncu**" bıkmaz mı?

Steam, çıkışından epey bir zaman geçtikten sonra GNU/Linux'a da gelmesi¹¹⁷ ile bu oyunseverleri (*ben de dahil ama hatamdan döndüm*) heyecanlandırdı ve GNU/Linux'u bir oyun canavarına dönüştüreceği -bazıları için de Windows'tan GNU/Linux'a göç- algısı yarattı. Fakat, Steam zaten Wine üzerinden sorunsuz

109<https://en.wikipedia.org/wiki/Idquake3>

110https://en.wikipedia.org/wiki/Urban_Terror

111<https://en.wikipedia.org/wiki/Tremulous>

112https://en.wikipedia.org/wiki/Smokin%27_Guns

113<https://en.wikipedia.org/wiki/Openarena>

114https://en.wikipedia.org/wiki/World_of_padman

115<https://en.wikipedia.org/wiki/Starcraft>

116https://en.wikipedia.org/wiki/Fallout_2

117[https://en.wikipedia.org/wiki/Steam_\(software\)#Linux](https://en.wikipedia.org/wiki/Steam_(software)#Linux)

çalışmaktaydı¹¹⁸. Burada amaç pazarı genişletmek (*el değmemiş ya da kısmen değmiş bir alan olarak GNU/Linux oyun pazarı*) ve bunda öncü olmaktı. Beraberinde Drm'li oyunlar, az oyun desteği (*artıyor ama her geçen gün*), açık kaynağın kapalı kaynakla dolması gibi bir sürü sıkıntıyı getirdi. Kullanıcı özgürlüğü tehdit edilmeye başlandı. Buradaki özgürlük tehdidi Stallman'ın dediği gibi¹¹⁹ ücretli olması veya kopya satılması değil, “**özgür**” olmayan bir yazılımdan kaynaklanıyor olmasıdır.

Şimdi ise gündemde SteamOS¹²⁰ var. Hakkında söylenen bir sürü şey var¹²¹, çoğu belki de söylendiği ile kalacaktır, bilemeyiz. Israrla vurgulanan “**free**” için benim şahsi görüşüm SteamOS'un “**ücretsiz**” olacağı yönünde (*ki öyle*). “**Özgürlük**” anlamında bir “**free**”yi ben şahsen beklemiyorum. Umarım bu konuda yanılırım. Bir diğer şey, Amazon vb. sunucularla film ve müzik konusunda anlaşmaya çalışması. Donanım konusunda ne tür bir yol izleyeceği üzerine spekülasyonlar var. Elbette her şey istenildikten sonra bulandırılabilir, altında anlamsız art niyet aranabilir. Benim ise bu duyuruya istinaden sormak istediğim bazı sorularım olacak. Fakat, soruları daha iyi anlayabilmeniz -ve açık kaynağı, hatta GNU/Linux'u için sizlere kısaca bilim etiğinden bahsedeyim. Bilimsel araştırmalarda bulgular test edilmek ve geliştirilmek üzere başkalarının kullanımına sunulur. Aynı şekilde GNU/Linux ve uygulamaları da başkalarının kullanımına, geliştirilmesine ve yeniden dağıtılmasına sunulur. İşte bahsedilen “**bilim etiği**” ya da “**açık kaynak**” budur.

118<http://appdb.winehq.org/objectManager.php?sClass=version&iId=19444>

119<https://www.gnu.org/philosophy/nonfree-games.html>

120<http://store.steampowered.com/livingroom/SteamOS/>

121<http://techcrunch.com/2013/09/23/valve-introduces-steamos-a-linux-based-platform-to-bring-steam-to-your-living-room/>

- SteamOS Linux tabanlı ve “**free**” yani ücretsiz olabilir. Fakat beraberinde oyun yapımcıları, oyunlarının bundan sonra “**açık kaynak**” olmasını isteyecekler mi?
- Steam ile gelen DRM, SteamOS ile gelmeye devam edecek mi?
- (*Eğer anlaşılırsa*) Amazon sunucularından kim film izlemek ve müzik dinlemek ister?¹²²
- Eğer oyun firmaları (*hepsi şart değil, bazıları da kabulüm*) kapalı kaynakta ısrarcı olursa, açık kaynağı kapalı kaynakla doldurmak (*oyun tercihleri doğrultusunda*) ne kadar mantıklıdır?
- Israrla üzerinde durulan “**özgürlük**” kavramı bundan nasıl ve ne kadar etkilenir?
- Fayda ile eş zamanlı gelecek zararı (*Drm, Amazon, kapalı kaynak vd.*) kabul etmek ne kadar etik bir davranış olur?
- Bütünün değil de bütünün bir parçasının açık kaynak içermesi, bütünün kalanının kapalı kaynak olmasını gözardı etmeye yeter mi?
- Eğer belirli donanımlarda çalışacaksa o zaman bu tekelleşme yaratmaz mı? Onu da geçtim biz bu donanımların chipsetlerine nasıl güvenebiliriz? Peki aynı şekilde firmware’lar ne olacak?

Sorular çoğaltılabilir. O size kalmış. Benim sormak istediğim başlıca sorular bunlar. Elbette ilerleyen günlerde neler olur, ne tür gelişmeler yaşanır bilemeyiz. Bekleyip hep birlikte göreceğiz.

¹²²<http://www.information-management.com/news/be-the-cloud-making-the-case-for-copying-amazon-and-the-cia-10024744-1.html>

15. Tor ve Günümüz İnterneti

Tor'un bizlere sağlamaya çalıştığı anonimlik ve günümüz İnternet'ine bir bakış açısı ve giriş yazısı olması adına umarım sizlere bir şeyler anlatır, anonimlikle ve anonimliğin de beraberinde getirdiği problemler konusunda bir farkındalık yaratır.

Tor'un ne olduğunu detaylı olarak anlatmayacağım. Merak eden varsa kendi sitesinden¹²³ detaylı bilgi alabilir. Tor, websitelerden IP'nizi saklayabilir veya ISS'nizden trafiğinizi Phorm¹²⁴ gibi kötücül uygulamalara karşı gizleyebilir. Tabi devamlı kullanımda ISS'niz trafiğinizden dolayı -göremediği için- kılınacaktır. Fakat küresel ölçekte bir izleme, dinleme, takip olduğu zaman, Tor bunun için yetersiz kalacaktır. Ayrıca, bu Tor'un hatası veya eksik olmasından kaynaklanmamaktadır. Şöyle düşünün, anonim olmayan bir İnternet üzerinde kendi anonim network'ünüzü (*Tor*) kullanıyorsunuz. Burada ne kadar çok şey denerseniz deneyin %100 başarılı bir sonuç elde edemezsiniz.

Tor'da eskiye nazaran "**relay**" oluşturmak ve çalıştırmak giderek kolaylaşmış durumda. Aynı hızla bunların "**dinlenmesi**" de arttı (*bu yüzden HTTPS-Everywhere¹²⁵ kullanın diyoruz!*). Bununla ilgili olarak, Freedom Hosting'e yapılan FBI baskını¹²⁶, ardından Hidden servis'te zararlı javascript bulunması¹²⁷ en güncel örnektir. Ayrıca, Tor kullanıcılarının gerçek kimliklerinin de ele geçirilmesi

¹²³<https://torproject.org/>

¹²⁴<http://enphormasyon.org/>

¹²⁵<https://www.eff.org/https-everywhere>

¹²⁶http://www.reddit.com/r/explainlikeimfive/comments/1jpbjf/eli5_how_the_fbi_to_ok_down_so_many_onion_sites/

¹²⁷<https://blog.torproject.org/blog/hidden-services-current-events-and-freedom-hosting>

bunlara paralel olarak daha basite indirgenmiş durumda. Şöyle anlatayım; bir Tor kullanıcısı günümüzde, eğer 3 ay boyunca düzenli Tor kullanırsa, örneğin IRC'ye bağlanmak, İnternette sörf yapmak gibi, bu relay gönüllüleri tarafından gerçek kimliğinin öğrenilme olasılığı %50, eğer 6 ay düzenli kullanırsa bu olasılık %80'lere çıkmaktadır. Bu konuyla ilgili olarak yazılmış **“Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries”** makalesini indirip¹²⁸ okumanızı tavsiye ederim.

Tor'un böyle bir sorununu ortadan kaldırmak için **“traffic padding”**'i öneren kullanıcılar mevcut. Kısaca traffic padding'i anlatmak gerekirse; bir veri akışındaki paketlerinizi gizlemektir. Günümüzdeki problem basitçe şudur; X paketini gönderirken beraberinde Y paketini alıyorsunuz ve bu işlem devamlı birbiriyle bağlantılı haldedir. Bu veri transferleri her zaman ve gerçek trafiğinizin bir kısmını içeren verilere sahiptir. Traffic padding ise bu noktada devreye girer ve sahte veri yığını göndererek trafiğinizi izleyen 3. şahıslar için X paketi ile Y paketi arasındaki bağlantıyı kolayca anlayamamasını sağlar. Watermarking saldırıları, eğer trafik yapısına gömülmüşse, onun alıcısını eşsiz olarak tanımlar. Daha sonra ise bu alıcı ile orjinal gönderen de eşsiz olarak tanımlanır. Bu saldırının başarılı olabilmesi için de saldırganın potansiyel göndericiler ve alıcılardan oluşan veri akışını monitörlemesi ve sarsıma uğratması gerekir. Okumanız ve detaylı bilgileri almanız için **“Countering Repacketization Watermarking Attacks on Tor Network”** makalesini buradan¹²⁹ indirebilirsiniz.

128<http://www.cryptome.org/2013/08/tor-users-routed.pdf>

129<http://dj.eas.asu.edu/snac/document/Tor-watermarking-v1.pdf>

Traffic padding beraberinde çeşitli sıkıntıları da getirir:

- Sörf gibi, chat gibi low-latency¹³⁰ işlemleri için büyük bir yüküdür.
- Tahmin ettiği gibi çok büyük bir yardımı olmayabilir.

Burada belki i2p¹³¹ modeli işe yarayabilir. i2p'de herkes node'dur. Böylece kendi trafiğinizi sizin bilgisayarınıza gelen ve giden diğer trafik akışı içinde gizleyebilirsiniz. Açıkçası, Tor ve genel olarak bu durum gerçekten zor ve akademik düzeyde bir problemdir. Bir çözüm olarak, günümüz Internet'i yerine Meshnet¹³² gibi kendi internetimize ihtiyacımız vardır. Çünkü, şu anki Internet boğulma noktalarından devamlı izlendiği, takip edildiği, kaydedildiği ve kullanıcıları fişlediği için Tor gibi anonim network'lerin %100 başarılı olması zordur. Günümüz Internetinin trafik akışı çoklu sekmelerden ve her adımı kriptolanmış ve anonimleştirilmiş yollardan akmamaktadır.

Sonuca gelirse, günümüz Internet yapısının ve anlayışının değişmeye ihtiyacı var ve anonimlik, sizin kişisel tehlike modelinize dayanır; kimsiniz ve kimden saklanıyorsunuz, neden ve ne tür bir risk almayı hedefliyorsunuz. Anonimliğiniz ölçülebilir bir şeydir. Kullandığınız herhangi bir uygulama (*Tor, i2p v.d.*) size hiçbir zaman %100 anonimlik ver-e-mez. Bunların her zaman bilincinde olmanız gerekir.

130https://en.wikipedia.org/wiki/Low_latency

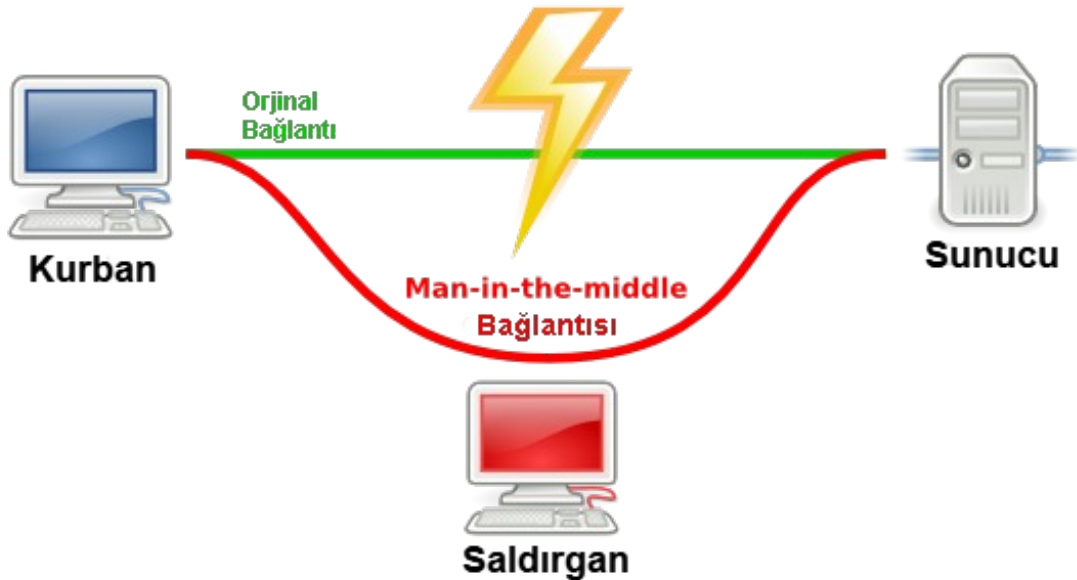
131<https://i2p2.de/>

132<https://wiki.projectmeshnet.org/>

16. SSL, Man In The Middle ve Turktrust

Wired'da¹³³ yayımlanan Law Enforcement Appliance Subverts SSL makalesinden¹³⁴ (haber mi deseydik?) sonra biraz geriye gidip makale üzerinden ve yakınlarda gerçekleşmiş TurkTrust'ın¹³⁵ hatalı sertifika üretimi üzerine enteresan bir benzerlikten bahsedeceğim.

Man in the middle attack nedir?



MitM saldırısı yapısı itibariyle aktif bir dinlemedir. Kurban ile sunucu arasındaki orjinal bağlantıya bağımsız bir bağlantı ile giren saldırgan, aslında kendi kontrolü altında bulunan iletişimi, kurbanı ve sunucu ile arasındaki iletişimin gizli ve sadece birbirleri arasında gerçekleştiğine inandırır. Tüm bu süreçte ise gönderilen ve alınan mesajlar saldırgan üzerinden gider. Daha iyi anlaşılabilmesi için

¹³³<http://www.wired.com/>

¹³⁴<http://www.wired.com/threatlevel/2010/03/packet-forensics/>

¹³⁵<http://turktrust.com.tr/>

wiki'de¹³⁶ bulunan çok güzel bir örnek üzerinden adım adım gidelim (şema Tails'tan alıntıdır¹³⁷):

1. Ali, hoşlandığı kız Ayşe'ye bir mesaj göndermek ve onunla pastanede buluşmak ister fakat aralarında bir üçüncü şahıs olan ve Ayşe'den hoşlanan ortak arkadaş Işık vardır ve ikisi de Işık'tan haberdar değildir;
2. Ali "Ayşe, ben Ali. Bana anahtarını ver."-> Işık Ayşe
3. Işık, Ali'nin gönderdiği bu mesajı Ayşe'ye yönlendirir fakat Ayşe bu mesajın Işık'tan geldiğini bilmez;
4. Ali Işık -> "Ayşe, ben Ali. Bana anahtarını ver." Ayşe
5. Ayşe anahtarı ile yanıt verir;
6. Ali Işık <- "Ayşe'nin anahtarı" Ayşe
7. Işık, Ayşe'nin anahtarını kendi anahtarı ile değiştirir ve mesajı Ali'ye yönlendirir;
8. Ali <- "Işık'ın anahtarı" Işık Ayşe
9. Ali, Ayşe'ye göndereceği mesajı Ayşe'nin sandığı anahtar ile şifreler ve Ayşe'ye gönderir;
10. Ali "Saat 22:00'da pastanede buluşalım(Işık'ın anahtarı ile şifrelenmiş)" -> Işık Ayşe
11. Anahtar aslında Işık'ın olduğu için, Işık mesajın şifresini kırar, içeriğini istediği gibi okur, eğer isterse mesajın içeriğini değiştirir, ve elinde bulunan Ayşe'nin anahtarı ile yeniden şifreler ve mesajı Ayşe'ye yönlendirir;
12. Ali Işık "Saat 22:00'da çorbacıda buluşalım(Ayşe'nin

136https://en.wikipedia.org/wiki/Man-in-the-middle_attack

137<https://tails.boum.org/doc/about/warning/index.en.html>

anahtarı ile şifrelenmiş)" -> Ayşe

13. Ayşe ise bunun Ali'den kendi anahtarı ile şifrelenmiş olarak ulaştığını düşünür. Garibim Ali saat 22:00'da pastanede
14. Ayşe'yi beklerken Ayşe ise Ali ile buluşacağını düşünüp saat 22:00'da çorbacıya, yani Işık'a gider.

SSL, bir kriptografik protokol olup, web trafiğini şifrelemek için kullanılmaktadır. Bu protokol sörf, e-posta, internet üzerinden fax ve VOIP gibi çok geniş çaplı uygulamaları kapsar ve yüksek düzeyde bir şifrelemedir. Tarayıcı ile sunucu arasındaki iletişim ve verinin yukarıda bahsettiğim şekilde dinlenilmesini önler. Hergün ziyaret ettiğiniz birçok site HTTP[S] kullanmaktadır. HTTP ise bu şifrelemeye sahip değildir, gönderilen mesajlar herkes (mesela İSS'niz, ağınızdaki başka bir şahıs) tarafından zorlanmadan okunabilmekte/dinlenebilmektedir.

Makaleye dönecek olursak, Packet Forensics isimli bir şirket bir kutu yapıyor ve bu kutu şifre kırmadan iletişimin arasına girerek gerçek SSL sertifikasını kendi oluşturduğu sahte SSL sertifikası ile değiştiriyor. Şirket sözcüsü Ray Saulino ise bu kutuyu kanun uygulayıcıları için yaptıklarını, Internette tartışıldığını ve çok özel bir şey olmadığını söylüyor. Bununla birlikte, TurkTurst firması 2013 yılı başında¹³⁸ 2 adet "hatalı" SSL sertifikası ürettiğini fark ediyor (konu ile ilgili ayrıntılı bilgi almak için bu yazıyı¹³⁹ okuyabilirsiniz!)

¹³⁸<https://blog.mozilla.org/security/2013/01/03/revoking-trust-in-two-turktrust-certificates/>

¹³⁹<http://www.sistemci.co/turk-guvenlik-rezaleti-turktrust/>

TurkTrust yapığı 4 Ocak 2013 tarihli¹⁴⁰ kamuoyu açıklamasında şöyle diyor:

“Yapılan incelemeler sonucunda, söz konusu hatalı üretimin sadece bir kez gerçekleştiğı, sistemlerimize herhangi bir müdahalenin söz konusu olmadığı, hatalı üretim sonucu ortaya çıkan bir zarar bulunmadığı tespit edilmiştir.”

Microsoft’un duyurusu:

“TURKTRUST Inc. incorrectly created two subsidiary CAs (.EGO.GOV.TR and e-islem.kktcmerkezbankasi.org). The *.EGO.GOV.TR subsidiary CA was then used to issue a fraudulent digital certificate to *.google.com. This fraudulent certificate could be used to spoof content, perform phishing attacks, or perform man-in-the-middle attacks against several Google web properties.”*

Microsoft, duyurusunda¹⁴¹ TurkTrust firmasının 2 tane hatalı sertifika oluşturduğunu (*.ego.gov.tr ve e-islem.kktcmerkezbankasi.org), bu hatalı sertifikanın çeşitli Google web özelliklerine karşı phishing ya da man in the middle saldırılarına neden olabileceğini söylüyor.

¹⁴⁰<http://www.turktrust.com.tr/kamuoyu-aciklamasi.1.html>

¹⁴¹<http://technet.microsoft.com/en-us/security/advisory/2798897#section1>

Microsoft çözümü:

“To help protect customers from the fraudulent use of this digital certificate, Microsoft is updating the Certificate Trust list (CTL) and is providing an update for all supported releases of Microsoft Windows that removes the trust of certificates that are causing this issue.”

Microsoft, kullanıcılarını bu sahte sertifikalardan koruyabilmek için bir yama yayımlamak zorunda kalıyor. Açık ve net olarak sahte sertifikadan kullanıcıların haberdar olmadığını (*muhtelemen man in the middle saldırısı ile ilişkili*), ve bunun için de kullandıkları hedef işletim sistemlerini güncellemelerini istiyor.

Mozilla'nın çözümü:

“Mozilla is actively revoking trust for the two mis-issued certificates which will be released to all supported versions of Firefox in the next update on Tuesday 8th January. We have also suspended inclusion of the “TÜRKRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. (c) Aralık 2007” root certificate, pending further review.”

Mozilla ise duyurusunda¹⁴² Firefox'un 8 Ocak Salı günü tüm desteklenen sürümleri için bu sertifikaları kaldıracıklarını ayrıca “Aralık 2007 tarihli” kök sertifikayı ise ileri bir inceleme için askıya alacaklarını söylüyor.

142<https://blog.mozilla.org/security/2013/01/03/revoking-trust-in-two-turktrust-certificates/>

Wired'in makalesinde geçen kısmı aynen buraya aktarıyorum:

"The boxes were designed to intercept those communications — without breaking the encryption — by using forged security certificates, instead of the real ones that websites use to verify secure connections."

Diyor ki; kutular, yukarıda da kısaca bahsettiğim gibi -şifreyi kırmadan- websitelerin güvenli bağlantıları onaylamak için kullandığı gerçek sertifikalar yerine, sahte güvenlik sertifikaları tarafından iletişimlerine müdahale etmek için tasarlanmıştır. Yani burada söz konusu olan saldırı "**man in the middle attack**"tır. Makalenin değindiği bir başka nokta ise daha da vahim bir şeyi ortaya çıkartıyor:

"To use the Packet Forensics box, a law enforcement or intelligence agency would have to install it inside an ISP, and persuade one of the Certificate Authorities — using money, blackmail or legal process — to issue a fake certificate for the targeted website. Then they could capture your username and password, and be able to see whatever transactions you make online."

Packet Forensics kutusunu kullanmak için mesela bir istihbarat servisinin (Türkiye için MİT diyelim) kutuyu İSS (mesela TTNNet) içine kurmalı, bir tane Sertifika Sağlayıcısı'nı (tesadüfe bakın, TurkTrust) para ile, şantajla ya da yasal bir süreçle hedef websitesi için sahte sertifika üretmesine ikna etmeli. Sonuçta ne oluyor, sizin çevrimiçi olarak yaptığımız işlemler görülebilir ve kullanıcı adınızla şifreniz elde edilebilir olacaktır.

Tabi ki yazından TurkTrust böyle bir şey yapmıştır sonucuna varılmamalı. Öncelikli olarak, Packet Forensics'in böyle bir kutu ürettiği, bu kutunun kullanıldığı ve kapalı kapılar ardında tanıtıldığı, kanun uygulayıcıları ya da istihbarat servislerinin hedef pazarları olduğu (*kim bilir başka kimler var?*) ve bunu pişkince söyleyebildikleridir. İkinci olarak, böyle bir kutunun kullandığınız ya da kullandığımız İSS tarafından “**kanun uygulayıcılarına**” ya da “**istihbarat servisine**” yardımcı olsun diye kurulup kullanıldığı ve bir SSL sertifika sağlayıcısının bir şekilde buna ortak edilebileceği olasılığıdır. Tüm bunlar “**olanaklı mıdır?**” sorusuna gelirsek (*TurkTrust'ı bunun dışında tutuyorum*); gönderdiğiniz bir e-postanın bir kopyasının aynı anda NSA sunucularında da yer alması, görüntülü konuşmaların simultane olarak NSA tarafından kaydedilmesi gibi uç örnekler, çok büyük boyutlardaki verinin NSA tarafından her yıl yedeklenmesi¹⁴³ gibi daha bir sürü örnek vereceğimiz şeylerin olması da çoğu insana olanaklı gözüküyordu.

Her şeyden önce (*bu örneğe istinaden*) deşifrelemek için uğraşmak yerine MitM (*kutunun yaptığı*) çok daha etkili bir sonuç verecektir. SSL sertifikasını kırmaya çalışmak yerine “**araya girmek**” ve akışa müdahale etmek çok daha basit ve hızlıdır. XKCD'nin şu karikatürü¹⁴⁴ ise çok güzel bir özet. Dahası, bir İSS düşünün, Phorm, DPI, Finfisher ve bilinmeyen bir sürü kötücül uygulamaya sahip ve (*gerçek olduğunu varsayarak*) böyle bir kutunun varlığından da bir şekilde haberdar, bunu mu kullanmayacak? Bir diğer nokta da, (bu akademik makaleye istinaden¹⁴⁵) diyelim ki devletin ve istihbarat servisiniz kapınızı

143<http://foxnewsinsider.com/2013/06/07/how-much-zettabyte-nsa-utah-facility-can-hold-immense-amount-data>

144<https://xkcd.com/538/>

145<http://cryptome.org/ssl-mitm.pdf>

çaldı ve sizden böyle bir şey istedi, kafa tutacak güce sahip misiniz?

Her geçen gün kişisel gizlilik haklarının yok sayıldığı, ihlal edildiği ve insan haklarına aykırı durumların çıktığı şu günlerde sizlere bol sabır dilerim.

17. Tor'a Giriş

Çok temel ve bir giriş yazısı olarak Tor'la ilgili yarım kalan bu yazıyı tamamlayayım istedim. Öncelike yazının ne son kullanıcıyı ne de ileri düzey kullanıcıyı tatmin etmek gibi bir amacı yok. Birçok şeyin gayet net, anlaşılır olduğunu düşünüyorum. Kullandığınız program vs. burada örnek verilmedi diye desteklenmediğini düşünmeyin. Bu yazı tamamen GNU/Linux temellidir.

Kısaca Tor Nedir?

Tor (*eski adıyla onion router*), ilk olarak Amerikan Donanması ile beraber¹⁴⁶, devlet içi iletişimlerini korumak için geliştirilmiştir. Günümüzde ise herkesin kullanabildiği (*aktivist, ordu, gazeteci, kanun uygulayıcı vs.*), sanal tünellerden oluşan, kişi ve grupların Internet üzerindeki gizliliklerini ve güvenliklerini sağlayan, geliştiren ve özgür yazılım olan bir anonimlik ağıdır.

Arkasında Kimler Var?

Sıklıkla raslatladığım ve çok eleştirilen -haklı- noktalardan biri de bu. Arkasında kimler var, kimler destekliyor, kim bunlar diyorsanız; Tor, senelik şeffaflık raporları yayımlıyor. Okumak isterseniz¹⁴⁷;

2012 yılı olağan raporu¹⁴⁸

2011 yılı finansal raporu¹⁴⁹

¹⁴⁶<http://www.onion-router.net/>

¹⁴⁷<https://www.torproject.org/about/financials.html.en>

¹⁴⁸<https://www.torproject.org/about/findoc/2012-TorProject-Annual-Report.pdf>

¹⁴⁹<https://www.torproject.org/about/findoc/2011-TorProject-Amended-Final-Report.pdf>

Baştan sona okumak isteyenlere, Tor and Financial Transparency¹⁵⁰ e-posta listesi tartışması var.

Bilindik isimlerden;

Jacob Applebaum¹⁵¹

EFF desteği (*tam destek olmasa da*) ve¹⁵²;

EFF¹⁵³ ile birlikte geliştirdikleri HTTPS-Everywhere¹⁵⁴ eklentisi.

Kaçamak cevap veriyorum gibi olmasın. Bu konudaki araştırmayı kullanacak insana bırakıyorum. Özellikle e-posta listesindeki tartışmadan ayrı birkaç yazı bile çıkabilir. Çok detaylı bilgiler içermekte.

150<https://lists.torproject.org/pipermail/tor-talk/2013-September/029744.html>

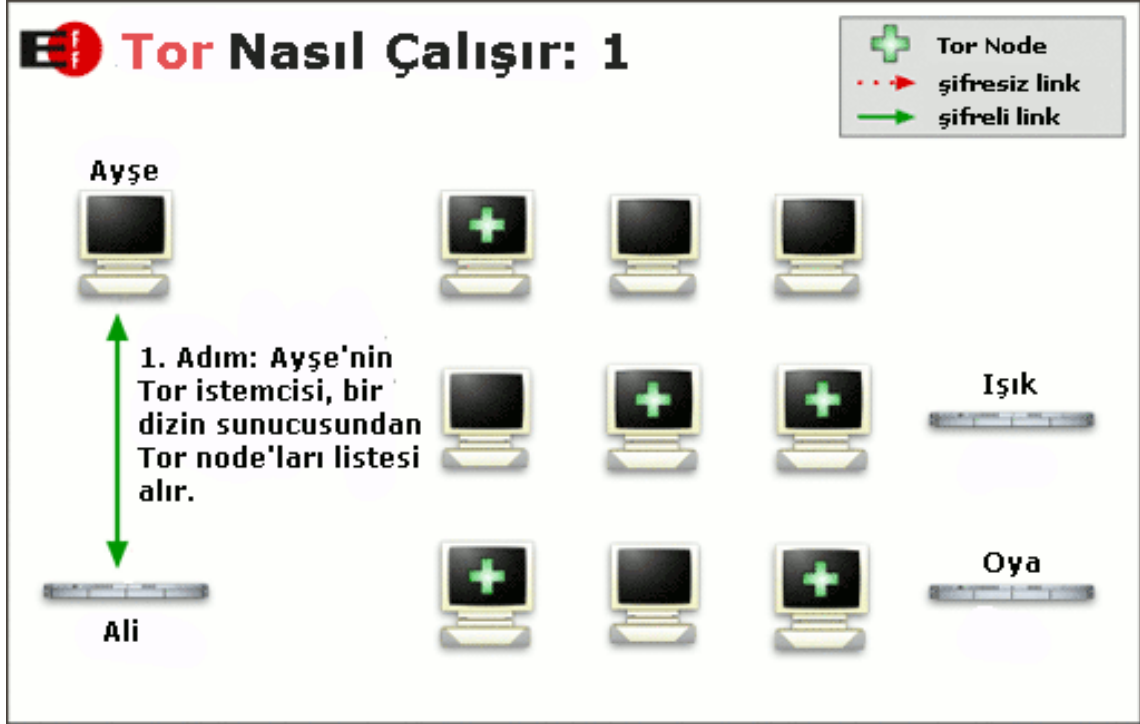
151<https://twitter.com/ioerror>

152[https://en.wikipedia.org/wiki/Tor_\(anonymity_network\)#Controversy_over_illegal_activities](https://en.wikipedia.org/wiki/Tor_(anonymity_network)#Controversy_over_illegal_activities)

153<https://www.eff.org/>

154<https://www.eff.org/https-everywhere>

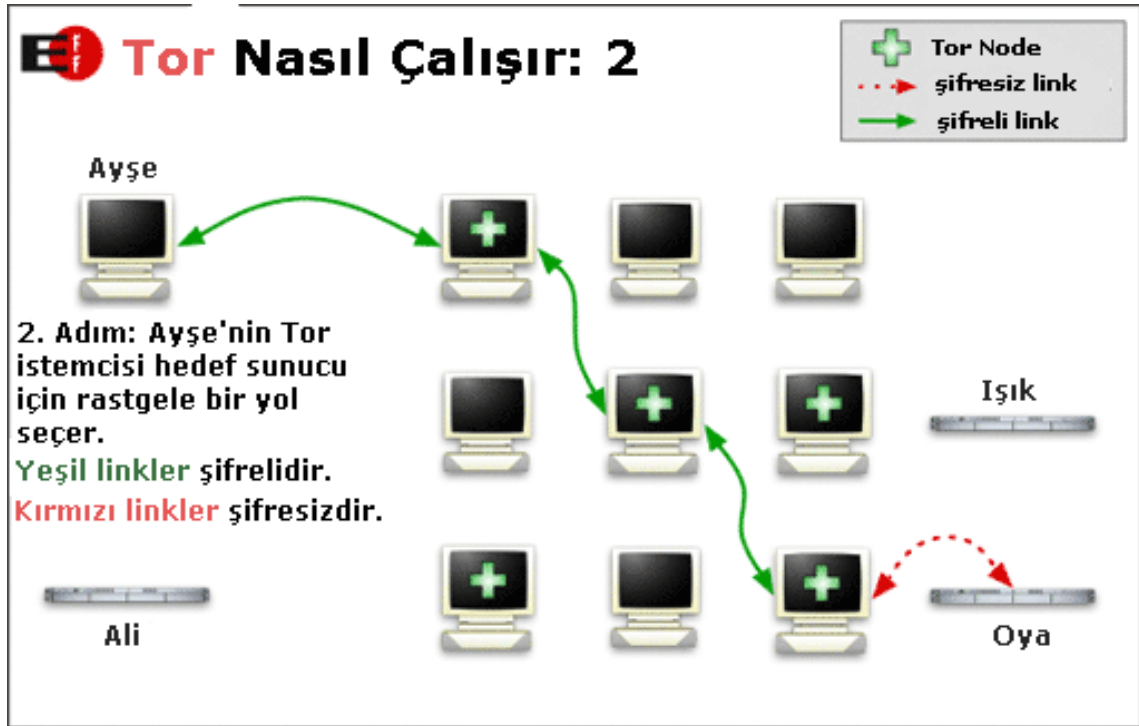
Tor Nasıl Çalışır?



İster basit, isterse karmaşık trafik analizi olsun, Tor; işlemlerinizi Internet üzerindeki birden fazla alana dağıtarak riski düşürmeye yardımcı olur. Temel fikir şudur; peşinizde sizi takip eden birini, dolambaçlı yollara sokarak hem takip edilmenizi engeller, hem de arkanızda bıraktığınız izleri (*fingerprint*) periyodik olarak temizlersiniz. Kaynaktan hedefe doğrudan bir yol seçmek yerine, Tor ağındaki veri paketleri birkaç relay üzerinde rastgele bir yol izler. Böylece, verinin nerden geldiği ve nereye gittiği belli olmaz. Sahip olduğunuz Tor istemcisi (Ayşe), dizin sunucusundan (Ali) şifreli bir bağlantı ile dolaşım oluşturacağı Tor node'larının listesini alır (bağlantıya şemada kısa olsun diye link dedim).

Bir örnek vererek kafanızda durumu daha da netleştirelim. Ayşe, elinde güvenli ara sokakların olduğu bir listeye (*Tor node*) onu

takip eden ailesine izini belli ettirmeden Oya'ya (*hedef sunucu*) gitmek ister.



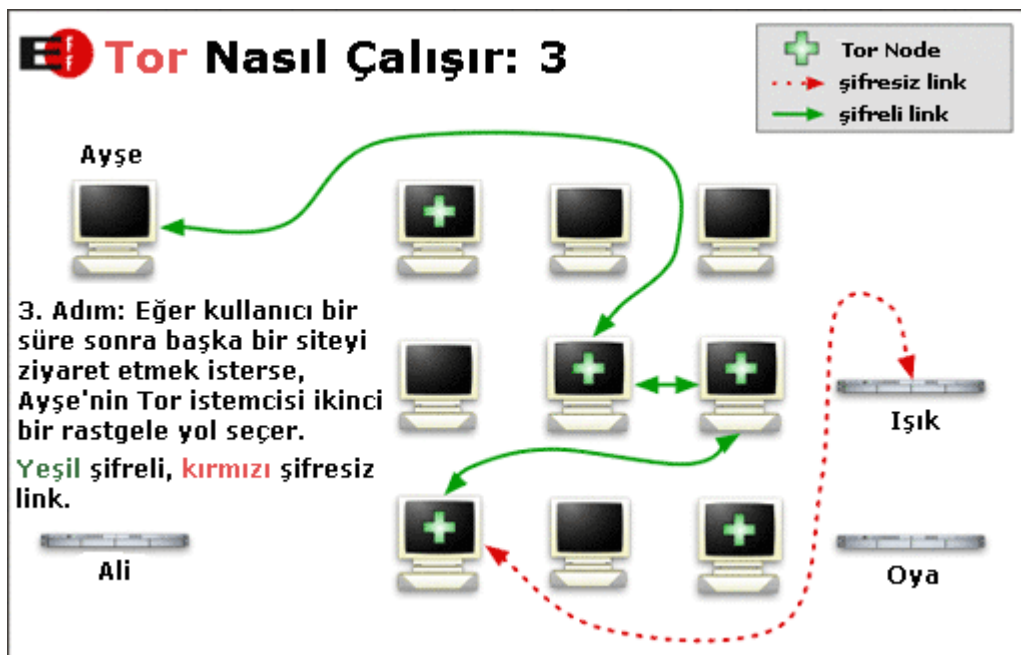
Tor; (*Ayşe'nin istemcisi*) ağ üzerinde bulunan relay'ler vasıtasıyla hedef sunucuya kadar şifreli bir dolaşım kurar. Dolaşım, her seferinde bir atlamaya (*Tor Node'lardaki yeşil linkler*) sahiptir, ve her relay sadece hangi relay'in kendisine veriyi verdiğini ve hangi relay'e vereceğini bilir. Relay'lerin hiçbiri bireysel olarak verinin aldığı tüm yolu bilemez. İstemci, dolaşım boyunca her atlamanın iletişimi takip edememesi için farklı anahtar setlerine sahiptir.

Örneğimize devam edelim; Ayşe, Oya'ya (*hedef sunucu*) ulaşabilmek için rastgele bir dolaşım yolu hazırlar (*circuit*) ve güvenli ara sokaklardan (*şifreli link*) sadece bir kez geçerek Oya'ya gider. Geçtiği ara sokaklar ise sadece hangi ara sokaktan geldiği ve

hangisine gittiğini bilir fakat tüm güzergahı bilemez ve ara sokakların hepsi farklı bir anahtar ile açılmaktadır.

Bu dolaşımdaki son relay, Exit Node olarak adlandırılır, ve hedef sunucuyla (*Oya*) asıl bağlantıyı kuran bu relay'dir. Tor'un kendisi, ve tasarım olarak da, Exit Node ile hedef sunucu arasındaki bu bağlantıyı (kırmızı) şifreleyemez. Bu şekildeki Exit Node'lar geçen her trafiği yakalayabilme durumundadırlar. Ayrıca, bu Exit Node'u çalıştıran kimse gelen ve giden verileri okuyabilir. İletişimlerin bu noktasında dinleme (*eavesdropping*) olabilmektedir. O yüzden devamlı "**end-to-end encryption**" kullanın diyoruz. Bu konuda da herkesi teşvik ediyoruz.

Örneğimize devam; son ara sokak (*Exit Node*) ile *Oya*'nın evi arasındaki yol açık bir yoldur ve bu yol istenirse son ara sokak tarafından izlenebilir, hatta *Ayşe*'nin ailesine (eğer kötücül ise) bile bilgi verebilir veyahut kızınız şuraya kaçtı diyerek polisi arayabilir.



Tor, daha etkili olabilmek için aynı dolaşımı yaklaşık 10 dakika boyunca kullanır. Sonraki istekler, mesela yeni bir websiteyi ziyaret etmek isterseniz (*Işık*) ise yeni bir dolaşım üzerinden yapılır. Böylece, bir önceki dolaşım ile yaptıklarınızı yenisiyle ilişkilendirmek isteyenleri engellemiş olur (*şemalar ve açıklamalar Tor'dan*¹⁵⁵, *dinleme ise Tails'tan alıntıdır*¹⁵⁶). Son olarak, Tor sadece TCP'den ve SOCKS desteği olan uygulamalarda kullanılabilir (*SOCKS desteği yoksa Polipo kısmına bakın*).

Örneğimizi bitirelim; Ayşe, eğer bir süre sonra fikrini değiştirir ve Oya'ya değil de Işık'a (*farklı hedef sunucu*) gitmek isterse, bu sefer de farklı güvenli ara sokaklardan (*Tor Node*) oluşan bir dolaşım yolu hazırlar ve izini belli ettirmeden Işık'a (*hedef sunucu*) gider.

Tor'u, dağıtımınızı bilmediğim için nasıl kuracağınızı yazmıyorum. Paket yöneticinizden tek bir komutla ve tıklamaya kurabilirsiniz. Basit bir örnek vermem gerekirse;

```
apt-get install tor  
pacman -S tor
```

Eğer grafik arayüzlü bir Tor kontrolcüsü isterseniz Vidalia'yı¹⁵⁷ da kurabilirsiniz. Vidalia; Tor'u başlatıp durdurmaya, ne kadar bandwidth harcadığınızı, aktif olarak hangi dolaşıma sahip olduğunuzu, bu dolaşımı harita üzerinde göstererek Tor'un durumuyla ilgili mesajlar yayımlar ve sizlere basit bir arayüz

¹⁵⁵<https://www.torproject.org/about/overview.html.en>

¹⁵⁶<https://tails.boum.org/doc/about/warning/index.en.html#index1h1>

¹⁵⁷<https://www.torproject.org/projects/vidalia.html.en>

üzerinden Tor'u ayarlamana, köprü, ve relay oluşturmanıza olanak verir.

Temel Tor Ayarları

Dağıtımınız ne olursa olsun (*Debian¹⁵⁸, Arch¹⁵⁹, Gentoo¹⁶⁰, Ubuntu¹⁶¹ denediklerim*) Tor kurulumunda kendi basit ayarlarıyla (*dağıtıma da özgü olarak*) geliyor. Bu ayarlar da Tor'un gayet güvenli ve sorunsuz çalışmasını sağlıyor. Bu arada, servis olarak çalıştırmayı unutmayın. Yukarıda da belirttiğim üzere eğer Exit Node'larının bazılarında bir dinleme varsa, veya gizli servislerin veri örnekleri aldıkları Exit Node'lar varsa Tor buna engel olamaz (*HTTPS kullanın!*). Belki güvendiğiniz ya da bildiğiniz Exit Node fingerprint'lerine sahipseniz sadece bunları kullanmasını da ayarlar üzerinden sağlayabilirsiniz (*ama uzun vadede kimliğinizin bulunmasını kolaylaştırabilir*). Farklı bir port (9050, *Vidalia için 9051*) kullanmadığınızı varsayarsak basitçe (*örnektir*) Firefox'u şu şekilde ayarlayabilirsiniz;

Seçenekler -> Gelişmiş -> Ağ -> Ayarlar -> Vekil sunucuyu elle ayarla

SOCKS = 127.0.0.1

Port = 9050 (9051)

158<https://debian.org/>

159<https://archlinux.org/>

160<https://gentoo.org/>

161<https://ubuntu.com/>

Tor Browser Bundle¹⁶² varken Firefox veya başka bir tarayıcı kullanmak mantıklı mıdır? Bana sorarsanız, Tor'u kullandığınız tarayıcı ile (*ya da TBB*) normal olarak kullandığınız tarayıcıyı ayrı tutarsanız daha mantıklı olacaktır. Ayrıca, tarayıcınız ile ilgili test yapmak isterseniz, Panoptick¹⁶³ ve JonDonym¹⁶⁴ var. Tarayıcınızı TBB ile kıyaslarsanız, biraz fikir sahibi olabilirsiniz.

Tor Ve Polipo

Polipo¹⁶⁵, basit ve hızlı bir web cache, HTTP proxy ve proxy sunucusudur. Kullanım ve ayarları gayet basit, özellikle Privoxy ile kıyaslarsak, ondan çok daha hızlıdır. Polipo'nun tek sıkıntısı disk önbelleğini herhangi bir kısıtlama yapmadan devamlı olarak arttırmasıdır. Harddisk dolmaya başladığında burayı bir kontrol ederseniz iyi olur.

“/etc/polipo/config” ayar dosyası (örnek);

```
daemonise=false
```

```
diskCacheRoot=/var/cache/polipo/
```

```
proxyAddress=127.0.0.1
```

```
proxyName=localhost
```

```
serverSlots=4
```

```
serverMaxSlots=8
```

```
cacheIsShared=true
```

```
allowedClients=127.0.0.1
```

162<https://www.torproject.org/projects/torbrowser.html.en>

163<https://panoptick.eff.org/>

164<http://ip-check.info/?lang=en>

165<http://www.pps.jussieu.fr/~jch/software/polipo/>

```
socksParentProxy = localhost:9050  
socksProxyType = socks5
```

http-proxy'yi localhost:8123 üzerinden kullanabilirsiniz. Polipo'yu sadece SOCKS desteklemeyen bir uygulamanız varsa (mesela Uzbl, Dwb gibi tarayıcılar) kullanmanız tavsiye. Diğer durumlarda SOCKS üzerinden sadece Tor'u kullanın.

Tor Ve Freenode (IRC)

Eğer Freenode'a¹⁶⁶ (*OFTC'de¹⁶⁷ ekstra bir ayara gerek yok!*) Tor üzerinden bağlanmak isterseniz (*bu örnek Weechat¹⁶⁸ için*);

```
/proxy add tor socks5 127.0.0.1 9050  
/server add freenode-tor p4fsi4ockecnea7l.onion  
/set irc.server.freenode-tor.proxy "tor"  
/set irc.server.freenode-tor.sasl_mechanism dh-blowfish  
/set irc.server.freenode-tor.sasl_username "kullanıcı adınız"  
/set irc.server.freenode-tor.sasl_password "şifreniz"  
/set irc.server.freenode-tor.nicks "kullanıcı adınız"  
/connect freenode-tor
```

¹⁶⁶<http://freenode.net/>

¹⁶⁷<http://www.oftc.net/>

¹⁶⁸<http://www.weechat.org/>

Tor Ve Pidgin

Eğer Pidgin'de herhangi bir servise Tor üzerinden bağlanmak isterseniz (*Hepsini denemeyin bence, desteleyen Jabber sunucuları için yapabilirsiniz örneğin.*);

Ayarlar -> Proxy

Proxy türü SOCKS5

Host 127.0.0.1

Port 9050

Bunun yanında bence OTR eklentisi de kurulabilir. OTR'de dikkat etmeniz gereken şeylerden birincisi iletişimde bulunan her iki tarafta da OTR eklentisi kurulu olmalıdır. Bir diğer şey de siz ve karşı taraf log tutmasın, gerekirse karşı taraftan bunu rica edin.

Tor Çalışıyor Mu?

Test etmek istiyorsanız; <https://check.torproject.org>

Hidden Services

Deep web¹⁶⁹, dark internet, Internetin karanlık yüzü, buz dağının görünmeyen kısmı gibi bir sürü tamlama yapıp çok detaya girmeyi pek planmadığım bir nokta. Tor kullanıcısı şunun her zaman bilincinde olmalı; Tor'u neden kullanıyor, nerede kullanıyor? Bu sorular doğrultusunda hidden services¹⁷⁰ profillerinizi clear web üzerinde kesinlikle ilişki kurulabilecek şekilde bağlamayın.

¹⁶⁹https://en.wikipedia.org/wiki/Deep_Web

¹⁷⁰https://en.wikipedia.org/wiki/List_of_Tor_hidden_services

Javascript'i deep web'de kapatın¹⁷¹. Freedom Hosting'in FBI baskınından sonra¹⁷² sunucuları gittiği için gördüğünüz sadece %50'sidir. Hidden services'ten bir şeyler indirecek ya da yükleyecekseniz bunu iş yerinizden yapmamanız tavsiyedir.

Dikkat Edilmesi Gereken Birkaç Nokta

Tarayıcınızın bir parmakizi (fingerprint)'i vardır, kullandığınız her şeyin kendine özgü ve “**eşsiz**” fingerprint'leri vardır. Şöyle bir örnek vereyim sizlere; kullandığınız tarayıcıyı tam ekran kullanmanız, onun araç çubuğunun boyutu ile ilgili eşsiz bir bilgi sızdırabilir ve ziyaret ettiğiniz siteye sizinle birlikte görüntüleyen diğer tarayıcılar arasında farklı bir konuma düşebilir. Bu da sizin gerçek kimliğinizin ortaya çıkmasını kolaylaştırır. Dahası, günümüzdeki çöznürlükler dikkate alındığında bu ayırım giderek belirginleşmektedir. Bu yüzden TBB, tarayıcı tam ekran yapıldığında kullanıcılarını uyararak için bir uyarı mesajı tasarlamaktadır¹⁷³.

Bir diğer nokta, diyelim ki sizler Internette flash video izliyorsunuz ve bir yandan da bunun için Tor kullanıyorsunuz (*pornocular dikkat*). Hiçbir çerez tutmayın, geçmişi silin, ne yaparsanız yapın webgl (*HTML5'te de bu durum vardı ne oldu son durum bilmiyorum.*) sizin ekran kartı bilginizi cache'leyecektir. Yani Büyük Birader sizleri evinizde ziyaret etmek isterse o ekran kartı benim değil deme şansınız var mı?

171<https://blog.torproject.org/blog/hidden-services-current-events-and-freedom-hosting>

172<https://openwatch.net/i/200/>

173<https://trac.torproject.org/projects/tor/ticket/7255>

Son Sözlür

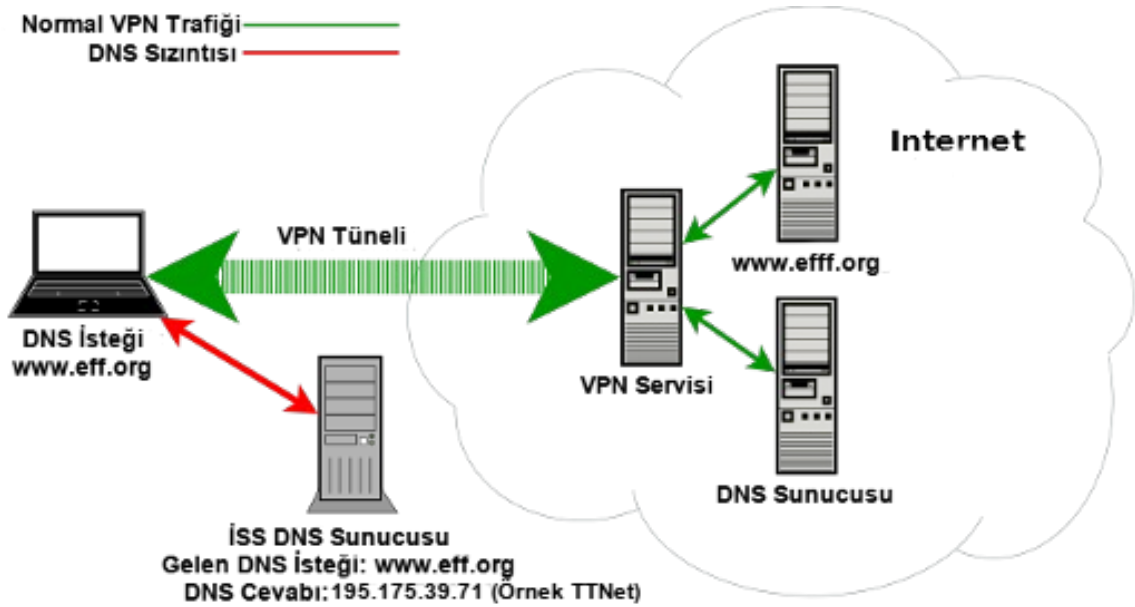
Daha önce söylemişim¹⁷⁴ ama yinelemekte fayda var. Anonimliğiniz sizin kişisel tehlike modelinize dayanır. Kimsiniz ve kimden saklanıyorsunuz? Neden ve ne tür bir risk almayı hedefliyorsunuz? Öncelikli olarak sizin cevaplamanız gereken soruların başında bu gelmektedir. Bir diğer durum da Tor, anonim olmayan bir İnternet üzerinde kendi anonim ağını oluşturmaya çalışmaktadır. Burada %100 bir sonuç alma ihtimaliniz yoktur. Gmail gibi servislere Tor üzerinden girmeniz pek mantıklı olmayacaktır (*şifre yenileme talebi gönderecek*). Torrent için kullanmayın (*yavaş ve bilgi sızdırabilir*). Eğer kullandığınız servis Tor'u desteklemiyorsa ya da kara listeye almışsa ısrarla Tor'la bağlanmayı denemeyin. Sonun sonu, gerçek kimliğinizle (*mesela Facebook profiliniz*) Tor üzerinden oluşturacağınız herhangi bir profil (*mesela Twitter'daki takma adlı profiliniz*) arasında ilişki kuracak/kurduracak (*Twitter'ı Facebook profili ile ilişkilendirmek*) hatalar yapmayın.

174<https://network23.org/kame/2013/09/28/tor-ve-gunumuz-interneti/>

18. DNS Leak Tehlikesi

Kullandığımız anonim ağlara ya da VPN tünellerine aldanıp anonim olduğumuzu zannederken, aslında tüm Internet aktivitelerimizin İSS tarafından rahatça izlenip kaydedilebilmesi, bir DNS sızıntısı ile o kadar kolay ki.

DNS Sızıntısı (Leak) Nedir?



Anonim bir ağ ya da VPN servisi kullandığınız zaman, bilgisayarınızdan geçen tüm trafiğin bu anonim ağ ya da servis üzerinden güvenli bir şekilde gönderildiği varsayılır. Tor veya VPN kullanmanızdaki temel neden, trafiğinizi İSS'nizden ve diğer üçüncü kişilerden gizlemek, anonimliğinizi arttırmaktır. Fakat bazı durumlar vardır ki, siz güvenli bir VPN bağlantısı kurduğunuzu düşünseniz bile, İSS'niz Internet trafiğinizi izleyebilir ve çevrimiçi aktivitelerinizi monitörleyebilir. Yani, bir nedenle sorgularınız VPN bağlantınız ya da anonim ağ yerine İSS'nizin DNS sunucularına da yönlenebiliyor,

burada bir DNS sızıntısı (*leak*) var demektir. Şema üzerinden anlatırsak; bir VPN tüneline sahipsiniz ve EFF¹⁷⁵ için bir sorguda bulundunuz. Normal olarak sorgunuz tünelden VPN servisine, VPN servisinin DNS sunucusu ve oradan da EFF'ye ulaşmalı. Fakat, sorgunuza İSS'niz DNS sunucusu da cevap vermektedir. Bu da şu anlama gelmektedir; İSS'niz İnternet aktivitelerinizi bir bir kaydetmekte, sizleri rahatça izlemektedir.

Anonimliği tehdit eden en büyük tehlikelerden biri DNS sızıntısıdır. Çünkü, anonim bir ağa bağlı olsanız bile (*mesela Tor*¹⁷⁶), işletim sisteminiz anonim servis tarafından atanan anonim DNS sunucuları yerine kendi varsayılan sunucularını kullanmaya devam etmektedir. Bu da kullanıcılara sahte gizlilik hissi vermekte ve sonuçları üzücü olmaktadır.

Etkilenenler;

- VPN sunucuları
- Socks proxyleri (Tor gibi)

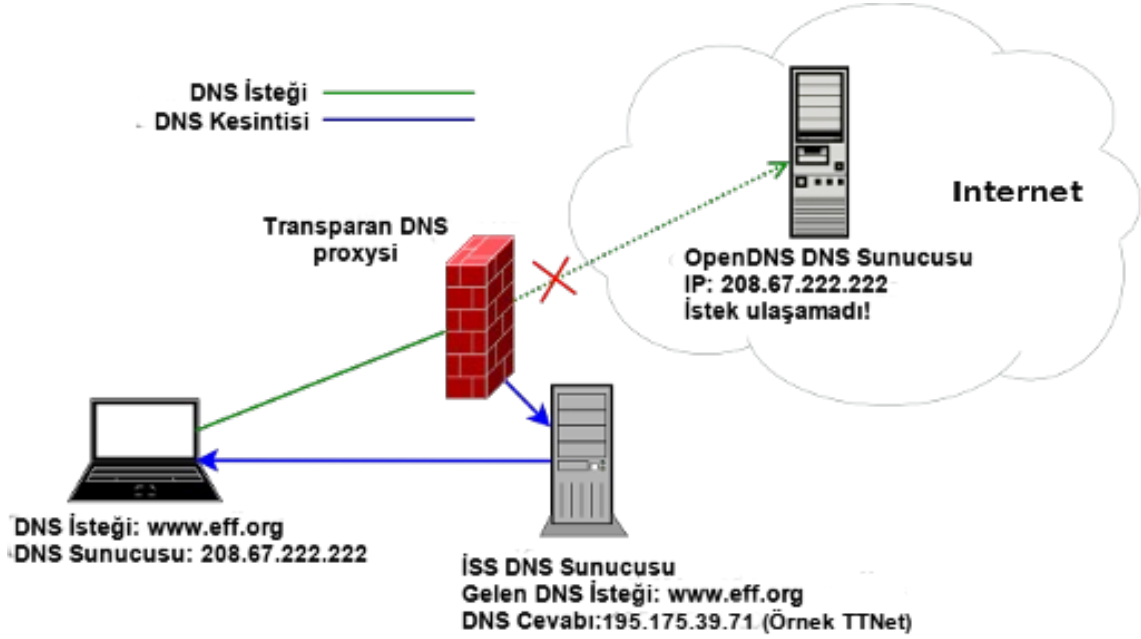
Etkilenmeyenler;

- CGI Proxyleri
- SSH tünel ile HTTP proxyleri

175<https://eff.org/>

176https://trac.torproject.org/projects/tor/wiki/doc/Preventing_Tor_DNS_Leaks

Transparan DNS Proxyleri



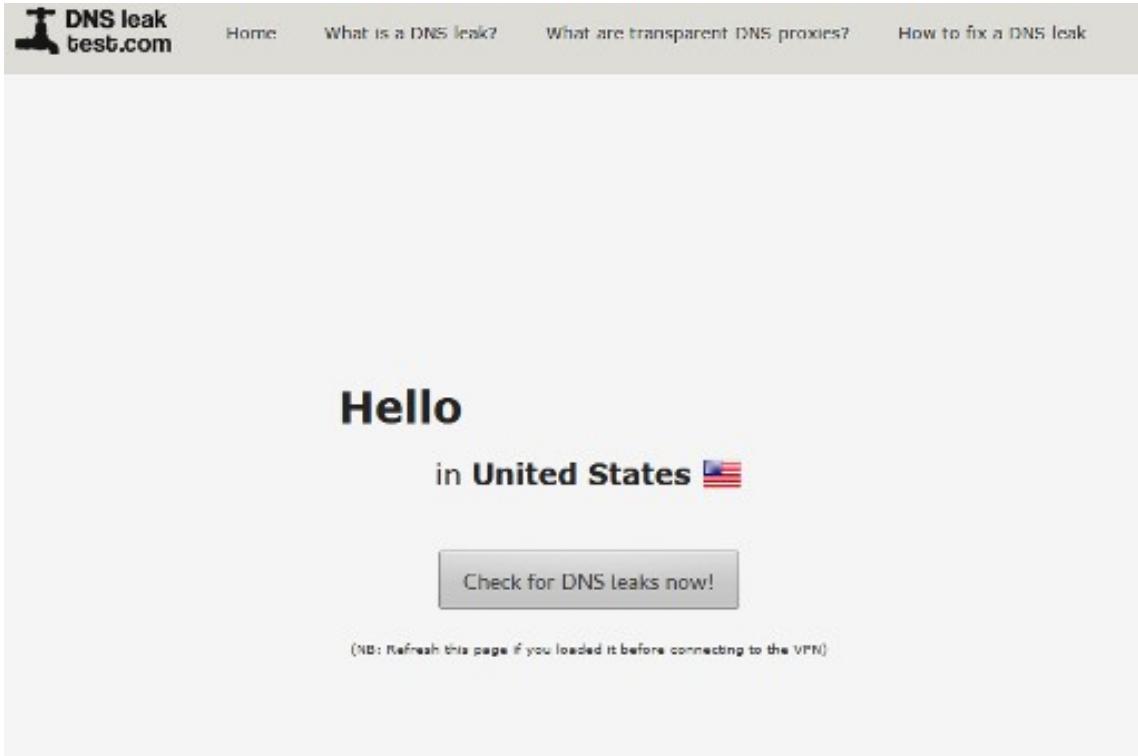
Günümüzde bazı İSS'lerin Transparan DNS Proxyleri adında bir teknoloji kullandığı bilinmektedir. Bu şu işe yarıyor; siz eğer bir DNS sorgusu yaparsanız, İSS bunu sadece kendi DNS'leri üzerinden (*TCP/UDP port 53*) yapılmaya zorluyor. Bir örnek vererek anlatalım. Siz DNS sunucusu olarak OpenDNS'i¹⁷⁷ kullanmaktasınız ve EFF için bir sorgu yapacaksınız. Transparan DNS Proxyleri sizin isteğiniz OpenDNS sunucularına ulaşmadan araya girip akışı keserek İSS'nin kendi DNS sunucusuna yönlendirmekte ve OpenDNS sunucusu yerine İSS DNS sunucusu cevap vermektedir. Siz tabi bu noktada **"Ben VPN kullanıyorum, güvendedim."** veya **"Tor kullanıyorum, güvendedim."** diyebilirsiniz. Fakat, sonuçlar sizin beklediğiniz yönde gerçekleşmemektedir (şemalar DNS leak test'ten alıntıdır¹⁷⁸).

¹⁷⁷<http://www.opendns.com/>

¹⁷⁸<https://dnsleaktest.com/>

Tehlikenin Boyutlarına Dair

Bir tehlike modeli üzerinde (Modeller çoğaltılabilir. Mesela ücretsiz anonim socks proxyler üzerinden modeller oluşturulabilir, denemesi size kalmış.) sizlere DNS sızıntısı göstereyim. Modelimiz şu; Amerika lokasyonlu bir VPN servisi kullanıldığınızı düşünün. Ayrıca tarayıcınız da Tor üzerinden internete (*exit-node da Amerika'da*) girdiği farzedilmekte. Fakat, dinamik ip kullanmaktasınız ve özel bir DNS ayarına sahip değilsiniz;



Tor veya VPN servisinizin DNS sunucularını görmeniz (*görmezseniz daha iyi*) doğal olarak beklenendir. Sizin tek görmek istemeyeceğiniz şey ise, trafiğinizi ondan gizlediğinizi sandığınızı İSS'niz olacaktır. Fakat, sonuca bakarsak;





DNS leak testb.com Home What is a DNS leak? What are transparent DNS proxies? How to fix a DNS leak

Your DNS test results

This page shows the DNS servers that your computer is using to resolve DNS names. **The owners of the servers listed below have the ability to log the names of all websites you connect to.**

WARNING: If you are connected to a VPN service and ANY of the servers listed below are not provided by the VPN service then your DNS may be leaking. (You should be able to recognise them based on the hostname, ISP and location). This is not an issue if you trust the owners of these servers with your private data.

We detected the 4 DNS servers listed below.

<p>IP:</p> <p>Hostname:</p> <p>ISP:</p> <p>Country: United States </p>	VPN Servisi
<p>IP: 195.175.39.71</p> <p>Hostname: 195.175.39.71.static.turktelekom.com.tr</p> <p>ISP: Turk Telekom</p> <p>Country: Turkey </p>	
<p>IP: 195.175.39.75</p> <p>Hostname: 195.175.39.75.static.turktelekom.com.tr</p> <p>ISP: Turk Telekom</p> <p>Country: Turkey </p>	İSS
<p>IP: 195.175.39.74</p> <p>Hostname: 195.175.39.74.static.turktelekom.com.tr</p> <p>ISP: Turk Telekom</p> <p>Country: Turkey </p>	

Tam bir facia! En üstte VPN servisinizi görüyorsunuz. Daha da kötüsü, siz Tor kullanmanıza ve VPN tüneli oluşturmanıza rağmen, ve tüm bunların üzerine kendinizi tamamen güvende (*tamamen olmasa da bir nebze*) hissederken, farkında olmadığınız bir DNS sızıntısına sahipsiniz. Diğer enteresan nokta, Firefox, socks proxy (*Tor*) yerine işletim sisteminin bağlı olduğu ağ (*İSS*) üzerinden DNS sorgusu gerçekleştirip, Tor'ü tamamen atlamış. Tabi burada benim aklımı daha çok kurcayalayan şey, TNet'in ya da Türkiye'de hizmet veren

herhangi bir İSS'nin transparan dns proxysine ya da proxlerine sahip olup olmadığı. Gerçi, TNet pişkin pişkin Phorm¹⁷⁹ kullanmaya devam edip ve DPI ile paket analizlerine dalmış olduğu için bunu sormak (*gene de şunda veya bunda vardır diyemiyorum*) abesle işigaldir.

DNS Sızıntı Testi

Böyle bir durumla karşıya karşıya olup olmadığınızı anlamak için;

- DNS Leak Test: <https://www.dnsleaktest.com>
- IP Leak: <http://ipleak.net/>

İSS'nin DNS Gaspı (Ekleme: 19.11.2013)

Buradaki işlemleri terminalden gerçekleştireceğiz. Önce, varolmayan bir domain adresine ping atalım;

```
kame $ % ping yokboylebirdomain.ltd
PING yokboylebirdomain.tld (195.175.39.75): 56 data bytes
64 bytes from 195.175.39.75: icmp_seq=0 ttl=236 time=336 ms
64 bytes from 195.175.39.75: icmp_seq=1 ttl=236 time=292 ms
64 bytes from 195.175.39.75: icmp_seq=2 ttl=236 time=274 ms
```

İşte aradığımız! Var olmayan bir domain'e 195.175.39.75 IP'si üzerinden yanıt geliyor. Yani İSS'niz (örnekte gerçek) sahte bir adres üzerinden sorgularınıza yanıt veriyor.

¹⁷⁹<http://enphormasyon.org/>


```
kame $ % nslookup yokboylebirdomain.tld
```

```
Server: 192.168.2.1
```

```
Address: 192.168.2.1#53
```

```
Non-authoritative answer:
```

```
Name: yokboylebirdomain.tld
```

```
Address: 195.175.39.75
```

```
Name: yokboylebirdomain.tld
```

```
Address: 195.175.39.71
```

Sahte IP'yi sonunda yakaladık; 195.175.39.71!

Ne Yapmalı?

Öncelikle, testi yaptığınızı ve kötü sonuçla karşılaştığınızı varsayarak; bir, statik ip ayarını yapmayı öğrenin. İnternette bununla ilgili girilmiş tonlarca yazı, alınmış ekran görüntüsü ve nasıl yapacağınızı anlatan videolar bulunmakta. Bir aramanıza bakar. Hangi işletim sistemini kullanırsanız kullanın, bunu yapın.

İki, iyi bir DNS servisi bulun. Benim bu konudaki önerim aşağıda. Eğer, sizin farklı görüşleriniz varsa, ben sadece Google DNS'i kullanmamanızı tavsiye ederim. Onun yerine OpenDNS'i¹⁸⁰ gönül rahatlığıyla (*dediğime pişman olmam umarım*) kullanın, kullandırım.

¹⁸⁰<http://www.opendns.com/>

Üç, Firefox'unuzu aşağıda anlattığım şekilde ayarlayabilirsiniz. Ayrıca, kötü bir VPN servisi kullanmayın, para veriyorsanız da paranızı ziyan etmeyin.

Dört, eğer Windows kullanıyorsanız, öncelikle Torero'yu Windows cmd üzerinden kapatın (*netsh interface teredo set state disabled*). İyi bir firewall kurabilirsiniz. Son olarak, DNS Leak Test'in şu önerilerini¹⁸¹ uygulayın.

Beş, GNU/Linux'ta alternatif olarak Polipo¹⁸² kurup kullanabilirsiniz.

Altı, Dnscrypt¹⁸³ kurup kullanabilirsiniz (*Platform bağımsız!*).

Hangi DNS Servisi?

Ben OpenNIC Project'in DNS sunucularını kullanmaktayım. Beni kullanmaya iten en önemli ayrıntısı, ücretsiz, sunucuların kayıtlarını bir süre sonra (*saatte bir, 24 saatte bir ya da hiç tutmayarak*) silmesi (*anonimleştirmesi*), birçok ülkeden, istediğiniz DNS sunucusunu kullanmanıza olanak vermesi. Şimdilik, sicili gayet temiz ve sunucuları da performans olarak üzmecek düzeyde.

Firefox Ayarı

Firefox'ta bu dertten kolayca kurtulmak isterseniz eğer, adres çubuğuna **about:config** yazarak Firefox'un ayarlarını açabilirsiniz.

181<https://www.dnsleaktest.com/how-to-fix-a-dns-leak.php>

182<http://www.pps.univ-paris-diderot.fr/~jch/software/polipo/>

183<http://dnscrypt.org/>

Açtıktan sonra; **network.proxy.socks_remote_dns** bulun ve onu **true** yapın. Böylece Firefox bağlı olduğu ağ üzerinden değil socks proxy üzerinden (*ayarladıysanız Tor*) DNS sorgusu yapacaktır. Eğer kullandığınız uygulamalar DNS ön yüklemesi yapıyorsa, ayarlarında DNSPrefetch var mı yok bu bir bakın. Firefox için `network.dns.disablePrefetch` bulun ve true yapın.

Sonuç

DNS sızıntısı basit ve küçümsenecek bir durum değildir. Bunu iyice anlamak lazım. Bir diğer nokta da, “**ben Tor’la yasaklı siteye girebiliyorsam nasıl isteğim İSS’me gitsin?**” sorusu. Burada bir hataya düşüyorsunuz; Tor’la siteye girmek farklı bir şeydir, siteye girmek için gönderdiğiniz isteğin aynı anda İSS’nize de gitmesi (*İSS üzerinden girmesiniz dahi*) farklı bir şeydir. Sizin kaçınmanız gereken, konunun da özü, isteğin İSS’nin DNS sunucularına da gitmesi. “**Onu kullanmayı bilen zaten şunu da ayarlar.**” yanlış bir bakış açısidir. Ayarladığınızı zannedersiniz, güncellersiniz ayarlarınız sıfırlanır, değişir, “**VPN kullanıyorum ya, n’olcak.**” dersiniz, böyle bir olasılıktan haberdar değilsinizdir ya da iyi bir tehlike modeliniz yoktur, zor duruma düşersiniz.

Anonimlik sizin tehlike modelinize dayanır ve anonimlik düzeyiniz ölçülebilir (*bunu her yazımda tekrarlayacağım*). Bunun bilincinde olun!

19. Ccrypt ile Şifreleme

Platform bağımsız ve kullanması kolay bir uygulama olarak, ccrypt, dosya şifrelemede kullanmak için gayet basit ve güvenli, ayrıca sistem kaynaklarını da bir o kadar az tüketen bir araç olarak durmakta. Bu basit rehberi en azından denemeniz ve hatta kalıcı olarak kurup kullanmanız için hazırladım.

ccrypt¹⁸⁴, dosyaları şifrelemek ve şifresini çözmek için kullanılan, Rijndael Blok Şifresi üzerine kurulu açık kaynak, özgür yazılım bir uygulamadır. ccrypt'in sahip olduğu algoritma simetrik değildir. Bununla birlikte, ccencrypt ile dosya şifrelerken ccdecrypt ile şifre çözemektedir (*ccrypt -e ya da ccrypt -d ile de yapabilirsiniz*). Ayrıca ccat ile şifresiniz çözdüğünüz dosyayı sadece terminal ekranına yazdırabilir ve bilgisayarınızda geçici dosyalar bırakma riskinizi düşürebilirsiniz.

ccrypt güvenliği

ccrypt 256-bitlik bir şifrelemeye sahiptir. AES'in de seçtiği Rijndael Blok Şifresi'ni¹⁸⁵ kullanmaktadır. ccrypt'in AES ile farkı ise, AES 128-bit blok boyutu kullanırken kullanırken, ccrypt, Rijndael'in izin verdiği 256-bit blok boyutu kullanmaktadır. Bu onu elbette AES'ten daha az güvenli yapmamaktadır. Sadece AES standartına sahip değildir. Ayrıca, bu şifreleme eğer kırılırsa duyulması da o kadar çabuk olacaktır.

184<http://ccrypt.sourceforge.net/>

185<http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf>

ccrypt ile bir dosyayı şifrelerseniz eğer, ccrypt o dosyanın üzerine yazacak, yeni bir dosya oluşturmayacaktır. Bununla birlikte, artık harddiskinizde orjinal dosya olmayacaktır. Fakat, siz bu dosyayı silseniz dahi donanım ataklarında harddiskiniz/ram'iniz/takasınız bu dosyanın izini taşıyabilir. Eğer bu izleri silmek isterseniz, bunun için çeşitli araçlar mevcut. Bunlardan bir tanesi GNU/Linux için wipe¹⁸⁶.

Eğer, şifreleme esnasında “-tmpfiles” parametresi kullanırsanız, orjinal dosyanın üzerine yazmak yerine geçici bir dosya oluşturabilir, ardından da wipe ile silebilirsiniz.

```
kame ~ % ccencrypt --tmpfiles sifrelenecekdosya && ls
sifrelenecekdosya
sifrelenecekdosya.cpt
```

Dosya ve izin şifreleme, şifre çözme

ccrypt ile herhangi bir dosyayı sorunsuz bir şekilde şifreleyebilirsiniz. Fakat, sizinleri şifreleyemezsiniz. Dizin için farklı bir yol izleyeceğiz.

Dosya şifreleme;

```
kame ~ % ccencrypt sifrelenecekdosya
Enter encryption key:
Enter encryption key: (repeat)
```

186<http://wipe.sourceforge.net/>

Gördüğünüz üzere `ccencrypt` (*ya da ccrypt -e sifrelenecekdosya*) ile dosyamızı anahtarımız ile şifrelemiş olduk. Anahtarı ise unutmamanız çok önemli. Tamamen unutursanız eğer şifrelenen dosyayı kurtarmanız mümkün olmayacaktır.

Dizin şifreleme;

```
kame ~ % tar -zcvf sifrelenecekdizin.tar.gz dizin/  
kame ~ % ccencrypt sifrelenecekdizin.tar.gz
```

İlk komutumuz `dizin` adındaki dizinimizi (*balık adındaki balık, komik değil biliyorum.*) `tar.gz` formatında sıkıştırmak olacaktır. Ardından arşiv dosyamızı `ccrypt` ile sorunsuz bir şekilde şifreleyebilirsiniz.

Şifre çözme;

```
kame ~ % ccdecrypt sifrelenmisdosya.cpt  
Enter decryption key:
```

`ccrypt`'in şifrelediği dosyaların uzantısı “**.cpt**” olarak değiştirmektedir. Eğer şifreyi çözmek isterseniz kullandığınız `ccdecrypt` ile (*ya da ccrypt -d sifrelenmisdosya.cpt*) anahtarınızı girerek dosyanızın şifresini çözebilirsiniz.

Anahtarımı unuttum, ne yapmalıyım?

Eğer anahtarınızı unutmuşsanız, şifrelediğiniz dosyaya erişmeniz mümkün olmayacaktır. Fakat, `ccguess` ile şifrenizi yanlış

yazmış olabileceğinizi düşünerek ne olabileceğine dair bir kalıp deneyebilirsiniz.

Diyelim ki, şifrenizi “**abcdefg**” yaptınız (*ben yaptım siz yapmayın*), ve aklınızda sadece a, b, c, d ile e’yi içerdiği kalmış;

```
kame ~ % ccguess sifrelidosya.cpt
Enter approximate key: abcde

Generating patterns...1..2..3..4..5..sorting...done.

Possible match: abcdefg (2 changes, found after trying 1890639
keys)
```

Burada şu unutulmamalı; anahtarınız ne kadar çok karakter içerirse doğru tahmin için o kadar çok karakteri doğru hatırlamak zorundasınız, yoksa çabalarınız boşuna olacaktır.

Şifreleme esnasında sistem çöktü, peki şimdi ne olacak?

Örneğin, elinizde 100mb bir dosya var ve tam bunu şifrelerken ya da şifreyi çözerken sisteminiz kitlendi, elektrikler gitti vs. Ayrıca, bu dosyanın yedeğini şifrelemeden önce almadınız ve tek kopya şifrelemeye çalıştığınız dosya. Öncelikle yapmanız gereken şifrelenen dosyanın şifresini “**-m**” parametresi ile çözmek olacaktır.

```
kame ~ % ccdecrypt -m bozukturdosya.cpt
```

Bu yöntemle dosyanın çözülen şifrelenmiş kısmı ile bozuk kısmından oluşan 2 ayrı dosya oluşturacak. Orjinal dosyayı bu iki kısmı birleştirerek tekrar oluşturabilirsiniz, fakat şifreleme ve çözümün birleştiği noktadaki 32-63 byte'lık bölümü malesef kaybedeceksiniz.

Anahtar oluştururken neleri kullanmamalı?

Yazdırılabilir ASCII karakterlerin hepsini kullanabilirsiniz. Sadece '\n', '\r' ve '"'ı kullanamazsınız. Bunların dışında, işletim sisteminiz eğer bazı özel karakterleri yazdıramıyorsa, doğal olarak onları da anahtar oluştururken kullanamayacaksınız.

Windows'ta şifreledim, GNU/Linux veya Mac Os'ta açabilir miyim?

Evet! ccrypt, platform bağımsız bir uygulamadır.

Şifrelenecek dosyanın boyutu önemli mi?

Hayır! İsteddiğiniz büyüklükte bir dosyayı ccrypt ile şifreleyebilirsiniz. Önemli olan sisteminizin bunu kaldırabilmesi.

20. Şifreler, Şifreler ve Şifreler

Basit ve etkili bir şifrelemeden bahsettim fakat bir şifrenin nerede saklandığı, nasıl saklandığı, bu şifrelerin nasıl kırıldığında dair bir yazım yoktu. En azından temel kriptografi bilgisi ve basit bir Hashcat örneği ile bu eksikliği giderebilirim. Yazının eksik kaldığı noktalar elbette vardır ve herhangi bir grubu tatmin etme amacı yoktur. Bu yazı bunun¹⁸⁷ ve bunun¹⁸⁸ derlenmiş halidir.

Şifreler nerede saklanıyor?

Veritabanlarında. İlk bakışta dalga geçiyorum gibi gelecek ama durum bu. Unix ve Unix benzeri işletim sistemlerinde şifreler tek bir metin dosyasında, Windows'ta ise binary dosyasında saklanmaktadır. Elbette şifrelerin kriptosuz hallerini herhangi bir metin dosyasında bulundurmamak mantıklı değildir. Bu dosyayı eline geçiren bir saldırgan şifrelerinize de sahip olacaktır. Bu nedenden dolayı bütün işletim sistemleri şifreleri bir hash algoritması ile çalıştırır, sonuç olarak veritabanlarında kriptografik hash olarak saklarlar. Bu ise şunu sağlar; eğer bir saldırgan bu veritabanını bir şekilde eline geçirirse, hash olarak saklanmış şifreleri bakarak çözemeyecektir.

Örneğin, GNU/Linux'ta kullanıcı için bir şifre¹⁸⁹ oluşturduğunuz zaman bu şifre sha-512 algoritması ile hashlenerek /etc/shadow¹⁹⁰ dosyası içinde yerini alır (AES ve Rijndael şifrelemesini de ekleyelim). Bu dosyaya baktığımız zaman;

187<http://sickbits.net/articles2/passwords.txt>

188<http://sickbits.net/articles2/passwords2.txt>

189<https://en.wikipedia.org/wiki/Passwd>

190<http://www.cyberciti.biz/faq/understanding-etcshadow-file/>

kame:

```
$6$7gNvdbpz$c6fb024a22c4db9101ea1d20596034..:15758:0:99999
:7::
```

\$6 = Sha-512 hash algoritması.

\$7gNvdbpz = Salt değeri.

\$6fb024a22c4db9101ea1d20596034.. = Şifre.

:15758= Son şifre değişikliği tarihi (*gün sayıdır, başlangıç tarihi 1 Ocak 1970*).

:0 = Şifre değişiklikleri arasındaki minimum süre.

:99999 = Şifrenin maksimum geçerlilik süresi (*gün sayıdır*).

:7 = Hesap kapatıldıktan sonra şifrenin dolma süresi.

Peki hash nedir?

Hash, bir hashing algoritmasının (*md5, sha-1, sha-2 vs.*) kriptografik çıktısıdır. Bir hashing algoritması açık metin ile şifrelenmiş metin arasında tek yönlü bir dönüşüm sağlar. Bu şu demektir; eğer ben herhangi bir açık metni bir hashing algoritması ile şifrelenmiş metne dönüştürmüşsem, hashing algoritmasını tekrar kullanarak şifrelenmiş metinden açık metne ulaşamayacağım. Herhangi bir hashing algoritması tarafından boyutu standart olmayan bir girdinin şifrelenmiş çıktısı hashing algoritmasına göre eşit uzunluktadır. Diğer bir deyişle, bir e-kitabın boyutu ya da bir filmin boyutu ya da bir metnin boyutu ne olursa olsun, çıktının uzunluğu algoritmaya göre sabittir. Bunun kriptografide önemli olmasının sebebi, eğer bütün algoritmalar kendi türleri içinde aynı uzunlukta çıktıyı verirse, girdinin boyutunu ya da türünü belirlemek

mümkün olamaz.

Salting, biz buna tuzlama mı desek?

Salting'in¹⁹¹ türkçeye nasıl çevrildiğini ya da ne denildiğini bilmiyorum. Nedir noktasına gelirsek eğer, Salt¹⁹² rastgele verilen bir değer olup gizli değildir ve rastgele oluşturulur, şifre hashi ile birlikte saklanır. Büyük boyutlardaki salt değeri önceden hesaplanmış saldırılarını, mesela rainbow tablousu, her şifreyi eşsiz olarak hashleyerek engeller. Yani Ali ile Ayşe, aynı veritabanında saklanan tıpatıp aynı şifrelere sahip olsa bile, salt değerleri ile birbirinden farklı hash değerlerine sahip olacaklar ve bir saldırgan veritabanına erişse bile bu iki kişinin şifresinin aynı olduğunu bilemeyecektir.

Saldırmanın başarılı olabilmesi için her salt değerini de ayrı ayrı hesaba katması gerekmektedir. Salting'in kullanılmasının nedeni şifrelerdeki entropi¹⁹³ düzeyini arttırmaktır. Bir diğer deyişle, bizlere fazladan koruma sağlar.

Kripto fonksiyonunda iki girdi vardır. Bunlar \$salt ve \$key'dir, crypt(\$salt, \$anahtar). Eğer salt değerimizin "0Z" ve şifremizin "kame" olduğunu varsayarsak \$salt + \$şifre;

0Zkame

191[https://en.wikipedia.org/wiki/Salting_\(cryptography\)](https://en.wikipedia.org/wiki/Salting_(cryptography))

192<http://stackoverflow.com/questions/420843/how-does-password-salt-help-against-a-rainbow-table-attack>

193<https://en.wikipedia.org/wiki/Entropy>

Artık bu hashlenecek ve şifre veritabanında saklanacaktır. Bu şifrenin eğer bir kullanıcı şifresi olduğunu varsayarsak, /etc/shadow altında hash ile birlikte saklandığını görebiliriz. Örneğin, sisteme giriş yapmak istediğimizde, doğrulama yapmamız gerekecektir.

Doğrulama, kullanıcı adı ve şifresi girildiğinde önce salt değerini alacak ve girilen şifre ile birlikte kriptofonksiyonunu çalıştıracaktır. Ardından, eğer şifreniz doğru ise hashler birbirini tutacak ve sisteme girebileceksiniz.

Birkaç örnek

En popüler hashing algoritmalarından biri (*bugünlerde zayıf olduğu sıkça tekrarlanırsa da*) MD5'tir¹⁹⁴. MD5 hashing algoritması 128 bit yani 16 byte'tır. Çıktısı 32 haneli, onaltılı (0,...,9, a,...,f) (hex) sayıdan oluşur. Yani, 2 hex = 1 byte, 16 byte = 128-bit.

“**kame**” dizisini MD5'e dönüştürürsek;

```
kame ~ % echo -n 'kame' | md5sum | cut -f 1 -d " "
366b18ce0695e44bfc30423b9eb8a793
```

İçinde sadece “**test**” yazan “**test.txt**” dosyasını MD5'e dönüştürürsek;

```
kame ~ % md5sum test.txt
098f6bcd4621d373cade4e832627b4f6 test.txt
```

¹⁹⁴<https://en.wikipedia.org/wiki/Md5>

MD5'e göre daha güçlü ve NSA tarafından tasarlanan bir diğer hashing algoritması ise SHA-2'dir¹⁹⁵. SHA-2, 224, 256, 384 ve 512 gibi çeşitli bit uzunluklarında 4 farklı seçenek sunar.

```
kame ~ % echo -n 'kame' | sha256sum | cut -f 1 -d " "  
be45d72f76fc702161620f5d5462443cb038fffd5b839d28d5c85dcf3b4  
6cac5
```

```
kame ~ % sha256sum test.txt  
9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0  
f00a08 test.txt
```

$256/128 = 2 > 32 \times 2 = 64!$ Yani, algoritma, 64 hex haneli hash üretir.

Hashing algoritmaları ayrıca bir veriyi doğrulamak için de kullanılmaktadır. Örneğin, İnternet üzerinden indirmek istediğiniz herhangi bir dosya için yayınlayan kişi bu dosyaya ait bir hash bilgisi de vermektedir. Böylece indirdiğiniz dosya ile İnternette verilen hashleri karşılaştırıp doğrulama yapabilirsiniz.

Hashlere saldırılar ikiye ayrılmaktadır. Birincisi çevrimiçi saldırılar, yani elinizde kırmak isteyeceğiniz bir hash listesi yoktur, İnternet üzerinden bulunan bir uygulama ya da servise, veritabanlarında bulunan hashlerle karşılaştırması için çoklu şifre tahminlerinde bulunursunuz. İkincisi ise çevrimdışı olan saldırılardır.

¹⁹⁵<https://en.wikipedia.org/wiki/Sha-2>

Bunlarda ise elinizde bulunan veya bir yerlerden elde ettiğiniz hash listesini çeşitli saldırı türleri ile kırmaya çalışırsınız. Bu saldırı türlerinden en bilinenleri, bruteforce¹⁹⁶, rainbow tablosu¹⁹⁷ ve sözlük¹⁹⁸ saldırılarıdır.

Bruteforce

Varolan bütün kombinasyonların denenmesi anlamına gelmektedir. Kullanılan karakterlere göre değişmektedir. Örneğin sadece a,z aralığı ya da a,z ve A,Z aralıkları veya A,Z,0,9 aralığı gibi çok çeşitli kombinasyonlar oluşturabilirsiniz. En yavaş yöntem olabilir fakat sadece kombinasyon oluşturmaz. Ayrıca her kombinasyon için hash de oluşturur ve bunları karşılaştırır.

Elbette 4 hanelik bir şifrenin hash'ini kırmak çok uzun sürmez fakat hanesi sayısı artarsa, bunu kırmak için geçecek süre de artacaktır.

Rainbow Tablosu

Bir Rainbow (*gökkuşağı*) tablosu, daha önceden hesaplanmış hash'leri içermektedir. Yani, diğer bir deyişle, hash'ler hazır ve karşılaştırılmayı beklemektedir. En önemli artısı, işlemci yükünü azaltarak küçük boyutlu işlerde çok etkili sonuç verir. Sözlük saldırılarında, önce hash oluşturup ardından bunu kırmak istediğimiz hash ile karşılaştırırız. Gökkuşağı'nda ise hashlere zaten sahibiz ve tek yapmamız gereken bunları karşılaştırmak. İyi bir gökkuşağı tablosu oluşturmak vakit alacak bir iştir fakat etrafta çok büyük boyutlu ve işe yarar tablolar da dolanmaktadır¹⁹⁹.

196https://en.wikipedia.org/wiki/Brute-force_attack

197<http://project-rainbowcrack.com/>

198https://en.wikipedia.org/wiki/Dictionary_attack

199<http://www.freerainbowtables.com/>

Gökuşağı tablosunun etkisini azaltmak için yukarıda bahsettiğim salt yöntemi etkili bir yöntemdir.

Sözlük

Sözlük, kelimelerden, karakterlerden ve bunların kombinasyonlarından oluşan basit bir metin dosyasıdır. Sağda solda gördüğünüz **“wordlist”** ya da kelime listeleri de aynı anlama gelmektedirler. Sözlük, genel olarak kullanıcının basit şifreler kullanması fikrine dayanır. Bu yüzden herhangi bir sözlük metin dosyasına baktığınız zaman **“12345678”**, **“qwerty”** gibi ya da **“home”**, **“pass”** gibi dizilerden oluştuğunu görebilirsiniz.

Sözlük saldırıları şu şekilde olur; kırmak istediğiniz hash'e karşılık sözlükteki her dizinin bir hash karşılığı oluşturulur ve bununla karşılaştırılır. Eğer iki hash de birbirini tutarsa, kırılmış demektir. Günümüzde artık CPU'lar epey güçlü olduğu için 1-2 dakika içerisinde 14 milyon girdi test edilebilir.

Bu saldırıları gerçekleştirebileceğimiz çevrimdışı bir uygulama arıyorsak eğer Hashcat bu iş için biçilmiş kaftan.

Hashcat

Hashcat²⁰⁰, çok hızlı ve çok yönlü hash kırıcısı (cracker)'dır. Dağıtımlarınızın repolarında muhtemelen vardır, kurarsanız altta vereceğim örnek üzerinde nasıl çalıştığını daha iyi anlayabilirsiniz.

200<http://hashcat.net/>

kame dizisinin MD5 çıktısı “**366b18ce0695e44bfc30423b9eb8a793**” olduğunu yukarıda söylemiştik. Bunu bir metin dosyası içine, örneğin test.txt, yapıştırın ve kaydedin. Bu örneğimiz için bize bir sözlük lazım;

- [1ANORMUSWL](#)
- [RockYou](#)

İstediklerinizi indirebilirsiniz. Bu örnekte 1ANORMUSWL dosyasını kullanacağım.

```
kame ~ % hashcat -m 0 -a 0 -o /home/kame/hashcat/sonuc.txt
/home/kame/hashcat/test.txt
/home/kame/hashcat/pass/1aNormusWL.txt
Initializing hashcat v0.46 by atom with 8 threads and 32mb segment-
size...
```

```
Added hashes from file /home/kame/hashcat/test.txt: 1 (1 salts)
```

```
Activating quick-digest mode for single-hash
```

```
NOTE: press enter for status-screen
```

```
366b18ce0695e44bfc30423b9eb8a793:kame
```



```

All hashes have been recovered

Input.Mode: Dict (/home/kame/hashcat/pass/1aNormusWL.txt)
Index.....: 1/5 (segment), 3498468 (words), 33550338 (bytes)
Recovered.: 1/1 hashes, 1/1 salts
Speed/sec.: - plains, 33.39M words
Progress...: 3428536/3498468 (98.00%)
Running...: --:--:--:--
Estimated.: --:--:--:--

Started: Tue Oct 29 20:49:48 2013
Stopped: Tue Oct 29 20:49:49 2013

```

Görüldüğü üzere “-m”, seçtiğim hash algoritmam, 0, yani MD5, “-a” ise saldırı türüm , 0, yani doğrudan (*burada sözlüğe bakıp her dizi için hash karşılaştırması yapıyor*).

Herhangi bir sözlük kullanmadan bu saldırıyı yapmak istersek;

```

kame ~ % hashcat -m 0 -a 3 -o /home/kame/hashcat/sonuc.txt
/home/kame/hashcat/test.txt ?l?l?l?l

```

Terminal çıktısı çok uzun olduğu için onu koymadım. Burada, farklı olarak saldırı türünü 3, yani bruteforce olarak belirledik ve sözlük yerine “?l” parametresini, yani sadece küçük harfleri (a,...,z)

kullanmasını söyledik. 4 tane koymamın nedeni 4 haneden (*kame*) oluşması. Hangi şifrenin kaç haneden oluştuğunu, hangi karakterleri içerebileceğini bilemeyeceğimiz için saldırı modellerini kendiniz geliştirmeniz gerekmektedir.

Hashcat, çok başarılı ve hızlı bir hash kırıcısıdır. Burada çok temel bir örnek vererek anlatmam, sizlerin sağda solda denk getirdiğiniz herhangi bir hash algoritmasını oturup kırsın diye değildir. Daha fazla ayrıntılı bilgi almak isterseniz Hashcat'in wikisi²⁰¹, özellikle mask saldırısı²⁰² ya da RTFM²⁰³ ve internette bulabileceğiniz sayısız döküman var.

201<http://hashcat.net/wiki/>

202http://hashcat.net/wiki/doku.php?id=mask_attack

203<https://en.wikipedia.org/wiki/Rtfm>

21. Kızlı Erkekli Gizlilik Hakkı

Amacım, gizlilik hakkını hukuki boyutta tartışmaktan ziyade gizlilik hakkının kısaca ne olduğu, Türkiye’de yaşanan son kızlı-erkekli saçmalığı üzerine bu konularda daha önceden alınmış kararların ne olduğu ile ilişkilendirip bir inceleme yapmaktır.

Tayyip Erdoğan, Kızılcahamam’daki parti kampında yaptığı konuşmada²⁰⁴ **“Denizli ilinde şahit olduk. Yurtların yetersizliği beraberinde çeşitli sıkıntılar doğuruyor. Üniversite öğrencisi genç kız, erkek öğrenci ile aynı evde kalıyor. Bunun denetimi yok. Muhafazakar Demokrat yapımıza bu ters. Vali Bey’e bunun talimatını verdik. Bunun bir şekilde denetimi yapılacak.”** dedi. Bu söylem çok uzun bir süre tartışılacak elbette, kimi **“gündem yaratmak için böyle diyor”** diyebilir kimi **“ahlak polisi hayaldi gerçek oluyor”** diyebilir, birçok farklı bakış açısından incelenebilir. Ben bunu gizlilik hakkı üzerinden kısaca bir değerlendireceğim.

Politik, sosyal ve ekonomik değişiklikler, yeni hakların tanınmasına yol açmakta ve bunlar toplumun ihtiyaçları doğrultusunda gelişmektedir. Bunlardan bir tanesi, özellikle son dönemde giderek önemi artan ya da ağırlığı artan gizlilik hakkıdır. Gizlilik hakkı, öncelikle bir insan hakkıdır. Bu, bizi, devletlerin ve gizli oluşumların ya da partilerin yasal veya yasal olmayan yollardan tehdit etmelerini kısıtlar veya engeller. Bir diğer tanıma bakacak olursak, kişinin özel alanına rızası alınmadan girmemek demektir. Bu tanımı en iyi açıklayan cümle de 1890 yılında yazılmış olan The Right
204<http://haber.sol.org.tr/devlet-ve-siyaset/erdoganin-freni-patladi-kiz-erkek-ogrenci-ayni-evde-kaliyor-denetleyecegiz-haberi->

to Privacy²⁰⁵ makalesinde geçiyor. Warren ve Brandeis, buna “**yalnız kalma hakkı**” demektedir. 2005 yılında yayınlanan *Privacy in the Digital Environment* kitabından (sayfa 7) gizlilik hakkı üzerine (sadece dijital ortamlar için geçerli değil tabii ki) bir alıntı yapayım;

“Gizlilik hakkı, bizi biz yapan şeylerin tümünü içeren, örneğin bedenimiz, evimiz, mülkiyetimiz, düşüncelerimiz, duygularımız, gizlerimiz ve kimliğimiz gibi, bizi çevreleyen bir alana sahip olma hakkıdır. Gizlilik hakkı, bizlere, bu alandaki parçalara kimlerin erişip erişemeyeceğini, ve açığa çıkarmak istediğimiz parçaların kapsamını, niyetini ve zamanlamasını kontrol etme yeteneği verir.”

Gizliliğin korunması üzerine kronolojik alıntılar yapmadan önce benim de benimsediğim (*Privacy in the Digital Environment*, sayfa 12-14) şu şeyleri netleştirelim;

- Gizlilik hakkı kendimizi özgürce ifade etmek için bizleri cesaretlendirir.
- Gizlilik hakkı bizim için yapay bir ada gibidir. Bu ada üzerinde hem fiziksel hem de sanal bir alana sahip oluruz ve bu alanda aşağılanacağım hissi olmadan hatalar yapabilir, birileri beni izliyor korkusu ve toplum baskısı olmadan deneyim kazanabiliriz.
- Gizlilik olmadan neyin iyi veya neyin kötü olduğuna dair özgürce düşünemez ve karar veremeyiz.
- Gizlilik, izlendiğimiz zaman daha farklı davranmamızın (*oto-kontrol, oto-sansür*) önüne geçer.

²⁰⁵<http://www.english.illinois.edu/people/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf>

- Gizlilik hakkı yarattığı özel alan ile insanların fiziksel ve akıl sağlığını korumasına yardımcı olur.
- Konuşmalarımız dinleniyorsa bu bizi daha resmi olmaya iter ve dürüstlüğümüzden ödün verebiliriz. Gizlilik, daha etkili ve daha dürüst (*bu tartışılabilir*) konuşmamızı sağlar.
- Bir göz tarafından devamlı gözetlenirsek bireyselliğimizi kaybederiz (*mobese'ler ne güzel örnek buna*). Fikirlerimiz, düşüncelerimiz bu gözün yarattığı baskı tarafından şekillendirilir ve hiçbir eşsizliği kalmaz.
- Gizlilik hakkıyla ilişkili olarak konuşma özgürlüğümüz kısıtlanırsa bu ayrıca araştırma özgürlüğünün de kısıtlanmasını tetikler.
- Konuşma özgürlüğünün kısıtlanması demek açık bilgi akışının da bundan olumsuz etkilenmesi demektir. Açık bilgi akışı varolan bilgilerden yeni bilgilerin yaratılmasını, paylaşılmasını ve geliştirilmesini sağlar. Eğer bu açık bilgi akışı bundan etkileniyor/engelleniyor ise bu yeni bilgilerin araştırılması, okunması ve kullanılması da etkilenmiş/engellenmiş olur.

Yukarıda saydıklarım elbette çoğaltılabilir. Gizliliğin korunması üzerine alıntılara geçecek olursak (*felix'e yönlendirme için teşekkürler.*);

1. 1948 yılı İnsan Hakları üzerine Evrensel Deklarasyonu, bölüm 12²⁰⁶;

"Hiçkimsenin gizliliğine, özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez;

206<https://www.un.org/en/documents/udhr/index.shtml#a12>

onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz. Herkes bu tarz müdahale ya da saldırılar karşısında hukuk tarafından korunma hakkına sahiptir.”

2. 1950 yılı İnsan Hakları üzerine Avrupa Kongresi (AİHS), bölüm 8²⁰⁷;

“1. Herkes özel hayatına, aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.”

“2. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir.”

3. 1966 yılı Kişisel ve Siyasal Haklar üzerine Birleşmiş Milletler Kongresi, kısım 17²⁰⁸;

“1. Hiçkimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez; onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz.”

“2. Herkes, bu tarz müdahale ve saldırılara karşı hukuk tarafından korunma hakkına sahiptir.”

²⁰⁷https://en.wikipedia.org/wiki/Article_8_of_the_European_Convention_on_Human_Rights

²⁰⁸<http://www.cirp.org/library/ethics/UN-covenant/>

4. 2000 yılı Temel İnsan Hakları üzerine Avrupa Sözleşmesi, bölüm 7²⁰⁹;

“Herkes özel hayatına, aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.”

5. 2007 yılı Avrupa Birliği’nin Temel Haklar üzerine sözleşmesi, bölüm 7²¹⁰;

“Herkes özel hayatına, aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.”

Israrla vurgulanan şey, her birey, gizliliği için, özel hayatı için, aile hayatı için, evi için, iletişim özgürlüğü için (*telefon, e-posta vs.*) saygı görme hakkına sahiptir ve bu hak (*ayrıca kişisel verilerin kötüye kullanılmaması için*) bir yasa ile korunmalıdır. Bunu, ne tür bir müktedir olursa olsun, kendi keyfi yaptırımları için eğip bükmesi, kafasına göre müdahale etmesi ya da ettirmesi, karışması ya da gözetlemesi söz konusu olamaz. Muktedir dedim ama buna “**ihbarcı komşular**²¹¹” da dahildir. Her ne kadar bana göre böyle bir demokratlık olmasa da Tayyip Erdoğan’ın muhafazakar demokrat yapısı, kendi şahsi ve parti yapısıdır. Bunun üzerinden toplumu hukuk dışı olarak denetlemesi ya da denetletmenin, ihbar ettirmenin yolu ne insan haklarıyla bağdaşır ve bir sonucu olarak ne de gizlilik haklarıyla.

209http://www.europarl.europa.eu/charter/pdf/text_en.pdf

210<http://eur-lex.europa.eu/en/treaties/dat/32007X1214/htm/C2007303EN.01000101.htm>

211<http://www.sendika.org/2013/11/komsu-ihbar-hatti-ankarada-da-devrede-nasil-kiz-erkek-kalirsiniz/>

Hukuk dışı deniliyor diye yarın bir kanun çıkartılıp (*özellikle ulusal güvenlik çıkarlarını bahane ederek, Muammer Güler'in bu konuda bir çıkışı oldu*²¹²) bu tarz bir denetlemenin ve ihbarın yolu hukuki olarak açılırsa, sanmayın ki bu insan hakları ihlali değildir. Türkiye'nin yukarıdaki alıntılarının altında (1, 2, 3) imzası vardır.

Benim şahsi görüşüm, burada direkt gizlilik haklarına da bir saldırı vardır. Amaç kızlı-erkekli evlerden çok yukarıda saydığım gizlilik haklarının sağladığı faydaları engellemeye yönelik olduğunu düşünüyorum. Farklı açılardan değerlendirenler olacaktır, farklı görüşler yazılıp çizilecektir. Yazıya yeni şeyler eklemekten çekinmeyin. Sağlam miğdeli günler dileğiyle.

212<http://vagus.tv/2013/11/06/kizli-erkekli-ogrenci-evleri-terror-sucuna-giriyor/>

22. Büyük Birader'le Mücadele Etmek

Çocukluğumda yaptığım yaramazlıklar için en çok duyduğum öğüt, “karda yürü ama izini belli etme” idi. Her anımızın gözetlendiği, bir şekilde kaydı tutulduğu ya da bir şekilde bize ait özel dediğimiz verilerin okunduğu şu günlerde Büyük Birader’le mücadeleye nereden başlamalı, bir giriş olarak anlatmak istedim.

Biraz paranoya iyidir

Anonimlikte, bence, motivasyon çok önemli. Her adımınızı gözetleyen Büyük Birader’e karşı zihnen de bir mücadele vermektensiniz ve bu konuda motive, sizlere çok büyük bir destek kaynağı olacaktır. Motivasyonun yanına biraz da paranoya eklersek, bence harika olur. Paranoya’nın kısa bir tanımına²¹³ bakalım:

“Paranoya, bireyin herhangi bir olay karşısında olayın oluşumundan farklı olarak gelişebileceğini kendi içerisinde canlandırma yolu ile öne sürdüğü ve sınırsız sayıda çeşitlendirebileceği hayal ürünlerinin tümüdür.”

Sizlere yazılarımda devamlı “**tehlike modeli**”nden bahsetmekteyim. Tehlike modeli oluşturmak (*kişisel görüşüm*) biraz da paranoyaya dayanıyor (*ayrıca hesapları ayırbilmekte örnek bir model var*). Çünkü her olay karşısında, bu olayın gelişimi için farklı canlandırmalar oluşturuyor ve buna karşı güvenliğinizi sağlamak üzerine yeni yöntemler geliştiriyorsunuz. Elbette bunu hastalık boyutuna taşımak kişise zarar verecektir. Fakat, paranoyanın model

²¹³<https://tr.wikipedia.org/wiki/Paranoya>

geliştirmedeki etkisini gözardı etmemek gerekli. Anonimlikle ilgili ısrarla söylediğim şeylerden birisi de; **“kimsiniz ve kimden saklanıyorsunuz, neden ve ne tür bir risk almayı hedefliyorsunuz?”**. Yani, anonimlik düzeyiniz hesaplanabilir, biraz paranoyak olun, iyi bir model oluşturun ve kendinizi koruyun!

Kriptografiye önem vermek

Türkiye’deki üniversitelerde kriptografi ile ilgili ne kadar eğitim veriliyor ya da ne kadar insan bu konuda bilgilendiriliyor, bunun üzerine pek bilgi sahibi değilim. Kriptografi çok çok önemli bir konu ve üzerine ciddi olarak düşünülmesi, ayrıca bu konuda yerel literatüre çok şey katılması gerekli olduğu düşünüyorum. Kısa bir tanım²¹⁴ yapacak olursak:

“Kriptografi, gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür. Bu yöntemler, bir bilginin iletimi esnasında karşılaşılabilecek aktif ya da pasif ataklardan bilgiyi -dolayısıyla bilgi ile beraber bilginin göndericisi ve alıcısını da- koruma amacı güderler.”

Sizin için önemli olan tüm verileri şifrelemelisiniz. Bunun daha başka bir açıklaması yok. Eğer mümkünse tüm verilerinizi şifreleyin. Bu, sizi güvende tutmanın temel ve başlıca yollarından biridir. Bu konuda ne tür araçlar kullanabilirsiniz, kısaca bir göz atacak olursak:

214<https://tr.wikipedia.org/wiki/Kriptografi>

- E-postalarınız için GnuPG²¹⁵ kullanabilirsiniz.
- Dosyalar için ccrypt²¹⁶ ya da encfs²¹⁷ kullanabilirsiniz.
- Disk için TrueCrypt²¹⁸ ya da dm-crypt + LUKS²¹⁹ kullanabilirsiniz.
- Anlık mesajlaşmalarda OTR²²⁰ eklentisini kullanabilirsiniz.
- Ağ için SSH²²¹ kullanabilirsiniz.

Örnekler elbette çoğaltılabilir. Burada iş sadece şifrelemekle bitmiyor. Temel bir örnek ve tavsiye olarak, kullanacağınız şifre ya da şifreler sizinle ilgili ya da size ait herhangi bir bilgi içermemeli. Güvenli bir şifrenin yolu akılda kalması (*inanın kalıyor*) zor da olsa, rastgele şifrelerden geçiyor. Bu, sözlük saldırılarında ya da brute force saldırılarında sizlere ciddi bir avantaj sağlamakta. Dikkati çekmek istediğim bir diğer nokta ise kanun uygulayıcılarının yoktan delil var etme ya da herhangi bir şeyi delil olarak kullanma konusundaki tutumları. Bu nedenle, şifrelediğiniz herhangi bir şey yazılı/basılı olarak elinizde bulunmamalı. Elinizdeki basılı dökümanlarla işiniz bittiyse, yakın gitsin. Yedek alacaksanız, aldığınız bu önemli ve şifreleri verilerin yedeğini ailenize, eşinize, dostunuza ait bilgisayarlarda saklamamanız tavsiyedir.

215<https://network23.org/kame/2013/08/28/pgp-kullanin/>

216<https://network23.org/kame/2013/10/25/ccrypt-ile-sifreleme/>

217<http://www.arg0.net/encfs>

218<http://www.truecrypt.org/>

219<https://wiki.archlinux.org/index.php/LUKS>

220https://en.wikipedia.org/wiki/Off-the-Record_Messaging

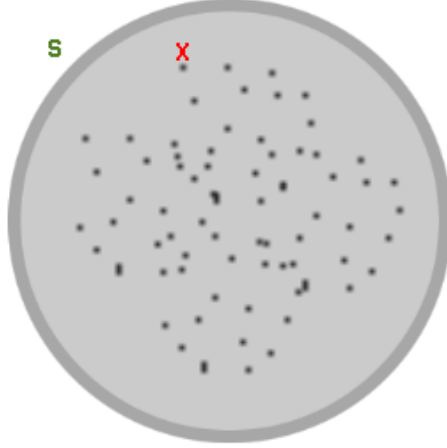
221https://en.wikipedia.org/wiki/Secure_Shell

Hesapları ayırabilmek

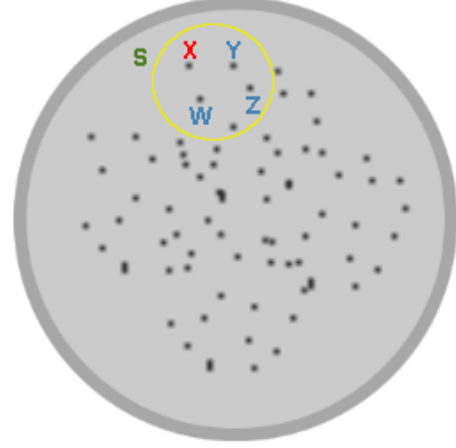
Hesapları ayırmaktan kastettiğim, anonim kimliğiniz ile gerçek kimliğinizi içeren hesapların ayrımını yapmak çok önemli. Anonim hesabınız üzerinden gerçek hesaplarınıza bir bağlantı kurulmamalı. Eğer bu bağlantı kurulursa, artık anonim de değilsinizdir. Anonimlik, tanımı gereği içinde anonim özneleri aşmaya çalışan saldırganları da içerir. Yani, eğer bir anonimlik varsa bu anonimliği ortadan kaldırmak için çalışanlar da olacaktır. Bu, kanun uygulayıcı olur, gizli servisler olur, başka bir anonim özne olur. Önemli olan bir saldırgan varlığını asla unutmamak.

Bir diğer nokta da anonim hesabınız üzerinden gerçekte tanıdığınız ve sizin bu kimliğinizi bilen insanlarla pek iletişime geçmemeniz (*özellikle telefonla*) gerekliliği. Bu konuda kararınız net olmalı ya da en azından ne kadar bilgiye sahip ya da ne zaman bilgiye sahip olacaklarını iyi kararlaştırmak gerekli. Bu, bence çeşitli riskleri de beraberinde getiriyor. Saldırgan ne kadar dar bir çevre oluşturabilirse, sizin kimliğinizi tespit etmesi de o kadar çabuk olabilir. Şimdi bunu basitçe örneklendirelim (*şema eklendi*):

1. Durum: S, X öznesinin gerçek kimliğini (A) bulmak için birçok öznenin oluşan bir küme oluşturur. Artık incelemesi, izlemesi ve saldırıları bu küme üzerinde gerçekleşir.



2. Durum: Eğer S, X öznesinin W, Y veya Z gerçek kimlikleri ile iletişimde olduğunu farkederse kümesini daraltır ve saldırı için yeni küme sınırları belirler.



Sınır: ———

Yeni sınır: ———

Ben anonim kimliği “X”, gerçek kimliği “A” olan bir bireyim. “X” kimliğini gerçekte kim olduğunu (A’yı) bilen “W”, “Y” ve “Z” gerçek kimlikleri var. Ayrıca, “X” kimliğini aşır “A” kimliğine ulaşmak isteyen saldırgan “S” var. Eğer, saldırgan “S”, benim “W”, “Y” veya “Z” gerçek kimlikleri ile iletişimde olduğumu bir şekilde farkederse saldırı kapsamını daha karmaşık ve kapsamlı bir halden daha spesifik ve daha dar bir hale getirir. Gerekirse, “W”, “Y” ya da “Z”ye doğrudan veya dolaylı olarak baskı/saldırı düzenleyerek benim gerçek kimliğime ulaşabilir. Bu saldırı, örneğin, bir man-in-the-middle saldırısı²²² olabilir. Siz “X” anonim kimliği üzerinden “W” gerçek kimliği ile iletişime geçerken, saldırgan araya girip mesaj içerikleri ile oynayarak sizin “A” gerçek kimliğinizi elde edebilir. Bu bahsettiğim örnek, ayrıca bir tehlike modelidir. Bu yüzden ısrarla diyorum ki, bir tehlike modelinizin olması şart!

²²²<https://network23.org/kame/2013/10/04/ssl-man-in-the-middle-ve-turktrust/>

Kayıtlar

Özellikle /tmp, /var/log ve kullanıcı dizininde (/home/kullanıcı) kalan geçmiş ya da yedek dosyaları sizin için bir risk teşkil etmekte. Kullandığınız program, araç vs. her ne ise bunun nerede kayıt tuttuğunu bilmeniz sizin faydanıza olacaktır. Bir diğer noktada terminal üzerinde gerçekleştirdiğiniz şeylerin (*kabuktan kabuğa değişmekte*) de ayrı ayrı kaydı tutulmakta. Örneğin:

```
bash: .bash_history
zsh: .zsh_history
vim: .viminfo
.
.
```

Yedekler için:

```
*.swp
*.bak
*~
.
.
```

Bu sizin kullandığınız ortama göre değişim göstereceği için temel olarak sıralayabileceğim belli başlı şeyleri örnek olarak gösterdim. Sistemden çıkış yaparken bunları silerseniz ya da en azından nelerin kaydını tuttuklarını incellerseniz sizin yararınıza olur.

Uygulama olarak Bleachbit²²³, temizleme konusunda tercih edilebilir (*Emre'ye teşekkürler.*).

Karda yürü ama izini belli etme

Ceza hukukunun ciddi bir eleştirisini hukukçu olmadığım için yapamam. Fakat, kanun uygulayıcılarının hukuk dışı deliller elde ederek bireyi hapse atıp, daha sonra mahkemede tutuklu olarak yargılamaya başlaması ne vahim bir durumda olduğunun göstergesidir. Sonuca gelirse, iyi bir motivasyon, biraz paranoya, önemli verileri şifreleyip anonim kimliğimizle gerçek kimliğimizin ayrımı tam olarak yapabilmek, kendimize uygun tehlike modelleri geliştirip bunlara karşı savunma yöntemleri hazırlamak, ve son olarak karda yürüyüp izimizi belli etmemek! Ayrıca, bu yöntemler sadece burada yazanlarla sınırlı değildir. Herkesin ayrı bir modeli olacak ve yöntemler de ona göre şekillenecektir.

Büyük Birader'i artık her zamankinden daha soğuk bir kış bekliyor.

223<http://bleachbit.sourceforge.net/>

23. Veriyi Unutmak ve Unutulma Hakkı

*Türkiye’de ciddi sıkıntılar doğuran, verilerin elden ele dolaştığı, veritabanlarının yüksek fiyatlara satılıp size ait kişisel verilerin ve gizlilik hakkınızın hiçe sayıldığı bir ortam mevcut. Durup dururken gelen bir telefonla “**Merhabalar ... bey, ben ..., sizlere bir ürünümüzü tanıtmak istiyorum...**” şeklinde yapılan tacizkar pazarlamaların bitmek tükenmek bilmediği şu zamanda, verinin unutulması ve unutulma hakkı²²⁴ üzerine bolca eleştiriye açık fikirlerimi belirtmek istedim.*

Kafanızda önce bir örnek²²⁵ canlandıralım. Sarhoşsunuz, canınız sıkın veya çok mutlusunuz, bilgisayarın başında sosyal medya profillerinizin birinde (*Facebook, G+ vs.*) kendinize ait bir fotoğraf ya da bir yazı vs. paylaştınız. Bu fotoğraf (*veya yazı*) sizinle ilgili ileride başınıza iş açabilecek, her zaman karşınıza çıkabilecek bir şey taşıyor. Örneğin yarı (*veya tamemen*) çıplaksınız, (*birine veya birilerine*) nefret (*veya aşk*) dolu (*küfür şart değil*) bir yazı yazdınız. Sabah uyandığınızda bir de baktınız ki gönderdiğiniz fotoğraf 10 arkadaşınızın da duvarında, bir sürü yorum almış, üstüne arkadaşlarınızın duvarından başka yerlere aktarılmış, Internet Wayback Machine²²⁶ tarafından Internet tarihin tozlu sayfalarına eklenmiş ve arama motorlarında adınız ve soyadınız aratıldığında direkt karşınıza çıkmış. Hemen kullandığınız sosyal medya sitesiyle iletişime geçtiniz, fotoğrafı duvarınızdan sildiğinizi ve sunuculardan da silinmesini istediğinizi söylediniz. Kabul edildi veya edilmedi (*fakat yasa varsa buna bir şekilde zorlayacaktır*), bir de baktınız

²²⁴https://en.wikipedia.org/wiki/Do_Not_Track_Policy#Right_to_be_forgotten_.28European_Union.29

²²⁵<http://www.forbes.com/sites/davidcoursey/2012/02/24/how-the-right-to-be-forgotten-threatens-the-internet/>

²²⁶<https://archive.org/>

arkadaşlarınızın duvarlarında fotoğraf durmaya devam ediyor, aramalarda karşınıza çıkıyor, ya şimdi ne olacak?

Bir Internet sitesi bu durumda kimin duygularını esas almalı? Duvardan duvara aktarılan o fotoğraf artık kimin? Siz üzgünsünüz diye bir Internet sitesi başkalarına da müdahale etmeli mi? Bununla ilgili söylenen²²⁷ temel şeylerden birisi; **“eğer bir salaklık yapip açık bir alan adı üzerinde, gruplarda, forumlarda vs. böyle bir paylaşımda bulunmuş veya kendinizle ilgili tüm özel şeyleri anlatmışsanız, ileride bunlardan dolayı başınıza bir şey gelmesi durumunda şaşırmanızdır”**. Bir diğer nokta da Jeffrey Rosen’in²²⁸ **“Internet yapısına, Google, Facebook ve Yahoo gibi sitelere zarar vereceği ve en önemlisi de Internet’te konuşma özgürlüğünün bundan olumsuz etkileneceği”** görüşü. Bunlar haklı bir cevap, fakat bir kişinin yaptığı bir salaklıktan dolayı bir verinin saatli bomba gibi, kontrolü dışında ve ulaşamayacağı bir bulut üzerinde durmaya devam etmesi de doğru değildir. Bu işin bir orta yolu olmalı. Peki bu orta yol nasıl olacak?

Benim şahsi görüşüm, unutulma hakkı açık ve net olarak ne çok aşırı detaylı ne de çok basit bir şekilde tanımlanmalı, konuşma özgürlüğü, bilgi alma özgürlüğü, ifade özgürlüğü ve Internet özgürlüğü gibi temel hak ve özgürlüklere zarar verici olmamalı. Kanun uygulayıcının veya Internet sitelerinin (*bu tartışılabilir. çünkü bir Internet sitesi jüri görevi de görmeli mi yoksa sadece teknik hizmet mi vermelidir?*) bu yasaya baktıklarında herhangi bir olay için uygulanabilir veya reddedilebilir olmasına karar verebilmeli. Bu şunu sağlar:

- Konuşma özgürlüğü, bilgi alma özgürlüğü, ifade özgürlüğü ve

²²⁷<http://www.npr.org/blogs/kulwich/2012/02/23/147289169/is-the-right-to-be-forgotten-the-biggest-threat-to-free-speech-on-the-internet?ps=cprs>

²²⁸<http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-88.pdf>

Internet özgürlüğü gibi temel hak ve özgürlüklerin bundan olumsuz etkilenmesinin önüne geçecektir.

- Yasanın açık, anlaşılır ve uygulanır olması yasayı eđip bükmek isteyen, bunu kendi çıkarları için kullanmak isteyen muktedirlerin önüne geçecektir.
- Sosyal medyanın, Internet sitelerinin ve Internet yapısının bundan en az zararlı etkilenmeleri sağlanmış olacaktır.
- Her **“ben bir salaklık yaptım bunu silin”** diyenin isteđiyle kafasına göre verinin silinmesi engellenmiş olacak (*yukarıda bahsettiđim temel hak ve özgürlükler doğrultusunda*).

Bir sosyal medya sitesine (*ya da herhangi bir siteye*) üye oldunuz, bir şeyler paylaştınız, daha sonra aldığınız hizmetten vazgeçmek istediniz ve hesabınızı silmeye karar verdiniz. Hesabınıza ait veriler ne olacak? Bu veriler üçüncü şahıslara kişinin izni alınmadan satılıyor mu ya da satıldı mı? Nasıl oluyor da hiç tanımadığınız birileri sizi arayıp bir ürün satmaya çalışıyor? Veya nasıl oluyor da hesabını sildiğiniz bir Internet sitesi sizlere düzenli olarak e-posta göndermeye devam ediyor? Tacizkar pazarlama demiştim kısaca bir anlatayım. Bir bara gidiyorsunuz ve biri kabul edene kadar önünüze gelene evlenme teklif ediyorsunuz. Kimse kabul etmezse de suçu kendinizde bulmuyor o barı size önerene kızılıyorsunuz. Sizleri arayıp ürün satmaya çalışan insanlar da ürünü satana kadar birilerini aramaya ya da hesabını sildiğiniz Internet sitesi sizi geri kazanana kadar bilgilendirme, gelişme, haber vs. adı altında e-posta göndermeye devam ediyor.

Kısa bir tanımdan sonra verinin unutulması ile ilgili olarak benim şahsi görüşüm, eğer bir kullanıcı hesabını silmişse, o hesap silinmiştir. Bitti! Bir banka hesabının, bir sosyal medya hesabının, bir cep telefonu operatörü hesabının ya da bir e-posta hesabının silinmesi arasında bana göre fark yok. Şirketler, belirli bir süreliğine (*mesela 6 ay, en fazla 1 sene, daha fazlasına karşıyım!*) verileri saklayabilirler ama bunu sadece ve sadece şirket içi performans ölçümü ve yeni teknolojilerin geliştirilmesi için “anonim” olarak kullanabilirler.

Ayrıca, bu verilerin kesinlikle ve kesinlikle belirli bir süre sonra silinecek diyerek 3. şahıslarla paylaşılması veya satılması (*ben buna da karşıyım ama söylemekte yarar var; eğer kullanıcı aksini belirtmemişse ve izinli pazarlama için onayı varsa verebilirler*) söz konusu dahi olamaz. Bu konuda gelecek en temel itirazlardan bazıları şunlar; **“eğer biz hesap silindikten sonra o hesaba ait tüm verileri (mesela banka için hesap numarası) de silersek ilerde o hesap numarası boşa kalacağı için başkasına verilebilir, (internet için) kullanıcı adı (ya da banka için hesap numarası) başkası tarafından alınıp kötüye kullanılabilir (inceleme yapılırsa eski kullanıcı bundan dolayı olarak etkilenebilir) ve kullanıcı tekrar geri dönmek isterse bu onu olumsuz (kullanıcı adım alınmış, hesap numaram başkasının vs.) etkileyebilir...”**.

Eğer böyle sıkıntıların doğabileceğinden bahsedilebiliyorsa konuyla ilgili en temel çözüm; hesap silinmişse ve kullanıcı, verinin unutulma süresi içinde dönmemişse hesap numarasını, kullanıcı adını vs. tamamen bloklansın ve bir daha kullanılamasın. Bu kadar basit. **“O zaman bir sürü ölü hesap, kullanıcı adı vs olur.”** safsatasını

geçelim. Çünkü ciddiye almayacağım.

Son olarak Almanya'dan bir örnek²²⁹ verelim. İki kişi birlikte ünlü birini öldürüyor ve mahkemeye çıkartılıp yargılandıktan sonra suçlu bulunup hapse gönderiliyor. Ceza süreleri tamamlanıp hapisten çıktıktan sonra Wikipedia'da²³⁰ öldürdükleri ünlü kişinin sayfasına girdiklerinde "tarafından öldürüldü" şeklinde kendi isimlerini de görüyorlar. Wikipedia'yı "**Biz hapiste cezamızı çektik, topluma olan borcumuzu ödedik ve bu kazanın unutulmasını istiyoruz.**" diyerek isimlerinin kaldırılması için dava ediyorlar. Peki, Tarih, unutulma hakkı için bu iki kişiyi silebilir mi? Geçmişe bu nedenle müdahale edilmeli mi? Orwell'den gelsin; "**geçmiş kontrol eden geleceği kontrol eder.**" Tüm bunlar bir hikaye değil, yaşanmış ve yaşanmakta olan durumlar.

Sonuçta, unutulma hakkı çok detaylı ve detaylandıkça da zorlaşan bir yapıya sahip. Bunun üzerine ne kadar çok çalışma yapılırsa bizim için o kadar iyi olacak, o kadar çok farklı fikir üretilecek ve değerlendirilecek ve bu çalışmalar herkes için yararlı olacaktır.

229http://www.nytimes.com/2009/11/13/us/13wiki.html?_r=0

230<http://wikipedia.org/>

24. Casus Yazılım ve Teknoloji Kültürsüzlüğü

Kapalı kapılar ardında sözde kanun tasarı hazırlanıyor ve bu kanunda geçen maddeler direkt anayasaya aykırı düşüyor. Bir de yetmiyor, Türkiye’de yayınlanan teknoloji dergilerinden birinin online yayın yönetmeni çıkıp pratik olarak devlet casus yazılım yerine gitsin İSS’den takip etsin kullanıcıları diyebiliyor.

Geçenlerde “**İnternette müzik indirene casus önlemi**” diye bir haber çıktı²³¹. Haberde:

“Bir siteden programlar vasıtasıyla bir müzik parçası veya film indirdiğinizde, buradaki hükümlerle karşı karşıyasınız. Diyor ki bu hüküm, ‘Hak sahibinden izin alınmaksızın noktadan noktaya ağlar üzerinden eserleri umuma ileten bireysel internet kullanıcılarının IP adresleri, telif birliklerince Telekomünikasyon İletişim Başkanlığı tarafından akredite edilmiş yazılım vasıtasıyla tespit edilir. Burası çok tehlikeli. Bu ne demek biliyor musunuz? Yani kanun koyucu sizin bilgisayarınıza casus yazılım gönderecek. Buna sistem müsaade edecek. Erişim sağlayanlar müsaade etmek zorunda kalacaklar. Siz güvenli şekilde internette sörf yaptığınızı sanırken bu yazılım sayesinde bilgisayarda hangi işlemleri yaptığınız ve hangi hak ihlallerinde bulunduğunuz tespit edilecek. Ardından bu casus yazılım akredite olacak, Telekomünikasyon İletişim Başkanlığı tarafından da bu yazılım onaylanacak.”

231 <http://www.aa.com.tr/tr/bilim-teknoloji/255356--internette-muzik-indirene-quot-casus-quot-onlemi>

Bu yasanın arkasında ne tür bir güç olduğunu, alıntıda geçen “**telif birlikleri**” çok iyi özetlemektedir. Birilerinin “**sanatçıyı ve sanatı koruma**” adı altında böyle keyfi yaptırımlarına hepimiz alıştık. Ama bu yapılanları normalleştirmek anlamına gelmesin kesinlikle. Akredite edilmiş yazılım ile kastedilen (*benim anladığım*); kullanıcıları tespit etmek için yazılıma (*ya da onu kim kullanacaksa*) yetki verildiği ve yazılımın sağlayacağı bilginin resmen tanındığı ve kabul edildiği anlamına geliyor. Şimdi, “**casus**” bir yazılım var, bu yazılım telif birlikleri ile kanun uygulayıcı tarafından kullanıcının İnternette müzik indirip indirmediğini tespit edip bunun üzerinden yasal işlem uygulayacak. Bu, öncelikle TCK’nın onuncu bölümünde²³² bahsettiği bilişim suçlarından hangisine giriyor, onunla ilgili bir bilgi verilmemiş. 243-246 aralığında maddelere bakıldığında, bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme, banka veya kredi kartlarının kötüye kullanılması ve son olarak da tüzel kişiler hakkında güvenlik tedbiri uygulanması adında ana başlıklara sahip.

Bu başlıklar altında tanımlanan hiçbir madde haberde söylenenle ilişkili değil, onu da geçtim “**casus yazılım**” ile böyle bir izleme/cezalandırma yapılması T.C. Anayasası, madde 20’de²³³ belirtilen özel hayatın gizliliği ilkesine tamamen aykırı. Düşünün ki bir anayasanız var, bu anayasada özel hayatın gizliliği ilkesinde böyle kafanıza göre izleme yapamayacağınız, kişinin şahsi olan bilgisayarına “casus” bir yazılımla girip acaba hangi hakkı ihlal etti diye izleyemeyeceğiniz kısa ve net olarak (*haberleşme özgürlüğü*) belirtilmiş. Haberde geçen ve tasarı halinde olduğu söylenen “**Fikir ve Sanat Eserleri Kanunu**” var fakat buradan sızan bilgilere

²³²<http://bidb.osmaniye.edu.tr/dosyalar/files/tck.pdf>

²³³<http://www.tbmm.gov.tr/develop/owa/anayasa.maddeler?p3=20>

bakarsak TCK ve anayasa ile şimdiden çelişmeye ve aykırı düşmeye başladı bile.

Bu haber çıktıktan birkaç gün sonra bu habere Türkiye’de “**Teknoloji Kültürü**” adıyla yayınlanan Chip dergisinin²³⁴ online yayın yönetmeni Cenk Tarhan ve PCNet²³⁵ yayın yönetmeni Erdal Kaplanseren’in açıklamaları eklenerek²³⁶ tekrar sunuldu. Kaplanseren yasaya aykırılığını söylemese de en azından insanların izlenebilmesi için bir bahane üretildiğini ve asıl bunları yayınlayan sitelerle uğraşılması gerektiğini söylemiş. Fakat, Tarhan’ın yaptığı açıklamayı okurken şok geçirdim:

“CHIP Online Yayın Yönetmeni Cenk Tarhan, illegal olarak MP3 indirmenin elbette kötü bir şey olduğunu; ancak devletin casus yazılım kullanmak yerine çok daha pratik yollara başvurabileceğini hatırlattı ve şu sözleri kaydetti: Devlet isterse internet servis sağlayıcılarının kayıtlarına bakarak kullanıcıların hangi siteye girdiğini, hangi dosyaları indirdiğini anında görebilir ve illegal bir durum söz konusuysa bu kayıtları delil olarak kullanabilir.”

Tarhan’ın bunu hangi kafayla söylediğini (*gene iyi niyetli davranıp söyleminin yanlış aktarılmış olabileceğini de ekleyeyim*) anladığım söylenemez. Öncelikle, devlet isterse diye bir durum söz konusu değil. Böyle bir keyfiyet yok, yasayla da belirtilmiştir. İkincisi, **“devlet kullanıcıların hangi siteye girdiğini ya da hangi dosyaları indirdiğini anında görebilir”** demek, devletin gayri hukuki izleme yaptığını ve kendini teknoloji kültürünün parçası

234<http://chip.com.tr/>

235<http://www.pcnet.com.tr/>

236<http://www.hurriyet.com.tr/teknoloji/25195411.asp>

olarak gören bir yayın yönetmeninin bunu pratik yol diye söylemesi ise nasıl bir aklın tezahürüdür bilemiyorum. Öncelikle Tarhan'a TCK'nın dokuzuncu bölümü²³⁷ olan "**özel hayata ve hayatın gizli alanına karşı suçlar**"dan birkaç madde göstereyim:

"Madde 134 (1) - Kişilerin özel hayatının gizliliğini ihlâl eden kimse, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlâl edilmesi hâlinde, cezanın alt sınırı bir yıldan az olamaz."

"Madde 135 (1) - Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir."

"Madde 136 (1) - Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır."

Basit bir dille, veriler yasal bir merci tarafından istense dahi;

- Hukuka aykırı yollarla delil toplayamazsın.
- Hukuka aykırı yollarla topladığın delilleri mahkemede kullanıcının aleyhine sunamazsın.
- Kullanıcı o suçu işlemiş dahi olsa, hukuka aykırı yollarla topladığın deliller üzerinden kullanıcıyı suçlayamazsın.
- Bunun üzerine alacağın cezalar da yasada mevcut.

²³⁷<http://www.orgtr.org/tr/turk-ceza-kanunu-5237-sayili-kanun-madde132140>

Devam edelim, bir kullanıcının hak ihlalinde bulunduğunu “**casus yazılım**” haricinde kanun uygulayıcı nasıl anlayabilir? Tahminde bulunacak değil, örneklem oluşturup belirli bir sayıda kullanıcıyı izleyerek de bir sonuca ulaşamaz. Onun yerine tüm trafik akışını “**izlemek**” ve verileri de bir şekilde “**kaydetmek**” durumunda. Böyle bir şey teknik olarak mümkün olsa bile tekrar yasaya aykırı (*yukarıda da belirttiğim üzere*) bir durum söz konusu. Onu da geçtim (*felix’e tekrar tekrar teşekkürler*), CMK 134. maddeyi²³⁸ açıp hiç okumuş mudur merak ediyorum. O maddeye bakarak, diyelim ki; hakim kararı çıkartıldı, anayasaya da uygun bir karar (*bu tartışılır elbette*) ve benim buna benzer bir suç işlediğim üzerinden bilgisayarına el konuldu. Ben harddisk’im yedeğini istedim, kanuna uygun olarak da harddiskimin yedeği kanun uygulayıcı tarafından alındı ve bana geri verildi. Yani, beni suçladıkları “**illegal mp3’leri**” bana “**buyur al kardeş mp3’lerini**” diyerek geri mi verecekler? Ee, hani ben yasalara aykırı bir suç işlemiştim?

Burada söylemek isteyeceğim bir başka şey de bu tarz haberlerin temel amacı oto-kontrolü sağlamaya çalışmaktır. Yani, sizi bir üçüncü göz, casus yazılım, olmadı “**pratik olarak**” İSS’niz tarafından ne yapıyorsunuz, ne indiriyorsunuz, hangi sitelerde geziyorsunuz takip edebilir, yasa üzerinde çalışıyoruz, “**ha çıktı ha çıkacak**” diyerek “**kapalı kapılar ardında**” muktedirlerin kafalarınca anayasaya aykırı yasalar çıkartıyor gözükmemesinin ve haberlerinin yapılmasının amacı, içinize korku yerleştirmektir. İçinizdeki bu korku üzerinden de sizler oto-kontrolünüzü sağlayacaksınız. Bir diğer nokta da bireysel-sansürdür. Devlet sizlerin sözüm ona illegal içeriklere ulaşmanızı engellemek yerine bu korku

238<http://www.ceza-bb.adalet.gov.tr/mevzuat/5271.htm>

ile hareketlerinizi ve söylemlerinizi kendiniz sansürleyeceksiniz.

Türkiye'deki teknoloji kültürünün sıkıntılı olduğunu açık ve net olarak artık söyleyebilirim. Bundan sonra bu tarz söylemlerde bulunan kişileri de yakından takip edeceğim. Bakalım başka ne yumurtlayacaklar insan merak ediyor doğrusu.

25. Anonim Hesapların Korunması

Üye olduğunuz bir sitenin hiç Privacy Policy kısmını okuyor ya da sizi yasal süreçte neler bekliyor farkında mısınız? Gelin küçük bir inceleme yapalım.

İddiam şu; hemen hemen hiçbirimiz üye olduğumuz sosyal medya sitelerinin gizlilik politikaları (*Privacy Policy*) bölümünü okumuyoruz. Okumuyoruz ve eğer bizimle ilgili herhangi bir yasal süreç işlerse, bu noktada üyesi olduğumuz sosyal medya sitelerinin nasıl tepki verebileceğini, bizimle ilgili nerenin/hangi yasalara uygun olarak ifşalarda bulunabileceğini de bilmiyoruz. Diyelim ki, benim (*çok kullanılan hesaplardan biri olarak*) bir last.fm²³⁹ hesabım var (*siz başka sitelerin Privacy Policy kısımlarını inceleyebilirsiniz, iyi de olur.*), bununla birlikte bir de anonim kimliğim “X”²⁴⁰’e ait, aktivistlik yaptığım bir Twitter²⁴⁰ hesabım var. Ayrıca, Twitter daha önce Türkiye hükümetinin yapmış olduğu bilgi paylaşımı isteğini reddettiği²⁴¹ için üzerime de bir rahatlık çökmüş durumda.

Öncelikle last.fm’in Privacy Policy²⁴² sayfasının 16 numaralı, yasal olarak mecbur kalınan ifşalar anlamına gelen “**Legally-Compelled Disclosures**” bölümüne bakalım:

“We believe in privacy and therefore will take all reasonable measures to ensure that your personally identifiable information remains private. However, in the event that we are required to

²³⁹<http://last.fm/>

²⁴⁰<http://twitter.com/>

²⁴¹<http://bianet.org/bianet/ifade-ozgurlugu/148894-twitter-turkiye-ye-hic-olumlu-yanit-vermedi>

²⁴²<http://www.last.fm/legal/privacy>

disclose personally identifiable information by a court, the police or other law enforcement bodies for their investigations, regulation or other governmental authority we will make such a disclosure without being in violation of this Policy.”

Diyorlar ki, bizler gizliliğe inanıyoruz ve kişisel kimliğinizi saptayabilecek bilginizin gizli kalaması için tüm sorumlulukları alacağız. Fakat, bir olayda bizden kişisel kimliği saptayabilecek bilginin mahkeme, polis ya da kanun uygulayıcının arařtırmaları, düzenlemeleri ya da devletin diđer bir yetkilisi tarafından istenirse bu politikayı ihlal etmeden bir ifşada bulunuruz. İddiamın olasılıđını merak edip last.fm ile iletiřime geçtim. Soru olarak da:

“Örneđin, ben bir internet akvisitiyim ve ayrıca last.fm hesabım da var. Bir řekilde devlet, Twitter’da yazdıklarım için ifşa edilebilir kişisel bilgilerimi Twitter’dan istedi ve Twitter reddetti. Daha sonra last.fm hesabımı farkettiler (tweet’lerden) ve sizden benim kişisel bilgilerimi istedi. Bu noktada siz ne yaparsınız?”

dedim. Sorduđum bu soru için bana 25 Kasım’da **“bunu hukuki olarak kabul ettiklerini ve konuyla ilgili bir arařtırma yapacaklarını”** söyledi. Tabi tüm bunları söylerken de tam bir açıklama olmadığını, bu açıklama üzerinden hiçbir hak talep edilemeyeceđini ve řirkete çemkirilemeyeceđini de belirttiler. Bunu belirtmezsem ben de last.fm’e ayıp etmiř olurum.

2 gün sonra, 27 Kasım’da gelen yeni cevapta ise last.fm’in ilgili ülkenin tatbik edilebilir kanunları ile birlikte **“Legally-Compelled**

Disclosures“a uygun olarak yükümlüğünü yerine getireceğini ve bireysel sorunlar üzerine daha fazla yardımcı olamayacaklarını belirttiler. Yani, eğer sizin kişisel bilgileriniz last.fm’in belirttiği doğrultuda (*mesela mahkeme kararı, devlet yetkilisinin isteği gibi*) istenirse (*muhtemelen diyelim biz gene*) kanun uygulayıcı ile paylaşılacaktır.

Örnek senaryo; yukarıda bahsettiğim iddiama uygun olarak bir senaryo oluşturayım. Diyelim ki ben anonim kimliği “X” olan bir internet aktivistiyim (*aktivist olmanız şart değil*). Twitter üzerinde iktidar karşıtı söylemlerde (küfür de ediyor olabilirsiniz) bulunuyorum. Bir yandan last.fm profilimle ilgili bir şeyler paylaşıyorum (*tekrar diyeyim last.fm şart değil, sadece bir örnek!*). Diğer yandan Hayyam rt’leri yapıyorum (*hahah*). Eğer, benim hesabımın bir savcı tarafından polise (*ya da başkasına*) takibinin yapılması için bir istekte bulunulmuşsa polis, önce Twitter’a gidecektir. Twitter, polisi reddeder, işbirliğinde bulunmayacağını, kullanıcı bilgilerini paylaşmayacağını söylerse, polis; bu sefer takip ettiği hesabımın başka hesaplarla ilişkili olup olmadığını inceleyecektir. Çünkü (*felix’e teşekkürler*), mecra (*Twitter, last.fm vs*) farketmeyecek (*mecra sadece nerenin savcılığının soruşturacağı noktasında anlamlı*), savcılık resen veya şikayet doğrultusunda benim profilimi inceleyip kanun uygulayıcıya vermişse, kanun uygulayıcı incelemesi için önce Twitter’a, sonra eğer ben diğer hesaplarımı burada paylaşmışsam oradan hareketle gidecektir. Bunun bir sonucu olarak, benim anonimliğim tehlikeye girmiş, ayrıca önümde bir yasal süreç olacaktır.

Sonuç, anonim hesaplarınızı ve sizi ifşa edebilecek diğer sosyal medya hesaplarınızı birbirleri ile ilişkilendirmeyin. Anonim kimliğinize ait hesaplarınızla yapmak istediğiniz şey neyse sadece onu yapın. Diğer sosyal medya hesaplarınızı da bu yaklaşımla kullanırsanız, anonim ve gerçek hesaplarınızı birbirinden ayrı tutmada ilerleme kadedersiniz. Bunu sansür olarak da algılamayın lütfen. Diğer sosyal medya hesaplarınızı silmeniz için bir neden olarak da düşünmeyin. Vurgulamak istediğim şey iddiamda da söylediğim üzere kendimizi sosyal medyanın içine atıp orada kayboluyor, başımıza bir şey gelene kadar da üyelik sözleşmesi olsun, gizlilik politikaları olsun hiçbirini okumuyor ve incelemiyoruz. Dikkatli olmakta ve hesapları temiz tutmakta fayda var! Çünkü kullandığınız servis tarafından anonim hesabınıza ait kişisel bilgileriniz paylaşılmasa bile bu hesapta üzerinde paylaştığınız diğer servisler sizin bilgilerinizi ifşa edebilir.

26. Çalışanın İzlenmesi ve İş Yerinde Gizlilik Hakkı

Gizlilik hakkından yazılarda devamlı bahsediyorum fakat bunu kategorilendirip hiç yazmadım. Özellikle sanayi devrimi ve teknolojinin çok hızlı ilerlemesi, üretim için büyük avantajlar getirdiyse de işverenin açgözlülüğü, çalışma saatleri ile özel hayatın iç içe geçmesi dünyayı kocaman bir ticari köy haline getirdi. Peki teknoloji bu konuda kimin tarafını tutuyor?

Ofisi 7/24 izleyen kameralar, işverenin sağladığı cep telefonların takibi ve hatta dinlenmesi, bilgisayarların uzaktan kontrolü, hangi siteye girdiklerini, kimlerle e-posta trafiğine sahip olduklarını ve çalışma ortamına ani ziyaretlerle günümüz iş ortamlarının gizlilik haklarının en çok ihlal edildiği yerlerden biri haline geldi. İşverenin genel düşüncesi bellidir; daha çok kâr etmek, üretim sürecinde çalışanların iş saatleri ve hatta bunu nasıl kullandıkları üzerine tam kontrole sahip olmak. Bu da sonuç olarak gizlilik hakkının işverenin ekonomik çıkarlarıyla ters düştüğünü söylemektedir. Özellikle ticari sırların ifşası, çalışanların güvenilirliği işvereni gizlilik ihlaline ittiği konusunda durulsa da çalışanın iş saatleri ile özel hayatının birbirine girmiş olması, bu iki durumun birbiri içine girdiğini göstermektedir.

Amerika'da yapılan bir araştırmada çalışanlar iş saatlerinin %25'ini Internette gezerek ve e-posta okuyarak harcadıkları ve her 5 işletmeden biri aşırı/yersiz e-posta kullanımından çalışanlarını çıkartmakta²⁴³ olduğunu söylüyor. Bunun bir sonucu olarak, işveren sistem yönetimi masraflarını arttırıyor, çalışanların üzerindeki kontrol ve izleme varlığı üretkenliği azaltıyor, e-posta ve Internet

243http://www.computerworld.com/s/article/9065659/Over_50_of_companies_have_fired_workers_for_e_mail_Net_abuse

aktivitesini bir denetim süzgecinden geçmeye başlıyor. Böylece, iş ortamında takip edilen ve hareketleri izlenen bir çalışan verimliliğini, çalışma ortamı ise moral ve güveni kaybetmektedir²⁴⁴.

Bir çalışanın gizliliği nasıl ihlal edilebilir (*Privacy in the Digital Environment, s. 152*)?

- **E-postaların takibi.** Günümüzde işverenler çalışanlarına (*hepsi olmasa da*) bir e-posta adresi sağlamaktadır. Bu e-postaların içerikleri disk üzerinde bir yer kapladığı için işveren bu konuda istediği gibi davranabilmektedir. Bunu şöyle örneklendireyim; diyelim ki size gelen bir e-postayı silseniz dahi disk üzerinden silinip silinmediği konusunda herhangi bir fikre sahip olamazsınız. Denetim de sizin elinizde olmadığı için işveren isterse bu sildiğinizi düşündüğünüz e-postaları belirli kurallarla (*mesela anahtar kelimeler*) inceleyebilir.
- **İnternet takibi.** İşyerinde İnternet olmazsa olmazlardan. Bazen belirli sitelerin erişime kapatılması (*çalışma alanından dolayı*) mümkün olmayabiliyor. Böyle olunca da işveren çalışanlarının hangi sitelere girip buralarda ne kadar zaman kaybettiklerini de öğrenmek isteyebiliyor. Analiz sonuçları, çalışanın azar yemesini ve hatta işten atılmasına kadar işi götürebiliyor.
- **İçeriğin filtrelenmesi.** Genel anlamıyla tam bir gizlilik ihlali olmasa da anahtar kelimelerle belirli algoritmalar üzerinden içeriğin filtrelenmesi erişim olanaklarını olumsuz yönde etkilemekte, bazen çalışanın ihtiyaç duyduğu içeriklere ulaşamamasına neden olmaktadır.
- **Yüklenen yazılımların takibi.** Burada temel neden iş

²⁴⁴<http://www.emeraldinsight.com/journals.htm?articleid=848053>

ortamında kullanılan bilgisayarlara zararlı yazılımların bulaşmasını engellemek ve lisanssız yazılımlar yüzünden sıkıntıya düşmemektir. Fakat, bunun takibi iş saatleri dışında olabildiğinden biri sizin bilgisayarınızı bunun için tarayabilir ve size sormadan yazılımları silebilir. İşveren size o bilgisayarı verdi diye kafasına estiğince siz yokken girip incelemesi bir ihlaldir.

Sıradan eleştirerek ilerleyelim:

E-postalar yukarıda da bahsettiğim üzere siz silseniz dahi disk üzerinde kalabilir ve işveren tarafından incelenebilirler. Bir diğer nokta da e-postaların bu şekilde takip edilmesi üçüncü şahısların gizliliğini de ihlal etmektedir. Şöyle anlatayım; e-posta gönderdiğiniz kişinin iletişim bilgilerini ve mesaj içeriğini sadece sizinle onun arasında geçen bir iletişime ait olarak kullanıldığını düşünürken, işverenin bunu takibe alması hem mesajı hem de iletişimde olduğunuz kişiye ait (*varsa*) özel bilgilerin ifşasına neden olur. Bu yüzden işveren sadece çalışanın gizlilik hakkını değil iletişim halinde olunan üçüncü kişilerin de gizlilik hakkını ihlal eder.

Çalışanın Internet'te hangi sitelere girdiğini, hangisinde ne kadar süre harcadığını detaylı bir şekilde takip etmek uzaktan zararsız gibi gözükebilir. Hatta şöyle bir inanç da var; işveren uygunsuz bir şeyi farkedirse çalışanın azarlar, konu kapanır. Durum malesef bundan daha karışık. Şimdi bunu örneklendirerek anlatayım. Diyelim ki siz bir eşcinselsiniz (*illa olmanız şart da değil*), eşcinsel arkadaşlık sitelerini ziyaret ediyor, LGBT haberleri okuyor, etkinliklerini takip ediyorsunuz. İşvereniniz ise Internet takibi yaptığı için sizin eşcinsel olduğunuzu (*olmasanız bile*) düşünüyor, eğer

eşcinselliğe olumsuz yaklaşıyorsa iş yerinde (*sadece işveren tarafından değil*) size karşı homofobik tutumlar sergilenebilir, cinsel tacizlerde bulunulabilir. Tekrar diyeyim, illa eşcinsel olmanız da şart değil. Eşcinsel cinayetlerin sayısındaki artışa ait bir haber bile homofobik bir işvereni size karşı olumsuz tutumlar içine itebilir. Devam edelim, bir kanserle ilgili doktor sitelerini gezip bilgi toplamanız işverenin sizi hasta olarak algılamasına ve sizinle uzun vadeli çalışamayacağını düşünüp işten çıkarmaya bile yol açabilir.

İçerik filtrelemesi -bence- en zarar verici ihlallerden biridir. Bunda biraz daha uç örnekler vereyim. Çalıştığınız iş yeri çeşitli kelimeleri filtreliyor ve bunlara her türlü erişim yasaklanıyor. Örneğin, ateizm, ateist, atheist, atheism, agnostik gibi kelime grubunu filtrelenmiş durumda. Bu, sadece Internet'te ateizm ilgili herhangi bir içeriğe erişimi değil ateist çalışanların ifade özgürlüğü ve inanç özgürlüğünü de etkiler. Buna gizlilik literatüründe dondurucu etki de denir. Hem doğrudan hem de dolaylı yoldan çalışanın gizliliği ihlal edilmiş olur, beraberinde diğer özgürlükleri (**ifade, inanç vs**) de kısıtlanmış olur.

E-posta, Internet takibi ve içerik filtrelemesini bir arada incelersek; Internette gezmek ve e-postalar çalışanın kendi kişisel kimliğine işaret eder. Ayrıca, iş yeri çalışanların birçok etkileşimde bulunduğu sosyal bir alandır. Bu alanda gizlilik hakkının korunması gerekir. Internet'te özgürlük konuşma özgürlüğü tarafından korunur. Takip edildiğini bilen bir çalışan kendini açıkça ifade edemeyecektir. Böylece konuşma özgürlüğü engellenmiş olacaktır. İnancını, cinsel görüşünü veya düşüncelerini gizlemek, iş yerinde yaşayabileceği baskılardan dolayı da olmadığı gibi gözükme durumunda kalabilir.

Ayrıca, tüm bu haklar birbirleri ile etkileşim halindedir. Örneğin, inanç özgürlüğü, bunu ifade edemedikten ya da bu inancın gerekliliklerini yerine getiremedikten ve özgürce bunları söyleyemedikten sonra bir şey ifade etmez. Bununla birlikte, çalışanların beklentilerine işveren tarafından saygı duyulması gerekir. İşverenin bu şekilde yapacağı takipler ya da işverenin böyle bir takip yaptığı söylememesi, çalışanları olumsuz yönde etkiler.

Size tahsis edilen bilgisayara herhangi bir yazılım kurdunuz ve siz yokken bu yazılım farkedildi. Görevli bilgisayarı açtı ve yazılımı sildi. Sabah geldiniz, bilgisayarınızı açtınız, yazılım yok, biri bilgisayarınıza **“böyle şeyler kurma”** diye not bırakmış. Size tahsis edilen bilgisayar, bir başkasının kafasına göre açıp bir şeyleri silebileceği ya da kurabileceği bir şey olmamalıdır. Burada genel bahane sisteme sızabilecek, bilgi çalabilecek her türlü zararlı içeriğin yüklenen yazılımdan gelebileceğidir. Eğer böyle bir olasılıktan bahsediliyorsa, bunu engellemek çalışanın bilgisayarının takibi ile değil çalışana temin edilecek yazılımdan, iyi bir güvenlik duvarından, anti-virüs programlarından vs. geçer. Ek olarak, bana göre bir görevlinin gelip **“Bilgisayara ne yükledin? Aç bakacağım!”** demesi bile kabul edilebilir bir şey değildir.

Başka bir olumsuzluktan bahsedecek olursak, çalışma ortamının evden olduğu durumlarda işverenin herhangi bir takip yapması sadece çalışanın gizliliğini ihlal etmez. Çalışanın aile ve özel yaşamına dair gizlilik hakları da çiğnenmiş olur. İşveren şunu iyi anlamalı; çalışan onun mülkiyeti değildir. Eğer tüm bu izlemeleri ticari sırların, şirkete ait özel bilgilerin ya da lisansların sızdırılmasını ya da kaynak israfını engellemek amacıyla yaptığını söylüyorsa,

işveren bunlar için gizlilik haklarını ihlal etmeye yönelmemeli. Onun yerine bu hakların sızdırılması ve sonrasında işvereni koruyacak ve iş yerinde gizlilik hakkını ihlal etmeyecek yasaların oluşturulması için çaba sarfetmelidir.

Teknoloji bu konuda kesinlikle tarafsız olmalı. Ne pazarı domine eden gücün haklarını ne de bir başkasının haklarını koruyup diğerlerini hiçe saymalı. Yukarıda da bahsettiğim üzere bu haklar iş içi geçmiş durumdadır. Konuşma özgürlüğü olmayan bir çalışandan inanç özgürlüğü beklenemez. Bu, toplum için de geçerlidir. Bir gizlilik hakkının ihlali iş ortamını bir taciz ortamına dönüştürebilir. Çalışanı dolaylı (veya *doğrudan*) olarak farklı görüşlerin baskısı altında kalmasına neden olabilir.

Sonuç, çalışan iş yerindeki gizliliğini kontrol edememekte, İnternet'te hangi sitelere girdiği, gönderdiği e-postalar takip edilmekte, konuşma özgürlüğünden uzak ve verimliliğini kaybetmektedir. İş yerinde gizlilik hakkı daha çok pazar güçleri tarafından gizlice düzenlendiği için işveren kâr maksimizasyonu hırsıyla birçok tacize ve hak ihlaline neden olabilecek bir iş ortamı oluşturmaktadır. İş yerinde gizlilik hakkı ve çalışanın izlenmesini engellemek yasal bir düzenleme ile korunmalıdır.

27. Girift Haklar

Gizlilik hakkı birçok hakla girift haldedir. Bu hakkı ihlal etmek ya da birilerinin çıkarları için kullanmak veya sadece muktedire hizmet etmesi diğer hakların da doğrudan etkileneceği anlamına gelir. Bir inceleme yazısı olarak eleştirilerinizi bekler.

Girift: Birbirinin içine girip karışmış, girişik, çapraşık.

Önce gizlilik hakkının bize ne ifade etmesi gerektiğine bir bakalım ve kısaca tanımlayalım:

“Gizlilik hakkı, bizi biz yapan şeylerin tümünü içeren, örneğin bedenimiz, evimiz, mülkiyetimiz, düşüncelerimiz, duygularımız, gizlerimiz ve kimliğimiz gibi, bizi çevreleyen bir alana sahip olma hakkıdır. Gizlilik hakkı, bizlere, bu alandaki parçalara kimlerin erişip erişemeyeceğini, ve açığa çıkarmak istediğimiz parçaların kapsamını, niyetini ve zamanlamasını kontrol etme yeteneği verir.”

Tanımda da görüldüğü üzere gizlilik bizi biz yapan değerlerin tümünü içeren bir yapıya sahiptir. Gizlilik açık toplumlar için bir gerekliliktir. Gizlilik, gizli kapaklı işler yapmak ya da **“saklanmak”** değildir. En önemli noktası ise kişi eğer kimliğini açıklamak istiyorsa **“kendi”** açıklar, açıklayacağı kişileri ve zamanını kendi seçer. Genelden özele doğru gideceksek eğer gizlilik hakkından özel hayata doğru bir yol izlemek daha uygun gözükmemekte. Fakat, aynı yöntemle özel hayattan gizliliğe doğru da alternatif bir yol izlenebilir. Seçimini ilk söylediğim yol üzerinden yapacağım.

Açık toplum, devletin şeffaf, bürokrasiden uzak, toleranslı olduğu, sırrını halkından gizlemediği, otoriterlik karşıtı bir yapıyı ifade eder. Açık toplum için o toplumda ifade özgürlüğünün olması şarttır. İfade özgürlüğü bireyin düşüncelerini açıklamasıdır. Düşünce ise bir kişi, olay vs. hakkında görüş sahibi olmak, zihinsel hüküm kurmak, değerlendirmek ve yorumda bulunmaktır. Bunu ise yazıyla, sözle, resimle, fotoğrafla, video vs. ile yansıtmasıdır. Zihinsel hüküm şunu söyler; bu süreç bireyin kendi iç dünyasındadır, başkası tarafından bilinemez. Birey özgür olarak düşünemiyorsa, kendini özgürce ifade edemez. Ayrıca, düşüncenin oluşabilmesi için birey kaynaklara özgürce ulaşabilmeli, erişmek istediği bilgileri özgürce seçebilmelidir.

Şimdi gizlilik hakkının ihlal edildiğini düşünün. Örneğin, iletişim sürecinde herhangi bir mekanizma tarafından (*dinleme vd. yollarla*) kişisel kimliğiniz ve mesaj içeriğiniz ifşa edildi. İletişim süreci içerisinde kendinizi özgürce ifade ettiğinizi düşünmekteydiniz. Yazılı veya sözlü, nasıl olduğunun çok bir önemi yok. Sonuçta, gizliliğinizle birlikte iletişim özgürlüğünüz ihlal ve ifşa edildi. Böylece ifade özgürlüğünüz darbe yemiş oldu. Bu ihlalden dolayı artık kendinizi rahatça ifade edemeyecek, düşüncelerinizi “**kimliğim ifşa edilirse**” korkusu yüzünden açıklayamayacak, daha farklı davranacak, dürüstlüğünüzden ödün vermeye başlayacaksınız.

Gizlilik ihlali = İletişim gizliliği ihlali -> Düşünce özgürlüğü ihlali -> İfade özgürlüğü ihlali

Dijital bir çağda yaşıyoruz. Kendimizi en çok ifade ettiğimiz yerlerden biri Internet. Yazılı, sözlü, görsel, işitsel, her türlü ifade şeklini rahatça yapabilmekteyiz. Sadece biz değil, basından, partilere aklınıza gelebilecek herkes, her oluşum kendini Internet'te ifade etmekte. Internet'te yapılacak herhangi bir sansür doğrudan ifade özgürlüğünü kısıtlar. Çünkü, Internet özgürlüğü ifade özgürlüğünün koruyucusudur. Eğer herhangi bir sitede kendini ifade edenlerin kimlikleri ifşa edilirse, site sansürlenir olmadı içerikler kaldırılmaya zorlanırsa, ifade özgürlüğünü de sansürlemiş olur zıt düşünceleri ortadan kaldırılmış olur. Devletin buradaki rolü kendi koyduğu normlara uygun düşmemeyi güvence altına almaktır, engellemek değil. Devlet eğer bir sınırlama yapacaksa uluslararası sözleşmelerle çizilmiş meşru sınırları dikkate almalı. Kısaca bir örnek verirsem, müslüman iktidar için ateist içerikler sansürlenemez.

Gizlilik ihlali = Internet sansürü -> Düşünce özgürlüğü ihlali -> İfade özgürlüğü ihlali

Birey ev, aile ve özel hayatında gizlilik hakkına sahiptir. Bunun nasıl ifşa edildiğinin -bence- bir önemi yok. Seks kasedi, bireyin özel hayatına dair ses kayıtları, görseller vs. Bunu sadece ahlaksızlık ya da **“sevişiyorlarsa bizi ilgilendirmez”** diye kestirip atmak büyük resmi görmemizi engeller. Özel hayatı ifşa olan (*sadece özel hayat değil elbette*) birey kendini ister istemez bireysel-sansüre alır. Sadece hareketlerini değil düşüncelerini de sansürler. Düşüncelerini sansürleyen birey, ifade özgürlüğünü de kısıtlar. Görebildiğiniz üzere bir gizlilik ihlali yapıldığı zaman diğer hakların nasıl etkilendiği çorap söküşü gibi gelmekte.

Gizlilik ihlali = Özel hayatın ifşası -> Bireysel-sansür -> Düşünce özgürlüğü sansürü -> İfade özgürlüğü sansürü

Bireyin nereye gittiğinin ve nasıl gittiğinin fişlendiğini THY'nın kendisiyle uçanları MIT ile fişlediklerinden öğrenmiştir. Birey, seyahat özgürlüğüne sahiptir. Anayasal bir hak olarak birey yaşadığı ülke içinde özgürce dolaşabilir ya da oturma izni alabilir. Bireyin nereye ne zaman gittiğini sadece kullandığı şirket bilmelidir. Bunun ifşa edilmesi ya da üçüncü şahıslarla paylaşılması dahi düşünülemez.

Gizlilik ihlali = Seyahat özgürlüğü ihlali (ifşası, paylaşılması)

Örnekler çoğaltılabilir, hak ve özgürlükler kapsamında daha da ilerlenebilir. Görüldüğü üzere bu hakların hepsi giriftir. Birini ihlal ettiğiniz zaman ya bu süreç içerisinde ya da sonrasında diğer hakları da ihlal etmiş oluyorsunuz. O yüzden sürekli vurguladığım şey şu; bir hakkın eksik, kusurlu, muktedirin çıkarlarını korumaya yönelik ya da kontrolü altında olması diğer hakların da bundan etkileneceği ve eksik, kusurlu veya doğrudan muktedirin çıkarlarını koruyacağı ya da kontrolü altında kalabileceğidir. İhlal edilen sadece sizin hakkınız değil, herkesin hakkıdır.

Birinin düşüncelerine katılın veya katılmayın ama onun bunları özgürce söylebilmesi için çaba sarfetmeniz ve bunun için çalışmanız gerekmektedir.

28. Arch Linux'u USB Belleğe Kurmak

Bu rehberin amacı kendinize ait ve USB bellek içinde taşıyabileceğiniz, sizin özelleştirdiğiniz ve kurulumun her adımını bilerek yaptığınız bir GNU/Linux'a sahip olmak. Yani, ihtiyaçlarınız nelerse sadece onları ekleyecek, her an yanınızda taşıyabilecek ve sorunsuz bir şekilde güvenle kullanabilecek, kişiselleştirilmiş bir dağıtımınızın olması.

Herhangi bir GNU/Linux dağıtımını da USB belleğinize yazdırabilir, tüm bu aşağıda anlattığım kısımlara girmeden kolayca USB belleğinizde çalışan bir dağıtıma sahip olabilirsiniz. Fakat bu yöntemin sağlayacağı faydalara bakarsak eğer:

- Kurulumun her aşamasını görme, yapma ve düzenleme fırsatına sahip olacaksınız.
- Bu sizin GNU/Linux bilginizi arttıracak mükemmel bir fırsat olabilir.
- İstemediğiniz bir sürü gereksiz uygulama yerine sadece sizin istediğiniz uygulamalardan oluşan bir sisteme sahip olma olanağı.
- Güvenliği kendi ihtiyaçlarınız doğrultusunda sağlayabilme (iptables vs).
- Güvenmediğimiz makinelerde kullanabilme. (Eğer internet dinleniyorsa gene güvenliğiniz tehlikede olabilir fakat Tor ve VPN seçenekleri mevcut.)

O kadar faydasını saydım peki bize zararı olabilir mi?

- Zaman gerektirebilir.
- Aşamalarda karşılaşılabileceğiniz sorunlar sizi yıldırabilir. Ama yılmayın, arayın muhakkak yazılmış bir şeyler bulursunuz.

Karışık bir rehber gibi gözükebilir ama elimden geldiğince her şeyi çok açık olarak yazacağım. Önce, elimizde GNU/Linux kurulu bir sistem olursa (*Arch olmadığı varsayılarak anlatılacak rehber*) sorunsuz bir şekilde ilerleyebilirsiniz. Hemen hemen tüm işlemler root olarak gerçekleştirilecek, o yüzden dikkatli olmanızda fayda var. Komutlar “~ \$” ile düzenlenecek kısımlar “#” (başlarına # koymayın) ile gösterilmiştir.

1. USB belleği biçimlendirmek

USB belleğimizi taktık ve öncelikle bunda bir bölüm oluşturmalıyız. Bu da cfdisk'i kullanarak yapacağız. Sizin dikkat etmeniz gereken USB'nin bağlama noktasının ne olduğu. Ben /dev/sdc olarak alıyorum. Sizde bu /dev/sdb olabilir veya /dev/sd[x] (x herhangi bir değer) olabilir. Yanlışlıkla kullandığınız alanı seçerseniz bilgileriniz silinecektir.

```
~ $ cfdisk /dev/sdc
```

```
New -> Primary -> Linux, Write diyerek yazıyor ve Quit diyerek bu ekrandan çıkıyoruz.
```

2. Arch Linux Bootstrap paketi

Arch Linux'un cd imajını yazdırıp oradan da gidebilirsiniz. Fakat, bu rehberde bootstrap ile kurulumu gerçekleştireceğiz.

Öncelikle Arch Linux'un bu paketini indirip arşivden çıkartmalıyız. İndireceğiniz dizinde açacağınızı varsayıyorum.

```
~ $ wget -c http://mirrors.kernel.org/archlinux/iso/2013.12.01/archlinux-bootstrap-2013.12.01-x86_64.tar.gz
~ $ tar xzf archlinux-bootstrap-2013.12.01-x86_64.tar.gz
```

Arşivi çıkarttıktan sonra elimizde root.x86_64 adında bir klasörümüz olacak. Burada chroot olmadan önce Arch Linux'un yansı dosyasını düzenlemeliyiz.

```
~ $ nano root.x86_64/etc/pacman.d/mirrorlist
```

Size en yakın olan sunucunun başındaki # işaretini kaldırın ve kaydedip çıkın. Buradan sonra şu işlemleri gerçekleştirin:

```
~ $ cp /etc/resolv.conf root.x86_64/etc
~ $ mount --rbind /proc root.x86_64/proc
~ $ mount --rbind /sys root.x86_64/sys
~ $ mount --rbind /dev root.x86_64/dev
~ $ mount --rbind /run root.x86_64/run
```

Önemli noktaları bağladıktan sonra chroot için artık hazırız:

```
~ $ chroot root.x86_64 /bin/bash
```

Kuruluma geçmeden önce son adım olarak Arch Linux paket yöneticisi pacman'ın anahtarları kurması gerekmektedir.

```
~ $ pacman-key --init  
~ $ pacman-key --populate archlinux
```

İlk bölümde USB belleğimizde bir alan oluşturmuş fakat bunu biçimlendirmemiştik. Şimdi bu oluşturduğumuz alanı biçimlendirelim:

```
~ $ mkfs.ext4 /dev/sdc1 -L /
```

Görüldüğü üzere “-L /” ile biçimlendirdiğim bu alana “/” etiketini verdim. Bu seçenek size kalmış. Ext4 yerine farklı bir dosya sistemi de seçebilirsiniz. Daha sonra USB belleğimizi bootstrap altında bağlamalıyız:

```
~ $ mount /dev/sdc1 /mnt
```

Her şey buraya kadar yolunda gittiye rahatça kuruluma geçebiliriz.

3. Arch Linux kurulumu

Önce, temel Arch Linux kurulumu gerçekleştirip Grub yerine Syslinux'u tercih edeceğiz. Grub'la devam etmek isteyen varsa kurulumu yapıp Grub ayarları için Arch Linux'un wikisine bakabilir. Biraz sıkıntılı olduğu için ben Grub'u atladım. Syslinux hiç sıkıntı çıkartmadı bana. Temel kurulum:

```
~ $ pacstrap /mnt base syslinux
```

Bu işlem biraz sürebilir. Yaklaşık 150mb kadar paket indirip kuracak. USB belleğinizin yazma hızı da önemli. Kurulum tamamlandıktan sonra fstab'ı oluşturalım:

```
~ $ genfstab -p /mnt >> /mnt/etc/fstab
```

Burada /dev/sdc1 olarak değil de UUID üzerinden gitmeliyiz. Çünkü farklı makinelere taktığımız zaman bağlama noktası farklılık gösterebilir ve sistemimiz açılmayabilir. USB belleğinizin UUID numarası fstab içinde var. Eğer yoksa:

```
~ $ ls -l /dev/disk/by-uuid/
```

```
total 0
```

```
lrwxrwxrwx 1 root root 10 Dec 31 17:09 6c27259c-bff8-42a2-b14a-  
df16aad78ba4 -> ../../sdc1
```

UUID numaranız 6c27259c-bff8-42a2-b14a-df16aad78ba4, fstab ise:

```
~ $ nano /etc/fstab  
  
#        UUID=6c27259c-bff8-42a2-b14a-df16aad78ba4    /    ext4  
defaults,noatime 0 1
```

Şeklinde düzenlemeniz yeterli. Buradan sonra syslinux'u kurarak ayarlarını gerçekleştireceğiz:

```
~ $ syslinux-install_update -i -a -m  
~ $ nano /boot/syslinux/syslinux.cfg
```

Syslinux'un ayar dosyasını açtıktan sonra LABEL Arch kısmını bulun ve USB belleğinizin UUID numarasını yazın:

```
LABEL Arch  
MENU LABEL Arch Linux  
LINUX ../vmlinuz-linux  
APPEND root=UUID=6c27259c-bff8-42a2-b14a-df16aad78ba4 ro  
INITRD ../initramfs-linux.img
```

Kaydedin ve çıkın. Şimdi sıra Arch Linux içinde chroot olmaya geldi:

```
~ $ arch-chroot /mnt
```

Hostname -diğer deyişle bilgisayarınızın adı- oluşturalım:

```
~ $ nano /etc/hostname
```

Hosts dosyamızı düzenleyelim (*localhost'u bilgisayarınızın adıyla deęiştirin*):

```
~ $ nano /etc/hosts
```

Vconsole dosyamızı -klavye, yazı tipi düzeni- oluşturalım:

```
~ $ nano /etc/vconsole.conf  
# KEYMAP=trq  
# FONT=iso09.08
```

Locale dosyamızı -sistem dilini- oluşturalım:

```
~ $ nano /etc/locale.conf  
# LANG=tr_TR.UTF-8
```

Yerel saatimizi belirleyelim:

```
~ $ ln -s /usr/share/zoneinfo/Europe/Istanbul /etc/localtime
```

Karakter desteęi (başlarındaki # işaretini kaldırın):

```
~ $ nano /etc/locale.gen
```

```
# tr_TR.UTF-8 UTF-8
# tr_TR ISO-8859-9
~ $ locale-gen/
```

Initramfs imajını oluşturmadan önce mkinitcpio.conf dosyası içinde küçük bir yer değişikliği yapacağız (*block görüldüğü üzere udev'den sonra gelecek*):

```
~ $ nano /etc/mkinitcpio.conf
# HOOKS="base udev block autodetect modconf filesystems
keyboard fsck"
~ $ mkinitcpio -p linux
```

Root şifremizi belirleyelim:

```
passwd
```

Kullanıcı (kullanici yerine kendi kullanıcı adınızı seçin) ve kullanıcı şifresi oluşturalım:

```
~ $ useradd -m -g users -G
audio,video,wheel,storage,optical,power,network,log -s /bin/bash
kullanici
~ $ passwd kullanici
```


4. Xorg kurulumu

Şimdi Xorg kuracağız. Farklı makinelerde çalışan bir sistem hazırladığımız için Xorg'u tüm sürücülerıyla kurmalıyız (all diyin).

```
~ $ pacman -S xorg
```

5. ALSA kurulumu

Ses için gerekli olan ALSA paketini kurmamız gerekmektedir:

```
~ $ pacman -S alsa-utils alsa-firmware
```

6. NetworkManager kurulumu

Ben NetworkManager'ı seçtim. Wicd veya başka alternatifler size kalmış. NetworkManager'ı seçmemdeki neden OpenVPN. Kurulumu bunu da dahil edeceğiz:

```
~ $ pacman -S networkmanager networkmanager-openvpn networkmanager-applet
```

```
~ $ systemctl enable NetworkManager
```

7. Masaüstü ortamının kurulması

USB belleğinizin boyutu ne kadar bilmiyorum. Tavsiye olarak ben pencere yöneticisi ya da LXDE gibi hafif masaüstü ortamlarını tercih ederdim. Rehberde LXDE'yi seçtim. Bu seçim size kalmıştır, isterseniz XFCE, isterseniz Openbox vs. de kurabilirsiniz. Fakat seçimlerinizin yanında bir tane de giriş yöneticisi seçmeli ve

ayarlamalısınız. LXDE'de lxdm var o yüzden farklı bir şey seçmemize gerek yok.

```
~ $ pacman -S lxde ntfs-3g dosfstools
~ $ systemctl enable lxdm
```

8. Basit bir kişiselleştirme

Buradan sonra kullanmak istediğimiz programların kurulumu var. Ben basit bir örnek üzerinden göstereceğim. Tarayıcı seçiminden ofis ortamına kadar her şey size kalmıştır.

```
~ $ pacman -S firefox pidgin pidgin-otr abiword abiword-plugins
gnnumeric transmission-gtk icedtea-web-java7 gimp epdfview tor vlc
ttf-dejavu
~ $ systemctl enable tor.service
```

Kurulumda indirilen paketleri yer kaplamaması için temizlemek isterseniz:

```
~ $ pacman -Scc
~ $ exit
```

9. Son adımlar

Buraya kadar da her şey sorunsuz bir şekilde kurulmuşsa artık bağlama noktalarını kaldırabilir ve chroot'tan çıkabiliriz.

```
~ $ umount /mnt  
~ $ exit  
~ $ umount -lf root.x86_64/proc  
~ $ umount -lf root.x86_64/sys  
~ $ umount -lf root.x86_64/dev  
~ $ umount -lf root.x86_64/run
```

Artık bilgisayarınızı USB belleğinizden başlatabilir ve Arch Linux'unuzu kullanmaya başlayabilirsiniz. Kurulumun 5, 6, 7 ve 8. adımları kuracak kişiye kalıyor. Burada her adımı kendinize göre özelleştirebilir ve istekleriniz doğrultusunda kurulum yapabilirsiniz. Hepinize kolay gelsin, iyi yıllar.

İletişim

Twitter: <https://twitter.com/songuncelleme>

E-posta: kusburnu@riseup.net

Blog: <https://network23.org/kame>

Bağış: 17qsapk4FzU9hpQP65GKmDe7WZrAv6J3vZ (BTC)