İnternette Anonimlik ve Tor Projesi

FBI ve ABD Adalet Bakanlığı tarafından hazırlanan el ilanında, vatandaşlar internet kafelerdeki terörist faaliyetlere karşı duyarlı olmaya çağrılıyorlar (bkz. http://info.publicintelligence.net/FBI-SuspiciousActivity/Internet_Cafe.pdf). El ilanı, vatandaşların teröristi nasıl tanıyacağı konusunda ipuçları veriyor. İnternette terörist ve devrimci yazının incelenmesi, polise ve hükumete karşı mücadele taktiklerinin araştırılması, silah, patlayıcı madde ya da askeri teçhizatlar ile ilgili belgelerin indirilmesi, internette gezinirken ip adreslerini gizleme amaçlı web sitelerinin ya da anonimleştiricilerin kullanılması şüpheli durumlar olarak nitelendiriliyor.

Her şey bir yana, internette anonim gezintinin şüpheli davranışlar listesine girmesi, internette gözetim olgusunun ABD hükumetinin gözünde olağanlaştığını gösteriyor. İnternete içsel olan anonim kullanım eğilimi, Google ve Facebook gibi bilişim şirketlerinin baskısıyla kimliklendirilmeye çalışılıyor. Kullanıcıların Facebook'a gerçek kimlikleriyle üye olmaya zorlanması, Gmail'in arada bir bizden telefon numaramızı istemesi ve son derece geniş bir uygulama yelpazesine sahip olan Google'ın uygulamalarında tek ve bütünleşik bir gizlilik politikası kullanmaya başlaması bu kimliklendirme sürecinin bir parçası. Daha önceki sayılarımızda, yeni gözetime, internetteki hareketlerimizin kaydedilip analiz edildiğine, sosyal ağlardaki ilişkilerimizin analizinden elde edilebilecek verilere yer vermiştik. Bu yazıda ise internette anonimlik ve bunun hükumetlere ve şirketlere rağmen nasıl gerçekleştirilebileceği tartışılacak.

Anonimlik Nedir?

Anonimlik, en az iki kişiyi içeren toplumsal bir ilişkidir. Bir diğer deyişle, dağ başında, insanlardan uzakta tek başına yaşayan biri için anonimlik söz konusu değildir. Bir kişinin mutlak anonimliğinden bahsedebilmemiz için kimliğini belirlenebilir kılan aşağıdaki yedi boyutun hiçbirinde tanımlanabilir olmaması gerekir (http://web.mit.edu/gtmarx/www/anon.html):

1- Ad Soyad : Kim sorusuna verilen yanıttır. En temel kimlik bilgisi, kişinin adı ve soyadıdır. Bu bilgi, kimi zaman ayırt edici olmayabilir. Bu nedenle, anne ve baba adıyla da ilişkilendirilebilir.

2- Adres : Nerede sorusuna yanıt verir. Normal adres bilgisinin yanı sıra, telefon numarası ve e-posta adresi de bu kapsamda değerlendirilir.

3- Kalıcı kodlamalar: TC kimlik numaralarımız buna en güzel örnektir. Ad soyad ya adres bilgisi, birden fazla kişiye işaret edebilir. Fakat TC kimlik numarası tektir. Bunun yanında, dernek, meslek odası, parti vb üye numaraları da özel kodlamalar sınıfına girer. Hepsinin ortak yanı, ortada bir aracı kurumun olması ve kodlarla gerçek kişileri eşleştirmesidir.

4- Geçici kodlamalar: Kişiye ait geçici kodlar oluşturulabilir. Örneğin bazı ülkelerde AIDS testlerinin sonuçları bu geçici kodlar üzerinden takip edilir ve bu geçici kodların kişinin adı ya da adresi ile doğrudan ilişkisi yoktur.

5- Görünüşe ya da davranış kalıplarına dayalı kimliklendirme: Bazen kişiye dair net bilgi olmamasına karşın "hafta içi her gün saat 8:00'da işe giden uzun boylu adam" tarzında kimliklendirmeler de yapılabilir. Ya da kişi internetteki bir sohbet odasında yazışırken bazı kelimeleri sürekli yanlış yazıyor ve aynı imla hatalarını tekrarlıyorsa, kişi ad ve soyad olarak

tanınmamasına rağmen davranış kalıplarına göre kimliklendirebilir.

6- Toplumsal kategoriler: Kişiler, ırk, din, dil, sınıf, cinsiyet, cinsel yönelim ya da bir kuruluşa üyelik bağlamında tanımlanabilirler.

7- Seçilebilirlik sembolleri: Herhangi bir yere giriş şifresi, kodu, giyilen üniforma, dövme vs tanımlanabilirliğin bir diğer boyutudur.

Pfitzmann ve Hansen tarafından hazırlanan ve anonimlik tartışmalarında kullanılan kavramlara açıklık getiren çalışmaya göre, saldırganın perspektifinden bakıldığında anonimlik, saldırganın özneyi yeterince belirleyememesidir (bkz . http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf). Anonimlik mutlak olarak değerlendirildiğinde, İnternet üzerinden mesaj atan n tane kullanıcı varsa saldırganın özneyi tespit etme ihtimali 1/n'dir. Fakat burada, yeterince kelimesine dikkat edilmesi gerekir. Anonimlik için farklı durumlarda, farklı eşik değerleri geçerli olabilir. Bilişim teknolojileri, iletişimde 1/n'e yakın anonimlik olanağı sunarken Biz ve 1984 romanlarını aratmayacak düzeyde toplumsal gözetimi kolaylaştırmaktadır.

Anonimliğin savunucularının ve kulllanıcılarının başında gazeteciler gelmektedir. Kimliğini açıklamak ya da kimliğinin kamuoyuna açıklanmasını istemeyen haber kaynakları ve kamu kurumlarındaki yolsuzlukları ismini açıklamadan basına sızdıran bürokratlar gazeteciler için, dolayısıyla da toplum için faydalı olmaktadır.

Alkol ya da uyuşturucu bağımlısı, taciz mağduru, AIDS'le ya da başkalarıyla paylaşmak istemediği herhangi bir hastalıkla mücadele eden bir çok kişi internette gerçek kimliğini gizleyerek araştırma yapabilmekte, benzer sorunları olanlarla iletişime geçebilmektedir.

Şirketler tarafından takip edilmek ve onlardan gelen istenmeyen (spam) mesajlara maruz kalmak istemeyen bir çok insan internette gerçek kimliğini kullanmaktan kaçınmaktadır. Kadınlar, internette erkeklerin tacizine maruz kalmak istemedikleri için cinsiyetlerini erkek olarak belirtmekte ya da kullanıcı adlarını seçerken erkek adlarını tercih ederek anonim kalmak istemektedirler.

İnternete yazılanlar kadar okunan ve ziyaret edilen web siteleri de baskıcı yönetimlerin dikkatini çekebilmektedir. Hem bu nedenle hem de sansürlenen sitelere erişebilmek için dünyada birçok aktivist internet erişiminde anonimleştirici yazılımları kullanmaktadır.

Ya da sadece Google, Facebook, Microsoft vb. şirketlerin hazırladıkları gözetim toplumundan kaçabilmek için anonimleştirici yazılımlar kullanılabilmektedir. 2006 yılında AOL arama motorunda aranan kelimelerin yayınlanmasından ve bunlardan yola çıkarak kişinin gerçek kimliğine ulaşılabilir olmasından sonra bu korku daha çok kendini hissettirmeye başlamıştır: (http://www.thenewnewinternet.com/2010/04/01/staying-anonymous-in-a-time-of-surveillance/).

Ancak İnternet'te anonimliğe karşı çıkanların tezleri de haklı gerekçelere dayanmaktadır. En başta, toplumda suç olarak kabul edilen etkinlikler internette gizlenebilmektedir. Dolandırıcılık, nefret söylemi, uyuşturucu ticareti vb faaliyetler kendini gizleyebilmektedir. Ayrıca bir diyalogda, taraflardan birinin anonimlik hakkı kadar karşı tarafın iletişimde bulunduğu kişiyi tanıma hakkının da olabileceğini göz önünde bulundurmak gerekir. Bu nedenle, farklı boyutları olan ve şu anki şartlarda aşılması olanaksız çelişkiler içeren anonimliğin yararları/zararları tartışmasını bir kenara bırakalım.

Tüm olumsuzluklarına rağmen, ifade özgürlüğü ve bilgiye özgür erişim hakkımız için anonimliğe

gereksinimiz olabilir. Bunu en kolay nasıl sağlayabiliriz?

Anonimleştiriciler

Bu soruya yanıt vermeden önce herhangi bir saldırganın, web sitesinin ya da internet servis sağlayıcının, internet kullanıcılarını nasıl takip ettiğine değinmekte fayda var. İnternete bağlanıldığı anda internet servis sağlayıcısı (ISP) kullanıcıya, ip numarası adı verilen özel bir numara tahsis eder. İnternette gerçekleşen iletişimde kullanıcılar ip numarası aracılığıyla tanımlanır. Bu ip numarası ISP (ttnet, superonline, vodafone vs.) tarafından verildiğinden ve kullanıcının adı da ISP'de tutulduğundan internet kullanıcısının kimliği bilinmektedir. Fakat yukarıda belirtildiği gibi anonimlik, toplumsal bir ilişkidir ve anonimlik sorunsalı kullanıcı internette toplumsal ilişkiler (web sitelerine erişim, e-posta gönderme, bir sunucuya dosya yükleme, sanal sohbet) kurmaya başladığında ortaya çıkar.

İnternette bilgisayarlar belirli protokoller çerçevesinde hazırlanan veri paketlerinin transferi ile haberleşirler. Bu paketler iki tip veri taşırlar: İçerik ve paketin gideceği adresin bilgileri. Günümüzde çeşitli yazılımlarla içeriği şifrelemek olanaklıdır. Ancak paketin gideceği yerle ilgili bilgiler de önemlidir. *Trafik analizi* denilen yöntemle kullanıcılar ya da kullanıcı-web sitesi arasındaki iletişimin, kimin kiminle, ne zaman, ne kadar süre gerçekleştiği bilgisine erişmek mümkündür.

E-posta gönderildiğinde, ip adresi de gönderilir. Örneğin herhangi bir hukuksal sorunda, e-postanın içerdiği ip adresi bilgisinden kullanıcının gerçek kimliğine erişmek mümkündür. Ya da herhangi bir web sitesine erişildiğinde, erişilen sitenin sahibi, ISP veya kullanıcıyla web sitesi arasında pusu kurmuş bir saldırgan iletişimi takip edebilir ve kullanıcının ip adresine ulaşabilir. ISP'ler, ip'leri gerçek kullanıcı kimliklerine dönüştürdüklerinde elde edecekleri istatistiksel bilgilerden kullanıcı profilleri oluşturabilir. Web siteleri de ellerindeki erişim istatistiklerinden çok detaylı analizler yapabilirler.

Devletler ve şirketler, internetin anonim karakterini yok etme ve kullanıcıların faaliyetlerini gerçek kimlikleriyle ilişkilendirme yönünde önemli adımlar atmaktadır. Ancak tam tersi yönde girişimler de vardır. İnternetteki iletişimin tipine göre farklı anonimleştiriciler kullanılmaktadır. Örneğin, iletişimin aynı anda gerçekleşmesine gerek duyulmayan e-posta iletişiminde yüksek gecikmeli anonimleştiriciler kullanılabilirken, web sitelerine erişim ve anlık yazışma için düşük gecikmeli anonimleştiriciler kullanılmaktadır. Yüksek gecikmeli anonimleştiriciler, düşük gecikmeli anonimleştiricilere göre daha yüksek bir anonimlik sağlamaktadır.

İnternetin anonim kullanımı için geliştirilmiş farklı düşük gecikmeli anonimleştiriciler vardır (Ayrıntılı bilgi için bkz. Yüksel(2010)). Bu anonimleştiriciler arasında en yaygını, 1996 yılında ABD Donanması Araştırma Laboratuvarı'nda tasarlanan ve soğan yönlendirmesi (onion routing) adı verilen tasarımdan yola çıkarak gerçekleştirilen Tor'dur (The Onion Router). Tor Projesi, Özgür Yazılım Vakfı tarafından, Toplumsal Fayda İçin Geliştirilen Projeler kategorisinde ödüle de layık görülmüştür. Tor'un yaygın olma nedenlerinin başında tasarımdaki kurulabilirliğin, kullanılabilirliğin, esnekliğin ve sadeliğin rolü vardır. Ayrıca Yüksel'in belirttiği gibi ,

> Kullanımı zor olan anonim sistemlerinin kullanıcı sayısı az olacağından ve az sayıda kullanıcısı olan anonim sistemlerin de anonim kümesindeki eleman sayısı az olacağından kullanım zorluğu anonimliği de azaltır. Bu sebeple Tor kolay kullanımı hedef almıştır. Tor, kullanımı artırmak için Win32, Linux, Solaris, BSD-style Unix, MacOS X işletim sistemleri üzerinde çalışabilecek şekilde geliştirilmiştir. Aynı zamanda Tor kullanımı artırmak için trafik gecikmelerini mümkün olduğu kadar

düşük tutmayı amaç edinmiştir.

Tor, tek bir uygulamaya değildir. Tor'u, kişilerin ya da grupların iletişimini daha güvenli ve mahremiyete duyarlı hale getirmeyi hedefleyen, sanal tünellerden oluşan bir ağ olarak tanımlamak daha yerinde olacaktır. Tor, mahremiyeti gözeten farklı uygulamaların geliştirilmesi için bir temel oluşturur. Tor projesi kapsamında geliştirilen uygulamalardan bazıları:

- Tor web tarayıcısı
- Orbot (Android İşletim Sistemi için)
- Tor2Web (Gizli Tor servislerine erişmek için)
- Tails (Debian Gnu/Linux temelli çalışır Tor Cd'si)

Soğan yönlendirmesinin ortaya çıkışı ve gelişimi, internetinkine benzemektedir. Proje, hükumetin iletişimini daha güvenli hale getirebilmek amacıyla başlatılmasına rağmen Tor bugün, gazeteciler, aktivistler ve normal insanlar tarafından da kullanılmaktadır.

FBI broşüründeki iddianın tersine normal insanlar Tor'u, şirketlerin kullanıcı hakkında bilgi toplayıp bunlardan kazanç sağlamasını ve kişisel bilgi güvenliğini korumakla görevli kurumların aksi davranışlarını önlemek amacıyla kullanmaktadır. Ayrıca, çocuklara internet üzerinden kurdukları iletişimde kimliklerini açık etmemeleri söylense ve onlar da bu öğüdü tutsalar da kötü niyetli kişiler ip adresinden bir takım bilgilere ulaşabilir. Bu nedenle Tor, çocukların internetteki kötü niyetli kişilere karışı korunması için de faydalıdır.

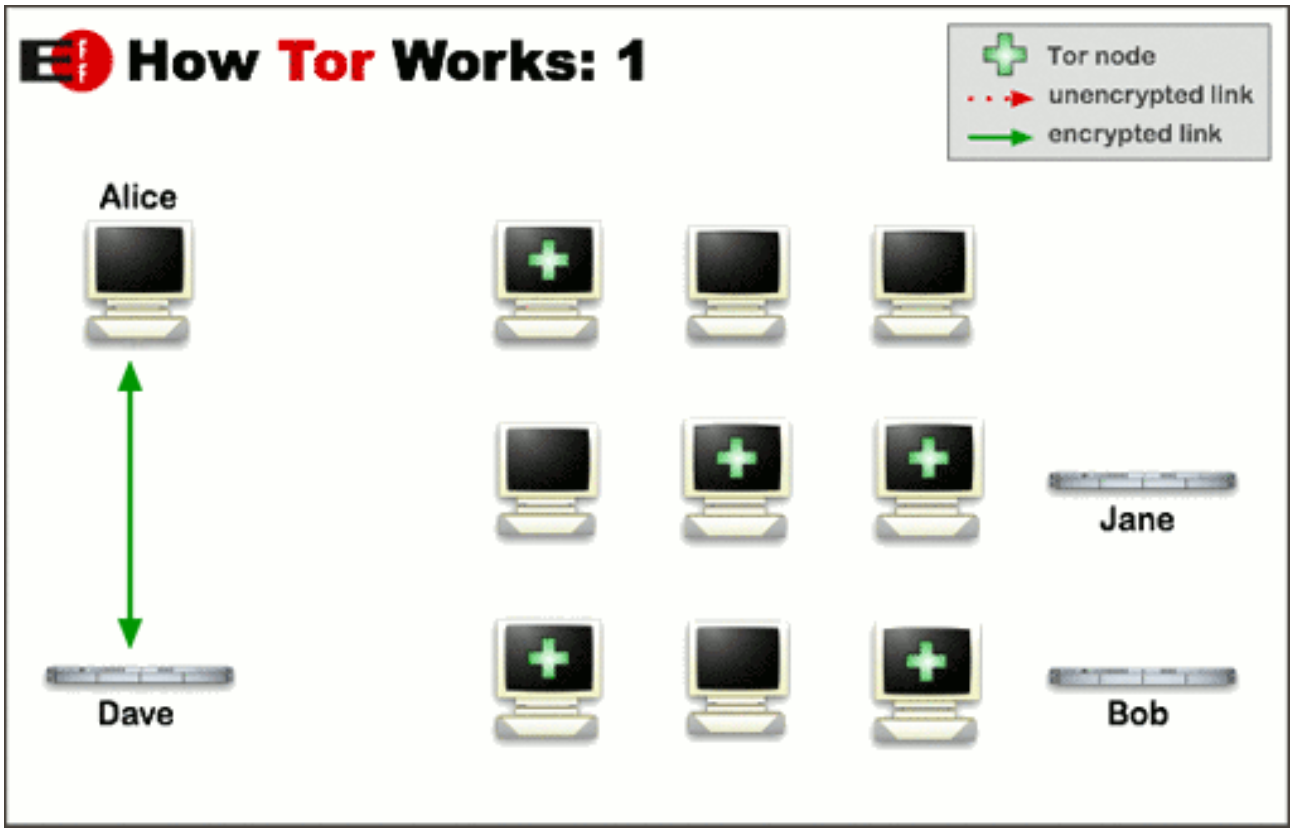
Gazeteciler, Tor ile kimliklerinin açıklanmasını istemeyen haber kaynaklarıyla Tor üzerinden iletişime geçebilirler. Sınır Tanımayan Gazeteciler ve Indymedia adı ile bilinen Bağımsız Medya Merkezi, üyelerinden kendi gizlilikleri ve güvenlikleri için Tor'u kullanmasını tavsiye etmektedir.

Tor'un tüm dünyada aktivistler tarafından kullanımı da son derece yaygındır. Tor hem hükumetlerin elektronik takibini zorlaştırmak, hem de sansürlenen sitelere erişim için olanak sunmaktadır. Örneğin, interneti etkin kullanan bir sınıf hareketinin karşılaşabileceği sorunların başında web sitesinin engellenmesi gelir (bkz http://www.cbc.ca/news/canada/story/2005/07/24/telus-sites050724.html). Böyle olumsuzluklara karşı hazırlıklı olunması gerekir ve Tor bunun için idealdir. İstatistikler, son zamanlardaki gelişmelere paralel olarak Ortadoğu ve Arap ülkelerinde, belirli dönemlerde Tor kullanımının arttığını göstermektedir (Daha ayrıntılı analizler için bkz. https://metrics.torproject.org/users.html?graph=direct-users&start=2009-01-21&end=2012-06-21&country=eg&dpi=72#direct-users).

Tor Nasıl Çalışır?

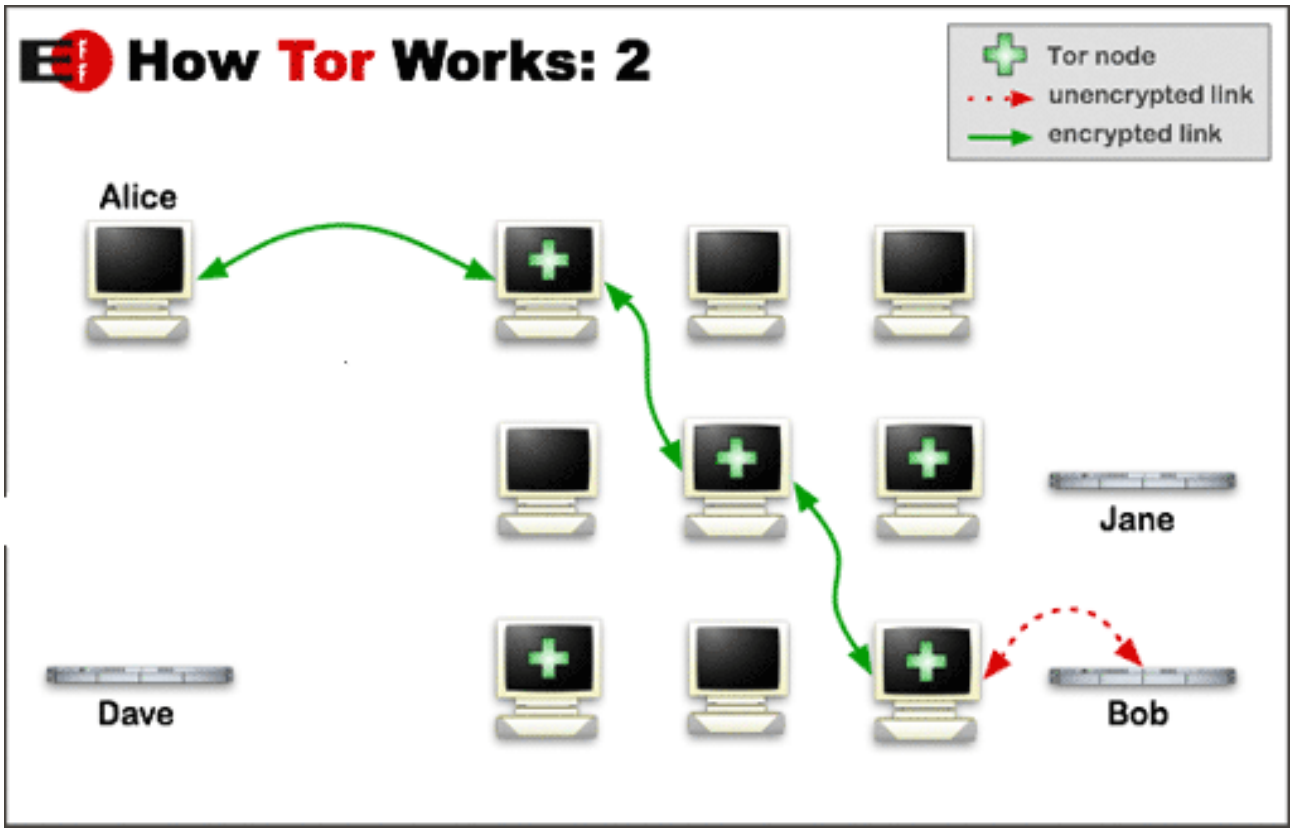
Alice'in Bob adlı bir kullanıcıyla ya da web sitesi ile iletişime geçmek istediğini varsayalım.

Alice'in doğrudan Bob'a erişmesi durumunda, trafik analiziyle iletişimin takibi olanaklıdır. Alice'in kullandığı Tor istemcisi ilk adımda Dave adlı Tor rehberinden kullanabileceği Tor sunucularının listesini alır (Bkz. Resim 1).



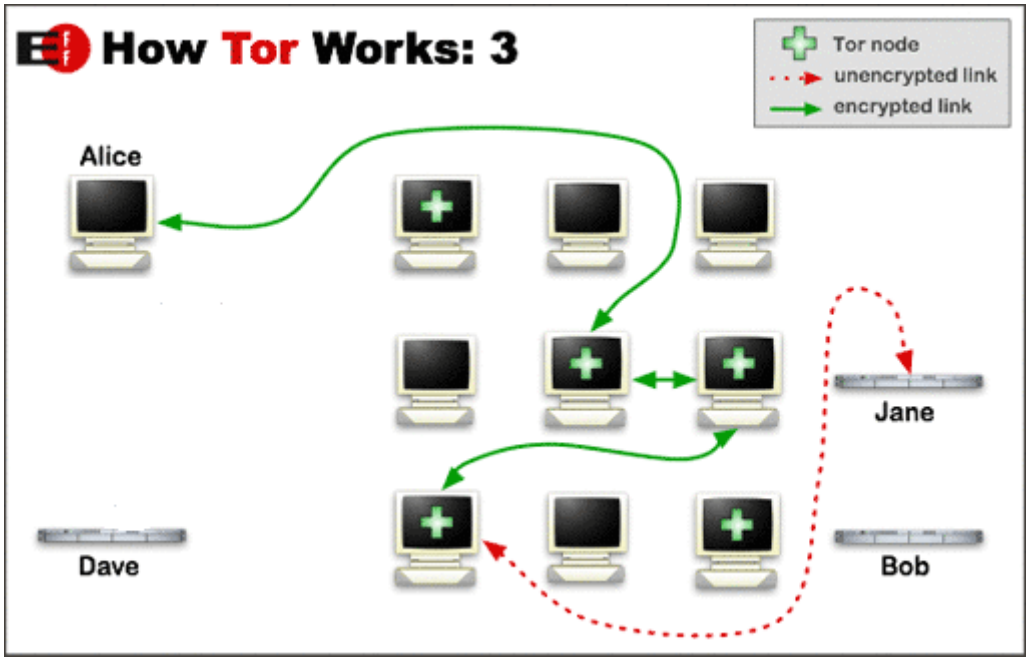
Resim 1

Daha sonra aktif sunucular arasından rastgele yaptığı bir seçimle kendine bir güzergah oluşturur. Güzergahtaki hiçbir Tor sunucusu güzergahın bütününün bilgisine sahip değildir; sadece veriyi aldığı ve ileteceği sunucunun bilgisine sahiptir. Bu nedenle, herhangi bir sunucunun ele geçirilmesi durumunda bile iletişimin taraflarının (Alice ve Bob) bilinebilmesi olanaklı değildir. Resim 2'de yeşil renkle gösterildiği gibi veri güzergah boyunca şifrelenmiş olarak iletilir. Kırmızı renkle gösterilen son kullanıcı erişiminde veriye şifresiz olarak erişilir.



Resim 2

Ağı verimli kullanmak adına bir güzergah oluşturulduktan sonra belirli bir süre saklanır. Gönderi iletimi , ortalama on dakika boyunca, hedef aynıysa yine aynı güzergah üzerinden gerçekleştirilir. Fakat, hedefin değişmesi ya da sürenin aşılması durumunda yeni bir güzergah oluşturulur (bkz. Resim 3).



Resim 3

Tor'un çalışma prensibi basitçe yukarıdaki gibidir. Tor web tarayıcısının kurulumu ve kullanımı ise son derece kolaydır.

Tor Web Tarayıcısı (Tor Browser Bundle) Kurulumu

Tor web tarayıcı, Firefox web tarayıcısı üzerine geliştirilmiş özgür bir yazılımdır. İşletim sisteminize uygun sürümünü https://www.torproject.org/download/download.html.en adresinden indirebilirsiniz.

Herkesten emeği kadar, herkese ihtiyacı kadar kuralına göre işleyen bu özgür yazılımın kurulumu henüz (!) dilimize çevrilmemiştir. Ama kurulum son derece basittir. Kuruluma yardımcı olmak için hazırlanan videoları da izleyebilirsiniz:

- GNU/Linux (https://media.torproject.org/video/torbrowser-docs/How-to-download-and-use-TBB-in-Linux.mp4)
- Windows (https://media.torproject.org/video/torbrowser-docs/How-to-verify-signatures-in-Windows.mp4)
- Apple (https://media.torproject.org/video/torbrowser-docs/How-to-download-and-use-TBB-in-OSX.mp4)

Tor web tarayıcısının arayüzü Firefox kullanıcılarına yabancı gelmeyecektir. Tor'u kullanırken, kurulum sayfasında yayınlanan uyarıları dikkate almak gerekiyor:

- Flash, RealPlayer, Quicktime vb videoların gösterimi engellenmiştir. Bu videoların gösterimi, ip adresinizi açığa çıkarıp anonimliğinizi tehlikeye atabilir. Diğer firefox eklentilerinde de benzer sorun vardır.
- Tor aracılığıyla indirdiğiniz dosyaları, çevrimiçiyken (online) açmayın.
- Tor, erişilen web sitelerini gizleyecektir. Ancak saldırgan, bilgisayarınızın Tor ağını bağlanıp bağlanılmadığını anlayabilir. Bunu da engellemek isterseniz Tor köprüsünü kullanabilirsiniz (https://www.torproject.org/docs/bridges.html.en).

Daha da güvenli bir internet kullanımına gereksinimiz olduğunda ise, Debian GNU/Linux tabanlı Tails adlı yazılımı bir USB'ye ya da DVD'ye yazıp bilgisayarınızı onun üzerinden de kullanabilirsiniz (https://tails.boum.org/download/index.en.html)

***

Tor kullanımının ülkemiz yasalarına göre suç olup olmadığına dair bir bilgimiz yok. Ancak Tor'un kullanımını destekleyen EFF (Electronic Frontier Foundation) bu sorunu ABD yasaları çerçevesinde yanıtlıyor: ABD'de Tor kullandığı için ceza alan ya da hakkında dava açılan herhangi biri yok. Tor kullanımının ya da Tor sunucularına destek vermenin herhangi bir davaya konu olup olamayacağını da bilemeyiz.

Ancak gözetim toplumsal bir sorundur ve bu sorunu teknik çözümlerle ancak geçici bir süre aşabiliriz. Fakat toplumsal koşulları değiştirmek için de teknolojiye gereksinimiz olacaktır...

Yararlanılan Kaynaklar

Yüksel, M. İ., 2010, *Tor Anonimleştiricisinde Sınırlı Kaynak Kullanarak Trafik Analizi*

Gerçekleştirmi, Yüksek Lisans Tezi, Ege Üniversitesi Fen Bilimleri Enstitüsü