HTTPS'e Güveniniz Tam mı?

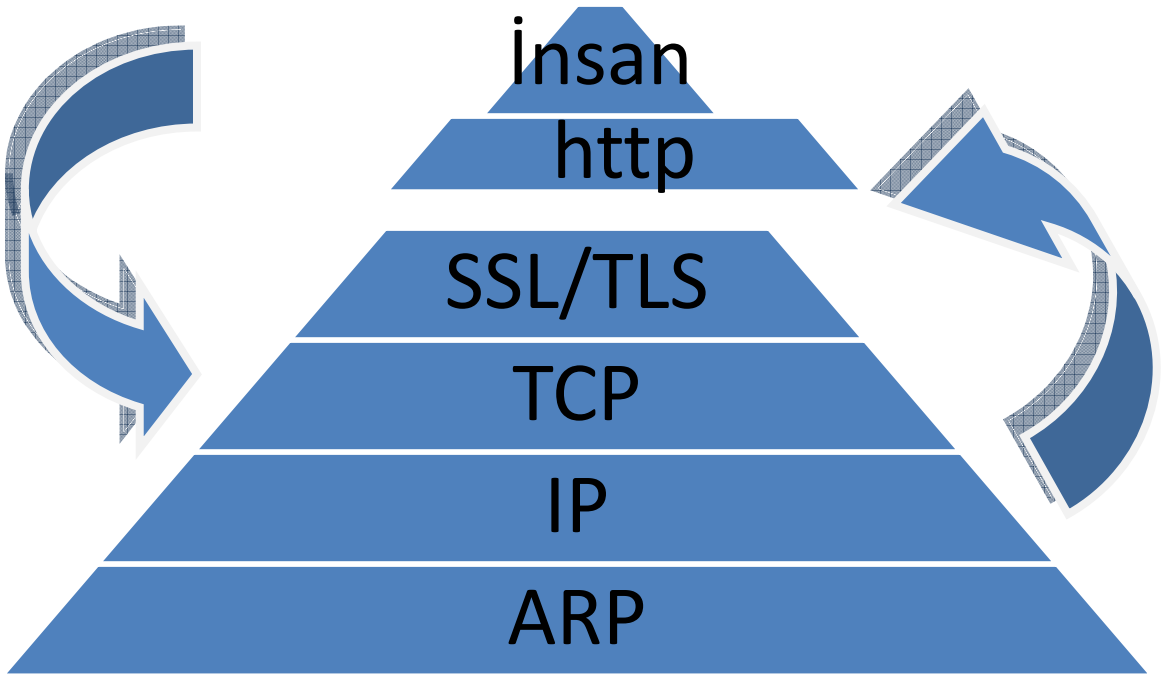
Bu yazının konusu günlük hayatımızda güvenli olduğunu düşünerek kullandığımız HTTPS protokolünün güvenliğine dairdir.

Katmanlı Güvenlik Anlayışı

Meşhur bir söz vardır: "biz zincir en zayıf halkası kadar kuvvetlidir". Bu söz bilgi güvenliği için de geçerlidir. Zira güvenlik de bir zincir misali çeşitli katmanlardan(halkalardan) oluşur ve bir sistemin güvenliği kendisini oluşturan katmanlardan en basiti kadardır. Günümüzde güvenliğin en çok ihtiyaç duyulduğu nokta iletişim dünyasıdır. Bu dünyanın da temelini TCP/IP oluşturur.

TCP/IP protocol ailesi bundan yıllar önce amacı güvenlik olmayan işler için geliştirilmiş bir protokoldür ve günümüzde ise çeşitli eksiklikleri hissedilmektedir. Bu eksiklikler yeni yeni protokollerle kapatılmaya çalışılsa da temelde olan bir problem tüm sistemi etkileyebilmektedir.

Mesela HTTPS üzerinden çalışan bir uygulamaya güvenli diyebilmemiz için sistemin hangi katmanlardan oluştuğunu iyi bilmek ve bu katmanlardaki güvenlik zaafiyetlerini ölçeklemek gerekir.

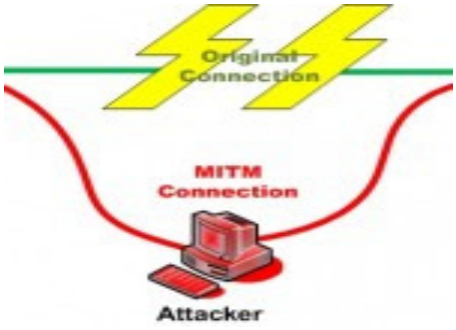


Şekilde görüleceği üzere HTTPS bağlantısının gerçekleşmesi için ek 4 protokol daha devreye girer. HTTPS ne kadar güvenli olursa olsun diğer protokollerdeki bir açıklık HTTPS'i de etkileyecektir. Peki HTTPS güvensiz midir?

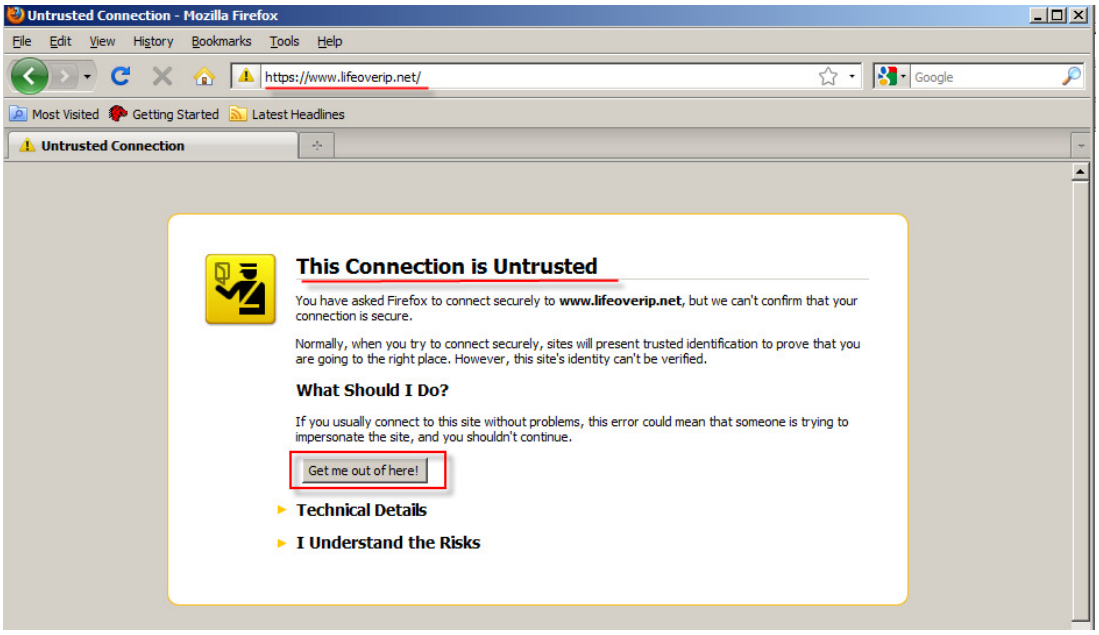
HTTPS Güvensiz Midir?

Bankalar, online alışveriş siteleri vb. kurumlar için güvenlik denilince akla 128 bitlik şifreleme gelir. Evet 128 bitlik şifreleme günümüz ölçülerinde güvenilir kabul edilse de iş sadece şifrelemeyle kalmıyor, şifreleme ile birlikte kullanılan diğer altyapıların da güvenli olması gerekir.

SSL'in karşı karşıya kaldığı ilk ve önemli saldırı tipi MITM(Man in The middle) ataklardır. MITM tipi ataklarda saldırgan kendisini istemci(kurban) ile sunucu arasına yerleştirerek tüm trafiği dinler ve değiştirebilir.



HTTPS bağlantılarında MTIM ile araya giren saldırgan sahte sertifika üretse de sertifika geçerli bir CA kurumu tarafından imzalanmadığı için kullanıcının browserinda hata verecektir. Eskiden browser uyarıları kolaylıkla atlanabilir, gözden kaçabilir uyarılardı fakat günümüzde browserlarin verdiği SSL uyumsuzluk uyarıları gerçekten uyarıcı, uyarmanın ötesinde rahatsız edici olmaya başladı. Özellikle Firefox'un yeni sürümlerinde bu durum belirgin olarak karşımıza çıkmaktadır.



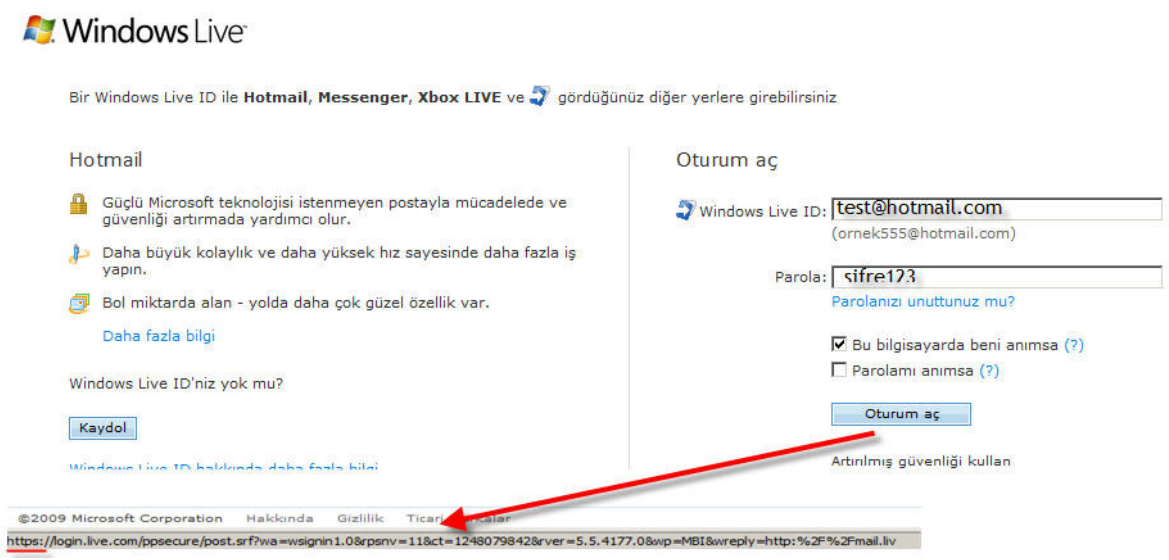
Yukarıdaki çıktıda SSL sertifika uyumsuzluğundan Firefox'un verdiği uyarılar serisi sıraadn bir kullanıcıyı bile sayfadan kaçıracak türdendir.

Dikkatsiz, her önüne gelen linke tıklayan, çıkan her popup okumadan yes'e basan kullanıcılar için bu risk azalsa da hala devam ediyor ama bilinçli kullanıcılar bu tip uyarılarda daha dikkatli olacaklardır. Peki bilinçli kullannıcıların gözünden kaçabilecek ve HTTPS'I güvensiz kılabilecek başka açıklıklar var mıdır?

Bu sorunun kısa cevabı evet, uzun cevabına gelecek olursak…

SSL'in HTTP ile İmtihanı

SSL(HTTPS)'I güvenlik amacıyla kullanırız fakat günümüzde SSL kullanılan çoğu sistemde HTTP ve HTTPS birlikte kullanılmaktadır. Yani once sayfaya HTTP üzerinden girilir, sonra hassas bilgiler içerecek linklerde HTTPS'e çevrilir. Bu durumad yeni oluşacak HTTPS'in güvenliği buradaki HTTP'e bağlı oluyor.



Firmaların neden sadece HTTPS kullanmadığı sorusuna verilecek en kısa cevap SSL'in sunucu tarafında ek kapasite gerektirmesidir. HTTP ile HTTPS arasındaki yük farkını görebilmek için aynı hedefe yapılmış iki farklı HTTP ve HTTPS isteğinin Wireshark gibi bir snifferla incelenmesi yeterli olacaktır.

HTTP'de oturum bilgisi çoğunlukla cookie'ler üzerinden taşındığı düşünülürse eğer sunucu tarafında kod geliştirenler cookilere "secure" özelliği(cookielerin sadece güvenli bağlantı üzerinden aktarılması) eklememişlerse trafiği dinleyebilen birisi hesap bilgilerine ihtiyaç duymadan cookieler aracılığıyla sizin adınıza sistemlere erişebilir.

Bunun için çeşitli yöntemler bulunmaktadır, internette "sidejacking" ve surfjacking anahtar kelimeleri kullanılarak yapılacak aramalar konu hakkında detaylı bilgi verecektir. Bu yazının konusu olmadığı için sadece bilinen iki yöntemin isimlerini vererek geçiyorum.

Göz Yanılgısıyla HTTPS Nasıl Devre Dışı Bırakılır?

Bu yıl yapılan Blackhat konferanslarında dikkat çeken bir sunum vardı: *New Tricks For Defeating SSL In Practice.* Sunumun ana konusu yukarda anlatmaya çalıştığım HTTPS ile HTTP'nin birlikte kullanıldığı durumlarda ortaya çıkan riski ele alıyor. Sunumla birlikte yayınlanan sslstrip adlı uygulama anlatılanların pratiğe döküldüğü basit bir uygulama ve günlük hayatta sık kullandığımız banka, webmail, online alış veriş sitelerinde sorunsuz çalışıyor. Kısa kısa ssltrip'in nasıl çalıştığı, hangi ortamlarda tehlikeli olabileceği ve nasıl korunulacağı konularına değinelim.

SSLStrip Nasıl Çalışır?

Öncelikle sslstrip uygulamasının çalışması için Linux işletim sistemine ihtiyaç duyduğu ve saldırganın MITM tekniklerini kullanarak istemcinin trafiğini üzerinden geçirmiş olması zorunlulugunu belirtmek gerekir.

Şimdi adım adım saldırganın yaptığı işlemleri ve her adımın ne işe yaradığını inceleyelim;

1.Adım: Saldırgan istemcinin trafiğini kendi üzerinden geçirir. Saldırgan istemcinin trafiğini üzerinden geçirdikten sonra trafik üzerinde istediği oynamaları yapabilir. Saldırgana gelen paketleri hedefe iletebilmesi için işletim sisteminin routing yapması gerekir. Linux sistemlerde bu sysctl değerleriyle oynayarak yapılabilir. (echo "1" > /proc/sys/net/ipv4/ip_forward)

2. Adım: Saldırgan iptables güvenlik duvarını kullanarak istemciden gelip herhangi biryere giden tüm TCP/80 isteklerini lokalde sslstrip'in dinleyeceği 8000. Porta yönlendiriyor.

İlgili Iptables komutu: iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8000

3.Adım)Saldırgan sslstrip uygulamasını çalıştırarak 8000.portu dinlemeye alıyor ve istemci ve sunucudan gelecek tüm istek-cevapları "topla" isimli dosyaya logluyor.

#sslstrip -w topla --all -l 8000 –f

Şimdi şöyle bir senaryo hayal edelim: Masum kullanıcı ailesiyle geldiği alışveriş merkezinde ücretsiz bir kablosuz ağ bulmuş olmanın sevinciyle mutlu bir şekilde gelip bilgisayarını açsın ve ilk yapacağı iş maillerini kontrol etmek olsun.

Ortama dahil olmuş masum bir kullanıcının yaşadığı süreç şu şekilde olacaktır:

İstemci ağa bağlanıp internete erişmek istediğinde ortamdaki saldırgan el çabukluğu marifetle istemcinin trafiğini üzerinen geçirir(ARP Cache poisoning yöntemiyle).

İstemci durumdan habersiz webmail uygulamasına bağlanmak için sayfanın adresini yazar. Araya giren saldırgan sunucudan dönen cevaplar içerisinde HTTPS ile başlayan satırları HTTP ile değiştirir ve aynen kullanıcıya gönderir.

Hiçbir şeyden haberi olmayan kullanıcı gelen sayfada kullanıcı adı/parola bilgilerini yazarak Login'I tıklar.

Kullanıcıdan gelen login bilgisi HTTP üzerinden olduğu için saldırganın bilgisayarında çalışan sslstrip bu bilgileri alır, kaydeder ve yine bu bilgileri kullanarak web uygulamasına HTTPS bağlantısı açar, web uygulamasından dönen cevapları yine içerisindeki HTTPS satırlarını HTTP ile değiştirerek kullanıcıya döndürür.

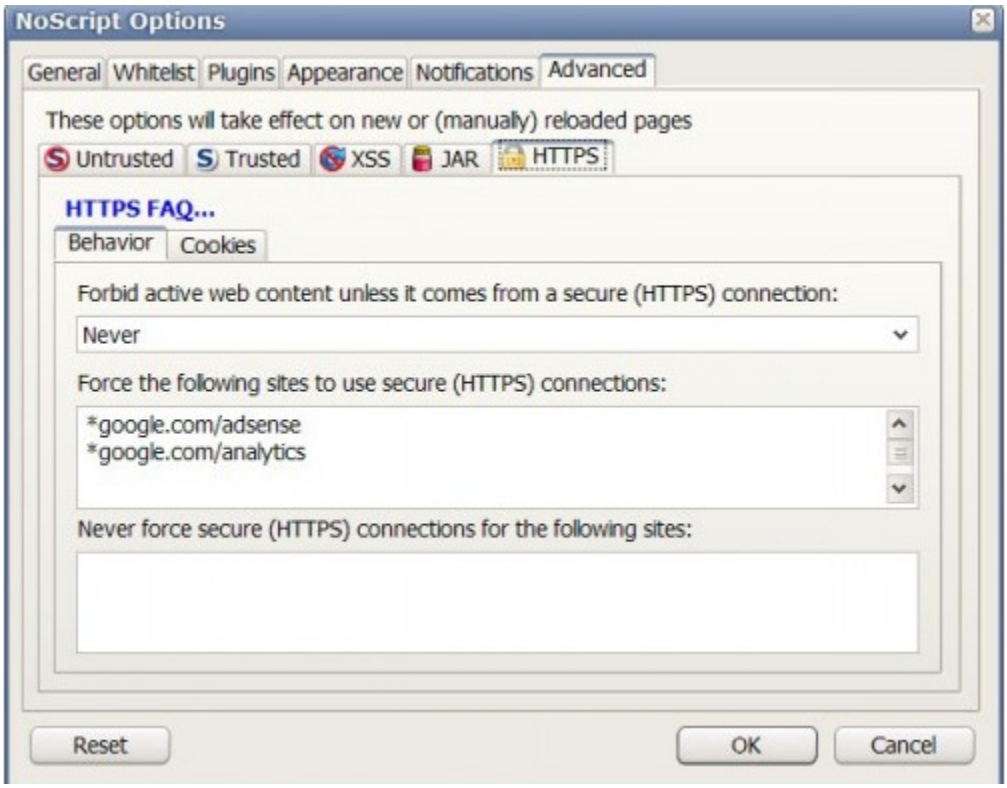
Böylece istemci farketmeden HTTPS yerine HTTP kullanarak tüm bilgilerini kaptırır.

Böyle bir senaryo, halka açık kablosuz ağlarda, şirketlerin yerel ağlarında, TOR vs gibi ücretsiz proxy hizmeti kullanılan yerlerde yaşanabilir

Nasıl Korunurum?

Bu yazıda anlatılan saldırı yönteminden korunmak sunucu tarafından ziyade istemci tarafını ilgilendirir. İstemci HTTPS olarak gitmek istediği sitelere giderken isteklerinin HTTPS olarak gittiğine dikkat etmeli, ötesinde bu işi kendine bırakmayıp otomatize edecek bir yazılıma bırakmalı.

Firefox kullanıcısıysanız aşağıdaki [3]nolu kaynaktan indireceğiniz ForceHTTPS ya da Noscript eklentlerini kullanarak belirlediğiniz sitelere sadece HTTPS bağlantısı yapılmasını sağlayabilirsiniz.



Kaynaklar:

[1]SSL strip Uygulaması: www.thoughtcrime.org/software/**sslstrip**

[2]Noscript firefox Eklentisi: http://www.**noscript**.net

[3]ForceHTTPS Firefox eklentisi https://crypto.stanford.edu/forcehttps/