ŞİFRELEME(ENCRYPTION)

AHMET ERDEM

Internet Society
Turkey Chapter

İÇİNDEKİLER

1 ŞİFRELEME GİRİŞ

- Bilgilerin gizli kalmasını sağlamaya ve bu bilgileri görme yetkisi olmayan kişilerden korumaya yönelik bir kodlama yöntemidir.
- Kişisel bilgilere ulaşılmaması için kişi tarafından belirlenen ve kullanılan özel karakterler ve sayılardan oluşan şifrenin kullanılmasıdır
- Şifreleme verinin sadece istenen kişiler tarafından orijinaline döndürülüp okunması için yapılan karıştırılma işlemidir.
- Bilgisayar sistemlerindeki (data at rest) verileri ve bilgisayar ağları ile taşınan verilerin(data in transit) korunması için kullanılır.

1.1 ŞİFRELEME NEDİR?

- Verinin geri dönüştürebilir şekilde dönüştürülmesidir
- Bilgiyi anlaşılmaz ve erişilmez hale getirir
- Veri bütünlüğü sağlamaya yardımcıdır
- 3. taraflar erişse bile ancak anlaşılmayan haline erişebilirler
- Verinin silinmesini engellemez

1.2 UÇTAN UCA ŞİFRELEME

- Uçtan uca şifreleme (End-to-end-E2E) sadece veriyi gönderen ve alanın okuyabilmesini sağlayan bir şifreleme metodudur.
- Herhangi bir üçüncü taraf mesajı okuyamaz.
- Uçtan uca şifreleme en güvenli şifrelemedir.
- Uçtan uca şifreleme metodu kullanan bazı mesajlaşma uygulamaları (WhatsApp, Signal, Telegram, and Threema)

1.3 ŞİFRELEMENİN ÖNEMİ (I)

- Şifreleme Internet'te güvenin anahtar yapı taşıdır.
- Verinin açığa çıkmasını engeller ve
- Verinizin karıştırılmaya karşı korur,
- Kiminle iletişim kurduğunuzdan emin olmanızı sağlar,
- Gönderdiğiniz dokümanları imzalamanızı sağlar.
  - Bu sayede dokümanı sizin hazırladığınız doğrulanır

1.3 ŞİFRELEMENİN ÖNEMİ (II)

- Günlük hayatımızda şifrelemeye bağlıyız
- Güçlü şifreleme sakladığımız ve taşıdığımız verilerin güvenlik, mahremiyet ve gizliliğini(confidentiality) garanti eder
- Toplumdaki bir çok anahtar elemanın çalışması için
  - Webde gezinme(tarayıcılar ve web siteleri HTTPS protokolü kullanır. HTTPS verimizin iletilirken başkaları tarafından okunmasını engelleyen güvenli iletişim saplayan şifrelenmiş bir protokoldür.)
  - Elektronik Ticaret: Çevrimiçi (online) alışveriş veya bankacılıkta finansal bilgilerimizin firmalar tarafından korunduğuna güvenmek isteriz. Şifreleme bunu gerçekleştirmek için önemli bir yöntemdir.
  - Güvenli Mesajlaşma: Mesajlaşma uygulaması kullanırken mesajların gizli ve kişiye özel olmasını bekleriz. Bazı uygulamalar kullanıcı iletişiminin gizlilik ve güvenliğini sağlamak için iletilen mesajların şifrelenmesini sağlar. Bazıları sadece gönderen ve alıcının mesajları okuyabildiği uçtan uca şifreleme yöntemi kullanırlar (iMessage, WhatsApp, Signal gibi)

1.3 ŞİFRELEMENİN ÖNEMİ (III)

- Bazıları yanlış bir şekilde saklayacak bir şeyiniz yoksa şifreleme ve sonuç olarak verinin gizlilik ve güvenliği o kadar da önemli değil diye düşünebiliyor.
- Ancak veriniz yanlış kişilerin eline düşerse,
  - İtibarınıza zarar vermek
  - Finansal olarak zarar vermek, örnek: Kimlik bilgilerinin çalınması
  - Sizi taklit etmek, Ör.: Bir ödemeyi başka kanala yönlendirmek
  - Kişisel bilgilerinizin paylaşılması

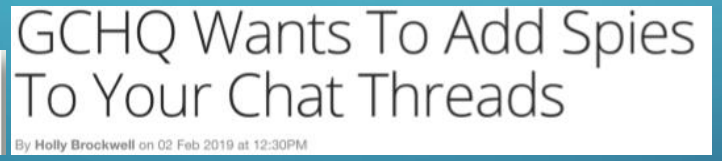
amaçları için kullanılabilir

1.3 ŞİFRELEMENİN ÖNEMİ (IV)

- Bazı hükümetler, kolluk kuvvetlerinin ve ulusal güvenlik kuruluşlarının işlerini(suçluları tespit etme, başkalarına zarar verecek eylemleri durdurma) yapmasını engellediği gerekçesiyle uçtan uca şifrelemeden şikayet etmektedirler.
- Uçtan uca şifreleme ve verilerin cihazlarda şifrelenmesi sorun mudur?
- Hayır. Ticari işlemlerin yanı sıra kolluk kuvvetleri ve ulusal güvenlik kuruluşları gibi toplumun kilit işlerinin güvenli ve etkin yürütülmesi için güçlü şifreleme temel bir gereksinimdir.

1.4 ŞİFRELEME RİSK ALTINDA

- Bazı hükümetler firmalardan şifreli içeriğe erişmeleri için yöntemler geliştirmelerini istiyor. (Şifreleme arka kapısı)
- Bazıları şifrelemenin filtreleme veya engellemeye izin verecek şekilde zayıflatılmasını talep ediyor
- Bazı firmalar veriden para kazanma amacıyla şifreli veriye erişmek istiyor



1.5 ŞİFRELEMEYE KARŞI TEHDİTLER (I)

- Yasamayla İlgili: Kolluk kuvvetleri için arka kapı erişimi oluşturmayı zorunlu tutan kanunlar çıkarılması
  - Gerekçe: Genellikle şüphelileri ya da teröristleri hedef almak için kullanılır.
  - Örnek: Investigatory Powers Act (UK; 2016), Assistance and Access Act (AU; 2018)
- Adli: Mevcut yasaların kolluk kuvvetleri için arka kapı erişimi oluşturmak amacıyla kullanılması
  - Gerekçe: Genellikle şüphelileri ya da teröristleri hedef almak için kullanılır.
  - Örnek: FBI ve Apple (US; 2015)
- Dolaylı: Şifrelemeyi hedef almayan ancak şifrelemeyi riskli hale getiren yöntemler
  - Gerekçe: Sayısal yanlış bilgilendirme ya da aşırılık içeren içerik
  - Örnek: Şifrelemeyi imkansız hale getiren içerik filtreleme gereksinimleri (India, Brazil 2019)
- Bu tür tehditler her ülkede olabilir. Öncesinden tanınması gerekir.

1.5 ŞİFRELEMEYE KARŞI TEHDİTLER (II)

- Hangi yöntem olursa olsun «arka kapı erişimin sadece otorite tarafından kullanılacağı ve güvenliği zayıflatmadığı» gibi bir durum olamaz. Suçlular aynı yöntemi tespit edip kullanabilirler.
- Böyle bir durumda kanunsuz iş yapacaklar iletişim kurmak için başka bir şifreli hizmet bulacaktır. Yargının ve hükümetin kontrolü dışında bu tür yöntemler çokça mevcuttur.

1.6 ŞİFRELEME ARKA KAPILARI NEDEN İSTENİYOR

- Kolluk kuvvetlerinin vatandaşı korumak ve kanunları uygulama kabiliyetinde şifrelemenin olumsuz etkisi olabilir. Kanunsuz işleri yürütenler faaliyetlerini gizlemek için şifreleme kullanabilirler.
- Kolluk kuvvetlerine şifrelenmiş iletişim içeriğine ve cihazlara erişim için istisnai erişim yetkileri verilmelidir düşüncesi bazılarında hakim

1.7 ŞİFRELEME ARKA KAPILARINDAKİ SORUNLAR

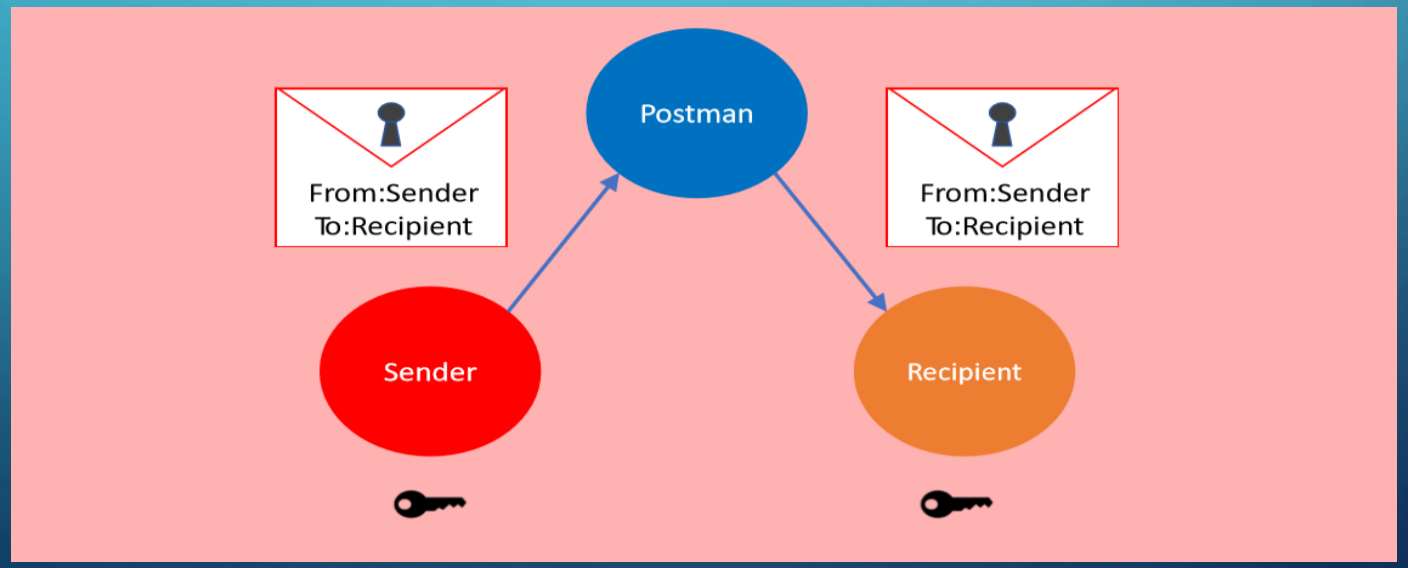
- Kullanılan yöntemden bağımsız olarak arka kapı erişimi (suç örgütleri ya da başka hükümetler gibi) başka tarafların da güvenli veriye erişmesine imkan sağlar
  - Bilgi güvenliği uzmanları arasındaki konsensüse göre arka kapı erişimi mekanizmaları sistemlere daha fazla karmaşıklık katar ve güvenlik açıklarına yol açar. Bu güvenlik açıkları başkalarının tespit edip kullanabileceği giriş noktaları olarak kullanılır.
- Arka kapı erişimi suçluların serbestçe gizli iletişimini engellemez
  - İletilmekte olan ya da depolanan veriyi şifrelemek için alternatif araç ve yöntemler bulunabilir. Bu durum suçluların iletişimi gizli olurken sıradan insanların iletişiminin kötü niyetli müdahalelere açık olmasına yol açar.

2 SİSTEM OLARAK ŞİFRELEME

- Kullanım Durumu:
- Erişim yasaları uygulama teklifimiz hala güçlü şifrelemeye izin veriyor, çünkü değiştirmek istediğimiz tek şey anahtar değişim protokolü. Şifrelemeye hiç dokunmuyoruz
- Bu gerçek anlamda ne anlama gelir?
- Bunun şifrelemeyi zayıflatmadığı doğru mudur?

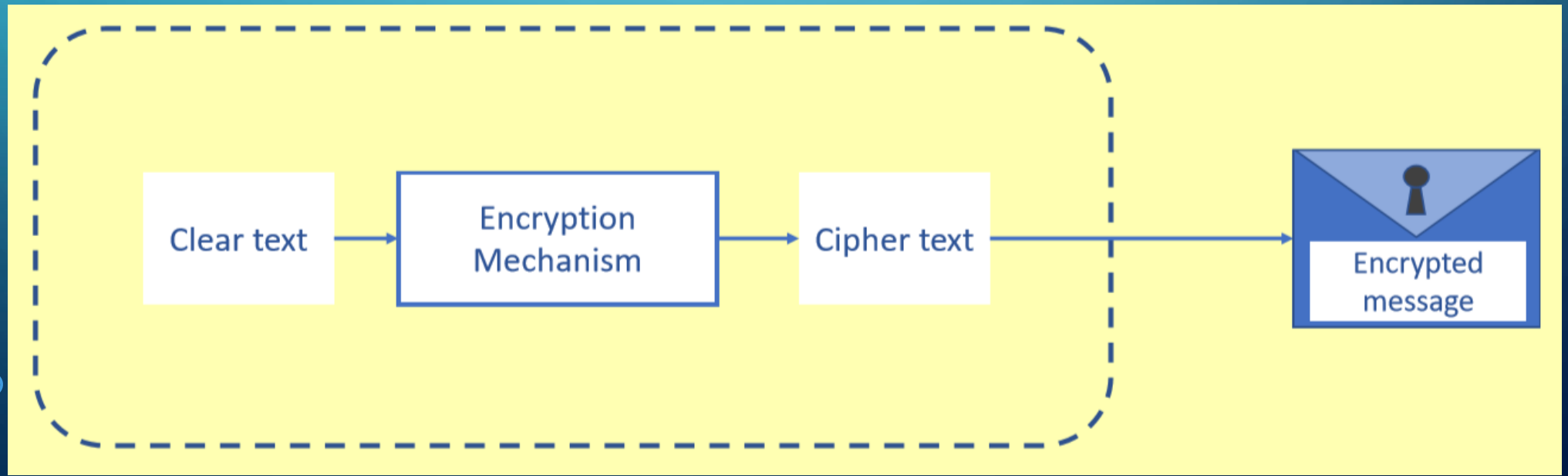
2.1 KULLANICI PERSPEKTİFİ

- «Mesajlarımı gizli tutmak istiyorum»
- «Gönderdiğim mesajları gönderdiğim kişi dışında kimsenin okumasını istemiyorum.»



2.2 ÜST SEVİYE AÇIKLAMA

- Şifreleme, şifreli mesajların gizliliğini sağlamak için kullanılır
- Mesaj gönderen tarafından şifrelenir ve alıcı tarafından şifresi çözülür
- Başka hiç kimse içeriği okuma imkanına sahip değildir.
- Bu, gönderenin ve alıcının anahtar değişimi için güvenilir bir yolu olduğunu varsayar.



2.3 SALDIRI TÜRLERİ

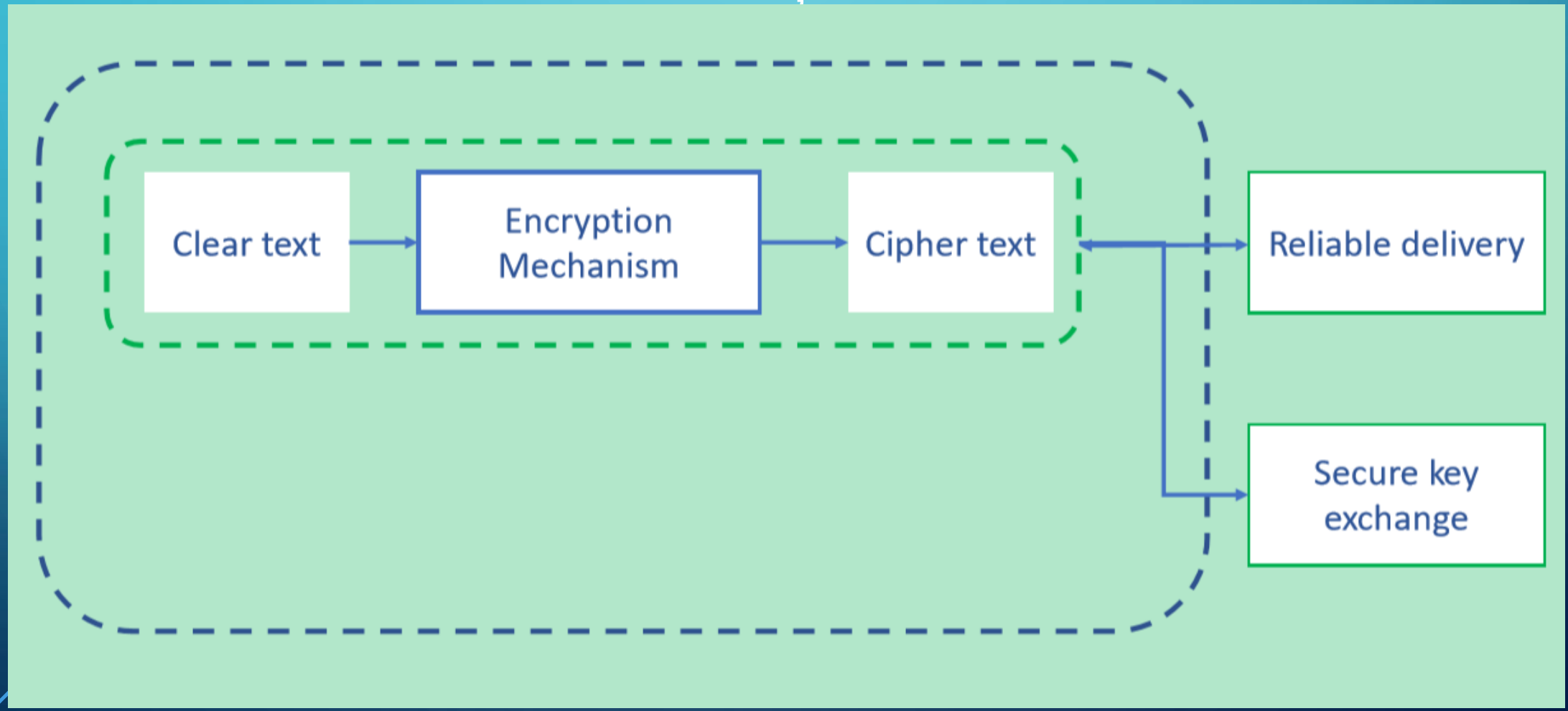
- Pasif saldırı, verilerin gizlice okunmasıdır
  - Ücretsiz bir web posta hizmetinin, ilgi alanlarınız ve satın alma gücünüz hakkında bilgi almak için e-postalarınızı incelemesi
  - Banka bilgilerinin ele geçirilmesi

- Aktif saldırı, verinin okunması yanında değiştirilmesini de içerir

2.4 SİMETRİK ŞİFRELEME

- Veri güvenliği için şifrelemenin en temel yöntemi simetrik şifrelemedir.
- Veriyi şifrelemek ve tekrar deşifre etmek için bir anahtar kullanılır.
- Simetrik şifrelemedeki anahtarlar gizli tutulur.

2.5 ORTA SEVİYE AÇIKLAMA-ŞİFRELEME VE GÜVENLİ ANAHTAR PAYLAŞIMI



2.6 SİMETRİK ŞİFRELEMEDEKİ SORUNLAR

- Simetrik şifrelemede anahtar güvenli bir şekilde mesajı alan tarafa iletilmelidir
- Eğer şifre gönderilirken ele geçirilirse ele geçirenler ortadaki adam gibi davranabilirler

2.7 ASİMETRİK ŞİFRELEME- GENEL ANAHTAR ŞİFRELEMESİ

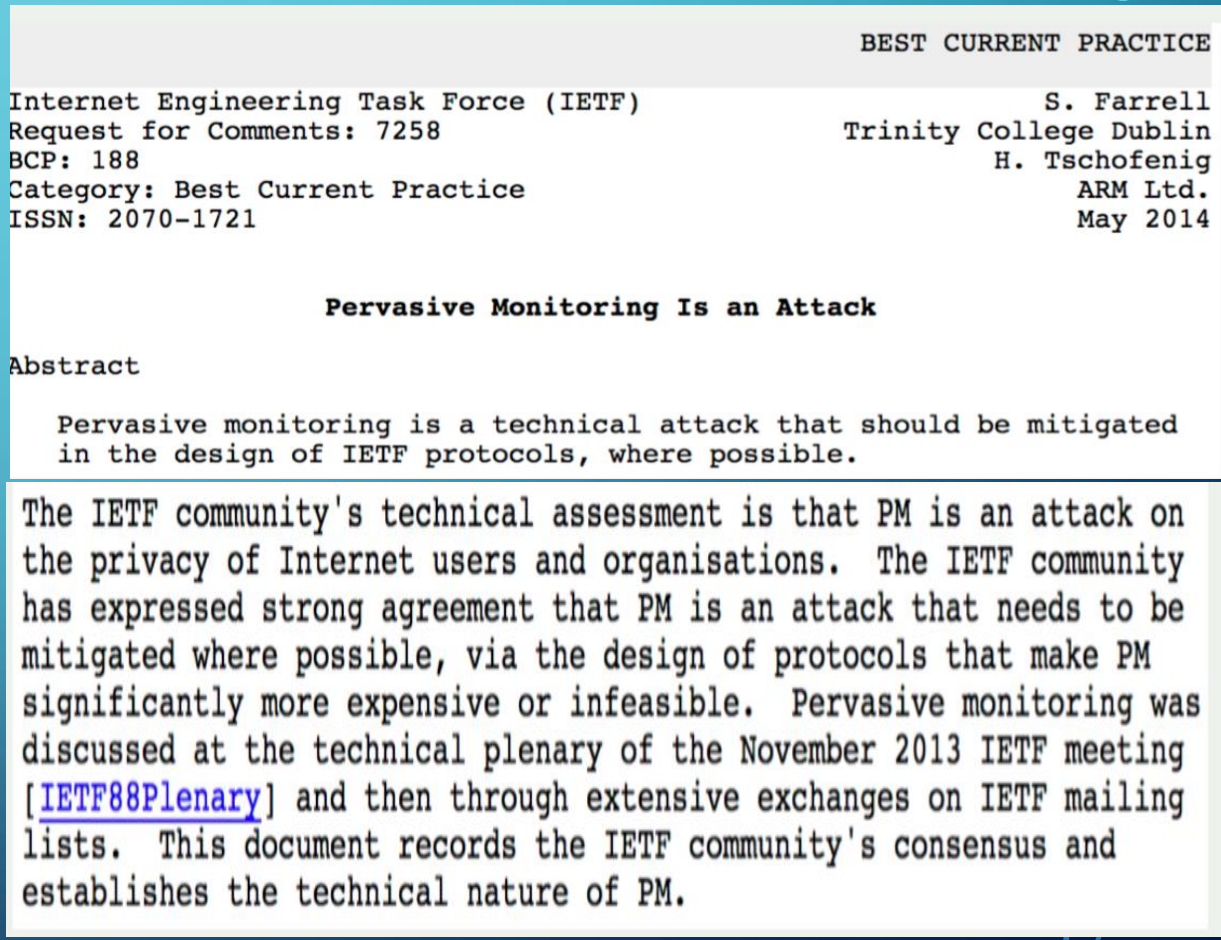
- Ortak anahtar şifrelemesi, verileri şifrelemek için bir (genel) anahtar ve şifresini çözmek için farklı bir (özel)anahtar kullanır
- Simetrik şifrelemenin aksine, şifreleme işlemi genel anahtarla ters çevrilemez
- Bu nedenle, genel anahtarı yayınlamak güvenlidir, mesajın şifresi yalnızca ilgili özel anahtarları kullanarak çözülür
- Bir yönde, veri ortak anahtarla şifrelenir ve özel anahtarla şifreyi çözülür. Diğer yönde, özel anahtarla imzalanır ve herkes gönderenin genel anahtarı ile imzayı doğrulayabilir.

2.8 ASİMETRİK ŞİFRELEME İLE ANAHTAR DAĞITIMI

- Simetrik şifrelemenin aksine, gizli anahtarın güvenli bir şekilde paylaşılmasına dayanmaz
- Ortak anahtarın doğru kişiye ait olduğundan emin olmak için ortak anahtar altyapısına veya her bir ortak anahtarın sahibini "onaylayan" otoriteye ihtiyacınız vardır.
- Açık anahtar sertifikaları, ortadaki adam saldırılarına karşı korunmaya yardımcı olur
- Ortak anahtar şifreleme simetrik şifrelemeye göre yavaş ve daha az verimlidir.
- TLS, Signal gibi şifreleme sistemleri hibrit çözümler kullanır. Genel anahtar şifrelemesi anahtar paylaşımı için kullanılır. Gizli anahtar paylaşıldıktan sonra simetrik şiferleme yöntemine geçilir.

3. SÜRECİN İLERLEMESİ RFC 7258 YAYINLANMASI

- RFC 7258 Yayınlanması
- Google, Gmail kullanıcıları ve sunucuları arasında HTTPS'ye geçti
- Google, Yahoo, Microsoft ve diğerleri, veri merkezleri arasında akan verileri tamamen şifreliyor
- Şifreli mesajlaşma uygulamalarında artış gözlendi



BEST CURRENT PRACTICE

Internet Engineering Task Force (IETF) — S. Farrell
Request for Comments: 7258 — Trinity College Dublin
BCP: 188 — H. Tschofenig
Category: Best Current Practice — ARM Ltd.
ISSN: 2070-1721 — May 2014

Pervasive Monitoring Is an Attack

Abstract

Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.

The IETF community's technical assessment is that PM is an attack on the privacy of Internet users and organisations. The IETF community has expressed strong agreement that PM is an attack that needs to be mitigated where possible, via the design of protocols that make PM significantly more expensive or infeasible. Pervasive monitoring was discussed at the technical plenary of the November 2013 IETF meeting [IETF88Plenary] and then through extensive exchanges on IETF mailing lists. This document records the IETF community's consensus and establishes the technical nature of PM.

3.1 INTERNET ARCHITECTURE BOARD (IAB) INTERNET GÜVENLİĞİ AÇIKLAMASI

- Kasım 2014
- «IAB artık protokol tasarımcılarının, geliştiricilerinin ve operatörlerinin şifrelemeyi İnternet trafiği için norm haline getirmesinin önemli olduğuna inanmaktadır. … Yeni tasarlanan protokoller açık metin işlemine göre şifrelemeyi tercih etmelidir. … Şifrelemenin tüm protokol yığını boyunca dağıtılmasını öneriyoruz… IAB protokol tasarımcılarını varsayılan olarak gizliliği sağlayacak şekilde tasarlamaya çağırmaktadır. Geliştiricilerin uygulamalarına şifreleme eklemelerini ve varsayılan olarak şifrelemelerini öneriyoruz. Benzer şekilde, ağ ve hizmet operatörlerini henüz dağıtılmadığı yerlerde şifreleme dağıtmaya teşvik ediyoruz ve güvenlik duvarı yöneticilerini şifreli trafiğe izin vermeye çağırıyoruz.»

3.2 W3C TECHNICAL ADVISORY GROUP (TAG) AÇIKLAMASI

- Web platformunun güvenlik garantilerini bozmadan "istisnai erişim" yeteneklerini güvenli bir şekilde destekleyebilecek sistemler oluşturmak imkansızdır. Bu tür yeteneklerin getirilmesi, herhangi bir varsayımsal faydadan çok daha ağır olan bilinen riskleri dayatır.

4. BAZI ARKA KAPI ERİŞİM YÖNTEMLERİ

- Şifreli iletişime erişim için bir başka önerilen yöntem şifreleme mekanizmalarının zayıflatılmasıdır. Her türlü arka plan, önemli verilerin çalınması, çoğaltılması, keşfedilmesi ve kötüye kullanılması riskini artıran güvenlik açıklarıdır.
- Anahtar Emanet Etme (key escrow): Şifrele çözme anahtarlarının daha sonra kolluk kuvvetleri tarafından kullanılması için güvenilir bir üçüncü tarafın gözetiminde saklanmasıdır. Saklanan bir anahtar kötü nitelik taraflarca bulunma ve kullanılma riski taşır.
- Şifreleme arka kapı savunucuları «sorumlu şifreleme», «istisnai erişim», «yasal erişim» gibi anahtar kelimeler kullanmaktadır. Hepsi şifreleme arka kapısı açmadır ve güvenlik açığı oluşturma riski taşırlar.

4.1 ŞİFRELEME ARKA KAPISI RİSKLERİ

- Bir kolluk kuvvetinin erişim kazanmasının herhangi bir yolu aynı zamanda kötü niyetlilerin erişim elde etmesinin bir yoludur.
- Arka kapı sırrını saklamak ve kötü niyetlilerin onu bulmasını ve sömürmesini engellemek neredeyse imkansızdır.
- Şifreleme arka kapsının ek karmaşıklığı, hizmetin güvenliğini veya performansını daha da zayıflatabilir.

Photo credit: Chris L / Flickr(CC BY 2.0) and Antti T. Nissinen / Flickr(CC BY 2.0)

4.1 ALTERNATİF ARKA KAPI ÖNERİLEN ALTERNATİFLER

- Şifrelenmiş verilere erişmek için bir çok yöntem önerilmiştir.
- Farklı isimleri ve saldırı planları olsa da şifreli iletişimin güvenliğini zayıflatır
- Bazı Metotlar:
  - Anahtar Emanet Etme (key escrow): Anahtarın kopyasının saklanması
  - Ortadaki Adam Saldırısı (Man-in-the middle attacks)
  - İstemci Tarafı Taraması (Client-side-scanning)
  - Hayalet Teklifi (Ghost Proposal)
- Ya da sadece mevcut güvenlik açıklarını kullanırlar(«idare müdahalesi»), teknik belirtmeden uyumu zorlama
- Bu yöntemlerin hiçbiri, kullanıcıların güvenliğini daha fazla riske sokacak yeni güvenlik açıkları getirmeden şifreli verilere erişim sağlayamaz
- Şifreleme arka kapılarının kullanımını zorunlu kılacak politikalar veya yasalar çok tehlikelidir ve kaçınılmalıdır.

4.2 ORTADAKİ ADAM (MAN İN THE MİDDLE) SALDIRILARI

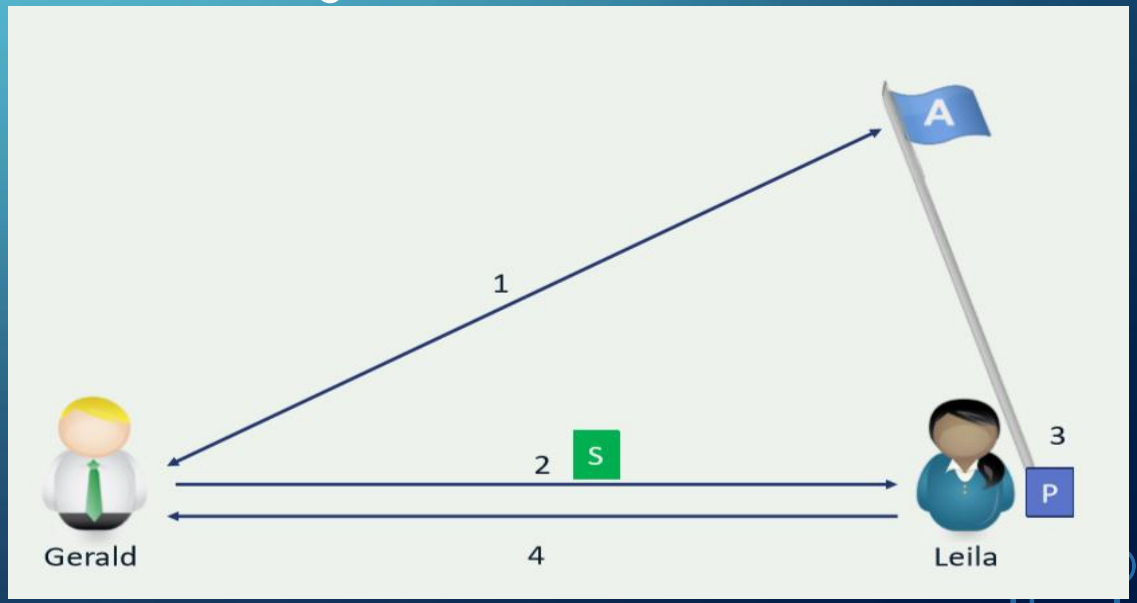
Başlangıç Anahtar Değişimi:

1. Gerald Leila'nın genel anahtarına(public key)[A] bakar ve kendi cihazına kopyalar.

2. Gerald gizli(simetrik) anahtar[S] üretir ve bunu Leila'nın genel anahtarı ile şifreler ve Leyla'ya gönderir.

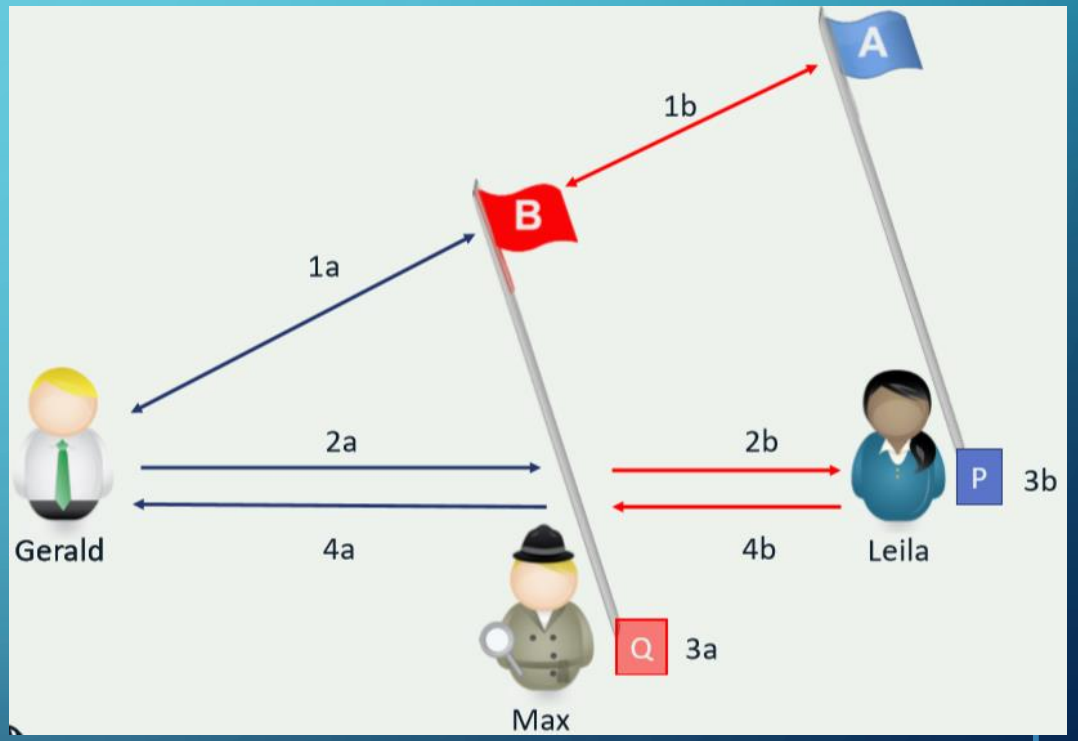
3. Gelen mesajı sadece Leila (özel anahtarını [B] kullanarak) deşifre edebilir.

4. Gerald ve Leila [S]'in kopyasına sahip olmuştur.



4.2.1 UÇTAN UCA ŞİFRELEME: ORTADAKİ ADAM SALDIRISI

- 1a: Geral Leila'nın genel anahtarına[A] eriştiğini sanıyor ancak Max Leila'nın genel anahtarı yerine kendi anahtarını yerleştirmeyi başarmış. Max, Gerald'a geçerli bir simetrik anahtar gönderiyor.
- 1b: Max aynı zamanda Gerald gibi davranarak Leila'ya simetrik anahtar gönderiyor.
- 2-3: Max'ın Gerald'la ayrı, Leila'yla ayrı paylaştığı simetrik anahtarları oldu.
- 4: Geral ve Leila birbirleri ile iletişim kurduklarını sanıyorlar ancak Max her mesajı durduruyor okuyor tekrar şifreleyip gönderiyor.



4.2.2 ŞİFRELEME ORTADAKİ ADAM SALDIRILARINI NASIL ENGELLER

- İletiyi şifrelemek gizliliği korur.: Üçüncü tarafların mesajı görmesini engellemez ancak içeriğini okumalarını engeller.
- Veriyi, belgeyi veya iletişimi dijital olarak imzalamak için şifreleme kullanmak, içerik başka biri tarafından değiştirildiği durumda kurcalamanın tespitini sağlar.
- Transport Layer Security 1.3 (TLS 1.3), Ortadaki adam saldırılarına karşı bir Internet güvenlik protokolüdür. TLS 1.3, Internet trafiği için zorunlu iletme gizliliği yaratır, böylece bir saldırgan özel anahtarı ele geçirse bile ele geçirilen trafiğin şifresinin çözemez.

4.3 İSTEMCİ TARAFI TARAMASI

- Mesaj içeriklerini(metin, görüntü, video, dosya vb) tarayan sistemlerdir.
- Mesaj alıcıya iletilmeden önce şüpheli durumları içeren veritabanı ile kontrol edilirler. Şifrelenmeden önce kontrol sağlanır.
- İçeriğin parmak izleri (hashleri) oluşturulur. Veritabanındaki sayısal parmak izleri ile karşılaştırılır.
- Eğer bir eşleşme olursa ilgili mesaj karşıya iletilmeyebilir ve/veya üçüncü taraflara(kolluk kuvvetleri) bilgi verilir.
- Uç nokta filtrelemesi, yerel işleme gibi isimler de kullanılır

4.3.1 İSTEMCİ TARAFI TARAMASI YÖNTEMLERİ

- Karşılaştırmanın kullanıcı cihazında gerçekleştirilmesi.
  - Bu durumda sorunlu içerik veritabanının kullanıcının bilgisayarına bulunması gerekir.
  - Karşılaştırma için kullanıcı cihazının kaynakları yetersiz olabilir.
- Karşılaştırmanın uzak sunucuda gerçekleştirilmesi.
  - İçerik parmak izleri hesaplanır ve uzak sunucuya iletilir.
  - Veritabanı ile karşılaştırma uzak sunucuda gerçekleştirilir.

4.3.2 İSTEMCİ TARAFI TARAMASI SORUNLAR(I)

- Güvenlik açıkları oluşturur
- İstemci tarafı tarama saldırı yüzeyini artırır.
- Veritabanına dijital parmak izi ekleme ve bu parmak izleriyle eşleşmeler bulunduğunda bildirim alma yeteneğine sahip kötü niyetli kişiler, seçili kullanıcı içeriğini şifrelenmeden ve gönderilmeden önce izlemenin bir yoluna sahip olacaklardır
- Bu parmak izleri, sosyal mühendislik, gasp veya şantaj gibi saldırıları etkinleştirmek için yaygın olarak kullanılan şifreler veya diğer bilgileri içerebilir.
- Bu yöntemle kullanıcıların belirli içerik göndermesini engellemeyi bile seçebilir.
- Kullanıcıların güvenliği ve gizliliği ile ilgili yeni bir dizi sorun açarak, kullanıcın faaliyetlerini sunucuya erişimi olan herkese açar
- Veritabanına verilerin nasıl eklenip çıkarılacağı, bunun nasıl denetleneceği ve yanlış kullanımların nasıl önüne geçileceği ayrı birer sorundur.

4.3.3 İSTEMCİ TARAFI TARAMASI SORUNLAR(II)

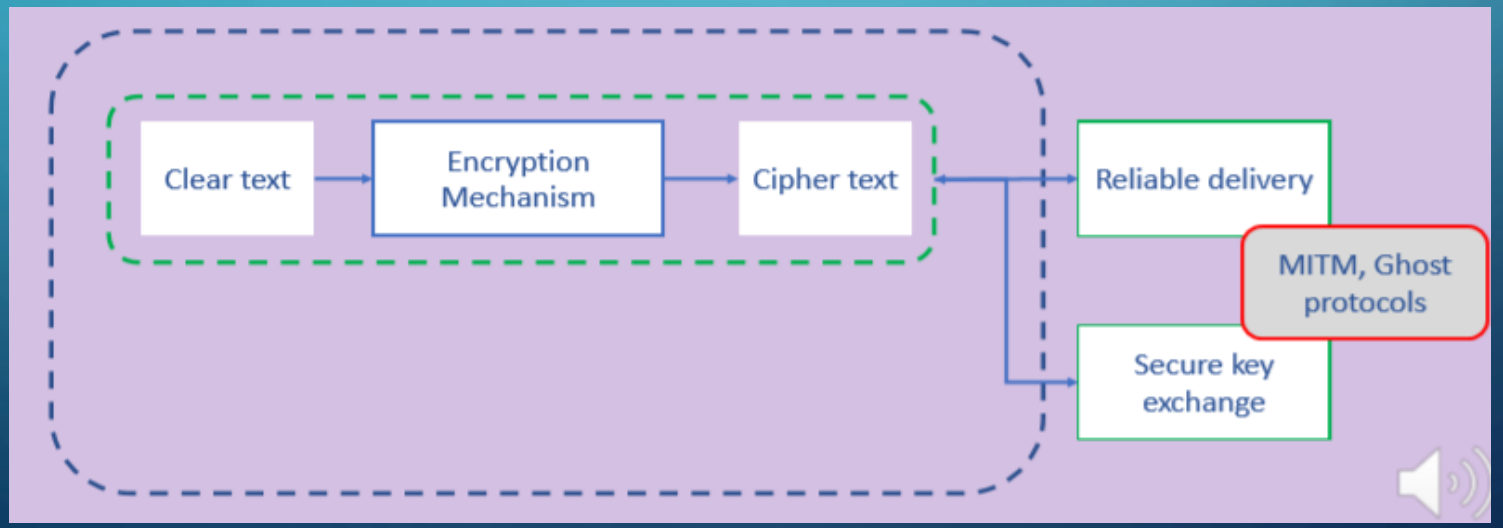
- Karşılaştırma sonucu ilgili otoriteye bilgi verilirken bilgi mesajı başkaları tarafından ele geçirilebilir.
- Uçtan uca şifreleme hedefinden uzaklaşılır
- İstemci tarafı tarama teknikleri kötü niyetlilerce reklam, iletişimi kesme gibi amaçlarla kullanılmanın önünü açabilir.
- Kullanıcılar bu konudan haberdar olunca oto sansür uygulamaya başlayabilirler.
- Suçlular başka iletişim kanalların kayar. Ayrıca istemci tarafı taramasından kaçınmak için içeriği değiştirebilirler.

4.3.4 İSTEMCİ TARAFI TARAMA DEĞERLENDİRME

- Müşteri tarafında tarama, insanların birbirlerine söylediklerini potansiyel olarak izlemek için iletişim altyapısını değiştirerek her kullanıcının güvenliğini zayıflatmayacak şekilde yapılamaz
- Uçtan uca şifreleme milyarlarca insanın güvenli ve gizli iletişim kurmasına olanak sağlamaktadır.
- Uçtan uca şifreli iletişim hizmetlerinde istemci tarafı taraması sakıncalı içeriğin filtrelenmesi için bir çözüm değildir.
- Güvenli ve özel iletişimin temelini zayıflatan tüm yöntemlerin olumsuz etkileri olacaktır.

4.4 HAYALET(GHOST) PROTOKOLLERİ

- Hayalet protokolünde amaç şifreli iletişime sessizce yeni bir taraf eklemektir.
- Yeni eklenen taraf tüm trafiği görebilir.
- Diğer tarafların konuşmanın artık gizli olmadığından haberi yoktur.

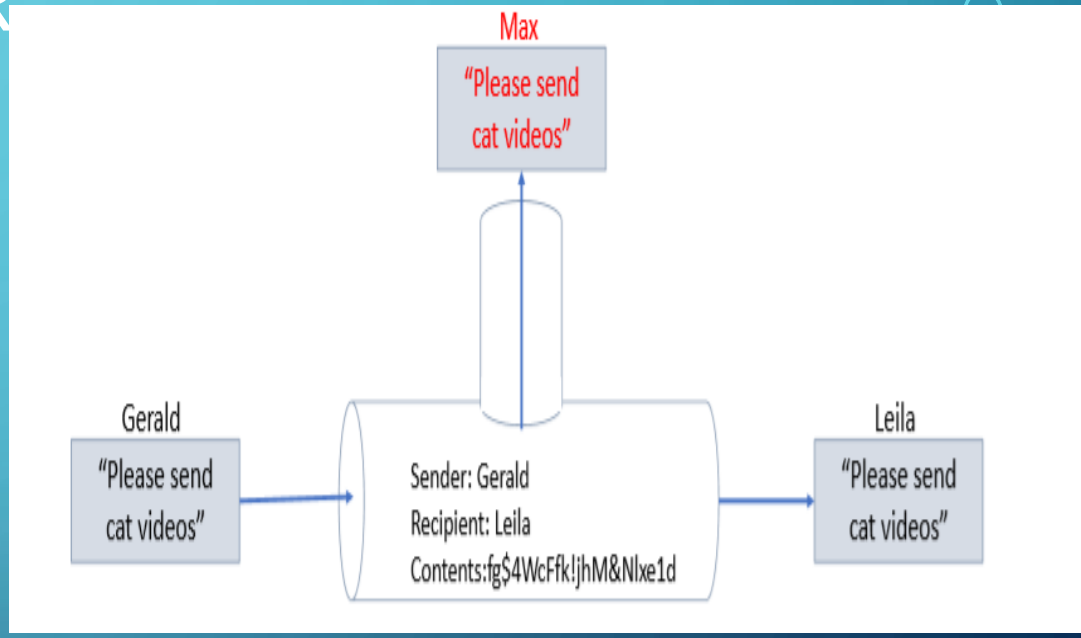


4.4.1 ŞİFRELEME VE ŞİFRELEME ARKA KAPILARI

- Kitlesel gözetim hakkında farkındalık, çevrimiçi hizmet sağlayıcıların şifreleme yoluyla güvenliği artırmasını hızlandırdı.
- Google Gmail kullanıcıları ile sunucular arasında HTTPS protokolüne geçti.
- Google, Yahoo, Microsoft ve diğerleri veri merkezleri arasında akan veriyi tamamen şifreliyorlar
- Apple iOS8'de şifrelemeyi varsayılan olarak atadı
- Twitter ileri gizlilik özelliği ekledi
- Mesajlaşma uygulamaları uçtan uca şifrelemeye geçtiler.

4.4.2 HAYALET PROTOKOL ŞİFRELİ İLETİŞİMİN GİZLİLİĞİNİ ORTADAN KALDIRIR

- Örnekte Max, Gerald ve Leila arasındaki konuşmaya gizlice dahil olmuştur. Max mesajları değiştirmese bile okuyabilir.
- Gerald ve Leila konuşmalarında gizlilik olmamasına rağmen öyle olduğunu sanmaktadır.



- Böyle bir durum çevrimiçi hizmetlerin güvenilirliğini ortadan kaldırır
- Güvenilir teslimatı ve güvenli anahtar değişimini zayıflatırlar
- Güvenli haberleşme uygulamaları konuşmaya başka biri dahil olursa bunu taraflara bildirmelidir.

4.4.3 HAYALET PROTOKOL SONUÇ

- Şifreleme algoritmalarının değiştirilmediği söylenebilir, ancak şifreleme bir sistemdir ve bu teklifler sistemin diğer önemli unsurlarını baltalar, sonuçta gönderen ve alıcı arasındaki gizli iletişim artık olmayacaktır.
- Kullanıcılar ile Servis Sağlayıcılar arasındaki güven ilişkisi zarar görecektir.
- Anahtar değişimi için endüstri standardı protokolleri sessiz dinleyicileri içerecek şekilde değiştirilirse, kullanıcılar Internet altyapısının diğer yönlerinde kimlik doğrulama ve anahtar değişimi protokollerine nasıl güvenebilirler?
- Hayalet protokol önerileri pasif olarak sessiz dinleyiciler eklemez: üçüncü tarafların sözde güvenli ve gizli hizmetlere müdahalesini aktif olarak gizlerler.

4.5 İDARENİN MÜDAHALESİ

- ISOC İdarenin Müdahalesini, hükümet kurumlarının (kolluk kuvvetleri) şifrelenmiş bilgilere erişmek için sistemlerde, yazılımlarda veya donanımda bulunan güvenlik açıklarından yararlanması olarak tanımlamaktadır.
- Kolluk kuvvetleri, güvenlik testleri veya başka herhangi bir amaç için herhangi bir tür güvenlik açığından yararlanabilir.
- Teknik açıdan bakıldığında, kullanıcının / sahibinin izni olmadan bir bilgi, iletişim veya teknoloji (BİT) kaynağına müdahale etmek bir aygıta, sisteme veya etkin iletişim akışına zarar verebilir veya daha az güvenli bir durumda bırakabilir. Bu, sonraki ihlal riskini önemli ölçüde artırır ve potansiyel olarak sistemin tüm kullanıcılarına zarar verir.

4.5.1 İDARENİN MÜDAHALESİNİN TEHLİKELERİ

- Müdahale sonuçları çalınabilir, sızdırılabilir ya da kopyalanabilir ve idarenin kontrolü dışına çıkabilir.
  - Shadow Brokersgroup, 2017 yılında ABD Ulusal Güvenlik Ajansı'nı hackledi ve Eternal zero-day istismarını kamuya açıkladı.
  - İtalyan güvenlik firması Hacking Team, 2015 yılında hacklendi
  - Vault 7 olarak bilinen CIA hackleme araçlarından oluşan bir koleksiyon 2017'de sızdırıldı
- Ticari bilgisayar korsanları ekipleri sadece hizmetlerini "iyi adamlara" satmazlar.
  - 2019'da güvenlik araştırmacıları, NSO Group'un yazılımının gazetecilerin ve aktivistlerin WhatsApp hesaplarına gizlice saldırmak için kullanıldığını keşfetti.
- Bir hedef çoklu hedefe dönüşebilir. İleri kalıcı tehditlere dönüşebilir.
  - Bunun en ünlü örneği, ABD ve İsrail hükümetleri tarafından İran'ın nükleer santrifüjlerini yok etmek için oluşturulan ve daha sonra hedeflenenin ötesinde milyonlarca diğer sistemi etkileyen ve dünyaya yayılan Stuxnetvirüs'tür.

4.5.2 İDARENİN MÜDAHALESİ ŞARTLARI

- Ciddi bir tehdit vardır. İnsan hayatını korumak, kamu güvenliğini sağlamak ya da önemli bir suçu engellemek için müdahale edilebilir.
- Başka alternatif yol yoktur.
- Yargı denetimi vardır.
- Müdahale tehditle orantılıdır.
- Olası riskler bertaraf edilmiştir.
- Risk değerlendirme prosedürleri uygulanmıştır.
- Her müdahale ayrıca ele alınmıştır.

4.6 ŞİFRELEME ARKA KAPILARI HAKKINDA DEĞERLENDİRMELER

- Adli erişimi sağlamak için şifreleme veya diğer güvenlik mekanizmaları zayıflarsa, herhangi bir üçüncü tarafın erişim kazanması daha kolay hale gelir (özellikle organize suç örgütleri, endüstriyel casusluk yapan şirketler ve diğer devlet aktörleri gibi).
- Ayrıca, kimlik hırsızlığını, finansal ve fikri mülkiyet haklarıyla ilgili hassas bilgilere erişimi kolaylaştırmak vatandaşların ve şirketlerin meşru menfaatlerini zayıflatır.
- İyi niyetli bile olsa şifreleme kullanımını sınırlamaya yönelik yasal ve teknik girişimler, yasalara uyan vatandaşların ve genel olarak Internet'in güvenliğini olumsuz yönde etkileyecektir.
- Şifreleme arka kapı önerilerinin, suçluların gizli iletişimine karşı faydasından çok sıradan vatandaşlara önemli güvenlik riskleri getirir.

4.6.1 ŞİFRELEME ARKA KAPILARI İÇİN BİR METAFOR – VALİZ KİLİTLERİ

- TSA onaylı valiz kilitleri yolcuların valizlerinin güvenliğini sağlarken TSA'nın valiz içeriğini incelemek üzere açabilmesine imkan sağlamak üzere geliştirilmişti. TSA'da ana anahtar olacak ve valizleri açabilecekti.
- Fakat bu ana anahtar gizi kalmadı ve 3D yazıcıda üretilerek ve 10$ maliyetler satılarak herkesin eline geçmesi sağlandı. Bu da TSA onaylı kilitlerin kötü niyetlilerce açılabilmesine imkan sağladı.

5 ŞİFRELEMENİN İNSANİ AÇIDAN ÖNEMİ

- Kişisel verilerin korunması
- Sağlık verilerine yetkisiz erişimin engellenmesi
- Ayrımcılığa karşı korunma
- Özgür basının haberi ulaşması ve haber kaynaklarını koruması
- Veri bütünlüğünün sağlanması
- Çocukların kişisel verilerinin, sağlık bilgilerinin, arkadaşlarıyla iletişimlerinin korunması

6 SONUÇ

- Şifreleme her gün milyonlarca insanı güvende tutar.
- Şifrelemeyi zayıflatma çabaları, hassas bilgilere erişmek ve bu bilgileri kullanmak için suçlulara, terörist örgütlere ve yabancı hükümetlere yeşil ışık yakan tehlikeli bir emsal oluşturacaktır.
- Şifrelemeyi zayıflatmak, hem kişisel güvenlik hem de ulusal güvenlik için yıkıcı sonuçlarla yol açabilir.
- Suçu önlemenin ve ülkeleri korumanın en iyi yolu, daha güçlü şifreleme politikaları ve endüstri uygulamaları benimsemektir.
- Suçun önlenmesi, vatandaşların korunması ve ulusların korunması için güçlü şifreleme politikaları ve endüstri uygulamaları için zorlamalıyız.

7. KAYNAKLAR

- Internet Society Encryption homepage: https://www.internetsociety.org/issues/encryption/
- Internet Society Encryption policy brief: https://www.internetsociety.org/policybriefs/encryption/
- Internet Society Encryption resources page: https://www.internetsociety.org/encryption/internetcommunity-stands-up-for-encryption/
- Internet Society Factsheet for policymakers on lawful access: https://www.internetsociety.org/resources/doc/2019/factsheet-for-policymakers-6ways-lawful-access-puts-everyones-security-at-risk/

KAYNAKLAR

- Internet Society's Client-Side Scanning Factsheet: https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/
- Matthew Green, Dec 2019. Can end-to-end encrypted systems detect child sexual abuse imagery? https://blog.cryptographyengineering.com/2019/12/08/on-client-side-mediascanning/
- Electronic Frontier Foundation, Nov 2019. Why Adding Client-Side Scanning Breaks End-To-End Encryption. https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-endend-encryption

TEŞEKKÜRLER