

Demystifying SSL/TLS security: Past, present and future of secure connections.



kub0x@elhacker.net

Sobre mí

- Autodidacta al que le apasiona la seguridad informática y la programación.
- Investigador de seguridad y malware en tiempo libre.
- Colaboro activamente en varios proyectos como desarrollador.
- Participo como moderador en elhacker.net resolviendo dudas de programación y seguridad.

Objetivo de la ponencia

- Explicar el funcionamiento de los procedimientos seguros en internet y su seguridad.
- Concienciar al usuario de la inseguridad de dichos procedimientos.
- Desmitificar la idea de la internet segura.
- Proveer ataques conocidos así como soluciones alternativas y tendencias del futuro.

Mirada al pasado

- Las conexiones seguras se introdujeron en 1996 de la mano de HTTPS (HTTP over SSL/TLS).
- Infraestructura basada en PKI.
- Se definió el estándar de los certificados X.509.
- Se abrió paso al e-commerce.
- Muy pocos sitios webs lo implementaban.
- Muy pocas entidades certificadoras (CAs).
- Lo peor estaba por venir...

DEMO #1

Squid MITM



EAR PROTECTION

You're doing it wrong

DEMO #2

Squid .js injection



Situación actual

- Sistema de confiabilidad dependiente de las CAs. Hay demasiadas, algunas dudosas.
- Mantiene el esquema de la infraestructura inicial.
- La ley obliga a proteger datos sensibles como la identificación del usuario y sus transacciones.

Análisis de la situación actual

- Implementar SSL/TLS = \$\$
- !Privacy && Surveillance= Gobiernos, ISPs, empresas...
- Errores en la validación de certificados de lado del cliente.
- Vulnerabilidades en: CAs, certificados X.509 y distintas librerías de lado del cliente.
- Usuarios no informados sobre las protecciones necesarias.

Seguridad en SSL/TLS (I)

- Falsa sensación de seguridad:
 - Certificados falsos emitidos a gobiernos, ISPs, empresas...
 - Software malicioso que instala CAs confiables en el equipo del usuario para posteriormente espiar sus comunicaciones.
 - Servicios anónimos (TOR, VPNs, Proxys) que registran y descifran la actividad de sus usuarios.

Seguridad en SSL/TLS (II)

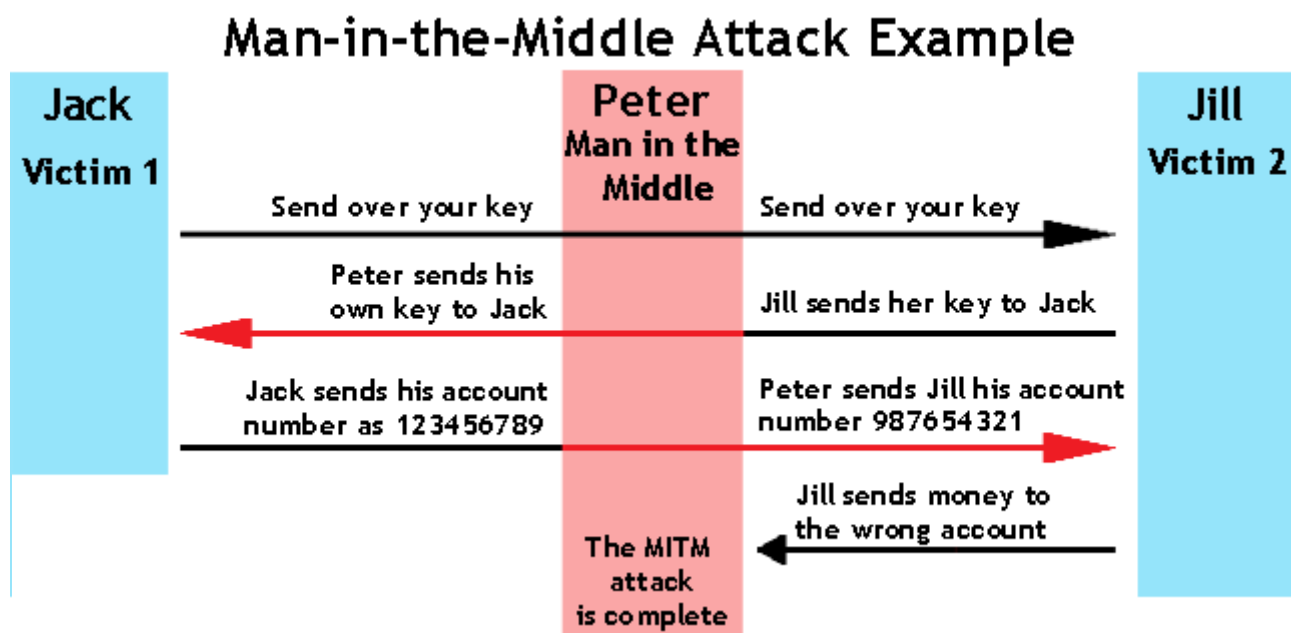
- Desconocimiento del usuario:
 - Si Facebook le planta error de certificado, seguramente acepte el certificado presentado, ya que Facebook no funciona.
 - No actualizar el Software a su última versión. Attacker → exploit-unpatched → 0wn3d.
 - Otras meteduras de pata típicas: Phising, Ing social, Warez/P2P, Hoax/Scams...

Seguridad en SSL/TLS (III)

- Mala praxis en software:
 - Notificaciones de error demasiado técnicas.
 - Permiten al usuario decidir.
 - Algunos no indican si se está estableciendo una conexión segura.
 - Malas prácticas en la validación de los certificados.
 - Vulnerabilidades críticas no parcheadas.

Man in the middle (MITM)

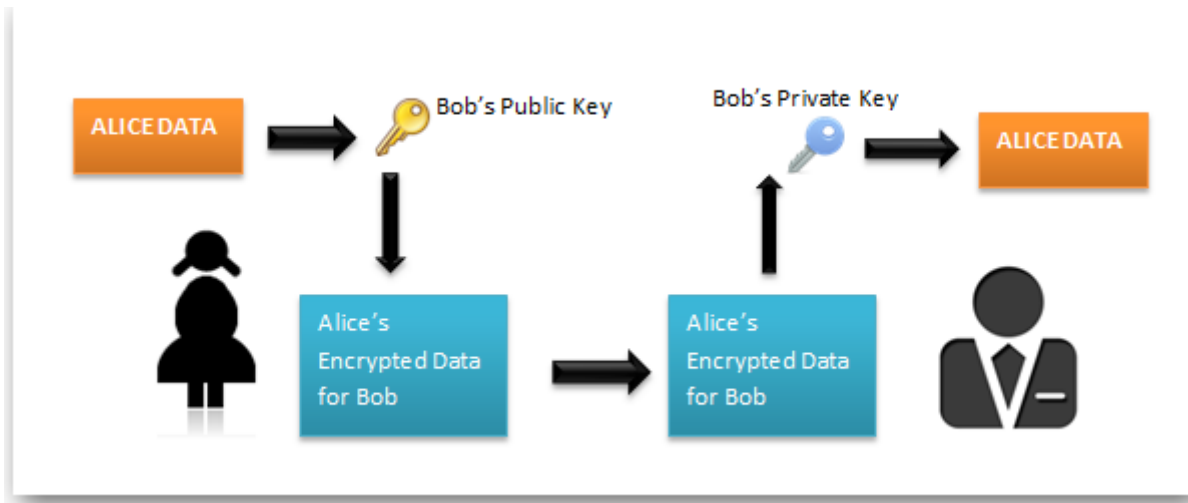
- Consiste en interceptar las conexiones de un objetivo. (ARP/DNS Spoofing).
- Variantes:
 - Pasivo: registra la comunicación.
 - Activo: registra y modifica la comunicación.



Crypto in a nutshell

- Criptografía simétrica
 - Alice y Bob cifran/descifran con la misma clave.
- Criptografía asimétrica
 - Alice genera un par de claves público/privado así como Bob.
 - Alice y Bob intercambian las claves públicas.
 - Los mensajes se descifran con las claves privadas.
- SSL/TLS combina criptografía asimétrica y simétrica para agilizar el intercambio de datos.

El mundo sin PKI



- El atacante intercepta el intercambio de claves públicas y entrega su propia clave pública a Alice y Bob.
- Alice envía un mensaje a Bob cifrándolo con la pública del atacante. El atacante descifra con su privada y cifra con la pública de Bob.
- Bob descifra el mensaje con su privada. Los datos han llegado, pero han sido leídos.

Certificate Authorities (I)

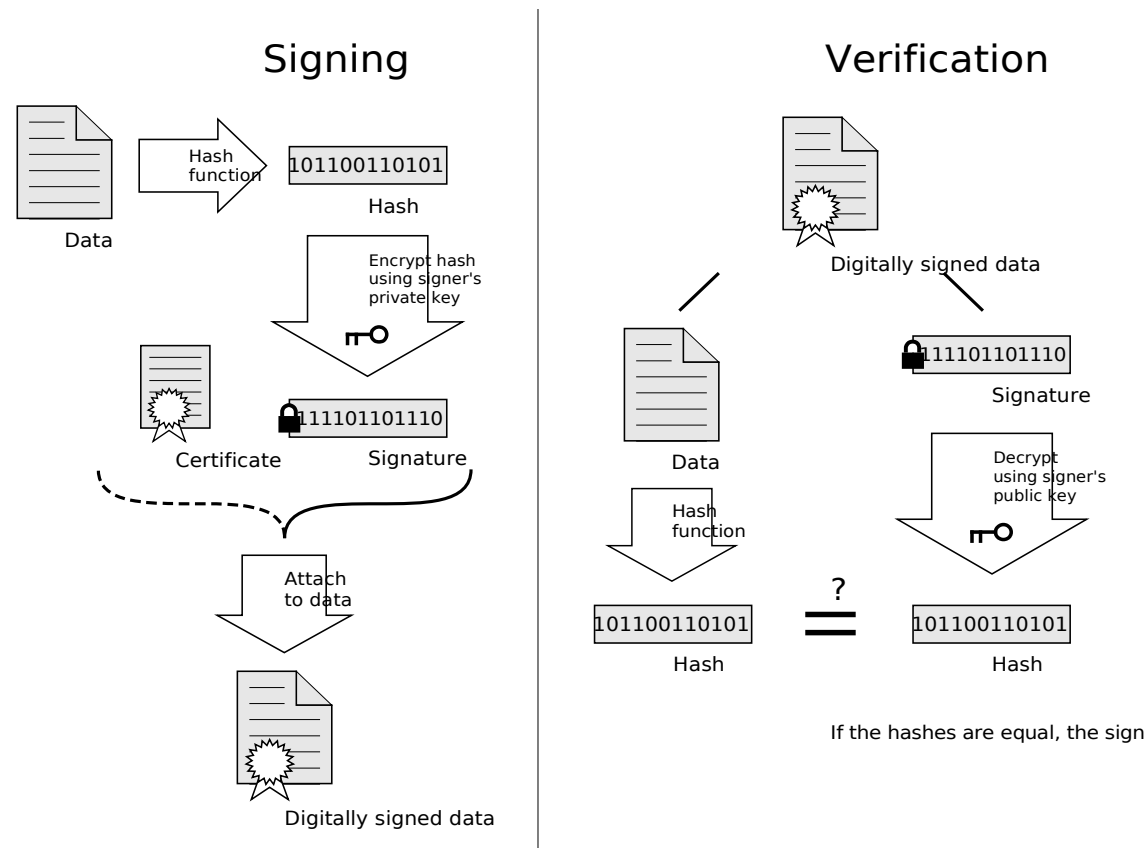
- Actua como un notario.
- Comprueba las solicitudes de emisión de certificados.
- Emite certificados.
- Revoca certificados.
- Renueva certificados.

Certificate Authorities (II)

- Ejemplo en la vida real:
 - Alice y Bob quieren comunicarse.
 - Contratan a un notario llamado VeriSign.
 - Bob le envía a Alice un certificado firmado por VeriSign.
 - Alice comprueba que el certificado está firmado por un notario de confianza.
 - Alice comprueba que el certificado proviene de Bob.
 - Alice establece el canal de comunicación.

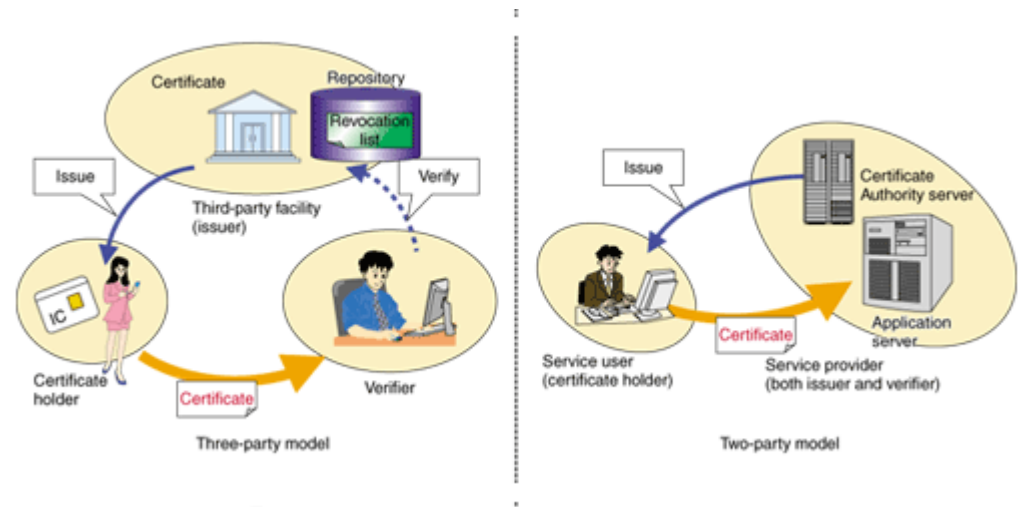
Firma Digital

- Ofrece mecanismos de autenticación sobre una clave pública empleando certificados.
- Autenticación, integridad y no repudio.



PKI

- Public Key Infrastructure.
- Formado por los elementos encargados de emitir, verificar, revocar, mantener y confiar certificados.
- Soluciona el problema de la autenticidad, integridad y no repudio de los datos.



Lo que los usuarios ven...

 <https://www.youtube.com/>

 PayPal, Inc. (US) | <https://www.paypal.com/>



Está conectado a

google.es

Verificado por: Google Inc










La conexión con este sitio web es segura.



Más información...

Lo que los usuarios no ven...

Nombre del certificado	Dispositivo de seguridad
AddTrust External CA Root	Builtin Object Token
COMODO High-Assurance Secure Server CA	Disp. software de seguridad
COMODO RSA Certification Authority	Disp. software de seguridad
COMODO SSL CA	Disp. software de seguridad
PositiveSSL CA 2	Disp. software de seguridad
GlobeSSL CA	Disp. software de seguridad
Intel External Basic Policy CA	Disp. software de seguridad
InCommon Server CA	Disp. software de seguridad
SSL.com Free SSL CA	Disp. software de seguridad
TBS X509 CA pro hosting	Disp. software de seguridad
USERTrust Legacy Secure Server CA	Builtin Object Token
UTN-USERFirst-Hardware	Disp. software de seguridad
UTN-USERFirst-Hardware	Disp. software de seguridad
USERTrust RSA Certification Authority	Disp. software de seguridad

Emitido para	Emitido por	Fecha de expir
 AddTrust External CA Root	AddTrust External CA Root	30/05/2020
 Baltimore CyberTrust Root	Baltimore CyberTrust Root	13/05/2025
 Certum CA	Certum CA	11/06/2027
 Certum Trusted Network CA	Certum Trusted Network CA	31/12/2029
 Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	02/08/2028
 Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	08/01/2004
 Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	31/12/1999
 DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	10/11/2031
 DigiCert Global Root CA	DigiCert Global Root CA	10/11/2031
 DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	10/11/2031
 Disc Soft Ltd	GlobalSign CodeSigning CA - G2	30/05/2015
 Entrust.net Certification Author...	Entrust.net Certification Authority...	24/07/2029
 Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	22/08/2018
 GeoTrust Global CA	GeoTrust Global CA	21/05/2022
 GlobalSign Root CA	GlobalSign Root CA	28/01/2028
 Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	29/06/2034
 Go Daddy Root Certificate Auth...	Go Daddy Root Certificate Author...	01/01/2038
 GTE CyberTrust Global Root	GTE CyberTrust Global Root	14/08/2018
 http://www.valicert.com/	http://www.valicert.com/	26/06/2019
 Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	01/01/2000
 Microsoft Root Authority	Microsoft Root Authority	31/12/2020

Inside UPV/EHU (URL not_in_SAN)



Esta conexión no está verificada

Ha pedido a Firefox que se conecte de forma segura a **ehu.es**, pero no se puede confirmar que la conexión sea segura.

Normalmente, cuando se intente conectar de forma segura, los sitios presentan información verificada para asegurar que está en el sitio correcto. Sin embargo, la identidad de este sitio no puede ser verificada.

¿Qué debería hacer?

Si normalmente accede a este sitio sin problemas, este error puede estar ocurriendo porque alguien está intentando suplantar al sitio, y no debería continuar.

[¡Sácame de aquí!](#)

► Detalles técnicos

► Entiendo los riesgos

Nombre DNS: **www.ehu.es**

Nombre DNS: **login.ehu.es**

Nombre DNS: **loginso.ehu.es**



Nombre DNS: **nire.ehu.es**

Nombre DNS: **secure.ehu.es**

PKI Security (I)

- Comodo y DigiNotar fueron comprometidas.
 - Emitieron certificados válidos a cibercriminales.
 - CEO de Comodo → “Fue un ataque satisficado”.
 - El atacante no era muy habilidoso.
 - CEO de Comodo → Premio emprendedor del año.

PKI Security (II)

- CAs doing wrong:
 - (www.paypal.com|www.youtube.com|
www.ebay.com|www.bankofamerica.com|
www.amazon.com)\0.miweb.com
 - Hash collision attacks (MD5).
 - Basic constraints.
- Browsers doing wrong:
 -  PayPal, Inc. (US) | <https://www.paypal.com/>
 -  <https://www.youtube.com/>

PKI Security (III)

- Revocación de certificados:
 - Anulan certificados falsos, pasados de fecha...
 - Revocación basada en OCSP.
 - OCSP → HTTP → MITM → Bypass.

OCSP: URI: <http://clients1.google.com/ocsp>

Revocation Issue

- Ejemplo práctico:
 - Alice y Bob se quieren comunicar.
 - Bob le envía a Alice su certificado firmado por el notario VeriSign.
 - Eve intercepta la comunicación y sustituye el certificado por uno firmado por VeriSign, el cual es falso, está a nombre de Bob pero está revocado.
 - Alice comprueba si el certificado está revocado.
 - Eve modifica la conexión de revocación y hace creer a Alice que el certificado está vigente.
 - El canal seguro ha sido comprometido.

Software Issue (I)

- Actualizaciones de Software:
 - Muchas viajan en HTTP y descargan código sin firmar.
 - Un atacante podría modificar el Binario de la actualización para que nuestro equipo lo instale.
- Vulnerabilidades en Software:
 - 0 Days en Chrome, Firefox, Opera, Safari, IE...

Software Issue (II)

Update Server In The Sky

TLS Connection to:
aus2.mozilla.org

Hello, do you have any updates for me? Here's my product, version, build ID, OS, locale, and channel.

TLS Connection to:
aus2.mozilla.org

As a matter of fact, I do. Here's an unsigned blob of data – you'd do well to install it.



Software Issue (III)

- Librerías SSL/TLS:
 - Múltiples vulnerabilidades.
 - Muchos todavía siguen sin saber emplearlas.
 - Amazon, Paypal, Apache, Lynx...
 - Un mal uso deriva en agujeros de seguridad e incurre en costos (\$\$).

Breve repaso

- Las CAs no son seguras.
- OCSP no es seguro.
- PKI → bien pensado pero mal mantenido.
- Las aplicaciones no son seguras.
- Las librerías SSL/TLS no son seguras.
- Los programadores cometen fallos.
- Los usuarios lo complican.
- Casi 20 años con la misma historia.

En definitiva

- Tengo todos tus datos de navegación.
- Tengo acceso a tu equipo.
- Tengo acceso a los equipos de tu red.
- Tengo acceso a los datos cifrados de toda la red.
- Happy Hacking! =D

RESUMIENDO...

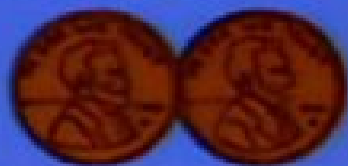


Futuro de SSL/TLS

- Web of trust (WOT): PGP, GnuPG.
- Repositorio público de certificados (Google).
- Perspective AKA Convergency.
- Deshacerse de los trust-anchors.
- DNSSEC.
- Let's Encrypt.
- TACKS.



MY TWO CENTS



WITH
KENT BROCKMAN



Referencias

- <https://github.com/FreeJaus/gea-PRISM/tree/master/Documentation>
- <http://convergence.io/>
- http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
- <http://tack.io/>
- <http://www.wired.com/2010/03/packet-forensics/>
- <https://www.youtube.com/watch?v=ibF36Yyeehw>
- <https://www.youtube.com/watch?v=GYwmPZIN6Ec>
- <http://www.globbtv.com/mundohackertv/>
- <https://foro.elhacker.net/profiles/kub0x-u350531.html>
- <https://twitter.com/freejaus>
- <https://www.youtube.com/user/FreeJaus>



**THANK
YOU
for
LISTENING
ANY QUESTIONS?**