Lección 10: Ataques al protocolo SSL

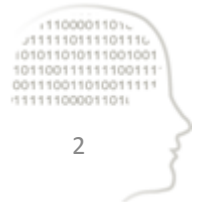
intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Luciano Bello - luciano@debian.org
Chalmers University
Dr. Alfonso Muñoz - amunoz@diatel.upm.es
T>SIC Group. Universidad Politécnica de Madrid

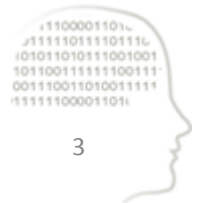
Seguridad del protocolo SSL (Secure Sockets Layer)

- SSL/TLS es seguro en su diseño teórico. Pero esto es una condición necesaria aunque no suficiente.
- La "seguridad real" del protocolo SSL tiene que ser matizada. Por ejemplo en su uso en la web va mucho más allá de la idea equivocada de que una página es segura si y solo si se muestra el famoso "candado amarillo".



Seguridad del protocolo SSL
Consideraciones

- Fallos de programación. Debilidades
- Criptoanálisis y Downgrade
- Mala configuración. Atacando a OCSP
- Engañar al usuario
- Robo o compromiso de una autoridad de confianza



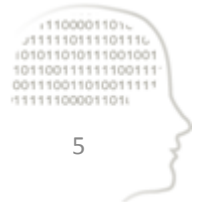
Fallos de programación. Debilidades

- Fallos de programación en las implementaciones del protocolo SSL afectan a su seguridad.
- Ejemplo: el investigador Luciano Bello en 2008 descubrió problemas en las funciones aleatorias de Openssl/Debian. Esto facilitó invertir procesos aleatorios, falsificar certificados X.509, claves SSH, etc.

Fallos de programación. Debilidades

- Ejemplo: ataque NULL byte (2009)

Moxie Marlinspike descubrió que los estándares de certificado X.509 y SSL definen la cadena CN (Common Name) como una cadena PASCAL (se declara la longitud de la cadena en la posición 0 y se pone la cadena en el resto de posiciones). Curiosamente la mayoría de software de procesamiento de certificados está escrito en C. Dicho software suele manejar la cadena como una cadena C, poniendo un NULL (\0) al final de la cadena para indicar dónde termina. El problema llega cuando alguien obtiene un certificado de la forma www.bancolegitimo.com\0www.atacante.org. Cuando se procesa por un navegador, sólo se leerá la primera parte, www.bancolegitimo.com, permitiendo falsificar fácilmente al banco.

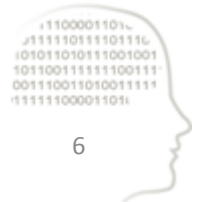


Criptoanálisis y Downgrade. Debilidades

- El uso de algoritmos criptográficos con vulnerabilidades facilitan ataques al protocolo.

  Ejemplo: en la 25 edición de la Chaos Communication Congress (2008) se falsificó un certificado SSL atacando al algoritmo criptográfico MD5.

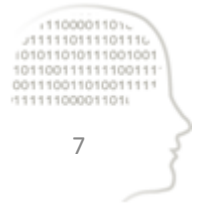
- Se debe evitar utilizar versiones del protocolo antiguas o que un atacante fuerce su uso (downgrade).



Mala configuración. Atacando a OCSP

Si un atacante está haciendo un ataque de hombre en el medio puede interceptar las peticiones OCSP y utilizarlas en su provecho

En un funcionamiento normal un servidor OCSP podría enviar una respuesta *Try Later* indicando al cliente que ahora no puede atender una petición. El atacante podría simular esta contestación (código 3), para indicar al cliente que ahora no puede atender su petición. Ante esta situación muchos clientes Web aceptarán el certificado digital al no poder corroborar su validez, lo que claramente es un fallo.

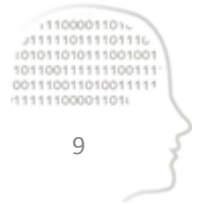


Engañando al usuario

1. Certificado digital creado por el atacante. El navegador web alerta que el certificado no es reconocido. El ataque solo tiene lugar si el usuario lo acepta.

Engañando al usuario

2. Herramienta SslStrip (Moxie Marlinspike, 2009) automatiza un ataque de hombre en el medio al protocolo SSL. Sustituye todos los enlaces https por http, con la intención que la comunicación entre el cliente y el atacante sea por http y la comunicación entre atacante y servidor por https.



Engañando al usuario

3. En un caso hipotético se podrían generar certificados válidos de entidades comerciales concretas para fuerzas gubernamentales, por ejemplo, por orden judicial, que permitiría hacer un hombre en el medio difícilmente detectable, en tanto en cuanto el certificado sería válido y firmado por una autoridad competente. Esto se podría realizar, por ejemplo, para un certificado digital con un número de serie concreto.

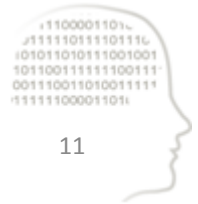
Robo o comprometer autoridad de confianza

Certificados “fraudulentos” firmados por una autoridad de confianza

Marzo 2011: Línea de negocio de certificados SSL de la empresa Comodo.

Se ejecutaron peticiones de firmado sin la correspondiente verificación. Lo que produjo emisión de certificados falsos para sitios tan populares como Google, Yahoo, Mozilla, etc.

Julio 2011: Comprometida autoridad certificadora Diginotar.

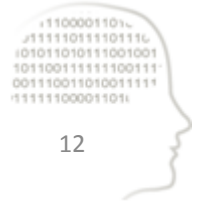


Recomendaciones

- La versión más moderna del protocolo TLS con las extensiones recomendadas, puede considerarse segura frente a los ataques conocidos.

  Septiembre 2011 (ekoparty Conference). ***Chosen-plaintext attack against TLS v1.0*** (no afecta TLS v1.1 y v1.2)

- Los ataques que vulneran su seguridad se centran especialmente en engañar al usuario con la dirección a la que se conecta o con el certificado digital que autentifica al servidor.

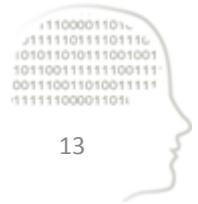


Alguna recomendación para navegación web

1. Navegador web actualizado

2. Conectar directamente a la dirección https por la url. El add-on para firefox “HTTPS Everywhere” puede ayudar a automatizar esto.

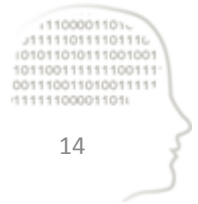
3. Denegar acceso a una página Web cuando el certificado no sea válido.



Alguna recomendación para navegación web

4. Configurar los navegadores web para que hagan comprobaciones OCSP por defecto.

5. Si la conexión OCSP falla, el certificado por defecto no será dado por bueno.



intypedia

INFORMATION SECURITY ENCYCLOPEDIA

  Contacto: info@intypedia.com