educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

Módulo 2

Criptoanálisis

Generalidades

El criptoanálisis puede intentar obtener la clave u obtener directamente el mensaje.

También cae dentro del criptoanálisis el **arte de explotar las debilidades de los protocolos de comunicación segura** (autenticación, administración de claves, fallas de *hardware* y/o *software,* etc.)

La práctica del criptoanálisis se denomina en la jerga como "***romper el criptosistema***".

Intenta determinar el lenguaje utilizado, el tipo general de cifrado o código, las claves utilizadas y finalmente, la reconstrucción del mensaje.

Estas determinaciones se realizan con base en cantidades variables de texto cifrado e información relacionada, tales como la identidad del emisor y receptor, análisis estadístico de tráfico y conocimiento de alguna información específica acerca de los contenidos del mensaje.

Tipos de ataques

Ataques blandos

Involucran la coerción (criptoanálisis de manguera de goma) o ingeniería social y a menudo son los más efectivos.

Ataques por fuerza bruta

Comprenden la búsqueda exhaustiva de una clave en todo el espacio de claves disponible. Pueden ser activo, pasivo u *offline*, o incluso una combinación de ellos. Es un tipo de ataque en franco aumento.

Ataques *man in the middle*

Son una generalización de la suplantación de IP *(IP address spoofing)* y por lejos es el ataque más poderoso. Es conocido desde la antigüedad y todos los cifrados son susceptibles a él.

Ataques de texto plano

Conocido utilizan una determinada cantidad de texto claro y su correspondiente texto cifrado (una criba) y a partir de ahí se encuentra su clave. Habitual en RSA, *emails* y *e-commerce.*

Ataques de texto cifrado conocido

Involucran una parte conocida de un texto cifrado para obtener la clave y el texto claro. Implican mucho trabajo (Ej.: Kasiski).

Ataques de retransmisión (*relay attacks*, *key cars fobs*)

Consisten en el reenvío del mensaje por parte de un adversario. Si el mensaje no se altera se trata de un ataque pasivo, en caso contrario es activo. Se han vuelto importantes por el uso de NFC (*Near Field Communication*). “Nunca deje la llave de su automóvil cerca del frente de su casa”.

Ataques de texto claro elegido

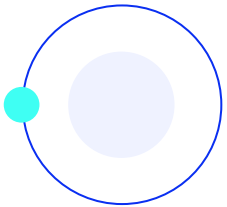
Implican definir un texto claro particular, pasarlo al dispositivo de cifrado y recuperar y analizar el texto cifrado resultante. Cualquier sistema que utilice las mismas claves para cifrar gran cantidad de información es susceptible a este ataque (por ejemplo, WEP). Puede ser usado contra RSA, donde la clave pública es conocida.

Ataques de cumpleaños

Son ataques específicos contra firmas digitales y algoritmos de logaritmos discretos.

Ataques de texto cifrado

Elegido consisten en intentar que la víctima descifre un texto cifrado predeterminado para obtener la clave. Una alternativa consiste en descifrar un criptograma con claves aleatorias para obtener algún tipo de información acerca de la clave verdadera. Se debe usar hashing para evitarlo.

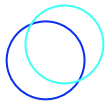


Ataques de repetición

Utilizan partes de un intercambio cifrado previo. Existen dos variantes: en la primera, el mensaje original llega a su destino, pero es copiado para ser repetido posteriormente. En la segunda variante, el mensaje es interceptado y se impide que llegue a destino, para ser usado posteriormente. La protección consiste en usar *timestamps* (Kerberos).

Ataques contra RSA

No son muy peligrosos, más bien ilustran el problema de una mala implementación. Un ataque es al ataque factorial mediante la técnica de Pollard. Otros ataques son reencriptar el texto cifrado, el ataque de pads breves de Coppersmith y el ataque de exponentes pequeños.



Criptoanálisis diferencial

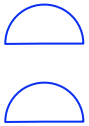
Fue desarrollado originalmente para atacar cifrados basados en redes de Feistel (por ejemplo DES) en los ‘80. Consiste en diseñar cuidadosamente textos planos con diferencias conocidas que resulten en distribuciones estadísticas particulares de los textos cifrados a través de las distintas rondas de cifrado.

Ataques con preprocesamiento

Incrementan dramáticamente la velocidad de ejecución de los algoritmos. La idea es calcular previamente con los datos que se dispongan en el momento para intentar romper los códigos más tarde, cuando se envíen los mensajes (Diffie-Hellman, 2019).

Ataques *cold boot*

Los ataques de este tipo sobre memoria DRAM volátil consisten en extraer los datos de los chips de memoria en una computadora recientemente apagada. Muchos expertos de seguridad y los sistemas operativos dan por sentado que los datos no persisten en la memoria más allá de segundos, por lo cual no toman ninguna medida preventiva. Un atacante que tuviera acceso al dispositivo físico inmediatamente después que fuera apagado, podría lograr que los datos se mantengan durante minutos o incluso horas si almacena los chips a baja temperatura. Los datos residuales pueden ser recuperados con técnicas simples, no destructivas, que solamente requieren acceso físico momentáneo a la máquina. Es un ejemplo de ataque de canal lateral.



Ataques de canal lateral

Son ataques basados en **información adicional** que se puede recopilar debido a la forma fundamental en que se implementa un protocolo o algoritmo informático, en lugar de fallas en el diseño del protocolo o algoritmo en sí.

Algunos ataques de canal lateral requieren conocimientos técnicos del funcionamiento interno del sistema, aunque otros, como el análisis de potencia diferencial, son efectivos como ataques de caja negra.

El auge de las aplicaciones Web 2.0 y el *software* como servicio han aumentado significativamente la posibilidad de ataques de canal lateral en la web, incluso cuando las transmisiones entre un navegador web y el servidor están encriptadas.

El principio subyacente es que los efectos físicos causados por el funcionamiento de un criptosistema pueden proporcionar información adicional útil sobre secretos en el sistema, por ejemplo, la clave criptográfica, información de estado parcial, textos planos completos o parciales, etc.

Tipos de ataques de canal lateral

- **Ataques de caché:** se basan en la capacidad del atacante para monitorear los accesos a la memoria caché realizados por la víctima tanto en un sistema físico compartido como en un entorno virtualizado o un tipo de servicio en la nube.
- **Ataques de tiempo:** se basan en medir cuánto tiempo tardan en realizarse varios cálculos (como, por ejemplo, comparar la contraseña dada por un atacante con la desconocida de la víctima).
- **Ataques sobre datos remanentes:** buscan acceder a datos supuestamente eliminados (por ejemplo, ataques *cold boot*).
- **Ataques de fallas iniciados por *software*:** son una clase rara de ataques, por ejemplo, Row Hammer, que aprovecha un efecto secundario en la memoria DRAM en la que las células de memoria interactúan eléctricamente entre sí filtrando sus cargas, posiblemente cambiando el contenido de las filas de memoria cercanas que no se abordaron en el acceso a la memoria original.

Criptoanálisis acústico: consiste en ataques que explotan el sonido producido durante un cálculo. La mayor parte del criptoanálisis acústico moderno se centra en los sonidos producidos por los teclados de las computadoras y los componentes internos de la computadora, pero históricamente también se ha aplicado a impresoras y máquinas de descifrado electromecánicas.

Análisis diferencial de fallos (DFA): es un tipo de ataque activo que consiste en inducir fallas (condiciones ambientales inesperadas) en operaciones criptográficas para revelar sus estados internos.

Ataques de monitoreo de energía: hacen uso de un consumo de energía variable por parte del *hardware* durante el cálculo.

Ataques electromagnéticos: se basan en estudiar la radiación electromagnética filtrada, que puede proporcionar directamente textos sin formato y otra información. Tales mediciones se pueden usar para inferir claves criptográficas utilizando técnicas equivalentes a las del análisis de potencia o se pueden usar en ataques no criptográficos, por ejemplo, ataques TEMPEST.

Ataques a listas de dispositivos autorizados: están basados en el hecho de que estos dispositivos se comportarán de manera diferente cuando se comuniquen con dispositivos permitidos (devolviendo las respuestas) y no permitidos (que no responden a los dispositivos en absoluto). Se puede utilizar para rastrear direcciones MAC de Bluetooth.

Ataques ópticos: se basan en el hecho de que los secretos y los datos confidenciales se pueden leer mediante grabación visual utilizando una cámara de alta resolución u otros dispositivos que tengan tales capacidades.

¡Sigamos trabajando!