Ataques a un Criptosistema

Modelos de ataques teóricos a un Criptosistema

Ciphertext-only attacks: El atacante conoce el algoritmo de cifrado y algunos textos cifrados

Known-plaintext attacks: El atancate conoce el algoritmo de cifrado y algunos pares arbitrarios de texto plano y cifrado

Chosen-plaintext attacks: El atacante conoce el algorimo de cifrado y algunos pares de texto plano y cifrado de los cuales ha podido seleccionar el texto plano

Chosen-ciphertext attacks: El atacante conoce el algorimo de cifrado y algunos pares de texto plano y cifrado de los cuales ha podido seleccionar el texto plano y/o el texto cifrado

Rompiendo un Criptosistema

Se dice que un Criptosistema esta “roto” cuando exite un método para **determinar el texto plano a partir del texto cifrado sin** que involucre recibir legítimimamente **la clave de descifrado**

Normalmente exiten **dos formas de “romper” un Criptosistema**:

- Encontrar un método para **determinar la clave de descifrado**. Esto permite descifrar textos cifrado previamente
- Encontrar una **vulnerabilidad en el algoritmo** de cifrado que permite obtener el texto plano a partir del texto cifrado sin requerir la clave de descifrado

Métodos de ataque | Fuerza bruta

Existe un método que puede ser utilizado para romper todos los algoritmos de cifrado: **Fuerza Bruta**

El ataque de fuerza bruta (*Ciphertext-only attack*) consiste en:

1. El atacante intercepta texto cifrado con un Criptosistema conocido
2. El atacante selecciona una clave del espacio de claves
3. El atacante intenta descifrar el texto cifrado utilizando esa clave y comprueba si el resultado tiene sentido
4. Si el texto plano resultante tiene sentido, entonces el atacante ha encontrado la clave de cifrado. En caso contrario, selecciona otra clave y comienza de nuevo el proceso.

Importancia del espacio de claves

El espacio de claves comprende todas las claves de descifrado posibles para un criptosistema concreto

Para evitar un ataque de fuerza bruta, **deben existir suficientes claves de descifrado como para que no resulte práctico el proceso**. Ya sea por que consume demasiado tiempo o demasiado dinero

Todas las claves de descifrado deben tener la misma probabilidad de ser elegidas. De no ser así, el espacio de claves se reduce

Otros métodos de ataque

Time memory trade-off attacks: El atacante construye una tabla con textos cifrados a partir de textos planos que se envían con frecuencia utilizando un número muy elevado de claves. Cuando el atacante intercepta un texto cifrado para el que conoce o supone el texto plano, comprueba en la tabla si se encuentra la clave.

Primitive-specific attacks: *Differencial and linear cryptoanalysis, Birthday attacks, Statistical attacks...*

Side-channel attacks: Estos ataques no se realizan directamente sobre el criptosistema sino contra su implementación. Algunos de los más interesantes: *Timing attacks, Power analysis, Fault analysis...*