

Lanka Education and Research Network

Attacks on Cryptosystems

Attacks on Cryptosystems

- Attempts to gain unauthorized access to secure communications have typically used brute force attacks (ciphertext attacks)
- Attacker may alternatively conduct known-plaintext attack or selected-plaintext attack schemes

Man-In-The-Middle Attacks

- Designed to intercept transmission of public key or insert known key structure in place of requested public key
- From victims' perspective, encrypted communication appears to be occurring normally, but in fact attacker receives each encrypted message, decodes, encrypts, and sends to originally intended recipient
- Establishment of public keys with digital signatures can prevent traditional man-in-the-middle attack

Correlation Attacks

- Collection of brute-force methods that attempt to deduce statistical relationships between structure of unknown key and ciphertext
- Differential and linear cryptanalysis have been used to mount successful attacks
- Only defense is selection of strong cryptosystems, thorough key management, and strict adherence to best practices of cryptography in frequency of changing keys

Dictionary Attacks

- Attacker encrypts every word in a dictionary using same cryptosystem used by target
- Dictionary attacks can be successful when the ciphertext consists of relatively few characters (e.g., usernames, passwords)

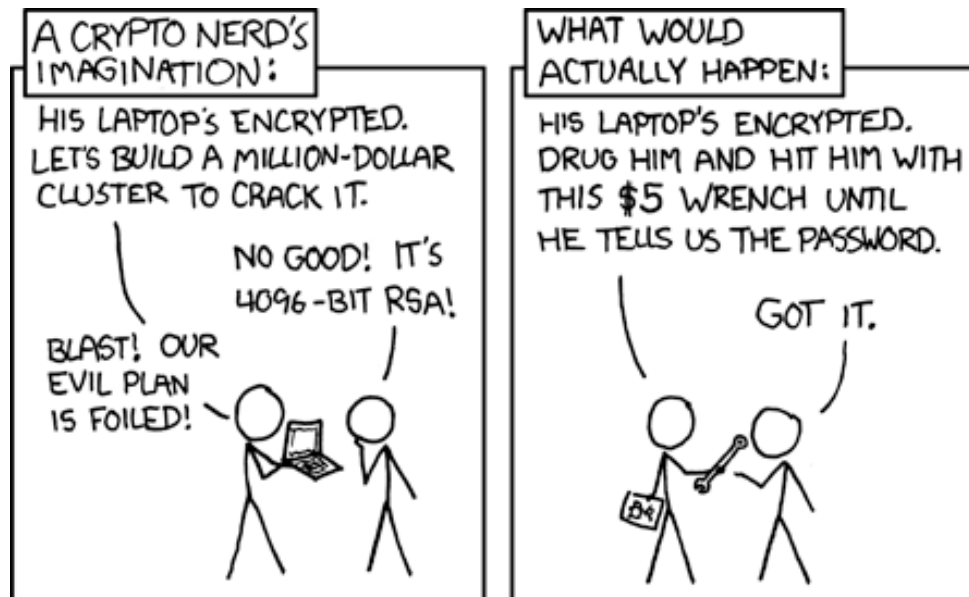
Timing Attacks

- Attacker eavesdrops during victim's session; uses statistical analysis of user's typing patterns and inter-keystroke timings to discern sensitive session information
- Can be used to gain information about encryption key and possibly cryptosystem in use
- Once encryption successfully broken, attacker may launch a replay attack (an attempt to resubmit recording of deciphered authentication to gain entry into secure source)

Defending from crypto Attacks

No matter how sophisticated encryption and cryptosystems have become, if key is discovered, message can be determined

Key management is not so much management of technology but rather management of people



Lanka Education and Research Network

Thank You