MH4311 Cryptography

Lecture 21

Side-Channel Attacks

Wu Hongjun

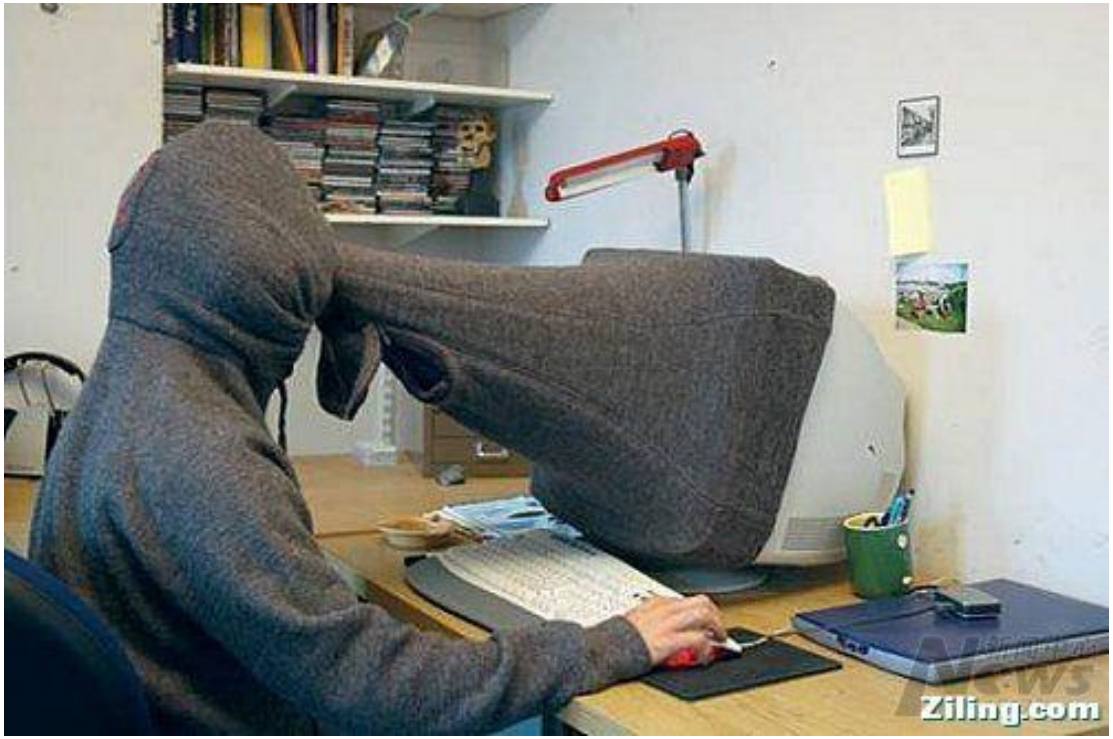
Lecture Outline

- Classical ciphers
- Symmetric key encryption
- Hash function and Message Authentication Code
- Public key encryption
- Digital signature
- Key establishment and management
- Introduction to other cryptographic topics
  - Post-Quantum Cryptography
  - **Side-channel attacks**

Recommended Reading

- Wikipedia
  - http://en.wikipedia.org/wiki/Side_channel_attack

Is it effective to protect your computer screen in this way?



Side-Channel Attacks in History

Side Channel Attack in History

1918

Herbert Yardley, head of the US War Department's cryptanalysis bureau, and his team found that various **electronic devices emanate information**, and that these emanations could be exploited to reconstruct the classified materials.

Side Channel Attack in History

1960 – 1964

British intelligence spied on the French Embassy

The French cipher machine leaks electromagnetic (EM) signal containing the plaintext information

In 1964, French installed metal sheets and copper tubes in cipher room.

Side Channel Attack in History

1962

Cuban missile crisis, NSA (aboard spy ship) spied on Russian communications station in Cuba

NSA to circumvent unbroken Soviet Union cipher

1) capture EM signal emitted from Soviet Union cipher machines
2) noise spikes are also captured, revealing rotor settings on older cipher machines

Side Channel Attack in History

1971

IBM began measuring emanations of all its devices for information-bearing radiation

This project also includes the design of DES

Side Channel Attack in History

Mid-1970s

Polish intelligence intercept power line emanations from military building in Moscow; caught by KGB

Soviet cipher machines replaced with steel enclosures with noise generators (causing interference to televisions as far as 1 mile away) and clean motor generators.

Side Channel Attack in History

1985

Wim Van Eck published paper on
eavesdropping video display of up to 1 km
(the technique is affordable by individuals)

The intelligence may know this technique
in the 1950's.

British government exploits TV display radiation
to enforce TV tax

Side Channel Attack in History

1990

Peter Smulders published paper on eavesdropping EM radiation from cables

More advanced techniques have been used in the cold war

Side Channel Attack in History

The sound of keystrokes of keyboard and ATM pads reveals passwords

Reason: different keys on the keyboard give slightly different sound since they are at different positions on the keyboard

Note: EM signal leaked from keystroke of a computer is more serious …

Side Channel Attack in History

The timing intervals between keystrokes can be used to identify a telegraph operator

=> used in war to trace the movement of enemy troops

This technique was later used in a research paper to authenticate a user of a server:

=> not that reliable, not that secure in practice

Side-Channel Attacks on Cipher Implementation

Side-Channel Attacks on Cipher

- Some side-channel attacks are remote
  - such as the remote timing attack on OpenSSL server
- Most of the side-channel attacks against ciphers are local
  - The attacker accesses the device locally (for example, the attacker uses a smart card, making various measurements), then retrieve the secret key stored in the device
- There are four main types of side-channel attacks against cipher implementation
  - Timing
  - Power
  - Electromagnetic signal
  - Fault

Timing Attack

- Timing attack
  - for a cipher, different inputs may result in slightly different amount of processing time
  - the attack is to retrieve the key by analyzing the difference in processing time
- We have learned the timing attack on modular exponentiation (RSA, DH, DSA) that results in remote timing attack on OpenSSL server.

Timing Attack

- Cache-timing attack is a serious attack on cipher implementation using table lookup and/or conditional code branch
- Memory cache
  - Most of the PC and server CPUs have memory cache
  - Memory cache is implemented on the CPU chip
  - Memory cache is faster than the main memory, but much more expensive than main memory
  - CPU uses memory-cache to store the recently accessed memory data so as to speed up memory access if some memory addresses get accessed for multiple times within a short period

Timing Attack

- Memory cache example
  - Intel i7-8850H Processor, released in Q2 2018
    - It is a processor with 6 cores
    - Level 1 cache (fastest)
      - Each core 32 KB data cache (KB -- KiloBytes)
      - Each core 32 KB instruction cache
    - Level 2 cache: each core 256 KB
    - Level 3 cache: shared, 9MB

Timing Attack

- Cache-timing attack against AES
  - For the fast AES software implementation, Sbox together with MixColumn are precomputed and stored in a table T (or four tables, depending on how to implement the table lookups)
  - When we perform AES encryption, the first table lookup is $T[P_0 \oplus K_0]$, the second table lookup is $T[P_1 \oplus K_1]$, where each P_0, K_0, P_1, K_1 is one byte

Timing Attack

- Cache-timing attack against AES (cont.)
  - Suppose that we want to attack K_0 and K_1
    If $P_0 \oplus K_0 = P_1 \oplus K_1$, after accessing the element $T[P_0 \oplus K_0]$, this data is stored in the memory cache, so it is fast to access $T[P_1 \oplus K_1]$. On average (by randomizing the rest of the plaintext bytes), we get shorter AES encryption time
  - By changing the value of P_1 and measuring the encryption time, we can identify the P_1 satisfying $P_0 \oplus K_0 = P_1 \oplus K_1$. It means that we find the value of $K_0 \oplus K_1$.
  - Similarly, we can recover $K_0 \oplus K_2$, $K_0 \oplus K_3$, $K_0 \oplus K_4$, $K_0 \oplus K_5$ …

Timing Attack

- Countermeasures against timing attack on AES
  - Method 1: Avoid using table lookup in AES implementation (slow for serial modes)
  - Method 2: Implement AES in hardware
    - Starting from 2009, the round function of AES is implemented in hardware in the Intel & AMD CPUs
      - Be accessed using the AES New Instructions (AES-NI)
      - Constant time computation of AES
      - Much faster than software implementation

Power Attacks

- For different inputs, a device consumes different amount of power
  - For example, on the hardware device using CMOS technology (complementary metal–oxide–semiconductor), $1 \oplus 1$, $1 \oplus 0$, $0 \oplus 0$ consumes different amount of energy.
- The power attack is to retrieve the key by analyzing the difference in the power consumption

Power Attacks

- Simple power attack
  - Measuring the power on a single device
- Differential power attack
  - To guess part of the subkey on another identical device. If the guess is correct, part of the power consumptions would be highly correlated.

EM Attacks

- The electrical current in a device emanates EM signal
- EM signal propagation and capture
  - radiation

    use field probes, antennas (wide-band, narrow-band)
  - conduction

    (faint currents on all conductive surface or lines attached to the device)

    use current probes

EM Attacks

- EM attacks on CMOS devices
  - break DES, AES, RSA, COMP128 on smartcards,
  - crypto tokens and TLS/SSL accelerators

Power & EM attacks

- Commercial products are available to apply power & EM attacks against the ciphers in smart cards.

- How to resist the power & EM attacks
  - To introduce extra randomized computations so as to hide the original signals

Fault Attack

- There may be fault during computation
  - natural faults
    - hardware defect
      - Example: In 2014, it was found that the frequent accesses to a DRAM address results in the error in the nearby address (rowhammer attack)
      - Example: voltage spike
    - cosmic ray
      - Studies by IBM in the 1990s suggest that computers typically experience about one cosmic-ray-induced error per 256 megabytes of RAM per month
    - ……

Fault Attack

- There may be fault during computation (cont.)
  - deliberate faults
    - Hardware
      - Introduce faults using laser, X-ray, neutron beam, …
      - Introduce faults by reducing the clock cycle duration so that some computations cannot be finished properly in one clock cycle
      - Introduce faults by increasing the device temperature
      - ….
    - Software: malicious code injection

Fault Attack

- Fault attacks can be successfully launched against many cipher implementations: RSA, DES, AES, …
- Commercial product is now available:
  - Use laser to inject fault into the computation in smart card
    - Recover AES key in smart card quickly

Fault Attack

- How to resist the fault attack
  - Method 1. Use the memory & registers with error correction capability
    - If the errors being introduced exceeds the error correction capability, there is still error
  - Method 2. Compute twice and compare the results
    - Multiple errors may leave the output unchanged. No error in the output with injected faults also leads to successful attack
  - In general, it is difficult to resist the fault attack completely

Summary

Side-channel attacks on cipher implementation:

- Timing attack
  - Cache timing attack on AES
    - Hardware implementation: AES instructions in CPUs (fast)
    - Avoid table lookup in software implementation (slow)
- Power attack
- EM attack
- Fault attack
  - Difficult to resist this type of attack

Cipher should be implemented to resist the above attacks