MAS 433: Cryptography

Lecture 19
Introduction to Other Topics
<u>(not required for exam)</u>

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**
  - Side channel attacks
  - Quantum cryptography
  - Quantum computing

Recommended Reading

- Wikipedia
  - http://en.wikipedia.org/wiki/Side_channel_attack
  - http://en.wikipedia.org/wiki/Quantum_cryptography
  - http://en.wikipedia.org/wiki/Quantum_key_distribution
  - http://en.wikipedia.org/wiki/Quantum_computer

Side Channel Attack: Stories

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: Stories

1960 – 1964

British intelligence spy on the French Embassy

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

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

Side Channel Attack: Stories

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: Stories

1971

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

This project also includes the design of DES

Side Channel Attack: Stories

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.

Cipher machines still vulnerable because of KGB breakthroughs in flooding intercept technology methods that included use of X-rays and radioactive isotopes.

Side Channel Attack: Stories

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 exploits TV radiation to enforce TV tax

Side Channel Attack: Stories

1990

Peter Smulders published paper on eavesdropping EM radiation from cables

More advanced techniques have been used in the cold war

Side Channel Attack: Stories

TEMPEST

The US classified standards for

limiting EM emanation from electronic devices

Original **TEMPEST** in the 1950's,

Being modified significantly and continuously

Partially declassified in the early 1990's

Side Channel Attacks on Cipher Implementations

- Timing
- Power
- Electromagnetic Signal
- Fault

Timing Attack

Timing attack –

 for a cipher, different inputs may result in slightly different amounts of processing time

 the attack is to retrieve the key by analyzing the difference in processing time

Timing Attack on Modular Exponentiation

Timing attack on DH, DSS, RSA (1996)

To compute $z = y^x \bmod n$

$$x = x_{t-1} x_{t-2} \cdots x_2 x_1 x_0$$

The simple algorithm is that

$y = a, z = 1$

for $i = 0$ to $t-1$ do

{

    if $x_i = 1$, then $z = z \cdot y \bmod n$

    $y = y^2 \bmod n$

}

Basic idea of the attack

knowing $x_0 \cdots x_{j-1}$, to determine x_j

1) find some y' so that at step j,

    $z_j \times y'$ is slow to compute;

2) find some y'' so that $z_j \times y''$ is fast

3) input a number of different y', y''

    if average computing time of y'

    larger than that of y'' => $x_j = 1$

    else => $x_j = 0$

Timing Attack on Modular Exponentiation

Remote practical timing attack on OpenSSL (2003)

If the timing variance over the network is less than one millisecond, it is possible to recover the secret key of RSA in OpenSSL with about 1/3 million queries.

Timing Attack on Modular Exponentiation

Defend timing attack on RSA

The simplest way – **RSA blinding**

To compute $z = y^d \bmod n$

we set a different random number r for each y, then

$$z = ((r^e y)^d \bmod n) / r \bmod n$$

so the inputs to RSA are random

Timing Attack on Table Lookup

Basic Idea:

- Memory cache used in modern CPU to speed up memory access
  - Memory cache (Level 1, Level 2, Level 3)
    - http://en.wikipedia.org/wiki/CPU_cache
    - Store the recently accessed data
    - Fast to access
- Timing difference
  - A table element is read directly from memory: slow
  - A table element is read from memory cache: fast
  - This timing difference can be used to detect whether two consecutive table lookups retrieve the same table element
    - If they are retrieving the same table element, the accessing period should be short (after the first table lookup, that table element is already is already in the cache.)
    - Otherwise, the accessing period **may** be longer

Timing Attack on Table Lookup

- Cache-timing attack on AES
  - Table lookup is used in the software implementation of AES
  - Two types of attacks
    - Local cache-timing attack
      - Measuring the encryption time precisely
      - Deliberately introduce cache missing
    - Remote cache-timing attack
      - So far not practical

Timing Attack on Table Lookup

- Countermeasures on timing attack on AES
  - Method 1: Avoid using table lookup in the AES computation (slow)
  - Method 2: Implement AES in hardware
    - Starting from 2009, the round function of AES is implemented in hardware in the Intel & AMD CPUs
      - Constant time computation of AES & very fast

Power Attacks

Power attack

for different inputs, the devices consumes different amounts of power

the attack is to retrieve the key by analyzing the difference in the power consumption

Power Attacks

- Simple power attack
- 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 computation emanates EM signal

EM signal propagation and capture

1) radiation

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

2) conduction

   (faint currents on all conductive surface or lines

   attached to the device)

   use current probes

EM Attacks

EM Attack v.s. Power Attack

many types of EM emanations

=> leak more information

=> EM attack more powerful than power attack

EM Attacks

EM attacks on CMOS

- many chips are CMOS devices
- break DES, RSA, COMP128 on smartcards,

  crypto tokens and SSL accelerators

Resist 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

Fault Attack –

 Error in the CPU, or memory (RAM)

  – **the leakage of the secret key**, or

  – the loss of the control of the process

Fault Attack

How the fault occurs

- natural (hardware defect, cosmic rays, …)
- deliberate
  - hardware: laser, X-ray, neutron beam, …
  - software: malicious code injection

Fault Attack

Fault attacks on RSA, DES, EEPROM, AES …

Commercial product is now available:

- Use laser to introduce fault into the computation in smart card
  - Recover AES key in smart card in a few minutes

How to resist the fault attack

- Method 1. Use the memory & registers with error correction capability
- Method 2. Compute twice and compare the results
- But in general, it is difficult to resist the fault attack

Quantum Key Distribution

- Based on uncertainty principle of quantum mechanics
  - Two parties can share a long secret key, then use one-time pad for encryption/decryption
  - "unconditionally/perfectly" secure if the quantum mechanics theory is perfect
    - eavesdropping can be detected

Quantum Key Distribution

- Two methods
  - BB84
    - Polarization of single photon
    - Simple, easy to implement
  - E91
    - Entanglement of two photons
    - Difficult to implement
      - NUS implemented it
        » One approach: Optical cable in campus
        » Another approach: 1.5 km free space transmission

Quantum Key Distribution

- Misconception on quantum key distribution
  - ~~QKD can be used to replace public key encryption~~
    - There is no signature mechanism in QKD
    - So a secret key should be shared between the sender and receiver for authentication (so as to prevent the man-in-the-middle attack)
      - For public key cryptography, public key certificate is used for authenticating public keys

Quantum Computer

- Based on quantum entanglement & superposition
  - n-qubit register can contain up to 2^n different values
  - An operation performed on such a register is "equivalent" to 2^n operations on classic computer
  - But reading a **specific** value from the quantum register is not as easy as that from classic computer
- Powerful
  - Public key cryptography
    - Large integer can be factorized easily on quantum computer (also discrete log problem can be solved easily)   (Peter Shor, 1994)
    - PKCs based on other hard problems seem secure against quantum computer
  - Symmetric key cryptography
    - Effective key size is reduced by half on quantum computer
  - Hash function
    - A collision can be found with complexity $2^{n/3}$

Quantum Computer

- When a large quantum computer can be built?
  - So far, quantum computer is able to factorize
    $15 = 3 \times 5$

- Misconception on quantum computer
  - ~~Quantum computer can be used to break all the ciphers~~

Summary

Side-channel attacks on cipher implementation:

- Timing attack
  - Timing attack on modular exponentiation
    - Counter measure: blinding to random the input
  - Cache timing attack on AES
    - Hardware implementation: AES instructions in CPUs (fast)
    - Avoid table lookup in software implementation (slow)
- Power attack
- EM attack

> Countermeasure: introduce extra random computations …

- Fault attack
  - Difficult to resist this type of attack

Cipher should be implemented to resist the above attacks

Summary

- Quantum key distribution
  - Two parties can establish a long secret key
  - Pre-shared secret key is needed for authentication (to prevent man-in-the-middle attack)

- Quantum computer
  - RSA, ElGamal, DSA can be easily broken on quantum computer
  - How to built a large quantum computer?