MTAT.07.006 Research Seminar in Cryptography

Seminar 6: Side-Channel Attacks

Aleksei Ivanov
Tartu University
aivanov@math.ut.ee

Overview of the Lecture

- Types of Information Leakage
- Attacks
- Countermeasures

Types of information leakage

- Execution time leakage
- Power consumption leakage
- Electromagnetic radiation leakage
- Error message leakage
- Combining side-channels

Types of attacks

- Passive attacks
  Attacker eavesdrops on some side-channel information, which is analysed afterwords to reveal some secret information

- Active attacks
  Attacker takes active part in the attack: assuming the attacker is able to deviate the device from its normal behaviour, and tries to gain additional information by analysing its reactions

Timing Attacks

- Cryptanalysis of a Simple Modular Exponentiator
- Montgomery Multiplication and the CRT

Simple Modular Exponentiator

- $R = y^x \mod n$
- known values to the attacher y, n, computation time
- x stays the same (unknown to the attacker)
- attacker knows the design of the target system (information can be obtained via observing system behaviour)
- attack can be done passively listening on a channel

Montgomery Multiplication and the CRT

- $\mod n$ makes usually the most difference in time (Montgomey eliminates the operation)
- Chinese Reminder Theorem (CRT) is often used for optimization
- $y \mod p$ and $y \mod q$ are computed first
- if $y < p$ then no operation, else some operations might be done and the time differs

Power Consumption Attacks

- Simple Power Analysis (SPA)
- Differential Power Analysis (DPA)

Simple Power Analysis (SPA)

- power consumed varies on microprocessor instruction being executed
- only visual analysis

Differential Power Analysis (DPA)

- consists of visual, statistical and error-correction statistical analysis (also noise filtering)
- little or no information is needed about the target implementation
- attacker observes n encryption operations and records k power samples and cipher text for each (no plain text is needed).
- it is possible to find DES keys in less than 15 traces for most smart cards

Fault Attacks

- Spike Attacks
- Glitch Attacks
- Optical Attacks
- Differential Fault Analysis(DFA)

Countermeasures

- General data-independent calculations
- Blinding
- Avoiding conditional branching and secret intermediates
- Licensing modified algorithms

Countermeasures against timing attacks

- Adding delays
- Time equalization of multiplication and squaring
- Making every computation take fixed amount of time
- Making every operation constant time
- Making entire transaction fixed-time

Countermeasures against power analysis attacks

- Power consumption balancing
- Reduction of signal size
- Adding noise
- Shielding
- Modification of the algorithms design

Countermeasures against fault attacks

- Running the encryption twice
- Checking the output
- Randomization

Conclusion

- Smart cards are in most danger of side channel attacks
- Servers are easier to protect against side channel attacks
- The subject needs more research