Hochschule **RheinMain**
University of Applied Sciences
Wiesbaden Rüsselsheim

Side-channel attacks in a microkernel environment

Thomas Frase
Thomas.b.Frase@student.hs-rm.de

Fabian Seiberling
Fabian.b.Seiberling@student.hs-rm.de

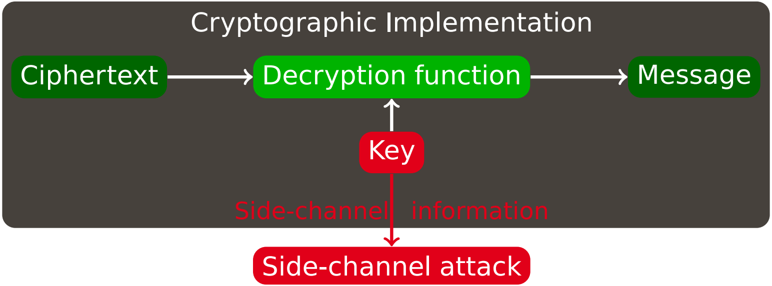
13.02.2014

1st Wiesbaden Workshop on
Advanced Microkernel Operating Systems

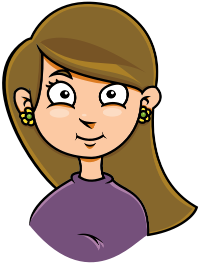
Table of contents

Introduction

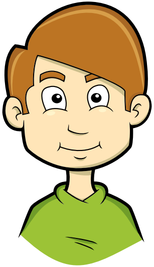
Side-channel attacks use the physical implementation of a cryptographic function to gain information about the key.



Public Key Cryptography



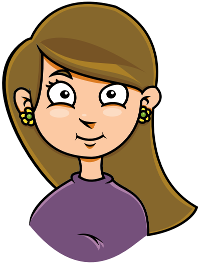
Alice



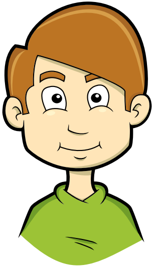
Bob

Generate big primes p and q

Public Key Cryptography



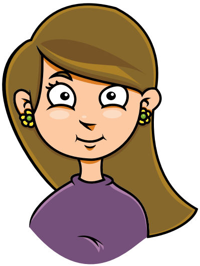
Alice



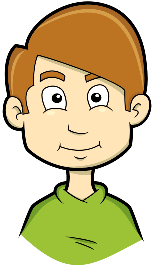
Bob

Calculate $n = p \cdot q$

Public Key Cryptography



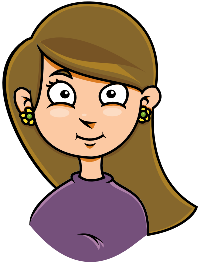
Alice



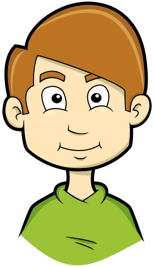
Bob

Find e with $\gcd(e, n) = 1$

Public Key Cryptography



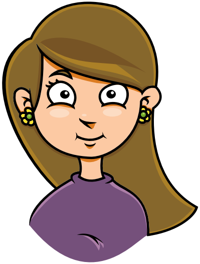
Alice



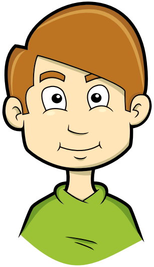
Bob

Find d with
$e \cdot d \equiv 1 \pmod{n}$

Public Key Cryptography



Alice

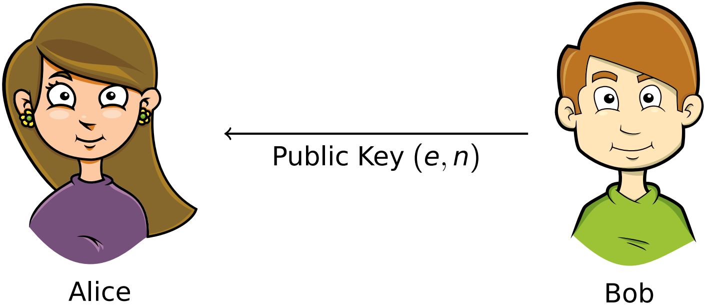


Bob

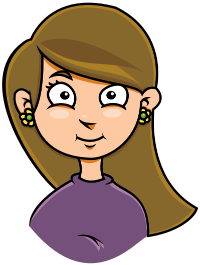
Public key: (e, n)

Private key: (d, n)

Public Key Cryptography



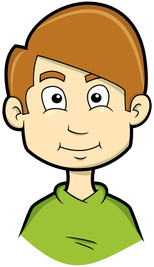
Public Key Cryptography



Alice

Encrypt message:

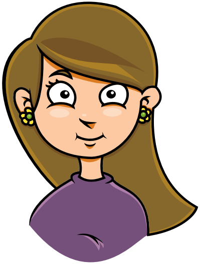
$c = m^e \pmod{n}$



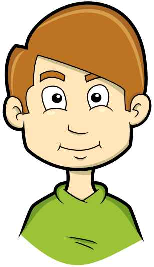
Bob

Public Key Cryptography

Public Key Cryptography



Alice



Bob

Decrypt mes-
sage:

$m = c^d \pmod{n}$

Exponentiation by squaring

Algorithm

Input: c, d, n

Output: m

let $d_1, ..., d_n$ be the bits of d;

let bits(x) be the bit-length of x;

$m \leftarrow 1$;

for $i = bits(d)$ *down to 1* **do**

  $m \leftarrow m^2 \pmod{n}$;

  if d_i = *1* **then**

    $m \leftarrow m \cdot c \pmod{n}$;

  end

end

Side-channel Attacks

Types of side channel attacks:

- Acoustic cryptanalysis
- Data remanence
- Differential fault analysis
- Electromagnetic attacks
- Power monitoring attack
- Timing attack

Side-channel Attacks

Acoustic cryptanalysis

Attacks which use the noise emitted by the computer while using the cryptographic function.

Data remanence

attacks which use to read the data which was used by a cryptographic function. The data can be restored after the cryptographic function delete them.

Side-channel Attacks

Differential fault analysis

This attack create a fault in the cryptographic function to gain information about the current state of the function. A fault can be created with high temperature, to high or low voltage or with electric or magnetic fields.

Electromagnetic attacks

Attacks which use the electromagnetic field to gain information about the secret of the cryptographic function.

Side-channel Attacks

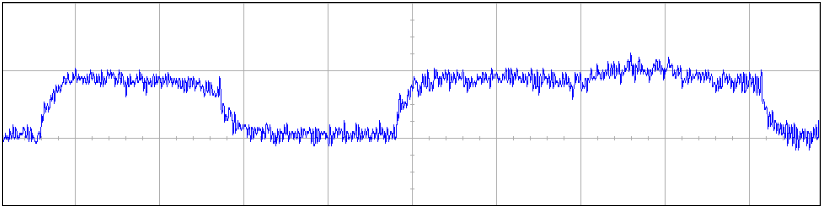
Power monitoring attack

This attack used the characteristic of the power consumption for each instruction of the CPU.

Timing attack

Attacks which measure the execution time of parts of the cryptographic function to gain information.

Example: Power monitoring attack



- Square-and-multiply algorithm
- Different amount of power
- Digital oscilloscope
- Differential power analysis

Acoustic Attack

Genkin, Shamir and Tromer

RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis

- Extraction of full 4096-bit RSA key
- Attack using various microphones
- Uses adaptive chosen-ciphertext
- Target: GnuPG on Laptops

Acoustic Attack

- Electrical components produce high-frequency noise
- Voltage regulator noise depends heavily on CPU instructions / load
- Various CPU instructions distinguishable in acoustic spectrum

Acoustic Attack

- GnuPG uses optimization (RSA-CRT)

$$m_p = c^{d_p} \pmod{p} \quad m_q = c^{d_q} \pmod{q}$$

- Attack targets each bit of q individually
  - Choose c
  - Determine $q_i = 1$ or $q_i = 0$
  - Modify c according to last step
  - Repeat
- Factorize n from q

Acoustic Attack

Consequences for microkernels?

- Attack is independent of operating system
- Mitigation best done on algorithm-level
- Self-eavesdropping can be mitigated by considering the microphone a security critical resource

Access-driven Cross-VM Attack

Yinqian, Juels, Reiter, and Ristenpart

Cross-VM Side Channels and Their Use to Extract Private Keys

- Almost complete extraction of private key
- Required brute-force search of about 10,000 keys
- Target: GnuPG in a Xen-based VM

Access-driven Cross-VM Attack

- Attacker and victim on different guest VMs
- Attacker spies on the instruction cache
- Cache-based delays reveals used code paths in victim

Access-driven Cross-VM Attack

- Preempting the victim
- Noise-reduction
- Classification
  - SVM (Support vector machines)
  - HMM (Hidden Markov model)
  - Fragment stitching

Access-driven Cross-VM Attack

Consequences for microkernels?

- Side-channel resistant algorithms
- Scheduling
  - Make it hard for the attacker to preempt the victim
- Flushing caches
  - Flush instruction cache on context switch for critical tasks

Conclusion

- Side-channel attacks can be used on a microkernel
- Some attacks can be prevented by additional security Implementations on the microkernel
- Some attacks can only prevented by changing the Implementation of the cryptographic function