Side Channels and Covert Channels

Daniel Bosk[1]

Department of Information and Communication Systems (ICS),
Mid Sweden University, Sundsvall.

sidechannels.tex 2068 2014-11-03 10:52:07Z danbos

Overview

1. Side Channels
   - Definition
   - Timing Attacks
   - Acoustic Cryptanalysis
2. Covert Channels
   - Definition
   - Bell-LaPadula
   - Page Faults and LEDs
   - Cheating on the Exam

Overview

1. Side Channels
   - Definition
   - Timing Attacks
   - Acoustic Cryptanalysis
2. Covert Channels
   - Definition
   - Bell-LaPadula
   - Page Faults and LEDs
   - Cheating on the Exam

Mittuniversitetet
MID SWEDEN UNIVERSITY

Definition

Definition (Side Channel)

A *side channel* is an unintended channel emitting information which is due to physical implementation flaws and not theoretical weaknesses or forcing attempts.

Example

Using the standard algorithms for addition and multiplication (using the binary number system) we can easily see that the time to perform 3×25 and 7×25 will be different.

Definition

- Looking at the numbers we have we see that $3_{10} = 11_2$, $7_{10} = 111_2$ and $25_{10} = 11001_2$
- Assume each step in the algorithm takes one time unit.
- Then for 11001×11 we get:
  - 5 time units for multiplying the last 1 in 11 with each digit in 11001,
  - another 5 time units for the next digit in 11,
  - we have an additional 1 time unit for shifting the second result one step,
  - finally, we get 6 time units for adding the numbers.
- For 11001×111 we get:
  - 5 time units for each digit, hence 15 in total,
  - we have two shifts, thus 2 time units more,
  - finally we have 7 time units for adding.

Definition

- Hence, the first multiplication takes 17 time units to perform whereas the second takes 24 time units.
- This is called a timing attack and is one example of why constant-time operations are desirable.
- However, in this example we cannot see the difference between multiplication of $2_{10} = 10_2$ and $3_{10} = 11_2$.
- But in more complex situations this might not even be necessary.

Timing Attacks

- In [SWT01] a timing attack on passwords sent over encrypted SSH sessions was shown.
- As each keystroke in the password is sent in a separate package, the attacker can observe the delay between keystrokes.
- They found that this gave a factor 50 advantage for guessing the password.

Acoustic Cryptanalysis

- In [GST13] the authors showed an attack to extract a 4096-bit RSA private key from a laptop PC (GnuPG implementation of RSA).
- Computers emit high-pitched noice during operation due to some of their electronic components.
- This was used to derive the key used for decryption of some chosen ciphertexts within an hour!
- Their results show that this attack can be accomplished by placing a mobile phone (microphone) next to the target laptop.
- They also show a similar attack is possible by measuring the electric potential of a computer's chassis, e.g. by just touching it.

Acoustic Cryptanalysis

- The acoustic signals are picked up from components in the power supply.
- Individual CPU operations are too fast for a microphone to pick up.
- But long operations such as modular exponentiation (as in RSA) can create a characteristic acoustic spectral signature which can be detected using a microphone.

Overview

1. Side Channels
   - Definition
   - Timing Attacks
   - Acoustic Cryptanalysis
2. Covert Channels
   - Definition
   - Bell-LaPadula
   - Page Faults and LEDs
   - Cheating on the Exam

Mittuniversitetet
MID SWEDEN UNIVERSITY

Definition

Definition (Covert Channel)

A *covert channel* is a mechanism that was not designed for communication but which can nontheless be abused to allow information to flow in a way which is not allowed in the security policy.

Definition (Side Channel)

A *side channel* is an unintended channel emitting information which is due to physical implementation flaws and not theoretical weaknesses or forcing attempts.

Definition

- The definitions do overlap.
- Usually one talks of side-channels in cryptography and covert-channels in larger systems.

Bell-LaPadula

- BLP says "no read up" and "no write down".
- What happens if I try to "write up" but something already exists?
- Using this you can create a covert channel.
- Each denied operation is one bit of information (entropy) revealed by the security mechanisms.

Bell-LaPadula

- The Naval Research Laboratory invented the NRL-Pump.
- This is a device used to limit the bandwidth of possible covert channels.
- The pump allows flow upwards.
- But we need some flow downwards too, e.g. acknowledgement that data was received correctly.
- Bandwidth of possible covert channels are limited using buffers and randomised timing of acknowledgements among other things.

Bell-LaPadula

Example (Logistics system)

- A military warehouse holds classified equipment, but the warehouse itself it not classified.
- A person in the logistics department doesn't have sufficient clearance.
- What happens when this person wants to use the space for other things?
- Make some things up and put in there so it looks occupied.
- What if this person needs some of the items in the cover story?

Page Faults and LEDs

- Another example of how a covert channel might be constructed is page faults.
- What if we manage to place things in memory in such a way that it extends into another page.
- What if that page is not in memory?
- Then we know from either measuring time (we notice if a page-fault occurs) or obsering the disk activity.

Page Faults and LEDs

- Yet another example is the LEDs indicating disk activity.
- If this LED is connected to the serial lines, indicating when data is sent, then information about the data is leaked.
- Further, the electronic components in computer displays leak radio signals caused by the states of pixels etc.
- There has been shown that you can pick up the picture of the screen from these signals two rooms away.

Cheating on the Exam

- Which times someone goes to the toilet: if it is an even minute it's a one, if odd it's a zero.
- The rythm someone clicks their pen against the desk: a change in rythm is a one. However, this needs some synchronisation.
- Drum Morse code on the table.
- . . .

Referenser

[GST13] Daniel Genkin, Adi Shamir, and Eran Tromer. *RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis*. Tech. rep. Cryptology ePrint Archive, Report 2013/857, 2013., 2013. URL: http://eprint.iacr.org/2013/857.

[SWT01] Dawn Xiaodong Song, David Wagner, and Xuqing Tian. "Timing Analysis of Keystrokes and Timing Attacks on SSH." In: *USENIX Security Symposium*. Vol. 2001. 2001.