ECE 443/518 – Computer Cyber Security
Lecture 27 Side-Channel Attacks

Professor Jia Wang
Department of Electrical and Computer Engineering
Illinois Institute of Technology

November 25, 2024

Outline

Reading Assignment

- This lecture: Side-Channel Attacks
- No final exam

Outline

Side-Channel Attacks

Case Studies

Side-Channel Attacks

- Unintended information leakage.
  - Via a channel that exists incidentally.
  - Mostly concerning of confidentiality
- Physical side-channels
  - Electromagnetism
  - Mechanical wave
  - Time

Related Topics

- Covert channel: hidden channel that leaks information intentionally.
  - Can be combined with side-channels to complete a sophisticated attack.
- Attacks on availability using similar mechanisms.
  - EMP attack on electronic devices
  - Acoustic attack on hard drives
- Any attack on integrity?

TEMPEST

- A NSA specification and a NATO certification
  - Information leakage through unintentional radio or electrical signals, sounds, and vibrations.
  - Methods to spy upon others and how to shield equipment against such spying.
- Dated back to 50's, with many details remain classified.
- Three levels of protection requirements.
  - Based on free-space attenuation: 1m, 20m, 100m.

Van Eck Phreaking

- The first public (unclassified) technical analysis on leakage from CRT monitors in 1985 by Wim van Eck.
- Technical details
  - In CRT monitors, images are generated by a moving electron beam with varying strength.
  - The electron beam is driven by an electronic signal of hundreds of volts and a few MHz of bandwidth.
  - The high voltage and high frequency (both baseband and harmonics) will create EM radio.
  - The EM radio can be detected at a distance, and be recovered at low cost ($15 equipment+TV at the time).
- LCDs were demonstrated to have the same security risk.
  - A covert channel based on the same mechanism was also demonstrated recently to leak key stokes.

TEMPEST Protection

- Distance
  - Between equipment and walls
  - Between wires or equipment and building pipes
- Shielding
  - In buildings
  - In equipments
- Filtering
  - On cables to reduce harmonics
  - On screen fonts
- Masking
  - Add noise.
  - Note that many channel coding techniques nowadays reduce the effectiveness of noise-based masking.
- RED/BLACK separation
  - Maintaining distance or installing shielding between wires carrying classified (BLACK) vs. unclassified materials (RED)

Outline

Cold Boot Attack

- A running computer may have the encryption key or related information in the memory (RAM).
- The attacker gaining physical access to the computer can circumvent access control to obtain the content of RAM.
  - Power off the computer.
  - Reboot the computer with a specially made OS/software that reads whatever remaining on RAM.
- Why it works?
  - RAM holds bits in capacitors.
  - Capacitors leak charge and need to be refreshed often to maintain content that can be read out correctly.
  - Cutting power will stop the refreshing mechanism. The content can still be read out – just less reliably as time goes.
  - Freezing the memory sticks shows to be effective to reduce charge leakage and increases chance of successful attack.

Acoustic Cryptanalysis

- Electronic components may emit high-pitched acoustic noise during operation.
  - A nuisance: "coil whine".
  - May convey information about software running, in particular sensitive information.
- RSA key extraction (Genkin et al. 2013)
  - Applicable to GnuPG implementation of RSA decrypting some chosen ciphertexts.
  - With a nearby ($<$1m) smartphone or a more sensitive microphone 4m away.
- A few follow-up works
  - Exploited other physical side-channels including chassis potential (touching laptop by hands) and EM radio.
  - Attacked ECDH and ECDSA.
  - Attacked software other than GnuPG.

The Visual Microphone

- It has long been known that sound causes other objects to vibrate, and a laser to a window may reveal the conversation.
- Passive recovery of sound from video (Davis et al. 2014)
  - Use of high-speed video
  - A few common objects are evaluated, with potato-chip bags and plants seeming to be very effective for sound recovery.
  - Normal video cameras using rolling shutter are also shown to be effective to recover sound without the need of high-speed video.

Summary

- Side-channel attacks exploit unintended information leakage, usually via an incidental physical channel.