Hardware Attacks

Target Course

Computer Design/Hardware

Learning Goals

1. Be able to describe foundational security concepts in securing networks and systems.
2. Be able to describe security design principles and identify security issues associated with common threats and attacks.

IAS Outcomes:

The CS2013 Information Assurance and Security outcomes addressed by this module are:

IAS Knowledge Topic	Outcome
Threats and Attacks	1. Describe likely attacker types against a particular system. [Familiarity] 6. Discuss the concepts of covert channels and other data leakage procedures. [Familiarity] (Elective)
Foundational Concepts in Security	4. Explain the concept of trust and trustworthiness. [Familiarity]
Principles of Secure Design	10. Explain the concept of trusted computing including trusted computing base and attack surface and the principle of minimizing trusted computing base. [Familiarity]

Dependencies

- None.

Summary

This module describes two basic types of hardware attacks with examples to illustrate each type, the types of attackers, some defenses against these attacks, and how these hardware attacks affect the security goals and foundational security concepts.

Estimated Time

30 minutes lecture.

Materials

What are some examples of hardware attacks?

Hardware attacks include invasive and non-invasive attacks.

Non Invasive attacks include covert channels attacks or data leakage attacks and involve closely observing a device's emissions to gain access to unauthorized data. Non-invasive do not harm the device or alter the signals being emitted, thus making them very hard to detect. As the examples below demonstrate non-invasive attacks can be carried out at different proximities to the device. Examples include

- Wiretapping – Given physical access to cables of a network, especially inexpensive coaxial copper cables, which transmit information via electrical impulses, attackers can see all data being transmitted.
    - Defense: Use expensive fiber optic cables which transmit light. While eavesdropping can still be carried out on fiber optics it is more expensive to do so and easier to detect. To fully protect data use data encryption.
- Optimal Emission - A photo-sensor placed in the room with the CRT display can be trained to reconstruct an image from a screen. The sensor can be 50 meters away.
    - Defense: use LCD monitors.
- Acoustic Emissions - Attackers use audio recording of users typing of a keyboard to reconstruct what was typed or recording a computer to reconstruct CPU instructions.

  - Defenses: attack requires training algorithm, thought to be hard to carry out
- Power Emissions - Attack use the fact that different instructions consume different amounts of power. By measuring the power that a device consumes attackers are able to deduce the value of cryptographic keys.
- Timing Emission - Cryptographic operations involve many modular multiplications whose computation time depends strongly on the input values. With suitable analysis, the time taken by a crypto processor to perform such operations leaks the value of its private key.

Invasive attacks involve direct electrical access to the internal components of the device. For example, the attacker might drill a hole into the device and place a probe on a bus line to capture a signal. Cryptographic algorithms, such as RSA and DES, have the property that an attacker who can monitor any bit plane during the computation can recover the key.

Who are possible attackers?

The list is wide and varies depending on the type of device. It could range from technical staff working on a high security machine to individuals looking to reverse engineer pay-TV smartcards- watch tv for free or unlocking a mobile phone to use on any network, to the mafia looking to build and deploy key-stealing terminals from credit cards.

What are some defenses against such attacks?

Protection from non-invasive attacks include preventative methods:

- Emanation *Blockage* - build hardware and devices out of materials that block emanation of various signals. For example, fiber optic cables for networks, screen shields to block visibility and faraday cages to block electromagnetic emanations in the air. For emanation techniques to work the computing devices must be completely enclosed.
- Emanation *Masking:* works by injecting noise (for example, a no-op instruction at random in the instruction stream or inserting bogus instructions in conditional braches). This makes it harder for attackers to analyze the data and pick out patterns.

Protections from invasive attacks:

- High end crypto-processors include tamper-sensing membranes that are designed to zero out data, erase memory or self-destruct on tampering. Although these methods do not prevent attacks, they certainly deter them and provide clear signs if the device has been tampered with. Many products on the market today claim to be tamper resistant, including smartcards used in mobile phones and bank cards, accessory control chips used in games-console memory modules, set –top TV boxes and crypto processors which are embedded within conventional systems to support encryption and store cryptographic keys.

Minimizing the trusted computing base:

- Crypto-processors are dedicated processor or microcomputer that performs a predefined set of cryptographic operations which are embedded within a conventional system. They are usually physically tamper-resistant eliminating the need to protect the rest of the sub-system with physical security measures. Crypto-processors highlight the principal of minimizing the trusted computing base.

How does hardware security relate to security goals and foundational concepts (CIA and AAA)?

A system's `trusted computing base' includes the set of hardware, software and procedural components whose correct functioning ensures that its security policy is enforced. Thus it is important to ensure that the hardware is not breached or compromised. Attackers who gain

close enough proximity to computing devices can tamper with the devices to gain unauthorized access to information. Thus hardware security measures are mainly upholding confidentiality.

Assessment Strategies

1. True or False? Invasive attacks on hardware are harder to detect than non-invasive attacks.
   Answer: False

2. Which of the following can be described as a covert channel attack?

a. An attacker drills a hole into the device and places a probe on the internal bus lines

b. An attacker records the sounds emitting from a keyboard to reconstruct what was typed

c. An attacker inserts in a usb port that fries the devices motherboard.

d. An attacker inserts a covert malware into an email.

e. None of the above.

Answer: b

3. True or False? One type of protection against non-invasive hardware attacks is to inject noisy/random instructions into normal operations.

Answer: True

References:

[1] Wikipedia: Secure Crypto processor. Available at https://en.wikipedia.org/wiki/Secure_cryptoprocessor. Accessed June 2017.

[2] R. Anderson, (2008). *Security Engineering, Second Edition*. Wiley. Chapter 16 available at http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c16.pdf

[3] Cryptographic Processors-a survey *Proceedings of the IEEE*, Vol. 94, No. 2. (2006), pp. 357-369 by R. Anderson, M. Bond, J. Clulow, S.Skorobogatov. Available at https://www.cl.cam.ac.uk/~mkb23/research/Survey.pdf

[4] Lecture Slides of M. Tehranipoor's course Introduction to Hardware Security and Trust. Available at http://www.engr.uconn.edu/~tehrani/teaching/hst/16%20Crypto%20Processors.pdf. Accessed June 2017.

[5] I M.T. Goodrich & R. Tamassia, (2011). *Introduction to Computer Security*. Addison Wesley