ECE 459/559
Secure & Trustworthy Computer Hardware Design

Security & Protection Objectives

Garrett S. Rose
Spring 2017

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Overview

- Definitions
  - What does it mean to be “secure”?
  - Attacks
  - Computer security
  - Adversaries
  - Methods of defense
- Security in embedded systems and design challenges
- The “secret” – roots of cryptography

What Does “Secure” Mean?

- Has to with an asset that has some value – what can be an asset?
- There is no static definition for “secure”
- Depends on what it is that you are protecting the asset from
- Protection may be sophisticated or unsophisticated
- Typically, breach of a security mechanism leads to awareness of shortcoming

Typical Cycle in Securing a System

- Predict potential breaches and vulnerabilities
- Consider possible countermeasures or controls
- Either actively pursue identification of new breach
  OR wait for a breach to happen
- Identify the breach and work out system protection all over

Computer Security

- No matter how sophisticated protection is – simple breaches can break-in
- Computing system – collection of hardware (HW), software (SW), storage, data, and the humans interacting with them
- Computer security (1) – security of SW, data and communication
- Computer security (2) – HW security is important and challenging
  - Manufactured ICs are obscure
  - HW is platform running SW, storage and data
  - Tampering can be conducted at many levels
  - Can be easy to modify because of its physical nature

Definitions

- **Vulnerability** – Weakness in the secure system
- **Threat** – Set of circumstances with potential to cause loss or harm
- **Attack** – Act of exploiting the vulnerability in the system
- Aspects of computer security:
  - **Confidentiality** – related assets only accessed by authorized parties
  - **Integrity** – asset is only modified by authorized parties
  - **Availability** – asset is accessible to authorized parties at appropriate times

Hardware Vulnerabilities

- Physical Attacks
- Hardware Trojans (or Trojan Horses)
- IP Piracy
- IC Piracy & Counterfeiting
- Backdoors
- Tampering
- Reverse Engineering

Adversaries

- Individual, group or governments
  - Pirating IP – illegal use of IP
  - Implementing Trojans
  - Reverse engineering of ICs
  - Spying by exploiting IC vulnerabilities
- System integrators
  - Pirating IP
- Fabrication facilities
  - Pirating IP
  - Pirating ICs
- Counterfeiting parties
  - Recycling, cloning, etc.

Adversaries

- Individual, group or governments
  - Pirating IP – illegal use of IP
  - Implementing Trojans
  - Reverse engineering of ICs
  - Spying by exploiting IC vulnerabilities
- System integrators
  - Pirating IP
- Fabrication facilities
  - Pirating IP
  - Pirating ICs
- Counterfeiting parties
  - Recycling, cloning, etc.

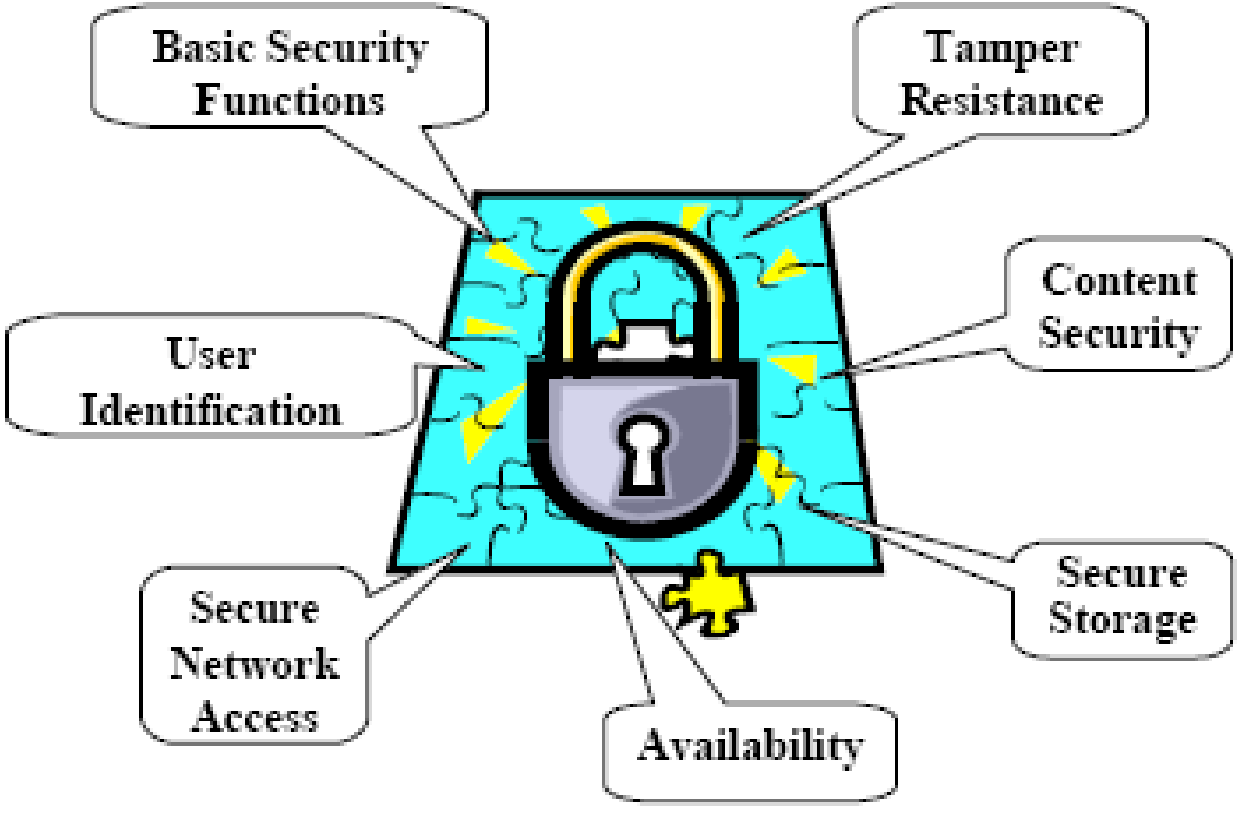
Hardware Controls

- Hardware implementations of encryption
  – Encryption essentially complex “scrambling” to hide information
- Design locks limiting access
- Devices to verify user identities
- Hiding signatures in design files
- Intrusion detection
- Hardware boards limiting memory access
- Tamper resistance
- Policies and procedures
- More …

Embedded System Security

- Security processing adds overhead
  - Performance and power
- Security is challenging in embedded systems
  - Size and power constraints, operation in harsh environments
- Security processing may easily overwhelm other system aspects
- Security has become *new design challenge* that must be considered during design time, along with other metrics (cost, power, area, ...)

Security Requirements



Secure Embedded Systems Design Challenges

- Processing gap
- Battery gap
- Flexibility
  - Multiple security objectives
  - Interoperability in different environments
  - Security processing in different layers
- Tamper resistance
- Assurance gap
- Cost

The Secret

- Underlying most security mechanisms or protocols is the notion of a “secret”

- Lock and key
- Passwords
- Hidden signs and procedures
- Physically hidden

Cryptography – History

- Has been around for over 2000 years
- In 513 B.C., Histiaeus of Miletus, shaved the heads of slaves, tattooed messages on their heads, then let hair grow back – Old school obfuscation!

Cryptography – Pencil & Paper Era

- Caesar's cipher – shift each letter of the alphabet by a fixed amount
  - Easy to break

- Cryptoquote – substitution cipher, permutations of 26 letters
  - Using the dictionary and frequencies, also easy to break

Cryptography – Mechanical Era

- Around 1900, people realized cryptography has mathematical roots
- Germans started a project to create mechanical device to encrypt messages
- **Enigma machine** – thought to be unbreakable
  - Some Polish mathematicians got a working copy
  - Machine later sold to UK, who then hired 10,000 people to break the code
  - They did crack it! German messages were transparent by end of war
  - British kept it secret until last working Enigma!

Cryptography – Mechanical Era

- Another German-invented code was Tunny
- Using pseudorandom number generator, seed produced a key stream ks
- The key stream XOR'd with plaintext p to produce ciphertext c:

$$c = p \text{ XOR } ks$$

- How was this code cracked by British cryptographers at Bletchley Park in Jan. 1942?

Cryptography – Mechanical Era

- Another German-invented code was Tunny
- Using pseudorandom number generator, seed produced a key stream ks
- The key stream XOR'd with plaintext p to produce ciphertext c:

$$c = p \text{ XOR } ks$$

- How was this code cracked by British cryptographers at Bletchley Park in Jan. 1942?
- A lucky coincidence!

Cryptography – Modern Era

- First major theoretical development in crypto after WWII was Shannon's Information Theory
- Shannon introduced the one-time pad and presented theoretical analysis of the code
- The modern era really started around 1970s
- Development was mainly driven by banks and military system requirements
- NIST developed a set of standards for banks
  - DES: Data Encryption Standard