Summary

CSIE 7190 Cryptography and Network Security, Spring 2018

https://ceiba.ntu.edu.tw/1062csie_cns

cns@csie.ntu.edu.tw

Hsu-Chun Hsiao

臺灣大學

National Taiwan University

Course objective revisited

By finishing this course, you should be able to answer the following questions:

- As an online user, how do I protect myself?
- As a developer, how do I design & build a secure system?
- As a researcher, how do I contribute to the field?

How to accomplish these objectives

- Practice **"security mindset"** – thinking like an attacker and thinking about how things can be made to fail
- Learn a variety of attack and defense techniques

What we have learned

Crypto Primitives

- Encryption
- Hash
- Message Authentication Codes
- Signature

Cryptographic Protocols

- Identification
- Key Exchange
- Public Key Infrastructure
- Anonymous Comm.

Network Security

- TCP, DNS, routing
- Transport Layer Security
- Denial of Service
- Internet of Things
- Cryptocurrencies

How to design secure systems?
How to evaluate existing solutions?

Let’s be more systematic and discuss general
security approaches & principles
(warning: not bulletproof theories)

Basic security approaches

Prevention

- Harden protocol itself
- Eliminate attacks at design time

Detection and recovery

- Monitor behavior of participants
- Upon detection of misbehavior: eliminate malicious nodes, restore functionality

Resilience

- Graceful performance degradation in the presence of compromised nodes and hosts

Deterrence

- Provide legal disincentives

Security principles

Simplicity

Open Design

Compartmentalization

Minimum Exposure

Least Privilege

Minimum Trust & Maximum Trustworthiness

Secure, Fail-Safe Defaults

Complete Mediation

No Single Point of Failure

Traceability

Generating Secrets

Usability

Saltzer, Jerome H., and Michael D. Schroeder. "The protection of information in computer systems." Proceedings of the IEEE 63.9 (1975): 1278-1308.

Basin, David, Patrick Schaller, and Michael Schläpfer. Applied Information Security: A Hands-on Approach. Springer Science & Business Media, 2011.

Simplicity (簡單化)

KISS Principle: Keep It Small and Simple

- http://en.wikipedia.org/wiki/KISS_principle

Simpler systems are less likely to contain flaws.

Simpler systems are easier to analyze and review.

Open Design (公開設計)

Kerckhoffs’s principle

- “A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.”

Secrets are hard to protect and thus should be minimized.

Open design allows systems to be examined by many people.

Compartmentalization (權限劃分)

Organize resources into isolated groups with limited and controlled exchange

Examples:

- Separation of data and code
- Levels of classified information

Compartmentalization facilitates simplification, enables isolation of attacks, and makes it easier to concentrate the protection of security-sensitive functionalities.

Minimum Exposure (最小化暴露)

Minimize the attack surface a system presents to the adversary

Examples:

- Turning off Bluetooth when it’s not used
- Disabling web directory listing
- Limitation of password attempts
- Session timeout

Least Privilege (最小權限)

Any component (and user) of a system should operate using the least set of privileges necessary to complete its job

Examples

- Students can access files and network on public computers but cannot install software.
- Firewalls restrict access to ports 80 and 443 only.

Minimum Trust and Maximum Trustworthiness

A **trusted** system is one “whose failure can break the security policy”

- Trust is an assumption and should be avoid if possible

A **trustworthy** system is one “that will not fail”

- System proved to always behave in expected ways

Examples:

- Defensive programming
- Input validation

Secure, Fail-Safe Defaults (失效也安全)

The system should start in and return to a secure state in the event of a failure.

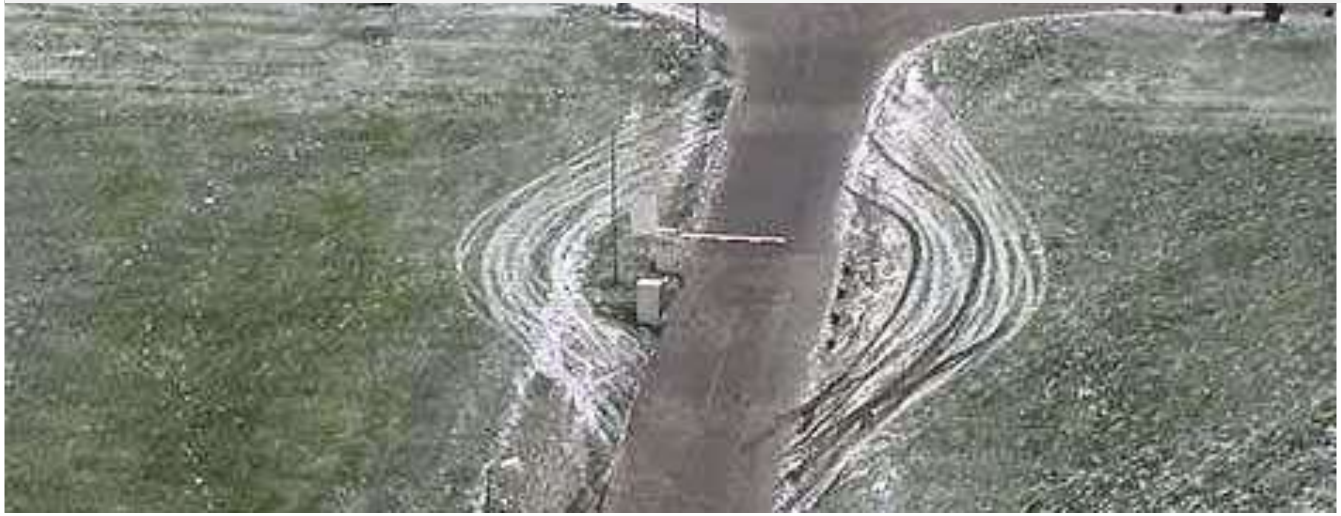
Examples

- Most firewalls take a whitelist approach and deny access to any packet by default.
- Sometimes security and safety are in conflict: in case of fire, it’s secure to lock down a bank vault, but it’s safe for people to leave it unlock.

Complete Mediation (完全仲裁)

Access to any object must be monitored and controlled

Example when complete mediation fails:

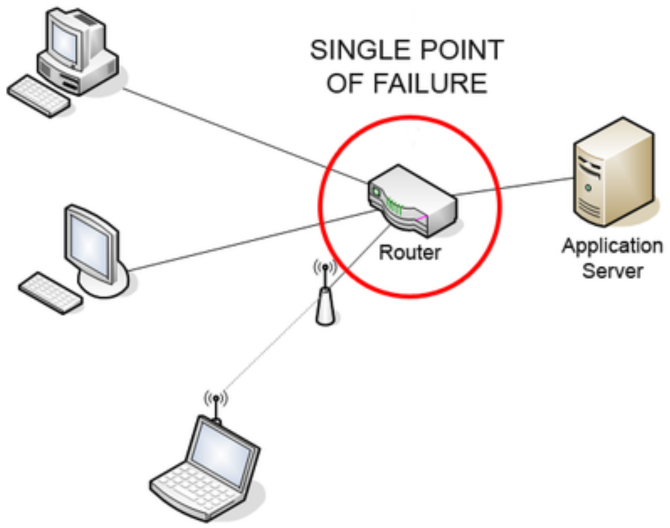


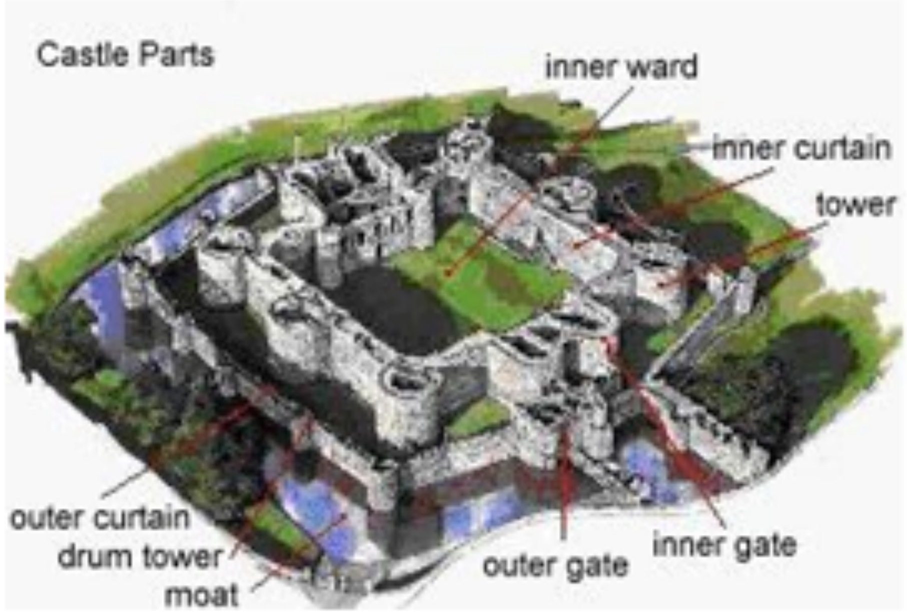
No Single Point of Failure (避免單點失效)

Build redundant security mechanisms whenever feasible

A.k.a. Defense in Depth

Examples: two-factor authentication





Traceability (可追溯性)

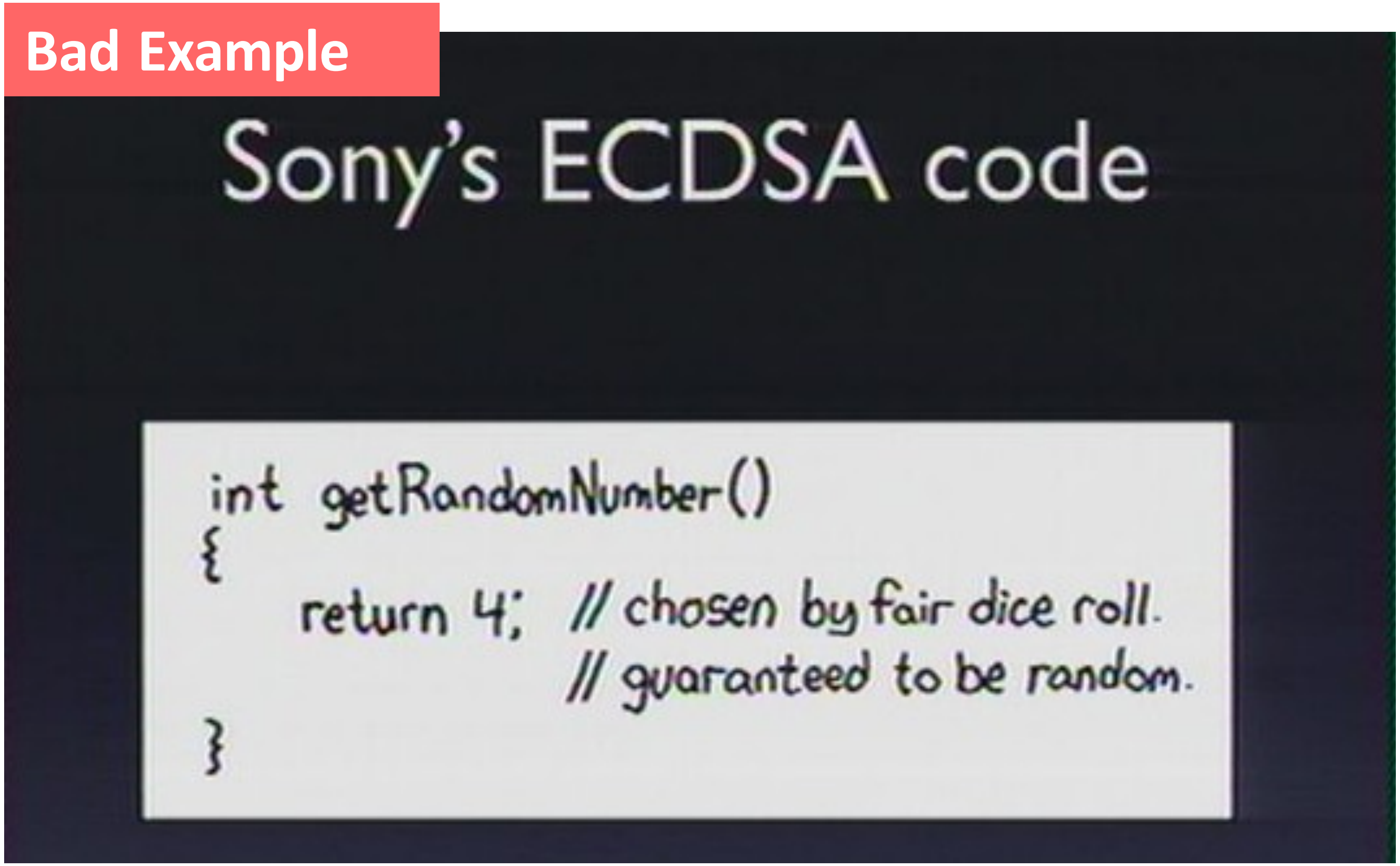
Log security-relevant system events

Logs are useful for attack detection and analysis Logs need to be secured as well.

Generating Secrets

Maximize the entropy of secrets

Bad Example



Sony's ECDSA code

```
int getRandomNumber()
{
        return 4;  // chosen by fair dice roll.
                   // guaranteed to be random.
}
```

Usability (好用性)

Design usable security mechanisms

A security mechanism with bad design is likely be used incorrectly or bypassed.

Moving Forward

Other areas in security (that we didn’t have time to cover)

Wireless security

Secure DNS

Firewall, IDS, IPS

Malware, virus

Cloud security

Mobile security

Usable security

OS security

Protocol verification

Monitoring algorithms

Physical security

Trusted computing

Side-channel attacks

PRNG

AI security

…

When security meets other disciplines

Computer science

- Machine learning
- Pattern recognition
- Game theory
- Algorithms

Economics

- Underground markets
- Models and analysis of online crime (e.g., botnets, phishing, and spam)
- The economics of privacy

Psychology

- Cognitive psychology
- The human side of security
- Deception

Law and social science

- Net neutrality
- Right to be forgotten
- How to fight against online crime
- Privacy
- Freedom of speech vs. censorship
- Cyber surveillance

期末教學意見調查

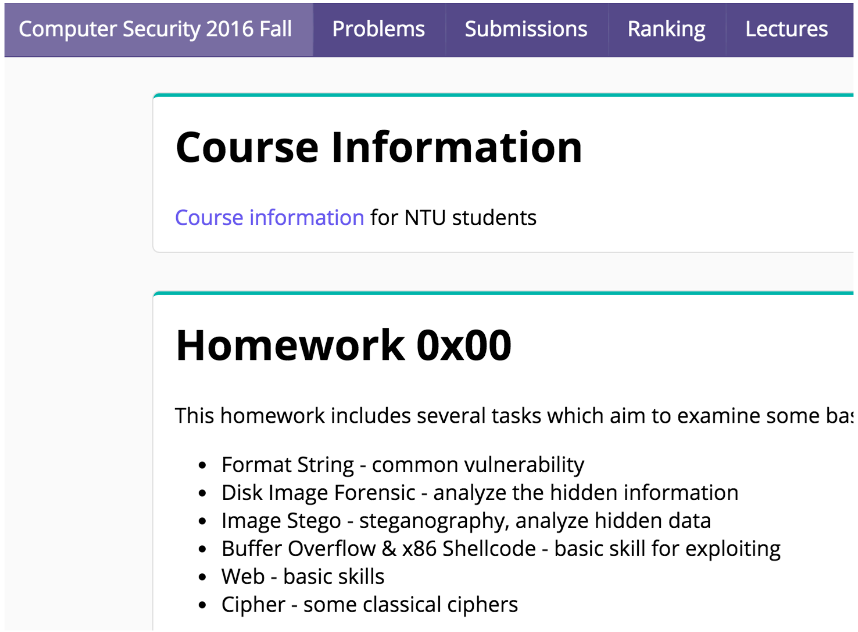
Help us improve this course ☺

[工商服務時間] 計算機安全課程

Fall 2015 台大+台科

Fall 2016 台大+台科大+交大

Fall 2017 台大+台科大+交大+中央



Course Information

Course information for NTU students

Homework 0x00

This homework includes several tasks which aim to examine some ba:

- Format String - common vulnerability
- Disk Image Forensic - analyze the hidden information
- Image Stego - steganography, analyze hidden data
- Buffer Overflow & x86 Shellcode - basic skill for exploiting
- Web - basic skills
- Cipher - some classical ciphers

Course Summary

Cryptography transfers (and hopefully reduces) trust base; other non-crypto security mechanisms are still required.

Central point: Security mechanisms depend heavily on domain.

Course goal: focus on fundamentals

- Establishing trust & cryptographic keys
- Achieve secrecy, authenticity, availability
- Consider deployment incentives
- Be aware of assumptions!