CS5285
Information Security for eCommerce

Prof. Gerhard Hancke

CS Department
City University of Hong Kong

Teaching Team

- Instructor:
  - Prof. Gerhard HANCKE
  - Email: gp.hancke@cityu-dg.edu.cn
  - Questions: Contact me
- Teaching Assistants:
  - BOSHOFF Dutliff(dboshoff2-c@my.cityu.edu.hk)
  - LI Yiyu (yiyuli2-c@my.cityu.edu.hk)
  - NKROW Raphael (renkrow2-c@my.cityu.edu.hk)
  - ZHANG Zhifu (zhifzhang3-c@my.cityu.edu.hk)

Teaching Materials

- Weekly lecture slides
  - Will be on Canvas few days before class.
  - After lecture will also put slides with additional comments
- Textbook:
  - William Stallings, *Cryptography and Network Security – Principles and Practices (any edition 3 – 8)*
    - *Additional reading and reference – core work in slides.*
- You have to check Canvas!
  - Announcements (these go to CityU email)!
  - Problem sets, tutorial solutions, etc.

Weekly Teaching Pattern

- Lecture (2 hours) 14:00-15:50
  - Traditional Lecture
  - Discussion on set reading/case studies
- Tutorial (1 hour) 16:00-16:50 (AC5 416) or 17:00-17:50 (AC5 417)
  - Theory course – we do problems/exercises on paper
  - Weekly question sheet
    - On Canvas (do not need to submit your answers)
  - Discussion
    - Open discussion 16:00-16:30/17:00-17:30
    - Discussion on tutorial solutions starts approximately 16:30/17:30
- ‘Homework’
  - Short extra reading, usually on real-world events/systems with one or two questions.
  - Optional exercises…if you submit you get the answer
- Recording of Lecture and Tutorial session will be made available.

Assessment

- **40% course work**:
  - 2 take home problem sets (10% each)
    - Due in week 6 and week 13 (15 October, 3 December)
    - Late submissions get **zero** mark
  - 1 midterm-quiz (20%)
    - Midterm-quiz in week 7 (22 October)
- **60% final examination**
  - Must achieve minimum 30% mark in final examination

Plagiarism not tolerated!

Do not copy any source without proper citation/referencing.

ChatGPT

- Students are not allowed to use GenAI for any programming tasks, *or to solve any numerical/logic problems*.
- For writing assignments and reports, students are allowed to use GenAI, but its use must be acknowledged through proper citation and referencing.

Course Overview

Intended Learning Outcomes

Upon completion of the course, students should be able to:

1. Identify the organizational requirements of eCommerce systems on data protection.
2. Demonstrate knowledge of the factors which have impacts upon the security of eCommerce systems.
3. Make critique and assessment on the security of eCommerce systems.
4. Describe relevant regulations governing electronic transactions, data privacy protection, and web access.
5. Create design and analyze security mechanisms to protect eCommerce systems and transactions.

Understand the goal of the course

- This is a MSc module
  - This course does not require a background in security
  - Potentially lots of different student backgrounds here
  - This serves as an introductory course on information security
    - Mostly studying foundation cryptography and security protocols
    - The real-world relevance of basic principles are illustrated using e-commerce examples
- So course satisfaction is also your responsibility!
  - If you know everything come talk to me
    - We can do more – extra reading or personal discussion
  - If you think it is all too much talk to me
    - Unfortunately we cannot do less – but I can help you more
  - Any problem with course– talk to/email me! I am friendly!

Tentative Course Overview

- Week 1: Admin and Basic Security Terminology
- Week 2: Symmetric encryption
- Week 3: No class
- Week 4: Symmetric encryption
- Week 4: Number Theory/Asymmetric Encryption (29 Sept)
- Week 5: Integrity
- Week 6: Authentication (Problem Set 1)
- Week 7: Mid-Term Quiz
- Week 8: Key Management
- Week 9: Key Management
- Week 10: Computer Security
- Week 11: Network Security
- Week 12: Network Security
- Week 13: Revision (Problem Set 2)

Lecture 1

Introductory Security Concepts

Today's Lecture

- Information security
  - Basic concepts and terminology
- Where to find security protocols/algorithms?
  - Brief discussion of standards
- CILO1, CILO2 and CILO3

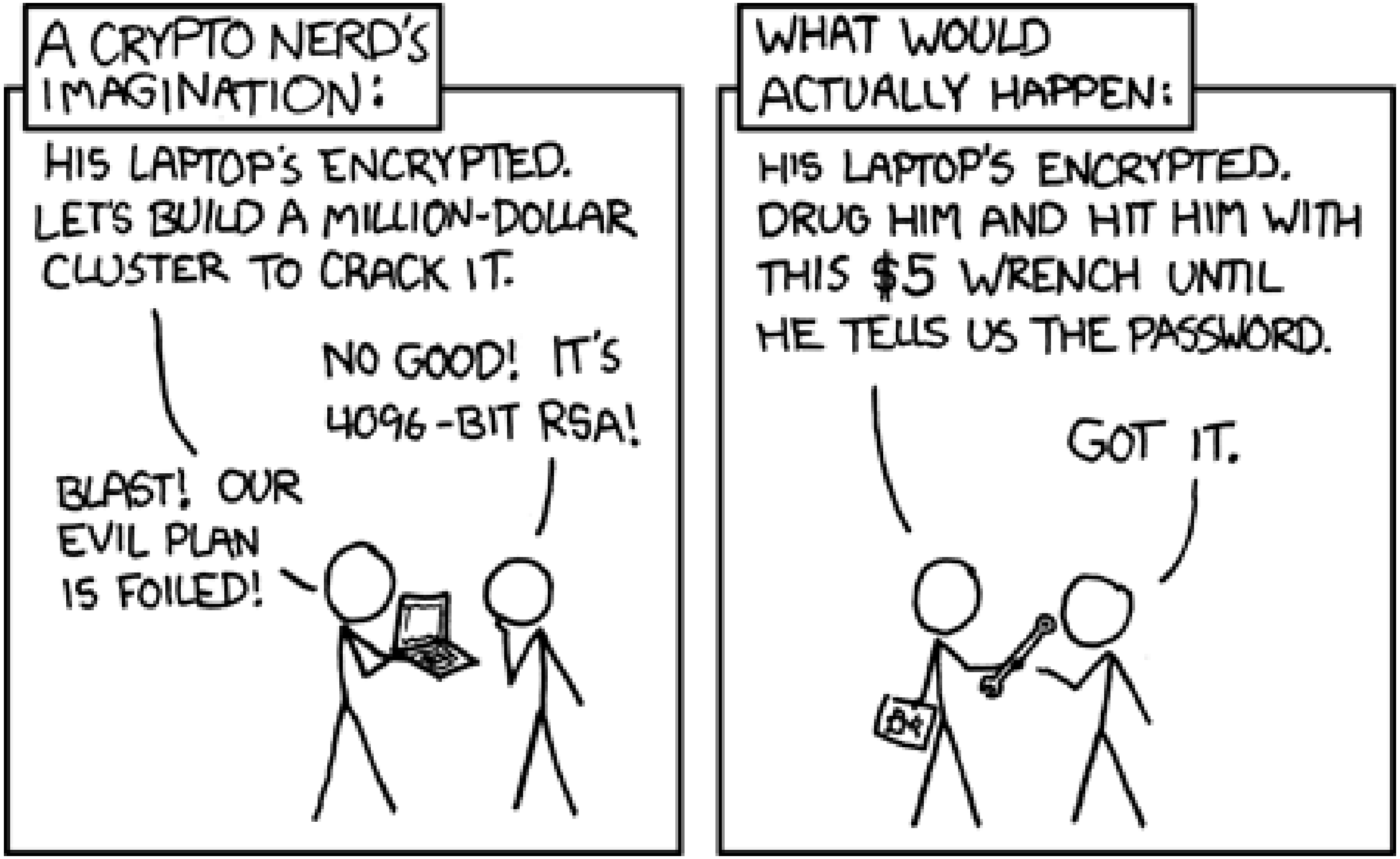
  (Security requirements and threats that impact systems, and basic standards for design)

What is a ‘security’?

- The security of a system, application, or protocol is always relative to
  - A set of desired properties: what do want to achieve?
  - An adversary with specific capabilities: what can they do?

- Why is this important?
  - Is good security not always secure?
  - We need to think: Appropriate? Strength? Cost?
  - Unconditionally vs computationally secure?

Can we make everything 'secure'?


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Information Security

- Security is about the protection of assets.
- Thus, **information security** is the basis for protecting our **information assets**.
- There are three broad classes of protection measures:
  - **Prevention**: prevent your assets from being damaged.
  - **Detection**: detect when you assets have been damaged, by whom and how.
  - **Reaction/Recovery**: recover your assets, or recover from the damage to your assets.

Basic Security Goals

- How can our information assets be compromised?
- The most frequently used definition covers three aspects of information protection:
  - **Confidentiality**: prevention of unauthorised disclosure of information.
  - **Integrity**: prevention of unauthorised modification of information.
  - **Availability**: prevention of unauthorised withholding of information or resources.
- Commonly abbreviated to: **CIA**.

Threats

- Security is only desirable when there is a need to protect a system from a threat.

- A **security threat** is a possible means by which a security policy may be breached (e.g. loss of integrity or confidentiality).
- **Countermeasures** are controls to protect against threats.
- **Vulnerabilities** are weaknesses in the system (and/or countermeasures).
- An ***attack*** is a realisation of a threat (exploiting a vulnerability).

Threats

- Threats can be classified as:
  - **deliberate** (e.g. hacker penetration);
  - **accidental** (e.g. a sensitive file being sent to the wrong address).
- The associated threats which CIA are responsible for countering are:
  - **Exposure of data**: the threat that someone who is unauthorised can access the data.
  - **Tampering with data**: the threat that the data could be altered from what it should be.
  - **Denial of service**: the threat that the data or service is unavailable when it is required.

Adversaries

- People whose aim it is to circumvent your security are generally called **adversaries**.
  - Sometimes called **intruders**, but not all adversaries are external to the system (insider threats).
- Adversaries act in two different ways:
  - **Passive** adversaries only attempt to get unauthorised access to information
  - **Active** adversaries take more direct action:
    - Unauthorised alteration
    - Unauthorised deletion
    - Unauthorised transmission
    - Falsification of origin of information
    - Unauthorised prevention of access to information

Adversaries

- When designing a system, it is important to consider the background and capability of your potential adversary.
- Here are some common categories of adversary in the literature:
  - Casual prying by nontechnical users
    - Bored people…
  - Snooping by insiders
    - Bored people with access to your system…
  - Determined attempts to make money
    - Criminals, organised crime
  - Commercial or military espionage
    - ‘Advanced Persistent Threats’
  - Hacktivists?
    - Unpredictable motivation and skill…

Security Services and Mechanisms

- A security threat is a possible means by which your security goals may be breached (e.g. loss of integrity or confidentiality).
- A security **service** is a measure which can be put in place to address a threat (e.g. provision of confidentiality).
- A security **mechanism** is a means to provide a service (e.g. encryption, digital signature).

Data Confidentiality and Integrity

- Protection against unauthorised disclosure of information.
- Integrity is protection against unauthorised modification of data

- Think back: What is ‘protection’ in each case?
  – Prevent, Detect, Recover?

Authentication

- **Entity authentication** provides checking of a claimed identity at a point in time.
  - Typically used at start of a connection.
  - Addresses masquerade and replay threats.
- **Origin authentication** provides verification of source of data.
  - Does not protect against replay or delay.
  - More examples later in the course…

Access Control

- Provides protection against unauthorised use of resource, including:
  - use of a communications resource,
  - reading, writing or deletion of an information resource,
  - execution of a processing resource.

Non-repudiation

- Protects against a sender of data denying that data was sent (**non-repudiation of origin**).
- Protects against a receiver of data denying that data was received (**non-repudiation of delivery**).
- Example: analogous to signing a letter and sending via recorded delivery.

Think back to Threats…

- Examples of Services (threats)
  - Confidentiality (data disclosure)
  - Integrity (data alteration)
  - Availability (DoS)
  - Entity Authentication (masquerade)
  - Origin Authentication (forgery)
  - Non-repudiation (repudation – it did not happen!)
  - Access Control (illegitimate access)

Mechanisms

- A *security mechanism* is a means to provide a service .
- Can be divided into two classes:
  - *Specific security mechanisms*, used to provide specific security services, e.g. digital signature
  - *Pervasive security mechanisms*, not specific to particular services, e.g. event detection, labelling.

Mechanisms

- Examples of Services/Mechanisms
  - Confidentiality (encryption)
  - Integrity (MAC/digital signature)
  - Availability (redundancy)
  - Entity Authentication (authentication protocol)
  - Origin Authentication(MAC/digital signature)
  - Non-repudation (digital signature)
  - Access Control (Access control model)

Algorithms

- Algorithms are used to build mechanisms
- Example of mechanisms/algorithms:
  - Encryption: DES/3DES/AES (modes) or RSA/ECC
    - CAST(Canada), MISTY1/Camellia (Japan), SEED (Korea)
  - MAC: CBC mode, HMAC
  - Digital Signature: RSA, DSA, ECC
  - Hash: SHA-3
  - Random number: True or Pseudorandom

Where to we find security countermeasures?

Standards

What is a standard?

A “document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidance or characteristics of activities and their results, aimed at the achievement of the optimum degree of order in a given context.”

ISO/IEC Guide 2: 1996

Why standards?

“Standards are essential to trade in increasingly competitive markets. They ensure any business offering products, services or processes is:

- cost-effective and time efficient
- commercially viable
- credible
- safe.”

How to use standards?

- Three common ways to use a standard.
- Certification is when a neutral third-party attests to a claim of compliance.
- Compliance may be declared without recourse to third-party certification.
- Use as the basis for new design (use the parts you need)
- Most security standards do not really “require” certification.

Why not standards?

- The use of standards does have problems:
  - Consensus decisions imply compromise.
  - Documents can be inconsistently implemented.
  - Commercial pressure can lead to partial implementation.
  - Aggressive market strategies by companies who adapt or extend standards can undermine their usefulness.

International standards

- Main international standards bodies relevant to Information Security are:
  - International Organization for Standardization (ISO),
  - International Electrotechnical Commission (IEC),
  - International Telecommunications Union (ITU).

North American standards

- Some US standards bodes have assumed international importance:
  - IEEE (a professional engineering body),
  - NIST (a US federal standards body),
  - ANSI (the US member body of ISO).

Internet standards

- The Internet is a loose collaboration between government, industry and academia.
- Internet standards are produced by the *Internet Engineering Task Force (IETF)*.
- Are there problems uniquely associated with Internet Standards?

Company standards

- Companies themselves also sometimes issue *de facto* standards for techniques that have been patented. These include:
  - PKCS (Public-Key Cryptography Standards, published by RSA Labs.)
  - SECG (Standards for Efficient Cryptography Group, a large group including Certicom, VeriSign and NIST).
  - PCI (Payment Card Industry) Data Security Standards

The end!

?

Any questions…