CS915/CS435 Advanced Computer Security - Introduction

Khalil Challita

Admin Stuff

- Module leader
  - Khalil Challita
  - Office: MB 3.20
  - Email: Khalil.Challita@warwick.ac.uk
- Teaching assistants
  - Mohammad Nourbakhsh <Mohammad-Sadegh.Nourbakhsh@warwick.ac.uk>
  - Jiaqi Lv <Jiaqi.Lv@warwick.ac.uk>

Module overview

- Three lectures per week (Thursday, Friday)
- Lab sessions
  - Available when the lecture content is covered
  - You can do each session at home or in DCS lab at your own time
  - Six lab sessions to be done in four weeks: Week 4 to 7
- Coursework: six post-lab assignments
  - Deadline:
    - Week 10
    - Monday, **2 December 2024** at 12:00 noon, via Tabula.
    - Submit only **1 coursework**, consisting of 6 Sections/Parts.
- Assessment: 70% exam, 30% coursework

Module content

Web security

Hardware security

Network security

Software security

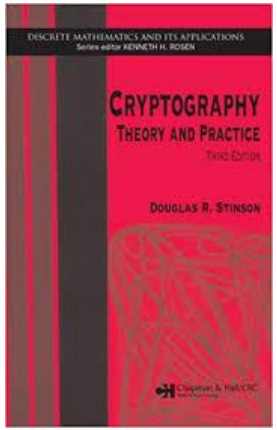
Emerging topics

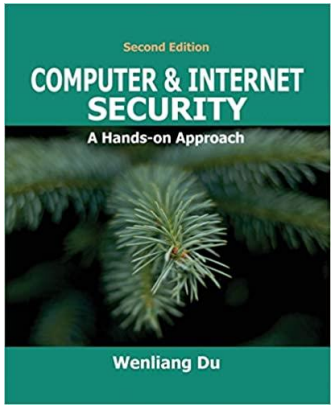
System security

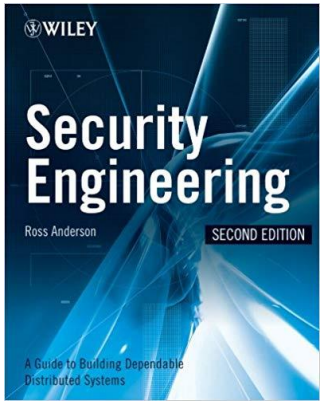
Cryptography

Textbooks

- We don’t use a single textbook, but the following books are useful to read.
- Exam will be based on content covered in the lectures.
- Additional materials will be posted on the module webpage.







Overview of lectures

- Introduction
- Users and security - strength and weakness of users
- Cryptography (Part 1) - symmetric and asymmetric crypto primitives
- System security (Part 2) - software, web, network security
- Hardware security - HSM, smart card, API
- Emerging topics - BitCoin

Today’s lecture

- Define computer security as well as basic computer security terms
- Introduce the C-I-A Triad
- Threats, vulnerabilities, and attacks
- Basics of security engineering

What is computer security

- Computer security is the protection of the items you value, called **assets**
  - Hardware
  - Software
  - Data

- Which of the above is the most valuable asset?

Assets

Hardware:

- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:

- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)
- Individual applications

Data:

- Documents
- Photos
- Music, videos
- Email
- Class projects

Values of assets

Off the shelf;
easily replaceable

Hardware:
- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:
- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)

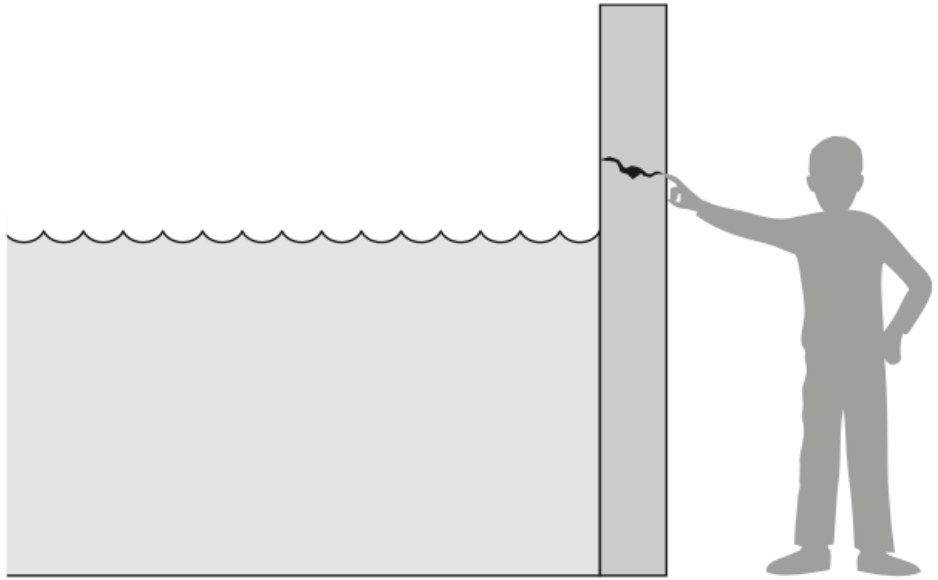
Data:
- Documents
- Photos
- Music, videos
- Email
- Class projects

- Individual applications

Unique; irreplaceable

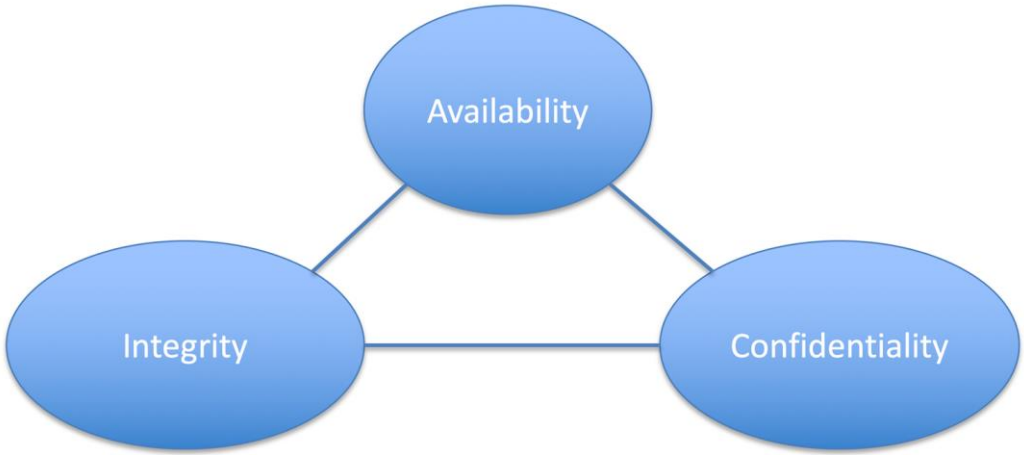
Basic terms

- A **vulnerability** is a weakness in the system that could be exploited to cause harm.
- A **threat** is a set of circumstances that has the potential to cause loss or harm.
- We use **control** or **countermeasure** to prevent threats from exercising vulnerabilities.



Basic goals in computer security

- Three fundamental aspects: availability, integrity and confidentiality.
- Known as the CIA triad.



Availability

- Availability: authorized users should not be prevented from accessing information and assets when required.
- System availability can be affected by device or software failure, but malicious Denial of Service (DoS) attacks are often more effective and devastating.

Integrity

- Integrity: detection of unauthorized modification of information.
- Bank A pays £1,000 to bank B over Internet, what if someone in the middle changes it to £1,000,000.
- The integrity of transaction data is the basis of confidence, and sometime matters more than secrecy.
- For example, the integrity of the e-voting result

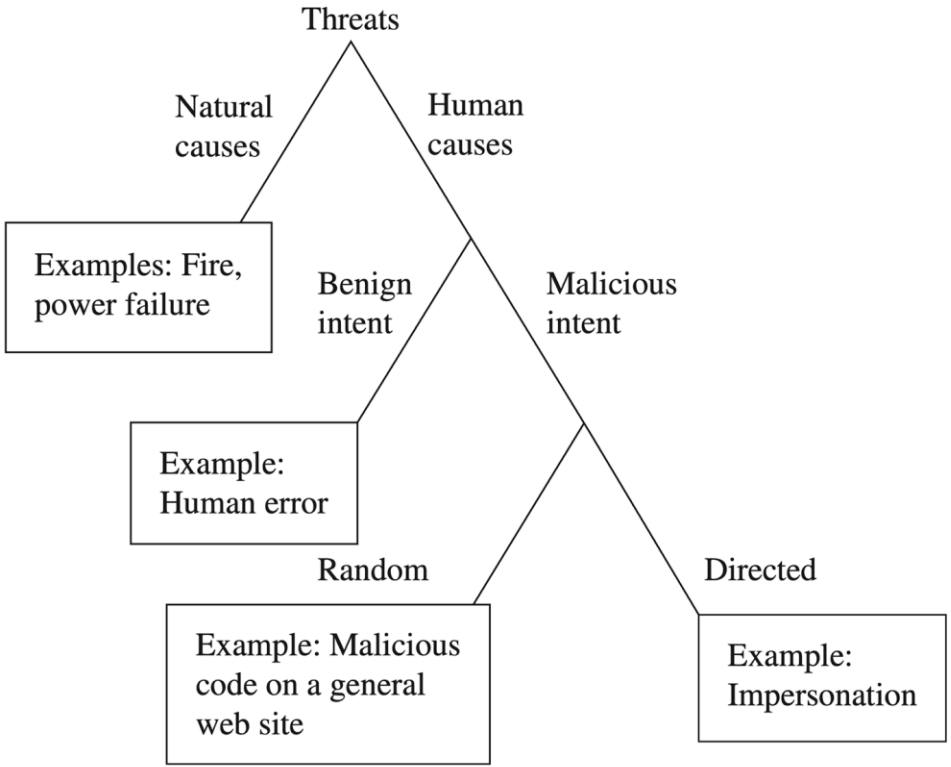
Confidentiality

- Confidentiality: prevention of unauthorized disclosure of information, i.e., info is accessible only to authorized users
- It is usually provided by encrypting data.
- However, there are many threats to confidentiality: shoulder surfing, electronic magnetic emanation (example of a side channel attack), acoustic side-channel, social engineering.

Other security requirements

- Authentication
  - Something you know: password
  - Something you have: token
  - Something what you are: biometrics
- Non-repudiation
  - Usually in the context of digital signature
  - But the real meaning is often disputed

Types of threats



What is security engineering?

- Security engineering is about building systems to remain dependable in the face of **malice**, **error** or **mischance**.
- A cross-disciplinary subject: cryptography, hardware tamper-resistance, formal methods, applied psychology, security economics etc.
- Wide range of applications: nuclear access control, cash machine security, medical records privacy, electronic voting integrity.

The weakest link property

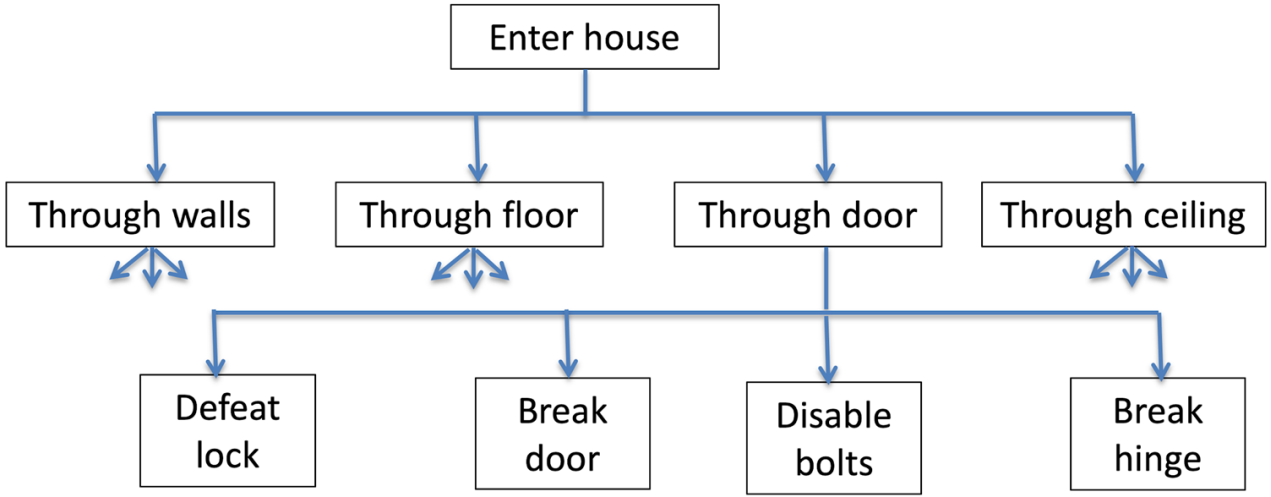
“A security system is only as strong as its weakest link”

- Bruce Schneier

- This is one of the main reasons why security systems are so hard to get right.
- We must assume our opponent is smart, extremely patient, wealthy and creative.
- Building a castle is all hard work, but it takes only one (weakest) entry to break it.

Example: build a secure house

- Given infinite money, build a house that even FBI can’t break in.
- First, we need to identify potential threats.
- We can then organize the threats to **an attack tree**.



Isn’t that easy?

- Assume you have spend 10 million pounds to build a super-secure house – job done!
- But …
  - After one movie night-out, you come back home and find you have lost your key.
  - How do you get back to the house without sleeping on the street?
- The challenge in security engineering is to deal with changing environment and requirements.
- You need to switch roles between defender and attacker.

Security is quite different from other disciplines

- The difference is in the adversarial setting
- Most engineers have to deal with problems like storms, heat, wear and tear.
- They are fairly predictable to an experienced engineer.
- Security engineering has to deal with a totally unpredictable enemy
  - He doesn’t play by the rules
  - He is extremely smart, creative and patient.
  - He has loads of money
  - He has no moral standards

An example

- Tacoma Narrows suspension bridge
- Finished in July 1940
- Collapsed in Nov 1940
  - http://www.youtube.com/watch?v=j-zczJXSxnw
- Caused by resonance of wind
- Valuable lesson to bridge engineers
- Thicker deck, wind tunnel test etc
- In security engineering, we have to consider “malicious” wind, which can behave in unpredictable and surprising ways

Challenges for security engineers

- Security versus efficiency
  - Security engineer treats security as top priority
  - Optimizing efficiency is important, but comes second
  - Many failures are caused by over-optimization
- Security versus usability
  - Security engineer must always consider usability
  - An unusable system can’t be secure.
- Security versus features
  - Security engineer must learn to keep things simple.
  - Complexity is the worst enemy of security.

Principles of security

- Don’t believe perfect security
  - “There are no secure systems, only degree of insecurity” (Adi Shamir)
- Secure systems can be expensive
  - “To halve the insecurity, double the cost” (Adi Shamir)
- Principle of least privilege
  - Need-to-know and separation of duty
- Minimize the number of trusted components
- Keep it simple
- Be skeptical
  - Don’t believe big security claims, unless you can verify them.
- Be professionally paranoid
  - Imagine you are in the attacker’s shoes