COMP3052.SEC Computer Security

Session 01: Introduction to COMP3052.SEC

ACKNOWLEDGEMENTS

- Some of the materials we use this semester may come directly from previous teachers of this module, and other sources ...

- Thank you to (amongst others):
  - Michel Valstar, Milena Radenkovic, Mike Pound, Dave Towey,…

OVERVIEW

- Convenor & Teacher Information
- Module Information
- Assessment
- Motivation for the Module
- Module Contents
- Textbook and Additional References
- Summary

TEACHING TEAM INFO

Convenors Information:

- Name: Dr. Alejandro Guerra Manzanares
- E-mail: Alejandro.Guerra@nottingham.edu.cn
- Room: PMB435
- Office Hours: TBA

- Name: Dr. Wooi Ping Cheah
- E-mail: Wooi-Ping.Cheah@nottingham.edu.cn
- Room: PMB323
- Office Hours: **Wed 1pm-3pm**

Technician Information:

- Name: Ms. Jane Zhao
- E-mail: Jane.Zhao@nottingham.edu.cn

Teaching Assistant:

- Name: Mr. Leshan Tan
- E-mail: Leshan.Tan@nottingham.edu.cn

MODULE INFORMATION

- Class Sessions
  - Classes and labs, … and maybe some other stuff, too
  - We'll frontload a bit
  - Wednesdays, 11am-1pm, IAMET-326 (Weeks 1-3)
  - Thursdays, 1pm-3pm, IAMET-326
  - Fridays, 4pm-6pm, IAMET-406
- Labs (and Coursework)
  - ~5 main labs
    - … more details soon!
- All materials on Moodle module page

TENTATIVE SCHEDULE

(Version: 2025Spring)

Week	Week Commencing	Wednesday (11am-1pm) (IAMET-326)	Thursday (1pm-3pm) (IAMET-326)	Friday (4pm-6pm) (IAMET-406)
01 (23)	17-Feb	Introductions	Motivating Examples	Foundations
02 (24)	24-Feb	Authentications	Access Control	Lab 1: Intro to Kali
03 (25)	3-Mar	Firewalls	Reference Monitor	Lab 2: Passwords
04 (26)	10-Mar		Network Sercurity Internet Security	Internet Security Unix/Linux Security
05 (27)	17-Mar		Windows Security	Lab 3: Firewalls
06 (28)	24-Mar		Intrusion Detection	Lab 4: Packet Sniffing
07 (29)	31-Mar		Software Vulnerabilities	Public Holiday
08 (30)	7-Apr	Data Security (1pm-3pm) (IAMET-406)	Crypto I	Lab 5: Attack & Defend
09 (31)	14-Apr		Crypto II & III	Lab Revision
10 (32)	21-Apr	Revision / Q&A (11am-1pm) (IAMET-326) Crypto IV & V (3pm-5pm) (IAMET-406)	Metamorphic Security	Revision / Q&A
11 (33)	28-Apr		Public Holiday	Public Holiday
12 (34)	5-May		No Teaching	No Teaching

ASSESSMENT

- 1 hour written examination 60 %
- Coursework 40 %
  - More details later … but it will almost certainly be based on your experiences and reflections on the series of lab activities

ACTIVITY …

- Come up with definitions for “security,” and “computer security,” and “security engineer”
- Why are we, as humans, concerned with these issues?

MOTIVATION

- People have protected their property and privacy for generations

  (Locks, Fences, Signatures, Seals, etc…)

- Big change
- Everything becoming electronic
- And security?
- What about the future?

ACTIVITY ...

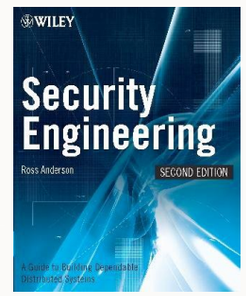
- List some points about what you ***expect*** to learn from this module, and what you ***hope*** to learn.
- Why?

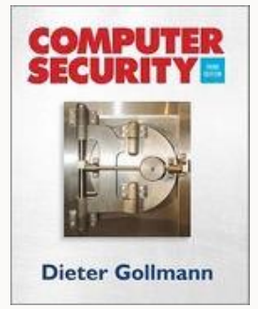
LEARNING OUTCOMES

- What is computer/information security ?
- Why is it so important ?
- How can we evaluate and measure it ?
- How can we enforce it ?
- How can we minimise its risks ?
- The bad guy's point of view
- The victim's point of view

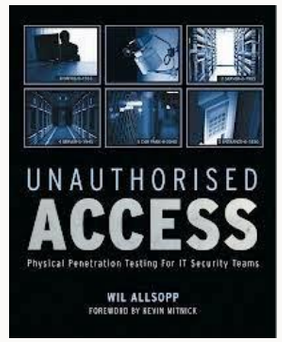
RESOURCES

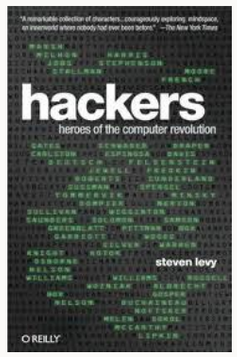
- Core text:
  - Security Engineering – Ross Anderson 2nd/3rd edition (some available online, for free)
  - Computer Security – Dieter Gollmann 3d edition (Amazon)





- Additional Reading:
  - Secrets & Lies – Bruce Schneier
  - Unauthorised Access - Will Allsopp
  - Hackers - Steven Levy





- Module materials on Moodle

INTRODUCTION TO SECURITY

OUTLINE

- On Security
- Attacks and Attackers
- Security Management
  - Security Policies
  - Measuring Security
  - Standards
- Risk and Threat Analysis
  - Assets
  - Vulnerabilities
  - Threats
  - Risks
  - Countermeasures

SECURE SYSTEMS

- A secure system is one which does not exist…

> *An almost secure system is one which is locked up in a nuclear bunker within an air locked titanium safe and disconnected from anything else in the world……and even such a system is not 100% secure!*

- It is not about achieving complete security
- It is about minimising risk to systems
- Both from a technical, and social, point of view

WIKILEAKS SERVER BUNKER

- http://www.youtube.com/watch?feature=player_embedded&v=wn8pz1HLYp8

ON SECURITY

- Original focus on systems with single, or few users
- Today focus on ubiquitous end systems
- Systems interconnected by networks
- Danger of possible attacks from ‘un-trustworthy’ nodes
- Both remotely as well as locally (insiders)

- Primarily a management issue!

ACTIVITY ...

- Based on your own impressions or knowledge, who are the "***attackers***"?
- What are the "***attacks***"?

ATTACKS AND ATTACKERS

- Landscape is changing
- Hackers -> Organised crime
- Website defacement -> Personal data harvesting
- Peer appreciation -> Earning money
- Viruses -> Trojans and Denial-of-Service attacks
- Complexity of our systems is increasing
- Our understanding of the system's intricacies can't keep up

SECURITY

- Reliability – Accidental failures
- Usability – Operating mistakes
- Security – Intentional failures

1. ‘Security is a people problem’
2. Legal system defines boundaries of acceptable behaviour
3. Management responsible for security

SECURITY MANAGEMENT

- Management responsible for assets
- Security measures must have clear full support of senior management
- Security awareness programs
- User is not (usually) the enemy!

- Developers need even more awareness!

SECURITY POLICIES

- State what should be protected
- And how this should be achieved

- Security Policy Objective
- Organisational Security Policy
- Automated Security Policy

MEASURING SECURITY

- Very difficult
- Measures only exist for some aspects of security

- Product Security
- System Security
- Cost of an Attack
- Cost of Assets

RISK AND THREAT ANALYSIS

- Risk Analysis
  - All information assets
  - IT infrastructure
  - Perform during development

- Risk – Possibility of an incident or attack to cause damage to your enterprise
- Risk = Assets * Vulnerabilities * Threat

ACTIVITY ...

- What are assets, vulnerabilities, and threats?
  - Come up with definitions, and list some examples

ASSETS

- Software
- Hardware
- Data and Information
- Reputation

- Identification easy, valuation difficult
- Data, Information, Reputation – difficult to measure

VULNERABILITIES

- Weaknesses of a system that could be accidentally or intentionally exploited to damage assets
- Badly configured accounts
- Programs with known flaws
- Weak access control
- Weak firewall configuration
- Can be rated according to impact

THREATS

- Actions by adversaries who try to exploit vulnerabilities to damage assets
- Categorisation by damage done to assets
- Identification of source of attacks
- Analysis of attack execution (Attack Graphs)
- Can be rated according to likelihood
- Attack Graphs
  - formalised and structured
  - assessable, reproducible

RISK

- Quantitative Risk Analysis
  - + probability theory based on mathematical theory
  - - quality of results depends on quality of inputs
  - - not always feasible
- Qualitative Risk Analysis
  - + more applicable
  - - scaling based on judgements of security experts

COUNTERMEASURES

- Risk analysis generates recommended countermeasures
- Up to date/continuous risk analysis not always possible
- Baseline protection – security requirements for typical cases with recommended countermeasures

SUMMARY

- Current security landscape
- Management is vital to security
- How security can be measured
- What is Risk and how it is analysed

Read Anderson: Chapter 1