COS30015 IT Security

Live Lecture Week 1

Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

Teaching Team

Convenor

Prof. Jun Zhang
Email: junzhang@swin.edu.au

Dr. Rory Coulter
Email: rjcoulter@swin.edu.au

Lecturer

Dr. Rory Coulter
Email: rjcoulter@swin.edu.au

Mr. Lin Li
Email: linli@swin.edu.au

Tutor

Ms JAMIE OOI
Email: jooi@swin.edu.au

Mr Daniel Hood
Email: dhood@swin.edu.au

Mr Andrew Plapp
Email: aplapp@swin.edu.au

Mr Yasas Akurudda Liyanage Don
Email: yakuruddaliyanagedon@swin.edu.au

SWINBURNE UNIVERSITY OF TECHNOLOGY

Teaching Strategy

- Lectures
  - Video-streaming lecture, around an hour, self-paced (Echo360 ALP)
  - Live-streaming lecture, around an hour, every Wednesday 12:30 pm – 13:30 pm (Collaborate Ultra)
  - Consultation in Teams (Wednesday 10:00 am – 11:00 am by appointment)

- Labs
  - On-campus (EN305)
  - Online lab (Thursday 10:30, Friday 8:30, 10:30) via Canvas.

Teaching Strategy

- Live Lecture
  - Last week revision (Questions about lecture notes)
    + this week lecture guidance
    + this week lab introduction (Andrew)
    + Some interesting knowledge or news (Andrew)
    + take away menu for this week
    + task list for this week

  - When the week release an assessment, then the first two regular content will be shorten. The spared time will be used to introduce the assessment.

  - When a guest lecturer joins us, the first two regular content will be shorten as well.

Teaching Strategy

- Lab Session
  - Tutor will give you a brief introduction.
  - Our tutor will lead you to complete the lab tasks.
  - Some slides will be used to explain the lab tasks.
  - Q&A and etc.

Teaching Strategy

- **Discussion Board**
  - Navigation discussion board
  - Each week's lecture discussion board
  - Each week's lab discussion board
  - Each assessment discussion board

  - ! Please leave the questions about the assessment requirements in the discussion board, so that other students could benefit from the Q&A

Three Assessments & No Exams

- Research Project (40%)
  - Due Thursday Week 6 (08 Sep 23:59)
  - Literature Review 2,500-4,000 words (> 6 pages)
  - The Assignment 1 will be released by Monday Week 2
- Lab Online Quiz (20%)
  - In Week 7
  - 60 minutes for 20 questions
- Practical Project (40%)
  - Due Sunday Week 12 (26 Oct at 23:59)
  - IT Security problem -> practical exercise -> results & analyze (~ 15 pages of text)
  - The Assignment 2 will be released by Week 7

Key Generic Skills for this Unit of Study:

- Analysis skills
- Problem solving skills
- Communication skills
- Ability to tackle unfamiliar problems

SWINBURNE UNIVERSITY OF TECHNOLOGY

Late submission?

- Meet any difficulties
  - Feel free to send us emails for help.
- Be penalized by 10% per day
  - 5 days maximum.
- Special cases?
  - Send me email in advance, well explain your reason to have some extension.
  - To gain my permission, I highly suggest a well-prepared plan about what would you do next.

What will you learn from COS30015 IT Security?

- 12 Weeks
  - Overview of IT Security
  - Physical and Converged Security (i.e., hardware, interface, location, etc.)
  - Operating System Security (i.e., kernel, process, memory, etc.)
  - Malware (i.e., trojan, spyware, etc.)
  - Network Security 1 & 2 (Network Structure)
  - Web Security (Website i.e., HTTP, packets, cookies, session, etc.)
  - Cryptography (Encryptions etc.)
  - Security Models
  - Web Application Security (i.e., Database & Email security)
  - Cloud Security and Law

Research Material

❑ Textbook

- Michael Goodrich and Roberto Tamassia, "Introduction to Computer Security: Pearson New International Edition", Pearson Education Limited

❑ Swinburne library

- https://www.swinburne.edu.au/library/

- Such as, IEEE Xplore, ScienceDirect (Elsevier), ACM digital library

SWINBURNE UNIVERSITY OF TECHNOLOGY

Security Concepts

Definitions

Cyber security?

Information Security, ICT Security?

A blend?

Magic?

Aus Gov Glossary

Measures used to protect the confidentiality, integrity and availability of systems, devices and the information residing on them.

Industry

Cyber security is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks.

It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks and technologies.

https://www.cyber.gov.au/acsc/view-all-content/glossary
https://www.itgovernance.co.uk/what-is-cybersecurity

Confidentiality, Integrity, Availability (CIA)

- Confidentiality
  - Only those entitled to access the information can see it.
- Integrity
  - Information cannot be altered and changes are immediately detectable.
- Availability
  - Information is available (to read, write) to those who need it without interruption or access restrictions

CIA Examples

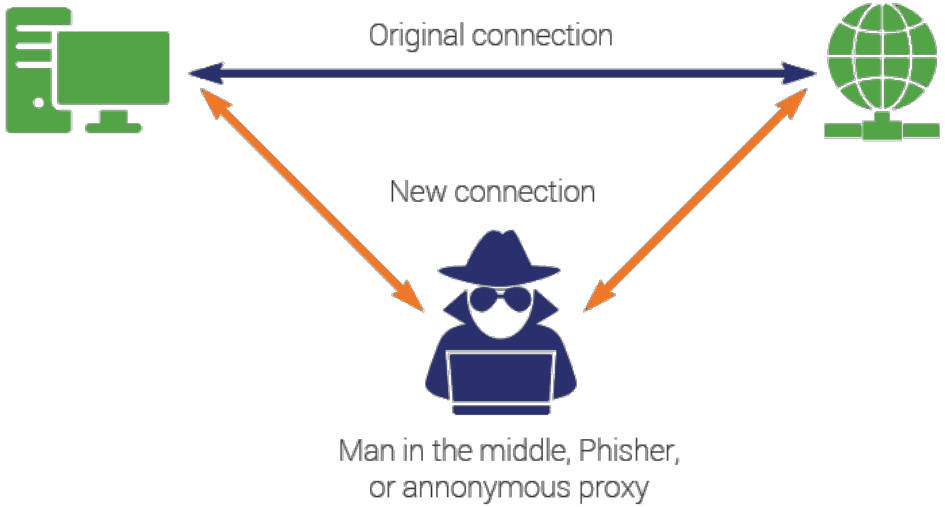
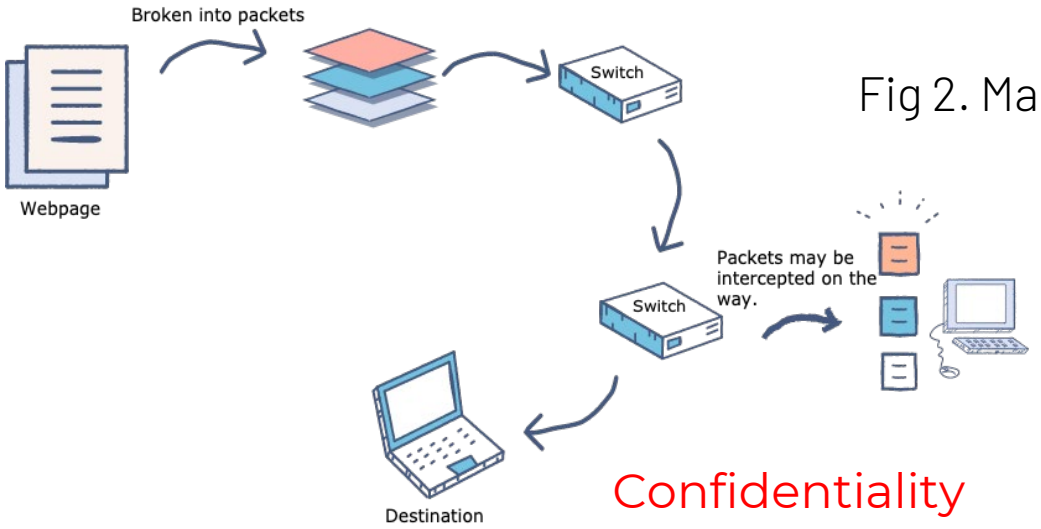


Fig 2. Man-in-the-Middle Attack

Integrity



Confidentiality

Fig 1. Packet Sniffing Attack

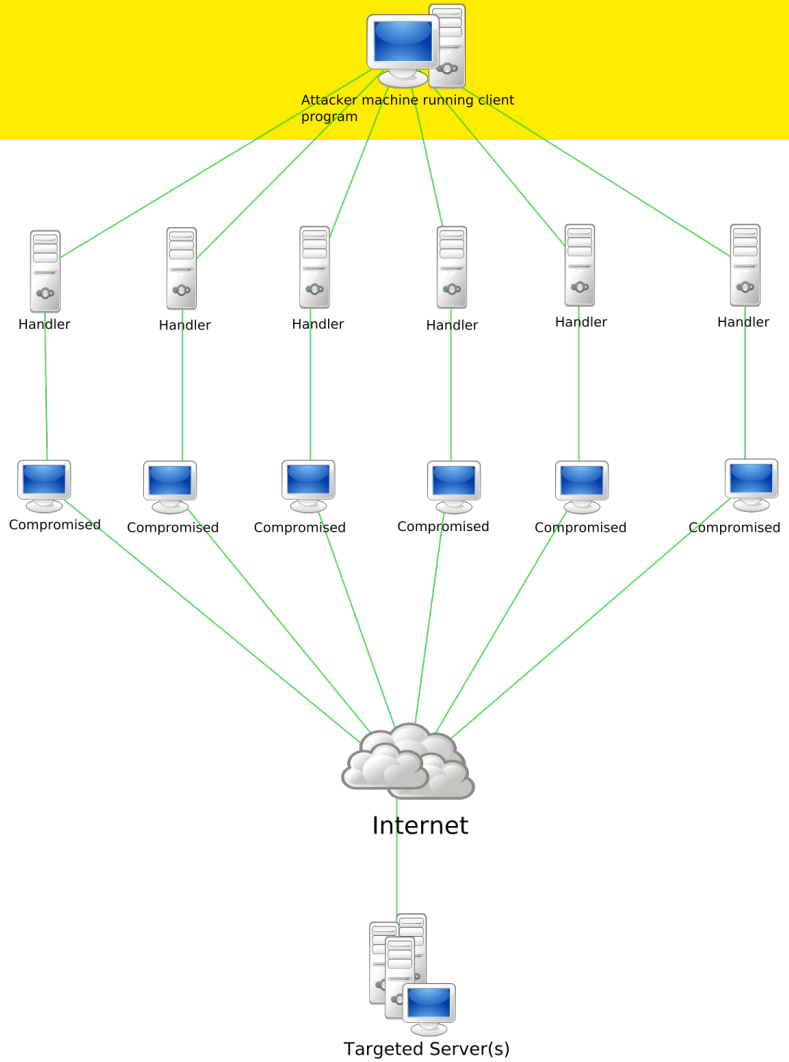


Fig 3. Denial-of-Service Attack

Availability

SWINBURNE UNIVERSITY OF TECHNOLOGY

Security paradigms

- In Practice…
  - Some blacklisted things
  - Some whitelisted things
  - Unknown threats slip through undetected.
  - Different policies for different resources (segmentation)
  - High-value targets are default deny, ACL;
  - Low value targets are default allow, daily re-image of SOE to minimise threat from 0-day attacks.
    - Persistent malware can defeat this
  - Need Defence in Depth because no single control is effective.

Cryptographic Concepts

Encryption

- Encryption provides privacy / secrecy
- Plain text is encrypted to cipher text.
- Uses encryption key(s)
- Reversible (can be decrypted with the right key)
- Encryption algorithms use 2 main techniques:
  - Permutation (P-Box)
  - Substitution (S-Box)

Easy to build in hardware

Encryption

Attacks:

- Permutation
  - vulnerable to known text attacks
- Substitution
  - vulnerable to statistical methods
- Strength depends on key length (measured in bits) and algorithm complexity.

Encryption

❑ Symmetric key

- same key to encrypt and decrypt.
- problem of *how you get the key to the recipient*.

❑ Asymmetric key

- 2 keys – one for encryption, one for decryption.
- problem of *how you get the public key from the recipient*.

Hashing

- A one-way ‘encryption’ algorithm, which cannot be reversed. Lossy.
- Used to *uniquely identify* something without looking at it.
- Used to *detect alteration of something*.
- Collisions = 2 different things with the same hash. Possible but unlikely.
- Strength depends on algorithm, bit length
  - Most attacks rely on *errors in implementation*

Certificates

- Combination of hash, symmetric and asymmetric crypto. and trusted party (problematic) used to authenticate.

- Trusted parties are not trustworthy.
  - Can be compelled (by government) to lie, divulge private keys, sign fake keys.
  - Keys, certificates can (and have) been stolen.
  - Inadequate diligence when signing (authorising) code.

- Users regularly ignore security warnings because of invalid certificates.

Implementation and Usability Issues

Usability

- If we make security too hard, users will avoid it.
  - Onerous password restrictions,
  - Organisation resource restrictions with dummy codes need for workarounds.

- Workarounds:
  - Shared logins, cloud storage, BYOD (iPads, phones),
  - Social engineering attacks become easier.

What's Legal

- Check your Internet service provider (ISP)'s Acceptable use policy – it's in your contract.
  - It may forbid hacking activities like port scanning.
  - Most hacking activities are covered by non-electronic crime laws.
  - Port scanning = trespass
  - Packet sniffing = privacy laws
  - Laws are constantly being updated to remove loopholes caused by new technology.

- Laws are not consistent across Australia or the world.
  - Makes enforcing difficult.

What's Legal

- ❑ Never attempt to test a system unless you have express permission to do so from the owner of the system.
  - Even then you may be breaking the law.
  - Be subtle. Don't break things. Be discreet.
  - Some changes to Australian law make it illegal for System Admins to test their own networks!
  - Never test cloud / live web services.
  - GET PERMISSION IN WRITING
- ❑ Real black hats create a duplicate of the target system and practice on it.
  - Build your own network and practice on it.

Testing security

Social engineering

- An off-line activity used by hackers to trick network administrators and other staff into providing passwords, usernames and access to secure systems.

- Activities include 'dumpster diving', phone calls and ‘pretexting’, shoulder surfing, tail-gating.

Testing security

- Penetration test
  - "...a method of evaluating the security of a computer system or network by simulating an attack by a malicious user... "(Wikipedia*).
  - Penetration testers may have some security product to sell, and may go to extreme lengths to compromise a system.
- Audit
  - A program of activities including penetration testing, risk analysis, interviews with staff and reviews of hardware and software access.

Philosophies: TNO

- "Trust no-one".
- Steve Gibson's philosophy on internet security.
  - Encryption keys are only known to the sender and the recipient (NOT CAs, Skype, 3rd parties).
  - Peer to peer connections are NOT mediated by a central server.
  - Cloud storage providers CANNOT decrypt your stuff if compelled by governments, law enforcement.
  - TelCos (Telstra, Optus, ISPs) CANNOT intercept (proxy) your secure web and mail sessions.

Philosophies: PIE

- "Pre-internet encryption".
- Steve Gibson's philosophy on encryption.
  - Encryption keys are only known to the sender and the recipient (TNO).
  - All encryption occurs on the end-point (the host you control)
  - All decryption occurs at the other endpoint (the host the recipient controls).
  - Good for secure comms., secure storage.

What's in this week's lab?

- Lecture Topic --- Overview of IT Security
- Lab Task --- Basic commands in Linux System
- Let's welcome Andrew to introduce this week's lab task

Task List for Week 1

- ❑ Lecture Activity
  - ❑ Video-streaming lecture
- ❑ Setup Virtual Machine before lab sessions
- ❑ Complete this week's Lab Task
- ❑ Suggest: external readings in Week 1 Module

SWINBURNE UNIVERSITY OF TECHNOLOGY

Thank You!