COS30015 IT Security

Live Lecture Week 2

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.

Assignment 1 --- Research Project

- Worth 40% of the subject assessment
- Due Date: Thursday the 8th of Sept 2022 at 23:59pm.
- Workload
  - The literature review should consist of 2500-4000 words (at least 6 pages, single spaced, 12pt fonts, on a normal A4 paper).
  - Each student should spend at least 30 hours working on the assignment.

SWINBURNE UNIVERSITY OF TECHNOLOGY

Assignment 1 --- Research Project

- What is a literature review?
  - A standalone literature review
  - As part of a thesis or research paper

- What is a good literature review?
  - Has a clear understanding of key concepts within the topic.
  - Clarifies important definitions and terminology.
  - Covers the breadth of the specific topic.
  - Critically discusses the ideas in the literature and evaluates how authors present them.
  - Clearly indicates a research gap for future enquiry.

SWIN BUR NE SWINBURNE UNIVERSITY OF TECHNOLOGY

Assignment 1 --- Topics

Attacks:

- Advanced persistent threat
- Insider threat
- Emerging Attacks on Blockchain or the defences
- Emerging Attacks on IoTs or the defences
- Emerging Attacks on AI or the defences
- Backdoor attacks or the defences
- Denial of service or Distributed Denial of service
- Eavesdropping
- Exploits
- Malware
- Spam
- Phishing
- Ransomware
- Vulnerabilities

Defences:

- Access control
- Application security
- Secure coding
- Authentication
- Multi-factor authentication
- Authorization
- Data-centric security
- Encryption
- Intrusion detection/prevention system
- Mobile security
- cloud security

Too much literature?

Not enough literature?

SWINBURNE UNIVERSITY OF TECHNOLOGY

Assignment 1 --- How to write (Brief Introduction)

- Abstract
- Introduction
- Overview/Background
- Literature Review
- Discussion
- Conclusion

Attachments

AssignmentCoverSheet.doc

COS30015-Assignment1-2021.pdf

SWINBURNE UNIVERSITY OF TECHNOLOGY

Assignment 1 --- How to write (Brief Introduction)

- Decide what you will write about
  - Spreadsheet, collect relevant information, record, help shape your narrative.

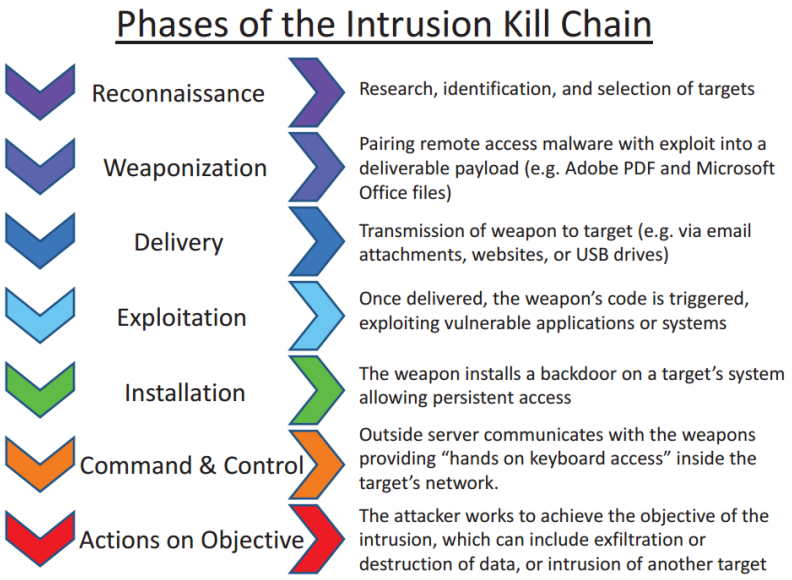
Year	Topic Class (Infra	Cyber Attack	Targeted Information (/	Methodology	Paper List	Problem Solving / Main Work	Similarities & Differencies	Limitations	Further/ Future Work	Experiment Datse	Query input & output	Comments
SP 2018	Cloud Service (MLaaS System)	Steal Controlled Model	Linear and Kernal ML Models' hyperparameters (Objective functions' coefficient)	hyperparameter stealing attacks (using Equotion solving attack)	Stealing Hyperparameters in Machine Learning	Hyperparameters stealing attack via observing minima objective function against MLaaS in black-box setting.	1. Trainig data was uploaded to train the popular classifier 2. The classifier was trained & stored in the cloud 3. Attacker aim at learning model hyperparameters (~ inference) 4. Attacker involve training process & attack after the process 5. Prior know: predictions + training dataset + learning algorithm	1. Successful Train-Steal-Retrain startegy relys on data quality in retraining an accurate model. 2. Cannot steal ML algorithm and hyperparameters when ML algorithm is unknown. 3. Do not consider other kinds of hyperparameters	1. The security of hyperparameters for other ML (i.e. K for KNN) 2. The possibility of stealing ML algorithm and hyperparameters 3. Defences except rounding para~	Regression: Diabetes; GeoOrig; UJIIndoor Classification: Iris; Madelon; Bank	Membership inputs (random d-dimensional inputs) Output: a label only (confidence value vector/ some data structure info -> API)	Amazon: extract model trained by ourselves Microsoft: extract model trained by ourselves
CCS 2015	Cloud Service (MLaaS System)	Steal Controlled Training Data	Participants' training dataset	Model inversion attack	Model inversion attacks that exploit confidence information and basic countermeasures (125)	Model inversion attacks leverage confidence information with predictions against MLaaS APIs in white-box (+) and black-box setting.	1. Trainig data was uploaded to train the DT & NN / black-box 2. The classifier was trained & stored in the cloud 3. Attacker aim at learning victim's training data 4. Attacker attack after training process 5. Prior know: prediction + input + learning algorithm (/+ para~) 6. Protect by rounding the confidence score (obfuscation)	1. Recover only prototypical examples [#11] 2. MI works well for MLP networks but fails with NNs clearly. 3. The proposed simple mitigation technique not guarantee any rigorous privacy notion [#14]	1. MI-resistant ML 2. Optimize the MI attack using approximate gradients	FiveThirtyEight survey. GSS marital happiness survey.	Input: sensitive attributes Output: label + confidence value	Decision tree API: Microsoft ML (black-box), Wise.io, BigML (white-box & black-box)
SP 2017	Cloud Service (MLaaS System)	Steal Controlled Training Data	Participants' training dataset	Membership inference attack	Membership Inference Attacks Against Machine Learning Models	Membership inference attacks leverage shadow training technique to determine the specific record's membership of original training set in black-box setting.	1. Trainig data was uploaded to train the black-box classifier 2. The classifier was trained & stored in the cloud 3. Attacker aim at learning victim's training data (membership) 4. Attacker attack after training process 5. Prior know: predictions + inputs + learning algrithm	1. The proposed simple mitigation technique not guarantee any rigorous privacy notion [#14]		CIFAR100, CIFAR10, Purchases, Foursquare, Texas hospital stays, MNIST, Adult (income)	Input: sensitive attributes Output: label + confidence value	Google API: black-box Amazon: black-box
CCS 2017	Cloud Service (MLaaS System)	Steal Controlled Training Data	Participants' training dataset	Generative Adversarial Networks attacks	Deep Models Under the GAN: Information Leakage from Collaborative Deep Learning	Collaborative deep learning model [77] which was used to preserve the training process of centralised training model -> attacked by GAN -> leaking user's training dataset.	1. Trainig data was uploaded to train the NN classifier 2. The classifier was trained & stored in the cloud 3. Training data protected with distributed collaborative learning 4. Attacker aim at learning victim's training data 5. Attacker participate in training process 6. Prior know: learning algorithm + parameters + inputs	1. No effective countermeasures to against GAN 2. The attack is specific to collaborative deep learning model 3. Attacker participate in training process	1. Build a real system for collaborative learning with device, class, or user-level DP	MNIST AT&T	Not query, participate in training process Upload part of parameters + differential privacy Download part of PS parameter (replace laocal parameter)	Key

- Considering this, what could we be writing about?

SWINBURNE UNIVERSITY OF TECHNOLOGY

Assignment 1 --- How to write (Brief Introduction)

- Literature Body
  - How you decide the space is organized, where literature goes, the review body should reflect this.



SWINBURNE UNIVERSITY OF TECHNOLOGY

Assignment 1 --- How to write (Brief Introduction)

- Questions
  - Help shape what you write about in the review body
  - Data collection
  - Example: What are the most pressing (APT issues/vulnerability types) being researched? Or What detection methods are most appropriate for current and future (attacks/vulnerabilities)?

- Discussion
  - Number of questions = number of subsections in the discussion
  - Answer your research questions

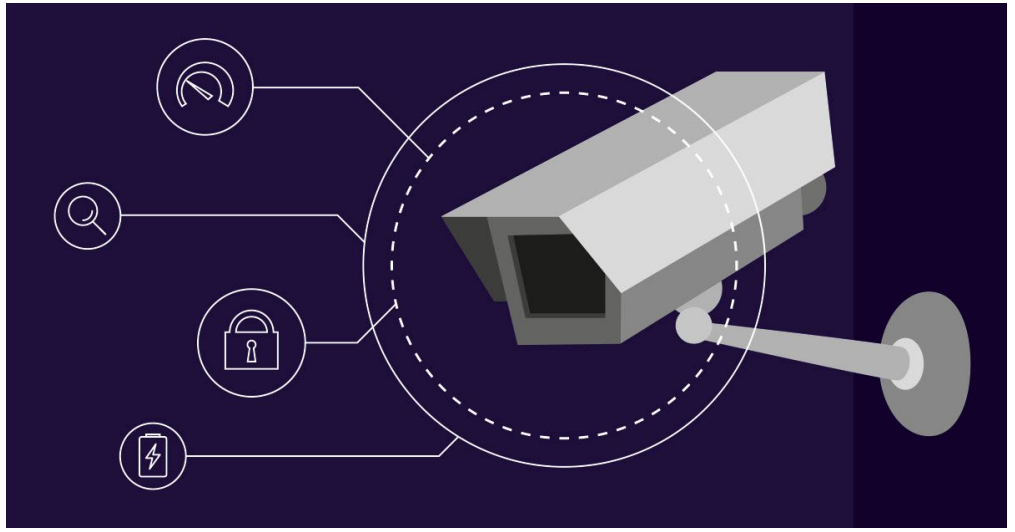
SWINBURNE UNIVERSITY OF TECHNOLOGY

Physical Security

Physical Protections and Attacks

- Physical security
  - The use of physical measures to protect valuables, information, or access to restricted resources.
  - Three important components: access control, surveillance, and testing.

- Locks
- Authentication technologies
- Physical Attacks
- Social Engineering
- Computer Forensics



SWIN BUR NE
SWINBURNE UNIVERSITY OF TECHNOLOGY

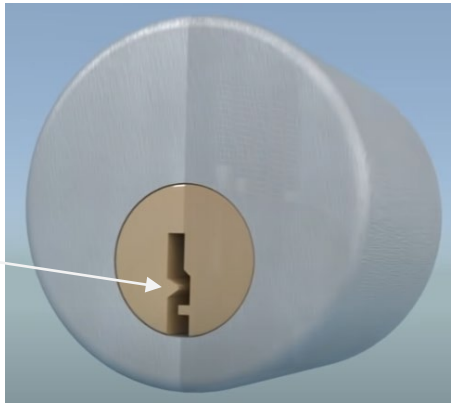
Locks

- Commonly used lock types
- Pin tumbler locks (easy to pick)
- Radial locks
- Wafer locks (medium security)
- Combination locks (low security)
- Electronic locks
  - Electronic combination
  - mag stripe
  - RFID
  - biometric
  - easy to change combination
  - easy to monitor

SWINBURNE UNIVERSITY OF TECHNOLOGY

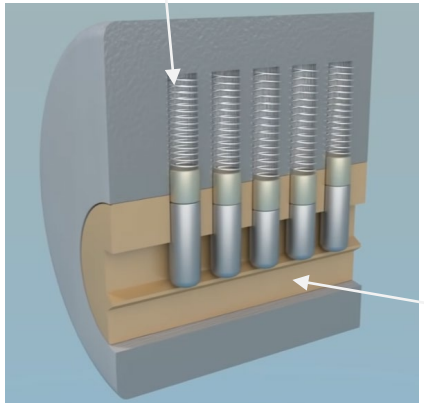
Pin tumbler locks

1



Keyway

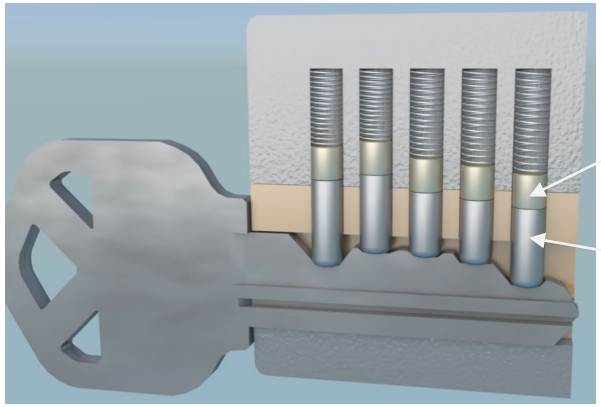
2



Spring

Plug

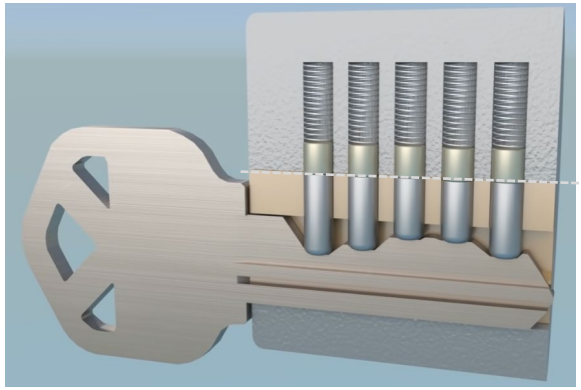
3



Driver pin

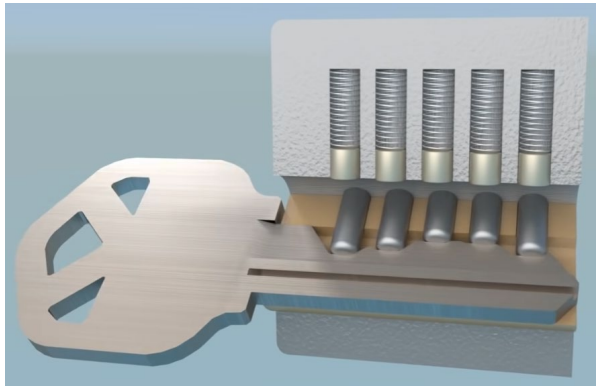
Key pin

4



Shear line

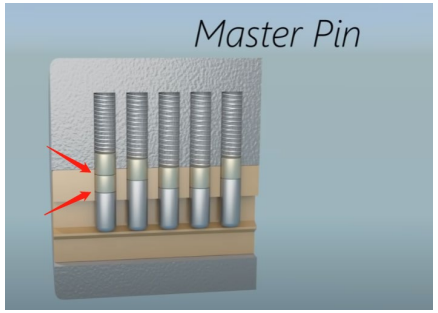
5

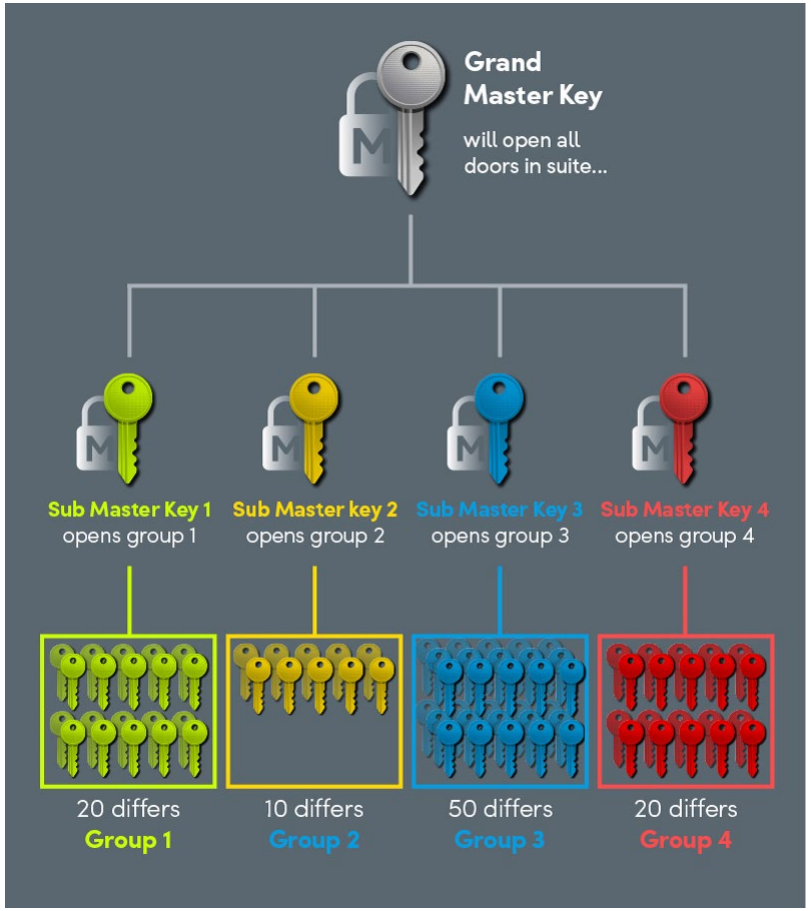


https://www.youtube.com/watch?v=smIdInCQ-kU

Master and Control Keys

- Organizations require a key system
- Access control
  - Who has which key
  - How are keys issued returned and disabled
  - Lost/stolen keys
- Key types
  - Change keys
  - Master keys
  - Grandmaster keys
  - Control keys





SWINBURNE UNIVERSITY OF TECHNOLOGY

Attacks on Locks

- Lock picking
- Lock bumping
- Key duplication and impressioning

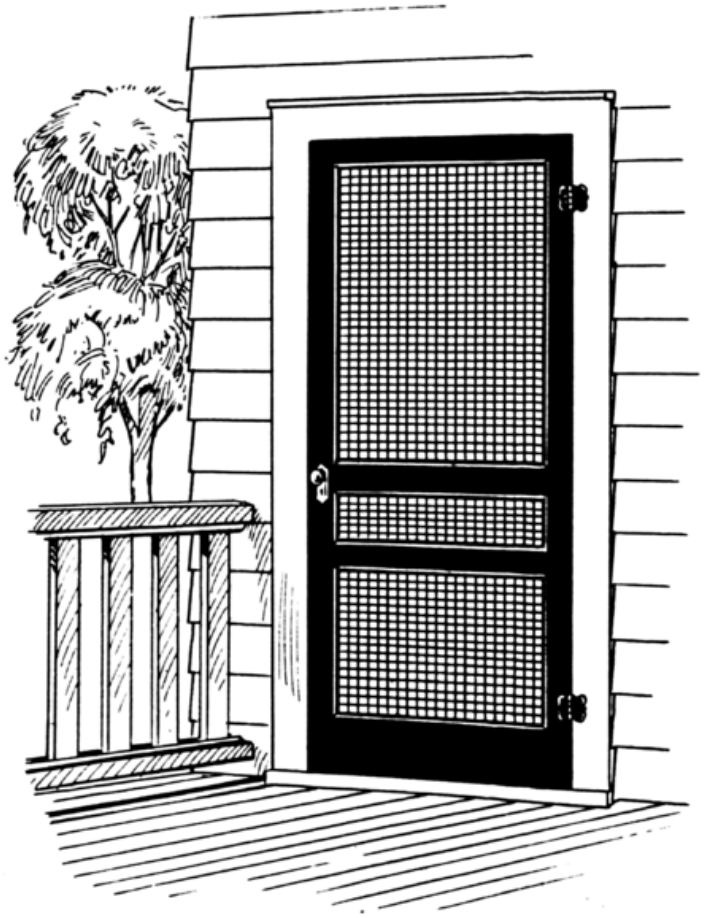
- Higher security locks are invented to make bypassing locks more difficult
- Security pins
  - Mushroom head pins
  - Serrated pin
- Disc tumbler lock

https://www.youtube.com/watch?v=TjRj69P5rKM&t=60s

SWIN BUR NE SWINBURNE UNIVERSITY OF TECHNOLOGY

Side Channel Attacks

- Remove the hinges
- Cut through the door
- Enter through the roof (tiles, vents, manhole)
- Enter through emergency exits, windows
- Social engineering
  - deliveries
  - tail-gating



SWINBURNE UNIVERSITY OF TECHNOLOGY

More Authentication Technologies

(alternatives to keys and locks)

Barcodes

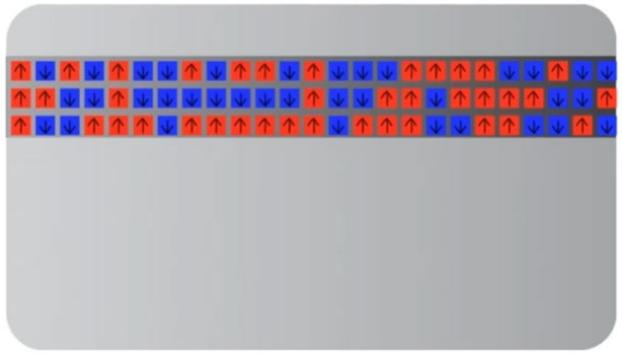
- Developed initially for improving efficiency in grocery checkout
- Supermarket checkout
- Parcel tracking
- Ticket confirmation
- Boarding pass
- Cashless Payment

- Non-alterable encoded data

SWIN BUR NE
SWINBURNE UNIVERSITY OF TECHNOLOGY

Magnetic Strip Cards

- Plastic card with magnetic stripe on the back
- ID Cards, Credit Cards, etc.
- Swipe to use
- Targeted for fraud



SWINBURNE UNIVERSITY OF TECHNOLOGY

Smart Cards

- Credit card size
- Built-in chip
- Used in financial, mobile phones, public transit, etc
- Security

RFIDs

- Three components:
  - RFID tags / smart label
  - RFID reader
  - Antenna

- Transmit information via radio waves
- Must be used with a separate reader or writer
- With/without battery
- Range varies from CMs to Ms

SWINBURNE UNIVERSITY OF TECHNOLOGY

Biometrics

- Measures a human characteristic and compares features of it to those stored in a database.
- Universal – everyone must have the characteristic.
- Distinctive – characteristic must be different for everyone
- Permanent – characteristic must not change with time
- Collectable – must be possible to collect characteristic.
- Low False-positive /false-negative rate
- Hard to forge

Physical identifiers - Biometrics

- Fingerprints
- Face, retina, iris
- Voice
- Signature
- DNA (law enforcement)

SWIN BUR NE SWINBURNE UNIVERSITY OF TECHNOLOGY

Behavioral identifiers - Biometrics

- Typing patterns
- Physical movements
- Navigation patterns
- Engagement patterns

SWIN BUR NE
SWINBURNE UNIVERSITY OF TECHNOLOGY

Risks

- All are problematic. Fingerprint probably the best.
- Database containing feature data can be compromised.

Physical Attacks

Environmental attacks and accidents

- Computing equipment operates in a natural environment. Computing environment includes:
  - Electricity
  - Temperature
  - Limited conductance

Eavesdropping

- Eavesdropping is the process of secretly listening in on another person's conversation
  - Keyboard Listening
  - WiFi Sniffing
  - MITM attacks (proxying, malware)
  - Phone tapping

Attacks on special purpose machines

- Attacking ATMS
  - Skimming
  - Shimming
  - Card Trapping
  - Cash Trapping
  - Physical attacks (brute force)

SWINBURNE UNIVERSITY OF TECHNOLOGY

What's in this week's lab?

- ❑ Lecture Topic --- Physical Security
- ❑ Lab Task --- Set up a Network
- ❑ Let's welcome Andrew to introduce this week's lab task

SWINBURNE UNIVERSITY OF TECHNOLOGY

Task List for Week 2

- ❑ Lecture Activity
  - ❑ Video-streaming lecture
- ❑ Complete this week's Lab Task
- ❑ Plan for your Assignment 1
- ❑ Suggest: external readings in Week 2 Module

SWINBURNE UNIVERSITY OF TECHNOLOGY

Next Week --- Guest Lecturer

- **Topic: “Converged Security”**
- **Guess Lecturer: Simon Lee-Steere**
  - --- Deputy Chief Security Officer at nbn® Australia

SWIN BUR NE
SWINBURNE UNIVERSITY OF TECHNOLOGY