# IFB240 Cyber Security

## Lecture 2 - Part C
## Security Incidents and Attacks

Dr Leonie Simpson
lr.simpson@qut.edu.au

# Security Incidents and Attacks

- When threats and vulnerabilities coincide, information assets can be harmed
  - a security incident occurs
- Security incidents
  - Referred to as an attack if the threat involves deliberate human action
    - Attacker - Person who deliberately attempts to exploit a vulnerability to gain unauthorized access, or perform unauthorized actions (also called threat actor, malicious actor)
- NOTE: Even if threat action is not deliberate, damage from a security incident can still be extensive

# Security incidents

- Example – August 2020 data breach Tasmania
- Data breach at University of Tasmania affects 20,000 students - ABC News

**Data breach at University of Tasmania affects 20,000 students**

By James Dunkerley and Alexandra Humphries

Posted Mon 21 Sep 2020 at 1:58pm, updated Mon 21 Sep 2020 at 7:43pm


UTAS said there was "no evidence the breach was the result of malicious activity". (Supplied: UTAS)

The University of Tasmania has had to contact almost 20,000 students after their personal information was accidentally made accessible to all users with a UTAS email address.

The data that became accessible due to the breach varied for individual students but could have included birth dates as well as whether the student had a disability or identified as indigenous.

UTAS said there was "no evidence this data breach was the result of malicious activity" and that "security settings on shared files were unintentionally configured incorrectly, which made the information visible and accessible to unauthorised users".

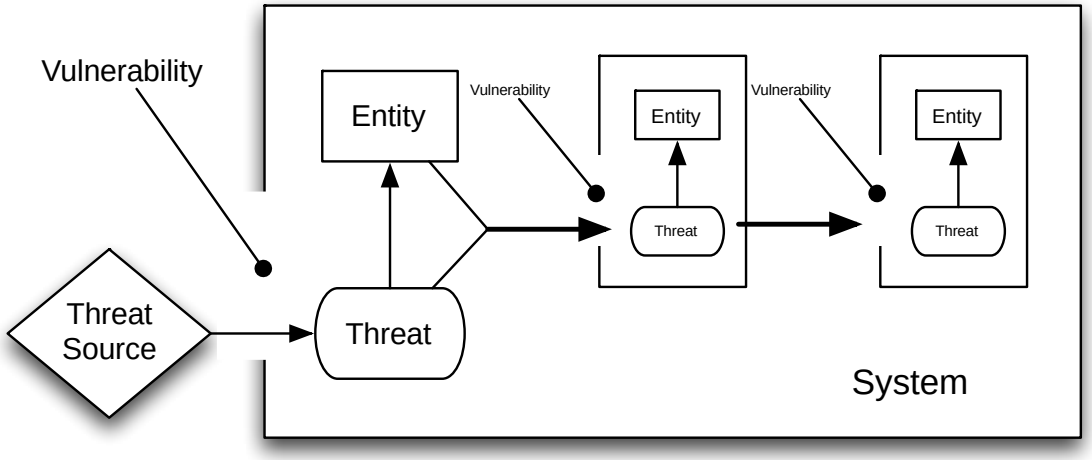
accessed by individuals with a University of Tasmania email address".

"The security settings for this SharePoint site were unintentionally configured incorrectly. This meant that individuals with a utas.edu.au email address not authorised to access documents saved in the site, were inadvertently granted access.

"This was the result of incorrect configuration. There is no evidence this data breach was a result of malicious activity. The system has now been correctly configured."

# Chain of events in an incident

- When threats and vulnerabilities coincide, information assets can be harmed
  - Each event or incident can create new vulnerabilities
  - If these are exploited, subsequent security incidents occur
  - Sometimes there is a chain of events, especially in interconnected systems



# Chain of events

- Example chain of events
  - Event 1 – *Personal information exposed*
    - Vulnerability: Misconfigured internet connected database containing personal information, including DOB, contact addresses, of students …
    - Threat: Personal information in database will be disclosed to unauthorised persons
    - Attack: Unauthorised person deliberately accesses database, observes and copies personal information (breaches confidentiality)
  - Event 2 – *Phishing the students*
    - Vulnerability: Students susceptible to email phishing
    - Threat: Email recipient opens attachment to email that contains malware, installs malware on their device
    - Attack: An unsuspecting student receives a phishing email (body may be a friend request, birthday message, discount coupon attached, request to review attached invoice, etc), opens the attachment and the malware is installed on their device

# Chain of events

- Example chain of events - continued
  - Event 3 – *Malware extracts information*
    - Vulnerability: Students computer allows them to install software, and/or their antivirus scanning software does not detect the malware in attachment or after installation
    - Threat: Key logging malware will be installed – information entered from keyboard will be recorded (say, passwords to other accounts, including online banking) and sent over network to attacker
    - Attack: Key logging malware used: after student victim has accessed accounts online, attacker now has record of phishing victim's credentials for other accounts (breaches confidentiality)
  - Event 4 – *Stealing money from student bank accounts*
    - Vulnerability: Student has online bank account that uses password as single authentication factor
    - Threat: Unauthorised person can access the bank account and perform transactions
    - Attack: Attacker uses victim's credentials (can provide correct credentials, so looks legitimate to bank system) to access victim's bank account and transfers money out of student's bank account (into a mule account – multiple used in path to attacker's account)

# Types of attacks

- Categorised based on attacker interaction
  - Passive
    - Attacker's goal is to obtain information
    - Attacker ***does not alter*** information system resources
      - No interaction by the attacker other than listening or observing
    - Difficult to detect; usually try to prevent the attack
  - Active
    - Attacker's goal may be to obtain, modify, replicate or fabricate information
    - Requires some action or interaction with the information system by the attacker
    - Usual approach is to try to detect attacker's actions, recognise them as signs of attack and recover

# Passive Attacks

- Eavesdropping
  - Listening to conversations of others
    - Without their knowledge or consent
  - Wiretapping
    - Eavesdropping over telephone network
    - May be harder to detect in wireless network
  - Information can be obtained from
    - The content of the conversations, and
    - Knowing who is talking to who and when (traffic analysis)

# Passive Attacks

- Shoulder surfing
  - Watching the actions of others (especially at data entry) without their knowledge or consent
  - Usually connected with entry of confidential information
    - PIN (for financial access at ATM)
    - Security code or password
  - Can also be for greater amounts of data
    - Use of mobile devices in insecure surroundings is vulnerability that can be exploited for this attack

# Passive Attacks

- Network monitoring and eavesdropping
  - A packet sniffer or network analyzer can monitor network traffic, can be used
    - For network maintenance (finding faults and traffic problems)
    - Or to gain knowledge of confidential information
      - For example, passwords corresponding to user names
  - Confidential information should not be sent over untrusted networks without protection
    - Example: when logging on to a remote resource, passwords should not be sent ‘in the clear’ (unencrypted)

# Active Attacks

- Denial of Service (DoS) Attack
  - Objective is to make an information asset or resource unavailable to authorized users
  - Common methods used by attackers are
    - Damage the resource, so that it cannot be used
    - Deliberately interrupt communications between users and resource, so that it cannot be accessed
    - Overload the resource by making a large number of requests for service, so it cannot respond to legitimate requests
  - Vulnerability - exists in information system providing service
  - Threat - that the service will be made unavailable
  - Attacker - deliberately exploits vulnerability to achieve this

# Active Attacks - Examples

- Example: Denial of Service (DoS) Attack
- Can also apply to telecommunications (TDoS)
  - Mirai malware in Nov 2016 attack on Deutsche Telekom
  - https://www.itnews.com.au/news/mirai-botnet-attacks-900000-german-broadband-routers-442887

## Mirai botnet attacks 900,000 German broadband routers

By Juha Saarinen
Nov 29 2016
9:00AM

2 Comments

**Malware attempts to infect routers via remote management feature.**

Hundreds of thousands of Deutsche Telekom broadband customers in Germany have been attacked by the Mirai malware, crashing their routers and degrading internet connections.

The telco said as many as 900,000, or about 4.5 percent of its 20 million fixed-line customers, began to have problems connecting to its network on Sunday afternoon.

# Active Attacks

- Distributed Denial of Service (DDoS) Attack
  - Objective is same as DoS attack
    - Breaches availability of information asset
  - *Slight difference* in method
    - Use *multiple* sources to make resource requests
      - Malware (virus) may be used to first compromise machines and make them bots in a net controlled by an attacker → botnet
      - All bots have same target and payload is activated at same time, to make simultaneous resource request
    - Overloads resource, so  it cannot respond to legitimate requests

# Active Attacks - Examples

- Example: Denial of Service (DoS) Attack
  - DoS and DDoS commonly applied to websites
- Feb 17 2023 The Record
  - German airports hit by DDoS attack, ‘Anonymous Russia’ claims responsibility - The Record from Recorded Future News


IMAGE: ALAN ANGELATS VIA UNSPLASH

Daryna Antoniuk

February 17, 2023

Briefs

**German airports hit by DDoS attack, ‘Anonymous Russia’ claims responsibility**

It’s been a difficult week for German airlines.

A day after a major IT failure at Lufthansa left thousands of passengers stranded, the websites of seven airports were hit by a suspected cyberattack.

Among the airports affected by a “large-scale DDoS [distributed denial-of-service] attack” on Thursday were Dusseldorf, Nuremberg, Erfurt-Weimar and Dortmund, according to Ralph Beisel, chief executive of the ADV airport association.

The airports’ websites were temporarily down, but are up and running again as of Friday. The websites of Germany’s biggest airports in Frankfurt, Munich and Berlin were not targeted.

# Active Attacks

- Masquerade/Spoofing
  - One entity pretends to be another to deceive others
  - Exploits human vulnerability
- Common spoofing attacks include
  - Caller ID spoofing
    - For phone calls, showing false caller ID or number
  - Email address spoofing
    - Altering the sender information on email to trick recipients into thinking the message is from another source
  - Webpage spoofing
    - Creating a fake webpage that looks like the page for a legitimate business to trick users
      - into giving up credentials they use at legitimate site
      - into downloading materials from an alternative site

# Active Attacks

- Social Engineering
  - Using social skills to convince people to reveal information or permit access to resources
  - Can happen in person, or by email, phone, text, …
  - Examples
    - **Claim to be new employee**, manager's assistant, maintenance person, etc
    - Ask for assistance in accessing resource to complete an urgent task
      - I've lost my password and I have to finish this today …
      - My swipe card doesn't work/left at home …
    - **Tailgating** – follow another person closely, so that when they go into secure area you can also get in without providing appropriate credentials

# Active Attacks

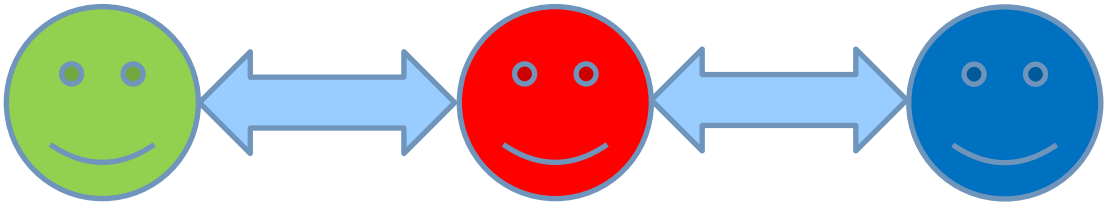
- Phishing
  - Usually involves
    - Spoofing (sender email address or caller ID, and/or web pages) + social engineering
  - Method used
    - Attacker initiates communication aimed at gaining information
      - Especially credentials to gain access to other resources
      - Example: account details, PIN number, password
    - Masquerades as a legitimate organisation you may have a relationship with (Bank, eBay, PayPal, Tax Office, Police, …)
    - Motivates user to respond urgently
      - With threat of penalty (Your account will be locked … )
      - Or promises of reward (First X replies gain a $$$ credit … )

# Active Attacks

- Man-in-the-Middle Attack (MITM)

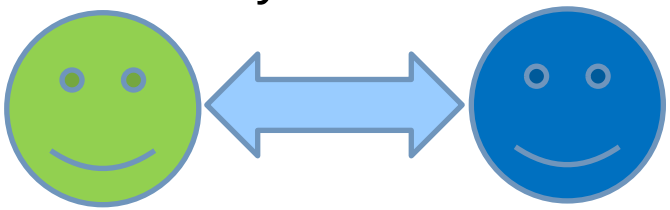
[Machine-in-the-Middle Attack (MITM)]

  - An attacker (Carol) positions themself between two entities who wish to communicate, say Alice and Bob.
  - Carol
    - pretends to Alice she is Bob and
    - pretends to Bob she is Alice (spoofing both ways)

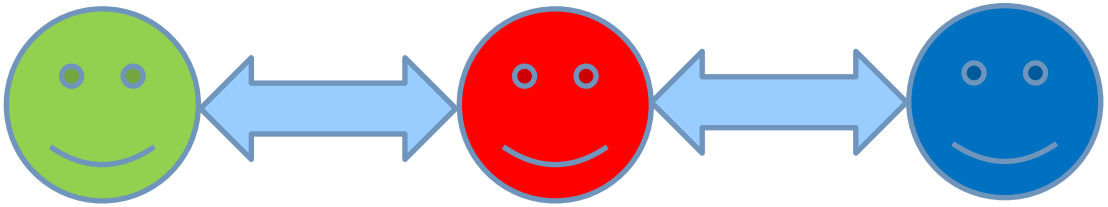


# Active Attacks

- MITM
  - Alice and Bob think they are communicating with each other:



  - **However** all messages between them go via Carol, so Carol can control the conversation
    - Could just monitor conversation (breaches confidentiality)
    - Can also insert or modify information (breach integrity)
    - Could even delete messages, prevent delivery (breach availability)



# Active Attacks

- MITM
  - Vulnerability: no authentication of the communicating endpoints
    - That is, you assume that the entity you are communicating with is who they say they are
    - But you do not have any check in place to be sure they are
  - A threat actor can exploit this vulnerability

# Active Attacks

- Replay attack
  - A valid data transmission is captured (recorded), stored and retransmitted at a later time
  - Example
    - Access to a system requires use of password, but password is encrypted during transmission
    - Attacker records encrypted password, and replays this information at another time to gain access
    - Doesn’t matter that attacker doesn’t know the password – they can provide the expected credential on request

# Case study: Ransomware

- Threat
  - Access to information system (phone/computer/network) will be restricted OR
  - Confidential data will be published (OR BOTH)
    - Restriction lifted upon payment of ransom
    - Examples: Cryptolocker, Locky, WannaCry – files encrypted
      - Pay fees to attacker to obtain the decryption key
- Vulnerability
  - People (if introduced by phishing email), processes
- Attack
  - Active or passive? Consider interactions and intent
- Control measures?

# Case study: Ransomware

- REvil ransomware to blame for UnitingCare Queensland's April attack | ZDNet
- May 2021
- Affected UnitingCare systems
  - Hospitals
  - Aged care centres
- Threat actor: Revil
  - Ransomware Evil
  - Ransomware-as-a-Service
- Cybercriminals – interested in obtaining ransom payment $$$
- Allegedly targeted other organisations
  - May 2021 - JBS Meat processing company

**REvil ransomware to blame for UnitingCare Queensland's April attack**

The healthcare organisation has confirmed the cyber incident it experienced last month was the result of a hit from REvil ransomware.

By Asha Barbaschow | May 5, 2021 -- 22:54 GMT (08:54 AEST) | Topic: Security

Image: Getty Images

After revealing late last month it had fallen victim to a cyber incident, UnitingCare Queensland has now named REvil/Sodin as the gang behind the attack.

The organisation, which provides aged care, disability supports, health care, and crisis response services throughout the state, suffered the attack on Sunday, 25 April 2021.

In a statement issued a few days later, UnitingCare said its systems were still hurting. On Wednesday, it said some of the organisation's systems have since been inaccessible.

The organisation also pointed the blame at REvil/Sodin as the source of the attack.

"We can confirm that the external group claiming responsibility for this incident has identified themselves as REvil/Sodin," it said.

MORE FROM ASHA BARBASCHOW

Innovation
RMIT partners with Intel and AARNet for new AWS cloud supercomputing facility

Security
ANAO: Auditing not driving improvements in Commonwealth cybersecurity adherence

Finance
Australia's largest bank accuses Apple of leaning on its market power

Innovation
Australia hears case for open access to Apple NFC tech as QR codes will not do

NEWSLETTERS

ZDNet Security
Your weekly update on security around the globe.

# Summary

- For information assets and their support systems
  - Many threats and many existing vulnerabilities
- If threats & vulnerabilities coincide security incidents occur
  - Result in breaches of C, I, A
  - Called attacks if deliberate human action is involved
    - Lots of different types, lots of different targets
  - Severity of impact depends on
    - Value and criticality of asset
    - Degree of compromise
    - Perspective
- Incidents may happen in isolation, or may be part of a chain of events
- Consequences can be devastating for orgs & individuals