COS80013 Internet Security

Week 2

Presented by Dr Rory Coulter

10 March 2025

SWINBURNE UNIVERSITY OF TECHNOLOGY

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.

Week 1 Recap

Key topics and theories

Recap

Information Security: Information assets

ICT Security: Secure access, storage, transmission and manipulation of information

Cyber Security: Information assets and non-information assets

CIA is a well established concept to approach cyber security

MITRE ATT&CK: Framework outlining the tactic, techniques and procedures of adversaries

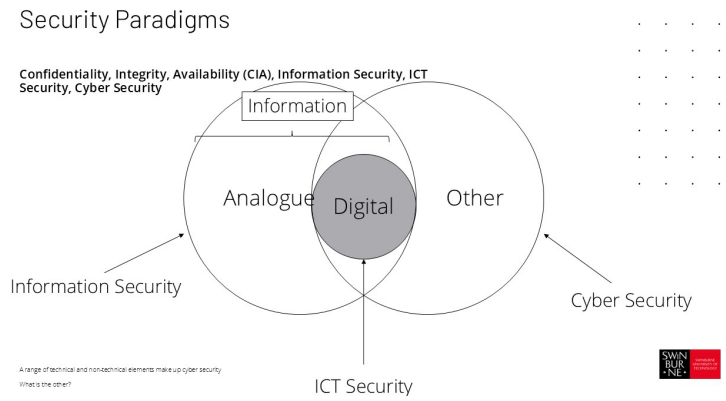
Risk: Drives cyber security

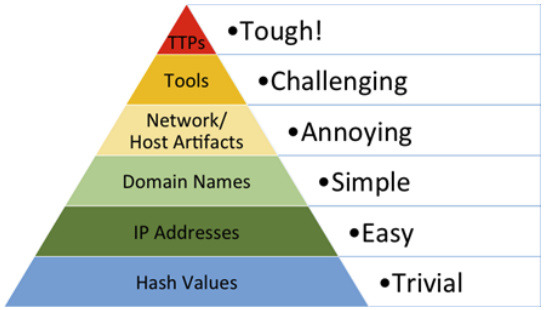
Further Reading

Cyber Kill Chain: Similar to MITRE ATT&CK, steps adversary must take to achieve aims

ACSC Most common TTPs

Cybersecurity Framework | NIST: Operational approach to cyber security





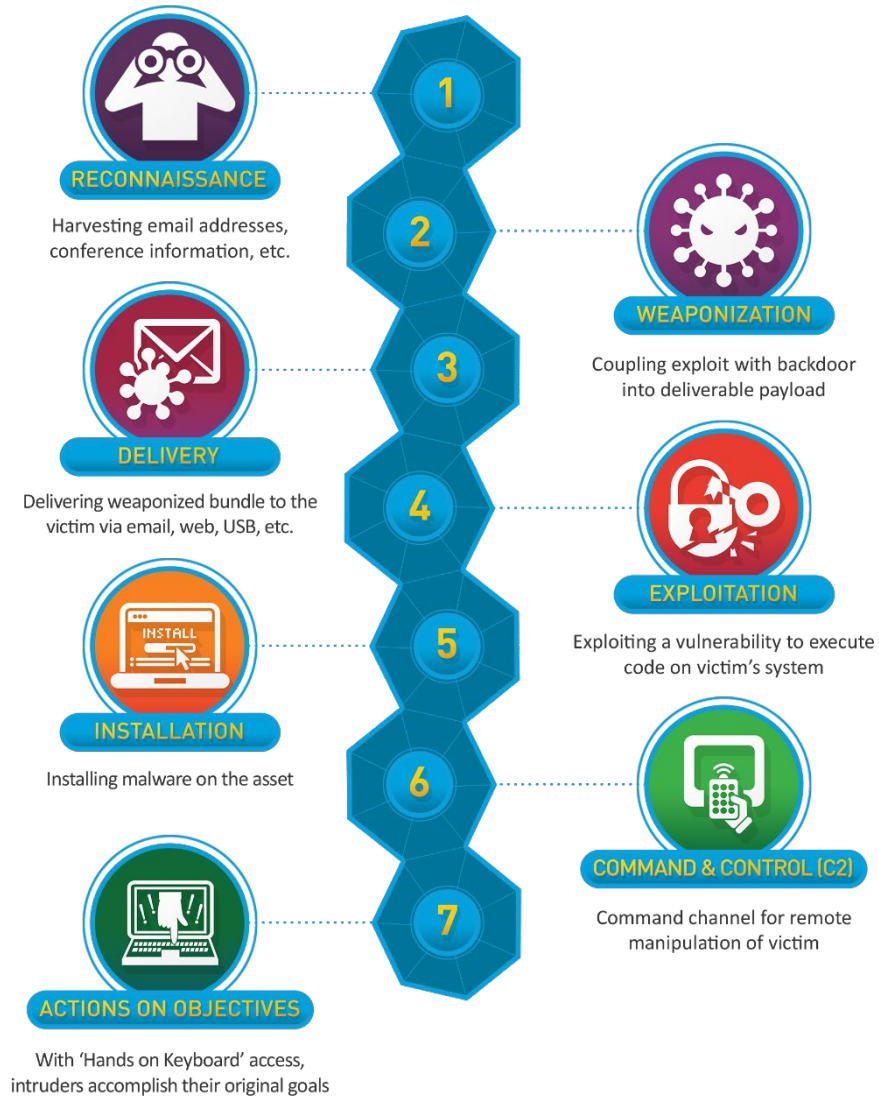
See: https://www.cyber.gov.au/about-us/advisories/summary-tactics-techniques-and-procedures-used-target-australian-networks

https://www.nist.gov/cyberframework

Cyber Kill Chain

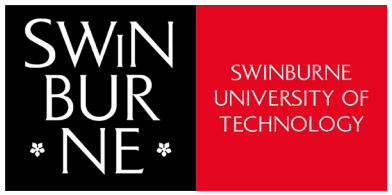
Pre-MITRE ATT&CK

Path, steps, or objectives an adversary must take to achieve their aims



SOURCE: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Offensive & Defensive Security

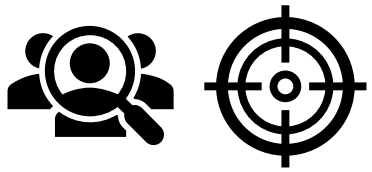


Offensive vs Defensive Security

Ultimately organisations favour defensive security over active probing production systems, but require a mixture

Understand the concepts

- Offensive
- Proactive approach to identify weakness, vulnerabilities
- Penetration tests***, mimic
- Active



- Defensive
- Preventative measures
- Detect incidents
- Passive

*** Very common for audit purposes

SWINBURNE UNIVERSITY OF TECHNOLOGY

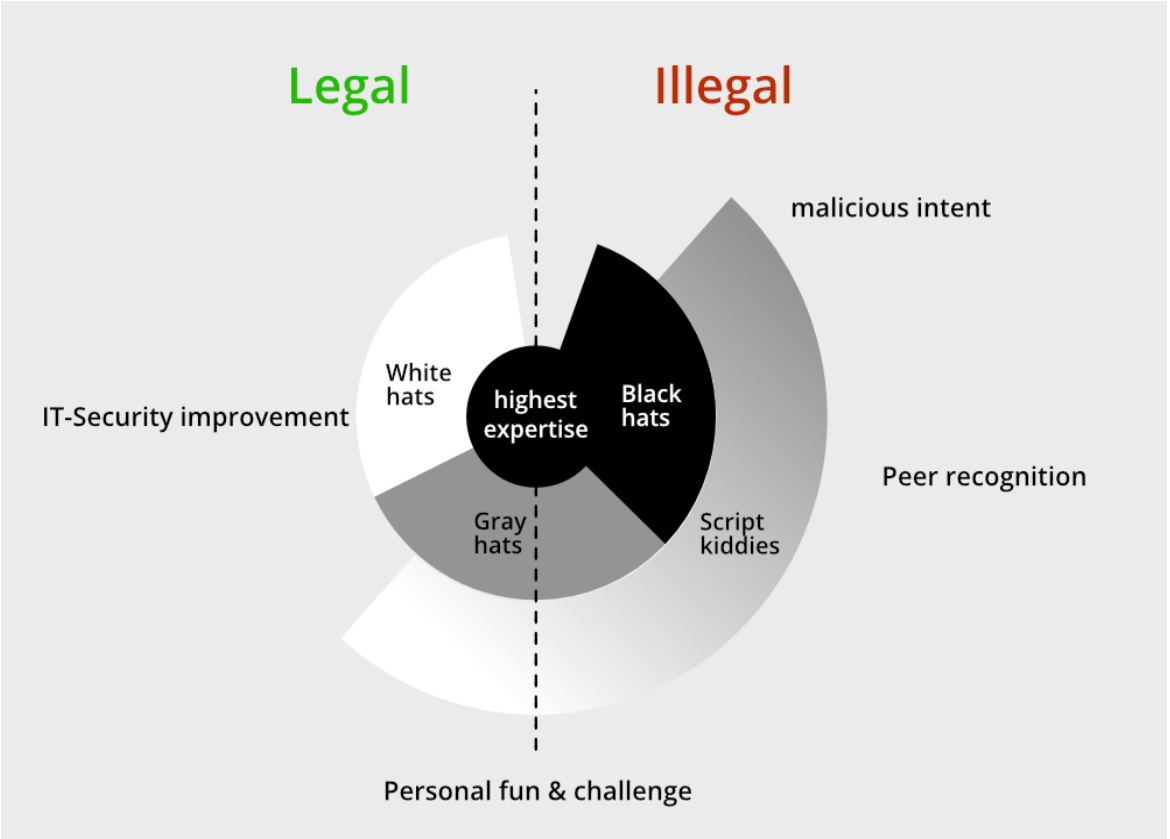
Player Recap

Broad Perspective(s)

Apposing sides defined by legality

Good intentions don't justify the action

Perspective 1	Perspective 2	Action
Patch	Exploit	Scan vulnerability
Report	Catalogue	Scan vulnerability
Automation/ administration	Persistence	Schedule task
Expose	Ransom	Website defacement
Expose	Ransom	Data leak

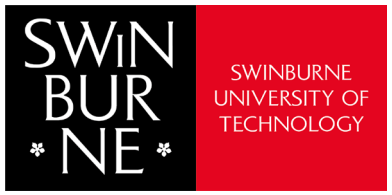


SOURCE: https://www.geeksforgeeks.org/what-are-white-hat-gray-hat-and-black-hat-hackers/

SWINBURNE UNIVERSITY OF TECHNOLOGY

Physical & Converged Security, Authentication, Human Weakness

Physical Security



Physical Security

Physical security refers to the measures taken to protect physical assets, such as people, property, and resources, from unauthorised access, theft, damage, or harm

Physical security framework is made up of three main components:

- Access Control
- Surveillance
- Testing

Protection of people, space/dwelling, equipment, inventory, or information

The success of an organisation's physical security program can often be attributed to how well each of these components is implemented, improved, and maintained

SWINBURNE UNIVERSITY OF TECHNOLOGY

Physical Security Importance

Enables expected protection

Reputation management : protect a company's reputation by preventing incidents that could damage its image

Compliance with regulations : banks and financial institutions are required to have certain security measures in place to protect customer information

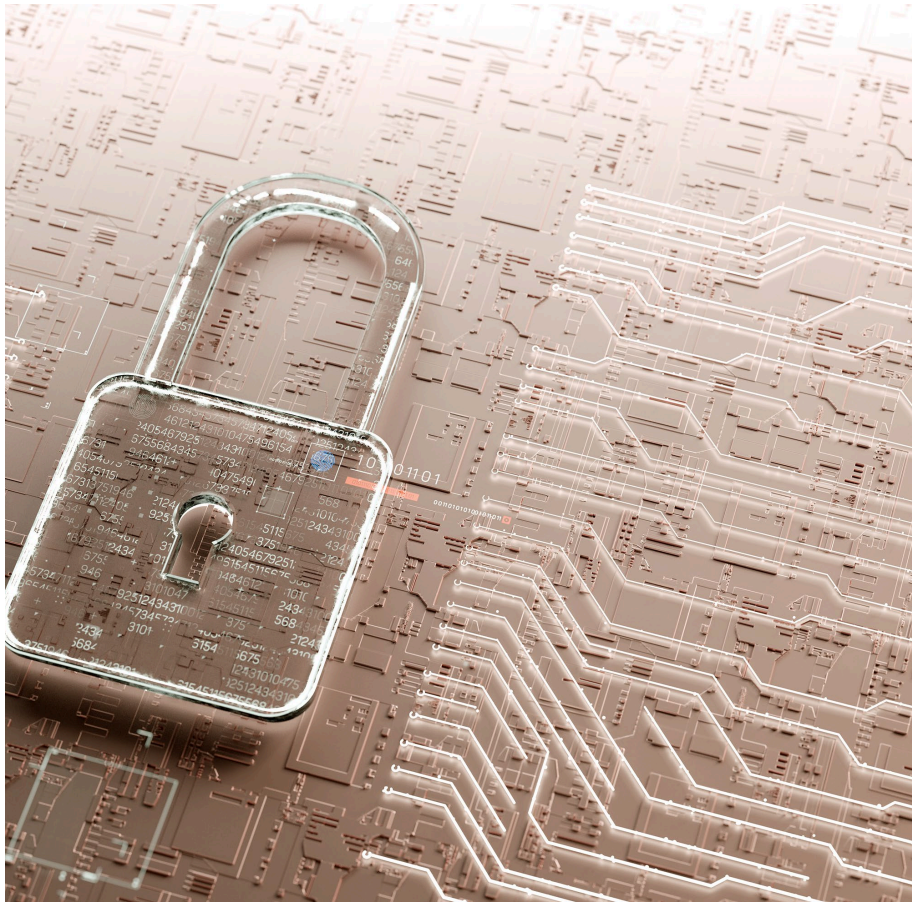
Perimeter Barriers: Physical barriers such as walls, fences, and gates can be used to prevent unauthorised access to a facility or area. They can also be used to control the flow of people and vehicles entering and exiting a site.

Security Personnel: Security personnel such as guards, patrols or on-site officers can provide a physical presence to deter potential intruders, respond to security incidents, and monitor activity in and around a facility

Alarm Systems: Alarm systems can be used to detect and alert security personnel to potential security breaches. These can include burglar alarms, fire alarms, and motion sensors

Regular audits: All security checks should be regularly audited to ensure that everything is working as expected.

Incident Response: The organisation should be prepared to handle incidents to ensure a rapid, organised and effective response



SWINBURNE UNIVERSITY OF TECHNOLOGY

Access Control

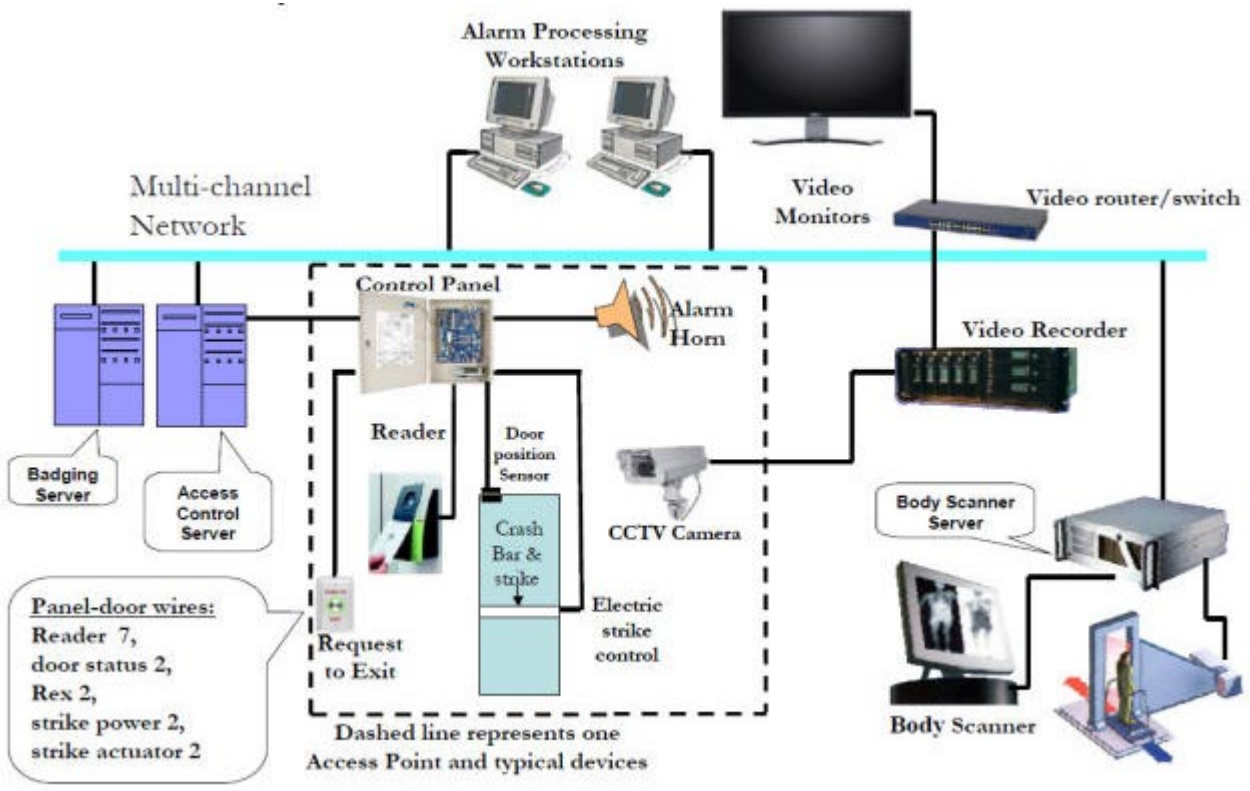
Limit and control what people have access to sites, facilities, and materials

Access controls include measures taken to limit access to certain assets to authorised personnel only

- More complex access controls involve methods of technology support

- ID Cards
- Card Readers
- Biometric Readers
- Locks
- Etc.

- Electronic controls allow for audit and logging



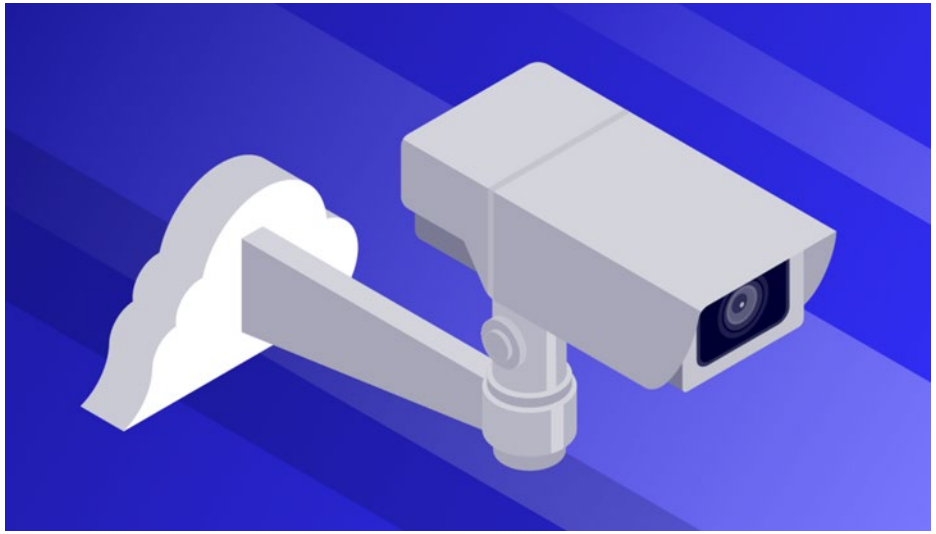
Access Control System Overview

Surveillance

Technology, people, and resources that organisations use to monitor the activities of different real-world locations and facilities

Common physical security component

- E.g. CCTV
- Activity across a range of time



SWINBURNE UNIVERSITY OF TECHNOLOGY

Testing

Disaster recovery policies and procedures are effective when proactive testing is employed

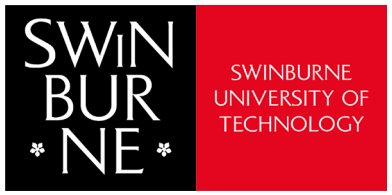
Testing is increasingly important, especially when it comes to the uniformity

- Rehearse incidents, prepare for the real thing
- Identify issues and gaps
- Improve and review in line with strategic aims

Common across many cyber areas

SWINBURNE UNIVERSITY OF TECHNOLOGY

Converged Security

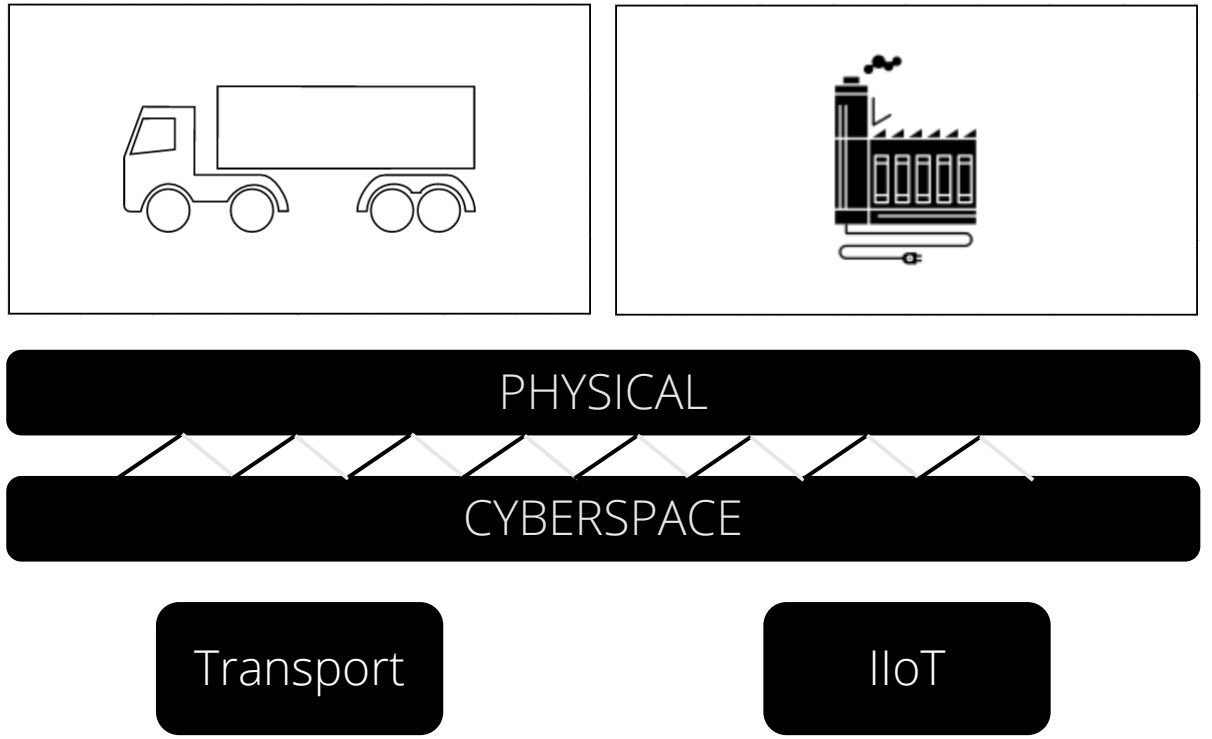


Physical Meets Cyber

Cyber Physical System

A few examples:

- Interconnection of physical and software
- Mechanism controlled by an algorithm
- Embedded and IoT (think connectivity), but to a greater degree
- Smart Grid, autonomous automobile, digital (autonomous) aviation



SWINBURNE UNIVERSITY OF TECHNOLOGY

Converged Security Overview

Example: Attacks from one domain to another

Domain 1: A gap in control anomaly detection allows a cyber attack to halt energy production, resulting in loss of power, potential physical loss of life (medical, transport), theft (security systems)

Domain 2: A gap in access controls allows a commercial printing services allows attackers to compromise kiosk and access to internal networks

SWINBURNE UNIVERSITY OF TECHNOLOGY

Converged Security Overview (Continued)

Security functions operating separately

Management lack visibility and oversight

Possible counterproductive decision making

Decision making alerting process potentially interrupted

SWINBURNE UNIVERSITY OF TECHNOLOGY

Converged Security Overview (Continued)

Risks

Typically:

Physical world: Potentially to get caught and spotted

Digital World: Easy to blend in with noise

Biggest threat type: Insiders

Converged:

Physical + Digital: Better blend of controls

Biggest threat type: Insiders

SWINBURNE UNIVERSITY OF TECHNOLOGY

Converged Security

Case Study

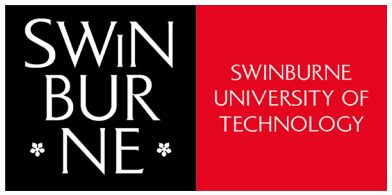
How to rob a casino

- Has anyone ever walked in the front door and gotten away with it?
- Occasionally yes, these things do happen, possibly a breakdown between physical and cyber systems?

- Why go in through the front door, why not through the fish tank?

IMAGE SOURCE: https://filmthreat.com/features/ranking-the-oceans-movies-from-worst-to-best/
https://www.hackread.com/hackers-casinos-fish-tank-smart-thermometer-hack/

Access Controls



Discretionary access control (DAC)

Allows the owner of a resource to control access to that resource and what level of access they are granted

- Access control list (ACL) is a
- List of users or groups who have been granted access to the resource and their corresponding level of access
- Examples ACLs in Windows, Linux: Assumes everyone who has permission exercises it responsibly
- Advantage :
  - simplicity , flexibility
- Limitations
  - not provide any protection against users who abuse their access privileges
  - difficult to manage ACL for large systems with many resources and users

SWINBURNE UNIVERSITY OF TECHNOLOGY

Mandatory access control (MAC)

Access to resources is determined by a security policy that is enforced by the operating system or security software

Every resource (files, folders, and devices) is assigned a security label or classification that indicates the sensitivity or importance of the resource

- The security policy defines the rules for how access is granted based on the labels assigned to resources and users
- Example – SE Linux
  - Assumes no-one who has access can be trusted to exercise it responsibly
- Even root can have no authority
- Advantages:
  - provides a higher level of protection against unauthorised access
  - reduces the risk of accidental data leaks or breaches
- Limitations
  - more complex and difficult to manage than DAC
  - security policy must be carefully designed and maintained

SWINBURNE UNIVERSITY OF TECHNOLOGY

Role-based access control (RBAC)

Provides access based on the roles and responsibilities of users within an organisation

Users can be assigned to multiple roles, each with a different set of permissions

- Users can be assigned to multiple roles, each with a different set of permissions
- These roles are based on the user's job function, responsibilities, and level of authority within the organisation
- Advantages:
  - simplifies the management of access control (central control)
  - more secure?

SWINBURNE UNIVERSITY OF TECHNOLOGY

Attribute-based access control (ABAC)

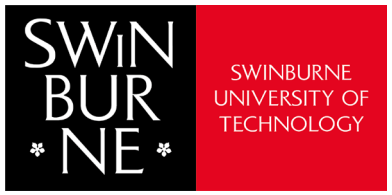
Grants access to resources based on a set of attributes associated with users, resources, and the environment

Attributes associated with a user or resource can include a wide range of factors such as time of day, location, device type , sensitivity of the data

- Advantages:
  - flexible
  - granular
- Limitations
  - more complex to manage than other access control models
  - it requires a well-defined attribute-based policy and a system for collecting and managing the attributes associated with users and resources

SWINBURNE UNIVERSITY OF TECHNOLOGY

Authentication



Authentication

Verifying the identity of a user, process, or device, often as required to allow access to systems, resources in an information system

Maintain confidentiality

- Authentication is critical in preventing unauthorised access to:
  - Data
  - Systems
  - Resources
  - Applications
- Can lead to system impact, data breaches, financial loss, and reputational damage if breached
- Authentication requires
  - Identity
  - Secret

- User identity and secret is shared to system to authenticate to
  - Password-based authentication is the predominate method for authentication
- Identity and password are passed, password is looked up in table for authenticate*
- Users re-use passwords
- Obtain the password list, adversaries can look up or try to match the password hash

Assuming a hash-based scheme is employed

See top 10000 passwords: https://en.wikipedia.org/wiki/Wikipedia:10,000_most_common_passwords

SWINBURNE UNIVERSITY OF TECHNOLOGY

Word List & Rainbow Tables

An adversary only needs to guess or compare exposed password hashes

Two key methods

- Word list
- A list of words to pass with identity to guess password
- Rainbow table
- Table of hashed passwords to look up
- Considering MITRE TTPs at a very high and non-exhaustive level, multiple types of password-based attacks
- See Credential Access
- The adversary is trying to steal account names and passwords
- https://attack.mitre.org/tactics/TA0006/

TECHNIQUES

- **Brute Force**
  - Password Guessing
  - Password Cracking
  - Password Spraying
  - Credential Stuffing
- Credentials from Password Stores
  - Keychain
  - Securityd Memory
  - Credentials from Web Browsers
  - Windows Credential Manager
  - Password Managers

11111	a	21111	cliche	31111	gee	41111	loom	51111	qu	61111	thea
11112	a&p	21112	click	31112	geese	41112	loon	51112	qua	61112	thee
11113	a's	21113	cliff	31113	geigy	41113	loop	51113	quack	61113	theft
11114	aa	21114	climb	31114	gel	41114	loose	51114	quad	61114	their
11115	aaa	21115	clime	31115	geld	41115	loot	51115	quaff	61115	them
11116	aaaa	21116	cling	31116	gem	41116	lop	51116	quail	61116	theme
11121	aaron	21121	clink	31121	gemma	41121	lope	51121	quake	61121	then
11122	ab	21122	clint	31122	gene	41122	lopez	51122	qualm	61122	there
11123	aba	21123	clio	31123	genie	41123	lord	51123	quark	61123	these
11124	ababa	21124	clip	31124	genii	41124	lore	51124	quarry	61124	theta
11125	aback	21125	clive	31125	genoa	41125	loren	51125	quart	61125	they
11126	abase	21126	cloak	31126	genre	41126	los	51126	quash	61126	thick
11131	abash	21131	clock	31131	gent	41131	lose	51131	quasi	61131	thief
11132	abate	21132	clod	31132	gentry	41132	loss	51132	quay	61132	thigh
11133	abbas	21133	clog	31133	genus	41133	lossy	51133	queasy	61133	thin
11134	abbe	21134	clomp	31134	gerbil	41134	lost	51134	queen	61134	thine
11135	abbey	21135	clone	31135	germ	41135	lot	51135	queer	61135	thing
11136	abbot	21136	close	31136	gerry	41136	lotte	51136	quell	61136	think
11141	abbott	21141	closet	31141	get	41141	lotus	51141	query	61141	third
11142	abc	21142	clot	31142	getty	41142	lou	51142	quest	61142	this
11143	abe	21143	cloth	31143	gf	41143	loud	51143	queue	61143	thong
11144	abed	21144	cloud	31144	gg	41144	louis	51144	quick	61144	thor
11145	abel	21145	clout	31145	ggg	41145	louise	51145	quid	61145	thorn
11146	abet	21146	clove	31146	gggg	41146	louse	51146	quiet	61146	thorny
11151	abide	21151	clown	31151	gh	41151	lousy	51151	quill	61151	those
11152	abject	21152	cloy	31152	ghana	41152	louver	51152	quilt	61152	thou
11153	ablaze	21153	club	31153	ghent	41153	love	51153	quinn	61153	thread
11154	able	21154	cluck	31154	ghetto	41154	low	51154	quint	61154	three
11155	abner	21155	clue	31155	ghi	41155	lowe	51155	quip	61155	threw
11156	abo	21156	cluj	31156	ghost	41156	lower	51156	quirk	61156	throb
11161	abode	21161	clump	31161	ghoul	41161	lowry	51161	quirt	61161	throes
11162	abort	21162	clumsy	31162	gi	41162	loy	51162	quit	61162	throw
11163	about	21163	clung	31163	giant	41163	loyal	51163	quite	61163	thrum
11164	above	21164	clyde	31164	gibbs	41164	lp	51164	quito	61164	thud
11165	abrade	21165	cm	31165	gibby	41165	lq	51165	quiz	61165	thug
11166	abram	21166	cn	31166	gibe	41166	lr	51166	quo	61166	thule
11211	absorb	21211	co	31211	giddy	41211	ls	51211	quod	61211	thumb
11212	abuse	21212	coach	31212	gift	41212	lsi	51212	quota	61212	thump
11213	abut	21213	coal	31213	gig	41213	lt	51213	quote	61213	thus
11214	abyss	21214	coast	31214	gil	41214	ltv	51214	qv	61214	thy
11215	ac	21215	coat	31215	gila	41215	lu	51215	qw	61215	thyme
11216	acadia	21216	coax	31216	gild	41216	lucas	51216	qx	61216	ti

User	Password
Stephen	auhsoJ
Lisa	hsifdrowS
James	1010NO1Z
Harry	sinocarD tupaC
Sarah	auhsoJ

User	Password Hash
Stephen	39e717cd3f5c4be78d97090c69f4e655
Lisa	f567c40623df407ba980bfad6dff5982
James	711f1f88006a48859616c3a5cbcc0377
Harry	fb74376102a049b9a7c5529784763c53
Sarah	39e717cd3f5c4be78d97090c69f4e655

User	Random Salt	Password Hash
Stephen	06917d7ed65c466fa180a6fb62313ab9	b65578786e544b6da70c3a9856cdb750
Lisa	51f2e43105164729bb46e7f20091adf8	2964e639aa7d457c8ec0358756cbffd9
James	fea659115b7541479c1f956a59f7ad2f	dd9e4cd20f134dda87f6ac771c48616f
Harry	30ebf72072134f1bb40faa8949db6e85	204767673a8d4fa9a7542ebc3eceb3a2
Sarah	711f51082ea84d949f6e3efecf29f270	e3afb27d59a34782b6b4baa0c37e2958

IMAGE SOURCE: https://www.thesecurityblogger.com/understanding-rainbow-tables/

https://latesthackingnews.com/amp/2016/10/30/generate-truly-random-yet-easy-remember-passwo

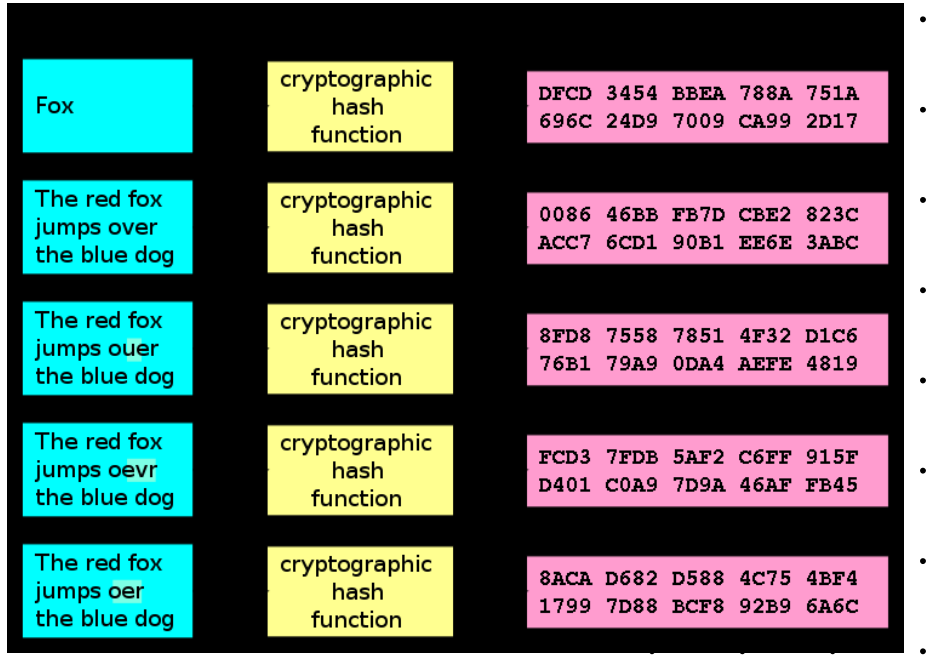
SWINBURNE UNIVERSITY OF TECHNOLOGY

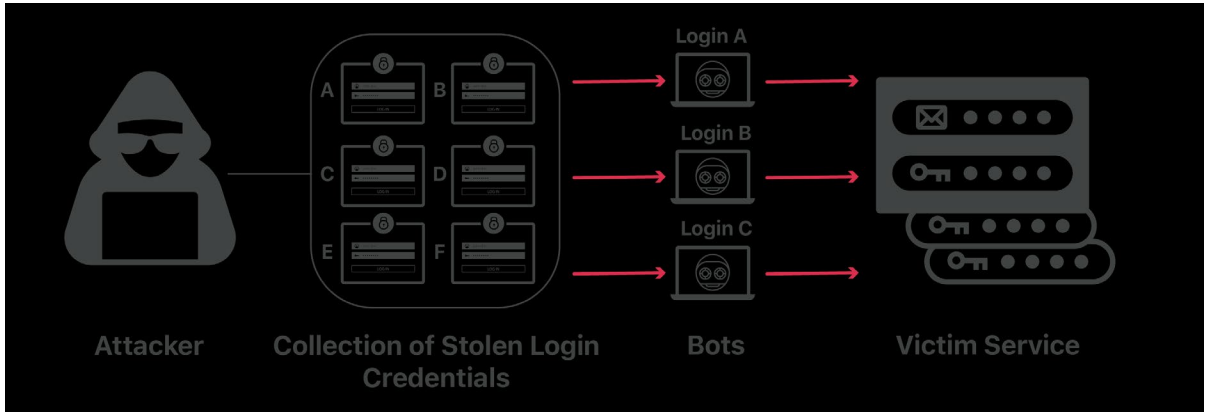
Password Attacks

Brute Force: T1110

Just a single technique and sub-techniques

Technique	Name	Details
T1110.001	Password Guessing	Guess password in attempt to login into account
T1110.002	Password Cracking	Try to crack or recover passwords, when pass the hash is not applicable*
T1110.003	Password Spraying	Single or small list of passwords across a range of accounts
T1110.003	Credential Stuffing	Using credentials obtained from data breach





Credential hashes are passed to authenticate

IMAGE SOURCE:

https://medium.com/@cmcorrales3/password-hashes-how-they-work-how-theyre-hacked-and-how-to-maximize-security-e04b15ed98d

https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/

SWINBURNE UNIVERSITY OF TECHNOLOGY

Other Authentication Methods

Non-Exhaustive List

Other methods and factors

- Certificate-based authentication
- Biometric authentication: e.g., fingerprint
- Token-based authentication: time-based one-time PIN (TOTP), reset every n seconds
- One-time password: generated for a specific login
- Push notification: approve or deny request
- Voice authentication
- Multifactor authentication
  - Something you know
  - Something you have
  - Something you are

Which are secure?

SWINBURNE UNIVERSITY OF TECHNOLOGY

Social Engineering, Phishing

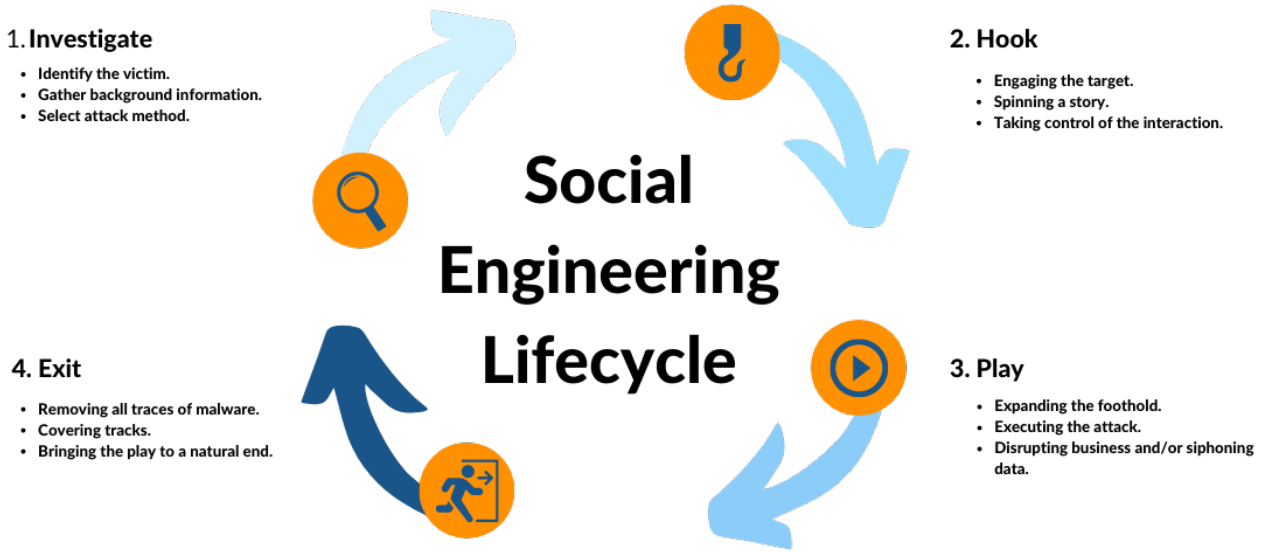
SWINBURNE UNIVERSITY OF TECHNOLOGY

Social Engineering

Manipulation of individuals in seeking action or the release (divulging) of sensitive information

Influence over another which is not in their best interest

- Information gathering
- Engaging with victim
- Attacking
- Closing interaction



SWINBURNE UNIVERSITY OF TECHNOLOGY

Social Engineering Forms

Some but not all

- Baiting: Like phishing, but using different items to lure victims (think free stuff for example)
- Dumpster diving: Physically sorting through rubbish
- Pretexting: Providing background or pretending to be another
- Phishing: Baiting with fake links to fake resources for
- Pharming: DNS level redirection to fake resources
- Reconnaissance: Information gathering
- Surveillance: Observing
- Shoulder surfing: Watching over someone's shoulder for information or passwords
- Tailgating: Trick employees to open doors for attackers

SET: Social Engineering Toolkit, open-source pen test framework geared for social engineering bundled within Kali Linux

SWINBURNE UNIVERSITY OF TECHNOLOGY

Key Takeaways

Humans are the weak element

Technology will work as configured

- Many security system are rule or pattern based
  - These will operate as configured, or misconfigured

- Humans are susceptible to phishing and social engineering attacks
  - Scams are continuously successful

He could be getting scammed/phished right now

SWINBURNE UNIVERSITY OF TECHNOLOGY

Phishing and Pharming

SWINBURNE UNIVERSITY OF TECHNOLOGY

Phishing [T1566]

“convincing emails or other messages to trick us into opening harmful links or downloading malicious software”

Attempted technique use to

Often obtain sensitive data, disclosure by deception

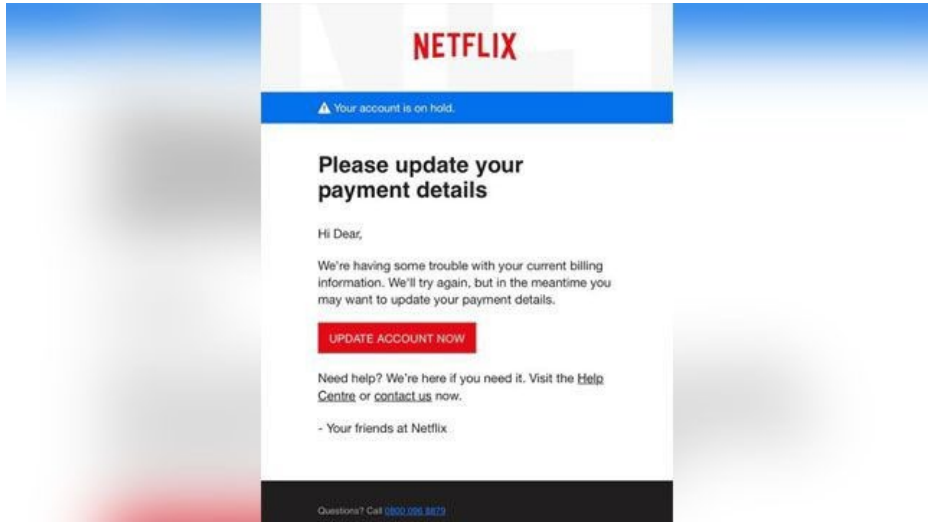
Offensive and passive in nature (just concepts to conceive actions of an adversary)

What is promised

- Fame
- Fortune
- Medication
- Romance

Characteristics:

- Poor spelling/grammar/punctuation
- Randomly generated-text
- Replica of legitimate service or communication



SOURCE: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing, https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

SWINBURNE UNIVERSITY OF TECHNOLOGY

Phishing (cont.)

Common examples

- Phishing: General, bulk in nature
- Spearphishing: Limited receipting, targeted
- Whaling: High profile targets
- Vishing: Calls made over IP
- Smishing: Messages sent to recipients via phone
- Watering hole attack: Set a fake/malicious website or service

These examples see an adversary making use of their own infrastructure* or “cold calling”

*Loosely

SWINBURNE UNIVERSITY OF TECHNOLOGY

Business Email Compromise (BEC)

Targeted phishing or spearphishing

Relationships are key in the success of phishing

- The relationship my introduce other characteristics:
- Pressure
- Time or financial sensitivities

Adversaries seek to leverage these with BEC

Emails are used to masquerade as business representatives

- Compromised accounts of employees
- Request payment through invoice
- Request change of details
- Request direct communication

External accounts can also be used, more time in preparing and grooming target

SWINBURNE UNIVERSITY OF TECHNOLOGY

Pharming

Two steps process to direct users to fraudulent/malicious websites and harvest information or credentials

Exploitation of DNS protocol

Malware-based methods:

- Malware is downloaded and installed
- User connections are re-directed to pharming site
- Credentials and information are farmed

DNS-based methods:

- Incorrect IP is returned which sends victim to pharming site
- DNS servers are poisoned via tables or caching

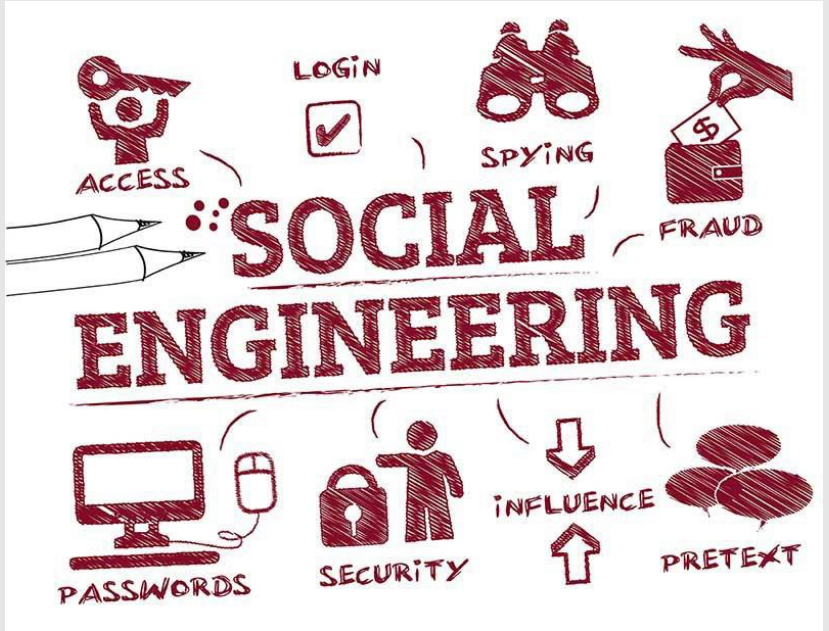
Can also consider compromised server has malicious code inserted which directs targets to spoofed website

SWINBURNE UNIVERSITY OF TECHNOLOGY

Social Engineering

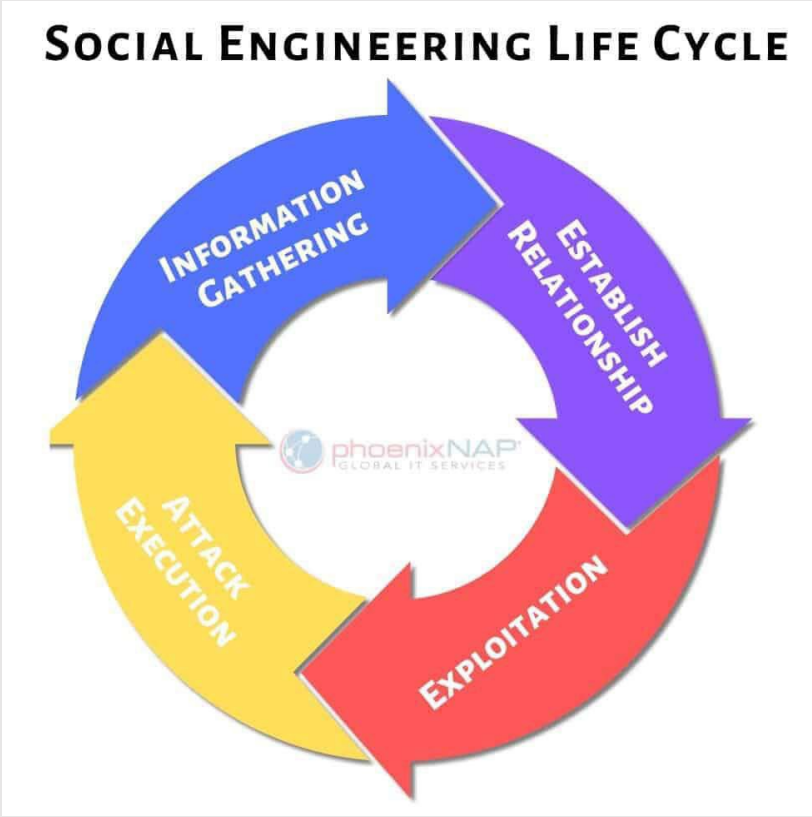
Social Engineering

- Social Engineering is a component of the attack in nearly 1 of 3 successful data breaches
- Manipulation of individuals in seeking action or the release (divulging) of sensitive information
- Influence over another which is not in their best interest



Life Cycle of Social Engineering

- Information gathering
- Engaging with victim
- Attacking
- Closing interaction



SWINBURNE UNIVERSITY OF TECHNOLOGY

Types

Baiting: Like phishing, but using different items to lure victims
Dumpster diving: Physically sorting through rubbish
Pretexting: Providing background or pretending to be another
Phishing: Baiting with fake links to fake resources
Pharming: DNS level redirection to fake resources
Reconnaissance: Information gathering
Surveillance: Observing
Shoulder surfing: Watching over someone's shoulder for information or passwords
Tailgating: Trick employees to open doors for attackers

SWINBURNE UNIVERSITY OF TECHNOLOGY

Baiting

- Similar to Phishing
- Different items used to entice victim
- Free music, movies, keygens, software…

Dumpster diving

- Attacker physically visits target's location and searches the rubbish to find useful information
- Financial paperwork
- User manuals (software, hardware)
- Used to support future pretexting attack

- https://youtu.be/c81NYcP2C0E

Pretexting

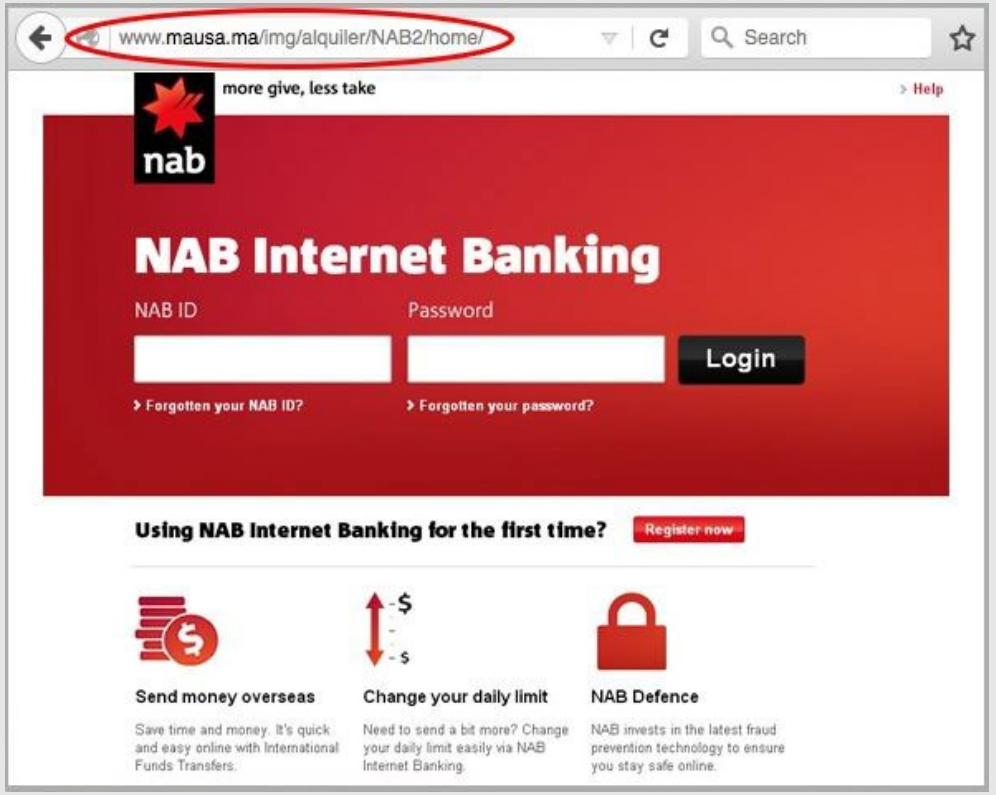
- **Defined as the practice of presenting oneself as someone else in order to obtain private information**
  - Good, compelling story
  - Fabricated scenario
  - Not a one-size fits all
    - Good targets: help desk, librarians

Phishing

- **Most phishing scams endeavour to accomplish three things:**
  - Obtain personal information
  - Redirect users to suspicious websites
  - Manipulate the user into responding quickly

Pharming

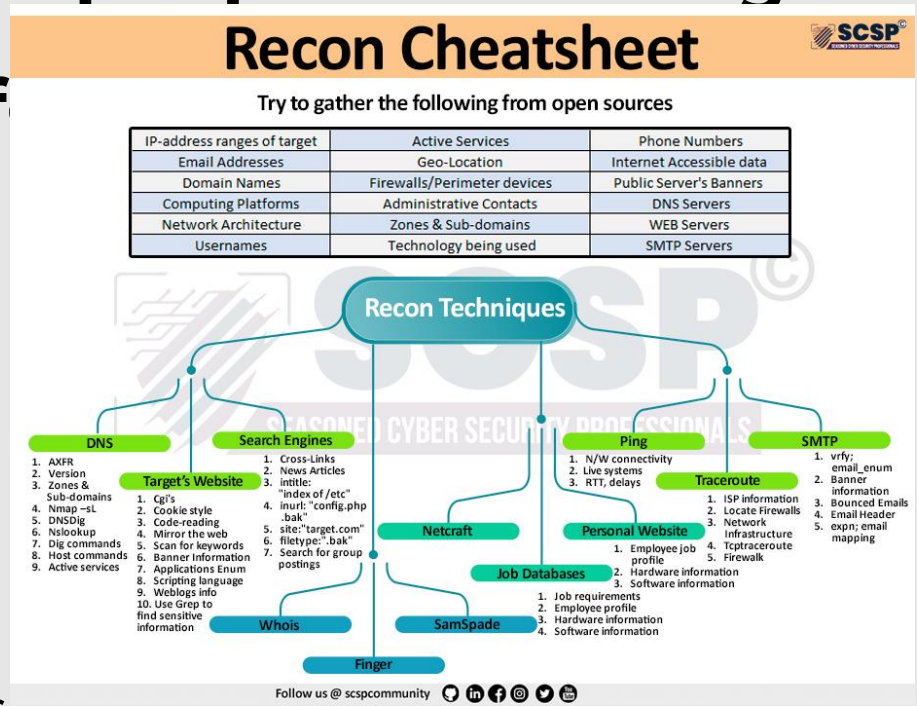
- **Setting up a fake web site which harvests user input**
  - Fake banking site
  - Uses current graphics, styles from real site
  - stores user name and password and then re-directs user to the real site
  - Fake anti-virus site (download "patches " containing malware)
  - Similar domain name to legitimate sites



SWINBURNE UNIVERSITY OF TECHNOLOGY

Reconnaissance

- **After enumerating the names of people in the Target premises, search social media f password reset info.**
  - Date of birth (age + birthday)
  - Names or relatives, pets
  - Car Rego
  - Password dumps from hacked sites



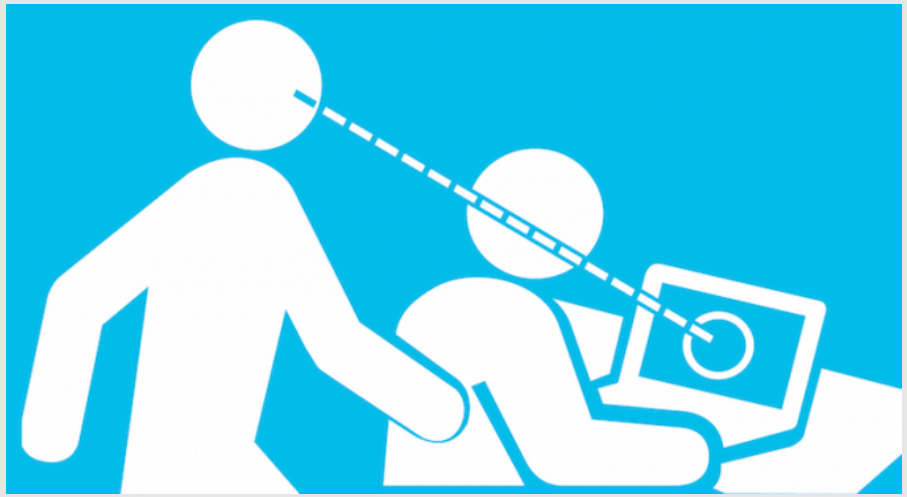
Surveillance

- **Google Earth**
- **Street View**
- **Surveillance cams**
  - http://mashable.com/2014/11/10/naked-security-webcams/
  - https://brinkshome.com/smartcenter/hacked-home-security-cameras-list
  - http://www.insecam.org/en/bycountry/AU/

SWINBURNE UNIVERSITY OF TECHNOLOGY

Shoulder Surfing

- After gaining entry to the target premises, attacker watches people logging on to their computers to get credentials



Tailgating

- Trick employees to open doors for attackers
- Existed in every organisation

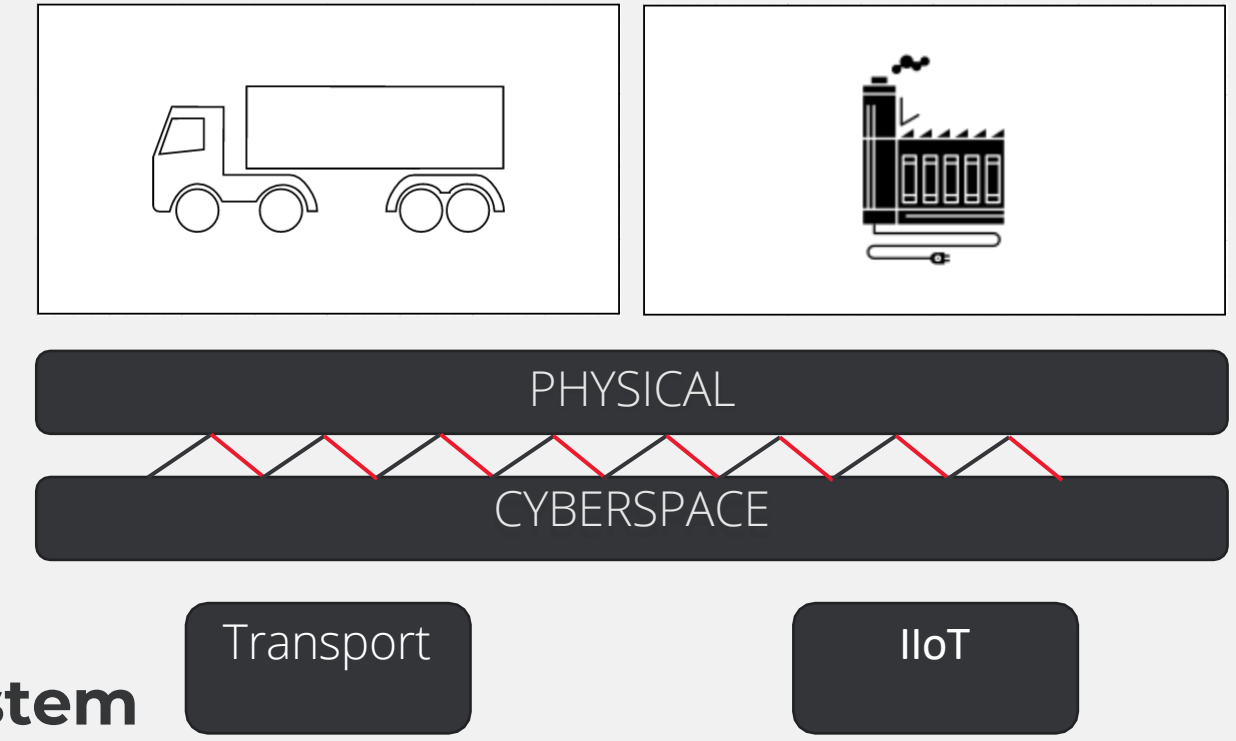
Helpful Tips - Defence

- Slow down
- Research the facts
- Don’t let a link be in control of where you land.
- Email hijacking is rampant
- Beware of any download
- Foreign offers are fake

SWINBURNE UNIVERSITY OF TECHNOLOGY

Converged Security

Converged Security Overview



Cyber Physical System

Interconnection of physical and software

Mechanism controlled by an algorithm

Similar to embedded and IoT (think connectivity), but to a greater degree

Smart Grid, autonomous automobile, digital (autonomous) aviation

SWINBURNE UNIVERSITY OF TECHNOLOGY

Converged Security Overview

Example: Attacks from one domain to another

A gap in control anomaly detection allows a cyber attack to halt energy production, resulting in loss of power, potential physical loss of life (medical, transport), theft (security systems)

A gap in access controls allows a commercial printing services allows attackers to compromise kiosk and access to internal networks

SWINBURNE UNIVERSITY OF TECHNOLOGY

Converged Security Overview

Security functions operating separately

Management lack visibility and oversight

Possible counterproductive decision making

Decision making alerting process potentially interrupted

SWINBURNE UNIVERSITY OF TECHNOLOGY

Risks

Typically:

Physical world: Potentially to get caught and spotted

Digital World: Easy to blend in with noise

Biggest threat type: Insiders

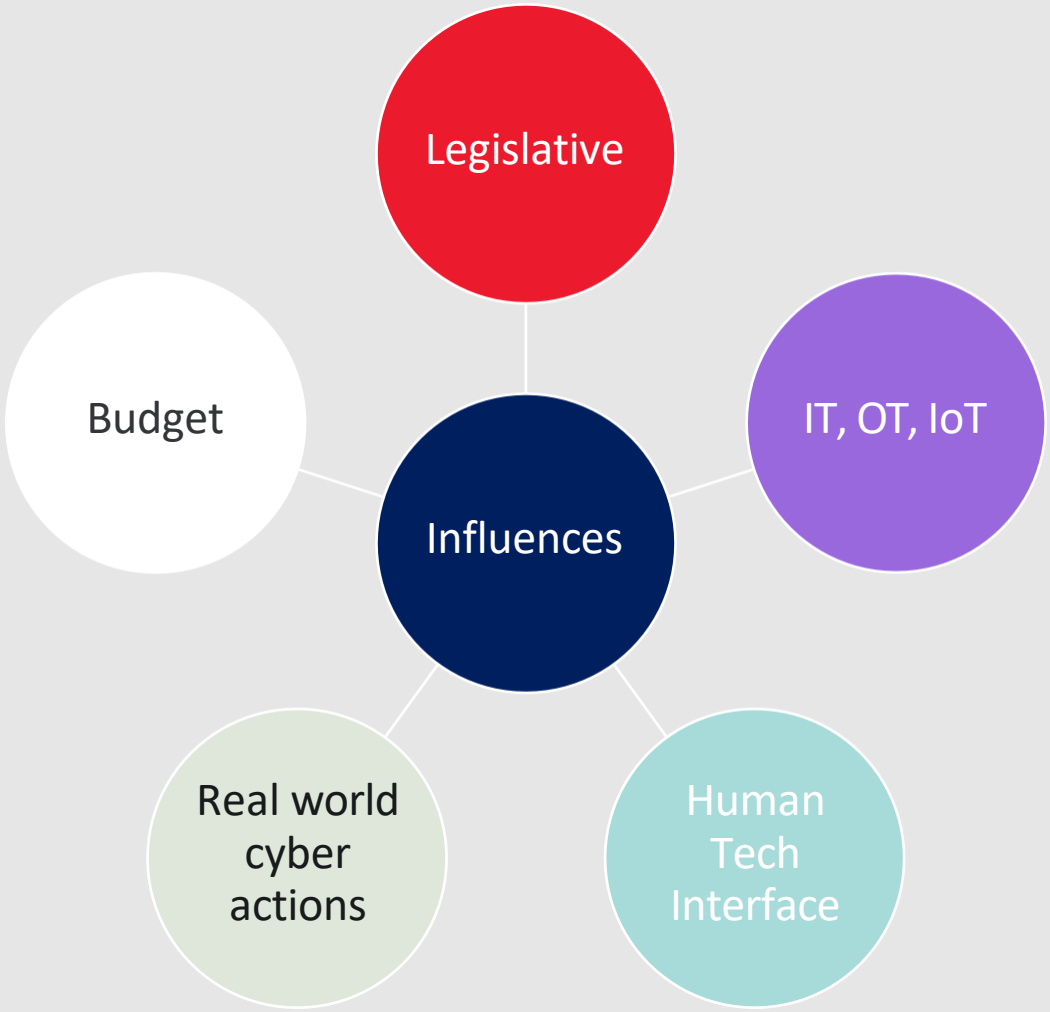
Converged:

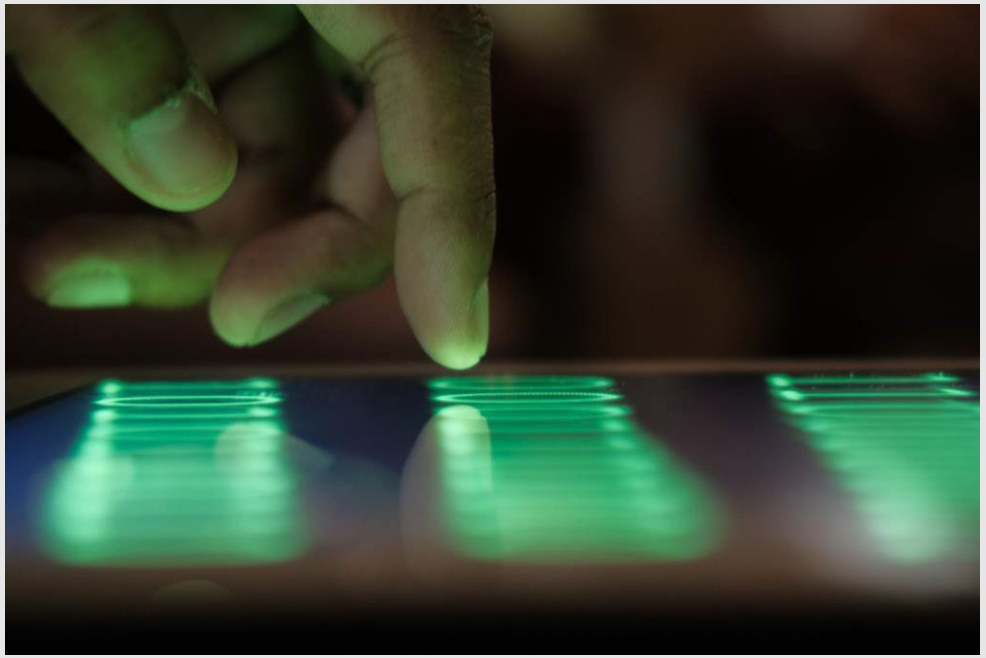
Physical + Digital: Better blend of controls

Biggest threat type: Insiders

SWINBURNE UNIVERSITY OF TECHNOLOGY

Influences


Legislative
Budget
IT, OT, IoT
Influences
Real world cyber actions
Human Tech Interface



Maturity

Domestically, maturity is low
US maturity is higher, leading the trend

Requires a re-shift of attitudes and large organisational change

Case Study

Internet connected fish tank:

thermometer connected to PC used to access internal casino network

Source: https://www.hackread.com/hackers-casinos-fish-tank-smart-thermometer-hack/

SWINBURNE UNIVERSITY OF TECHNOLOGY

Phishing and Pharming Attack

Phishing

- Dangling "bait" in front of a user.
  - Promise of riches/fame
  - Urgency (must act immediately)
  - Veiled threat (or your account will be locked)
  - Pay-off (your banking details, your money, your reputation)
- Characteristics
  - Poor spelling/grammar/punctuation
  - May contain randomly generated-text
  - From someone you don't know* … but…

SWINBURNE UNIVERSITY OF TECHNOLOGY

Spear-Phishing

- Phishing can be targeted to specific companies / groups / individuals.
- E-mails contain very relevant contents and are plausible.
- No poor grammar/spelling.
- Malicious attachments
  - RSA hack
  - Gh0st-NET

SWINBURNE UNIVERSITY OF TECHNOLOGY

More Phishing

❑ Whaling

- Spear-Phishing of CEOs and high profile victims.
- Public information easy to find.

❑ Watering-hole attacks

- Instead of phishing individuals, criminals target web sites and forums where potential spear-phishing victims meet.
- Infect the sites
- Infect the visitors or publish mis-information (spoofed links)

SWINBURNE UNIVERSITY OF TECHNOLOGY

Pharming – no bait needed

- The goal is the same as phishing – to steal your user name and password.
- Tools exist for duplicating a web site without the consent or access privileges if site administrator, so these sites are easy to set up.
- The user needs to look for inconsistencies in the appearance or behaviour of a site.
- Performing a ***traceroute*** on the domain name will pick up a change in the location of the spoofed site.
- Plug-ins like Certificate Patrol will detect changes in SSL certificates.

SWINBURNE UNIVERSITY OF TECHNOLOGY

Pharming

- Pharming involves setting up fake web sites that users will log into.
- **Cybersquatting** - Registering a domain name that is almost the same as the real one. This picks up traffic from users who type in the URI incorrectly. This practice is regulated (and mostly prevented) for the .au domain, but it is not prevented in the .com and other USA domains.
- **DNS cache poisoning** so that a user's DNS cache points to the wrong IP address when they have typed in the correct domain name.

SWINBURNE UNIVERSITY OF TECHNOLOGY

Pharming

Links on the page may appear to go to legitimate sites, but actually go to bogus ones rich in scripting and other nasties.

e.g. http://www.e-bay.com/

Actual domain names may be obfuscated:

http://spam-world.net@0xCE.191.0236.0x37/obscure.htm

SWINBURNE UNIVERSITY OF TECHNOLOGY

Log files

How do you know if you're being attacked?

- ❑ Check your bandwidth usage
- ❑ Use *Netstat* / *wireshark* to see what connections / traffic is going in / out of your site.
- ❑ Use tools such as *Tripwire*, *sfc (Windows)* and *ArpWatch* to detect modifications to system files
- ❑ Look at system logs:
  - /var/log/httpd/access_log, /var/log/httpd/error_log
  - \Windows\System32\Logfiles\MSFTPSVC1\ex*.log
  - \Windows\System32\Logfiles\W3SVC1\ex*.log
- ❑ Use tools like *LogCheck / logwatch* to monitor log files.

SWINBURNE UNIVERSITY OF TECHNOLOGY

Recent Web Security Research: Case Study and Intelligence Trend

- Lekies, Sebastian, Ben Stock, and Martin Johns. “25 million flows later: large-scale detection of DOM-based XSS.” In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 1193-1204. ACM, 2013.
- Lin, Guanjun, Sheng Wen, Jun Zhang, Yang Xiang. “Software Vulnerability Intelligence for Cyber Security: A Survey.” *Proceedings of the IEEE*, 2020. DOI: 10.1109/JPROC.2020.2993293

SWINBURNE UNIVERSITY OF TECHNOLOGY