COS30015 IT Security

Week 1

Presented by Dr Rory Coulter

31 July 2024

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.

Welcome to COS30015

The academic team wishes you the best for the semester

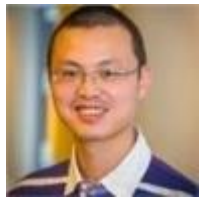
We’re here to support you over the semester, we’re looking forward to collaborating with you all.

COS30015

SWINBURNE UNIVERSITY OF TECHNOLOGY

Meet the Team

Who are we



Prof Jun Zhang, convenor

Head of the Swinburne Cyber Security Lab

Dr Rory Coulter, lecturer

Academic and industry professional: Incident response, threat detection and response, cyber security exercising, threat intelligence

Ms Yicun Tian, lecturer, tutor

PhD candidate, privacy and phishing

Mr Yasas Akurudda Liyanage Don, tutor

PhD candidate, shareable AI knowledge

Mr Fusen Guo , tutor

PhD candidate, Research Topic: AI Application on Electricity Load Forecasting, Grid Control, and Planning

Mr Di Cao (Troy) , tutor

PhD candidate, Forensics-based Automatic Firmware Vulnerability Analysis with Deep Learning Techniques

Mr Zeming Yao , tutor

PhD candidate, Neural Network backdoor attacks and defenses

SWINBURNE UNIVERSITY OF TECHNOLOGY

Unit Usuals

Common Questions or Requests

- Lectures are recorded
- Consultations meetings are recorded
- Lecture slides are to be available before the lecture
- Weekly announcements identifying what is going on, your responsibilities

- We have made a focus to enable you across the semester to complete your assessment. Labs are highly focused

- Swinburne email for correspondence
- Raise any concerns with your tutor first, escalate to Yicun if required

- Swinburne's extension policy is clear, please adhere to it: https://www.swinburne.edu.au/life-at-swinburne/student-support-services/special-consideration-assistance/

SWINBURNE UNIVERSITY OF TECHNOLOGY

Navigating the Unit

What, When, Expectations

All the usuals

- 12 weeks
- Mid-Semester break week 9 September
- 3 assessment types:
  - Released week 2 - Assignment 1: Offensive and Defensive security tools, practical
  - Week 7 - Quiz (weeks 1 – 6)
  - Released end of week 6 - Assignment 2: Practical exercise, digital forensic analysis of artefacts, review evidence and perform open source intelligence to
- Range of speakers from industry

SWINBURNE UNIVERSITY OF TECHNOLOGY

Navigating the Unit

What, When, Expectations

Expectations

- Regular attendance, both lectures and tutorials
- We are in the groove now as students, you know how to *student* by now, time management exists
- Disappear or prioritise another unit or work, extensions don't count
- Check weekly modules
- Communicate with your tutor, use discussion board
- Don't spend more time getting around plagiarism controls
- There are usually 3 types of students
  - Those who are enthusiastic
  - Those who participate and get the job done
  - Those who disappear week one, see above

- You can expect the following
  - Lectures update you on key tasks
  - Lectures provide guidance on how to do assessments
  - Lectures alert you to responsibilities
  - Labs directly relevant to your assessment
  - Tutorials give you a chance to get feedback
  - Weekly communication including those above
  - Consultations

Please see Discussion posts: *Navigating the Unit* and *Extension Policy*

SWINBURNE UNIVERSITY OF TECHNOLOGY

Twelve Weeks

Cyber Security unit, our focus is Cyber Security

What we're trying to do

- Introduce you to a wide range of ideas, concepts, and knowledge
- Some areas we get technical/in depth, others we just scratch the surface
- Provide some theoretical ideas, do some practical tasks
- Practical tasks are academic only, consider the ethics of what you might learn
- Not learning every "attack" type, we actually cover very few
- Do not perform any activities on live systems, laws exist

- Please consult the Syllabus
- There is additional content each week to watch and read

Why No Cool Hacks?

We will come to learn Tactics, Techniques and Procedures (TTPs) over cool hacks, but some resources to get started

Knowing TTPs is more beneficial than cool “hacks”, the underlying avenues stay the same

- https://www.asd.gov.au/cyber-security
- https://www.cyber.gov.au/
- https://www.cisa.gov/
- https://www.blackhat.com/
- https://attack.mitre.org/

SWINBURNE UNIVERSITY OF TECHNOLOGY

Core Concepts

Definitions

Principles

Cyber Security Frameworks

SWINBURNE UNIVERSITY OF TECHNOLOGY

Security Paradigms

Confidentiality, Integrity, Availability (CIA), Information Security, ICT Security, Cyber Security

Confidentiality

- Only those entitled to access the information can see it
- Authorise, encrypt, access control, authenticate, restrict physical access

Integrity

- Information cannot be altered and changes are immediately detectable
- Backup, checksum, hash, correction code

Availability

- Information is available (to read, write) to those who need it without interruption or onerous access restrictions
- Redundant systems, data recovery, disaster planning, UPS, backup power systems, redundant network connections

SWINBURNE UNIVERSITY OF TECHNOLOGY

Security Paradigms

Confidentiality, Integrity, Availability (CIA), Information Security, ICT Security, Cyber Security

Confidentiality

- Only those entitled to access the information can see it
- Authorise, encrypt, access control, authenticate, restrict physical access

Integrity

- Information cannot be altered and changes are immediately detectable
- Backup, checksum, hash, correction code

Availability

- Information is available (to read, write) to those who need it without interruption or onerous access restrictions
- Redundant systems, data recovery, disaster planning, UPS, backup power systems, redundant network connections

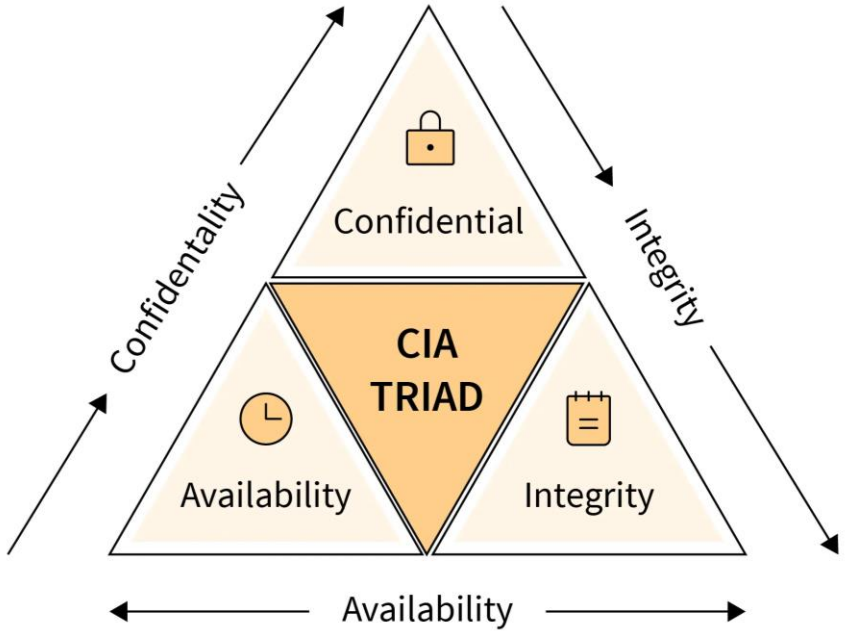


IMAGE SOURCE: https://www.scaler.com/topics/cyber-security/cia-triad/

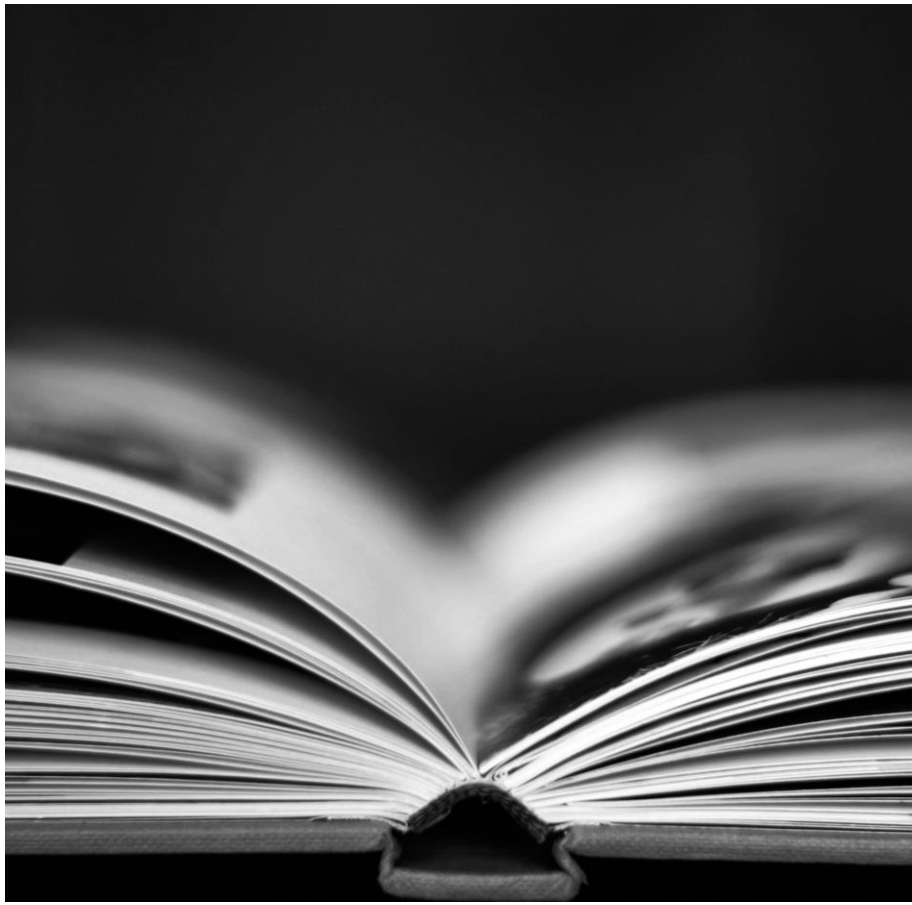
Security Paradigms

Confidentiality, Integrity, Availability (CIA), Information Security, ICT Security, Cyber Security

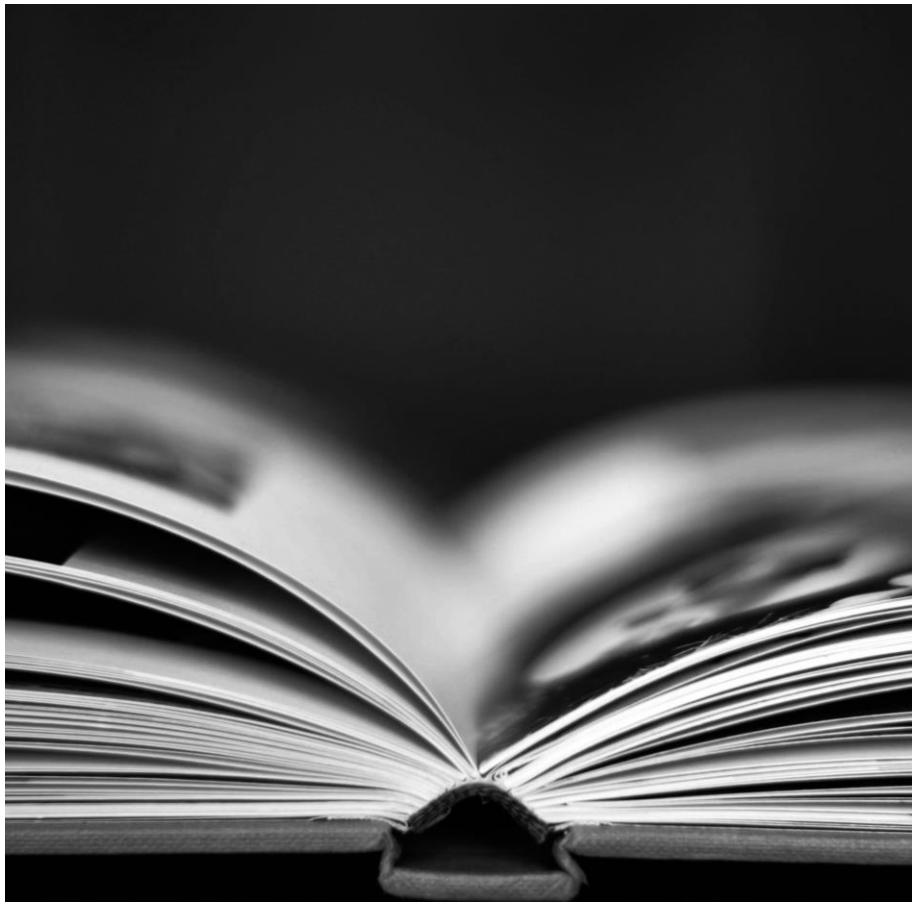
Information Security

Practices to keep data secure, defined in properties data should have CIA

"*The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability.*"



Security Paradigms



Confidentiality, Integrity, Availability (CIA), Information Security, ICT Security, Cyber Security

Information Security

Policy:

- What data needs to be protected and in what way
- Password Conditions
- Roles and responsibilities
- Access controls Required

Measures:

- Technical (hardware or software – e.g. encryption/firewall)
- Organisation (staff, team responsibilities)
- Human (training)
- Physical (Access control)

Security Paradigms

Confidentiality, Integrity, Availability (CIA), Information Security, ICT Security, Cyber Security

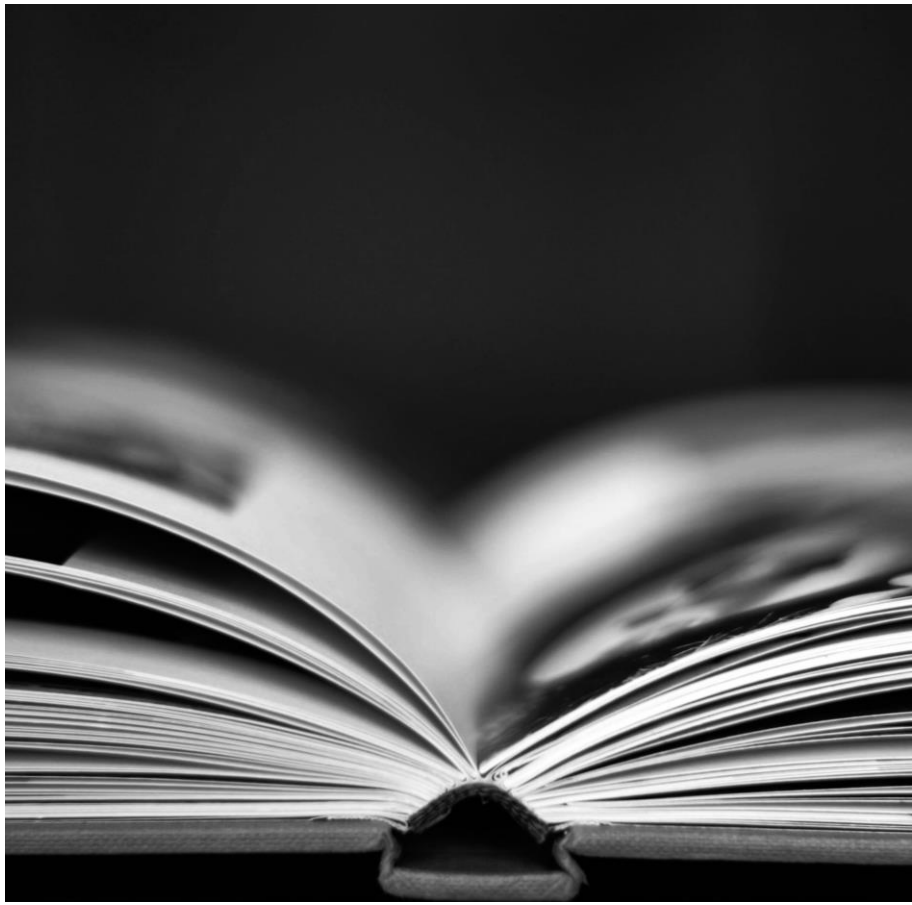
Information Communication Technology (ICT)

ICT:

- Unified communication using telecommunication and computer technology
- Software, storage, AV
- Enable users to access, store, transmit and manipulate information

Security:

- Protect confidential information from unauthorised use, modification, loss or release
- Monitoring and controlling access
- Safe transmission
- Secure storage and disposal



https://www.cyber.gov.au/acsc/view-all-content/glossary
https://statisticaldataintegration.abs.gov.au/topics/secure-data-management/information-and-communication-technology-security

SWINBURNE UNIVERSITY OF TECHNOLOGY

Security Paradigms

Confidentiality, Integrity, Availability (CIA), Information Security, ICT Security, Cyber Security

Cyber Security

- Information assets:
- Non-information based assets
- Real work assets

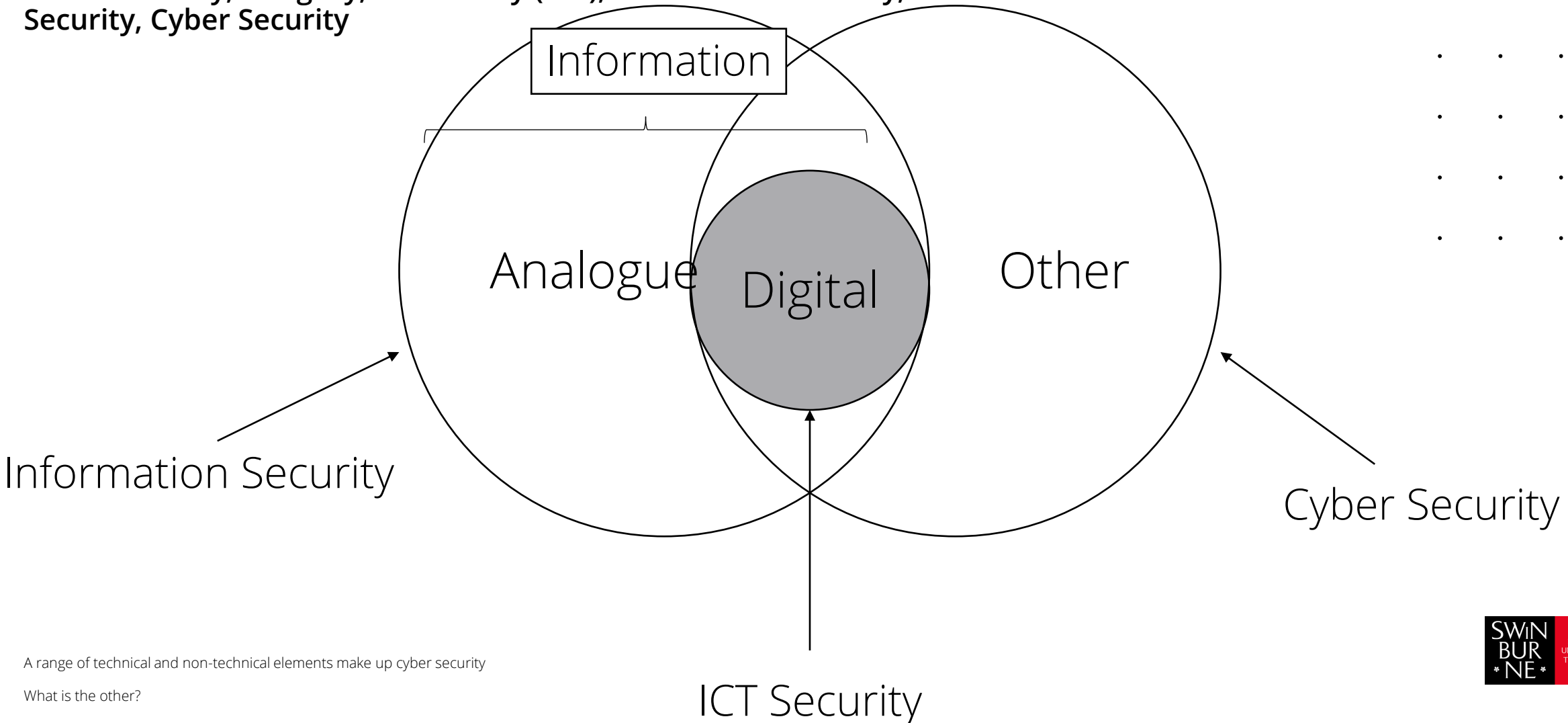
Protect CIA of systems, devices, information

https://www.cyber.gov.au/acsc/view-all-content/glossary
https://statisticaldataintegration.abs.gov.au/topics/secure-data-management/information-and-communication-technology-security

SWINBURNE UNIVERSITY OF TECHNOLOGY

Security Paradigms

Confidentiality, Integrity, Availability (CIA), Information Security, ICT Security, Cyber Security



A range of technical and non-technical elements make up cyber security

What is the other?

Cyber Security Complicates things

Security doesn’t play well with useability

Increased Complexity: Introducing cyber security measures adds layers of complexity to IT systems, making them harder to manage and maintain

Integration Issues: Cyber security solutions may not seamlessly integrate with existing IT infrastructure, leading to compatibility challenges

Resource Intensive: Implementing robust cyber security often requires additional resources, such as skilled personnel and advanced technology, increasing operational costs

User Resistance: Users may resist new security protocols and find them cumbersome, leading to potential non-compliance and security gaps

Training Needs: IT staff and end-users require specialised training to understand and follow cyber security best practices effectively

Balancing Usability and Security: Striking the right balance between usability and security can be challenging, as stringent security measures may impede productivity

Constant Updates: Cyber threats evolve rapidly, necessitating regular updates and adjustments to maintain effective security measures

Core Concepts

Definitions

Principles

Cyber Security Frameworks

Threat Landscape

A high-level look at actors

Threats	Objectives	Skill	Attack Span
Nation/States	Geopolitical/Espionage, profit	High	Long
Cyber Criminals/Gangs	Profit	Medium - High	Long - Short
Terrorist Groups	Ideology, profit	Medium	Somewhat Short
Hacktivists	Ideology	Medium	Somewhat Short
Insider Threats	Disgruntled, profit, corporate espionage	Medium - Low	Long to short
Script Kiddies	Satisfaction or notoriety	Low	Short

Skill and Span subject to change, variables

Threat Landscape

Common cyber threats

Not a complete list by any means

Threats	Objectives
Cryptomining	Often stealing processing power to mine crypto currency
Data Spill	Data leakage, exfiltration, breach
Denial of Service	Service or Resource is made unavailable (CIA?), Distributed DOS
Hacking	Unauthorised access to a computer system (CIA?)
Identity Theft	Stealing of personal information often for benefits
Malicious insiders	Employees, contractors for example with access, may steal, destroy and sabotage data, service or resources
Malware	Malicious software
Phishing	Steal confidential information
Ransomware	Type of malware which encrypts files for fee
Webshell Malware	Enable remote access to compromised device (think Trojan)

SWINBURNE UNIVERSITY OF TECHNOLOGY

Know your Extorsion

An example of how security is an ever changing game

We've heard of ransomware, lets understand the demands

Extorsion Type	Characteristic
Single	Encrypt, demand a ransom
Double	Threaten to release the data to encourage payment
Triple	Deny service to key systems (DoS)
Quadruple	Extort third parties and victims of incident to encourage payment

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti

Core Concepts
Definitions
Principles
Cyber Security Frameworks

Cyber Security Principles

Principles provide strategic aims to protect information and operation technology assets

GOVERN: A strong cyber security culture is developed (executive, risk management, audit data and applications)

IDENTIFY: Identify assets and associated security risks (criticality is assessed and documented, CIA assessed for systems, applications and data and documented, risks assessed for systems, applications and data and documented)

PROTECT: Implement controls to manage security risks (systems and applications design, deploy, maintained, decommissioned considering CIA, trusted suppliers, administer securely, manage vulnerabilities, encrypt data, backup, minimum access, identity controls, physical access)*

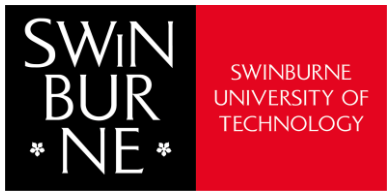
DETECT: Detect and analyse cyber security events to identify cyber security incidents (event logs collect and are analysed/security events are collected and analysed in a timely manner)

RESPOND: Respond to and recover from cyber security incidents (cyber incidents are reported timely internally/externally, incidents are analysed, contained, eradicated and recovered in a timely manner, incident response, business continuity and disaster recovery plans properly support returning to normal operations)

SOURCE: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-principles

*Not all

Core Concepts
Definitions
Principles
Cyber Security Frameworks



MITRE ATT&CK Tactics, Techniques and Procedures

Understanding attackers and attacks

"The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique"

- 14 Tactics
  - Consider as technical objective
- 240+ techniques and 370+ sub-techniques for enterprise
  - Way an adversary may achieve an objective
- Procedures as technique method and process

https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures

NIST SP 800-150 Tactics, Techniques, and Procedures (TTPs)

SWINBURNE UNIVERSITY OF TECHNOLOGY

TTPs

A method to categorise actions, behaviours, aims and objectives

MITRE ATT&CK: https://attack.mitre.org/

- We can observe a wide range of attackers, motivations and a diverse set of technologies (both attacker and defender)
- How may we standardise the attacks, actions, and technologies?
- De facto framework
- Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Replication Through Removable Media	System Service Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Securityd Memory					Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Scheduled Task	Gatekeeper Bypass	Two-Factor Authentication Interception					Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users						
	Signed Script Proxy Execution	Launch Agent		Hidden Window						
	Source			HISTCONTROL						
	Space after Filename			Image File Execution Options Injection						

Extra viewing: https://www.youtube.com/watch?v=Yxv1suJYMI8&embeds_euri=https%3A%2F%2Fwww.mitre.org%2F&feature=emb_imp_woyt

https://www.rapid7.com/fundamentals/mitre-attack/

SWINBURNE UNIVERSITY OF TECHNOLOGY

An Example – Impact [T1486]

Impact

The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach.

ID: TA0040
Created: 14 March 2019
Last Modified: 25 July 2019

Version Permalink

Techniques

Techniques: 13

ID	Name	Description
T1531	Account Access Removal	Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: changed credentials) to remove access to accounts. Adversaries may also subsequently log off and/or perform a System Shutdown/Reboot to set malicious changes into place.
T1485	Data Destruction	Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives. Common operating system file deletion commands such as `del` and `rm` often only remove pointers to files without wiping the contents of the files themselves, making the files recoverable by proper forensic methodology. This behavior is distinct from Disk Content Wipe and Disk Structure Wipe because individual files are destroyed rather than sections of a storage disk or the disk's logical structure.
T1486	Data Encrypted for Impact	Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.

Mitigations

ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	On Windows 10, enable cloud-delivered protection and Attack Surface Reduction (ASR) rules to block the execution of files that resemble ransomware. [95]
M1053	Data Backup	Consider implementing IT disaster recovery plans that contain procedures for regularly taking and testing data backups that can be used to restore organizational data.[96] Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery. Consider enabling versioning in cloud environments to maintain backup copies of storage objects.[97]

Detection

ID	Data Source	Data Component	Detects
DS0010	Cloud Storage	Cloud Storage Modification	Monitor for changes made in cloud environments for events that indicate storage objects have been anomalously modified.
DS0017	Command	Command Execution	Monitor executed commands and arguments for actions involved in data destruction activity, such as vssadmin, wbadmin, and bcdedit
DS0022	File	File Creation	Monitor for newly constructed files in user directories.
		File Modification	Monitor for changes made to files in user directories.
DS0033	Network Share	Network Share Access	Monitor for unexpected network shares being accessed on target systems or on large numbers of systems.
DS0009	Process	Process Creation	Monitor for newly constructed processes and/or command-lines involved in data destruction activity, such as vssadmin, wbadmin, and bcdedit.

Data Encrypted for Impact

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.[1][2][3][4]

In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as File and Directory Permissions Modification or System Shutdown/Reboot, in order to unlock and/or gain access to manipulate these files.[5] In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.[3]

To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like Valid Accounts, OS Credential Dumping, and SMB/Windows Admin Shares.[2][3] Encryption malware may also leverage Internal Defacement, such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").[6]

In cloud environments, storage objects within compromised accounts may also be encrypted.[7]

ID: T1486
Sub-techniques: No sub-techniques
Tactic: Impact
Platforms: IaaS, Linux, Windows, macOS
Impact Type: Availability
Contributors: ExtraHop; Harshal Tupsamudre, Qualys; Mayuresh Dani, Qualys; Oleg Kolesnikov, Securonix; Travis Smith, Qualys
Version: 1.4
Created: 15 March 2019
Last Modified: 16 June 2022

Version Permalink

Procedure Examples

ID	Name	Description
G0082	APT38	APT38 has used Hermes ransomware to encrypt files with AES256.[8]
G0096	APT41	APT41 used a ransomware called Encryptor RaaS to encrypt files on the targeted systems and provide a ransom note to the user.[9]

SWINBURNE UNIVERSITY OF TECHNOLOGY

Application of TTPs

TTPs contribute to many areas of cyber security

For example

- Threat Intelligence: Security teams leverage ATT&CK to enhance their threat intelligence by mapping and understanding the techniques and procedures used by various threat actors
- Incident Response: During incident response, ATT&CK provides a common language and framework for analysing and describing the actions of adversaries, aiding in effective incident handling and mitigation, remediation to combat TTPs
- Red Teaming: Organisations use ATT&CK in red teaming exercises to simulate real-world cyberattacks, test defences, and identify potential vulnerabilities.
- Defensive Strategies: Develop proactive defensive strategies by helping security professionals prioritise security measures based on known adversary behaviours
- Tool Selection: Security teams can use ATT&CK to evaluate and select cyber security tools that align with the specific techniques and tactics most relevant to their organisation's threat landscape

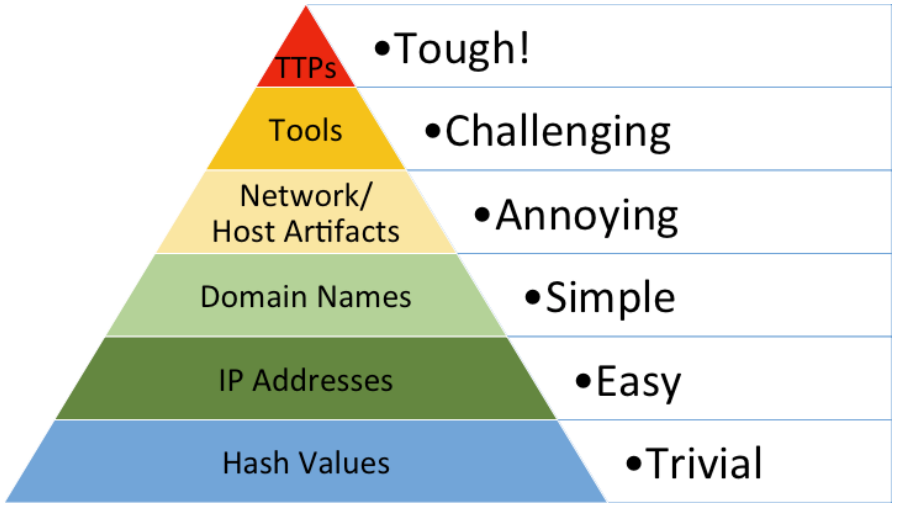
MITRE has lots more than TTPs, I would encourage you to explore Actors and Software too

Threat Detection or Incident Response

TTPs are the end game

Attacker artefacts which might contribute to TTPs

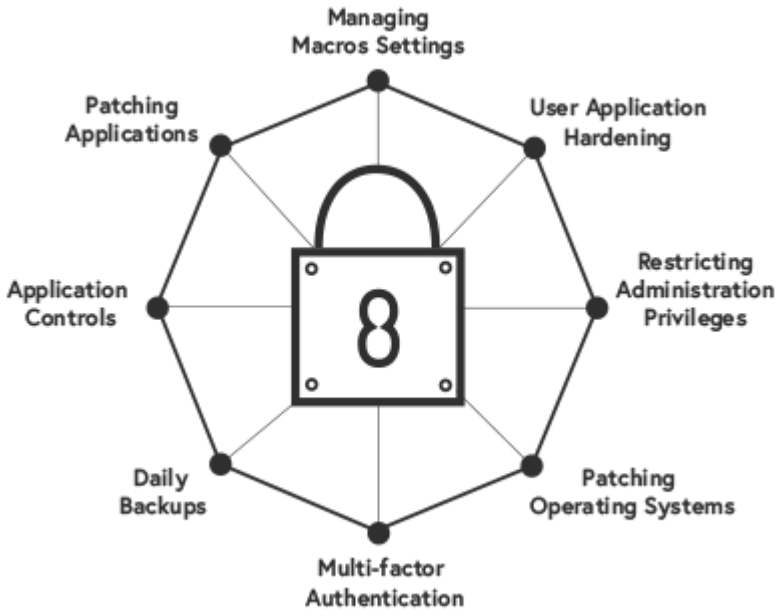
- Hash values: Signature of artefact, e.g., SHA-1 and MD5. Could be software or string
- IP addresses: Destination device
- Domain names: Attacker domain or compromised domain
- Network artifacts/host artifacts: Result of activity
- Tools: Attacker tools
- Tactics, techniques, and procedures (TTPs): Attacker behaviour or modus operandi which helps identify



Bianco, D. (2013). The pyramid of pain. Enterprise Detection & Response. https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

ASD - ACSC Essential 8

Covering 8 most essential areas from repeat analysis of threat landscape



- A set of mitigation strategies (8 in total)
- Administering application controls
- Patching vulnerable applications
- Managing macros setting
- User application hardening
- Restricting administrative privileges
- Patching operating systems
- Implementing and strengthening multi-factor authentication
- Initiate daily backups

IMAGE SOURCE: https://www.itstrategic.com.au/

SWINBURNE UNIVERSITY OF TECHNOLOGY

1. APPLICATION CONTROL

To prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Hosts, Powershell and HTA) and installer.

2. APPLICATION PATCHING

Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.

3. CONFIGURE MICROSOFT OFFICE MACRO SETTINGS

Block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.

4. USER APPLICATION HARDENING

Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet.
Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.

5. RESTRICT ADMINISTRATIVE PRIVILEGES

Restrict Administrative Privileges
Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.

6. PATCH OPERATING SYSTEMS

Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.

7. MULTI-FACTOR AUTHENTICATION

Implement multi-factor authentication (MFA) for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.

8. DAILY BACKUPS

Maintain a daily backup of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.

IMAGE SOURCE: https://acurus.com.au/what-is-the-essential-8-and-why-should-you-be-interested/

SWINBURNE UNIVERSITY OF TECHNOLOGY

An Example

Appendix A: Maturity Level One

Mitigation Strategy	Description
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.
	A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.
	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.

Appendix B: Maturity Level Two

Mitigation Strategy	Description
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.
	A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.

IMAGE SOURCE: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model

SWINBURNE UNIVERSITY OF TECHNOLOGY

An Example (cont.)

Appendix B: Maturity Level Two

Mitigation Strategy	Description
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.
	A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.

Appendix C: Maturity Level Three

Mitigation Strategy	Description
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
	Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.
	Online services that are no longer supported by vendors are removed.

IMAGE SOURCE: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model

SWINBURNE UNIVERSITY OF TECHNOLOGY

Mapping the ASD Essential 8 to the Mitre ATTACK™ framework

ASD Essential 8	MITRE ATT&CK™ Tactics	MITRE ATT&CK™ Techniques	Description
Application Whitelisting	Execution	T1204: User Execution	Prevents execution of unauthorized software.
		T1059: Command and Scripting Interpreter	
Patch Applications	Exploitation for Client Execution	T1203: Exploitation for Client Execution	Protects against exploitation of software vulnerabilities.
Configure Microsoft Office Macro Settings	Defense Evasion	T1027: Obfuscated Files or Information	Limits macro execution to prevent evasion techniques.
Multi-factor Authentication	Credential Access	T1110: Brute Force	Enhances security by requiring multiple forms of verification.
Daily Backup of Important Data	Impact	T1486: Data Encrypted for Impact	Ensures data recovery, mitigating ransomware impact.

SOURCE: https://www.reliaquest.com/blog/mapping-the-asd-essential-8-to-the-mitre-attck-framework/

SWINBURNE UNIVERSITY OF TECHNOLOGY

NIST Cyber Security Framework

- **Identify:** To protect against cyber attacks, the cyber security team needs a thorough understanding of the organisation's most important assets and resources

- **Protect:** The protect function covers much of the technical and physical security controls for developing and implementing appropriate safeguards and protecting critical infrastructure

- **Detect:** The detect function implements measures that alert an organisation to cyber attacks. Detect categories include anomalies and events, security, continuous monitoring and detection processes

- **Respond:** The respond function categories ensure the appropriate response to cyber attacks and other cybersecurity events

- **Recover:** Recovery activities implement plans for cyber resilience and ensure business continuity in the event of a cyber attack, security breach or other cybersecurity event

IMAGE SOURCE: https://www.cisco.com/c/en/us/products/security/what-is-nist-csf.html

Thank you