COS80013 Internet Security

Week 10

Presented by Dr Rory Coulter

12 May 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 10 Reflection
Security Policy
Classical Security Models
Contemporary Security Models
Frameworks
Assignment 2

SWINBURNE UNIVERSITY OF TECHNOLOGY

Week 10 Reflection

SWINBURNE UNIVERSITY OF TECHNOLOGY

Week 10 Reflection

Lets recap learning and put things in place

9 weeks, a range of security topics

- From what we know so far, we're seeking to reduce risk, and maintain Confidentiality, Integrity, and Availability
- Risk, cyber definition, TTPs
- Physical and converged security and authentication
- Operating system security
- Malware and vulnerabilities
- Network security
- Offensive and defensive security
- Intelligence
- Web and database security
- Cryptography

Together, a collection of aims, objectives, practices, methodologies

Several approaches* exist about how to apply them in combination

Do we just "secure" these things, or should we adopt an approach or strategy?

* And more outside of what is discussed today

SWINBURNE UNIVERSITY OF TECHNOLOGY

Applying Security

What if we just secure our environment – the aim is to secure

Operating systems

- Devices/Operating Systems
- Usernames and Passwords – Determine complexity
- Defender or Endpoint Detection and Response (*EDR*) - Do we put them on every device
- Policies and groups with different access – What do we restrict access too
- Apps: Do we need to lock down certain applications

Each of these require configuration, tweaking, and comes with a cost

Applying Security (cont.)

What if we just secure our environment – the aim is to secure

Network security

- Network equipment and connections
- Blacklists: Block known bad IPs and domains
- Geo-blocking: Do we restrict connections from a given country
- Network segmentation: Flat is easier, otherwise we need a firewall and more
- Access control lists: one list to rule them all

Applying Security

What if we just secure our environment – the aim is to secure

Operating systems

- Devices/Operating Systems
- Usernames and Passwords – Determine complexity MFA, repeat passwords, phish, target different class of account, dump out credentials
- Defender or Endpoint Detection and Response (*EDR*) - Do we put them on every device this is very big price point, level of administration
- Policies and groups with different access – What do we restrict access to find something not locked down, live off the land
- Apps: Do we need to lock down certain applications live off the land, install own

Each of these require configuration, tweaking, and comes with a cost

Applying Security (cont.)

What if we just secure our environment – the aim is to secure

Network security

- Network equipment and connections
- Blacklists: Block known bad IPs and domains rotate IP
- Geo-blocking: Do we restrict connections from a given country use a vpn or hop through a different compromised host
- Network segmentation: Flat is easier, otherwise we need a firewall and more use something not restricted between them all, port, protocol
- Access control lists: one list to rule them all bypass one bypass them all

Absence of a Security Model

Taking the approach to securing without a guiding process

Ultimately, we want to restrict TTPs in our environment

- High potential controls are disjointed
- Gaps are very likely to exist
- Process, planning is ad hoc
- Competing aims are chosen

A Security Model

A security model defines a scheme for enforcement of security policy

Implemented based upon a system developer/architect/designer's objective

- Security model outlines subjects that can, and objects that will have access to the system
- Security policy: security requirements/specification of a system
- Security requires models and frameworks working together
- There is no single one thing to stop all attacks/adversaries/reduce risk**
- Adopting a model to guide the approach security

** We will talk E8 about covering bases in general

Security Policy

Policy

Organisation intent, processes and objectives

Policy document outlines these in the management of risk

- Organisations will have a range of policy, outlining:
  - Technology
  - Information assets
  - Associated rules and objectives, controls
- It outlines things like
  - Acceptable use
  - Specification
  - Process
  - Delegation

Policy Types

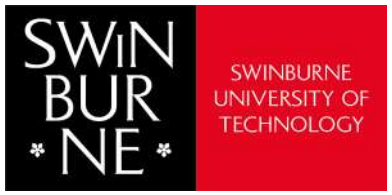
Scope for policy is broad

There are many moving parts to an organisation

- Aim: employees clear on their role, what is to be done, what is acceptable
- Acceptable use policy
- Digital signature policy
- Email retention, or logging policy in general
- Removable media policy
- Too many policies could become an issue

DEMO: https://www.sans.org/information-security-policy/

Classical Security Models



Bell-LaPadula

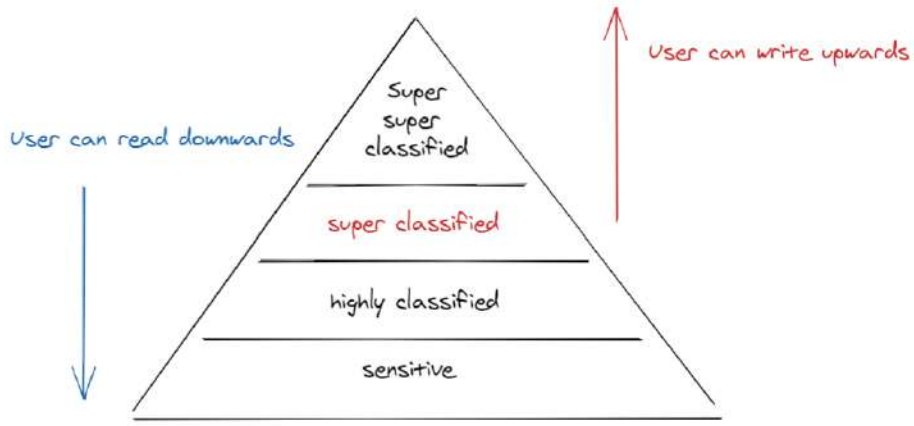
Users have a security clearance, Objects have a security classification

Model used* for enforcing access control in government and military applications

- Developed by David Elliott Bell and Leonard J. LaPadula, it formalizes the U.S. Department of Defense (DoD) multilevel security (MLS) policy, 1973
- Confidentiality in what users can access which objects (we're actually back in MAC territory)
- Subject is not allowed to read information at a higher level (no read up to another level of confidentiality) [Simple security property]
- Subject is not allowed to write information to a lower level (no write down) [Star * security property]
- No consideration of integrity of information
- Alternative to star * property is the concept of strong * property, whereby no write up or down

Security Levels

1. Top Secret
2. Secret
3. Confidential
4. Unclassified



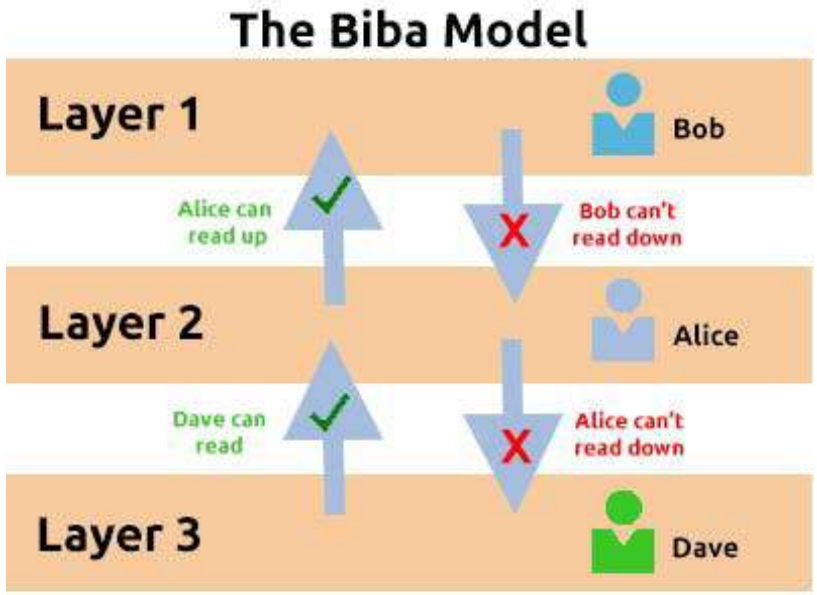
* was, SOURCE: https://www.vokke.com.au/permission-systems-and-access-controls-the-bell-lapadula-model/

Biba Model

Focus on integrity

Data can't be corrupted in a higher level

- Biba Model was developed by Kenneth J. Biba in 1975
- Simple integrity: Can read at same or higher level
- Star integrity: Can write down at same or lower level
- Strong integrity: Can neither read or write at a different level
- Prevent data modification



SOURCE: https://blog.cmpsamurai.com/information-security-series-part2-principles-of-privileges

High-Water Mark

Access control focus

Before BLP and Biba

- Introduced by Clark Weissmann in 1969, predates other models discussed
- Objects at a lower security level can be opened, but then assume the highest level
- If user A is writing a Secret report and uses a unclassified dictionary, the dictionary becomes Secret

SOURCE: Marvin Nauman

Perimeter Security

Classical(ish), many different names, such as M&M

Secure the outer shell, attention is focused on blocking external threats

- Assumes all users inside the network/organisation are trusted
- Those outside the organisation are untrustworthy
- Once perimeter is compromised there is lack of security controls

SOURCE: https://www.fs.com/blog/from-perimeter-to-zero-trust-the-evolution-of-cyber-defense-13598.html

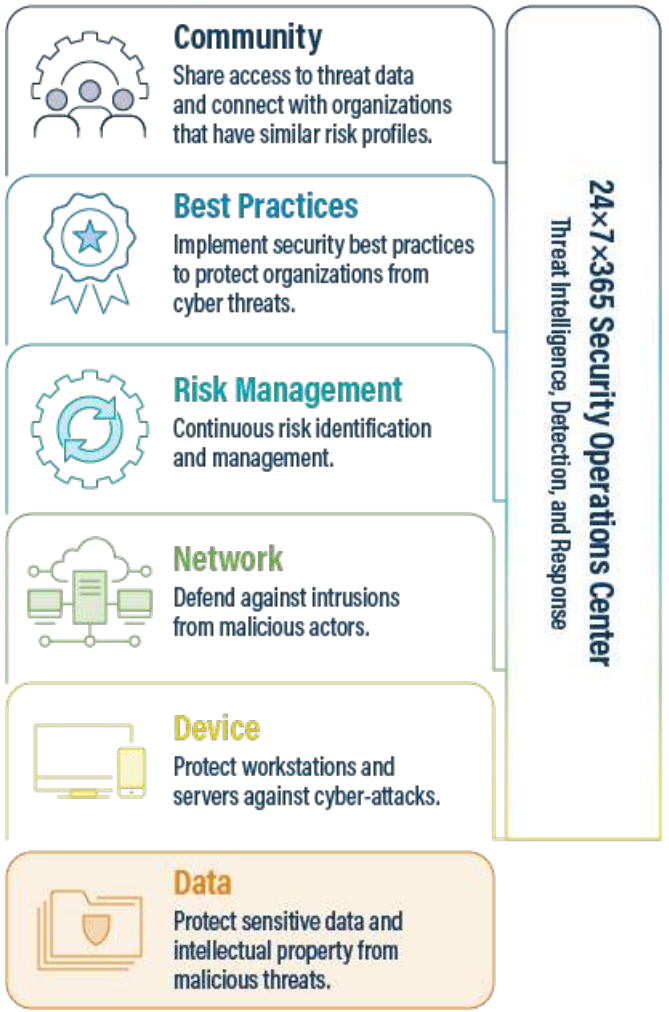
Contemporary Models

Defence in Depth

Not just an outer shell

Security is applied in many layers

- Ensures there is redundancy in security controls, using a range of security layers
- System and network complexity increases
- Restricts and presents a series controls against adversaries
- Also known as onion model



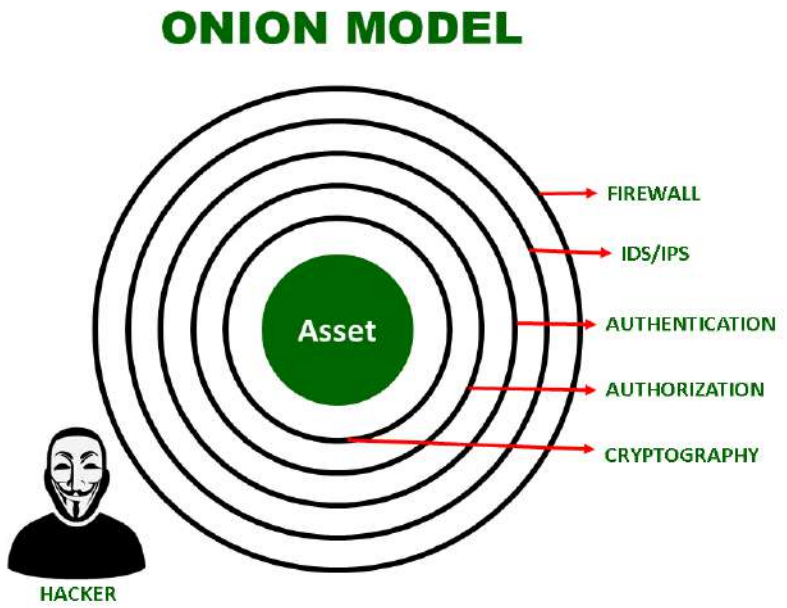
SOURCE: https://www.cisecurity.org/insights/blog/sltt-organizations-and-the-defense-in-depth-strategy

Defence in Depth

Sources of focus, multiple interpretations

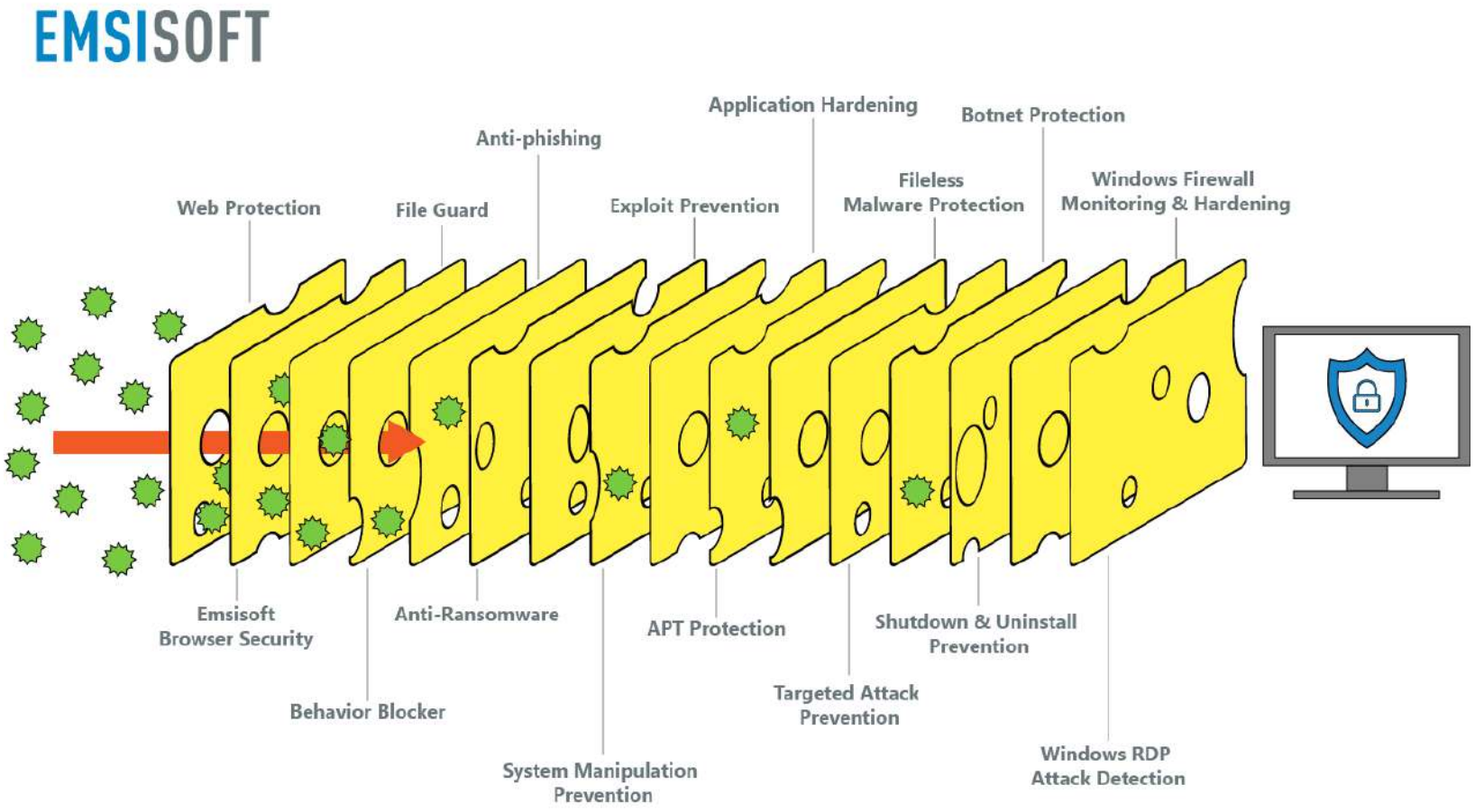
More than just the outside

- Physical
- Perimeter
- Network
- Endpoint
- Application and OS
- Data and Information
- Policy



SOURCE: https://www.geeksforgeeks.org/introduction-to-security-defense-models/

Defence in Depth (cont.)



SOURCE: https://blog.emsisoft.com/wp-content/uploads/2021/03/logo.png

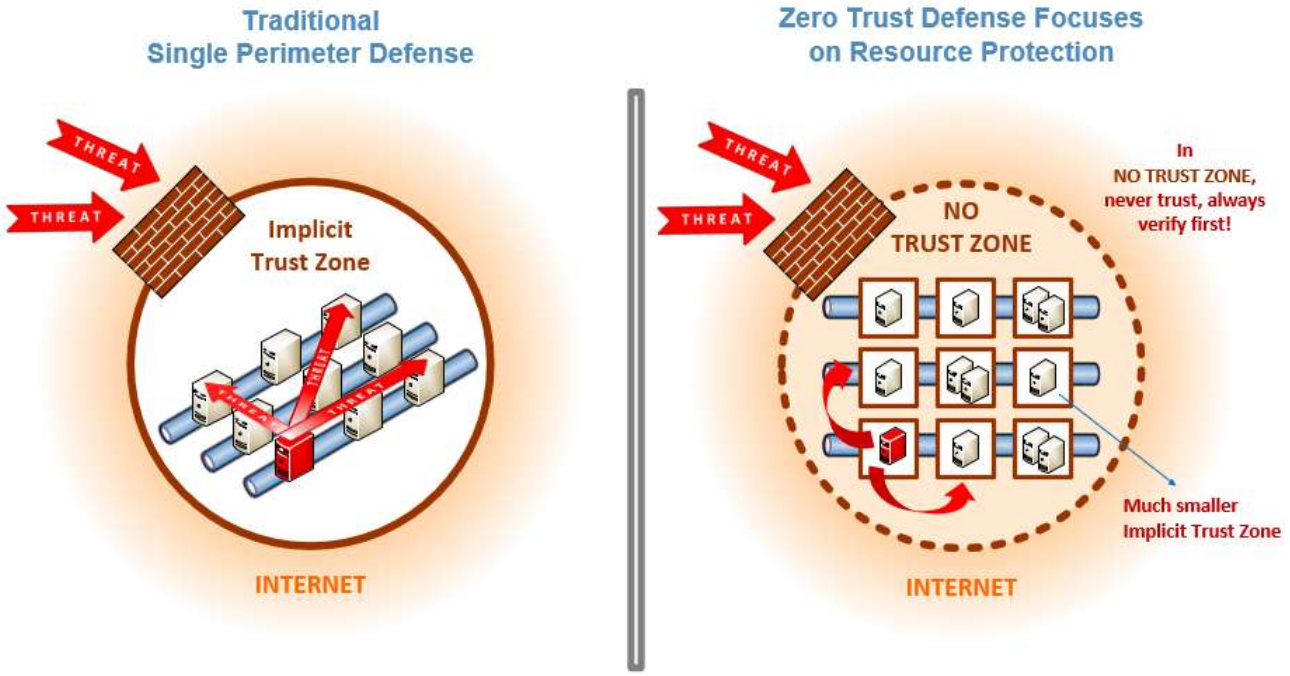
Zero Trust

Focus shifts to verification of users and assets, assumes compromise and not to trust

"Never trust, always verify"

- Previous models still operate on a trusted zone
- Trust, but verify
- Authenticated, in a trusted zone, surrounded by controls – it's ok to trust

- Zero trust removes the idea of a trusted zone
- All services, accounts must be understood ahead of time
- Development of zero trust policies



SOURCE: https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify

Key Principles

Of zero trust architecture (ZTA)

Three key principles applied

- Continuous verification
- Verify all access, for all resources, all the time
- Limit the "blast radius"
- Reduce the impact regardless on internal or external breach
- Automate context collection and response
- Incorporate a range of data/information from the IT stack to get an accurate picture (identity, endpoint, working hours, etc.)

SOURCE: https://csrc.nist.gov/pubs/sp/800/207/final

Continuous Verification

No trusted credentials, zones or devices at any time

Never trust, always verify

- Risk based conditional access
- Workflow will be interrupted when risk changes
- Scalable policy
- Must also align to organisation specification also

SWINBURNE UNIVERSITY OF TECHNOLOGY

Limit the Blast Radius

Identity and privilege

- Identity segmentation, not zone
- Segment based upon identity to required data and systems
- Least privilege
- User and service accounts, apply the minimum capability to apply the task

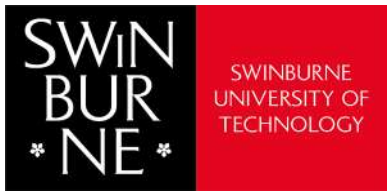
Automate Context Collection And Response

Accurate decisions required data

Realtime decision making from a range of sources

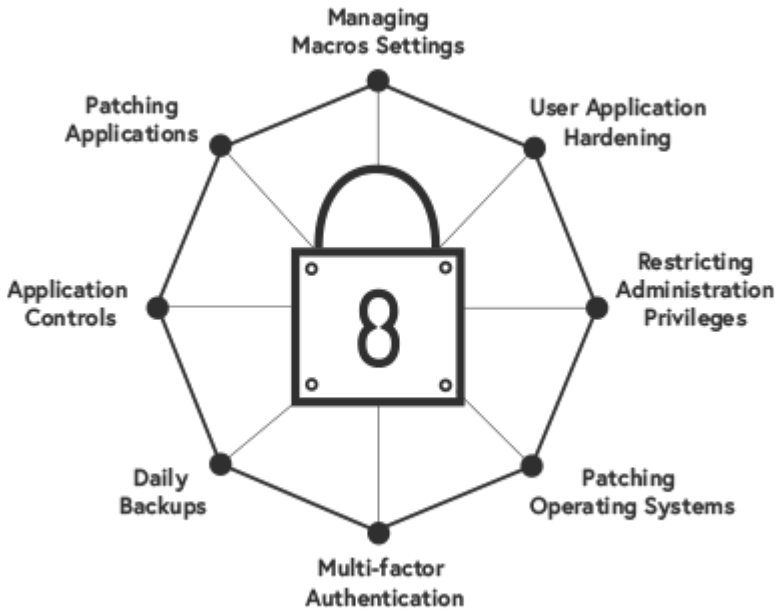
- Credentials
- Workload
- Endpoint
- Network
- Data
- SIEM
- Identity
- Etc.

Frameworks



Essential 8

Covering 8 most essential areas from repeat analysis of threat landscape



- 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

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

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

Essential 8 walkthrough

SWINBURNE UNIVERSITY OF TECHNOLOGY

NIST Cyber Security Framework

- **Identify:** To protect against cyberattacks, 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 cyberattacks. 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 cyber security events

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

What Is NIST Cybersecurity Framework (CSF)? - Cisco

Implementing the NIST Cyber security Framework

ISO 27001 provides guidelines and a framework, with requirements for "establishing, implementing, maintaining and continually improving" an information security management system (ISMS)

Tier 1: Partial	Tier 2: Risk informed	Tier 3: Repeatable	Tier 4: Adaptive
• Irregular, reactive risk management practices with limited awareness of cyber security risks	• Some awareness of cyber security risks, but limited establishment of a risk management program at an organisational level	• Consistent cyber security risk management program across an organisation with processes to respond based on changes in the threat landscape	• Advanced response system capable of effectively improving its risk management program based on previous incidents and predictive indicators

SWINBURNE UNIVERSITY OF TECHNOLOGY

ISO27001

ISO 27001 is an internationally recognised standard for information security that provides guidelines for creating and maintaining an effective information security management system (ISMS).

The current ISO 27001 standard has 14 domains in comparison to the older one which has 11 domains. These domains widely cover six security areas –

Information security policies	Organisation of information security
Human resource security	Asset management
Access control	Cryptography
Physical and environmental security	Operations security
Operations security	System acquisition, development and maintenance
Supplier relationships	Information security incident management
Information security aspects of business continuity management	Compliance

ISO 27001 role in cyber

Benefits of ISO 27001	The Challenges it solved
• Allows for the secure exchange of information • Makes information security everybody's responsibility • Brings a competitive advantage and builds reputation • Meets legal or third party obligations • Achieve a return on investment	• Organisation doesn't know its information assets • Information security isn't organised or structured • Organisations don't know what risks they're facing • Helps avoid legal hot water • Client Assurance

SWINBURNE UNIVERSITY OF TECHNOLOGY

Assignment 2

SWINBURNE UNIVERSITY OF TECHNOLOGY

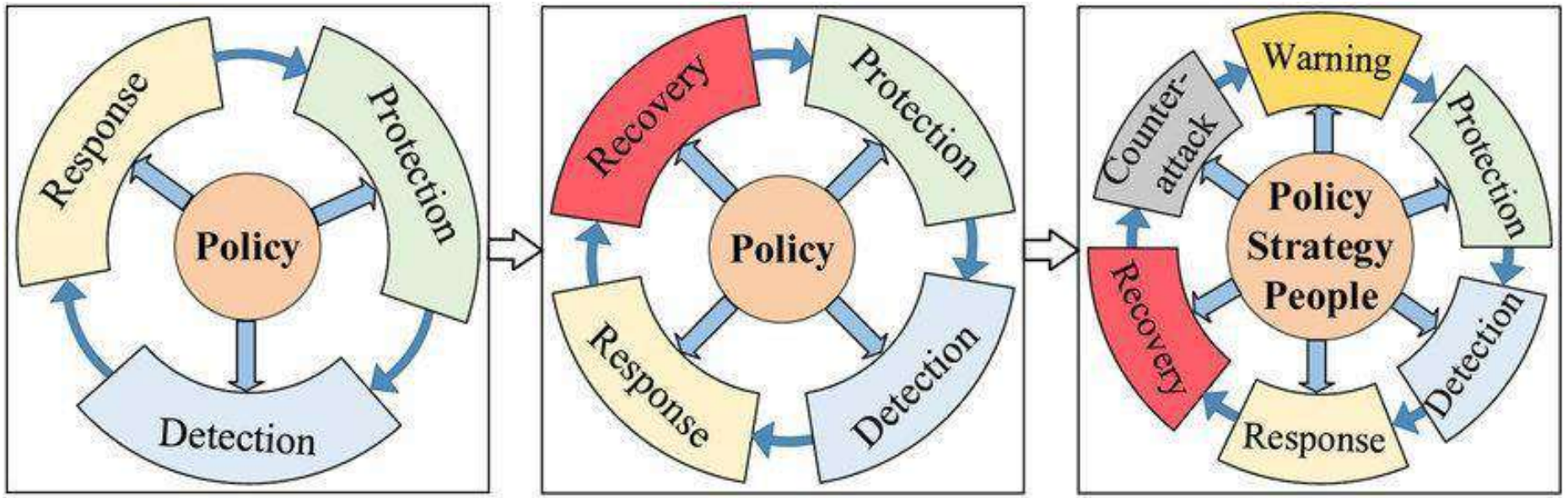
COS80013 Internet Security

Lecture Week 10A

- Security Models

Security Models

- Security means a complete system
  - Policies
  - Procedures - detail how the policies are implemented
  - Models



Security Policies

- Policies – the rules about what must be done.

– Policies include definitions of

  - Subjects – the actors
  - Objects – the information and equipment
  - Actions – what can and cannot be done
  - Permissions – map subjects, objects and actions together.
  - Protections – rules which prevent subversion of the policy

Security Models

- A classification scheme for people, secrets, activities
- A common language used by policy makers and security administrators.
- Types of models:
  - Discretionary Access Control
  - Mandatory Access Control

Discretionary access control

- DAC
- Users have the authority to set permissions on their own files.
- Users can grant permission to other users.
- Examples – ACLs in Windows, Linux

  Assumes everyone who has permission exercises it responsibly.

Mandatory access control

- MAC
- Users have no authority to set permissions.
- Centralised policy admins set permissions.
- Each rule maps a subject (actor) to an object (resource) with a specific set of permissions
- Example – SE Linux

  Assumes no-one who has access can be trusted to exercise it responsibly.

  Even root can have no authority.

Trust management

A form of security policy:

- Actions – sensitive operations
- Principals – actors
- Policies – rules which map principals to actions.
- Credentials – digitally signed documents which map allowable actions to principals.
- Example – XACML – xml-based language for defining trust management systems.

Bell-LaPadula Model

- Ensures confidentiality
- Based on multi-levels of classification
- Levels of secrecy for documents
  - Unclassified, Confidential, Secret, Top Secret
- Levels of clearance for users
  - Public, Agent, Commander, President
  - Document at a certain level can only be read by a person with equivalent or higher clearance.

Bell-LaPadula model

Progressively more strict classifications of data

- Clearance levels assigned to individuals
- 1. User cannot read data at a higher level
- 2. User cannot write data to a lower level

- Aggregate data is more sensitive than raw data; (only the commanders get the big picture).
- False data can move upwards and mislead decision makers.

Biba Model

- Ensures integrity
- Based on multi-levels of integrity.
- Levels of accuracy for objects
  - e.g. Document in data centre has more accuracy than document in laptop.
- Levels of integrity for users
  - Policy makers (highest), Public (lowest)
  - Document at a certain level is considered reliable by a person with equivalent or lower level.

Biba Model

Progressively less reliable classifications of data

- Integrity levels assigned to information
- 1. User cannot write data to a higher level
- 2. User cannot read data from a lower level
- Reliable data is must come from a reliable source. Low reliability data cannot be made to be reliable.
- False policy data can move downwards and misdirect workers.

More Models

- Low Watermark Model
  - Relaxed version of the Biba model.
  - Users at high levels can read low-reliability data.
- Clark-Wilson Model
  - Based on integrity of transactions.
  - Checks system state.
  - Separate auditing process which ensures that transactions are valid.

Chinese Wall Model

- Chinese Wall Model (Brewer & Nash Model)
- Prevents conflicts of interest (CoI)
- Puts resources, people into CoI Classes
- A user can only access resources from one CoI class at a time.
- CoI allocation can change with time.

Trusted Systems

- Implemented using Access Control Lists, Bell-La Padula, MAC
  - Users are authenticated, restricted access.
  - Users must be trustworthy (but have no discretion).
- Secured hardware:
  - Not on the internet (Air-gap)
  - Locked up in secure rooms
  - Isolated from power grid.
  - Rings of security/Defense in depth

Trusted Systems

- Air-Gap – what can go wrong?

NO automatic updates – Microsoft, Adobe, Oracle assume everyone is on the Internet.

Patch management is difficult to coordinate. Mission-critical systems are never shut down / re-booted.

Therefore new vulnerabilities are not patched.

Air-gapped systems are easy to compromise once the perimeter is breached (M&M security)

SWINBURNE UNIVERSITY OF TECHNOLOGY

Vulnerabilities

Vulnerability Assessment

- Black Box
  - Inner working of system unknown
  - Based on documentation, binary/working system only.
  - Simulates real attacker (zero knowledge)
- White Box
  - Source code, design docs available
  - More expensive than BB (experts needed)
  - Can uncover undocumented “features”

SWINBURNE UNIVERSITY OF TECHNOLOGY

Vulnerability Assessment

- Static Analysis
  - Examine code and data
  - Audit source code, binaries.
  - Use analysis tools to discover (e.g.) potential buffer overflows.
  - Disassemble binaries, reverse engineer.
  - Not so good for design / architecture problems.
- Dynamic Analysis
  - Examine running system.
  - Use debugger tools, VMs, sandboxes.
  - Use Fuzz testing to trigger errors, create *proof of concept* exploits.

Disclosure

- Responsible disclosure
  - Reveal vuln. to software vendor, suggest fixes, mitigation.
  - Pwn2Own, Bug Bounty
  - Some vendors don't want to patch; punish hackers

- Full Disclosure
  - Publish all details of vuln. immediately.
  - Force vendors to patch immediately.
  - Black hats, criminals get info. immediately and can craft exploits.

Secure Admin

- Adopt the right policies:
- Principle of least privilege
- Use a good Access control system
- Enforce strong passwords (but not too strong)
- Use well-known, well-tested crypto.
- Patch

Physical Security

Physical Security

- Disable USB
- Lock BIOS
- CD Boot (demo?)
- Cables, appliances
- Servers, media, network devices
- Doors, locks, windows, access systems
- Disaster mitigation, backup

Minimise the Attack Surface

- Segmented networks
- DMZ
- Internal firewalls
- Isolate machines from Internet
- Default deny on firewalls, services
- Whitelist needed services, applications
- MAC address monitoring / filtering
- SPAM mitigation

Auditing, Penetration Testing

Network Auditing

- Look at all of the business:
- e.g. Password policy
  - Strong passwords
  - Single sign-on or multiple passwords?
  - Account lock-out?
  - Password recovery process

Penetration Testing

- Simulated attack.
- Black box or white box.
- Get written agreement from customer.
- Take notes throughout the pen-test.
- Report details of findings and vulnerabilities to customer.
- Suggest mitigation, fixes.

Penetration Testing

1. Enumeration, network reconnaissance, IP scan, port scan, DNS records.

2. Network Vulnerability analysis, port scans, footprinting, find vulnerable services.

3. Web application testing, SQL mapping, injection, XSS testing, javascript injection, php passthrough, injection, fuzz testing.

4. Exploit vulnerabilities, establish foothold, additional reconnaissance, obtain privileged information/access.

Kerberos

Kerberos

- **Kerberos** is an authentication protocol and a software suite implementing this protocol.
- uses symmetric cryptography to authenticate clients to services and vice versa.
- Windows servers use Kerberos as the primary authentication mechanism, working in conjunction with Active Directory to maintain centralized user information.

Kerberos

- Other possible uses of Kerberos include
  - log into other machines in a local-area network,
  - authentication for web services,
  - authenticating email client and servers,
  - authenticating the use of devices such as printers.

Kerberos

- Uses **tickets** as tokens that prove user identity.
- Tickets are digital documents that store session keys:
  - During authentication, a client receives two tickets:
    - A **ticket-granting ticket (TGT), (**a global identifier)
    - A **service ticket,** which authenticates a user to a particular service (session ticket)

Kerberos

–Uses a **key distribution center (KDC),** which contains:

- An **authentication server (AS)**
- A **ticket-granting server (TGS)**

•Keeps a database storing the secret keys.

•Centralises authentication for an entire network.

•Each transmission is encrypted.

•Compares password hashes (never sends password).

Advantages

- Timestamps tickets to prevent playback attacks.
- Uses a cache of previously used tickets to prevent replay attacks (sort of OTP).
- Tickets may be specific to IP addresses.
- Uses symmetric keys.
- Open source version available.

Disadvantages

- Single point of failure:

  – If the KDC goes down, no-one can authenticate.

    - Can have multiple KDCs, or backup KDCs

  – If an attacker compromises the KDC, the authentication information of every client and server on the network would be revealed.

  – Requires that all hosts have synchronized clocks.

  – Used DES encryption - really out of date

  – http://media.blackhat.com/bh-us-10/whitepapers/Stender_Engel_Hill/BlackHat-USA-2010-Stender-Engel-Hill-Attacking-Kerberos-Deployments-wp.pdf

Secure Storage

Secure Storage

- Secure file formats:
- MS office, Acrobat allow password protection by encryption.
- MS Office creates an encryption key by hashing a password 50000 times
  - Makes brute force cracking impractical
  - Acrobat brute forcing can try 75million guesses per second.
  - Office brute forcing can only try 5000 guesses per second.

Windows EFS

- Encrypted file system
- Uses public/private keys
- Documents can store multiple copies of decryption key, encrypted by different public keys (allows many users to share a document).
- Data recovery Applets (DRAs) allow admin to decrypt documents.

Windows EFS

- But:
- Encrypts file contents, not names, metadata
- Only works with EFS file system
- Cached, temp files unencrypted
- Uses Windows password as part of private key.

Truecrypt

- 3rd party solution
- Encrypt complete hard drive or TC containers.
- Mount as a drive in windows; device in Linux
- Provision for plausible denial. Hide TC inside another TC.
- Requires root rights to create an NTFS container, but anyone can mount a TC container and use it.
- Shut down (not supported) since May 2014

Bit Locker

- Windows technology
- Creates a plain text partition for pre-booting, and an encrypted partition for Windows, data.
- Uses TPM to manage keys.

Free Compusec

- Open source solution
- Intercepts drive R/W commands and encrypts/decrypts the stream
- Full drive encryption only
- Modifies MBR to load Compusec drivers to mount drive.

Limitations

- These disk encryption schemes keep a symmetric key loaded into memory during operation.
- A RAM sniffing attack (e.g. cold boot attacks, *Inception, WinLockPwn* (Adam Bolieu)) can extract the key, making the entire drive visible to an attacker.
- Such attacks require physical access.

Trusted Platform Modules

Trusted Platform Modules

- A trusted platform module is a cryptography chip (usually a daughter board) attached to the mother board of a PC or other computing device.
- The TPM contains a small amount of ***eeprom*** and a dedicated CPU, ROM and temperature sensor (for seeding a true random number generator).

Trusted Platform Modules

- The idea is that all security and cryptographic functions performed on behalf of the BIOS and OS are performed by the TPM, which is harder to sniff or intercept because it is hardware.
- Items such as fingerprint metrics, certificates, keys and passwords can be stored on the module.
- The TPM should never display it's contents.

Trusted Platform Modules

But:

The TPM has a poor reputation due to it's early use in enforcing DRM (copy protection).

Few manufacturers / software vendors put the TPM on mobos because of this.

Provision has been added to allow the TPM to be backed-up –

keys can now be extracted from the TPM by crackers.