

CISSP Domain 1-4 General Review

PeiChen Chuang

Ai Network

Version: 1.4 (Sep 2025)

版權所有，翻印必究

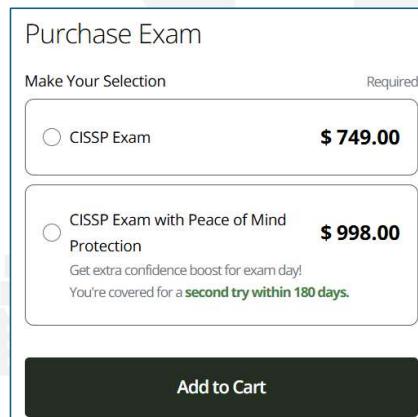
About CISSP Exam (簡體中文版)

關於考試報名

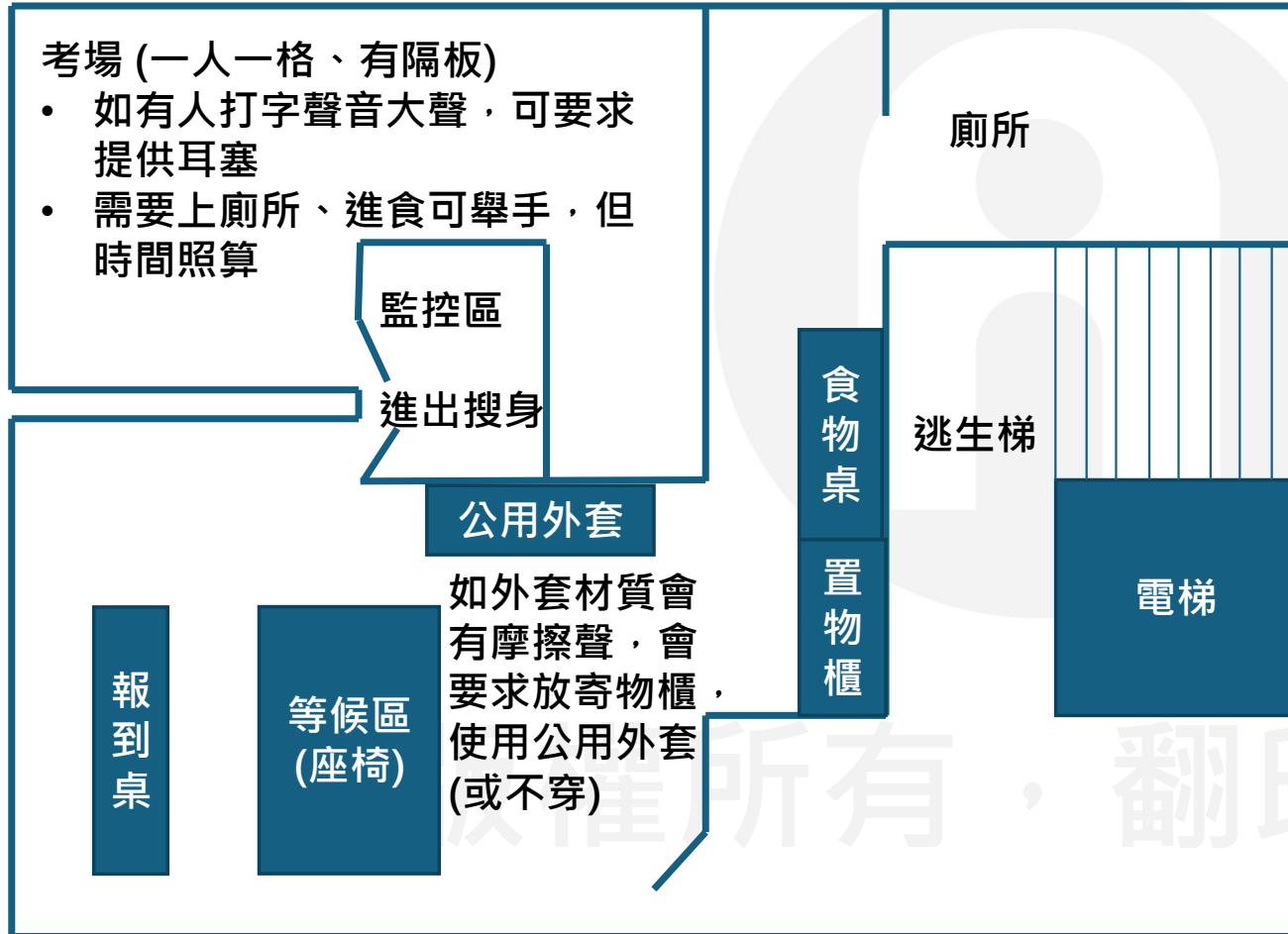
- 時常有限時福利，可購買“安心保障” 考試券
- 預約考試後，若需要改期或取消，需在至少2天前聯繫 Pearson Vue，改期手續費 50 USD、取消手續費 100 USD，365天內須完成考試(若未完成，費用不予退還)
- 若考試未通過，第 1 次重考須至少間隔 30 天，第 2 次重考須至少間隔 60 天

關於考試過程

- 共 100~150 題，最多可考 3 小時，休息次數、時間不限，考試時間照算
- 簡中、英文雙語可供切換，不可跳過問題再返回作答
- 考完當下即可知道是否通過考試
- 考生會由一個遠低於及格標準的考題開始考試，根據應試者作答的狀況調整難度，期望應試者約有 50% 機率正確作答，通過多題迭代的方式測試應試者的知識水平
- ISC2 考試為補償性考試，考試通過/未通過是根據所有有效題目答對率做計算，若在某一Domain 正確回答更多題目是可以彌補在另一個 Domain 表現不好的情況。(不要糾結，每個 Domain 都要顧好)



Floor Map



進場流程

1. 詳細閱讀入口大門的考場須知，關閉手機、課本收好走進去
2. 報到桌身分驗證(護照/(信用卡+身分證)核對、掌紋掃描)，取得考桌編號
3. 取得置物櫃鑰匙並寄物，按照置物櫃編號在食物桌上放所需的食物和水
4. 上廁所
5. 回報報到桌確認準備完成
6. 進入監控區搜身、掃掌紋
7. 進入考場
8. 試題做完，電腦畫面會突然黑掉，提示考試結束
9. 監控區人員帶出場、掃掌紋
10. 報到桌領成績單
11. 考試結束(或下一場連續考試開始)

Domain Weights

Domain #	Domain Name	Effective by 2024.04.15
1	Security and Risk Management	16%
2	Asset Security	10%
3	Security Architecture and Engineering	13%
4	Communication and Network Security	13%
5	Identity and Access Management	13%
6	Security Assessment and Testing	12%
7	Security Operations	13%
8	Software Development Security	10%

版權所有，翻印必究

CISSP Exam Outline



领域 1： 安全与风险管理

1.1 理解、遵守并促进职业道德

- » ISC2 职业道德规范
- » 组织道德规范

1.2 理解并应用安全概念

- » 机密性、完整性和可用性、真实性与不可抵赖性（信息安全的 5 大支柱）

1.3 评估和应用安全治理原则

- » 根据业务战略、目标、任务和目的调整安全职能
- » 组织流程（如收购、资产剥离、治理委员会）
- » 组织角色和责任
- » 安全控制框架（例如，国际标准组织 (ISO)、国家标准与技术协会 (NIST)、信息和相关技术控制目标 (COBIT)、Sherwood 业务安全架构 (SABSA)、支付卡行业 (PCI)、联邦风险和授权管理计划 (FedRAMP)
- » 尽职调查

1.4 全面了解与信息安全相关的法律法规事项

- » 网络犯罪和数据泄露
- » 许可与知识产权要求
- » 进出口控制
- » 跨境数据流
- » 与隐私相关的问题（例如，《一般数据保护条例》(GDPR)、《加州消费者隐私法案》、中国《个人信息保护法》、南非《个人信息保护法》）
- » 合同、法律、行业标准和监管要求

1.5 了解调查类型（即行政、刑事、民事、监管、行业标准）的要求

1.6 制定、记录和实施安全政策、标准、程序和指南

1.7 确定、分析、评估和实现业务持续性 (BC) 要求并确定优先次序



领域 2： 资产安全

2.1 对信息和资产进行识别和分类

- » 数据分类
- » 资产分类

2.2 制定信息和资产处理要求

2.3 安全地提供信息和资产

- » 信息和资产所有权
- » 资产库存（如有形资产、无形资产）
- » 资产管理

2.4 管理数据生命周期

- » 数据角色（即所有者、控制者、保管者、处理者、用户/主体）
- » 数据维护
- » 数据收集
- » 数据保留
- » 数据恢复
- » 数据位置
- » 数据销毁

2.5 确保适当的资产保留（如使用寿命结束 (EOL)、支持终止 (EOS)）

2.6 确定数据安全控制与合规要求

- » 数据状态（如使用中、传输中、静态）
- » 范围界定和定制
- » 标准选择
- » 数据保护方法（如数字化权限管理 (DRM)、数据丢失防护 (DLP)、云访问安全代理 (CASB)）

Ref. <https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/exam-outlines/CISSP-Exam-Outline-May-2021-Chinese.pdf>

Domain 1

Security and Risk Management (16%, 80min)

版權所有，翻印必究

Outline

- 1.1 理解、遵守并促进职业道德
- 1.2 理解并应用安全概念（信息安全的 5 大支柱）
- 1.3 评估和应用安全治理原则
- 1.1 Governance
 - 1.6 制定、记录和实施安全政策、标准、程序和指南
 - 1.7 确定、分析、评估和实现业务持续性 (BC) 要求并确定优先次序
 - 1.8 促成并执行人员安全方面的政策和程序
 - 1.12 建立并维护安全意识、教育和培训计划
- 1.2 Risk
 - 1.9 理解并应用风险管理概念
 - 1.10 理解并应用威胁建模的概念和方法
 - 1.11 应用供应链风险管理 (SCRM) 概念
- 1.3 Compliance
 - 1.4 全面了解与信息安全相关的法律法规事项
 - 1.5 了解调查类型（即行政、刑事、民事、监管、行业标准）的要求

印必究



1.1 Governance

版權所有，翻印必究

Ethics

(ISC)2 Code of Professional Ethics

Canon 1. Protect society, the common good, necessary public trust and confidence, and the infrastructure. 保護社會、公共利益與基礎設施，贏得必要的公眾信心與信任。

Canon 2. Act honorably, honestly, justly, responsibly, and legally. 行事端正、誠實、公正、負責、守法。

Canon 3. Provide diligent and competent service to principals. 勤奮盡責、專業勝任委託人(Principals)委託。

Canon 4. Advance and protect the profession. 推動行業發展、維護職業聲譽。 (CISSP持證人員不僅是要注意自己的職業行為，還需要注意同行的行為。如觀察到其他持證人員違反道德準則，應循程序投訴，如未執行，則違反此規定。)

Organizational code of ethics

Governance

Corporate Governance { Mission, Strategy, Goal, Objective
Organizational Process — 組織決策產生與執行的流程 — 核決權限、請採購...

Security Governance ☰

版權所有，翻印必究

Focus of Security

Enable business to achieve its goals and objectives

Increase value with less risk

C (Confidentiality) —— 避免有意或無意未經授權的資料存取

I (Integrity) —— 避免有意或無意未經授權的修改、刪除

A (Availability) —— 確保即時穩定的服務

N (Non-repudiation) —— 防止行為或訊息事後否認

P (Privacy) —— 防止個人識別資訊 (Personal Identity Information, PII) 被複製或用於詐欺

S (Safety) —— 防止數據錯誤導致未經授權的傷害、死亡或損壞

為了支持組織的業務、創造價值、實現組織的使命與願景，透過安全管制措施保護資訊資產免受危害。

Knowledge check

Bob is designing a messaging system for a bank and would like to include a feature that allows the recipient of a message to prove to a third party that the message did indeed come from the purported originator. What goal is Bob trying to achieve?

- A. Authentication
- B. Authorization
- C. Integrity
- D. Nonrepudiation

版權所有，翻印必究

Roles & Responsibilities

Roles — Senior management、Security manager / officer / director、Security personnel、Administrators / Technicians、Users

Due Care

執行階層人員是否有做該做的事情。

Polices and implemented actions that an organization has taken to minimize risk to its tangible and intangible assets.

考題：Which one of the following principles imposes a standard of care upon an individual that is broad and equivalent to what one would expect from a reasonable person under the circumstances? 下列哪一項原則對個人施加了廣泛且相當於在這種情況下對理性人的期望的謹慎標準？

Due Diligence

管理階層是否有盡責保護與降低組織的風險。

Continual actions that an organization are doing to protect and minimize risk to its tangible and intangible assets.

ARCI Responsibility Assignment Matrix

Accountable — Accountable parties ensure accountability to project deadlines, and ultimately, accountability to project completion. (負無限責任的人)

Responsible — The responsible team is comprised of the project's "doers", working hands-on to ensure that each deliverable is completed. (做事的人)

Consulted — Consulted individuals' opinions are crucial, and their feedback needs to be considered at every step of the game. (被諮詢的人)

Informed — Informed persons are those that need to stay in the loop of communication throughout the project. (被告知的人)

Implementation of Security – 對人的部分



Knowledge check

Lydia is processing access control requests for her organization. She comes across a request where the user does have the required security clearance, but there is no business justification for the access. Lydia denies the request. What security principle is she following?

- A. Need to know
- B. Least privilege
- C. Separation of duties
- D. Two-person control

Gary is implementing a new website architecture that uses multiple small web servers behind a load balancer.

What principle of information security is Gary seeking to enforce?

- A. Denial
- B. Confidentiality
- C. Integrity
- D. Availability

版權所有，翻印必究

Implementation of Security – 對事(物)的部分



Knowledge check

What type of access control is intended to discover unwanted or unauthorized activity by providing information after the event has occurred?

- A. Preventive
- B. Corrective
- C. Detective
- D. Directive

Which of the following types of controls does not describe a mantrap?

- A. Deterrent
- B. Preventive
- C. Compensating
- D. Physical

版權所有，翻印必究

Knowledge check

Beth is a human resources specialist preparing to assist in the termination of an employee. Which of the following is not typically part of a termination process?

- A. An exit interview
- B. Recovery of property
- C. Account termination
- D. Signing an NCA

版權所有，翻印必究

Knowledge check

The Acme Widgets Company is putting new controls in place for its accounting department. Management is concerned that a rogue accountant may be able to create a new false vendor and then issue checks to that vendor as payment for services that were never rendered. What security control can best help prevent this situation?

- A. Mandatory vacation
- B. Separation of duties
- C. Defense in depth
- D. Job rotation

Policy, Standard, Procedure, and Guideline



Knowledge check

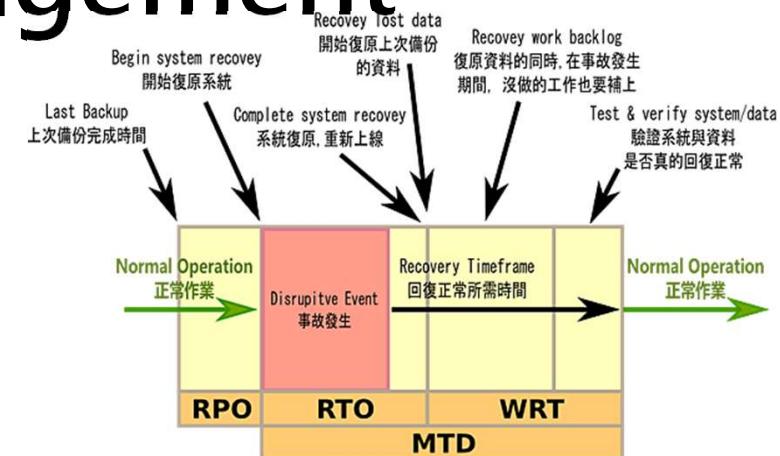
Yolanda is writing a document that will provide configuration information regarding the minimum level of security that every system in the organization must meet. What type of document is she preparing?

- A. Policy
- B. Baseline
- C. Guideline
- D. Procedure

版權所有，翻印必究

Business Continuity Management (BCM) – 評估

主要的內容在 Domain 7, BCM 包含了 BCP 和 DRP 的內容



Business Impact Assessment (BIA) 營運衝擊分析 -②

評估

RPO (Recovery Point Objective, 復原點目標) — 系統中斷到重啟期間所損失的資料量

RTO (Recovery Time Objective, 復原時間目標) — 系統重啟、初步回復正常運作所需花費的時間

Measurements of Time

WRT (Work Recovery Time) — 讓所有業務和作業，回到事故發生前的水平 (恢復SLA) 所需的時間

MTD (Max Tolerable Downtime) = AIW (Acceptable Interruption Window) — 可容許的最長系統 Down Time

計畫 -⑨

時間軸插圖 -①

演練 -⑨



Knowledge check

Florian is building a disaster recovery plan for his organization and would like to determine the amount of time that a particular IT service may be down without causing serious damage to business operations. What variable is Florian calculating?

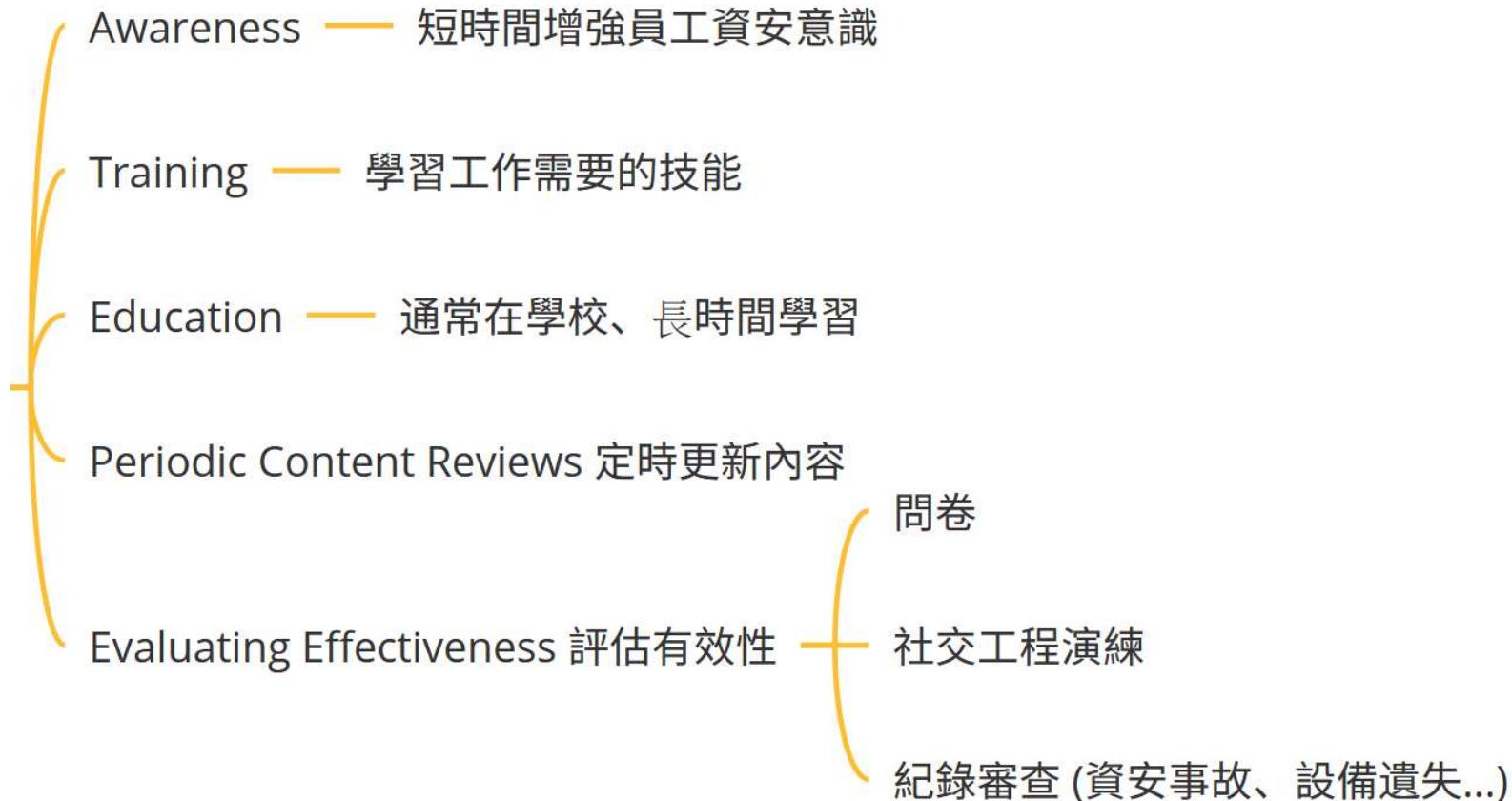
- A. RTO
- B. MTD
- C. RPO
- D. SLA

版權所有，翻印必究

Business Continuity Management



Training Awareness & Education

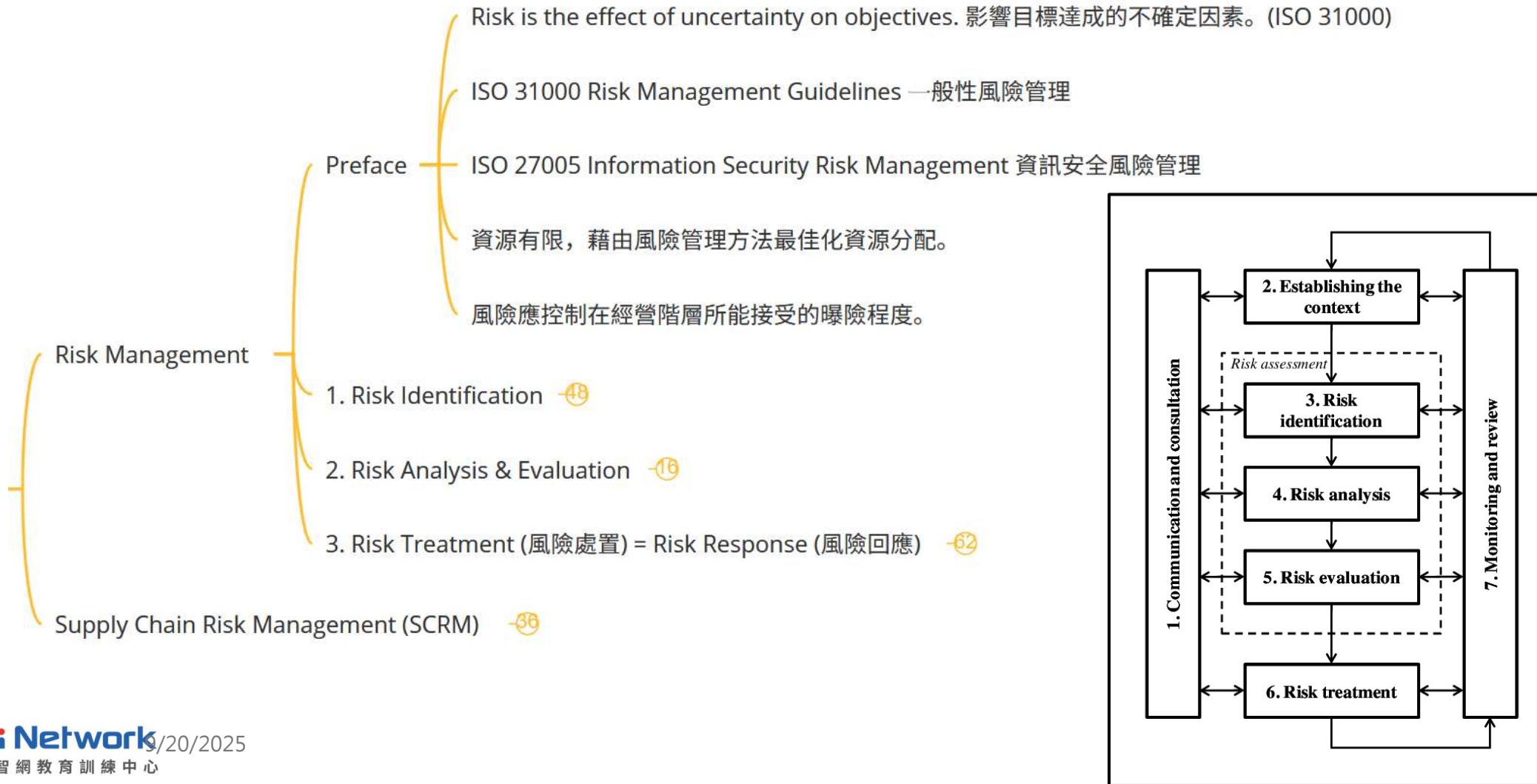


1.2 Risk

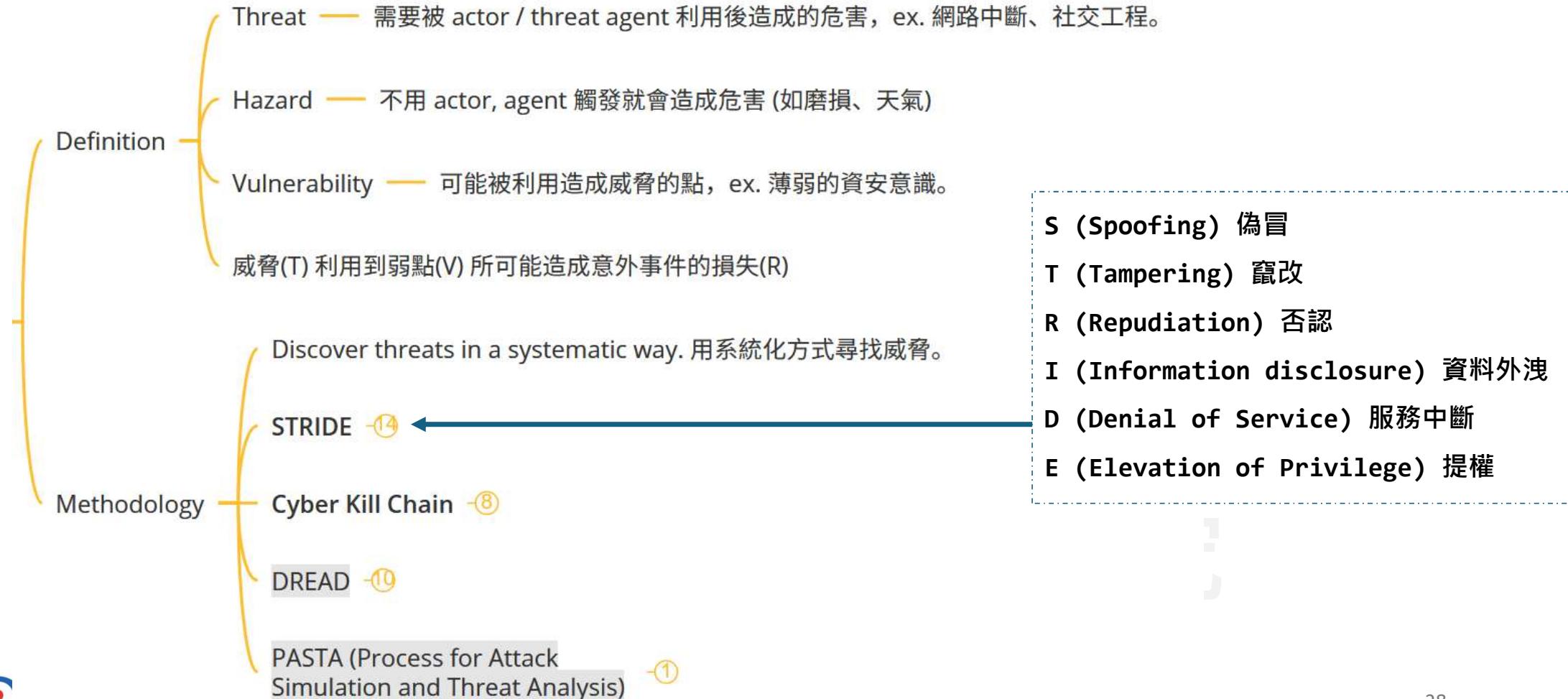


版權所有，翻印必究

Risk



Risk Identification - 1



Risk Identification - 2 (Cyber Kill Chain)



Risk Analysis & Evaluation



Knowledge check

Henry is the risk manager for Atwood Landing, a resort community in the midwestern United States. The resort's main data center is located in northern Indiana in an area that is prone to tornados. Henry recently undertook a replacement cost analysis and determined that rebuilding an reconfiguring the data center would cost \$10 million.

Henry consulted with tornado experts, data center specialist, and structural engineers. Together, they determined that a typical tornado would cause approximately \$5 million of damage to the facility. The meteorologists determined that Atwood's facility lies in an area where they are likely to experience a tornado one every 200 years.

Knowledge check

Base upon the information in this scenario, what is the exposure factor (EF) for the effect of a tornado on Atwood Landing' s data center?

- A. 10%
- B. 25%
- C. 50%
- D. 75%

版權所有，翻印必究

Knowledge check

Base upon the information in this scenario, what is the annualized rate of occurrence (ARO) for a tornado at Atwood Landing' s data center?

- A. 0.0025
- B. 0.005
- C. 0.01
- D. 0.015

版權所有，翻印必究

Knowledge check

Base upon the information in this scenario, what is the annualized loss expectancy (ALE) for a tornado at Atwood Landing' s data center?

- A. \$25,000
- B. \$50,000
- C. \$250,000
- D. \$500,000

版權所有，翻印必究

3. Risk Treatment - 1



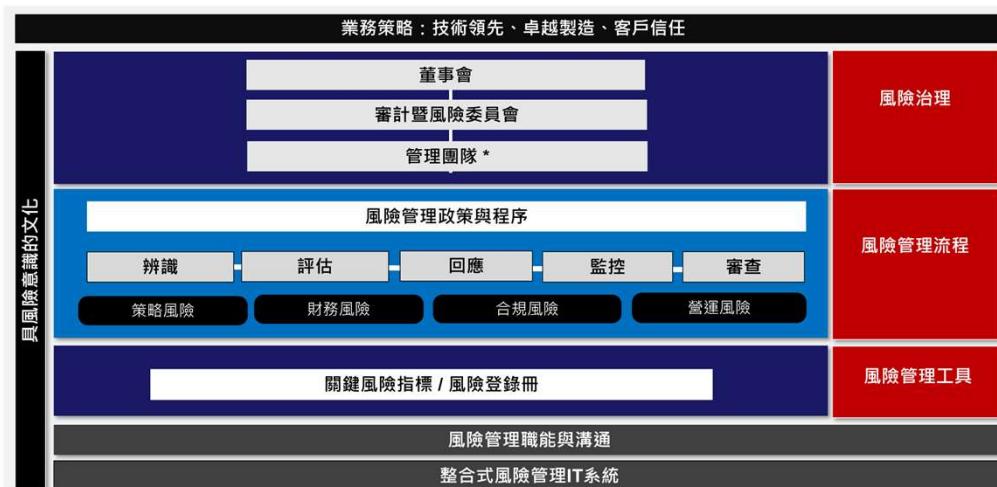
風險管理案例參考

風險胃納聲明與風險管理範疇

台積公司制定了風險胃納聲明，概述公司為實現企業目標而願意承擔的風險之性質和程度，包括：

- **策略風險**：應審慎評估公司所承擔的風險，確保與商業酬報相稱，並與公司的策略、投資、財務和企業目標相一致。
- **營運風險**：應將風險考量整合到營運流程中，並將風險控制在各廠處、功能組織和公司的風險容忍度（風險指標）之內。
- **財務風險**：台積公司不投資或參與任何超出風險忍受度的業務活動。
- **ESH與合規風險**：絕不縱容影響安全的違規或過失、違反法律法規以及詐欺、賄賂和貪汙腐敗等行為。

各功能組織與部門依據辨識、評估、回應、監控及審查的五個循環式流程來進行風險管理，提出企業層級風險矩陣及控制措施，呈報審計委員會，透過持續性的教育訓練來強化更具風險意識的思維與文化。



策略風險	營運風險
<ul style="list-style-type: none">• 產業發展• 科技變革（包含資訊技術安全）• 需求及平均售價下滑• 競爭• 重要政策及法律變動	<ul style="list-style-type: none">• 天然及人為災害• 產能擴充• 新建廠• 銷售集中• 採購集中• 智慧財產權• 訴訟或非訴訟事件• 併購• 招募人才• 未來研發計劃及預計投入之研發費用• 企業形象改變對企業危機管理之影響• 經營權改變• 未遵循出口管控、環保及氣候變遷相關法規及協議，或未即時取得營運所需相關許可之風險
財務風險 <ul style="list-style-type: none">• 經濟風險（包含利率變動、匯率變動、通貨膨脹及稅務法規變動或實施新稅法）• 融資• 高風險 / 高槓桿投資、資金貸與他人、背書保證及衍生性金融商品交易• 減損損失	
其他風險 <ul style="list-style-type: none">• 台積公司之董事或持股超過10%之大股東，股權之大量移轉或更換• 貿易政策	

Ref. <https://investor.tsmc.com/chinese/risk-management>

Knowledge check

Rolando is a risk manager with a large-scale enterprise. The firm recently evaluated the risk of California mudslides on its operations in the region and determined that the cost of responding outweighed the benefits of any controls it could implement. **The company chose to take no action at this time.** What risk management strategy did Rolando's organization pursue?

- A. Risk avoidance
- B. Risk mitigation
- C. Risk transference
- D. Risk acceptance

3. Risk Treatment – Mitigate (緩解)



Supply Chain Risk Management (SCRM) - 1



Supply Chain Risk Management (SCRM) - 2

甲方開出安全需求 (SLR)，之後甲乙雙方再針對安全要求協議出的安全內容 (SLA)，SLA作為合約的附件

Service Level Requirement (SLR)

Service Level Agreement (SLA)

服務供應商與客戶之間定義的正式承諾。服務供應商與受服務使用者之間具體達成了承諾的服務指標—品質、可用性，責任。

作為驗收依據(請款、減價驗收)

3rd Party Assessment and Monitoring (Domain 6)

Governance review
治理審查

—— 請廠商自評

Site security review
現地審查

—— 實體安全稽核、現地訪談

Formal security audit
正式審查

—— 依合約規範，用特定的標準稽核 (可利用的標準 ex. ISO, CSA STAR... 等等 Compliance 專章說明)

Penetration testing
滲透測試

—— 找到可以被利用的漏洞



1.3 Compliance

版權所有，翻印必究

Compliance – 基本法律

執行資訊安全的主要目的之一 (法規要求、客戶要求)

基本法律

FISMA (Federal Information Security Management Act) (美國)資訊安全根本大法。架構的宗旨是保護美國政府，避免遭受網路安全攻擊和自然災害，致使敏感資料遭遇風險

SOX (Sarbanes-Oxley Act) 沙賓法案 (美國)上市公司，對公司經營高層做法律的問責

HIPAA (Health Insurance Portability and Accountability Act) (美國)促進醫療健康產業善加利用新科技，並為醫療資訊的安全和隱私建立屏障

HITECH (Health Information Technology for Economic and Clinical Health) (美國)促進醫療健康產業善加利用新科技，並為醫療資訊的安全和隱私建立屏障

GDPR (General Data Protection Regulation) (歐盟)個資保護

Gramm-Leach-Bliley Act (GLBA) GLBA mandates requirements for securing personal account information in the financial and insurance industries

Compliance – IP, Import/Export Control



Compliance - Privacy



Compliance – Privacy – OECD Guidelines

Collection Limitation 限制蒐集原則 — 對個人資料的收集應該有所限制，任何此類資料都應該透過合法和公平的手段獲取，並在適當的情況下，在資料主體知情或同意的情況下獲取。

Data Quality 品質確保原則 — 個人資料應與使用目的相關且在這些目的的必要範圍內，應準確、完整並保持最新。

Purpose Specification 目的明確原則 — 應在開始收集資料之前或之時指定收集個人資料的目的，且隨後的使用應限於實現這些目的或與這些目的不相抵觸的其他目的，並在每次改變目的時予以指定。

Use Limitation 限制目的外使用原則 — 個人資料不應披露、提供或以其他方式用於[目的明確原則]所規定之目的以外的其他目的，除非：a) 經資料主體同意；或 b) 經法律授權。

Security Safeguards 安全保障原則 — 個人資料應受到合理的安全保障措施的保護，以防止資料丟失或未經授權的存取、破壞、使用、修改或披露等風險。

Openness 公開原則 — 在個人資料的開發、實踐和原則方面，應當有一個總體的開放性原則。

Individual Participation 個人參與的原則 — 個人應當有權詢問 Data Controller 是否有與之相關的資料、可以向 Data Controller 合理收費，可要求清除、修正資料。

Accountability 責任明確原則 — 資料控制者應該對遵守落實上述原則的措施負責。

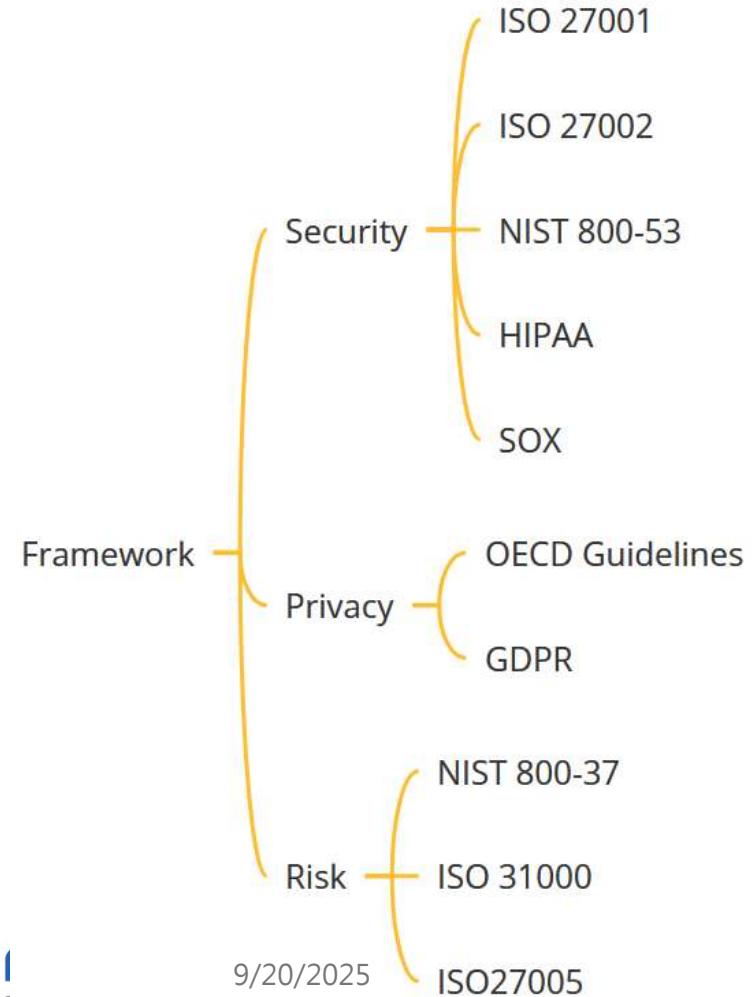
Compliance – Privacy – GDPR



Assurance 保證



Assurance - Framework



有，翻印必究

CC (Common Criteria) ISO 15408



CMMI / SAMM 能力成熟度模型

將軟體開發流程視為一種工程(製造)流程，利用控制、量測、改善(control, measure, and improve)等循序漸進的方法，達到軟體流程改善的一個框架

ML 1 (initial) —— 企業有開發軟體產品的能力，但掌控專案時程、成本、流程的能力不佳。

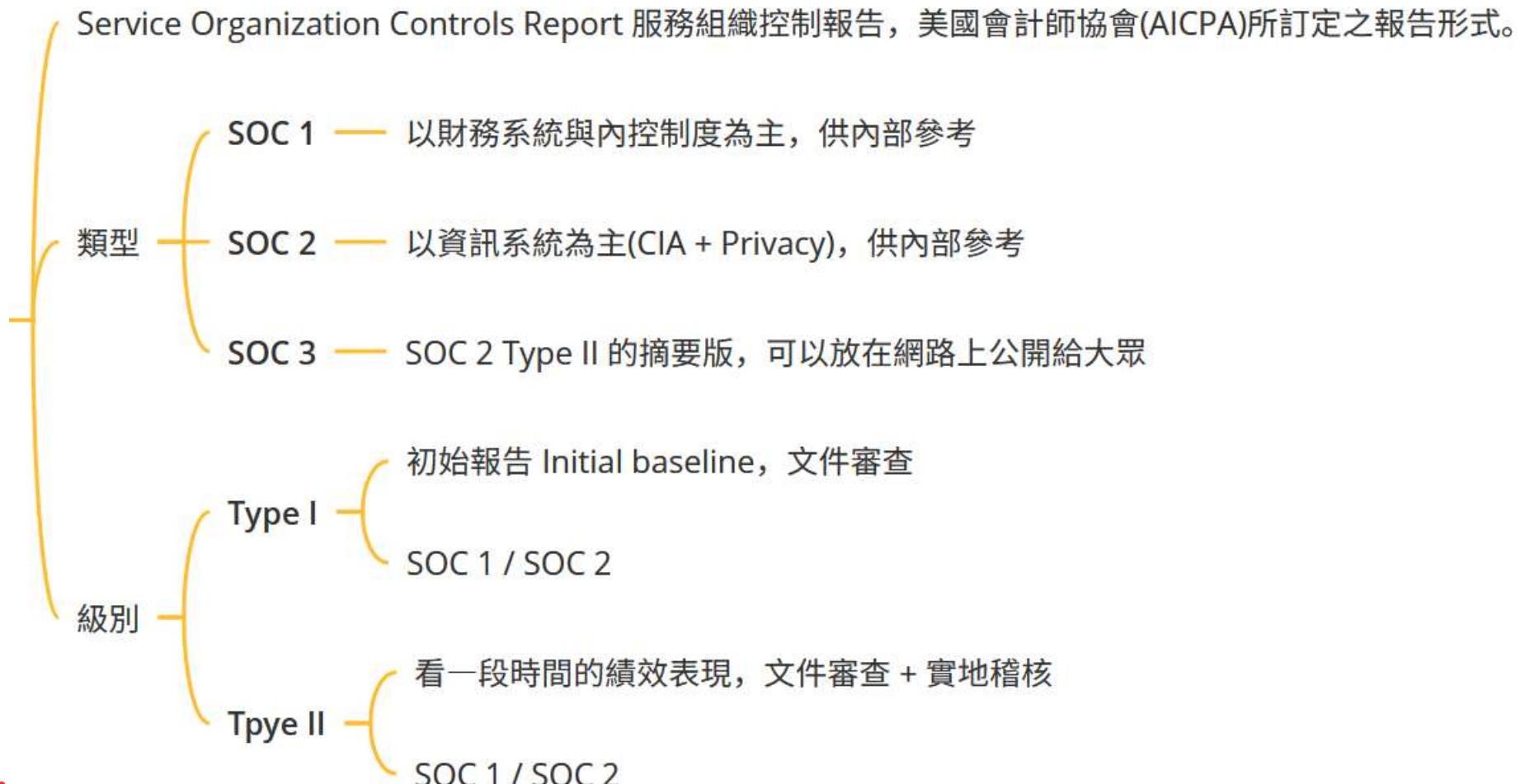
ML 2 (managed) —— 具備ML 1的能力，且對於專案的需求、流程、產出物具有管理能力，能在特定時間點(如專案里程碑到達時)交付產出物。但流程則可能因專案而異，仍未加規範。

ML 3 (defined) —— 具備ML 1、ML 2的能力，且企業對常用的流程以及其修改方式均加以定義。

ML 4 (quantitatively managed) —— 具備ML 1、ML 2、ML 3的能力，且以統計方法進行流程控管，了解其實施作法的變異性，以供採取因應措施。

ML 5 (optimized) —— 具備ML 1、ML 2、ML 3、ML 4的能力，且具有調整與修正流程的能力，使其達到最佳化。

SOC (AICPA SSAE 20)



PCIDSS & CSA STAR

PCIDSS — 行業標準 - 支付卡

CSA STAR 雲端安全認證
(Cloud Security Alliance
Security, Trust and
Assurance Registry)

雲端安全聯盟提出的，屬於ISO 27001 的加強版

CSA STAR = ISO27001 + 雲端控制矩陣(Cloud Control Matrix, CCM) + 成熟度評估

版權所有，翻印必究

Knowledge check

Robert is responsible for securing systems used to process credit card information.

What security control framework should guide his action?

- A. HIPAA
- B. PCI DSS
- C. SOX
- D. GLBA

版權所有，翻印必究

Knowledge check

You are evaluating and selecting software vendors to **customize** the transportation management system in a procurement project. Which of the following is **least likely** to be part of the evaluation criteria for the vendor qualification?

- A. FOCI (Foreign Ownership, Control, and Influence)
- B. Capability Maturity Model Integration (CMMI)
- C. Software Assurance Maturity Model (SAMM)
- D. Common Criteria (ISO 15408)

Knowledge check

You are the CISO for a major hospital system and are preparing to sign a contract with a software as a service (SaaS) email vendor and want to perform a control assessment to ensure that its business continuity planning measures are reasonable. What type of audit might you request to meet this goal?

- A. SOC 1 Type 1
- B. SOC 1 Type 2
- C. SOC 2 Type 1
- D. SOC 2 Type 2

Understand and support business continuity plan (BCP) and disaster recovery plan (DRP) activities

Glenda would like to conduct a disaster recovery test and is seeking a test that will allow a review of the plan with no disruption to normal information system activities and as minimal a commitment of time as possible. What type of test should she choose?

- A. Tabletop exercise
- B. Parallel test
- C. Full interruption test
- D. Checklist review

版權所有，翻印必究

Understand risk management

As a security professional, you are analyzing a sophisticated cyberattack targeting your organization's network. The attacker has successfully conducted reconnaissance and weaponized a phishing email with a malicious payload. Your intrusion detection system (IDS) has flagged unusual network traffic, indicating a potential compromise. According to the Cyber Kill Chain model, which of the following actions should you prioritize to disrupt the attack at the current stage, assuming the attacker is likely in the "Command and Control" phase?

- A. Deploy a patch to all systems to address a known vulnerability exploited in the initial attack vector.
- B. Block outbound traffic to the suspicious IP addresses identified by the IDS to disrupt communication with the attacker's server.
- C. Conduct a full system scan to identify and remove the malicious payload from infected endpoints.
- D. Reset all user credentials to prevent further exploitation of stolen credentials.

Understand risk management

An organization identifies a high-risk vulnerability in a legacy system critical to its operations. The system cannot be immediately replaced due to budget constraints and operational dependencies, but the vulnerability could potentially allow unauthorized access to sensitive customer data. As a security professional tasked with recommending a risk management strategy, which of the following approaches is most appropriate to address this vulnerability while balancing business continuity and security requirements?

- A.Accept
- B.Transfer
- C.Mitigate
- D.Avoid

版權所有，翻印必究

Understand legal and regulatory concerns (e.g., jurisdiction, limitations, privacy)

An international organization operates across multiple jurisdictions, each with distinct and sometimes conflicting legal and regulatory requirements. A new data protection regulation in one jurisdiction increases the risk of non-compliance due to its ambiguous language, which allows for varied interpretations. As a security professional, you are tasked with recommending a strategy to address the compliance challenges posed by this new regulation while minimizing the organization's risk exposure. Which of the following approaches is most effective in ensuring compliance and managing risk in this complex, multi-jurisdictional environment?

- A. Adopt a single, standardized compliance policy based on the strictest jurisdiction's requirements and apply it uniformly across all operations.
- B. Delegate compliance responsibilities to local teams in each jurisdiction, allowing them to interpret and implement regulations independently.
- C. Develop a flexible compliance framework that includes regular legal reviews, stakeholder consultations, and proactive monitoring to adapt to regulatory changes and interpretations.
- D. Ignore the ambiguous regulation until clearer guidelines are provided to avoid misinterpretation and potential penalties.

Operate and monitor security platforms (e.g., continuous monitoring)

An organization needs to meet compliance requirements for real-time threat detection and maintain customer trust. Which approach best uses continuous monitoring to ensure effective security controls?

- A. Use real-time monitoring only, without analyzing historical data.
- B. Rely on periodic audits without real-time monitoring.
- C. Implement real-time monitoring and retrospective analysis for threat detection and compliance.
- D. Monitor network performance without tracking security events.

版權所有，翻印必究

Operate and monitor security platforms (e.g., continuous monitoring)

An organization aims to enhance incident response with efficient log management across multiple servers. Which approach best balances log volume, security, and anomaly detection?

- A. Log every failed login, store locally, review monthly.
- B. Use centralized logging, clip at two failed logins per hour, secure logs, filter for anomalies.
- C. Use decentralized logging, retain one month, manually filter for issues.
- D. Outsource logging, retain three months, no clipping or filtering.

Analyze monitoring results

An organization is implementing security baselines to protect sensitive assets, including Personal Health Information (PHI), and enhance incident detection. Which approach best uses baselines to detect and respond to Indicators of Compromise (IoCs) like unauthorized privilege escalation or data movement?

- A. Set baselines for all assets without categorization, log all events, and review manually monthly.
- B. Categorize assets by sensitivity, define role-based controls, monitor for baseline deviations, and investigate anomalies like privilege escalation.
- C. Apply generic controls to all assets, monitor for session terminations only, and respond after incidents occur.
- D. Use baselines without monitoring, relying on audits to detect data copying attempts.



Domain 2

Asset Security (10%, 30min)

版權所有，翻印必究

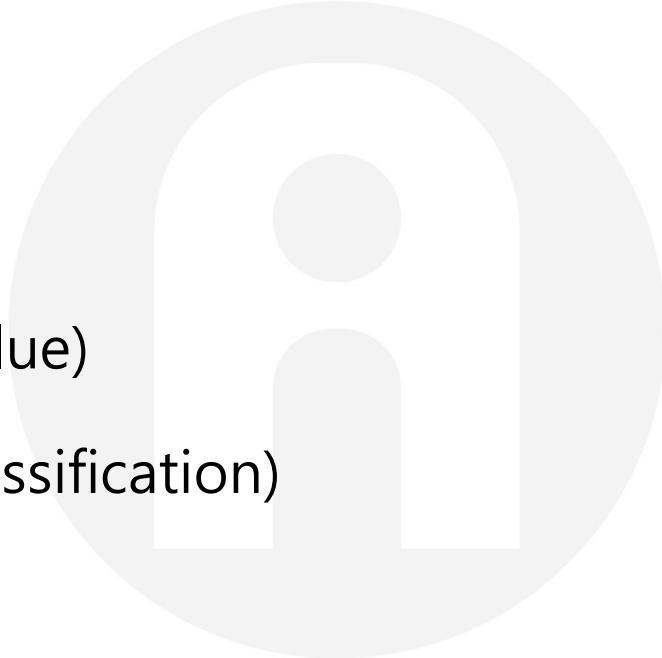
Outline

2.1 Asset Inventory

2.2 Classify (base on Value)

2.3 Protect (base on Classification)

2.4 Assess & Review



版權所有，翻印必究

2.1 Asset Inventory

- 實體資產、軟體資產、電子化資訊資產、書面文件、服務及人員
- Assign Ownership — 對保護資產負責、確定資產對組織的價值
- Configuration Management (CMDB) 組態管理 — We will discuss it in Domain 7 Security Operations

版權所有，翻印必究

2.2 Classify (base on Value)



2.3 Protect (base on Classification) - 1



Knowledge check

As a DBA, Amy's data role in her organization includes technical implementations of the data policies and standards, as well as managing the data structures that the data is stored in. What data role best fits what Amy does?

- A. Data custodian
- B. Data owner
- C. Data processor
- D. Data user

版權所有，翻印必究

2.3 Protect (base on Classification) - 2

Create — 盡早分類，應透過 Security Policy / Standard 影響 User，亦可透過應用程式強制 User 於存檔時進行分類

Access Control

確保「有」經授權的存取、修改、刪除

We will discuss it in Domain 5 Identity and Access Management (IAM)

Store

Backups

確保出事後仍有辦法還原

We will discuss in Domain 7 Security Operations

Encryption

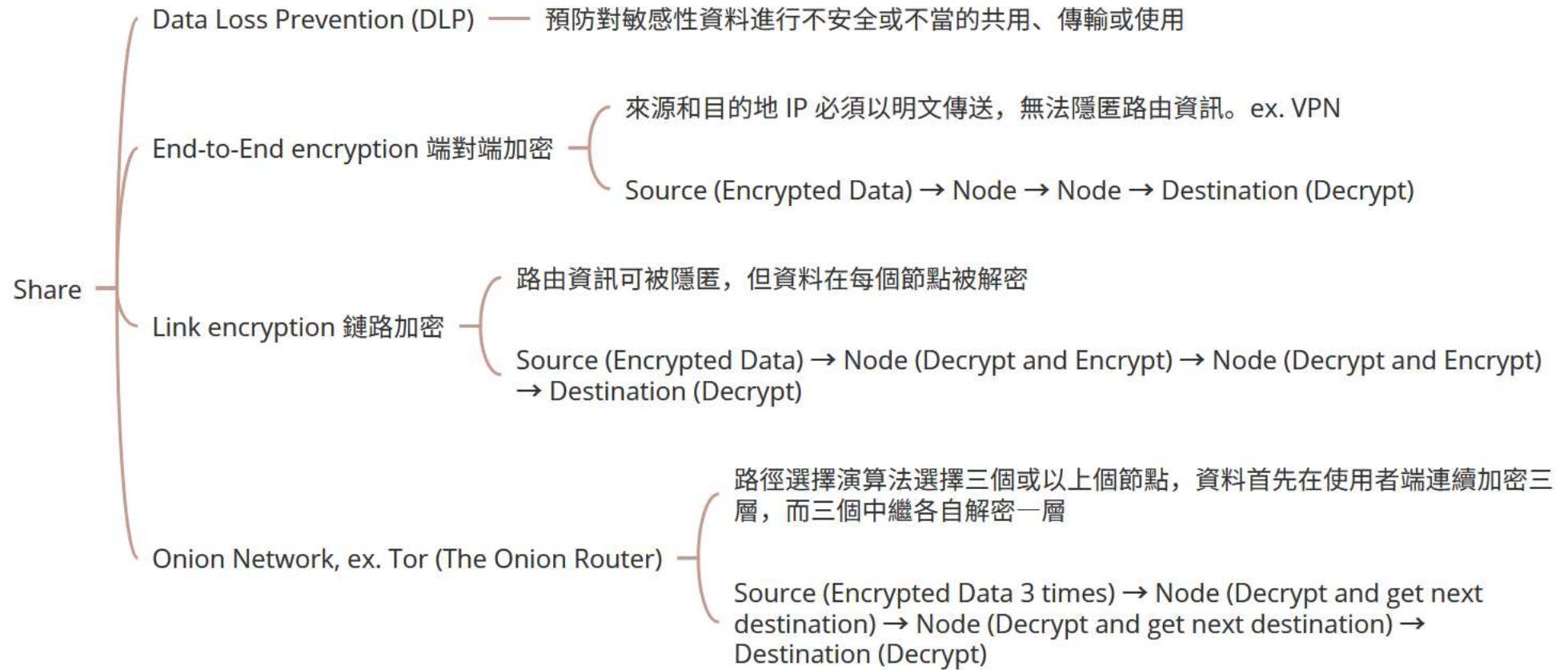
最後一道防線，在有限的時間內不被破解

We will discuss in Domain 3 Security Architecture and Engineering

2.3 Protect (base on Classification) - 3

Digital Right Management (DRM) 數位版權管理	管理版權內容的一系列演算法加密技術，重點是放在拷貝保護、複製控制等，主要應用在影音服務、電子書等
Cloud Access Security Broker (CASB) 雲端存取資安代理	在雲端軟體使用方及供應方之間控管雲端存取的第三方資安代理政策工具，也就是 User 及其存取的所有雲端服務之間的媒介
Use Pseudonymization (假名)	仍可使用對照表，還原可識別唯一性 (可逆)
Anonymization (匿名, 去識別化)	去識別化後的資料即為一般資料 去除可識別唯一性 (不可逆)
Tokenization	用隨機字串取代資料，ex. Apple Pay 信用卡使用虛擬卡號保護真實卡號

2.3 Protect (base on Classification) - 4



2.3 Protect (base on Classification) - 5

Archive

法遵要求、資料保留政策、久久查一次

Ex. 檔案伺服器檔案轉磁帶，空間釋出

需注意儲存媒體的 EOS/EOL · 以及封存資料的加密金鑰保管問題

資料銷毀，需考量資料殘留問題 (Data Remanence)

Clearing (可救回來)

Erasing — 用 UI 操作的方式刪除資料，ex. 把檔案丟到資源回收桶

Format — 格式化

Destroy

Purging (救不回來)

Degauss — 消磁只適用於磁性硬碟或磁帶

Overwrite / Wipe — 用到 Purge 指令集 (有特定的 pattern)、覆寫資料

Cryptoshredding — 檔案加密後把金鑰刪除

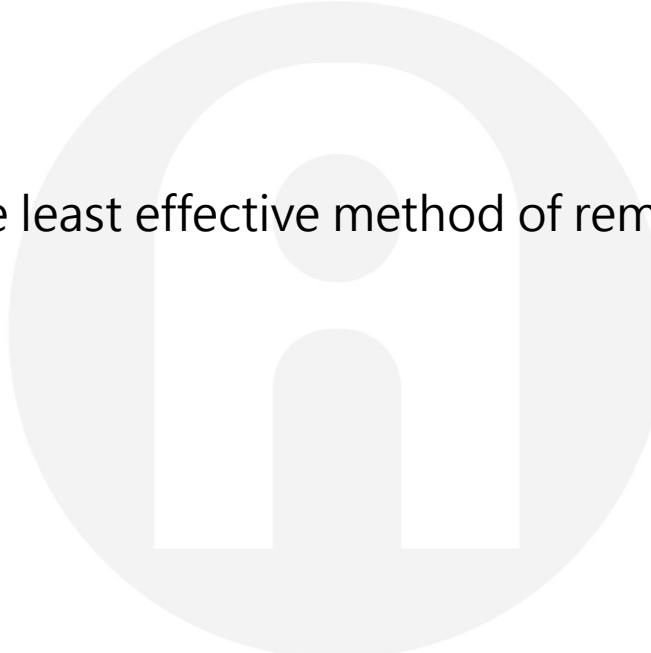
Destruction (救不回來、媒體無法重用) — Shred 粉碎 / Disintegrate 瓦解 / Drill 打孔

9/20/2023 Data Remanence: Destruction > Purging > Clearing

Knowledge check

Which of the following is the least effective method of removing data from media?

- A. Degaussing
- B. Purging
- C. Erasing
- D. Clearing



版權所有，翻印必究

Knowledge check

After scanning all the systems on his wireless network, Mike notices that one system is defined as an iOS device running a massively out-of-date version of Apple's mobile operation system. When he investigates further, he discovers that the device is an original iPad and that it cannot be updated to a current secure version of the operating system. What should Mike recommend?

- A. Retire or replace the device
- B. Isolate the device on a dedicated wireless network
- C. Install a firewall on the tablet
- D. Reinstall the OS

版權所有，翻印必究

Knowledge check

Bob is handling information that his organization classified as sensitive, which is a **moderate** security categorization in the NIST model. If the media is going to be sold as **surplus**, what process does Ben need to follow?

- A. Destroy, validate, document
- B. Clear, purge, document
- C. Purge, document, validate
- D. Purge, validate, document

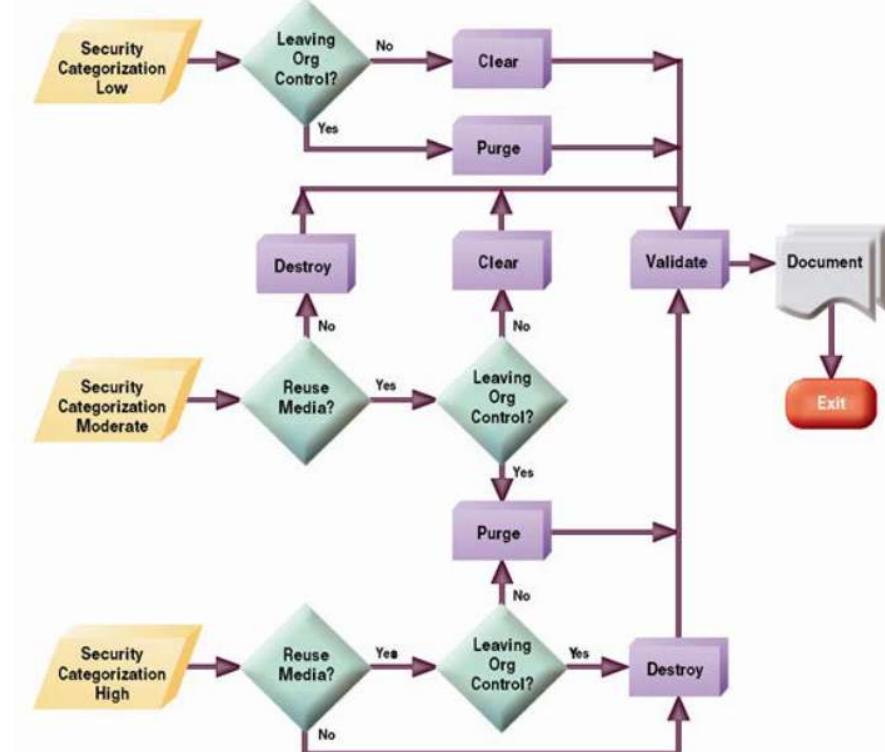


Figure 4-1: Sanitization and Disposition Decision Flow

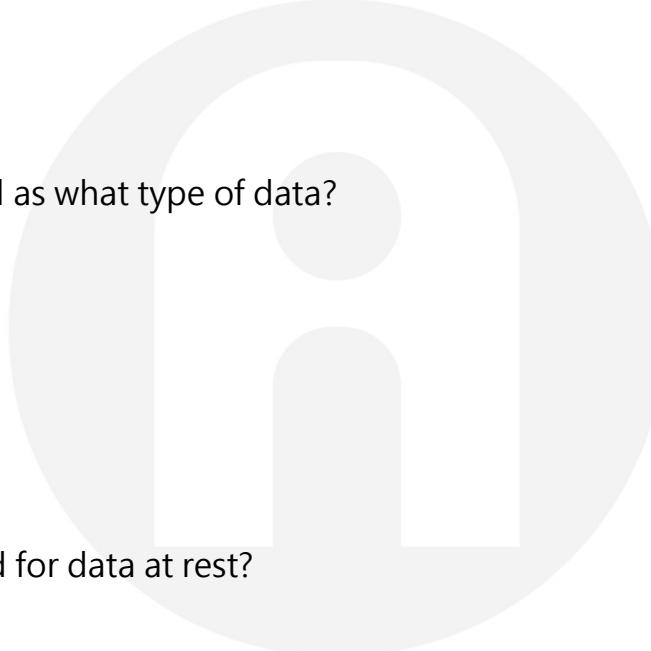
Knowledge check

Data stored in RAM is best characterized as what type of data?

- A. Data in rest
- B. Data in use
- C. Data in transit
- D. Data at large

What type of encryption is typically used for data at rest?

- A. Asymmetric encryption
- B. Symmetric encryption
- C. DES
- D. OTP



版權所有，翻印必究

2.4 Assess & Review

- 定期審查、評估當前的盤點、分類、保護是否符合公司全景 (Context)。
- 應依據法律、法規或業務需求進行調整。

版權所有，翻印必究



Domain 3

Security Architecture and Engineering

(13%, 120min)

板權所有，翻印必究

Outline

3.1 Models

3.2 Trusted Computing Base (TCB)

3.3 Vulnerabilities

3.4 Cryptography

3.5 Digital Certificates, Digital Signatures & PKI

3.6 Cryptanalysis

3.7 Physical Security



版權所有，翻印必究

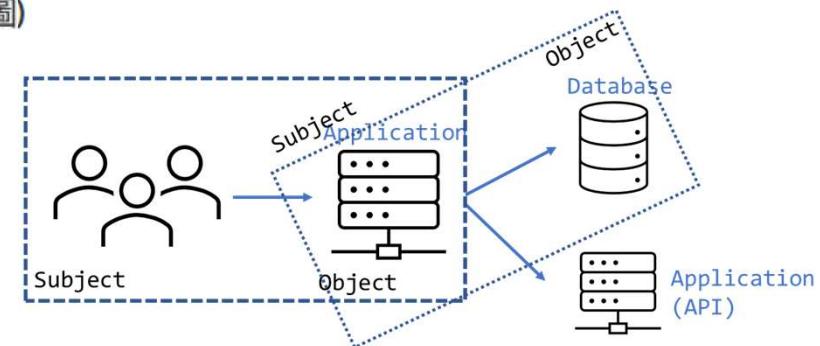
3.1 Models

Definition — conceptual representations of things 事物概念性的表徵 (簡圖)

Subject vs. Object

— Security Models (Category) —

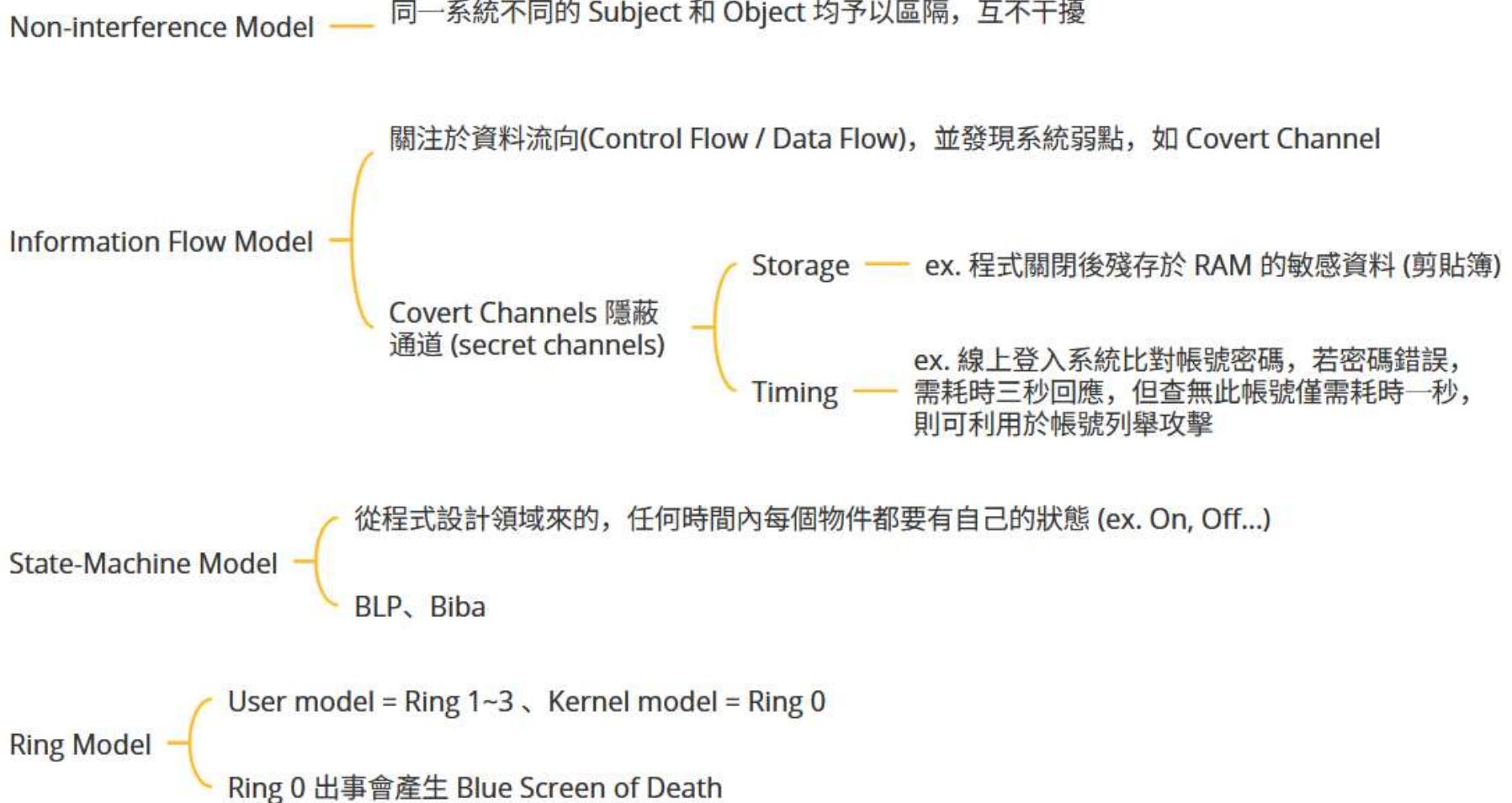
- Non-interference Model -①
- Information Flow Model -⑥
- State-Machine Model -②
- Ring Model -②



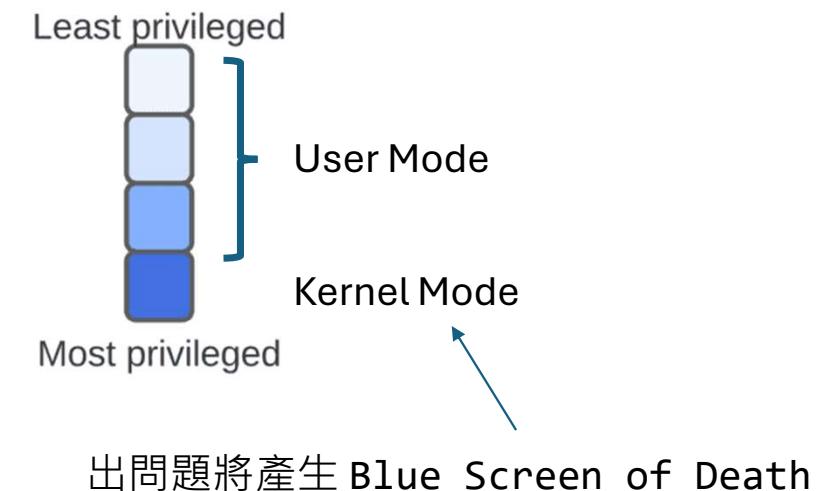
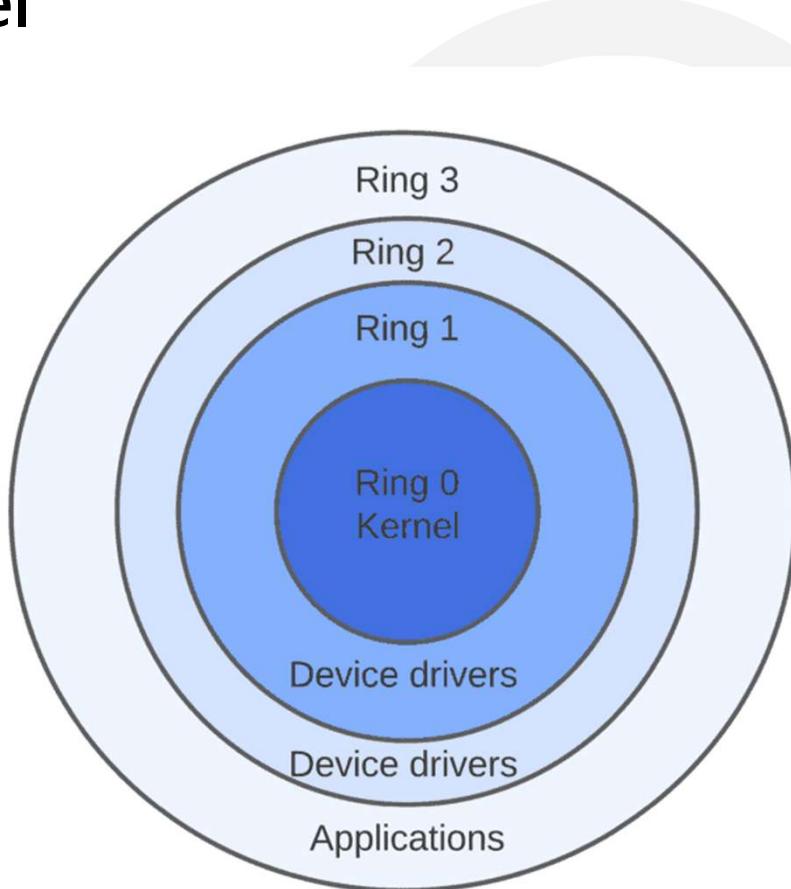
Security Models (Authorization)

- Non-Discretionary Access Control (NDAC) -⑤
- Discretionary Access Control (DAC) -⑨
- Mandatory Access Control (MAC) -⑩
- Others -⑫

3.1.3 Security Models (Category)



Ring Model



3.1.4 Security Models (Authorization) - NDAC

- 嚴格的模型，只有 Central Authority 決定存取權
- Role-based Access Control (RBAC) —— 依照使用者的身分給予對應的權限，系統的管理員可以依據組織內的架構或是分工項目，按照對應的職責身分開啟不同的權限，再將使用者賦予這些身分的權限。
- Risk-based Access Control —— 利用各種參數判斷使用者的訪問請求風險高低，如在低風險的情境下，系統僅使用雙因素身分驗證，當風險不斷增加時，則使用者需要通過額外的挑戰

版權所有，翻印必究

3.1.4 Security Models (Authorization) - DAC

- Data Owner 可自主決定
- Attribute-based Access Control — 屬性存取控制，以用戶 (or Subject) 的屬性，來落實存取控制的管理，譬如像是工作職位、層級、單位、部門、參與專案、以及各種其他的特徵，都可以被用來當作判斷的屬性
- Rule-Based Access Control — 權限的啟用與管理不再依據組織內的腳色進行設定與調整，而是由既定的規則、情況作為權限的依歸。比如說依靠使用者的位置進行權限開放與否的抉擇、針對使用的時間、裝置等。
- Access Control Matrix (ACM) —
 - Access Control List (ACL) + Capability Table
 - ACL 從資源設定權限 (存取控制清單)
 - Capability Table 從人的角度設定權限 (能力表)

九必印而印曲月川八月惟以

3.1.4 Security Models (Authorization) - MAC

嚴格的模型，只有 Central Authority 決定存取權，且為 Top-down

- Bell-LaPadula
 - Layer / Lattice-based、上層為機密性較高的資料
 - 關注機密性，通常用於軍方
 - Simple Security Property —— 不可以往上讀 (窺探機密)
 - Star Property —— 不可以往下寫 (洩漏機密)
 - Strong Star Property —— 只能寫入機密等級相同的 Obj

- Biba
 - Layer / Lattice-based、上層為完整度較高的資料
 - 關注完整性，通常用於商業
 - Simple Integrity Property —— 只准往上讀 (避免完整性破壞)
 - Star Integrity Property —— 只准往下寫 (避免完整性破壞)

9/20/2025 Invocation (調用屬性) —— Service Request 只能向Classification相同或更低的Obj 發送

3.1.4 Security Models (Authorization) - Others



Knowledge check

Matthew is the security administrator for a consulting firm and Must enforce access controls that restrict users' access based upon their previous activity. For example, once a consultant accesses data belonging to Acme Cola, a consulting client, they may no longer access data belonging to any of Acme' s **competitors**. What security model best fits Matthew' s needs?

- A. Clark-Wilson
- B. Biba
- C. Bell-LaPadula
- D. Brewer-Nash

版權所有，翻印必究

Knowledge check

Match the following numbered security models with the appropriate lettered security descriptions:

- Brewer and Nash
 - Graham-Denning
 - Bell-LaPadula
 - Biba
- A. This model blocks lower-classified objects from accessing higher-classified objects, thus ensuring confidentiality.
 - B. This * property of this model can be summarized as “no write-up”
 - C. This model uses security labels to grant access to objects via transformation procedures and a restricted interface model.
 - D. This model focuses on the secure creation and deletion of subjects and objects using eight primary protection rules or action.

版權所有：臺灣微軟

3.2 Trusted Computing Base (TCB)

Definition — 可信計算庫，電腦系統內保護機制的總和，包括硬體、韌體和軟體，負責執行安全策略的組合。

Reference Monitor Concept (RMC) -⑧

Hardware
Components
Processor, Central Processing Units (CPUs)
Storage -⑧

Protection Mechanisms -⑦

Software
Components
Firmware -①
System Kernel -②

Middleware -①

Protection Mechanisms -⑬

9/20/2025

89

3.2.2 Reference Monitor Concept (RMC) - 1

RMC 是一種概念，其將所有 Subject、Object 進行隔離，Subject 必須透過一定規則 (Security Kernel) 的中介 (Reference Monitor) 與存取 Object，並記錄和監視發生的行為(Audit)。

Subject 有自己的 Security Clearance、Object 有自己的 Security Classification

在電腦系統中，負責管制 Subject 及 Object 之間的存取行為

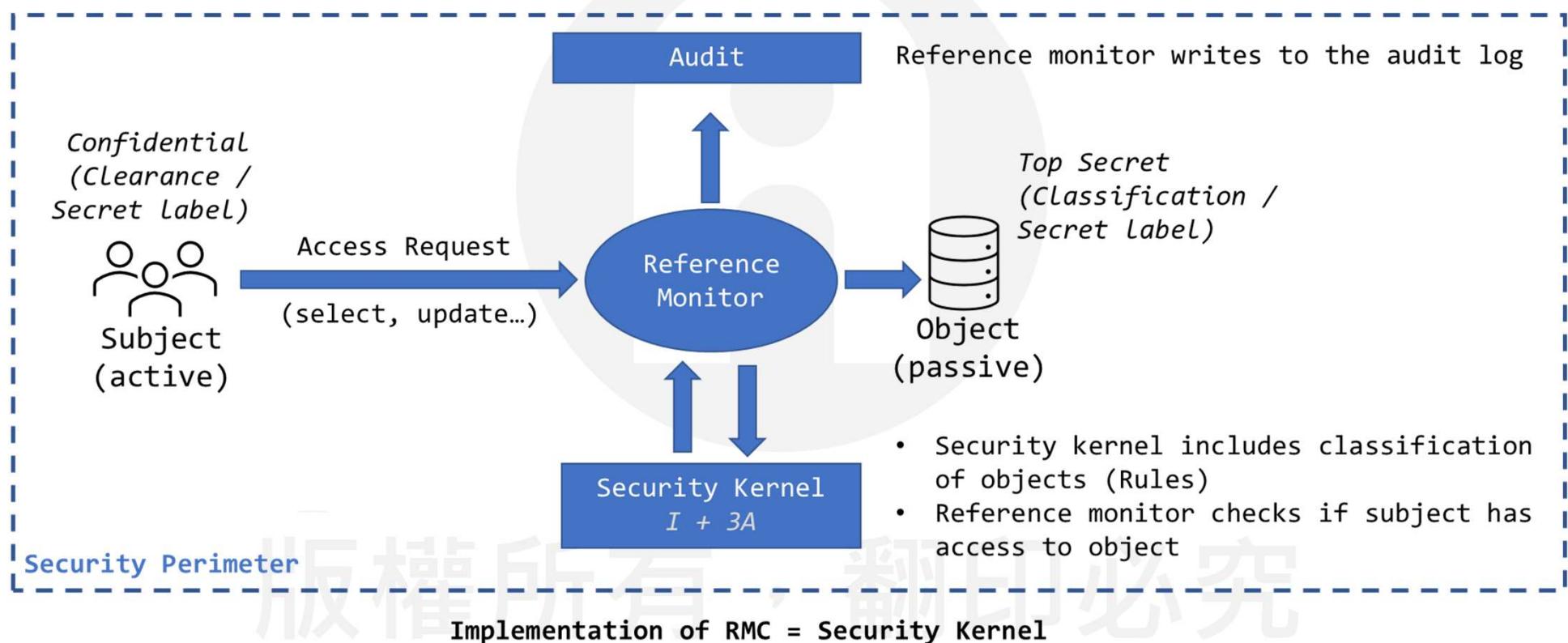
絕不能被繞過，要完全管制存取行為

中介層完全獨立不能被竄改

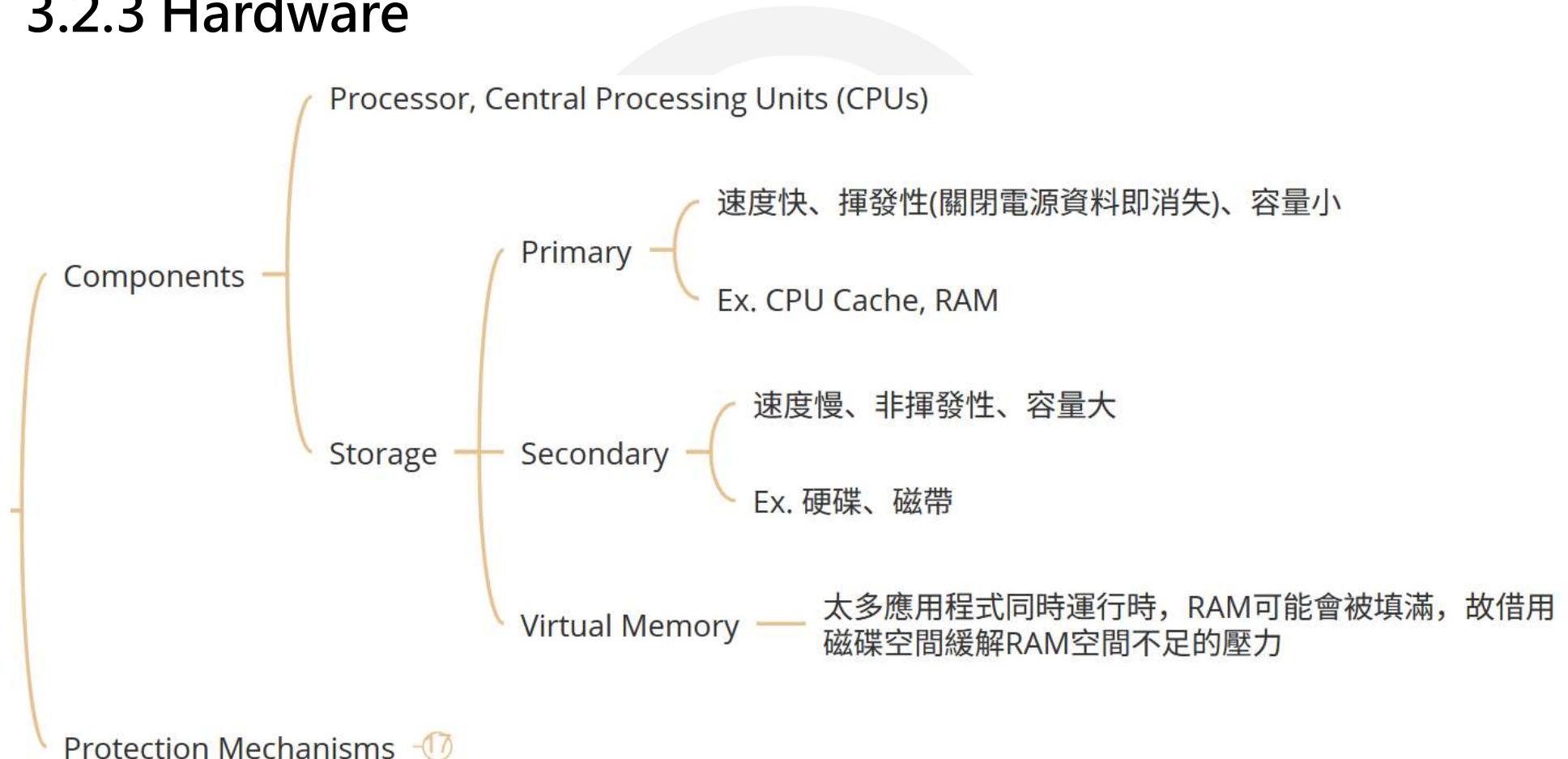
Subject 存取 Object 時，驗證 Subject 身份 (Authentication)、
確認行為授權 (Authorization)，並紀錄行為 (Accounting)

Security Kernel 安全核心

3.2.2 Reference Monitor Concept (RMC) - 2



3.2.3 Hardware



3.2.3.2 Hardware Protection Mechanisms

現代的系統均為多工(Multi-tasking)，代表可以同時運作多個應用程式。從安全的角度來看，必須確保所有的 Process 是隔離的，應用程式之間不能互相干擾，主要由兩種方式實現

Process Isolation

Memory Segmentation — 記憶體區隔，每個應用程式只能在固定的空間內運作

Time Division Multiplexing — 分時多工，每個 Process 只能在一小段時間內存取資源，然後在交給下一個，一次只允許 Process 訪問一個資源來隔離 Process

Ring Protection Model

Ring 3: User Programs

Ring 2: Libraries (理論, 未實作)、Ring 1: Drivers (理論, 未實作)

Ring 0: System Kernel

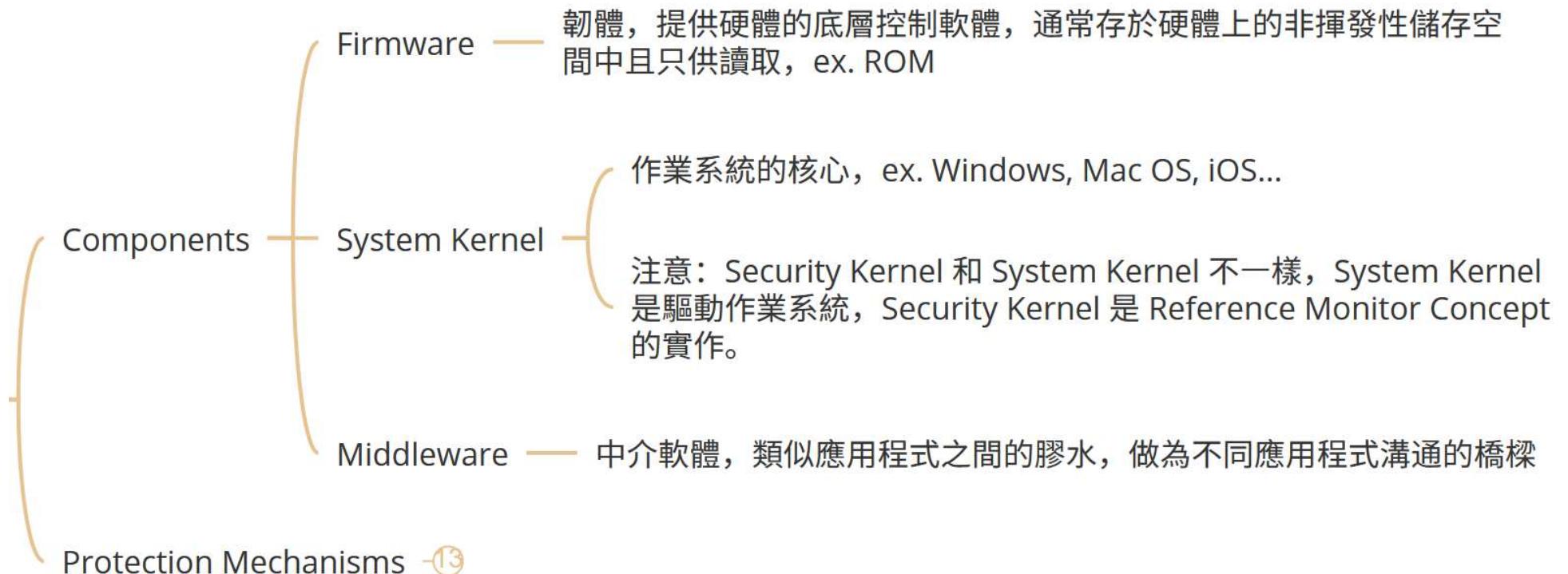
從安全的角度來看，CPU 只會運作在 Problem State 和 Supervisor State 兩種狀態，作為限制某些 Process 可以執行處理器的操作模式。

Processor States

Problem State — Ring 3 User mode，應用程式使用

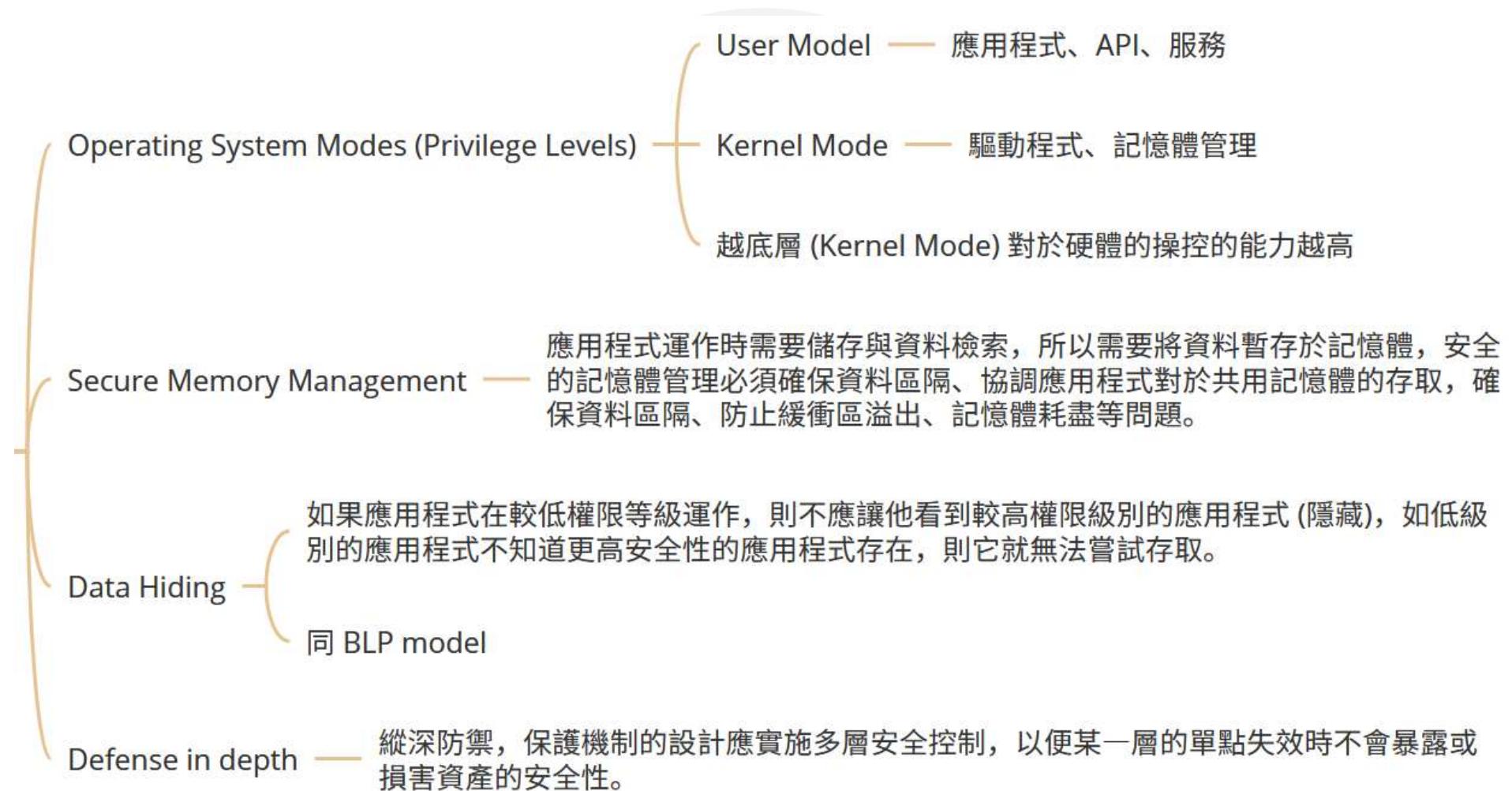
Supervisor State — Ring 0 Kernel mode，可存取任何硬體資源

3.2.4 Software



版權所有，翻印必究

3.2.4.2 Software Protection Mechanisms



3.3 Vulnerabilities

在建構、營運複雜系統時不可避免地會出現漏洞，可以想像單支程式就會有 Bug，更不用說數百、數千甚至百萬行的程式碼以及眾多互連的系統。作為資安人員，我們需要了解漏洞通常在哪？如何設計、開發系統來防止這些漏洞。

System -③〇

Mobile -③〇

Web-based -④〇

Cloud -⑦〇

3.3.1 System Vulnerabilities

Single Point of Failure

ex. 只有單一路由器或防火牆的公司網路

Redundancy 積餘

Bypass Controls

旁通控制，這是故意內建在系統中的方法，允許繞過安全控制，如網路設備背面的 Reset 按鈕，連續按 5 或 10 秒即可恢復原廠設定

Mitigating Controls 實施額外的緩解控制措施，如採用物理安全控制，確保只有授權人員可以接近該網路設備，增加日誌紀錄與監控、職責分離等均可，取決於組織的風險容忍度

TOCTOU (Time of Check Time
of Use, Race Conditions)

-⑤

Emanations -⑧

Covert Channels -③

Aggregation & Inference -④

TOCTOU (Time of Check Time of Use, Race Conditions)

應用程式在調用資源前檢查資源的狀態，但資源的狀態可能在檢查當下和使用之間發生變化，攻擊者試圖可能在這期間搶占資源（文件、記憶體、資料庫的數據...）

Increase frequency of Re-authentication

File locks

Exception handling

Transactions which provide concurrency controls

若選項同時出現，則 Increase frequency of Re-authentication 較為適當，因為攻擊者本身就不應該參與資源搶占，增加驗證頻率可以有效降低被攻擊的機會。

Emanations

系統發射任何類型的無線電波、訊號、光、聲音、震動等，這些都可以被竊聽系統攔截，從而導致訊息洩漏

Shielding (TEMPEST)

遮蔽，如用法拉第籠 (Faraday cage) 阻擋電磁場、絕緣材料阻擋聲音、不透明玻璃阻擋光線

TEMPEST 為軍方開發作為遮蔽電磁輐射的設備

White Noise — 白噪音，用強烈的隨機訊號淹沒設備發出的微弱訊號

Control Zones

高價值的系統放置在高物理安全區域中，只有經過授權的個人才能接近

Covert Channels / Aggregation & Inference

Covert Channels

無意的通信路徑，可能無意中洩漏機密訊息，主要有兩種類型：Storage、Timing
(見 Security Model > Information Model > Covert channels) [Link](#)

Analysis & Design

通過仔細分析流程 (Information Model) 可以解決隱蔽通道漏洞，識別出無意的路徑並設計控制措施防止或減輕。

Aggregation & Inference

聚合與推理是人員藉由大量數據進行未經授權的推理。

ex. 財會人員透過每月人事支出費用推算當月新進人員的薪資

Polyinstantiation

多實例化，在資料庫中為每一等級的 Subject 建立一個紀錄副本 (View)，省略該等級不該看到的訊息，減少推理攻擊的可能性

3.3.2 Mobile Vulnerabilities

OWASP Mobile Top 10:2023 -32

Policy, training & procedures — 最好的方法就是制定政策 (ex. BYOD Policy) 並實施教育訓練

Remote access security — 遠端存取公司網路資源的連線應加密，以保護傳輸中的敏感數據，ex. VPN

End-point security — 設備本身(即端點)安全性，強化驗證措施(MFA)、裝置加密(BitLocker)、遠程抹除功能

版權所有，翻印必究

OWASP Mobile Top 10:2023 - 1

- M1: Improper Platform Usage 安全功能未取用或誤用, ex. Face ID, Touch ID, Keychain 等
應正確地使用安全功能
- M2: Insecure Data Storage 敏感資料 (ex PII) 放在不安全目錄
不要儲存PII在移動裝置上
- M3: Insecure Communication 資料於傳輸過程不安全
採用 SSL/TLS 加密協定
- M4: Insecure Authentication 當攻擊者發現App後端的伺服器位址，他們可能會繞過 App 直接將 Request 發送到伺服器，從而繞過裝置內建的身分驗證機制
伺服器端應再進行身分驗證
- M5: Insufficient Cryptography 裝置使用不足或不當的加密算法
應選擇經得起時間考驗的良好加密算法

OWASP Mobile Top 10:2023 - 2

M6: Insecure Authorization

攻擊者繞過授權或授予自己無權的訪問權限

授權應由伺服器端進行而非裝置，並根據每個 Request 是否均為該用戶有權限執行的

M7: Client Code Quality

在終端運作的程式容易受到記憶體洩漏、緩衝區溢位 (Buffer overflow) 等攻擊

撰寫更安全的程式碼、開發人員需接受程式碼開發安全相關培訓課程、軟體品質管理(測試、邊界檢查)、輸入驗證

M8: Code Tampering

攻擊者在終端更改或添加惡意新的程式碼，使他們可以執行竊取身分或其他惡意行為

終端必須能檢測自身的程式碼在運行的時候是否有被竄改

M9: Reverse Engineering

逆向工程指的是攻擊者仔細分析App，找到其所連接後端伺服器的訊、加密問題弱點等

使用程式碼混淆工具 (We will discuss in Domain 8)

無關的功能指的是攻擊者仔細分析App找到開發者留下的隱藏功能進行後門攻擊 (Backdoor attack)

M10: Extraneous Functionality

後門有兩種，一種是開發者刻意留下的，一種是侵入者留下的(以便下次入侵用)

確保App在發布前進行程式碼審查以刪除無關的功能

3.3.3 Web-base Vulnerabilities

- Cross Site Scripting (XSS) -⑬
- Cross Site Request Forgery (CSRF) -⑦
- Server-side Request Forgery (SSRF) -⑦
- SQL Injection -⑤
- OWASP Web Top 10:2021 -⑩



版權所有，翻印必究

Cross Site Scripting (XSS)

攻擊者通過使用第三方站點誘使受害者的 Web 瀏覽器執行腳本的攻擊稱為跨站點腳本 (XSS) 攻擊

你 (User) 去一間餐廳點餐，一位陌生人 (Hacker) 在有你桌號的菜單 (Request) 備註寫上無敵大辣 (Script)，接著你沒發現就把菜單送給老闆 (Web Server)，老闆就送來一份無敵大辣的餐點

Store (Persistent) —— 儲存式跨網站指令碼攻擊，攻擊者將惡意程式碼注入 Web App 中 (ex. 在留言區留下 `<script> alert(1) </script>`) 的評論然後按送出，接下來訪問該網頁的每個用戶都會因為需要顯示先前評論而執行該段程式碼。這個 XSS 攻擊是持久的，每個後續使用者都會下載並執行此注入程式碼。

Reflected (Most Common) —— 反射式跨網站指令碼攻擊，將惡意程式會藏在網址列裡，放在 GET 參數傳遞，配合社交工程釣魚的技巧引誘使用者點擊 URL 才會生效。通常 URL 都會很詭異，所以通常都會用 HTML Encoder 或 短網址偽裝。

DOM —— 這種手法和反射型 XSS 一樣，只是 URL 裡面式 DOM 物件，都需要使用社交工程釣魚的技巧，使 User 點擊 URL 攻擊才會生效。
(DOM 就是 HTML 裡面物件的表示法)

Target of Attack —— Client / User's Browser

防止 XSS 的心態: Don't trust user input/request 任何輸入都有可能是危險的! 輸入框包含網址列、input、任何可以讓使用者更動網頁內容的地方

防範方式 —— (太深入可略過) HTTP HEADER - Secure, Samesite, HttpOnly, CSP, CORS

Cross Site Request Forgery (CSRF)

跨站請求偽造 (Cross-site request forgery, CSRF / XSRF)，也被稱為 one-click attack 或者 session riding，是一種挾制用戶在當前已登錄的Web應用程式上執行非本意的操作的攻擊方法。

你 (User) 去一間餐廳點餐，一位陌生人 (Hacker) 拿了一張有你桌號 (Cookie) 的菜單 (Request) 給老闆 (Web Server)，老闆問也不問便收了菜單並將帳記到你的身上。

User 訪問並登入 A 網站，Cookie 存至瀏覽器，User 在未登出 A 網站的情況下瀏覽 B 網站，接著 Hacker 以 B 網站的 Domain 以 A 網站給 User 的 Cookie 對 A 網站發送請求，如果 A 網站沒發現即攻擊成功。

Target of Attack — Server

防範方式 — (太深入可略過) 實作 CSRF token 放在 server 的 session

Server-side Request Forgery (SSRF)

CISSP 講義課本未曾提過，因列於 OWASP Top10:2021 A10 故作為補充

一位陌生人(Hacker) 觀察老闆 (Admin) 與廚房 (Web Server) 的互動方式，偽造了一張現在清空冰箱 (Database)的便條紙給廚房，廚房沒有驗證這便條紙的來源，便直接將冰箱食材倒掉。

Hacker 用目錄遍歷(Path Traversal) 漏洞鑽到資料管理後台(API) 透過中介伺服器發送惡意指令

Target of Attack — Server

防範方式 — (太深入可略過) 輸入驗證、避免目錄遍歷 (Path Traversal) 漏洞、API 加上 token 保護

奴惟所用，劍印必允

SQL Injection

SQL語法注入，攻擊者在前端輸入 SQL 語法直接讀寫或控制後端資料庫。

ex. SELECT * FROM users WHERE username = 'aaa' AND password = 'bbb'

ex. SELECT * FROM users WHERE username = 'aaa' OR 1=1 --' AND password = 'bbb'

防範方式 — Input Validation

版權所有，翻印必究

OWASP Web Top 10:2021

A01:2021-Broken Access Control 權限控制失效

A02:2021-Cryptographic Failures 加密機制失效

A03:2021-Injection 注入式攻擊

A04:2021-Insecure Design 不安全設計

A05:2021-Security Misconfiguration 安全設定缺陷

A06:2021-Vulnerable and Outdated Components 危險或過舊的元件

A07:2021-Identification and Authentication Failures 認證及驗證機制失效

A08:2021-Software and Data Integrity Failures 軟體及資料完整性失效

A09:2021-Security Logging and Monitoring Failures 資安記錄及監控失效

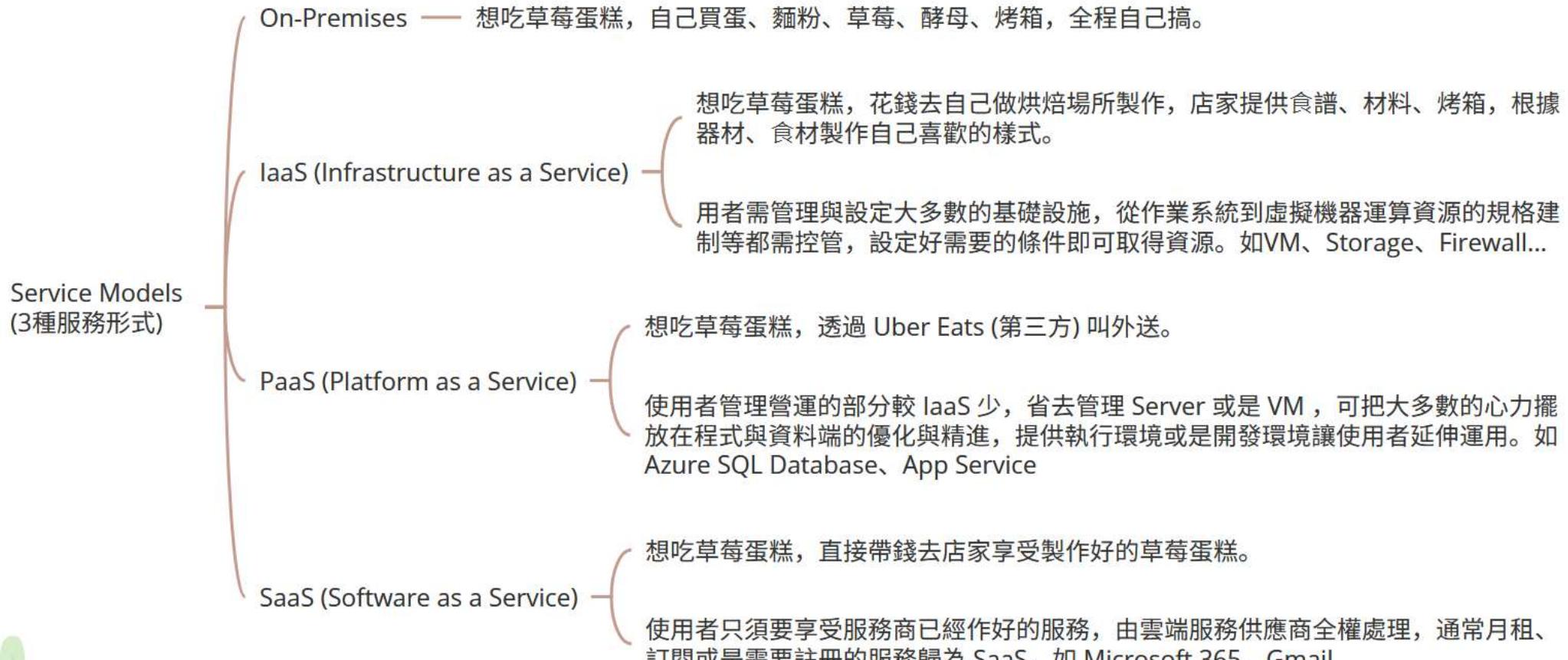
A10:2021-Server-side Request Forgery (SSRF) 伺服端請求偽造

必究

3.3.4 Cloud (討論弱點前先介紹 Cloud) - 1



3.3.4 Cloud (討論弱點前先介紹 Cloud) - 1



3.3.4 Cloud (討論弱點前先介紹 Cloud) -

- Deployment Models
(4種佈署模式)
- Public — 公共雲是任何人(公眾)都可以使用的雲服務，雲服務供應商(CSP)擁有並運營可供公眾使用的雲基礎設施。
 - Private — 私有雲是供單個客戶專用的雲基礎設施，可由客戶或雲服務供應商擁有和營運，並且可存在於內部或外部，且在物理上或邏輯上需與其他客戶分離。
 - Community — 由一群擁有共同任務、特定需求的組織共同成立，以服務該社群。
 - Hybrid — 公共雲、私有雲和社群雲的組合。
如大型組織會有自己專用的本地私有雲來儲存敏感資料，使用公有雲儲存不太敏感的資料或工作負載。



3.3.4 Cloud (討論弱點前先介紹 Cloud) - 3

Characteristics
(5種特徵)



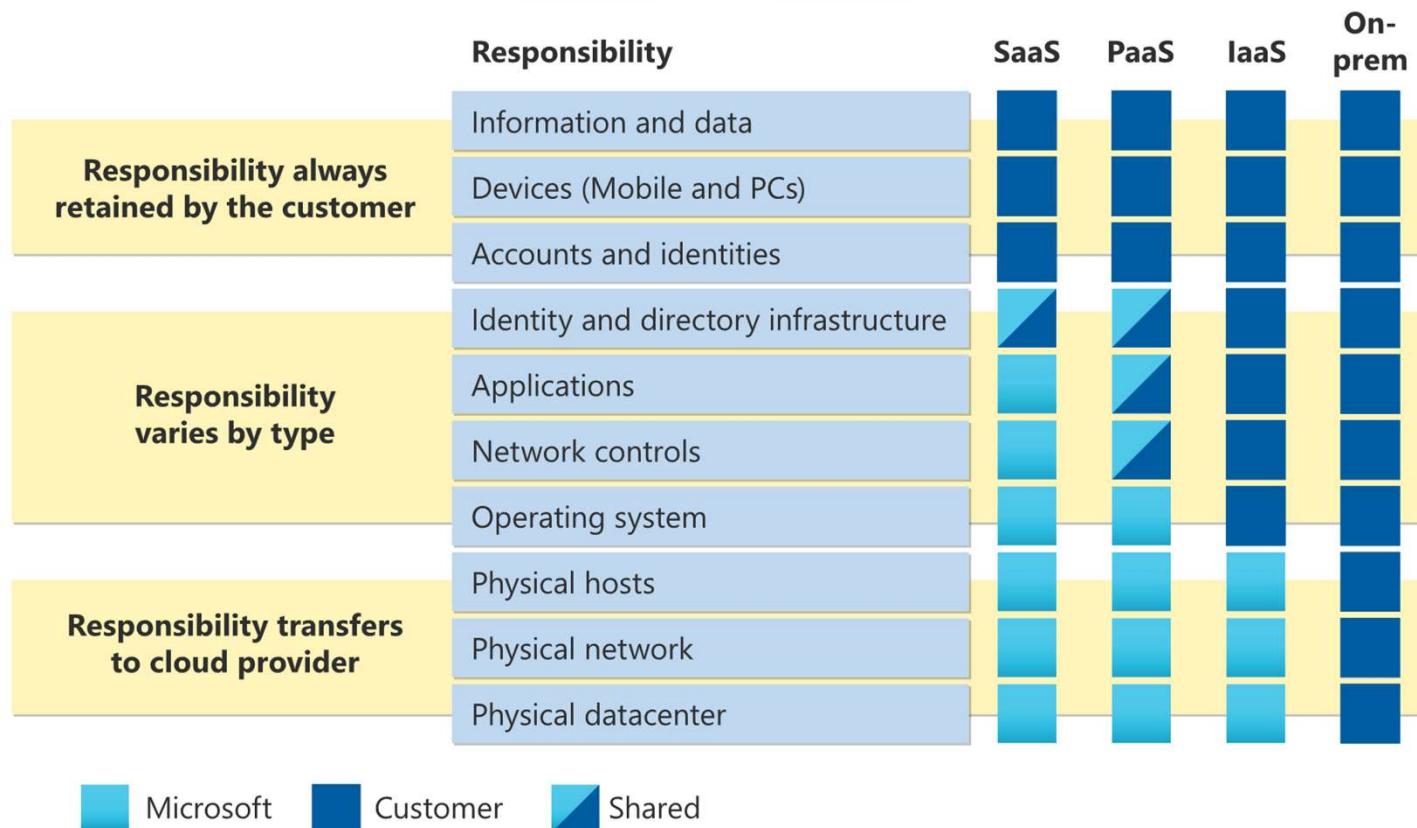
- On-Demand Self-Service 隨選所需自助服務 —— 用戶可以自行配置運算能力，像是伺服器時間與網路儲存空間，而且是在不需人工介入的情況下自動運作。
- Broad Network Access 網路存取方式多樣化 —— 雲端運算要能透過網路取得，並且能以標準的連線機制促成各式異質的終端平臺存取。ex. 筆電、手機
- Resource Pooling 共用資源池 —— 服務供應商的運算資源必須整合為一個共用資源池，依照用戶的需求，動態配置或取消實體與虛擬化的運算資源，達到多位用戶共同使用的多租戶型式。
- Rapid Elasticity 迅速伸縮自如 —— 可快速擴增架構，亦可快速縮小架構，在一些情況下甚至能夠自動化運作
- Measured Service 服務可測量 —— 資源的使用情況可以被監控、控制、匯報，對供應商與用戶而言都如同使用水電服務一樣透明化。

3.3.4 Cloud - Vulnerabilities

威脅類型	說明
1 · 濫用與非法使用	網路犯罪會利用雲端運算的特性，提升攻擊效率與躲避追查，而雲端服務供應商的註冊機制普遍缺乏有效的防堵與偵測，容易成為被利用的對象。
2 · 不安全的介面與API	雲端運算供應商提供API或軟體介面讓使用者接取，以管理運算資源配置、監控等作業，若這些軟體介面或API的設計不夠安全，就會危及雲端服務的安全性。
3 · 供應商員工蓄意不良	雲端服務供應商的員工蓄意不良，或遭有心人士利用，都有可能對使用雲端服務使用者造成危害，所以必須確認服務供應商是否有管制存取權限，以及採取監控措施。
4 · 資源共用問題	近年來已有針對共用平臺弱點的攻擊，像是磁區、處理器快取、繪圖處理器等共用元件，不見得有很好的隔離設計，容易成為滲透的漏洞。
5 · 資料遺失或洩露	雲端服務供應商如果沒有做好備份與保護，在刪除資料或是資料異動時，很容易發生資料遺失。遺失的若是金鑰之類的機密資料，就會造成更大的問題。
6 · 帳號被竊或服務被挾持	帳號被竊、服務被挾持並不是新鮮事，然而在雲端服務發生則會更嚴重，因為使用者不易發覺已被竊聽、被複製資料，甚至是被人用來做壞事。
7 · 未知的風險	雲端服務供應商通常大力宣傳優點，而對於安全防護著墨不多，因此採用雲端服務有必要進一步了解資料是如何保護、誰可以存取等供應商的安全措施。

資料來源：Cloud Security Alliance，ithome 整理，2011 年 6 月

Cloud Shared Responsibility



3.3.4 Cloud - Identity

當組織把部分的服務上雲後，傳統內部網路的防護邊界即消失，所以需要處理上雲後 IAM 的問題。 (Domain 5)

- Identity Provider
- Local — 使用者的 Identity 存在地端 (通常是 AD)
 - Cloud — 使用者的 Identity 存在雲端 (如 Okta、Azure AD)
- We will discuss in Domain 5 Identity and Access Management (IAM)
- Cloud Identity
- Cloud — 在雲端建立與管理身分
 - Linked — Identity 同時存在雲端和地端，只有固定的其中一端更改才能反映到兩端
 - Synced — Identity 同時存在雲端和地端，任一端更改會反映到兩端
 - Federated — 用戶的 Identity 透過 Federated Access 可訪問地端和雲端的服務

3.3.4 Cloud - Protocols

We will discuss in Domain 5 Identity and Access Management (IAM)

- Protocols
 - SPML — Service Provisioning Markup Language, 一種XML用於將跨資訊系統之創建和管理實體和屬性的過程自動化。ex. HR 系統可以透過 SPML 使 AD 自動設定新進人員的權限
 - SAML — 用戶登入一次便可以訪問各自獨立的不同 Web 網站 (單一登入 SSO), 提供身份驗證訊息給聯合身份管理系統。
 - OpenID — OpenID provides only Authentication
 - OAuth — OAuth provides only Authorization
 - OpenID Connect (OIDC) — 基於 OAuth 2.0 的基礎, 提供 Authentication + Authorization

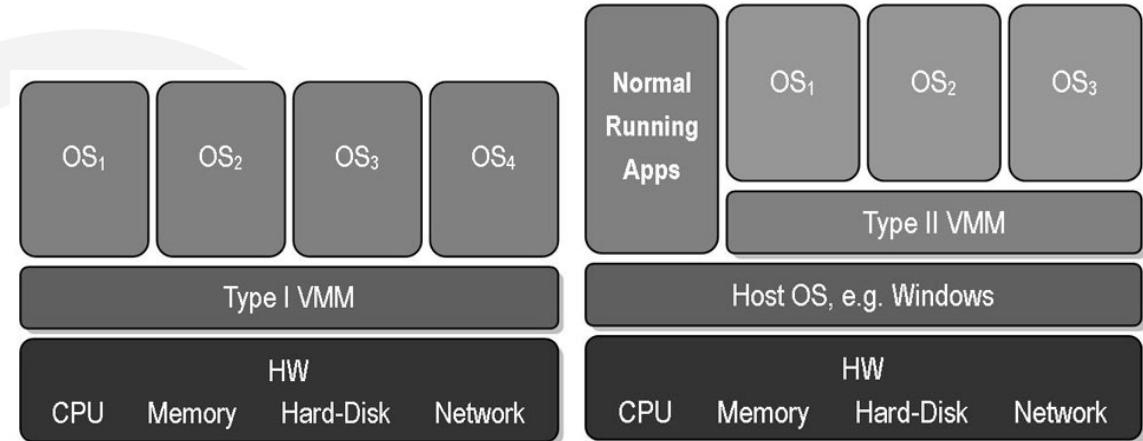
3.3.4 Cloud - Hypervisor

Hypervisor — 虛擬機器管理員

instance — 虛擬機本身

Type —
Type 1(bare metal hypervisor)

Type 2 (hosted hypervisor)



Hypervisor是直接控制著實體機器的硬體，也就是取代掉現有的作業系統，把原本要跟硬體溝通的事改由此類型的Hypervisor來處理，它的優點是效能高但是實作此類型之Hypervisor較複雜。 -①

一般安裝在OS上的應用程式一樣，VM 跑在此應用程式之上，相對於Type1，此類型的 Hypervisor 會多了一層OS，因此效能會比Type1來得差。 -②

3.3.4 Cloud – Migration & Data Destruction

當組織決定把系統或資料遷移到雲端時，從安全角度需要考慮的問題很多，如何確保資料的 CIA、適當的訪問控制 IAM、彈性、和規性等等。以下兩點建議

Migration

Data Centric — 以資料為中心的角度思考，從資料的分級、生命週期(建立、儲存、使用、共享、歸檔、銷毀) 檢討每個階段在雲端需要的安全控制。(Domain 2)

SLA — Service Level Agreements，服務級別協定是雲端服務供應商對消費者的書面承諾，包含機密性、完整性、可用性及響應能力(7×24)，是服務合約的其中一個附錄。(Domain 1)

Data Destruction

有許多法規會要求資料所有者確保敏感資料(特別是 PII) 進行適當的且可證明的銷毀。

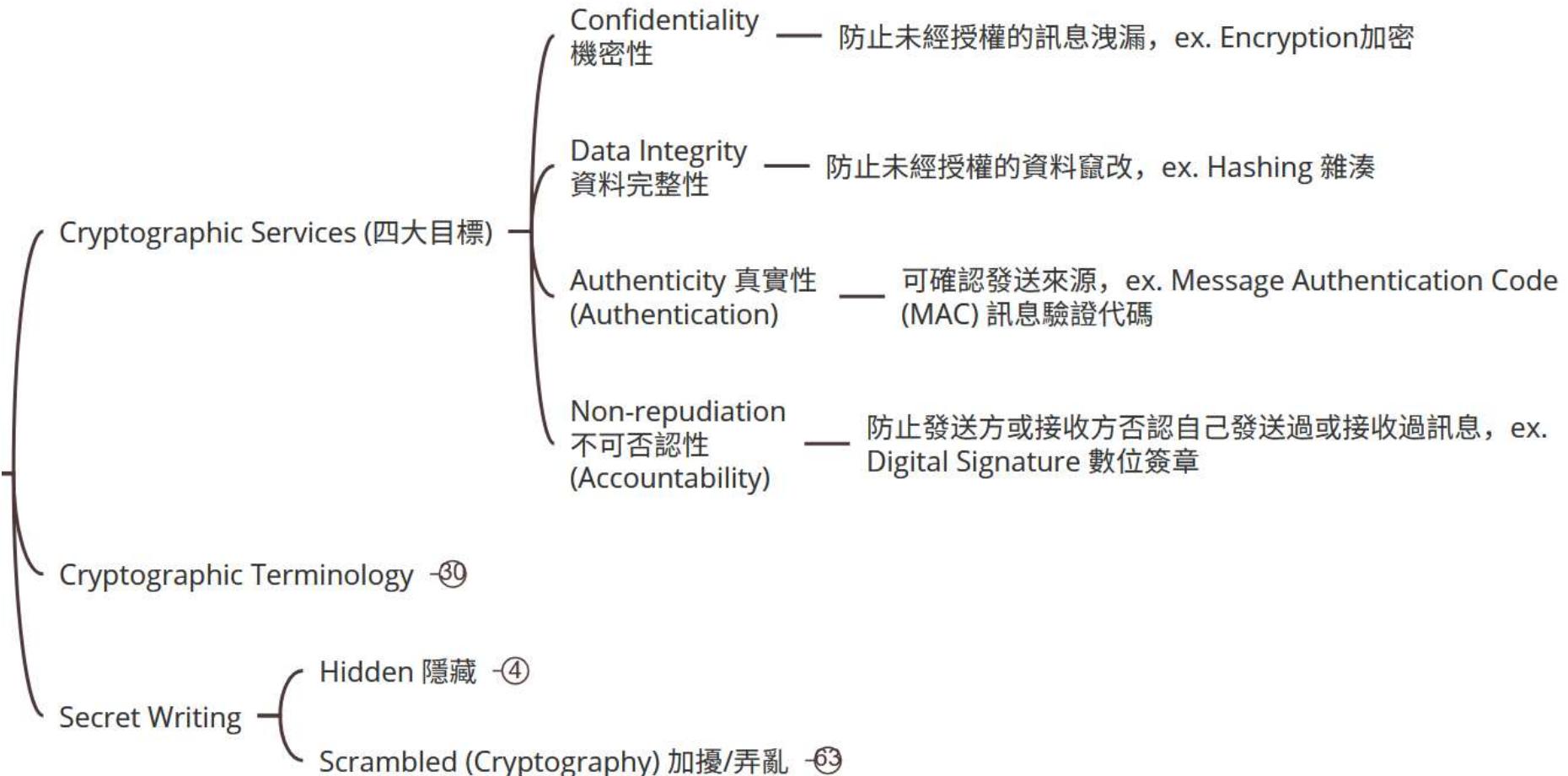
Crypto Shredding / Erase — 在雲環境中，無法進行物理銷毀，故最佳的方法為使用 AES等算法對敏感資料加密，且確保金鑰被有效的銷毀。(Domain 3)

3.3.4 Cloud – Investigation



版權所有，翻印必究

3.4 Cryptography



3.4.2 Cryptographic Terminology - 1

Plaintext 明文

Encrypt 加密

Ciphertext 密文

Key / Crypto variable 金鑰

Decrypt 解密 — 使用金鑰把密文還原成明文的過程

Key clustering — 使用不同的金鑰加密相同的明文生成相同的密文，這代表兩個不同的金鑰也可以解密同一密文，那麼執行暴力破解的難度就降低一倍

Work Factor — 破密所需的估計時間，Work Factor 越高，密碼系統越安全

3.4.2 Cryptographic Terminology - 2

Initialization vector / Nonce — 初始向量、隨機數是與金鑰一起使用的隨機數，IV只能使用一次，目的在防止使用相同的明文、金鑰、加密算法的情況下得到相同的密文

Confusion — 好的加密算法應有的特性 - 混淆，確保逆向工程是不可能的，關注於在於金鑰與密文之間的關係，如果金鑰的 1 bit 發生變化，密文應有大約一半的 bit 發生變化。通常是通過替代 (Substitution) 來進行的。

Diffusion — 好的加密算法應有的特性 - 擴散，確保逆向工程是不可能的，關注於明文和密文的關係，如果明文的 1 bit 發生變化，密文應有大約一半的 bit 發生變化。通常是通過轉化(Transposition)來進行的。

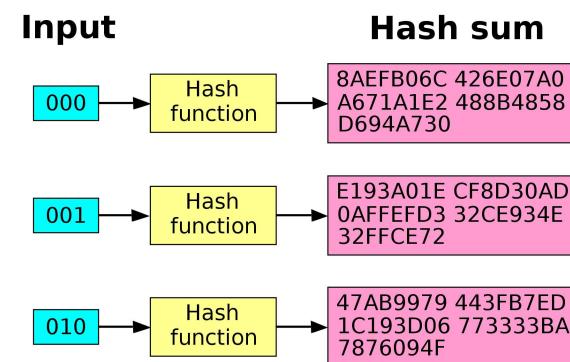
版權所有，翻印必究

3.4.2 Cryptographic Terminology - 3

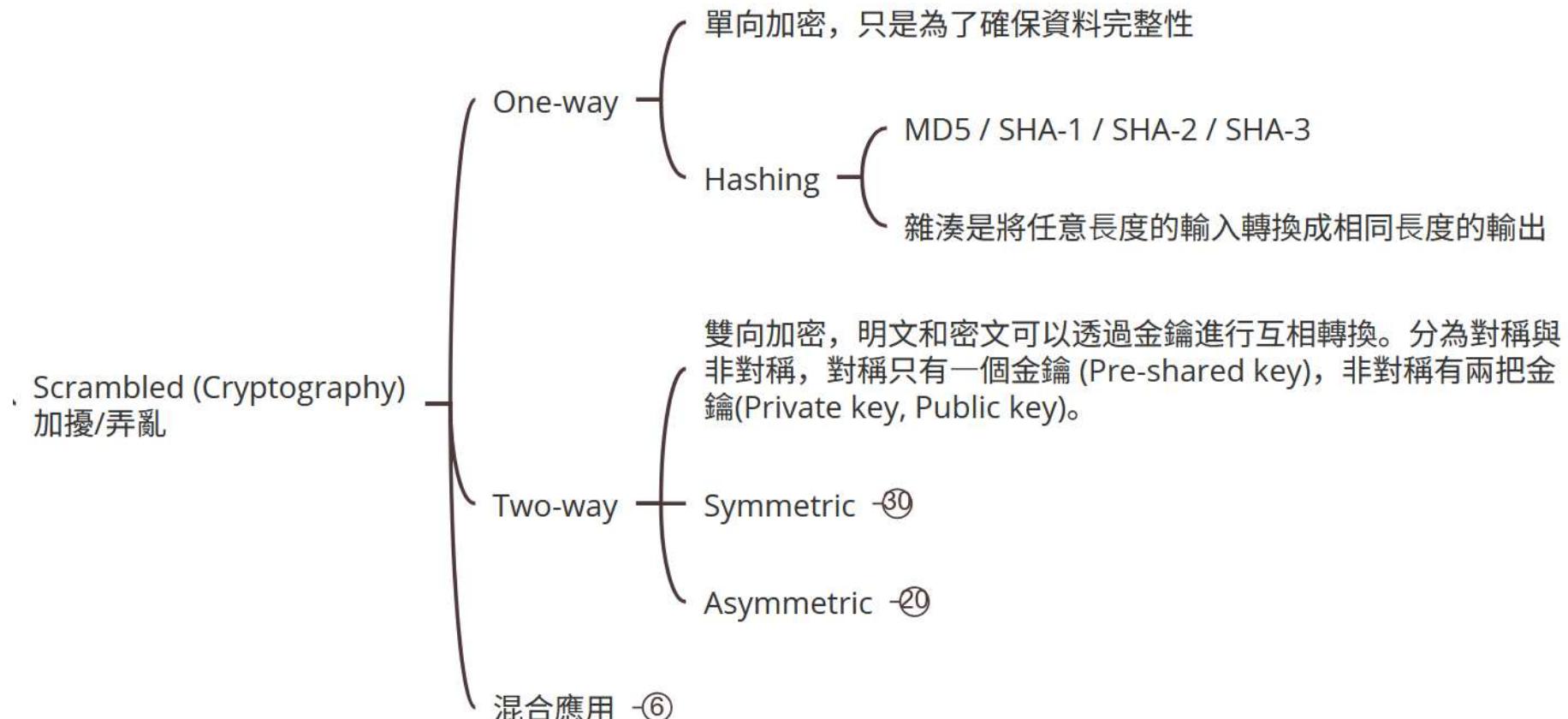
- Substitution — 替代只是將一個字元換成另外一個字元
- Caesar Cypher 凱薩密碼、Mono-alphabetic Substitution Cipher 單字母替換密碼 — 因為被發現有固定的替換模式，ex. A 換成 C、C 換 E
- Poly-alphabetic Substitution Ciphers — 為了解決上面的問題，用了多個替換字母表
- One-time Pads 一次性密碼本 — 如果使用真正隨機的一次性密碼本且永不重複使用，可以提供無法破解的加密。

Transposition — 重新排列明文中的所有字元

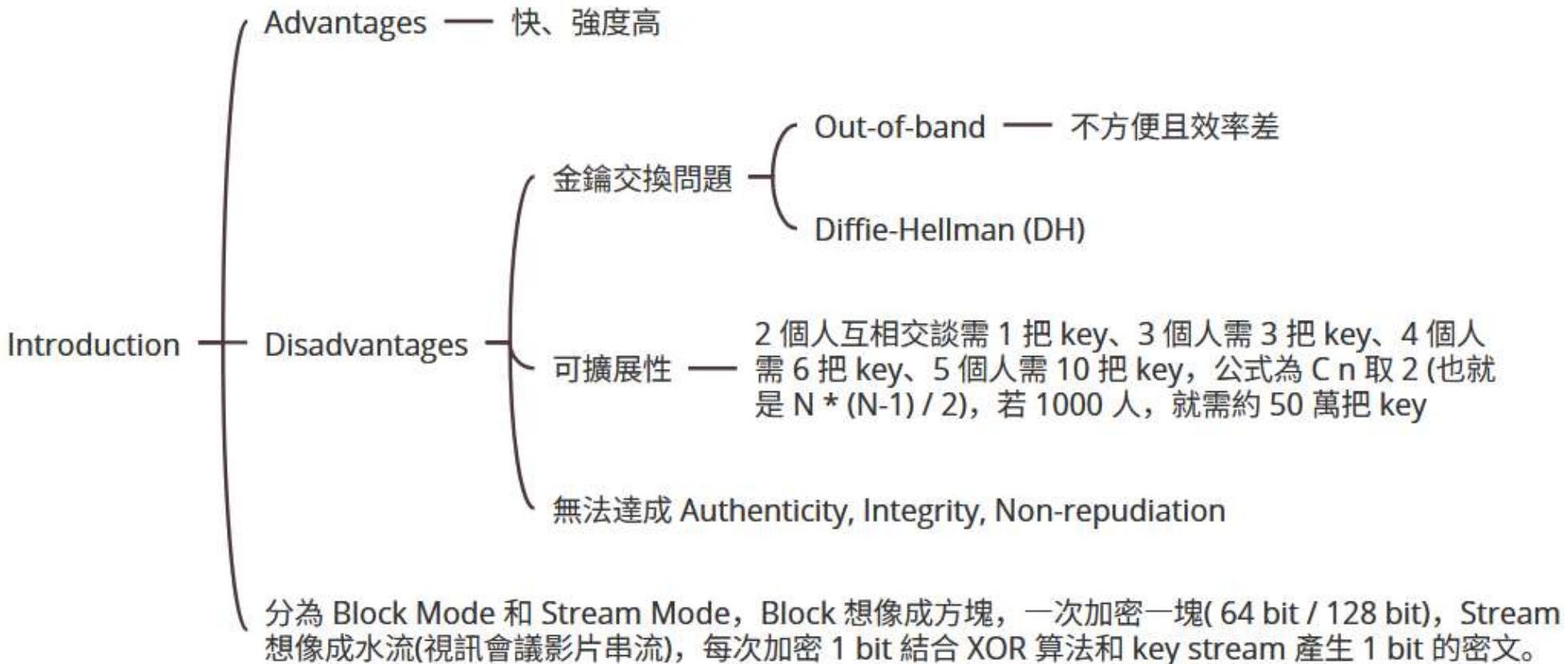
Avalanche Effect — 雪崩效應，演算法設計要求，以使輸入發生的最微小變化，導致輸出的急劇變化。①



3.4.4 Secret Writing



Symmetric - 1



Symmetric - 2

- DES / 3DES
 - DES 用 56 bit key 加密，容易被暴力破解
 - 3DES 用 DES 算 3 次，容易遭 meet-in-the-middle 在中間相遇攻擊
- Block
 - AES (Rijndael) —— 美國政府在 DES 即將過時時，舉辦尋找替代品的競賽，由 Rijndael 勝出，並更名為 Advanced Encryption Standard (AES)
 - CAST-128 / SAFER / Blowfish / Twofish / RC5 / RC6 —— 知道是對稱式就好
- Block Modes: ECB / CBC / CFB / OFB / CTR
 - ECB —— 最不安全，因不使用初始化向量，也因此加密速度最快，所以 ECB 僅能用於不重複的短位隨機內容。
 - CTR —— 計數器模式，被認為是速度和安全性的最佳平衡。它不是最安全的，且比 ECB 慢，但它是速度和安全性的最佳折衷方案。
 - 其他三種模式比 ECB 有很大的優勢，它們都使用初始化向量，因此它們都比 ECB 安全得多。
- Stream — RC4
 - 對稱式、串流加密
 - 曾用於 WEP 無線網路加密、傳輸層安全標準 TLS，但因為被破解，所以被替代 (WEP -> WPA2 使用 AES)。

Knowledge check

The Double DES (2DES) encryption algorithm was never used as a viable alternative to the original DES algorithm. What implementation attack is 2DES vulnerable to that does not exist for the DES or 3DES approach?

- A. Chosen ciphertext
- B. Brute force
- C. Man-in-the-middle
- D. Meet-in-the-middle

版權所有，翻印必究

Asymmetric - 1



Asymmetric - 2



版權所有，翻印必究

Knowledge check

Howard is choosing a cryptographic algorithm for this organization, and he would like to choose an algorithm that supports the creation of digital signatures. Which one of the following algorithms would meet his requirement?

- A. RSA
- B. 3DES
- C. AES
- D. Blowfish

版權所有，翻印必究

Knowledge check

Chris is designing a cryptographic system for use within his company. The company has 1,000 employees, and they plan to use an **asymmetric encryption system**. They would like the system to be set up so that any pair of arbitrary users may communicate privately. How many total keys will they need?

- A. 500
- B. 1,000
- C. 2,000
- D. 4,950

版權所有，翻印必究

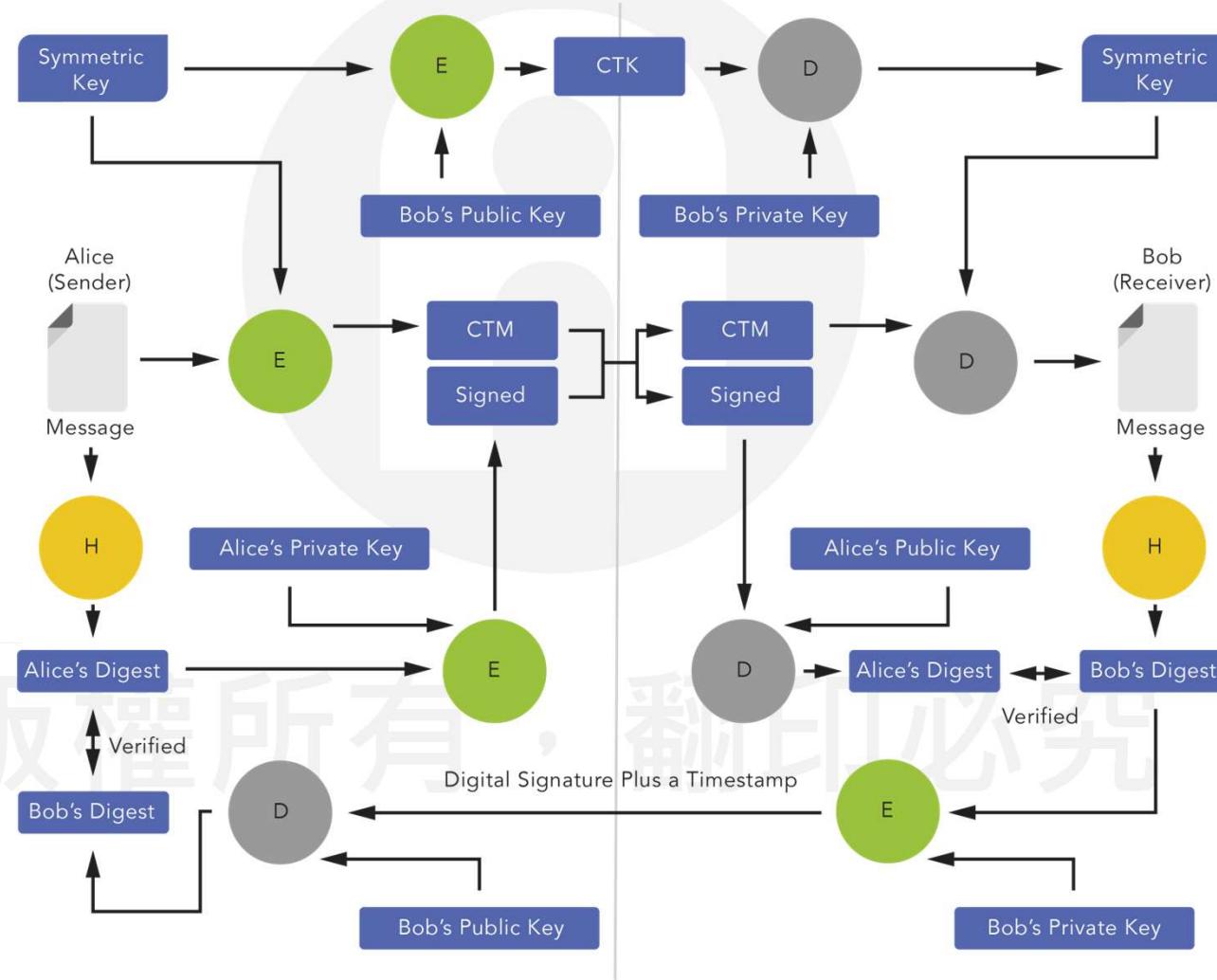
Knowledge check

Sherry conducted an inventory of the cryptographic technologies in use within her organization and found the following algorithms and protocols in use. Which one of these technologies should she replace because it is no longer considered secure?

- A. MD5
- B. AES
- C. PGP
- D. WPA3

版權所有，翻印必究

Hybrid Cryptography Examples



Digital Signature process

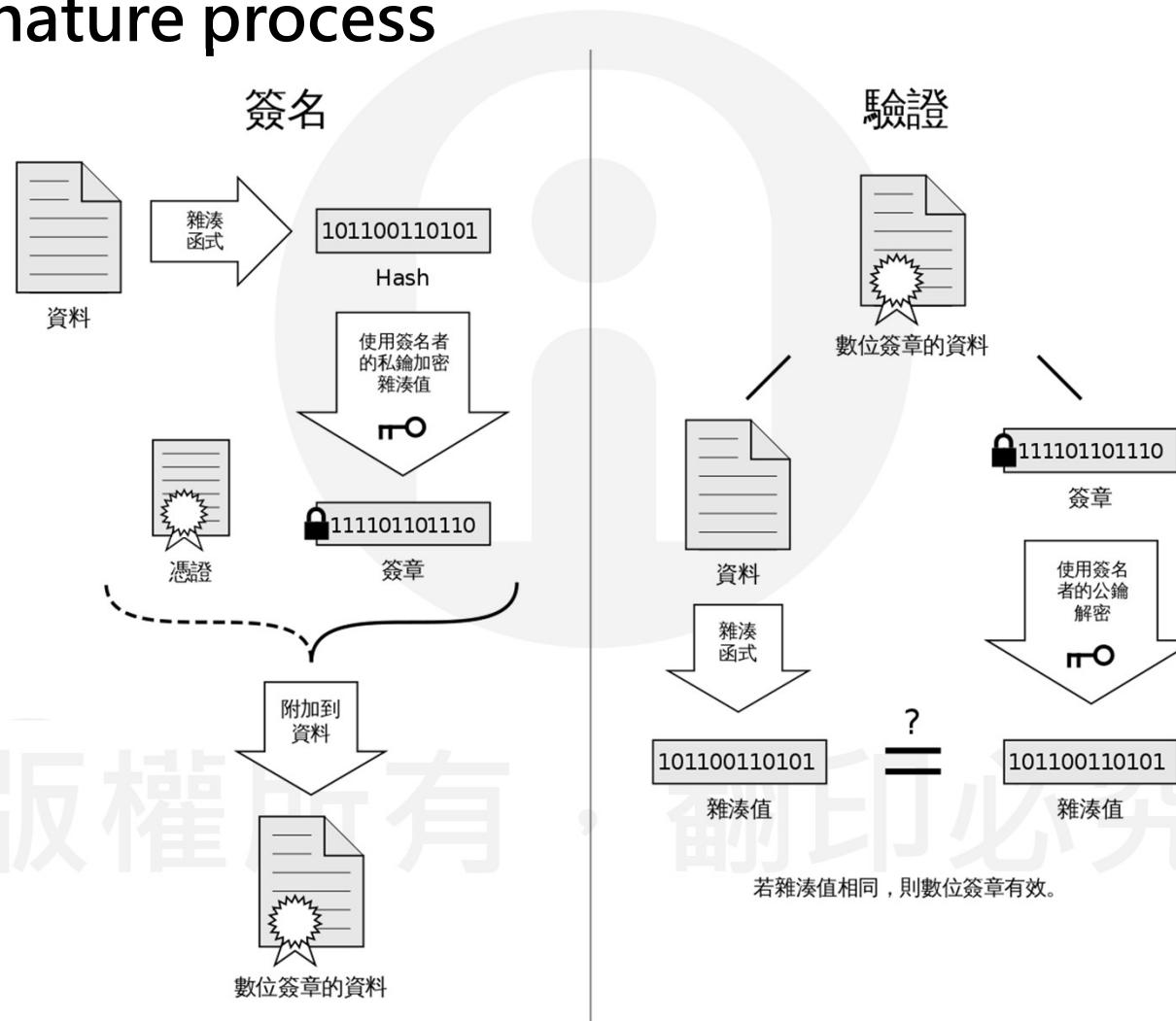
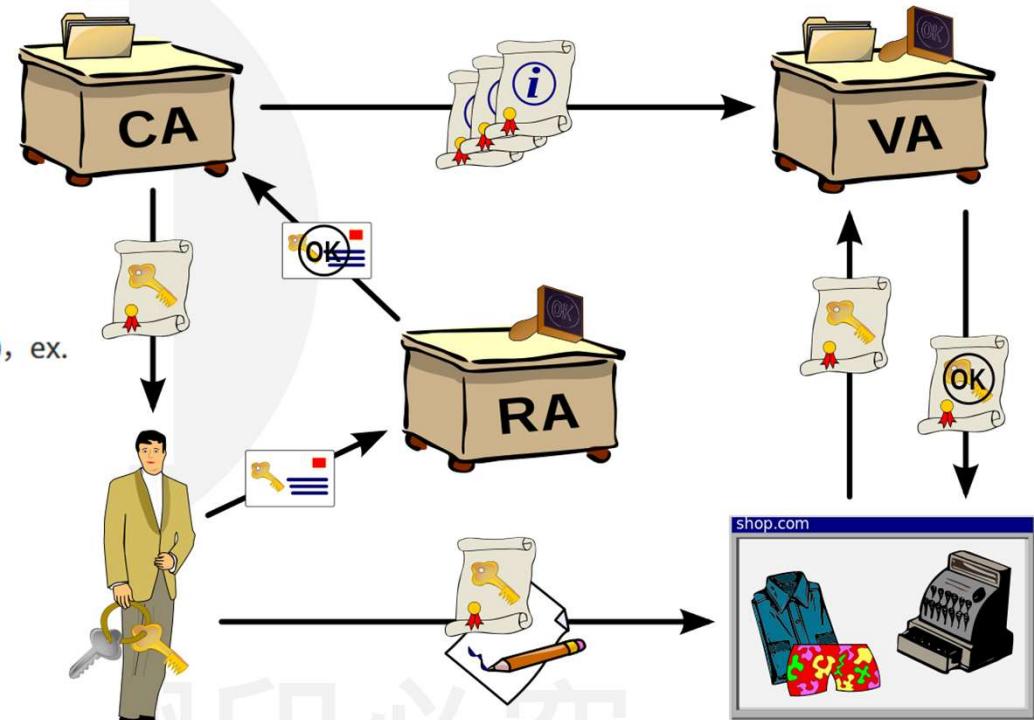


Diagram of PKI

- X.509
 - X.509 是公鑰憑證的標準格式
 - X.500 是目錄服務的標準，簡化版為 LDAP
- Replacement — 數位憑證的有效期通常是1~2年，憑證本身會註記到期日，網站管理人應注意定期更換過期憑證。
- Role
 - CA (Root of Trust) — Certification Authority (憑證管理中心)，ex. 內政部憑證管理中心
 - RA — Registration Authority (收件單位)，ex. 戶政事務所
 - VA — Validation Authority (檢查中心)
- Revocation
 - CRL — 紀錄被CA所撤銷的憑證清單
 - OCSP — 提供線上動態查詢憑證的狀態

Ref. <https://zh.wikipedia.org/zh-tw/%E5%85%AC%E9%96%8B%E9%87%91%E9%91%B0%E5%9F%BA%E7%A4%8E%E5%BB%BA%E8%A8%AD#/media/File:Public-Key-Infrastructure.svg>



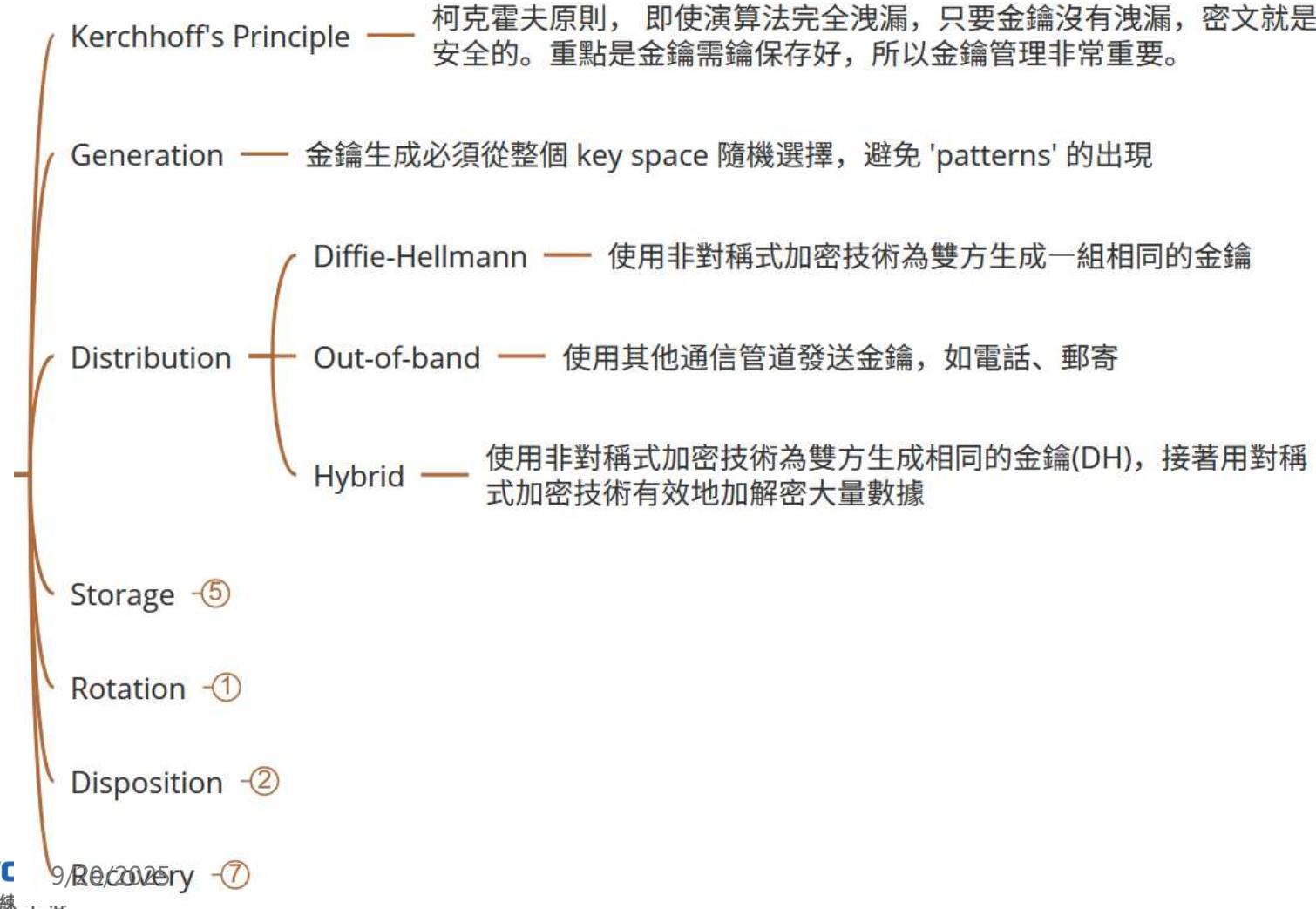
Knowledge check

Alison is examining a digital certificate presented to her by her bank's website. Which one of the following requirement is not necessary for her to trust the digital certificate?

- A. She knows that the server belongs to the bank
- B. She trusts the certificate authority
- C. She verifies that the certificate is not listed on a CRL
- D. She verifies the digital signature on the certificate

版權所有，翻印必究

Key Management - 1



Key Management - 2

- 
- 建立或接收金鑰後，需將其儲存在極安全的位置，有兩種硬體專門用於安全保存金鑰
 - Storage — TPM — Trusted Platform Modules，內建於筆電或手機主機板上獨立的晶片，目的在儲存金鑰、處理加解密算法
 - HSM — Hardware Security Modules，外部獨立設備，用於安全存放金鑰並作為加密加速器
 - Rotation — 金鑰輪轉為定期更改加密金鑰，頻率完全取決於受保護數據的價值與金鑰被洩漏的風險等因素
 - Disposition — Crypto-shredding, Key Destruction — 透過加密並銷毀用於加密的金鑰來安全地銷毀資料
還原金鑰的方式
 - Split Knowledge — 將金鑰的支式分給兩個或多個人，為了恢復金鑰，這些人需鑰聚在一起結合他們各自持有的知識來恢復完整金鑰
 - Recovery — Dual Control — 需要兩個或更多人執行某些操作才能恢復金鑰，ex. 兩人同時轉動自己的鑰匙才能發射導彈
 - Key Escrow — 加密金鑰的副本交由受信任的第三方託管

3.6 Cryptanalysis - 1

Cryptanalytic Attacks
密碼分析攻擊

Cryptographic Attacks
加密攻擊

目的在於推斷金鑰，找到可用於解密密文的加密變量(金鑰)

Brute Force — 最簡單的攻擊類型，嘗試每一種可能的金鑰，直到找到正確的

Ciphertext Only — 只依據密文推斷金鑰，這非常困難

Known Plaintext — 依據明文和對應的密文推斷金鑰，目的是用來解密其他密文甚至偽造其他密文

Chosen Plaintext — 攻擊者取得密碼機，透過選定的明文輸入，然後查看生成的密文以嘗試推斷金鑰

Chosen Ciphertext — 攻擊者取得密碼機，透過選定的密文輸入，然後查看生成的明文以嘗試推斷金鑰

Factoring — 分解攻擊，只能攻擊裡用因式分解的算法 - RSA

-28

Cryptographic Attacks 加密攻擊 - 1

目的不是在推斷金鑰，而是其他目的

1. Man-in-the-middle — 中間人攻擊，攻擊者將自己放在對話之中，透過竊聽來回發送的通信，改變通信或破譯內容
2. Replay — 重播攻擊是中間人攻擊的一種形式，攻擊者竊聽並攔截正在發送的數據，攻擊者不一定能破譯截獲的數據，但可透過稍後重新發送達成攻擊目的。ex. 截獲使用者登入帳號與密碼的雜湊值，可偽裝成使用者獲得未經授權的登入
3. Implementation — 實作攻擊針對算法、密碼系統協議或程式實作方式的弱點攻擊。ex. WEP (Wired Equivalency Protocol 有線等效協議) 用 RC4 保護無線流量，但 WEP 在 RC4 實作方式不佳，導致 WEP 非常不安全。(不是RC4的問題，而是加密機制實作的問題)

Cryptographic Attacks 加密攻擊 - 2

4. Dictionary Attack

暴力攻擊的一種形式，查找加密金鑰或使用者密碼。字典攻擊不是按順序嘗試每種可能的組合，而是先嘗試最可能的組合。ex. 破解用戶密碼可先嘗試 123456, password, p@ssw0rd 等 (用網路上有現成的密碼字典數據集)

5. Side Channel

仔細監聽正在執行加密任務的系統來蒐集相關資訊

Power —— 測量某些計算消耗多少功率

Timing —— 測量某些操作花多少時間

Radiation Emissions —— 測量系統發出的電磁波

6. Rainbow Tables

彩虹表是密碼字典的延伸，當攻擊者竊取密碼資料庫後發現裡面都是一堆雜湊值，於是就利用上面提到的密碼字典數據集經雜湊後進行比對，就可以還原使用者的密碼。

使用 Salt + Pepper (鹽和胡椒) 在雜湊時進行密碼前處理，Salt 所有用戶都一樣，Pepper 每個用戶不一樣，會放在另外一個資料庫裡

Cryptographic Attacks 加密攻擊 - 3

7. Birthday Attack — 取自生日迷失 (birthday paradox) 理論，在 23 個學生中任取 2 位 (C_{23}^2) 出現相同生日的機會超過 50%。換句話說，在 n 個訊息中需鑰嘗試多少種訊息才可以獲得相同的雜湊碼，其組合應為 2 的 64 次方，但依生日迷失計算僅需 2 的 32 次方的訊息可發現碰撞(雜湊值相同)
8. Social Engineering
Purchase Key — 用金錢賄絡使其交出金鑰
Rubber Hose (橡膠管) — 威脅、勒索，或者折磨某人，直到他給出密鑰為止
9. Frequency analysis — 字頻分析，最常出現的字母：e, t, a, o, i. 最常出現的單字：the, to, of, and.
10. Fault injection attack — 使執行條件超出了原本預設的規範，造成產品運作出錯，讓加密硬體系統錯誤的執行讀取密鑰的任務，使其載入空白密鑰(zero key)來加密資料，如此一來只要再使用空白密鑰，就能將密文還原成明文

Knowledge check

Ron is investigating a security incident that took place at a highly secure government facility. He believes that encryption keys were stolen during the attack and finds evidence that the attackers used dry ice to freeze an encryption component. What type of attack was likely attempted?

- A. Side channel attack
- B. Brute-force attack
- C. Timing attack
- D. Fault injection attack

Knowledge check

Tony believes that an attacker was able to eavesdrop on legitimate HTTPS communications between her users and remote web servers by engaging in a DNS poisoning attack. After conducting DNS poisoning, what technique would an attacker likely use to conduct this eavesdropping?

- A. Man-in-the-middle
- B. Brute force
- C. Timing
- D. Meet-in-the-middle

3.7 Physical Security

人命安全最重要，人員是組織中最有價值的資產，任何規劃都需將人員安全放至首位

Categories of Control -⑨

CPTED (通過環境設計預防犯罪) -⑤

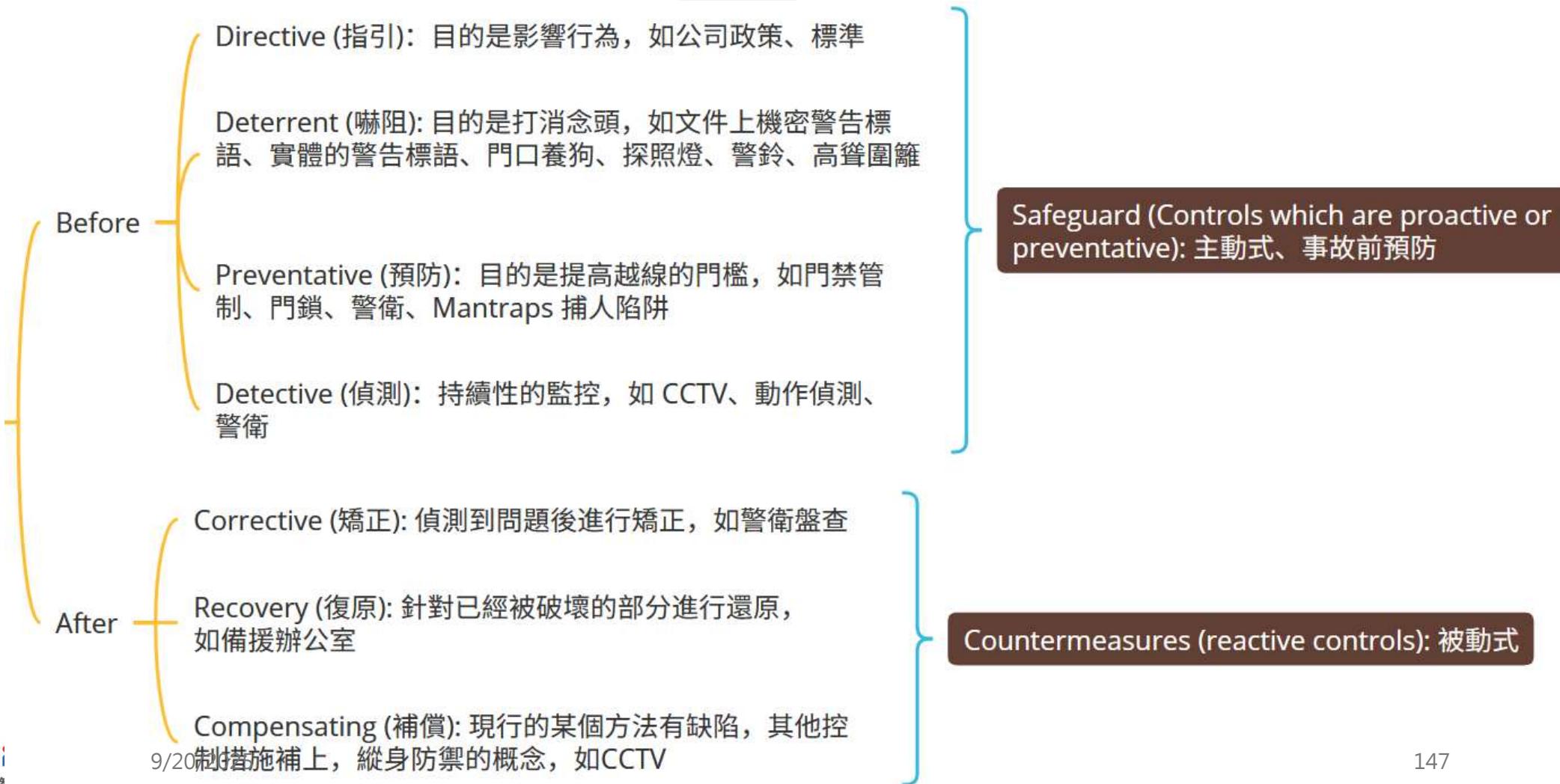
Fire -③

Power -⑯

Data Center -⑫

必究

3.7.1 Categories of Control



3.7.2 CPTED (通過環境設計預防犯罪)

大樓安裝窗戶，俯瞰停車場或其他可能吸引犯罪活動的僻靜區域

窗邊種植玫瑰叢（帶有鋒利的刺）以防止闖入企圖

圍欄、人行道、藝術裝置和標誌有助於為居民或顧客建立安全意識和責任感，同時阻止未經授權的訪問

添加娛樂設施或其他積極活動提升人數增加安全

修剪整齊的樹木和植物可保持視線暢通



帶有陽台的彎曲街道使居民更容易發現可疑活動，同時也使犯罪分子難以規劃逃跑路線



破舊的鏈節圍欄暗示其圍護的建築物並不安全，而經過修剪的灌木則表明此處有人活動，從而增加了犯罪者感知到的風險。



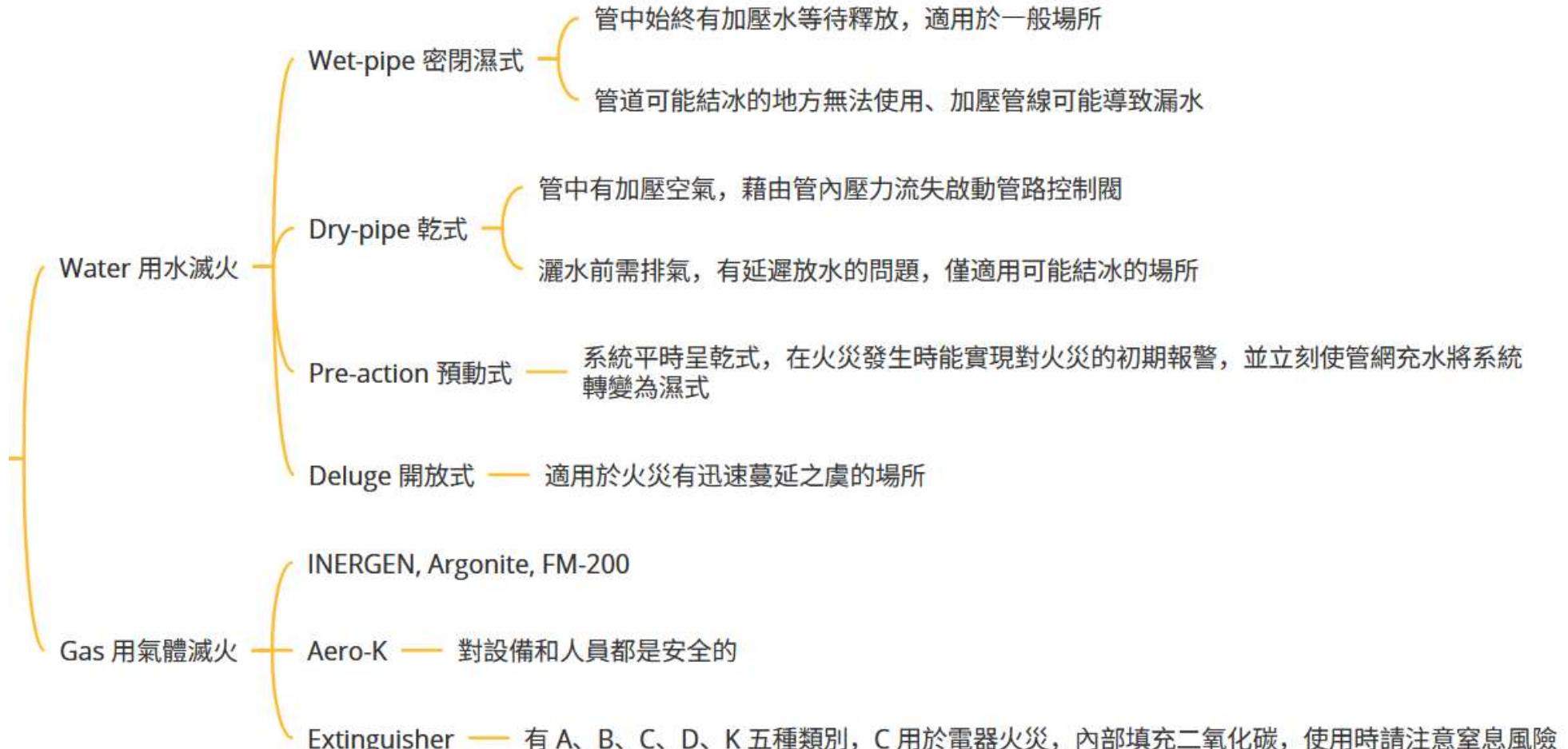
圍欄可減少通行，同時讓旁觀者看到可疑活動。

Ref. <https://zh.wikipedia.org/zh-tw/%E9%80%9A%E8%BF%87%E7%8E%AF%E5%A2%83%E8%AE%BE%E8%AE%A1%E9%A2%84%E9%98%B2%E7%8A%AF%E7%BD%AA>

3.7.3 Fire – Fire Detection



3.7.3 Fire – Fire Suppression



3.7.4 Power



3.7.5 Data Center

- Tier 1 基礎設施數據中心機房
 - 專門用於伺服器空間、不間斷電源 (UPS)、冷卻設備、發電機
 - 可用性 99.671% (每年停機小於 28.8 小時)
- Tier 2 夠餘容量設施數據中心機房
 - T1所有功能，添加冗餘關鍵電源和冷卻組件(部分 N+1)，如UPS、冷卻設備、發電機
 - 可用性約 99.741% (每年停機小於 22 小時)
- Tier 3 運行可同時維護數據中心機房
 - T2 所有功能，不需要關閉設備更換和維護 (全 N+1)
 - 可用性約 99.982% (每年停機小於 1.6 小時)
- Tier 4 容錯型數據中心機房
 - T3 所有功能，添加了容錯概念。容錯要求所有電源和冷卻組件都是2N完全冗餘 (2個完全獨立系統)
 - 可用性約 99.995% (每年停機小於 26.3 分鐘)

Knowledge check

What type of fire suppression system fills with water after a valve opens when the initial stages of a fire are detected and then requires a sprinkler head heat activation before dispensing water?

- A. Wet pipe
- B. Dry pipe
- C. Deluge
- D. Pre-action

版權所有，翻印必究

Understand reasons and requirements for cryptography

Carla's organization recently suffered a data breach when an employee misplaced a laptop containing sensitive customer information. Which one of the following controls would be least likely to prevent this type of breach from reoccurring in the future?

- A. Full disk encryption
- B. File encryption
- C. File integrity monitoring
- D. Data minimization

Which one of the following cryptographic goals protects against the risks posed when a device is lost or stolen?

- A. Nonrepudiation
- B. Authentication
- C. Integrity
- D. Confidentiality

版權所有，翻印必究

5.2 Apply cryptography concepts

What encryption algorithm would provide strong protection for data stored on a USB thumb drive?

- A. TLS
- B. SHA1
- C. AES
- D. DES

Chris wants to verify that a software package that he downloaded matches the original version. What hashing tool should he use if he believes that technically sophisticated attackers may have replaced the software package with a version containing a backdoor?

- A. MD5
- B. 3DES
- C. SHA1
- D. SHA 256

5.3 Understand and implement secure protocols

Susan would like to configure IPSec in a manner that provides confidentiality for the content of packets. What component of IPSec provides this capability?

- A. AH
- B. ESP
- C. IKE
- D. ISAKMP

Ed has been asked to send data that his organization classifies as confidential and proprietary via email. What encryption technology would be appropriate to ensure that the contents of the files attached to the email remain confidential as they traverse the Internet?

- A. SSL
- B. TLS
- C. PGP
- D. VPN

Understand and support public key infrastructure (PKI) systems

Andrew believes that a digital certificate belonging to his organization was compromised and would like to add it to a Certificate Revocation List. Who must add the certificate to the CRL?

- A. Andrew
- B. The root authority for the top-level domain
- C. The CA that issued the certificate
- D. The revocation authority for the top-level domain

版權所有，翻印必究



Domain 4

Communication and Network Security

(13%, 120 min)

Outline

4.1 Open Systems Interconnection (OSI) Model

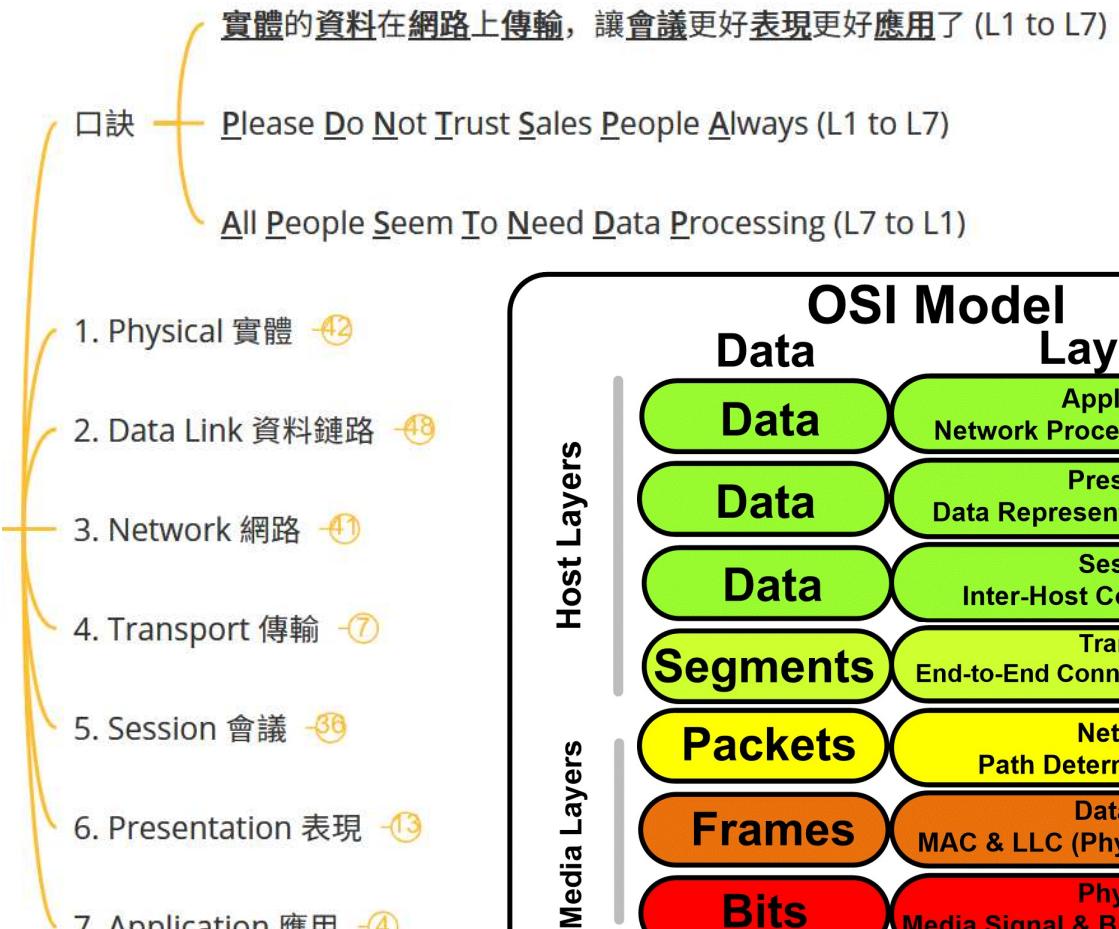
4.2 Secure network

4.3 Remote Access



版權所有，翻印必究

4.1 Open Systems Interconnection (OSI) Model



Knowledge check

Which of the following shows the layer of the OSI model in correct order, from layer 1 to later 7? Place the layers of the OSI model shown here in the appropriate order, from layer 1 to layer 7.

- A. Data, Physical, Network, Transport, Session, Presentation, Application
- B. Physical, Data, Network, Transport, Session, Presentation, Application
- C. Physical, Data, Network, Transport, Session, Application, Presentation
- D. Physical, Data, Network, Session, Transport, Presentation, Application

Knowledge check

SMTP, HTTP, and SNMP all occur at what layer of the OSI model?

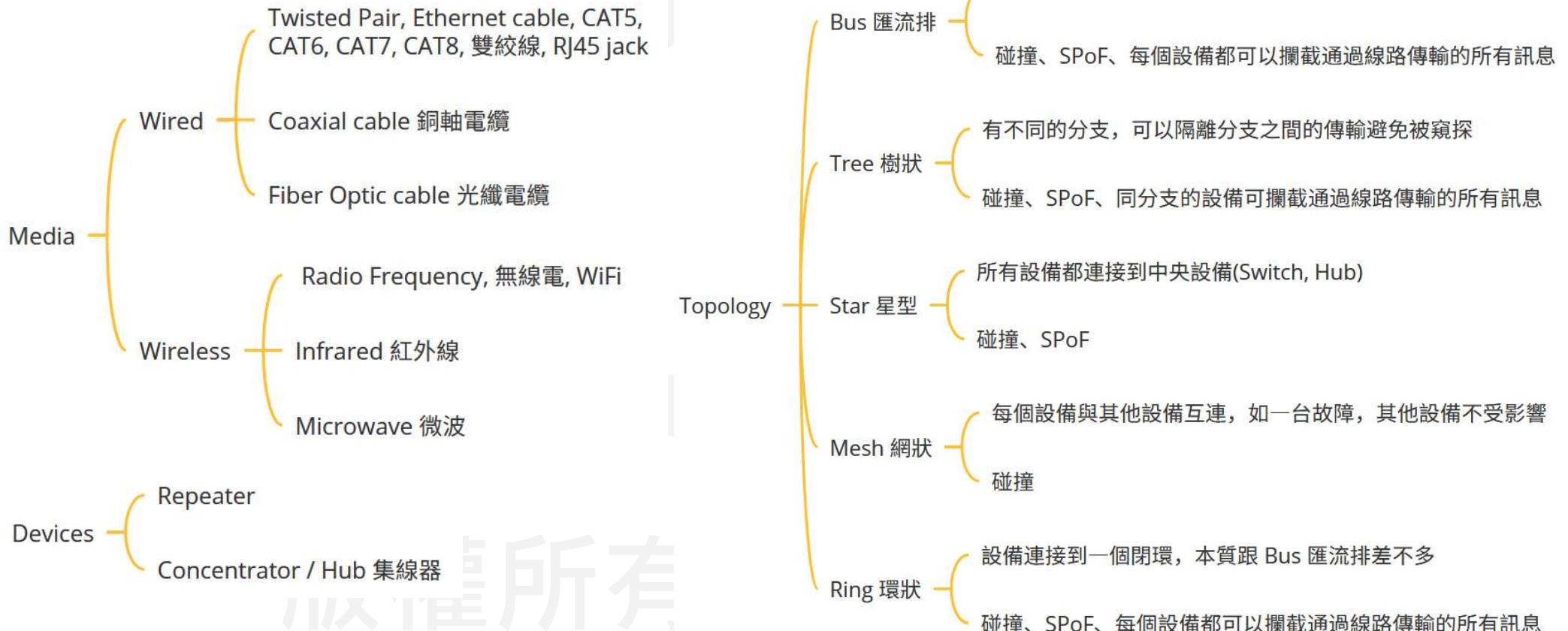
- A. Layer 4
- B. Layer 5
- C. Layer 6
- D. Layer 7

The Address Resolution Protocol (ARP) and the Reverse Address Resolution Protocol (RARP) operate at what layer of the OSI model?

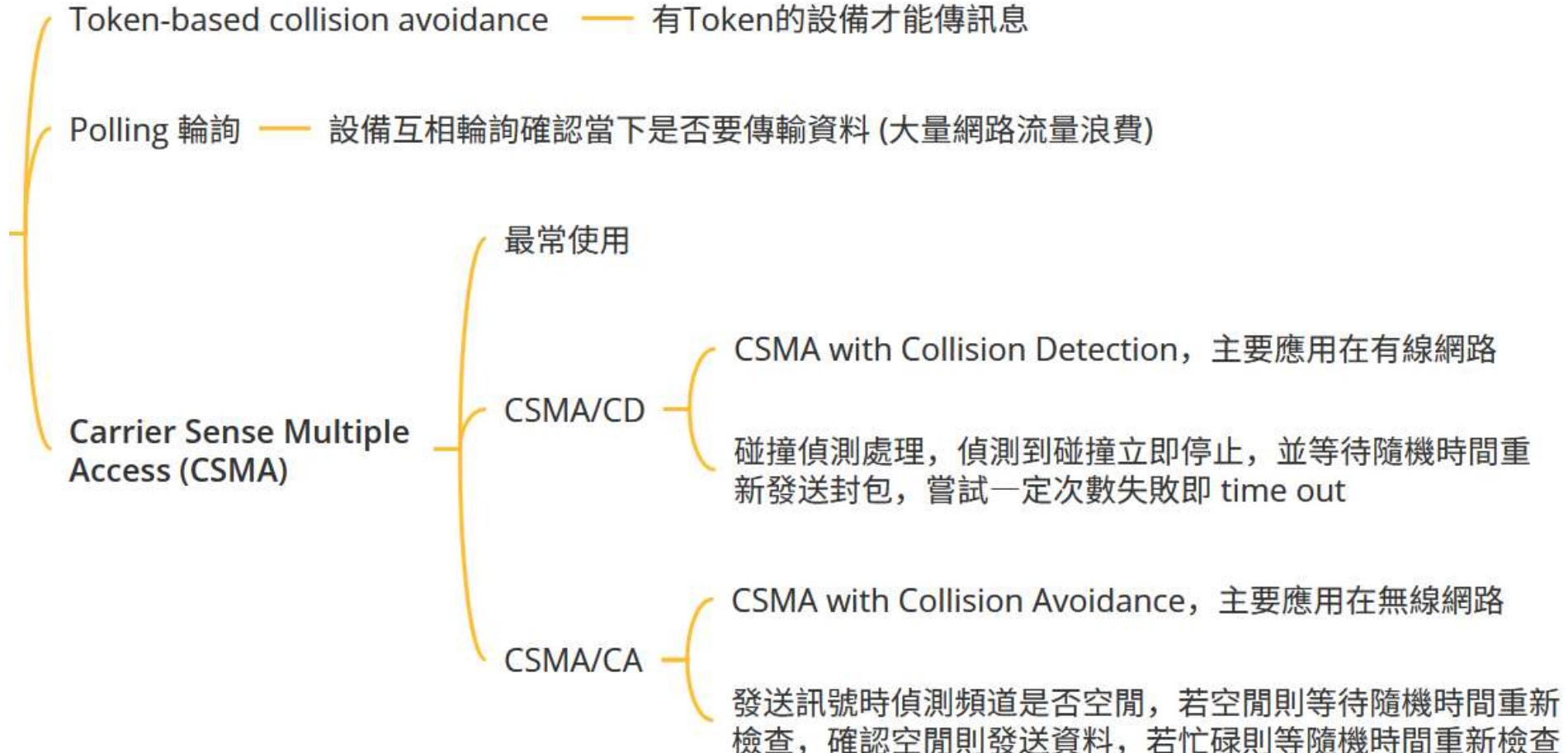
- A. Layer 1
- B. Layer 2
- C. Layer 3
- D. Layer 4

版權所有，翻印必究

4.1.1 Physical - Introduction



4.1.1 Physical - Dealing with collisions



4.1.2 Data Link – Introduction

- MAC Address
- unique physical address
 - 共 6 碼，前三碼為 OUI (Organizational Unique Identifier)、後三碼為 Device 流水號，所以可以透過前三碼推測廠牌
- Topology
- Modem 數據機 — Transmission of digital data over analog connections
 - Circuit-switched network 電路交換網路 — 兩個通訊的端點之間建立實體線路連線，一旦建立兩端之間的連線後，佔用線路並傳輸資料(即他人無法使用)。ex. 公共交換電話網路(PSTN)
 - Packet-switched network 封包交換網路 — 將資料組合成適當大小的區塊，稱為封包，再通過網路來傳輸

4.1.2 Data Link – Device

收到 Frames 看看 MAC 是不是自己的，是的話收下解封裝，不是的話就往外送

Bridges 橋接器

只有兩個 port

判斷是不是自己的負責範圍的 MAC Address 不是的話丟回去

Switches 交換機

多 port 的 Bridges, Create single port collision domain (不會有碰撞發生)

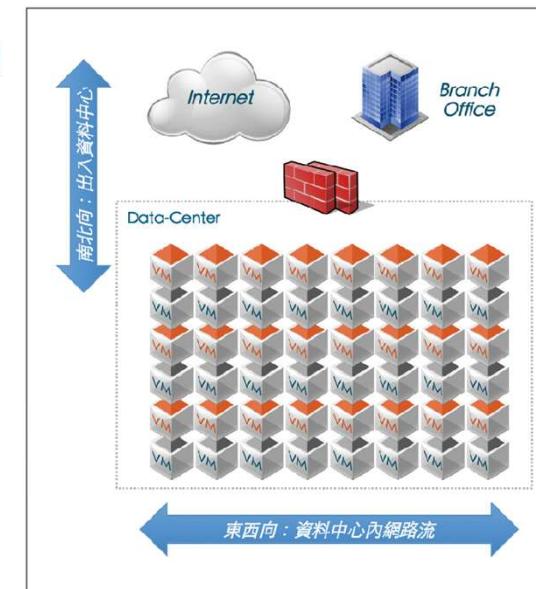
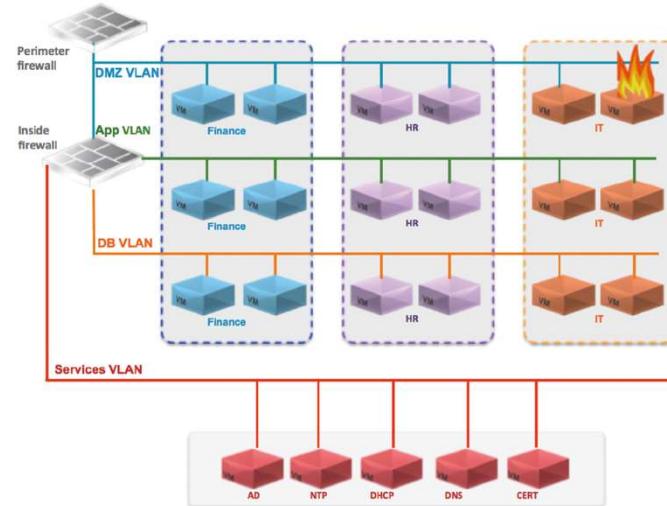
跟 Hub 不一樣，接任一 port 聽不到其他 port 的流量 (正常狀況下)

以前同一個單位的人只能在同一個實體網路

VLANs = Segement

透過 VLAN 可以跨 Switch 聯繫

VXLAN, Micro-Segmentation -②



4.1.2 Data Link – Protocols

- ARP- IP to MAC
- RARP - MAC to IP
- Tunneling protocol — L2TP (待會講VPN的時候會提)

版權所有，翻印必究

4.1.3 Network - Protocol

- IP Address
- ICMP — Internet Control Message Protocol, 用於傳遞消息及網路環境偵錯, ex. Ping 用於嘗試查看主機設備是否可到達、TraceRoute 顯示封包在IP網絡經過的路由器的IP位址
- IGMP — Internet Group Management Protocol, 可讓多個裝置共用一個IP 位址, 以便所有裝置都能接收相同的資料。這在提高多媒體傳輸時的網絡性能尤為重要
- IPSec — 建立安全網路連線的通訊規則或協定
- OSPF — Open Shortest Path First, 開放最短路由優先協定, 將鏈路視為路由器上的介面。鏈路的狀態描述該介面及其與其鄰居路由器的關係。最短路徑優先演算法來構建和計算到達所有目的地的最短路徑

4.1.3 Network – LAN Technologies

- Wired — IEEE 802.3 defines a collection of communication standards for physical connections on a wired Ethernet network.
- Wireless — IEEE 802.11 is a collection of communication standards specific to the implementation of WLAN communication
- Virtual LAN (VLAN) — IEEE 802.1Q defines the standard for virtual local area networks. VLANs are used to create isolated networks for purposes of security and to minimize broadcast traffic on a network.
- Private IPv4 Addresses —
 - RFC 1918
 - 10.0.0.0 – 10.255.255.255 (1 個 A 類網路) — 10.0.0.0/8 (255.0.0.0)
 - 172.16.0.0 – 172.31.255.255 (16 個連續 B 類網路) — 172.16.0.0/12 (255.240.0.0)
 - 192.168.0.0 – 192.168.255.255 (256 個連續 C 類網路) — 192.168.0.0/16 (255.255.0.0)

4.1.3 Network – Devices & IPv4 -> IPv6



版權所有，翻印必究

4.1.4 Transport - Introduction



4.1.4 Transport - Common Port

21 —— FTP —— 檔案傳輸協定

22 —— SSH —— 加密的網路傳輸協定，可在不安全的網路中為網路服務提供安全的傳輸環境，ex. SFTP (前面加S就是SSH)

23 —— Telnet —— 使用於網際網路及區域網中，使用虛擬終端機的形式，提供雙向、以文字字串為主的命令列介面互動功能，ex. BBS

25 —— SMTP —— 透過網路傳輸電子郵件

53 —— DNS —— Domain name 轉換 IP

161
61 —— SNMP —— 支援網路管理系統，用以監測連接到網路上的裝置是否有任何引起管理上關注的情況

69 —— TFTP —— 簡單文件傳輸的協議

80 —— HTTP —— 用於在聯網裝置之間傳輸資訊

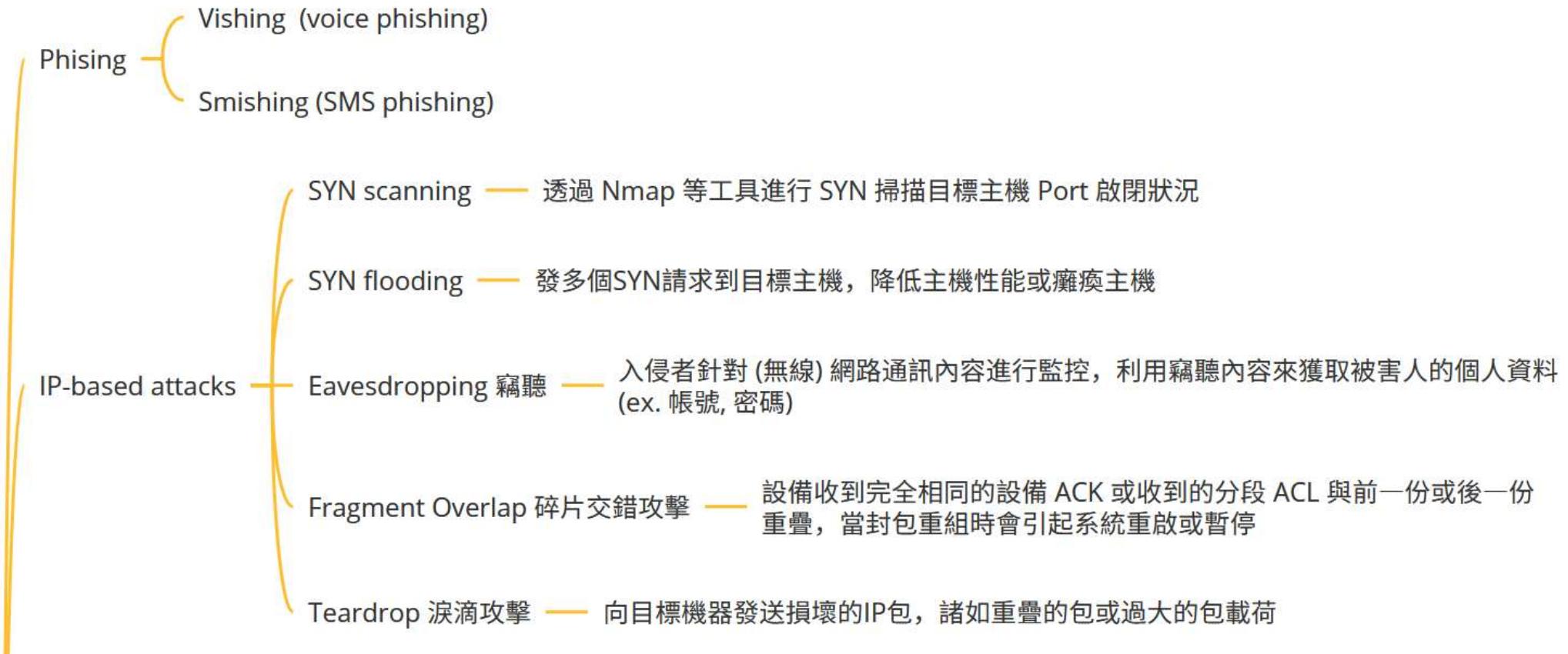
443 —— HTTPS —— 透過網路進行安全通訊的傳輸協定

RTP / SRTP —— 定義網路影音數據傳輸的標準格式 (VoIP)

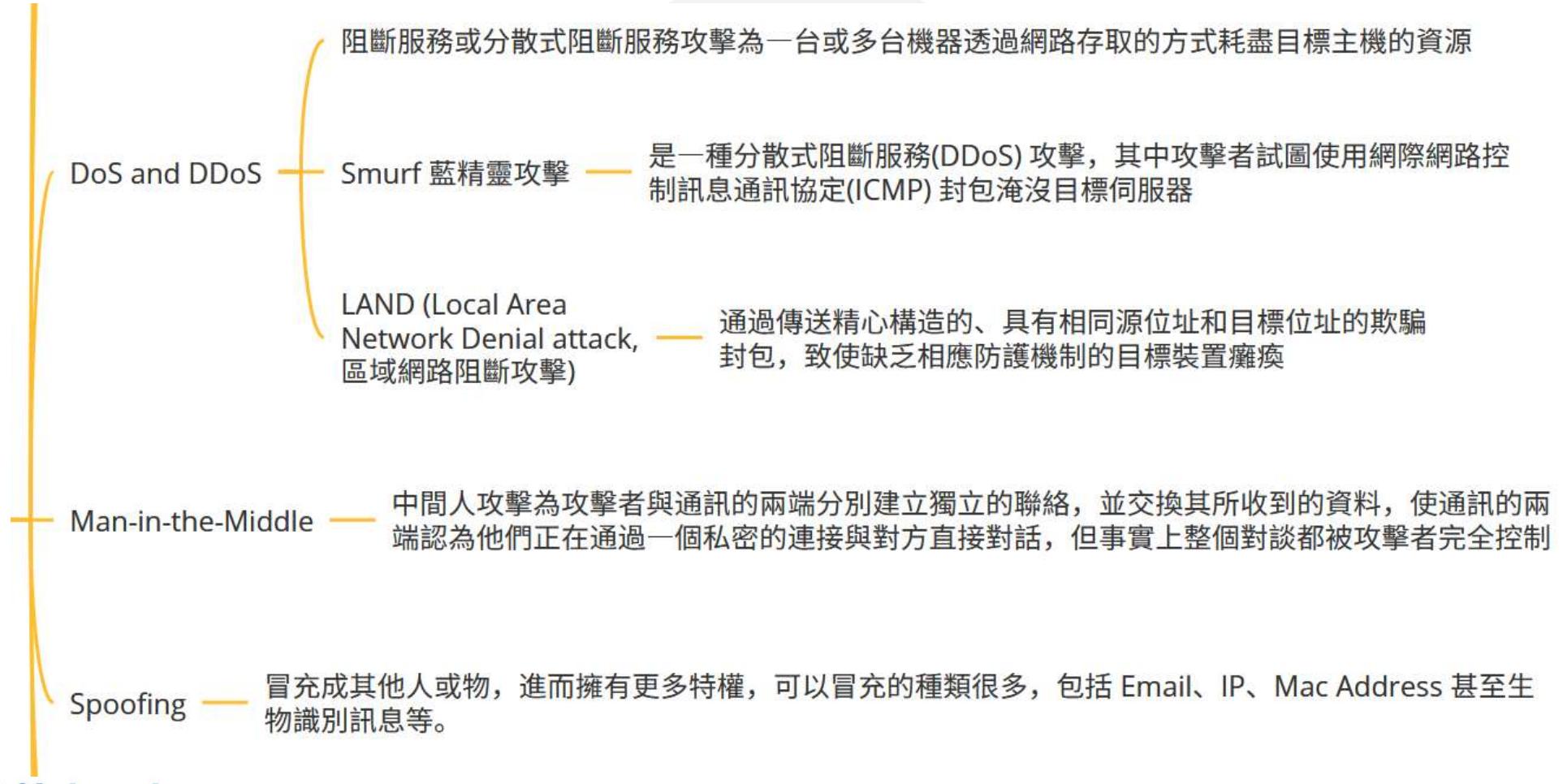
SIP —— 作為一個或多個使用者在網路上建立、修改、維護和終止會談的通訊使用(VoIP)

翻印必究

L1~L4 Threats - 1



L1~L4 Threats - 2



L1~L4 Threats - 3

ARP poisoning

攻擊者透過修改 ARP Table 將另一設備的網路流量導到攻擊標的。

開啟 Port Security 功能、關閉不需要的 Port 或服務、關閉實體沒在用的介面、指定特定的介面為管理或監控介面

Common tools
and protocols

-24

版權所有，翻印必究

L1~L4 Threats - 4

Ping —— 用來測試封包能否透過IP協定到達特定主機

Traceroute —— 顯示封包在IP網路經過的路由器的IP位址

ICMP —— 診斷網路通訊問題的網路層通訊協定

DHCP —— 使網路管理員能夠集中管理和自動分配IP網路位址的通信協定

Ipcconfig —— 顯示現時網路連線的設定

WHOIS —— 查詢網際網路中域名的IP以及所有者等資訊的傳輸協定

Dig —— 一個網絡管理命令行工具，用於查詢 DNS

Putty —— 整合虛擬終端、系統控制台

Nmap —— 檢測目標主機是否線上、埠開放情況、偵測執行的服務類型及版本資訊、偵測作業系統與裝置類型等資訊

John the Ripper —— 免費的密碼破解工具

Netstat —— 基於命令列介面的網路實用工具，可顯示當前的網路狀態，包括傳輸控制協定層的連線狀況、路由表、網路介面狀態和網路協定的統計訊息

Nslookup —— 網絡管理命令行界面工具，用戶可以利用nslookup查詢域名的ip地址以及ip地址所對應的域名

Knowledge check

In what type of attack do attackers manage to insert themselves into a connection between a user and a legitimate website?

- A. Man-in-the-middle
- B. Fraggle
- C. Wardriving
- D. Meet-in-the-middle

What type of attack is most likely to occur after a successful ARP spoofing attempt?

- A. A DoS attack
- B. A Trojan
- C. A replay attack
- D. A man-in-the-middle attack

版權所有，翻印必究

Knowledge check

Melissa uses the ping utility to check whether a remote system is up as part of a penetration testing exercise. If she does not want to see her own ping packets, what protocol should she filter out from her packet sniffer's logs?

- A. UDP
- B. TCP
- C. IP
- D. ICMP

版權所有，翻印必究

Knowledge check

As a security analyst, you are implementing Network Access Control (NAC) to secure your organization's network, ensuring only authorized and compliant devices connect. Which option best demonstrates proper NAC implementation?

- A. Use 802.1X authentication to verify user and device compliance, redirecting non-compliant devices to a remediation VLAN.
- B. Allow all devices to connect, logging MAC addresses for post-connection monitoring.
- C. Rely solely on MAC address filtering to block unauthorized devices.
- D. Grant full network access after VPN connection without checking device compliance.

4.1.5 Session

提供 Host to Host & 同個通訊協定的主機連線

- Protocols
 - RPC(Remote Procedure Call) — 允許執行於一台電腦的程式呼叫另一個位址空間的子程式，而程式設計師就像呼叫本地程式一樣
 - SQL(Structure Query Language) — 管理關聯式資料庫管理系統語法
 - NFS(Network File System) — 允許 Client 可以存取 Server 端檔案

- Authentication protocol
 - PAP (Password) — 最不安全的身分驗證方法，以明文形式完成驗證，容易被攻擊者攔截
 - CHAP (Challenge handshake) — 不使用密碼，採用挑戰(Server發)、回應(Client hash 後回給 Server)機制進行身分驗證(Server 跟驗算)，不易遭受中間人攻擊

- EAP (Extensible)
 - EAP-TLS — 把 EAP 封裝在 TLS 通道中，常用於無線網路中，AP與用戶端都要有憑證，採取雙向認證
 - EAP-TTLS — EAP-TLS改良版，AP有憑證即可，採取雙向認證
 - PEAP — EAP-TLS 微軟實作的改良版

Devices — Circuit-Level Proxy Firewall (待會講VPN的時候會提)

4.1.6 Presentation

- 不同通訊協定的主機連線起來，在這層
- 加解密、定格式(浮點運算 (小數點...), 影像檔, 字元集)
- Device —— Gateway —— 連接不同通訊協定

版權所有，翻印必究

4.1.7 Application

Devices — Application Firewalls (待會講VPN的時候會提)

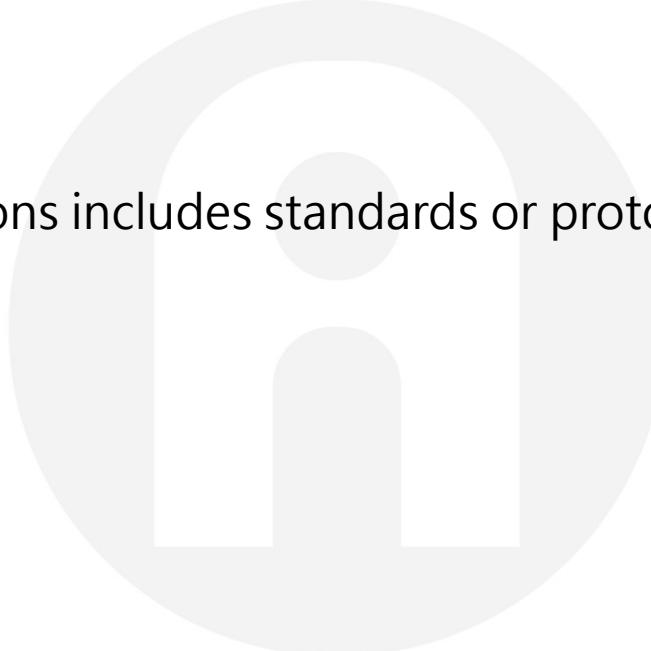
Protocols — HTTP/S, DNS, SSH, SNMP, LDAP, DHCP, SMTP

版權所有，翻印必究

Knowledge check

Which of the following options includes standards or protocols that exist in layer 6 of the OSI model?

- A. NFS, SQL, RPC
- B. TCP, UDP, TLS
- C. JPEG, ASCII, MIDI
- D. HTTP, FTP, SMTP

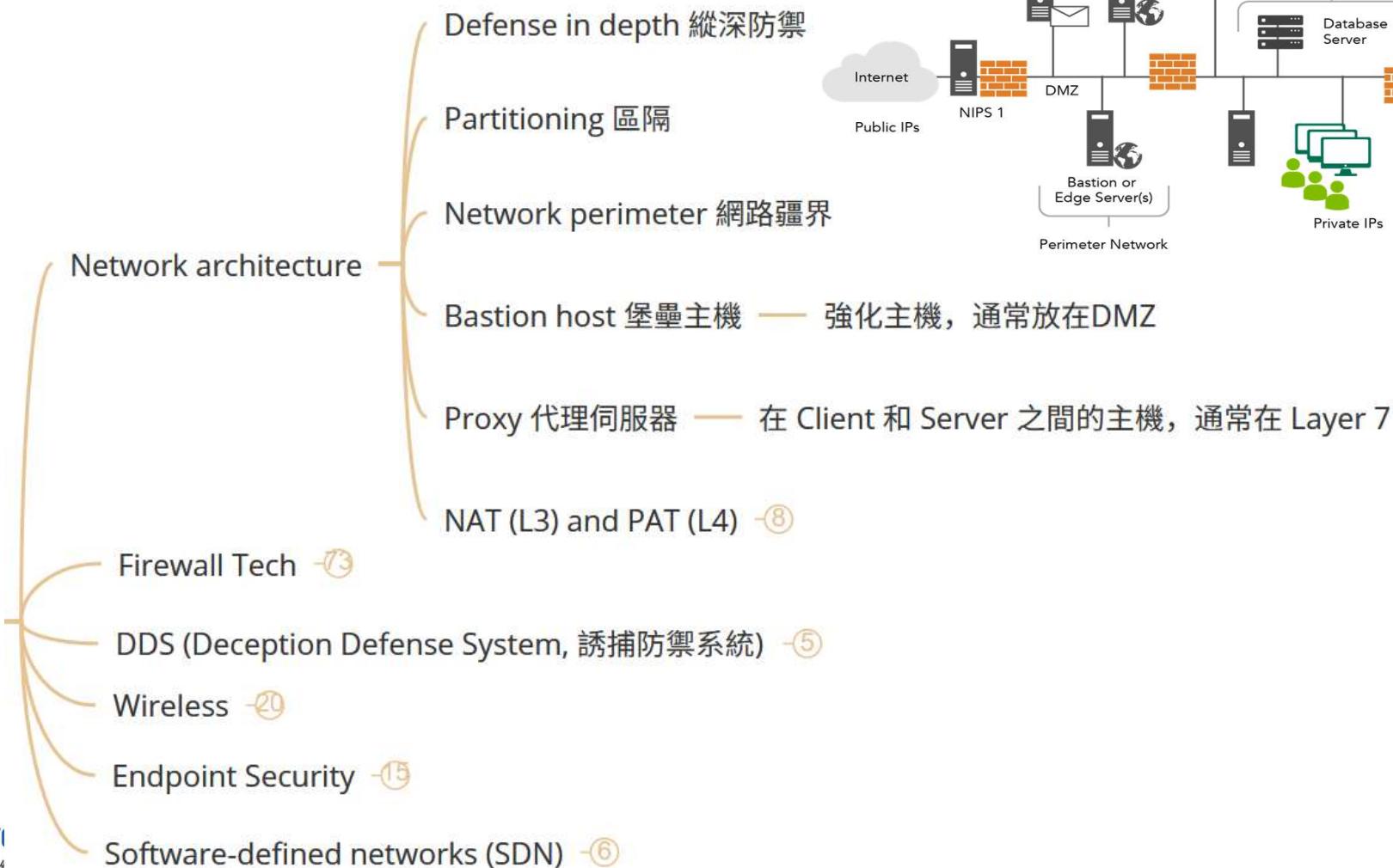


版權所有，翻印必究

L4 ~ L7 Threats



4.2 Secure network



4.2.1 Network Architecture – NAT / PAT

PAT = Port Address Translation

外部 IP 的 Port 可以對到內部不同 IP 和 Port

內部可以共用一個外部 IP 連到外部

ex. 10.0.0.1:2007 → 192.168.10.10:2007

ex. 10.0.0.1:2008 → 192.168.10.12:80

NAT = Network Address Translator

外部 IP 與 內部 IP 對應(1 對 1、多對多)

ex. 10.0.0.2 → 192.168.10.2

4.2.2 Firewall Tech

用於限制一個網路(通常是外部) 對特定網路(通常是內部)的訪問

必要設定：沒有明確的 Allow，預設 DENY

(L4) Static Packet Filtering — 封包過濾防火牆，查看來源 IP、目的 IP、Port、Service，使用 ACL 監控
(Access Control List, Domain 3 DAC 有講到)

(L4) Stateful Packet Filtering = Dynamic Packet Filter — 持續追蹤穿過這個防火牆的各種網路連線，使用 State Table (TCP)追蹤連線的狀態

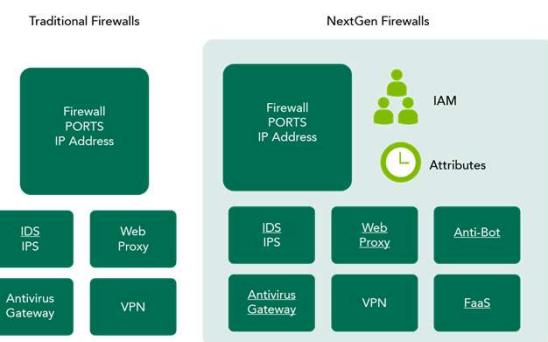
5 種類別 — (L5) Circuit-Level Proxy — 不監視 L6, L7 協定，處理速度快

(L7) Application-Level Proxy = Proxy Firewall — 監視每個協定，提供更高的安全，設定複雜且速度較慢

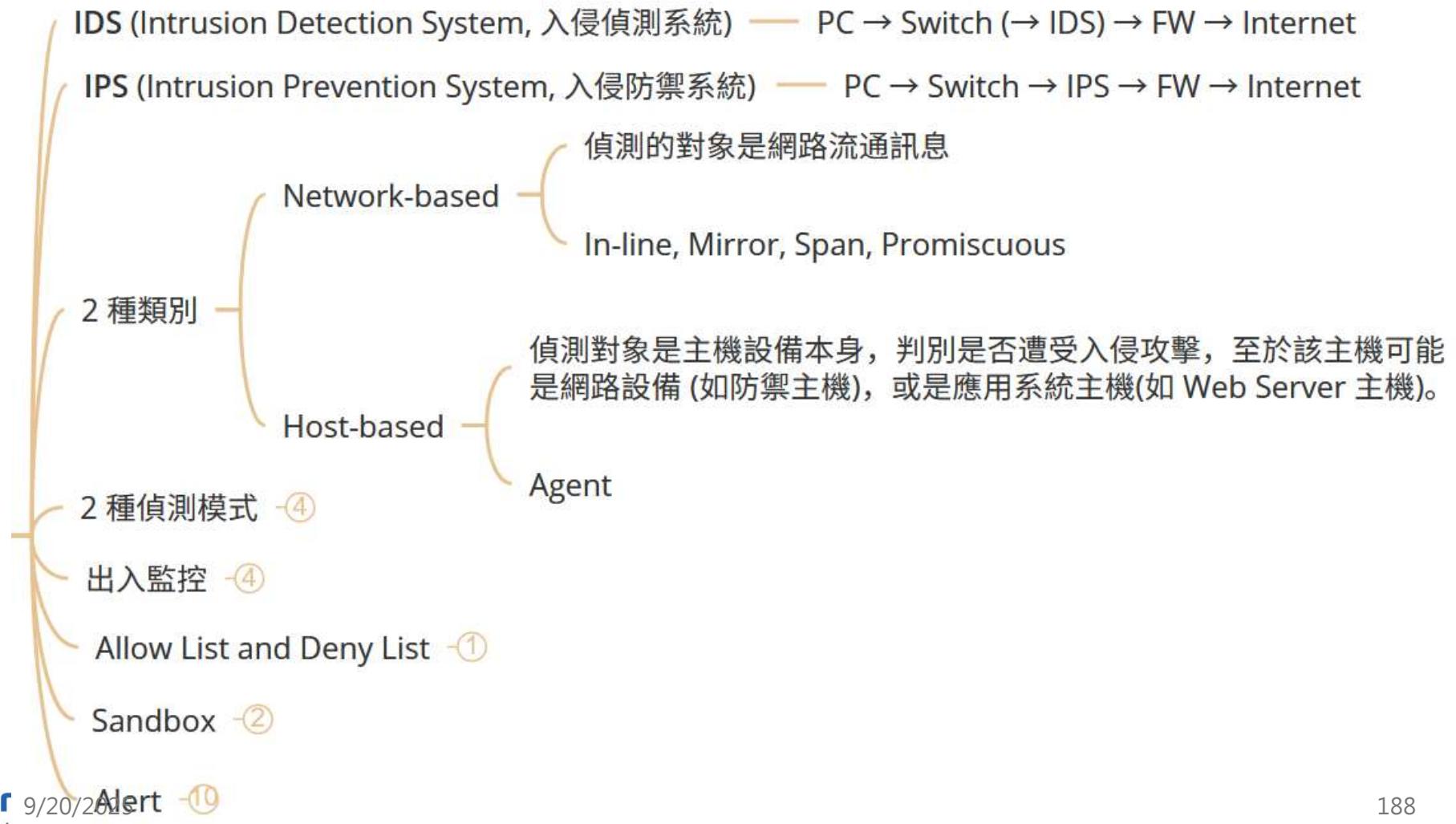
(ALL) Next Generation Firewall (NGFW) — 非常快速和支援高頻寬，內建IPS 能夠連接到 Active Directory等外部服務

5 種架構 → 13

IDS & IPS → 38



4.2.2 Firewall Tech – IDS & IPS - 1



4.2.2 Firewall Tech – IDS & IPS - 2

- 2 種偵測模式
 - Pattern-based —— 基於已知類型的攻擊進行檢查
 - Anomaly-based —— 偵測異常 (這代表需要先了解什麼是正常、異常)
- 出入監控
 - Ingress monitoring 輸入監控 —— 目的為防止惡意流量流入網路
 - Egress monitoring 輸出監控 —— 目的為防止資料出境或其他內部惡意橫向移動
- Allow List and Deny List —— 黑白名單 (涉及種族歧視，現已不用黑白)
- Sandbox
 - 沙箱，常用於防火牆用以隔離和運作未受信任的程式碼
 - 屬於一種 corrective 矯正措施 (Domain 1)

4.2.2 Firewall Tech – IDS & IPS - Alert

We will discuss it in Domain 5 Identity and Access Management (IAM) in detail.

原則：True False 是描述前面判斷結果是對還是錯的、Positive Negative 是設備判斷結果 (快篩)

True-Positive —— 駭客攻擊、資安工具發報

True-Negative —— 駭客沒有攻擊、資安工具沒有發報

False-Positive —— 駭客沒有攻擊、資安工具發報 (偽陽性, Type I Error)

False-Negative —— 駭客攻擊、資安工具沒有發報 (嚴重, 偽陰性, Type II Error)

補充：交叉錯誤率 (Crossover Error Rate, CER) 是型一錯誤和型二錯誤相等的點，代表了衡量生物識別有效性的最佳方法。

Knowledge check

Which one of the following security tools is not capable of generating an active response to a security event?

- A. IPS
- B. Firewall
- C. IDS
- D. Antivirus software

What technology could Lauren's employer implement to help prevent confidential data from being emailed out of the organization?

- A. DLP
- B. IDS
- C. Firewall
- D. UDP

版權所有，翻印必究

Knowledge check

You are a security analyst configuring a network-based security appliance to protect your organization's internal network. A recent audit revealed unauthorized access attempts via outdated protocols. You need to configure the appliance to mitigate these threats while ensuring legitimate traffic is not disrupted.

Which configuration best secures the network using a network-based security appliance in response to the audit findings?

- A. Configure the firewall to block all inbound traffic using the Telnet protocol (port 23) and enable deep packet inspection (DPI) to detect encrypted malicious payloads.
- B. Set the intrusion prevention system (IPS) to allow all traffic but log attempts to use deprecated protocols for later review.
- C. Enable a proxy server to redirect all outbound traffic to a single port without filtering specific protocols.
- D. Configure the firewall to allow all inbound traffic on port 80, assuming it is safe for web traffic, without additional protocol checks.

4.2.3 DDS (Deception Defense System, 誘捕防禦系統)

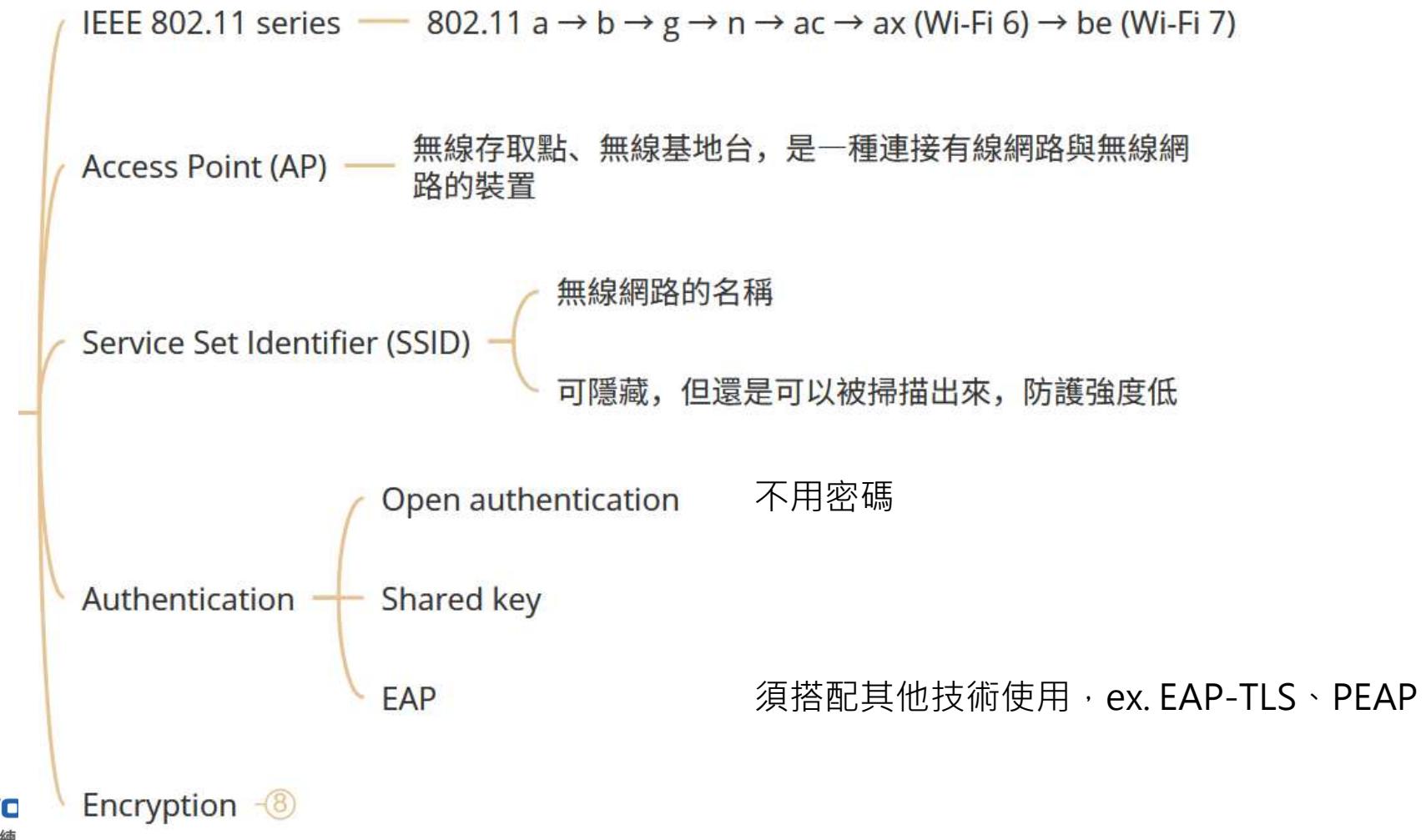
一種數位陷阱，Honeypot是特別架設的網路系統，就像昆蟲會被蜜罐吸引一樣，honeypot會偽裝成提供服務的一般伺服器，或者儲存看似有價值的資料，吸引入侵者攻擊

Honeypots —— 一台

Honeynets —— 多台

版權所有，翻印必究

4.2.4 Wireless



4.2.2 Wireless - Encryption

WEP (Wired Equivalent Privacy, 有線等效加密) — 不安全

WPA (Wi-Fi Protected Access, Wi-Fi存取保護) — 使用 Temporal Key Integrity Protocol (TKIP)

使用 Counter-Mode-CBC-MAC Protocol (CCMP), 用AES算法 in CBC-MAC (CCM)

WPA2 { WPA2-Personal 用 Pre-Shared key 驗證, 用於家庭環境
(2017年被發現 Key Reinstallation Attack (KRACK) 漏洞)

WPA2-Enterprise 用於企業 (802.1X = RADIUS + EAP)

WPA3-Personal 用 128 位元加密金鑰, 就算使用者的密碼太過簡單而有安全疑慮也無妨。這是因為 WPA3-Personal 採用 Simultaneous Authentication of Equals (SAE) 對等實體同時驗證來取代 WPA2-Personal 使用的單一共享金鑰

WPA3 { SAE 為 Diffie-Hellman 衍生物 (讓雙方在完全沒有對方任何預先資訊的條件下通過不安全信道建立起一個金鑰, Domain 3)

WPA3-Enterprise 採用 192 位元加密金鑰來提供更好的安全性。這是 WPA2 的進一步強化, 能讓整個企業套用一致的資安設定。

Knowledge check

You are a security analyst tasked with securing your organization's wireless network. Recent audits identified vulnerabilities in the current wireless setup, including weak encryption and unauthorized access points. You need to configure the wireless network to ensure secure communications while maintaining usability for employees. Which configuration best secures the organization's wireless communications?

- A. Implement WPA3-Enterprise with 802.1X authentication, enforce AES-256 encryption, and enable rogue access point detection.
- B. Use WPA2-Personal with a shared pre-shared key (PSK) and disable SSID broadcasting to prevent unauthorized access.
- C. Configure the wireless network to use WEP encryption and MAC address filtering to restrict access to authorized devices.
- D. Enable WPA2-Enterprise with TKIP encryption and allow guest access without authentication to improve usability.

4.2.3 Endpoint Security - 1

Network Access Control(NAC)
Network Access Protection (NAP)

網路存取管制系統，這類系統通常用於管制內部存取行為，避免有人不正當地存取公司網路資源，或拿筆電自行接上網路線，進行攻擊行為；同時在符合安全政策下，提供訪客存取內部網路資源的方便。

當設備接上網路 → NAC 偵測到設備，檢查是否為 Trusted device → 依據 Security Policy 紿予設當權限 → 非 Trusted Device 去 Captive Portal 驗證 → 驗證後給予適當權限

Traditional AntiVirus (AV) —— 傳統防毒軟體，針對已知威脅、特徵碼防禦

EPP (Endpoint Protection Platform) —— 端點保護平台解決方案通常是採用雲端管理，且會利用雲端資料協助進行進階監控和遠端修復作業

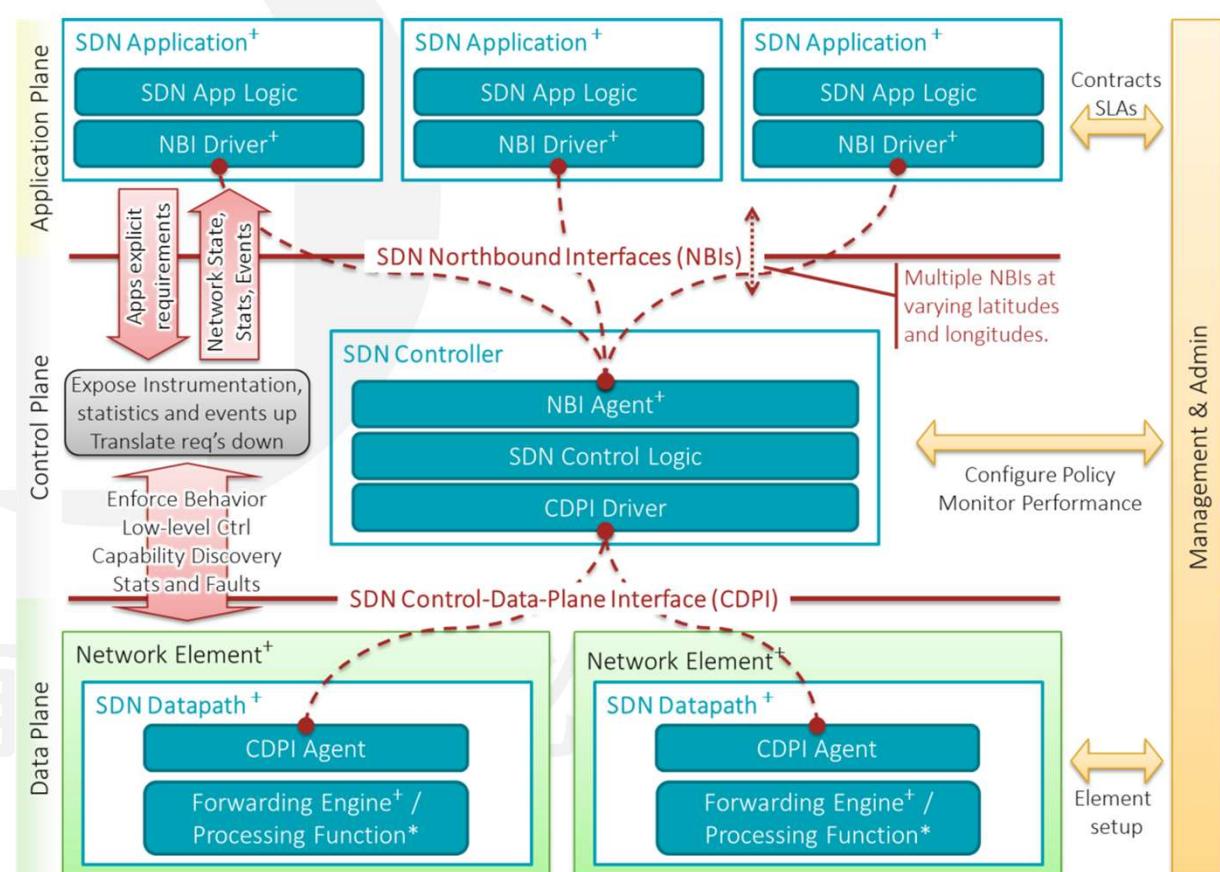
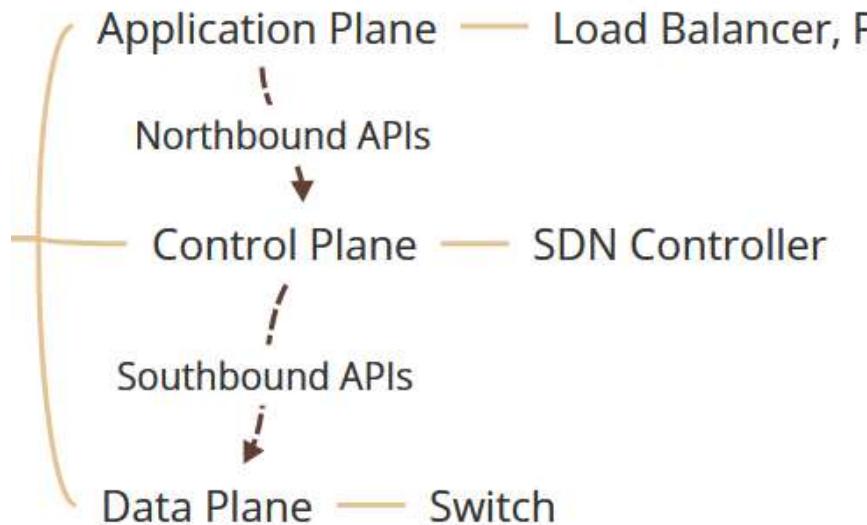
Endpoint Detection & Response (EDR) —— 為端點安全解決方案，其中包括即時監控與收集端點安全性資料的功能，並具備自動威脅回應機制。

4.2.3 Endpoint Security - 2

-  Endpoint Detection & Response (EDR) — 為端點安全解決方案，其中包括即時監控與收集端點安全性資料的功能，並具備自動威脅回應機制。
-  補充 NDR (Network) — 透過包括高效的工作流程和自動化、網路中的定位和機器學習(ML)的幫助，洞察和分析所有的網路，來識別和消除特別是橫向移動
-  補充 XDR (Extended) — 借助更強大的人工智能和自動化方法，擴展了 EDR 的潛力，過超越單向量點解決方案，將設備間流量以及用於分析和評估的應用程序包括在內，從而提供對企業網路的可視性 (EDR + NDR)
-  補充 MDR (Managed) — 託管式偵測及回應(重點在服務)，安全供應商為他們的 MDR 客戶提供存取專門從事網路監控、事件分析和安全事件回應之安全分析師和工程師的權限

九月’的印必九

4.2.4 Software-defined networks (SDN)



⁺ indicates one or more instances | * indicates zero or more instances

199

4.3 Remote Access - 1

- 建立虛擬線路 Tunnel
- VPN 的目的
- 安全的服務 (Tunnel 要不要加密), ex. IPSec
- Generic Routing Encapsulation (GRE) -③
 - Split tunneling -①
 - Authentication protocol -⑧
 - IPSec -④
 - Internet Key Exchange (IKE) -④
 - SSL / TLS -②
 - Remote Authentication -⑧

]必究

4.3 Remote Access - 2

Generic Routing Encapsulation (GRE)

當企業需要透過 Internet 使用 Routing Protocol 進行 Route 交換時，通常會在 Site 與 Site 之間建立 GRE Tunnel。

可以選擇要不要加上 IPSec

把原始封包(Original Header + Original Data) 加上 Encapsulating Header 和 GRE Header 一起送出去

Split tunneling

分割通道，透過加密的 VPN 傳送某些應用程式或裝置流量，其他應用程式或裝置則可直接存取網際網路。(不用全部流量都回總公司下車)

Authentication protocol

PAP (Password) — 最不安全的身分驗證方法，以明文形式完成驗證，容易被攻擊者攔截

CHAP (Challenge handshake) — 不使用密碼，採用挑戰(Server發)、回應(Client hash 後回給 Server)機制進行身分驗證(Server 跟驗算)，不易遭受中間人攻擊

EAP (Extensible) — 一種驗證框架，可與各種技術和協議一起使用

EAP-TLS — Client 和 Server 彼此使用數位憑證進行驗證

Knowledge check

Which one of the following protocols is commonly used to provide back-end authentication services for a VPN?

- A. HTTPS
- B. RADIUS
- C. ESP
- D. AH

版權所有，翻印必究

4.3 Remote Access - IPSec

提供機密性(不一定有加密!!)、完整性

Security Association (SA) — 在初始化時，雙方必須建立安全聯結(SA)，這個步驟的主要目的是定義了如何協商，還有要使用哪些 Policy 和參數

Transport mode
傳輸模式

只有在 Payload (存資料的載體) 加密，來源、目的地IP 等資料均未加密

通常是直接建立在兩台主機(Host to Host)上，因為不需要再多加一個 IP header，整體來說較省頻寬。

Operating Mode

Tunnel mode
通道模式

加密或認證整個封包，然後在最外面再加上一個新的IP表頭

Host to Gateway — Client to Site VPN, ex L2TP/IPSec

Gateway to Gateway — Site to Site VPN, ex. GRE/IPSec, L2TP/IPSec

AH (Authentication Header) -⑤

ESP (Encapsulating Security Payload) -④

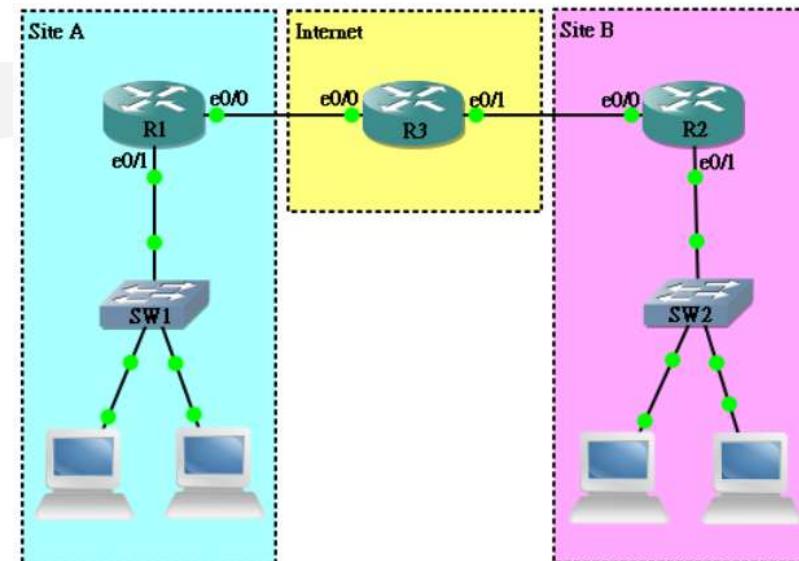
4.3 Remote Access – IPSec IKE

實作上會有兩個通道產生，一個做金鑰交換、一個傳資料

phase1: 主要做 Authenticate, Authentication 方面常常使用的都是 pre-shared key，基本上就是用同一組密碼，接著透過 Diffie-Hellman 來建立一組 Key，而這組 Key 是要被 Phase2 拿來用的。

phase2: 處理 IPsec security 協商，最後 IPSec SA 完成，接下來才會建立 IPSec 的連線

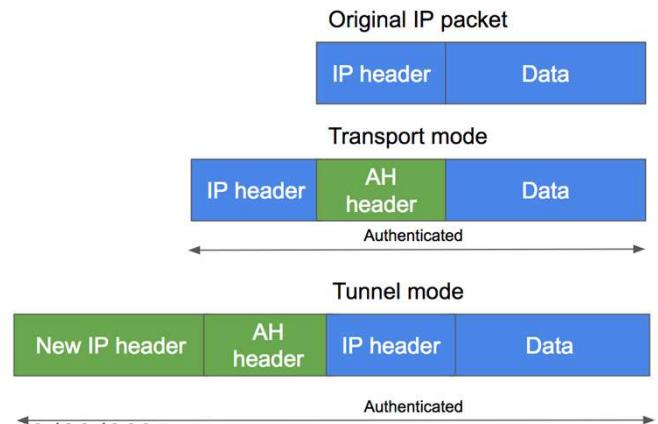
Port = 500



4.3 Remote Access - IPSec AH & ESP

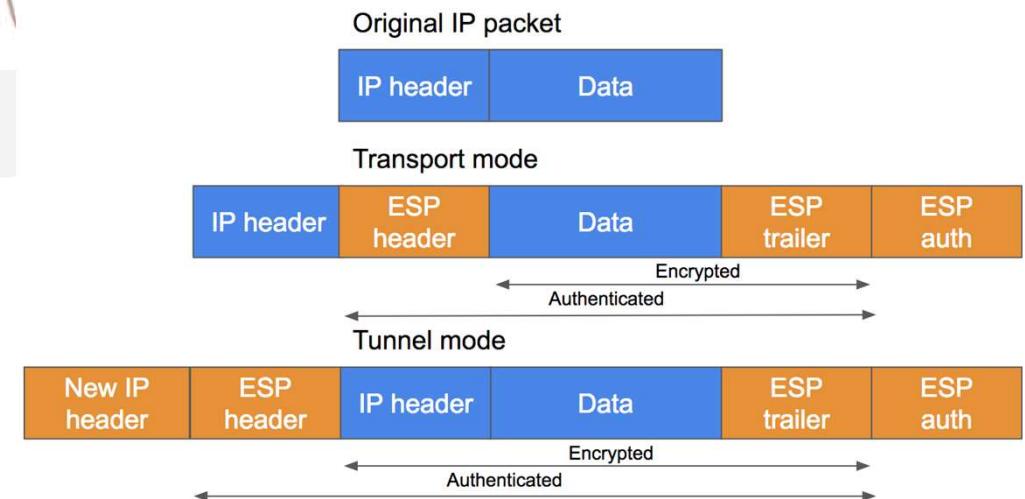
AH (Authentication Header)

- 提供完整性
- 使用 HMAC 算法，把 payload & header 和 IKE 定義好的 key 一起拿來 hash
- 注意因 NAT 會改變 header，而被改變的話，另外一邊就沒辦法解析正確，所以 AH 不能跟 NAT 共存

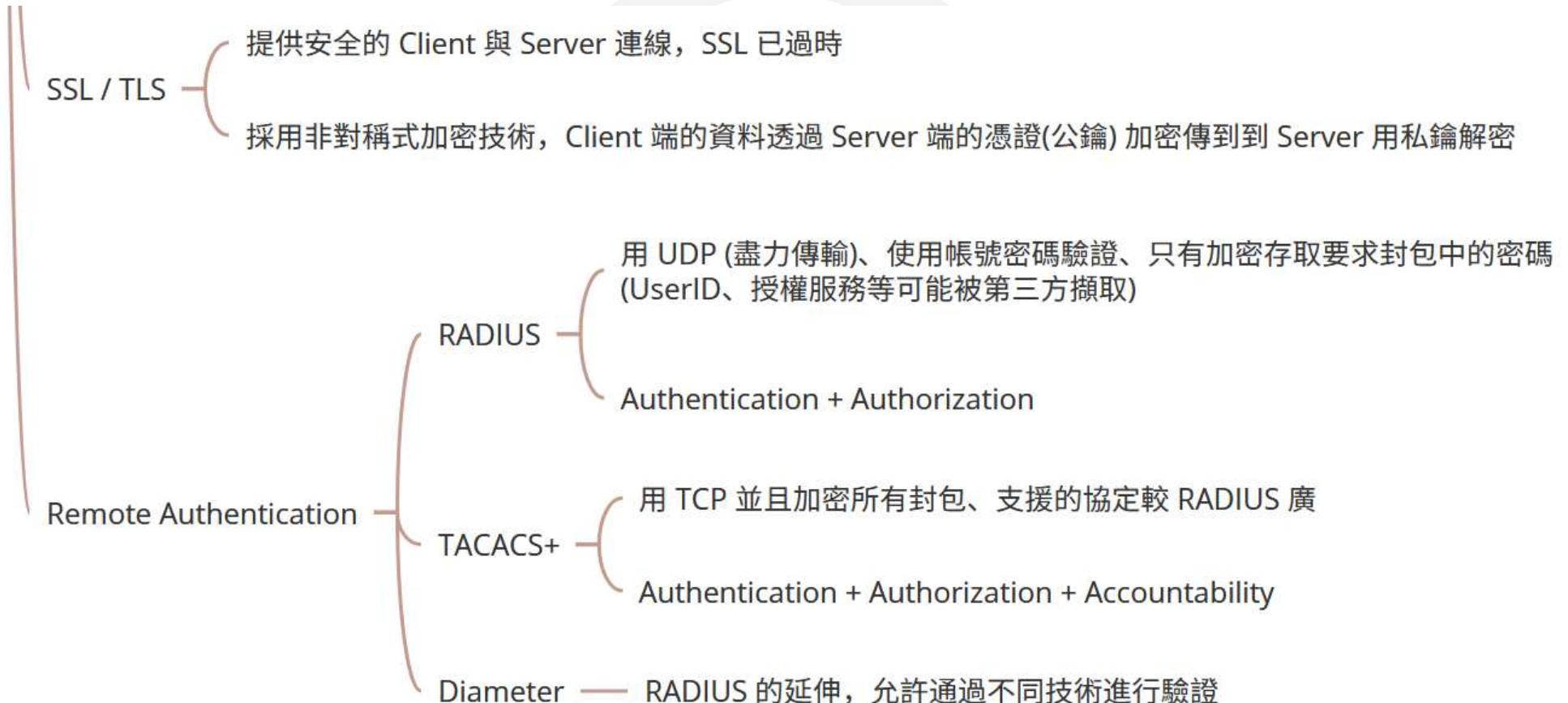


ESP (Encapsulating Security Payload)

- 提供機密性、完整性、驗證
- ESP 和 AH 最大的差別應該是 AH 會對於 Outer IP header 做驗證，所以其實 IPSec 唯有使用 ESP tunnel mode 才能和 NAT 共存



4.3 Remote – SSL/TLS & Authentication



4.4 Others

- Li-Fi
- 衛星通信
- Narrow-band wireless — Zigbee
- RFID, NFC
- 5G Cellular Network



版權所有，翻印必究