作業系統：Security and Protection

**目錄**

[作業系統：Security and Protection 1](#_Toc204271751)

[1. Background 1](#_Toc204271752)

# The Security Problem（安全問題）

電腦系統常含有薪資、財務資料或營運資料。即使是運算資源（如 CPU）也可能被用來偷挖比特幣、發送垃圾郵件（spam）與發動匿名攻擊（如 DDoS）。安全系統的定義為其資源被依照設計目的正常使用。完全的安全是不可能的，但我們可以設計機制使違規事件成為極少數異常狀況。

## 安全違規的分類：

|  |  |
| --- | --- |
| 分類 | 說明 |
| 意外 (accidental) | 使用者不小心或錯誤操作系統資源。 |
| 惡意 (malicious) | 惡意行為者（如駭客）故意破壞或入侵系統。 |

## 常見的安全違規類型

|  |  |
| --- | --- |
| **類型** | **說明** |
| **Breach of Confidentiality**（機密性破壞） | 未授權讀取機密資料（例如信用卡、身分資訊、未上映電影）。 |
| **Breach of Integrity**（完整性破壞） | 未授權修改資料（例如源碼遭竄改、嫁禍他人）。 |
| **Breach of Availability**（可用性破壞） | 使資料或系統無法被正常使用（例如網站被毀損、刪除資料）。 |
| **Theft of Service**（服務竊取） | 未經授權使用系統資源（例如駭客建非法 FTP server）。 |
| **Denial of Service (DoS)**（阻斷服務攻擊） | 阻止正常用戶使用服務，可能為意外也可能惡意。 |

# 程式威脅(Program Threats)

系統運作主要依賴程式（process）與核心（kernel）。因此，駭客通常的目標是：讓程式被惡意操控或執行異常行為，藉此達成入侵或破壞。

## Malware（惡意軟體）

Malware = Malicious Software，是指設計來破壞或入侵系統的軟體。

Least Privilege（最小權限原則）：每個程式或使用者應只擁有「完成任務所需的最小權限」，以降低被濫用的風險。

Table 1：常見惡意軟體類型

|  |  |
| --- | --- |
| 種類 | **說明** |
| Trojan Horse（木馬程式） | 表面上是合法應用（如手電筒App），暗中執行惡意功能（如竊取資料）。 |
| Trojan Mule（木馬騙子） | 偽裝成登入畫面，騙取密碼。用戶輸入密碼 → 顯示錯誤 → 實際是密碼已被盜。 |
| Spyware（間諜程式） | 偷偷記錄用戶行為、回傳資訊（如偷開相機、記錄鍵盤），常伴隨免費軟體安裝。 |
| Ransomware（勒索軟體） | 加密使用者檔案，要求付款換取解密金鑰。即使付款也不保證可取回資料。 |
| Trap Door（後門程式） | 程式開發者在系統中預留祕密入口，例如輸入某密碼就能繞過驗證。 |
| Logic Bomb（邏輯炸彈） | 程式在特定條件下觸發後門（如「被解僱後」自動刪除公司資料）。 |

## 程式碼注入(Code Injection)

程式碼注入(Code Injection)是指利用程式漏洞，將攻擊程式碼注入原本應該執行的程式中，造成控制權轉移。主要依靠C/C++ 等語言常見的錯誤記憶體操作，如：

* 沒有限制長度的輸入（如 strcpy()）
* 錯誤指標運算
* 未檢查邊界

// 經典案例：Buffer Overflow（緩衝區溢位）

char buffer[10];

strcpy(buffer, argv[1]); // 如果 argv[1] > 10 bytes → 溢位

// 三種可能後果：

// - 小範圍溢位：影響不到其他資料 → 無影響。

// - 中度溢位：破壞其他變數 → 邏輯錯誤、閃退。

// - 高度溢位：覆蓋 return address → 可改變程式流程，執行駭客提供的程式碼（shellcode）。

## 病毒與蠕蟲(Viruses and Worms)

* 病毒 (Virus)：程式碼片段寄生於正常程式中，需要使用者執行才會傳播。
* 蠕蟲 (Worm)：自我複製、透過網路散播，不需使用者介入。

# 系統與網路威脅（System and Network Threats）

程式威脅本身已構成風險，當系統連上網路後，風險會倍增，因為攻擊者可以從全球任何地方發動攻擊。越開放的系統 → 攻擊面越大（Attack Surface）

## Zombie 系統（殭屍電腦）

被駭入後依然看起來正常運作，但背後被駭客遠端控制常被用來：

* 發動 DoS/DDoS
* 中繼垃圾郵件

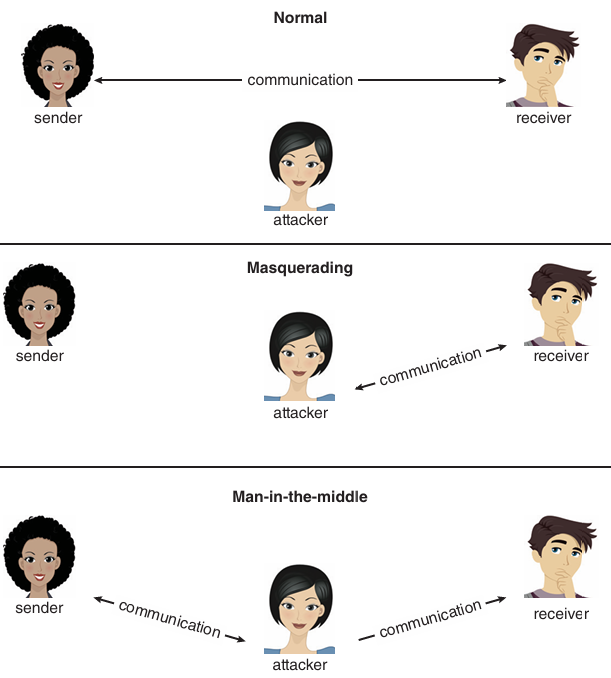
## WiFi & 寬頻問題

* WiFi 匿名接入 + WarDriving（尋找未加密WiFi） → 攻擊者容易偽裝身分。
* 家用或公共設備常被忽視 → 成為弱點。

## 攻擊網路流量（Attacking Network Traffic）

|  |  |
| --- | --- |
| 類型 | 說明 |
| Sniffing（窺聽） | 攔截封包內容，竊取機密資訊（如帳密）。 |
| Spoofing（偽裝） | 冒充合法主體發送資料，造成誤信任。 |
| Man-in-the-Middle（中間人） | 攔截雙方通訊，扮演雙邊角色並可能竄改資料。 |

Figure 1：Standard security attacks



## 阻斷服務攻擊（Denial of Service, DoS）

DoS 攻擊的目的不是竊取資料，而是讓服務癱瘓、合法使用者無法使用系統。可以分為：

* 資源耗盡型：使用大量 CPU/記憶體，如開啟無限視窗的 Java applet。
* 網路癱瘓型：攻擊封包癱瘓網站，例如洪水式流量癱瘓伺服器。

## 分散式阻斷服務攻擊(DDoS)

來自 多個來源（zombies）同時攻擊目標。難以追蹤攻擊來源。常用來勒索：「付錢否則不停攻擊你」。