第五章：關注網絡安全

第一節：設計流動支付的解決方案

在開發及設計流動支付解決方案，需要了解其技術及框架：

- 提供以近場通訊技術 (NFC)[1] 進行保密、無縫和單次接觸的支付服務
- 透過授權服務管理平台，提供跨平台流動繳費服務，採用最高安全標準加密保護
- 適用於不同的智能手機型號，電話網絡供應商和信用卡
- 運用不同的保安元素如外置配件或多功能智能卡 (SIM) 等
- 掌握前台及後台功能
- 開發流動應用程式及硬件
- 掌握網絡服務，包括流動通訊服務及通訊網絡基礎建設
- 掌握金融及交易安全性的架設
- 掌握相關開發平台及工具

[1] *NFC（Near Field Communication），可以讓設備透過近距離的非接觸式技術，進行數據交換，如：手機支付*

如何建立安全的應用系統？

要建立安全的應用系統，先了解此應用系統所面對的威脅。Threat Modelling(威脅模型分析) 的過程可協助您確定在整體應用程式方案上的威脅、攻擊、漏洞與抵禦措施。

步驟

那麼企業應該如何制定網站安全整體規劃方案？商家應先了解其公司電子商務網站當中潛在的風險。

1. 潛在風險：

- 虛假買賣： 通常會造成你因信用卡拒付 (Chargebacks) 的問題而損失收入
- 詐騙網站：有人設立看似你公司官方網站的詐騙網站
- 數據盜竊：入侵者也許偷取你的客戶資料，如信用卡號碼
- 入侵者攻擊：入侵者的攻擊也許會造成網站功能的篡改或損壞

近年發生不少網站被入侵的事件，導致客戶信用卡資料被盜，正在營運網店的你該如何保障客戶的個人資料？

1. 採用加密法 (encryption) 傳輸敏感性的個人資料 [1]

如網店需在網上傳輸的個人資料進行「損害測試」，店主必須確保其保安措施。例如：客戶需提供信用咭或銀行戶口資料；在傳輸有關個人資料時，應採用加密資料傳輸方式 * 在網上傳輸該等資料。

* 其中例子：「對稱 (Symmetric)」，使用對稱加密的優點是使用同一把秘密金鑰所以運算速度較快，如果使用足夠長度的金鑰則難以破解安全性高；缺點則是需要有一個安全機制分別將秘密金鑰安全的傳送到傳送端與接收端，只能提供機密性，無法提供不可否認性。

[1] *https://blog.trendmicro.com.tw/?p=17075*

2. SSL[2]

由 HTTP 轉到 HTTPS，這個「S」就是代表著「secure」，表示網站有多加了一層保護。SSL 網絡安全憑證 (Secure Socket Layer)，是網頁伺服器和瀏覽器之間以加密、解密方式溝通的安全技術標準，亦可以被視為是一層保護罩。SSL 最常用於 Web 瀏覽器與網頁伺服器間，以建立安全通訊通道。此外，Google 自 2017 年 1 月開始加強打擊非加密網站，當 Chrome 用家瀏覽到一些低安全性的 HTTP 網站時，網址將出現「不安全」的警告標示。此標示在提醒用家，他們所輸入的資料有可能會被遭竊。

SSL 提供以下主要服務：

i. 認證使用者和伺服器，確保資料傳送到到正確的客戶機和伺服器
ii. 加密資料以防止資料中途被竊取
iii. 維護資料的完整性，確保資料在傳輸過程中不被改變

3. CAPTCHA[3]

全自動區分電腦和人類的公開圖靈測試，俗稱驗證碼。

Completely Automated Public Turing test to tell Computers and Humans Apart，簡稱 CAPTCHA，是一種區分用戶是電腦或人的公共全自動程式。在 CAPTCHA 測試中，伺服器的電腦會自動生成一個問題由用戶來解答。這個問題可以由電腦提出並判斷，問題必須只有人類才能解答。由於電腦無法解答 CAPTCHA 的問題，所以回答出問題的用戶就會被認為是人類。

[2] https://serverguy.com/security/google-forcing-ssl-certificate-websites/
[3] https://www.lifewire.com/what-is-captcha-3486183

4. 防火牆

一種軟件或硬件工具，用於保護電腦以避免來自互聯網攻擊者的威脅

防火牆的種類：

- 軟件防火牆 (安裝在電腦之中)
- 硬件防火牆 (與你的系統及網路上的路由器整合)

5. 其他安全保護措施：[5]

- 使用網路入侵偵測系統，監控網路流量。確認未經授權而企圖上載或更改、網頁資訊或蓄意破壞者
- 裝設掃毒軟體並定期掃毒，提供更安全的網頁瀏覽環境予使用者。
- 不定期摹擬駭客攻擊，演練發生安全事件時的系統回復程序，並提供適當的安全防禦等級
- 每日進行備份作業

市面上的防毒軟件：

Avira avast AVG Norton by Symantec eset NOD32 ANTIVIRUS

[5] *https://www.infosec.gov.hk/tc_chi/virus/antivirus.html*