Module 11:網站安全架構
Web Security

學習目的

- 本章將介紹現今WEB網站安全性的隱憂、作為身份鑑別的SSL和TLS協定、經由SSL協定發展出的HTTPS傳輸協定，以及對目前建置WEB之工具的弱點來做解說。
- 本章利用五個小節介紹
  (1) WEB安全需求：包括面臨的威脅及對應的安全機制
  (2) SSL和TLS：SSL和TLS協定的演進及架構
  (3) Https：Https通訊安全
  (4) 建置WEB之工具的弱點：包括WEB資訊系統的弱點及WEB伺服器的組態設定
  (5)專案實作：實際建置一以https連結的Web Server
- 建議11-1~11-4使用三個鐘點教授，專題實作可作為學生homework。

Module 11:大綱

Module 11-1: WEB安全需求(*)

Module 11-2: SSL和TLS(**)

Module 11-3: Https(*)

Module 11-4:建置WEB之工具的弱點(*)

Module 11-5:專案實作(**)

u2

* 初級(basic):基礎性教材內容
**中級(moderate):教師依據學生的吸收情況，選擇性介紹本節的內容
***高級(advanced):適用於深入研究的內容

u2

user 2007/2/14
* 初級(basic):基礎性教材

**中級(moderate):教師依據學生的吸收情況，選擇性介紹本節的內容

***高級(moderate):適用於深入研究的內容
user, 2007/2/14

Module 11-1: WEB安全需求

WEB安全需求

- 網站的安全性面臨很多威脅
  - 完整性(integrity)
  - 機密性(confidentiality)
  - 阻斷服務(denial of service)
  - 身份鑑別(authentication)

完整性(integrity)

- 網路傳輸過程中，資訊傳輸到伺服端或客戶端之過程裡，必需確保資訊未經未授權之第三者竄改。
- 只有通過身份鑑別，擁有權限的使用者才能修改資訊的內容。
- 一般可藉由傳輸資訊中的數位簽章來判定資訊是否遭到竄改。

機密性(confidentiality)

- 安全的資訊傳輸必須確保傳輸過程中資訊的機密性。
- 傳輸的資訊必須先經加密後才能傳輸，並且只有指定的接受方有能力解開。

阻斷服務(denial of service)

- 阻斷服務是網際網路上常見的攻擊手法之一。
- 經由對遠端系統進行攻擊，藉此達成使遠端系統無法提供正常服務或是使其系統服務品質降低。
- 常見的攻擊方式有 ICMP Flooding、SYN Flooding 及 Mail Bomb。

身份鑑別(authentication)

- 證明個人或應用程式於傳輸過程中的身份合法性。
- 經由身份鑑別可以確認雙方的合法性。
- 目前全世界約有90%的身份鑑別機制是以Password為主，但其為最不安全的認證方式。
- PKI (Public Key Infrastructure,公開金鑰基礎建設)技術可讓身份鑑別機制更為完善、可靠。

	威脅	結果	對策
完整性	● 竄改使用者資料 ● 具特洛依木馬的瀏覽器 ● 竄改記憶體 ● 竄改傳輸中的訊息	● 遺失資訊 ● 危及機器 ● 易遭受其它威脅	使用密碼學上的總和檢查碼
機密性	● 在網路上竊聽 ● 偷取伺服端資訊 ● 偷取客戶端資料 ● 得知網路的配置 ● 得知與伺服端溝通的客戶端	● 遺失資訊 ● 喪失隱密性	加密，網路代理伺服端
阻斷服務	● 刪除使用者子程序(threads) ● 用偽造的請求訊息來塞爆機器 ● 填滿磁碟或記憶體 ● 利用攻擊DNS來孤立機器	● 系統分裂 ● 困擾使用者 ● 阻止使用者完成工作	目前尚無適當的預防對策
身份鑑別	● 假扮合法的使用者 ● 偽造資料	● 扭曲使用者 ● 相信錯誤的資料是正確的	密碼學技術

表12-1 網站安全性的各種威脅及後果

WEB安全需求

- 必須在網路協定(TCP/IP)的架構中加上安全機制
  - 網路層(network level)
    - IP security
  - 傳輸層(transport level)
    - 安全通道層(Secure Sockets Level, SSL)
    - 傳輸層的安全標準(Transport Layer Security, TLS)
  - 應用層(application level)
    - 安全電子交易 (Secure Electronic Transaction, SET)
    - Pretty Good Privacy (PGP)
    - S/MIME

Security facilities in the TCP/IP protocol stack

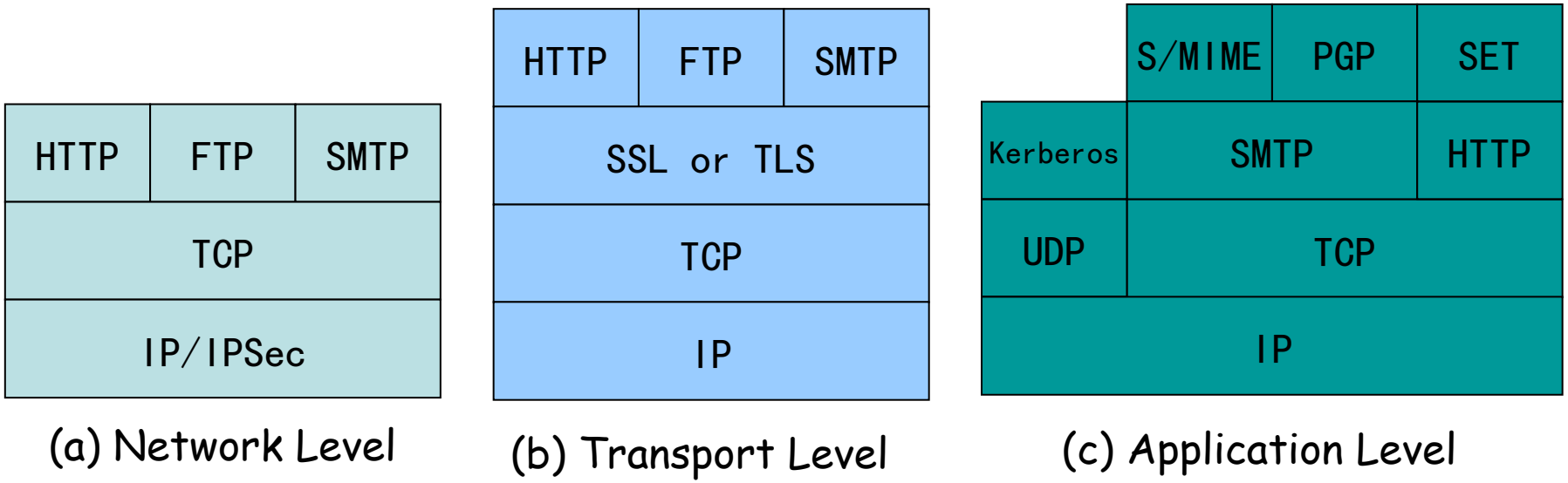


圖12-1 各種安全功能協定在TCP/IP的相關位置

Module 11-2: SSL和TLS

SSL (Secure Socket Layer)演進

- SSL V1.0
  - 於1994年以前由Netscape所設計
  - 只能在Netscape公司內部使用
- SSL V2.0
  - 於1994年11月由Netscape所發表
  - 可經由安裝提供Netscape Navigator Version 1.0及2.0的用戶端使用
  - 存在一些弱點
- SSL V3.0
  - 於1996年11月由Netscape及Paul Kocher 所設計
  - 修正 V2.0 的弱點
  - 做為其後網際安全協定TLS (Transport Layer Security)的基礎

SSL (安全通道層)

- SSL為定義在傳輸層上的安全傳輸協定,利用TCP 來提供可靠的點對點服務。
- SSL是由Netscape公司所開發的,v3.0是接受業界的建議所發展完成。
- SSL v3.1 被IETF的TLS工作小組(working group)接受並改訂為”傳輸層安全標準” (Transport Layer Security, TLS)。

TLS (Transport Layer Security)

- 內容與SSLv3 類似，已被IETF接納為標準 RFC 2246。
- 內容有些許的不同
  - 版本編號(version number)的格式
  - 使用的 HMAC產生訊息鑑別碼(MAC)
  - 更安全的虛擬亂數函數(pseudorandom function)
  - 額外的警告碼(alert codes)
  - 所支援的加密法(cipher suites)不盡相同
  - 認證的協商方式不同
  - 位元的附加(padding)方式不同

SSL架構

- 提供可靠的點對點(end-to-end)安全服務
- Netscape及IE瀏覽器已內建支援SSL
- SSL 是由兩層協定所組成如圖12-2

SSL 架構

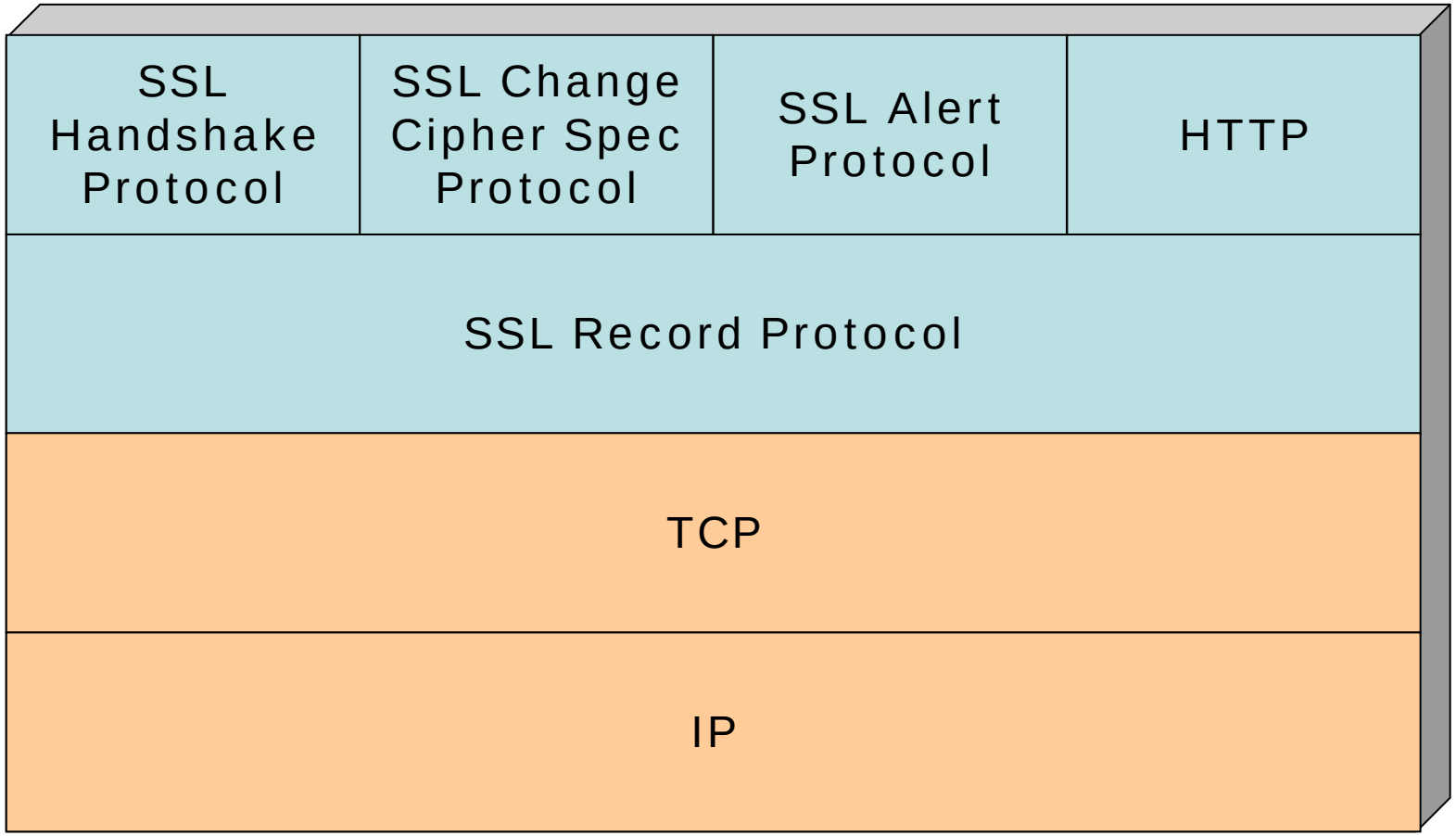


圖12-2 SSL 協定架構

SSL 連線的重要觀念

- **SSL 連線(connection)**
  - 一個暫時的、點對點的通訊連線
  - 每一個 SSL 連線對應至一個會期
- **SSL 會期(session)**
  - 客戶端與伺服端之間的一個連線
  - 透過握手(handshake)協定來產生
  - 定義了一組密碼安全參數供連線使用
  - 一個Session可能由多組 SSL 連線來共用

SSL 協定架構

- SSL 協定架構是由以下四個次協定所組成
  - SSL 記錄協定(record protocol)
  - SSL 密文規格變更協定 (change cipher spec protocol)
  - SSL 警告協定(alert protocol)
  - SSL 握手協定(handshake protocol)

- 其規格詳見圖12-5

SSL 架構介紹(一)
— SSL 記錄協定

- **機密性**
  - 利用對稱式加密法及握手協定達成資訊的秘密共享
  - 可使用IDEA, RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40, RC4-128等加密法
  - 訊息在加密前會先壓縮
- **訊息完整性**
  - 使用 MAC 及共享的秘密金鑰
  - 與 HMAC 類似，但是位元的附加方式不同

SSL Record Protocol Operation

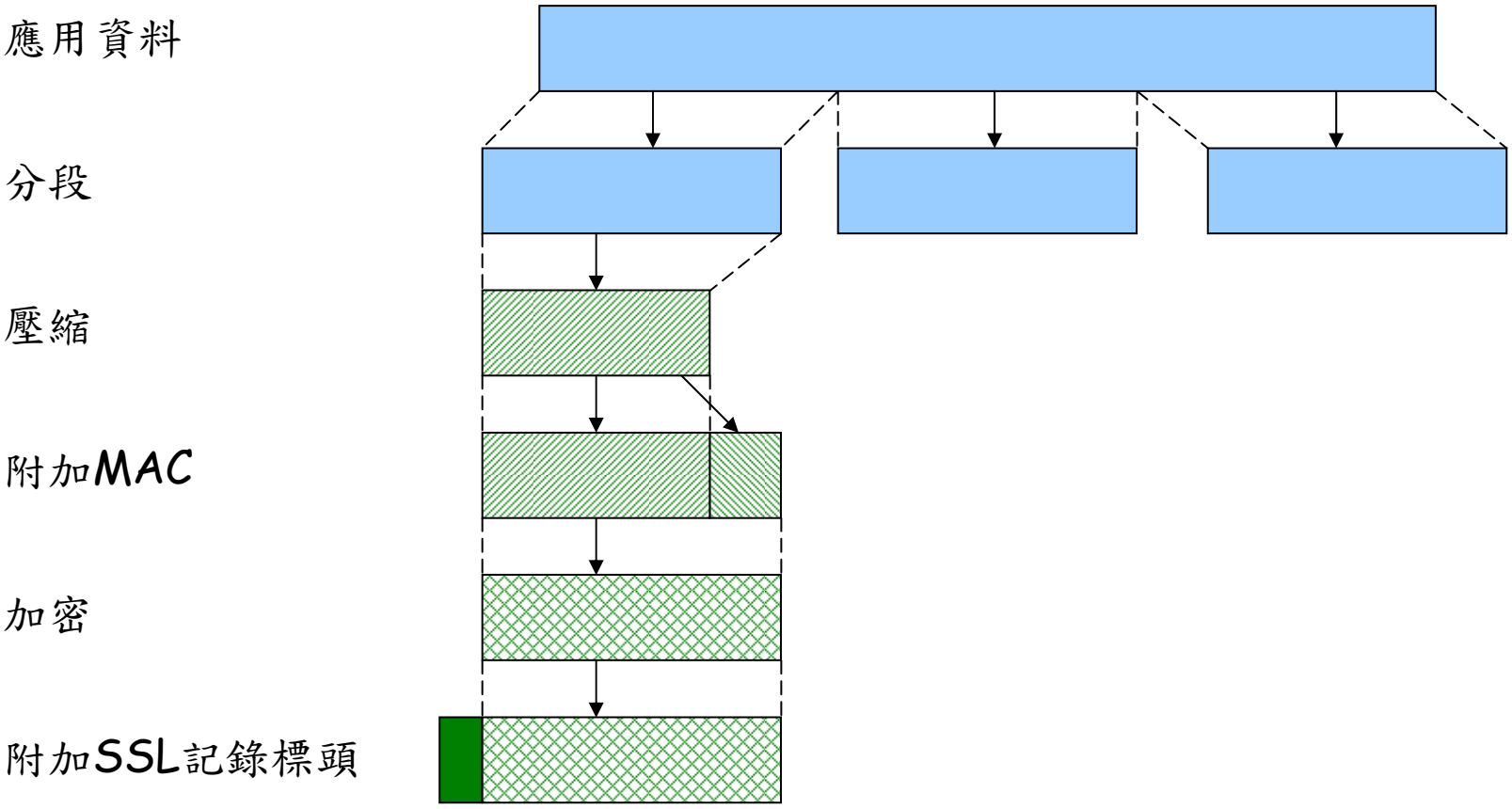


圖12-3 SSL 記錄協定運作

SSL Record Format

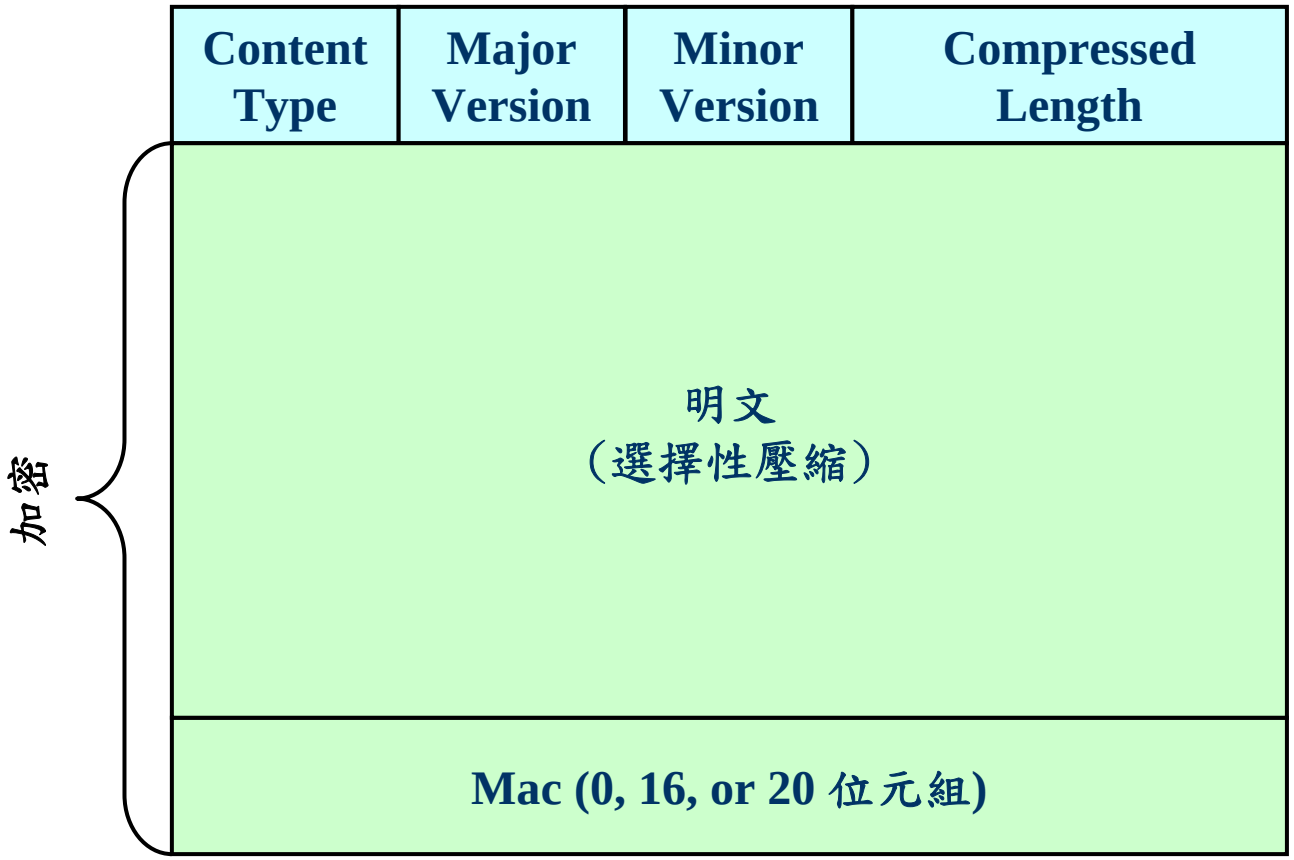


圖12-4 SSL 記錄格式

SSL 架構介紹(二)
— SSL 密文規格變更協定

- 會用到 SSL 記錄層協定的三個協定之一來通知連線雙方必須遵守的規定。
- 協定是由單一訊息所構成。
- 主要目的是提供更新連線雙方所使用的加密方法。

SSL Record Protocol Payload

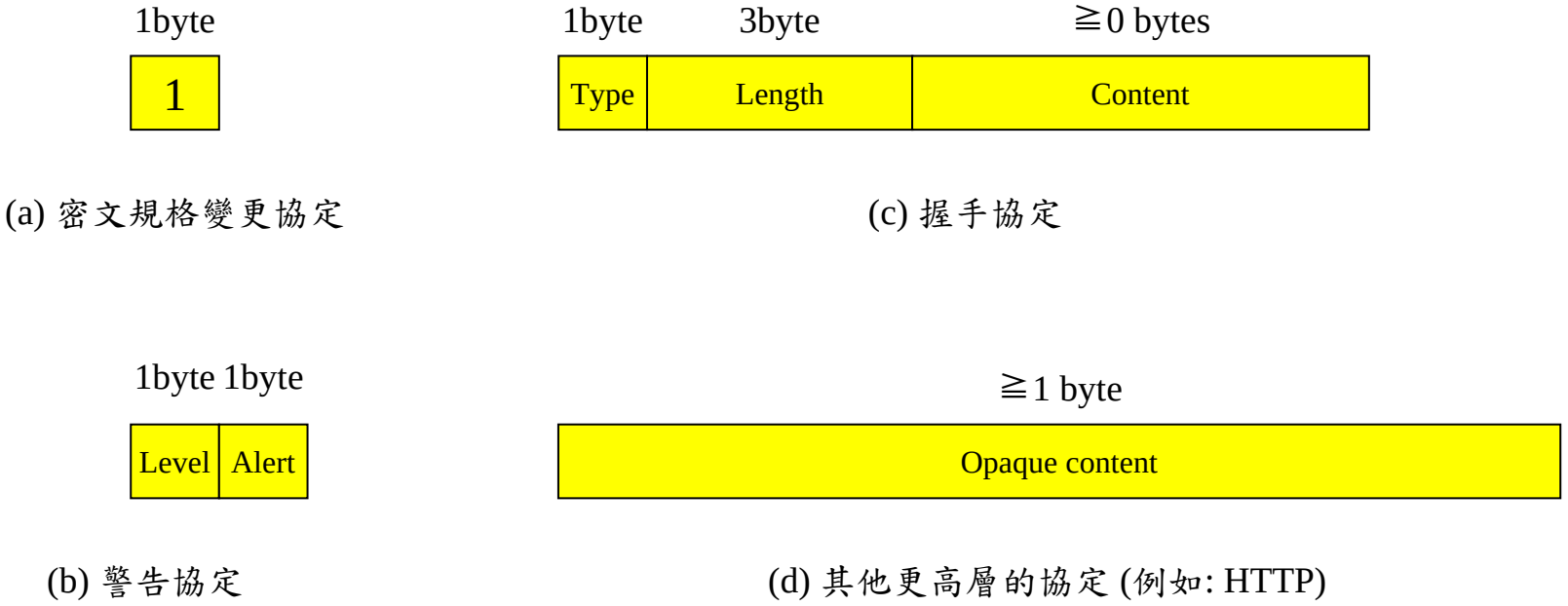


圖12-5 SSL記錄負載

SSL 架構介紹(三)
— SSL 警告協定

- 傳遞與 SSL 相關的警告訊息至另一端，警告訊息包括兩個層級(levels)
  - 嚴重性(fatal)
    - 警告或致命
  - 特定警告(warning)
  - 不預期的訊息、錯誤記錄的 MAC、解壓縮失敗、 握手失敗、非法的參數
    - 關閉通知、無憑證、錯誤的憑證、不支援的憑證、憑證撤銷、憑證逾期、未知的憑證
- 與所有的 SSL 資料一樣都會經過壓縮與加密的處理步驟。

致命警告

- 不預期的訊息(unexpected_message)
  - 一個不正確的訊息
- 錯誤的紀錄的MAC (bad_record_mac)
  - 收到不正確的MAC資料
- 解壓縮失敗(decompression_failure)
  - 解壓縮函數接收到不正確的輸入
- 握手失敗(handshake_failure)
  - 傳輸端無法產生一組合適的傳輸參數
- 非法的參數(illegal_parameter)
  - 一個握手訊息的某項欄位值超出合理的範圍或與其他欄位不一致

其他警告

- 關閉通知(close_notify)
  - 讓接收端知道傳送端不會再送出任何訊息了
- 無憑證(no_certificate)
  - 如果沒有適當的憑證可以送出此訊息來回應一個憑證申請訊息
- 錯誤的憑證(bad_certificate)
  - 接收到的憑證已經毀損
- 不支援的憑證(unsupported_certificate)
  - 並不支援所收到的憑證格式

其他警告

- 憑證撤銷(certificate_revoked)
  - 一個由簽署人所撤銷的憑證
- 憑證逾期(certificate_expired)
  - 一個逾期的憑證
- 未知的憑證(certificate_unknown)
  - 在處理憑證時發生其他未指定的問題，導致無法接受此認證

SSL 架構介紹(四)
—SSL 握手協定

- 讓客戶端與伺服端可以提供(詳見表12-2)：
  - 彼此身份的確認
  - 協商所使用的加密與 MAC 演算法
  - 協商加密時所使用的金鑰

- 運用一系列的握手協定訊息所組成，交換過程以下包括四個階段(phases)(詳見圖12-6)
  - 建立安全機制
  - 伺服端確認與金鑰交換
  - 客戶端確認與金鑰交換
  - 完成

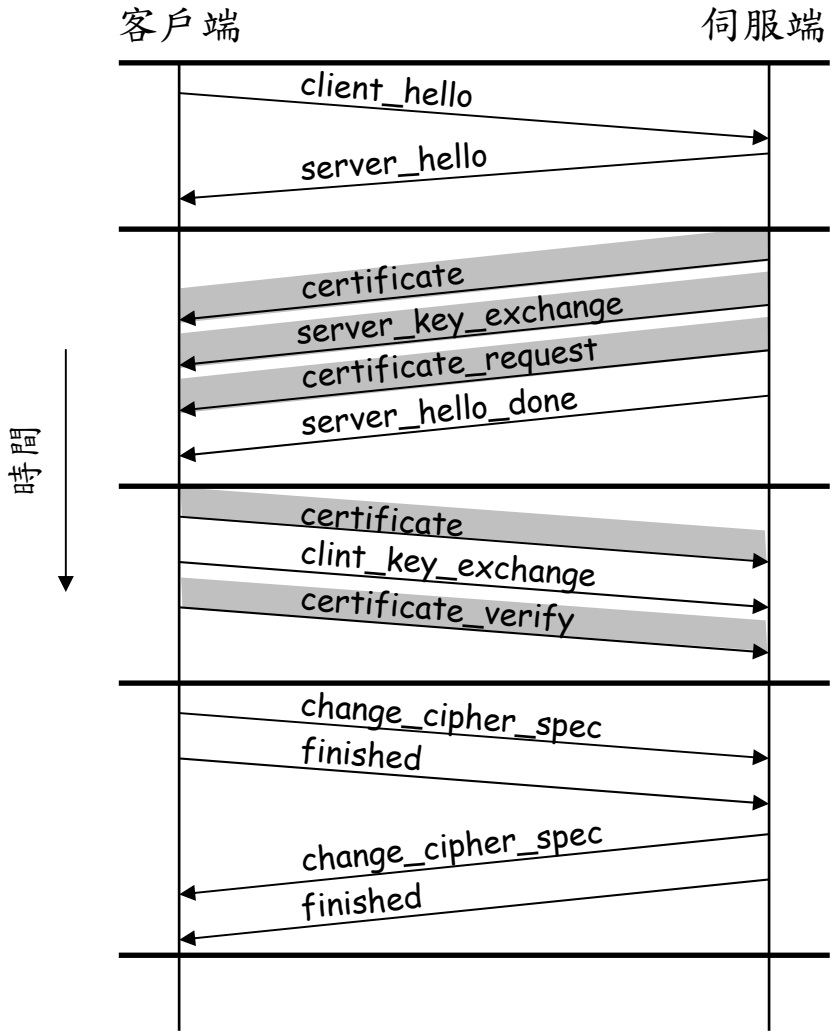
SSL 握手協定訊息類別

訊息類型	參數
hello_request	無
client_hello	版本、亂數、通訊編號、加密套件、壓縮方法
server_hello	版本、亂數、通訊編號、加密套件、壓縮方法
certificate	一連串的X.509v3憑證
server_key_exchange	參數、簽章
certificate_request	類型、認證中心
server_done	無
certificate_verify	簽章
client_key_exchange	參數、簽章
finished	雜湊值

表12-2 SSL Handshake 協定訊息類型

返回

SSL 握手協定(**)



第一階段
建立安全機制，包括協定版本、通訊編號、加密套件、壓縮方法、以及起始亂數。

第二階段
伺服器端送出憑證、金鑰交換訊息、以及申請憑證訊息。伺服器端再送出hello訊息之後停止。

第三階段
如果要求服務的話，客戶端會送出憑證、金鑰交換訊息。客戶端也可能送出憑證驗證訊息。

第四階段
變更加密套件，然後完成握手協定。

請注意，陰影部份的訊息傳送是選擇性的、或是視情況才需要的，並非一定要傳送。

圖12-6 Handshake 協定的流程

返回

Module 11-3: Https

Https通訊安全

- 電子商務應用的通訊安全問題，涵蓋了用戶端電腦系統和電子商務伺服器之間傳輸的資訊安全問題。
- 電子商務通訊安全包含伺服器傳送給用戶端的機密資訊，加密是這種問題實際可行的解決方案。
- 大部份標準網頁瀏覽器(IE、Netscape)都具有流量加密／解密的能力。
- 預設的解決方案就是利用HTTPS取代HTTP。

Https通訊安全

- 在使用HTTPS的時候，用戶端和伺服端之間會建立安全基座層（Secure Socket Layer，SSL）連線。
- 所有利用SSL傳送的流量，都會經過加／解密的處理。
- 從資訊離開用戶端電腦之後一直到抵達Web伺服器為止，HTTPS的加密都會保護資訊流量。
- 在公眾體認到某些人可透過Internet取得信用卡號碼的危險之後，HTTPS的使用已經變成網路交易的基本需求。
- HTTPS的連線阜(port)為443 。

Module 11-4:建置WEB之工具的弱點

WEB資訊系統的弱點

- 網站(Web) 已廣泛地使用在商業、政府以及個人的應用，隨電子商務的普及，網站的能見度也大為提高(very visible)，且已逐漸被作為企業產品對外展示的窗口。
- 網站伺服器具備容易安裝、架設與管理。
- 網站伺服器所安裝的複雜的軟體卻隱藏多項安全的漏動(security flaws)。
- 通常使用者並不知道網站伺服器相關弱點所帶來的風險(risks)。

WEB資訊系統的弱點

- 網站伺服器原有的弱點可查詢各cert網站相關資訊，下載系統的修補(patches)以強化抵抗惡意軟體及駭客的攻擊。
- WEB系統的部份弱點是由於使用者不當的組態設定所造成；良好的組態設定，系統可以達成一定的安全程度，但是如果設定不當可能會產生許多安全漏洞。

WEB資訊系統的弱點

- Web伺服器組態設定
  - 應該依據製造商的建議，適當地修補、更新伺服器軟體。
  - 絕對不要使用管理者或root帳號執行Web伺服器。
  - 如果是root帳號執行Web網頁伺服器，那麼攻擊者就會擁有root帳號的特權。

WEB資訊系統的弱點

- Web伺服器組態設定
  - 應該要建立一個新的帳號，然後使用新的帳號來執行Web伺服器。
  - 管理者必須替每個Web伺服器定義根目錄(root directory)。
  - 目錄是用來告訴Web伺服器，網頁位置和script及使用權限，並限制瀏覽器只能存取Web伺服器指定的檔案目錄。

WEB資訊系統的弱點

- Web伺服器組態設定
  - 不要將Web伺服器的根目錄設定成系統的根目錄，目錄裡面也不能含有作業系統重要的安全檔案和組態設定。
  - 大部分Web伺服器都可以執行共用閘道器介面指令(CGI script ， Common Gateway Interface script) 以發展Web伺服器的應用系統。
  - 某些預設的CGI script含有非常嚴重的弱點，這些弱點允許攻擊者存取系統的檔案或系統本身。

WEB資訊系統的弱點

- Web伺服器組態設定
  - 任何Web伺服器都含有script，只要網站不需要用到的就應該全部移除，才能防止攻擊者利用這些script存取系統。
  - 公眾也不應該看到CGI script的內容。
  - 如果瀏覽器沒有指定檔案時，Web伺服器就「不應該提供目錄的清單」。
  - 如果瀏覽器指定CGI或Perl script，Web伺服器應該設定成「執行」，而不是顯示程式碼的內容。

WEB資訊系統的弱點

- Web伺服器組態設定
  - Web伺服器在加入營運之前，作業系統應該進行已知弱點的掃描。
  - 要先確認Web伺服器的弱點掃描功能也包含在內。
  - 主機在加入營運之後也應該定期掃描。

※未來發展趨勢與研發議題

- 以WS-Security標準強化Web Services的SOAP資訊，包含資料加密、簽章、驗章。
- 制定具安全性網路應用程式的檢核(checklist)標準及推廣。

習題

習題一

- 請概要說明SSL是由哪些協定所組成？

習題二

- 請簡述SSL連線和SSL會期有何差異？

習題三

- SSL記錄協定提供哪些服務？

習題四

- SSL記錄協定的運作流程為何 ？

習題五

- 試以圖解Handshake協定的流程，並簡要的說明各階段的用意。

Module 11-5: 專案實作

專案目的

- 應用Windows Server 2000 系統平台。
- 建立 Certificate Services 元件。
- 經由本專案裡各步驟的解說與實作，建構出以Https協定連結的Web伺服器。

專案摘要

- 本專案將以下述七步驟進行實作
  - 建置CA
  - 製作憑證要求
  - 向CA要求伺服器憑證
  - CA管理者核發伺服器認證
  - 下載憑證檔案
  - 安裝伺服器憑證
  - 測試安全連結
- Certificate Services 元件只有Server版本才有支援，實作時務必以Windows 2000 Server 或 Advance Server版本實作。

參考文獻

1. 2004 CSI/FBI Computer Crime and Security Survey, www.usdoj.gov/criminal/cybercrime/CSI_FBI.htm
2. S. William, Cryptography and Network Security: Principles and Practice. Prentice Hall, Second Edition, 1999; pp. 441-473.
3. S. Garfinkel, and G. Spafford, Web security & commerce, O'Reilly and Associates: Cambridge MA, 1997.
4. E. Maiwald, Fundamentals of Network Security, McGraw-Hill Technology Education, 2004.

參考文獻

5. M. Naedele, “Standards for XML and web services security,” Computer, 36(4), pp. 96–98, Apr 2003.
6. A. Rubin, D. Geer, and M. Ranum, Web security sourcebook, New York, Wiley, 1997.
7. K. Bhargavan, R. Corin, C. Fournet, A. D. Gordon, “Secure sessions for web services,” Proceedings of the 2004 workshop on secure web service SWS '04, Oct. 2004.