計概補充講義－模擬考

一、 FSB：前端匯流排，First Side Bus

二、 安全付款系統

(一) S-HTTP〈安全性超文件傳輸協定〉

S-HTTP 是一以文件為基礎的安全協定，是一般 HTTP 的延伸。S-HTTP 所提供的安全功能是針對 HTTP 協定中傳輸的文件功能提供直接的安全保護機制，使超文件檔案中的每一個連結都能內含安全性的資料，只需修改原有的 HTML 文件就可以馬上應用，甚為方便。S-HTTP 允許網路客戶端與伺服器端各自進驗證功能，並且協商出一套共用的加密演算法，使其不需受限於任何特別的演算法。

S-HTTP 的安全保護機制可以分為下列三項：

1. 私密性
2. 完整性
3. 身份驗證及不可否認性

(二) SSL〈安全線上編碼協定〉

SSL 是一項由網景公司所發展出來的網路安全傳輸協定。由於網景公司所發展的瀏覽器與伺服器十分風行，SSL 已成為最為廣泛使用的網路安全協定。在網路輸協定層級中，SSL 層屬於 TCP 與應用程式層中間的一個層級，它提供網路傳遞資料的安全保護，避免資料在傳輸過程中被截取或竄改，其在網路協定層級中的位置較為低階。由於 SSL 是位於傳輸層之下的通訊協定，高層網路應用程式都屬於 SSL 的範圍，可透過 SSL 達到下列的安全機能：

1. 私密性
2. 完整性
3. 身份認證性

(三) SSL 與 S-HTTP 的比較

1. 應用層級的不同

- S-HTTP 的安全機制如力密或簽章都是在網路七層架構的上層—應用層或交談層完成之後再將加密的訊息透過運輸層等底層網路結構完成傳送，未對傳輸的網路住行保護。
- SSL 是將訊息以原本格式傳到中層如運輸層及網路層，然後才對訊息進行加密等安全處理，並透過事先協商的安全傳輸通路進行傳送。

2. SSL 應用範圍較為廣泛

- S-HTTP 主是針對 HTTP 元件進行安全性改進。
- SSL 的應用包含了 HTTP 及其以外的檔案傳送 FTP、遠端登錄、電子郵件等應用協定，應用層面較為廣泛。

3. 設計原理不同

- S-HTTP 是一種以保護文件為主的協定，直接在發送端將文件進行加密及簽章等安全處理，基本上不管傳輸的網路通道是否安全。
- SSL 則是以提供一個安全的傳輸路徑為主，只要協定中的安全機制不被破壞，基本上在此路徑上傳送資料都是安全的。

4. 不可否認性

- S-HTTP 中則定義了數位簽章的機制，因此較 SSL 增加了不可否認性的明顯定義。
- SSL 中並沒有明確定義數位簽章的安全機制，因此並沒有提供不可否認 性的保護。

(四) SSL 與 SET

SSL 是由 Netscape 首先發表的網路資料安全傳輸協定。SSL 是利用公開金鑰的加密技術(RSA)來做為用戶端與主機端在傳送機密資料時的加密通訊協定。目前，SSL 技術已被大部份的 Web Server 及 Browser 廣泛使用。

SET 是安全電子交易(Secure Electronic Transcation)的簡寫，用來保護消費者在開放型網路(如 Internet)持卡付款交易安全的標準。由 VISA、asterCard、IBM、Microsoft、Netscape、GTE、VeriSign、SAIC、Terisa 等公司聯合制訂，運用 RSA 資料安全的公開鑰匙加密技術，保護交易資料之安全及隱密性。

SET 的架構是由幾個成員所共同組合起來的。分別是 Electronic Wallet(電子錢包)，Merchant Server(商店端伺服機)，Payment Gateway(付款轉接站)，和 Certification Authority(認證中心)。而運用這四個成員，即可構成於 Internet 上符合 SET 標準的信用卡授權交易。SET 1.0 版於 1997/6 正式問世。時至今日，SET 已成為國際上所公認在 Internet 電子商業交易的安全標準。

數位簽章(Digital Signature)是實際簽章的數位電子表示法，用來防止資料內容在傳輸時被篡改或被冒名傳送假資料。數位簽章與傳送者及傳送內容完全相關，傳送者不可否認，他人也無法偽造，並可由第三者認證。

✓ **SET 優點**

(1) 每個人必須拿身份證明的文件到認證中心取得認證。

(2) 購物網站無法取得消費者的信用卡資料，不用擔心被盜刷的問題。

(3) 付款銀行看不到消費者的購物內容，保障了消費者的隱私權。

× **SET 缺點：**

(1) 需向認證中心取得認證，手續較麻煩。

✓ **SSL 優點：**

(1) 是目前線上交易最普及使用的安全協定。

(2) 不需事先取得認證，使用較方便。

× **SSL 缺點：**

(1) 消費者無法確認電子商務網站是否是正派、穩當的在經營，店家也無法知道消費者的真實身份，也無法防範盜刷的問題。

(2) 購物網站仍可取得消費者的信用卡資料，若保管不當，亦可能讓資料外洩被盜刷。

三、 XML VS HTML VS SGML

XML 全稱 EXtensible Markup Language，翻譯為可擴展標記語言，可擴展標記語言或可延伸標示語言，是一種標記語言。標記指電腦所能理解的資訊符號，通過此種標記，電腦之間可以處理包含各種資訊的文章等。目前可應用在各種領域，如數學、商業、醫學等等，各種領域透過自行定義的標記可定義與交換文件資料。

如何定義這些標記，既可以選擇國際通用的標記語言，比如說 HTML，也可以使用像 XML 這樣由相關人士自由決定的標記語言，這就是語言的可擴展性。XML 是從標準通用標記語言（SGML, Standard Generalized Markup Language）中簡化修改出來的。

超文件標示語言（HyperText Markup Language, HTML）提供一個精簡卻強而有力的文件建構機能，使你輕易地設計出多采多姿的超媒體文件（Hypermedia document）作品（取決於瀏覽器對 HTML 標籤之展現能力），並透過 HTTP(HyperText Transfer Protocl)網路通訊協定，能在全球資訊網(World Wide Web,WWW)架構上作跨平台的流通。目前您只要擁有諸如 mosaic、netscape、cello 等 WWW 的瀏覽器（Brower），就能輕易藉 Internet 感受漫遊全球多媒體資訊網之樂趣。

◆ **兩者的差異性：**

1. XML 設計理念是將資料與格式分開，不像以前撰寫 HTML 那樣，將要顯示的資料和格式寫在一起。

2. XML 是用來結構化與描述資料用的；HTML 則是用來格式化資料用的。

簡單的說，XML 是一套原則，可讓各行各業自行定義如 HTML 般的標注語，方便資料存取、處理、交換，轉換等。有了 XML,各式各樣的系統中的資料就可以輕易相互轉換,整合,而這對上下游合作廠商來說是個好消息,可以大大減少訊息/資料傳遞所需開發的人力。

以前不同的系統如採用不同的資料庫,當需要相互傳遞整合資料時,通常會耗費很多的人力,設計不同資料庫間的轉換介面,而現在有了 XML,這樣的工作將會更容易,甚至像下一版的 SQL 2005,完全支援 XML,直接可以在資料庫中就存入 XML 文件。