電子商務安全
Secure Electronic Commerce

行動商務安全
(Mobile Commerce Security)

992SEC13
TGMXM0A
Fri. 6,7,8 (13:10-16:00) L526

Min-Yuh Day
戴敏育
Assistant Professor
專任助理教授
Dept. of Information Management, Tamkang University
淡江大學 資訊管理學系

http://mail.im.tku.edu.tw/~myday/
2011-05-27

Syllabus

週次	月／日	內容（Subject/Topics
1	100/02/18	電子商務安全課程簡介 (Course Orientation for Secure Electronic Commerce)
2	100/02/25	電子商務概論 (Introduction to E-Commerce)
3	100/03/04	電子市集 (E-Marketplaces)
4	100/03/11	電子商務環境下之零售：產品與服務 (Retailing in Electronic Commerce: Products and Services)
5	100/03/18	網路消費者行為、市場研究與廣告 (Online Consumer Behavior, Market Research, and Advertisement)
6	100/03/25	電子商務 B2B、B2C、C2C (B2B, B2C, C2C E-Commerce)
7	100/04/01	Web 2.0, Social Network, Social Media
8	100/04/08	教學行政觀摩日
9	100/04/15	行動運算與行動商務 (Mobile Computing and Commerce)
10	100/04/22	期中考試週

Syllabus (cont.)

週次	月／日	內容（Subject/Topics
11	100/04/29	電子商務安全 (E-Commerce Security)
12	100/05/06	數位憑證 (Digital Certificate) [Module 4]
13	100/05/13	網路與網站安全 (Network and Website Security) [Module 5]
14	100/05/20	交易安全、系統安全、IC卡安全、電子付款 (Transaction Security, System Security, IC Card Security, Electronic Commerce Payment Systems) [Module 6, 7, 8, 9]
15	100/05/27	行動商務安全 (Mobile Commerce Security) [Module 12]
16	100/06/03	電子金融安全控管機制 (E-Finance Security Control Mechanisms)
17	100/06/10	營運安全管理 (Operation Security Management)
18	100/06/17	期末考試週

教育部顧問室編輯 “電子商務安全”教材

委辦單位：教育部顧問室資通安全聯盟

執行單位：國立台灣科技大學管理學院

Module 12:
行動商務安全

學習目的

- 本模組首先從行動商務的簡介開始，說明在行動商務中的安全需求以及各種現行保護行動商務安全的機制，並介紹幾種目前行動付款的方法，最後探討行動商務安全的管理。
- 本章利用五個小節介紹
  1. 行動商務概述: 定義行動商務，並簡介行動商務所使用之技術以及行動商務的應用
  2. 行動商務安全需求: 說明四大安全需求，包含鑑別、機密性、完整性和不可否認性
  3. 行動商務安全機制: 介紹包含在行動通訊網路、無線區域網路以及無線個人網路所使用的安全機制
  4. 行動付款機制: 說明行動付款機制的架構與流程，並且介紹數種現行使用的行動付款技術
  5. 行動商務安全管理:首先介紹無線通訊技術中可能面臨之安全威脅並且說明如何制定對應的安全政策

Module 14:行動商務安全

- Module 12-1: 行動商務概述
- Module 12-2: 行動商務安全需求
- Module 12-3: 行動商務安全機制
- Module 12-4: 行動付款機制
- Module 12-5: 行動商務安全管理

Module 12-1:
行動商務概述

Module 12-1-1: 行動商務之定義

- 透過無線網際網路所進行的商業行為稱之為『行動商務』（黃貝玲, 民 90）
- “Any transaction with a monetary value that is conducted via a mobile telecommunications network”, (Durlacher, 2000)
- “The mobile devices and wireless networking environments necessary to provide location independent connectivity ”, (Elliott and Nigel Phillips, 2004)
- 廣義定義：「透過各種可以連接網路的行動裝置，如PDA、手機等設備，來進行各種應用、交易及服務。」

Module 12-1-2: 行動商務之通訊技術

- 行動商務之通訊技術主要分為二大類，即為行動裝置以及無線通訊技術

- 行動裝置包含：
  - GSM／GPRS／3G手機
  - PDA／ Pocket PC
  - GPS導航設備
  - RFID／非接觸式智慧卡
  - Sensor
  - …

Module 12-1-2:
行動商務之通訊技術（續）

- 無線通訊技術可根據傳輸距離的長短來分為三大類，包含：
  - 無線廣域網路 (Wireless Wide Area Network，WWAN)
  - 無線區域網路 (Wireless Local Area Network，WLAN)
  - 無線個人網路 (Wireless Personal Area Network，WPAN)

Module 12-1-2:
行動商務之通訊技術（續）

- WWAN是指傳輸範圍可跨越國家或不同城市之間的無線網路，其傳輸距離較遠、範圍廣大，通常都需由特殊的服務提供者來架設及維護整個網路，一般人只是單純以終端連線裝置來使用無線廣域網路。常見的WWAN技術包含：
  - 第一代通訊技術(1G)：早期的類比通訊系統，如AMPS (Advanced Mobile Phone System)
  - 第二代通訊技術(2G、2.5G) ：技術如 GSM (Global System for Mobile Communications)，而2.5G如GPRS (General Packet Radio Service)
  - 第三代通訊技術(3G)：技術如 UMTS (Universal Mobile Telecommunications System)

Module 12-1-2:
行動商務之通訊技術（續）

- 1G、2G、3G之比較

比較項目	第一代通訊	第二代通訊	第三代通訊
通訊方式	類比式	類比式/數位式	數位式
發展年代	1980 年代	1990 年代	2000 年代
傳輸能力	聲音	聲音、資料	聲音、多媒體資訊
傳輸技術	AMPS	GSM	CDMA(Code Division Multiple Access)
	TACS	GPRS	W-CDMA(Wideb and-CDMA)
	NMT		
數據傳輸率	無	9.6K bps(GSM)、	2M bps
		115K bps(GPRS)	
安全考量	無	有，但不嚴謹	有，較嚴謹

Module 12-1-2:
行動商務之通訊技術（續）

- WLAN是指傳輸範圍在100公尺左右的無線網路，像是用於單一建築物或辦公室之內。通常會將 WLAN 和現有的有線區域網路結合，不但增加原本網路的使用彈性，也可擴大無線網路的使用範圍。目前最熱門的 WLAN 技術就是 IEEE (Institute of Electrical and Electronic Engineers,電機電子工程師協會) 的 802.11 及其相關標準，而常見的802.11標準為：
  - 802.11b
  - 802.11a
  - 802.11g
  - 802.11n

Module 12-1-2:
行動商務之通訊技術（續）

- 802.11b/a/g/n之比較

	802.11b	802.11a	802.11g	802.11n
Approved by IEEE	Dec-99	Jan-00	Jun-03	Dec-07
Maximum Data Rate	11 Mbps	54 Mbps	54 Mbps	600 Mbps
Typical Range	70 m	30 m	50 m	60 m
Freq Band	2.4 GHz	5 GHz	2.4 GHz	2.4/5 GHz

Module 12-1-2:
行動商務之通訊技術（續）

- WPAN是指在個人活動範圍內所使用的無線網路技術，這類技術的主要用途是讓個人使用的資訊裝置，像是手機、PDA、筆記型電腦等可互相通訊，以達到交換資料的目的。常見的WPAN技術包含：
  - UWB (Ultra Wide Band)
  - Bluetooth
  - ZigBee
  - NFC (Near Field Communication)

Module 12-1-2:
行動商務之通訊技術（續）

- WPAN各項技術比較

WPAN	UWB	Bluetooth	ZigBee	NFC
頻段	3.1~10.6GHz	2.4GHz (ISM)	2.4GHz/868 /915MHz	13.56MHz
距離	0~10m	0~10m	10~75m	<50cm
傳輸率	高 53.3~480Mbps	中 1Mbps+	低 10k~250kbps	低 424kbps
安全性	High	High	Medium	Very High
價格	High	Medium	Low	Very Low
標準	802.15.3	802.15.1	802.15.4	IEC 18092/21481

行動通訊技術之風險與挑戰

- 行動設備之遺失或遭竊
- 內部人員所引發的安全問題
- 中間者攻擊(Man-in-the-middle attack)
- 偽造或仿造之設備
- 病毒/木馬
- 阻斷服務攻擊(Denial of Service Attack，DOS Attack)
- 無線電波傳輸之安全性
- 無線區域網路之安全性
- …

Module 12-1-3:
行動商務與電子商務之比較

	電子商務	行動商務
產品或服務之重點	產品	服務
產品或服務之資訊	靜態資訊與資料	動態資訊與資料
產品或服務之存取方式	有線存取	無線存取
產品或服務之存取特性	固定非時間限制之存取	存取之行動性與可攜性

Module 12-1-4: 行動商務之應用範圍

- 目前行動商務的應用已經相當普遍，本小節將以B2C、B2E、B2B來分類介紹

- B2C在行動商務中應用的種類是最多的，不管在娛樂、購物以及資訊取得的服務等方面都可見行動商務的應用，包含：
  - 行動銀行／行動券商：客戶能透過手機或個人數位助理等無線上網設備，進行包括轉帳、查詢、通知、用戶管理等服務，或者是查詢即時股票的最新行情、各股股價移動通知、投資組合管理，以及買賣股票並於成交時傳送簡訊通知等

Module 12-1-4: 行動商務之應用範圍（續）

- 簡訊服務：包含SMS (Short Message Service)／MMS (Multimedia Messaging Service) 這類的簡訊服務也可算是B2C行動商務應用的範圍
- 行動購物：行動購物能讓消費者透過無線上網設備查詢商品及價格相關資訊、瀏覽購物網站、比較不同網站之價格、優惠特賣通知、買賣雙方彼此溝通及支付貨款等服務，例如威秀影城的手機購票服務
- 行動娛樂服務：提供消費者娛樂性的應用服務，如鈴聲下載、圖像下載、遊戲下載等。行動娛樂是僅次於行動通訊的第二大行動加值服務應用。如目前中華電信的emome
- 其他如行動廣告等服務

Module 12-1-4: 行動商務之應用範圍（續）

- 行動商務B2B的應用則包含：
  - WASP (Wireless Application Service Provider)：在B2B電子商務中相當熱門的一個領域—應用軟體租賃服務ASP，目前也開始發展成為無線應用軟體租賃服務WASP或稱MASP (Mobile Application Service Provider)。業者利用Linux、Java、XML等通用相容的標準，發展能讓不同無線上網設備連線接收內容的整合性解決方案等
  - Mobile CRM／ERP：行動顧客關係管理及企業資源規劃系統
  - 視訊會議／遠端協同工作等服務
  - …

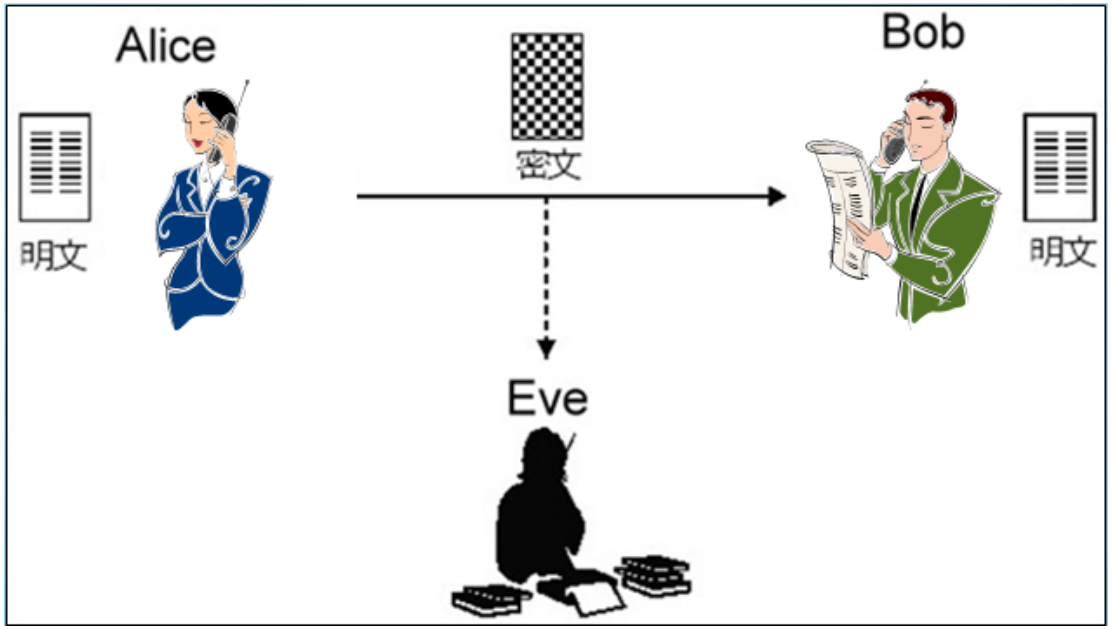
Module 12-1-4: 行動商務之應用範圍（續）

- B2E行動商務是指企業對員工之M化的應用，就適用對象而言，大多是以移動性較高的物流倉儲業、金融壽險業居多，目的是讓這些行動工作者，能透過無線上網設備，隨時隨地收發電子郵件、查閱及修改行事曆，包含以下服務：
  - Mobile PIM (Personal Information Management)
  - Mobile Scheduling
  - Mobile Email
  - Mobile Learning
  - Mobile Intranet Access
  - Document Retrieval and Management

Module 12-2:
行動商務安全需求

Module 12-2:
行動商務安全需求

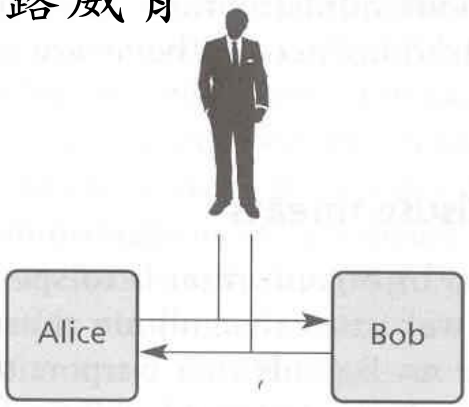
- 通訊系統模型



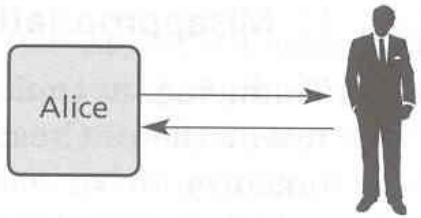
- 攻擊者可能採取以下方式進行攻擊
  - 竊取訊息
  - 竄改訊息
  - 偽造訊息
  - 阻斷服務

Module 12-2:
行動商務安全需求

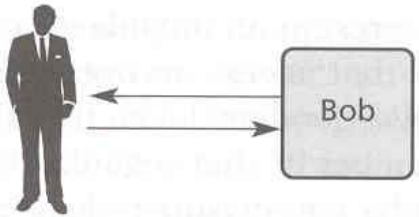
- 可能的揭露威脅



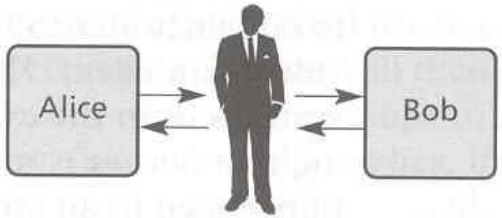
Eavesdropping



Masquerading as a service



Masquerading as a client



Man-in-the-middle Masquerading as service and client

Module 12-2:
行動商務安全需求（續）

- 為了保護使用者在進行行動商務時的資訊安全，必須達到以下四點安全需求，包含：
  - 身分鑑別 (Authentication)
  - 資料機密性 (Data Confidentiality)
  - 資料完整性 (Data Integrity)
  - 不可否認性 (Non-repudiation)

Module 12-2-1: 身分鑑別

- 為了確保通訊過程中，使用者的身分合法，而非仿冒的攻擊者，所以必須進行身分鑑別的動作
- 可依下列秘密特徵來鑑別確認無線裝置或其使用者之身分：
  - 所唯一具有之生理特徵：如指紋、聲紋
  - 所唯一擁有之秘密訊息：如私密金鑰
  - 雙方共同擁有之秘密訊息：如通行碼

Module 12-2-1:
身分鑑別（續）

- 鑑別程序

Alice

(1) 詢問，要求提供資料鑑別

(2) 應答，提示擁有之特徵

Bob

(3) 驗證是否擁有其特徵：

通過，確認Alice 身分；

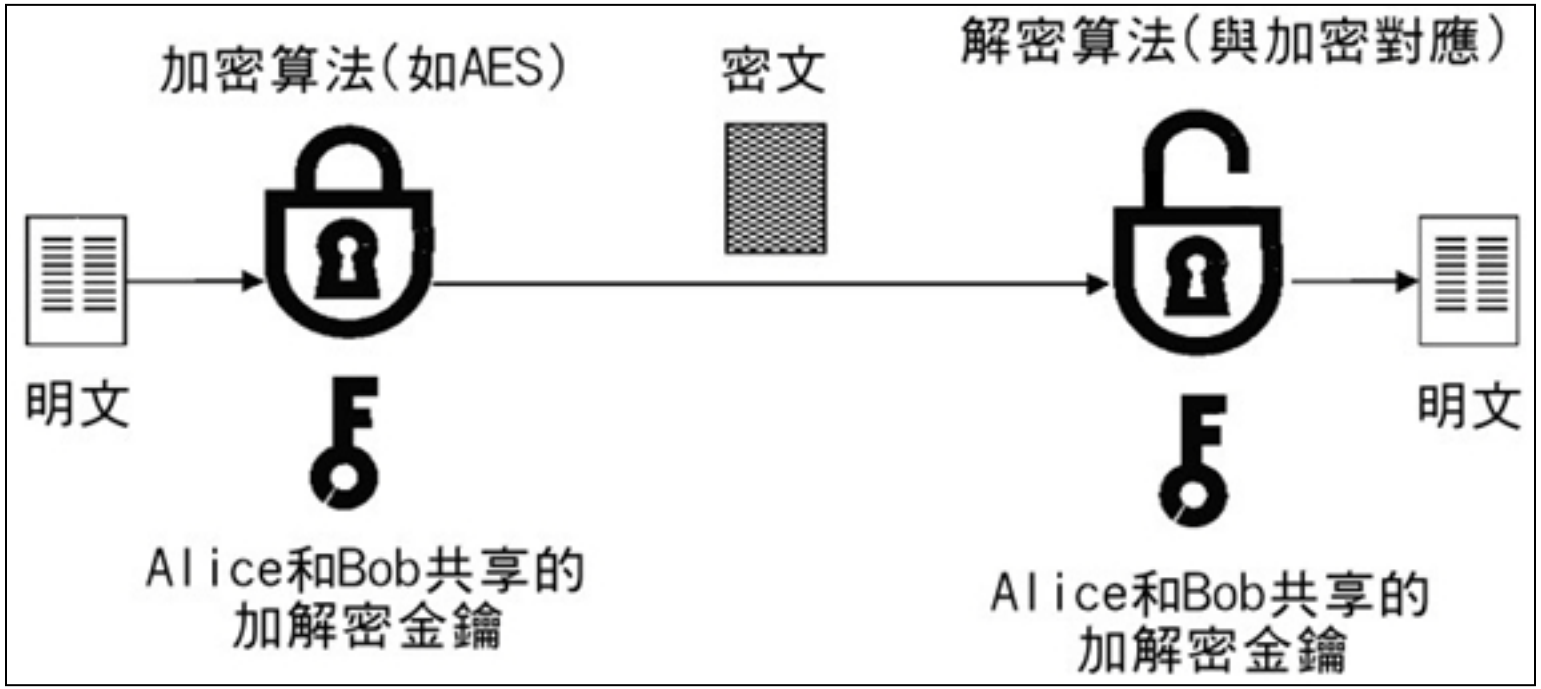
不通過，否定Alice身分

Module 12-2-2:
資料機密性

- 為了保護通訊中所傳遞的訊息被攻擊者攔截，這些訊息有可能是個人的隱密資訊，如使用者帳號、密碼或者是信用卡號，因此可以在訊息傳送之前先將訊息加密，以保護資料的機密性
- 現代密碼技術中最主要的即是私密金鑰密碼系統 (Private-Key Cryptosystems) 或稱對稱金鑰 (Symmetric-Key) 密碼系統，以及公開金鑰密碼系統 (Public-Key Cryptosystems) 或稱非對稱 (Asymmetric-Key) 金鑰密碼系統
- 私密金鑰密碼系統，例如：DES, AES
- 私密金鑰密碼系統，例如：RSA

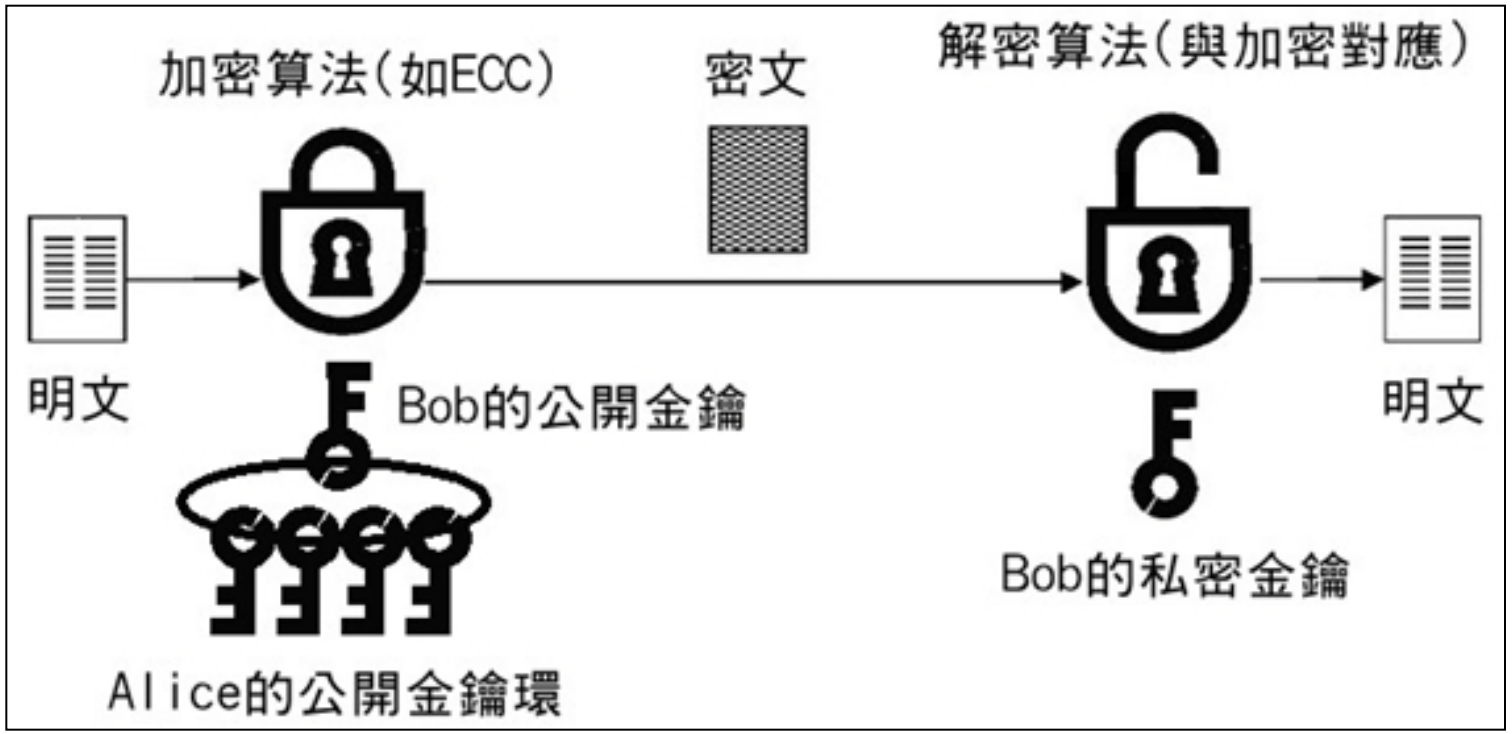
Module 12-2-2: 資料機密性（續）

- 私密金鑰密碼系統之概念
  - Alice和Bob使用同一把加解密金鑰



Module 12-2-2: 資料機密性（續）

- 公開金鑰密碼系統之概念
  - 加密與解密所使用的金鑰不同

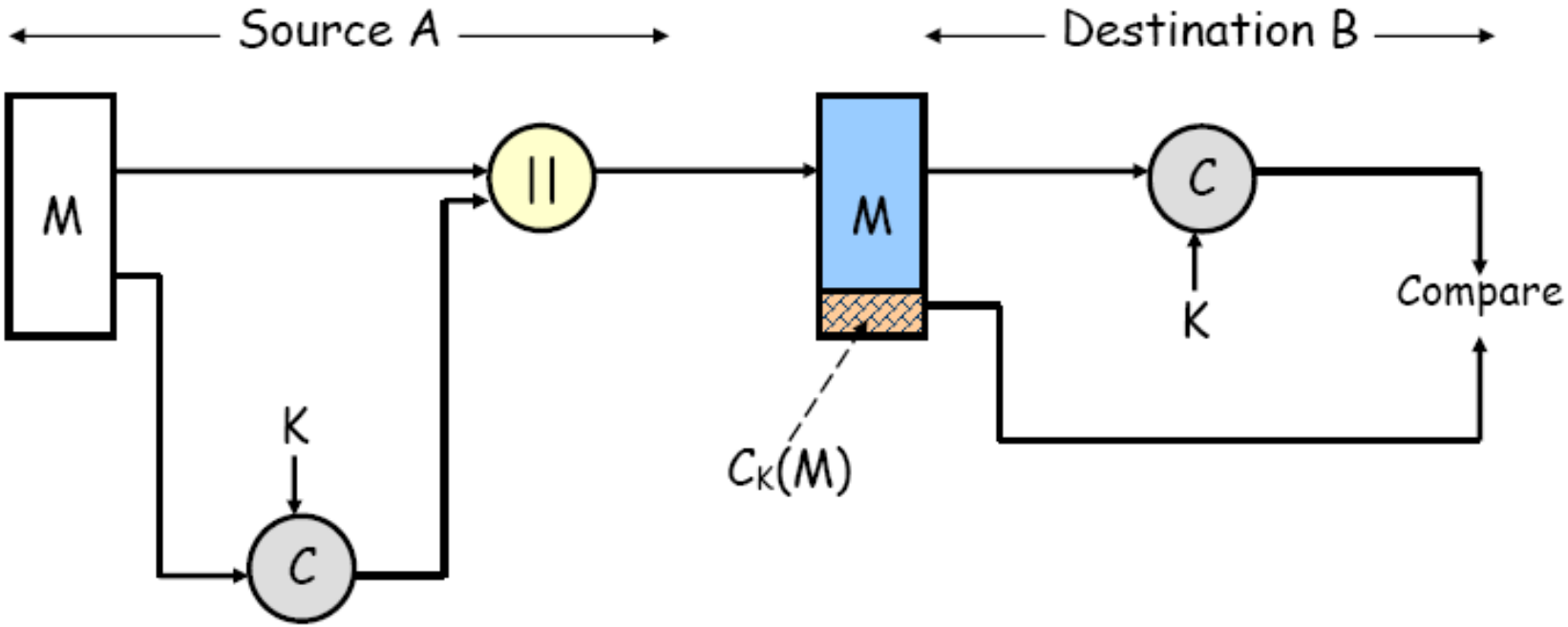


Module 12-2-3: 資料完整性

- 資料完整性則是提供保護以防止攻擊者對於通訊中的訊息進行更改或者是破壞，造成使用者接收到錯誤的訊息
- 為了保護資料完整性，可在訊息接收完成後進行檢查，常用的做法如訊息鑑別碼 (Message Authentication Code，MAC)
  - MAC=$C_k(M)$，其中M為訊息，C為MAC函式，k為私密金鑰， MAC為運算後產生的訊息鑑別碼
  - 將MAC加在每個訊息之後一起傳送給接收端，接收端使用同一把私密金鑰來執行相同的運算 ，比對兩個MAC即可確認訊息是否遭受修改

Module 12-2-3: 資料完整性（續）

- 訊息鑑別碼之概念

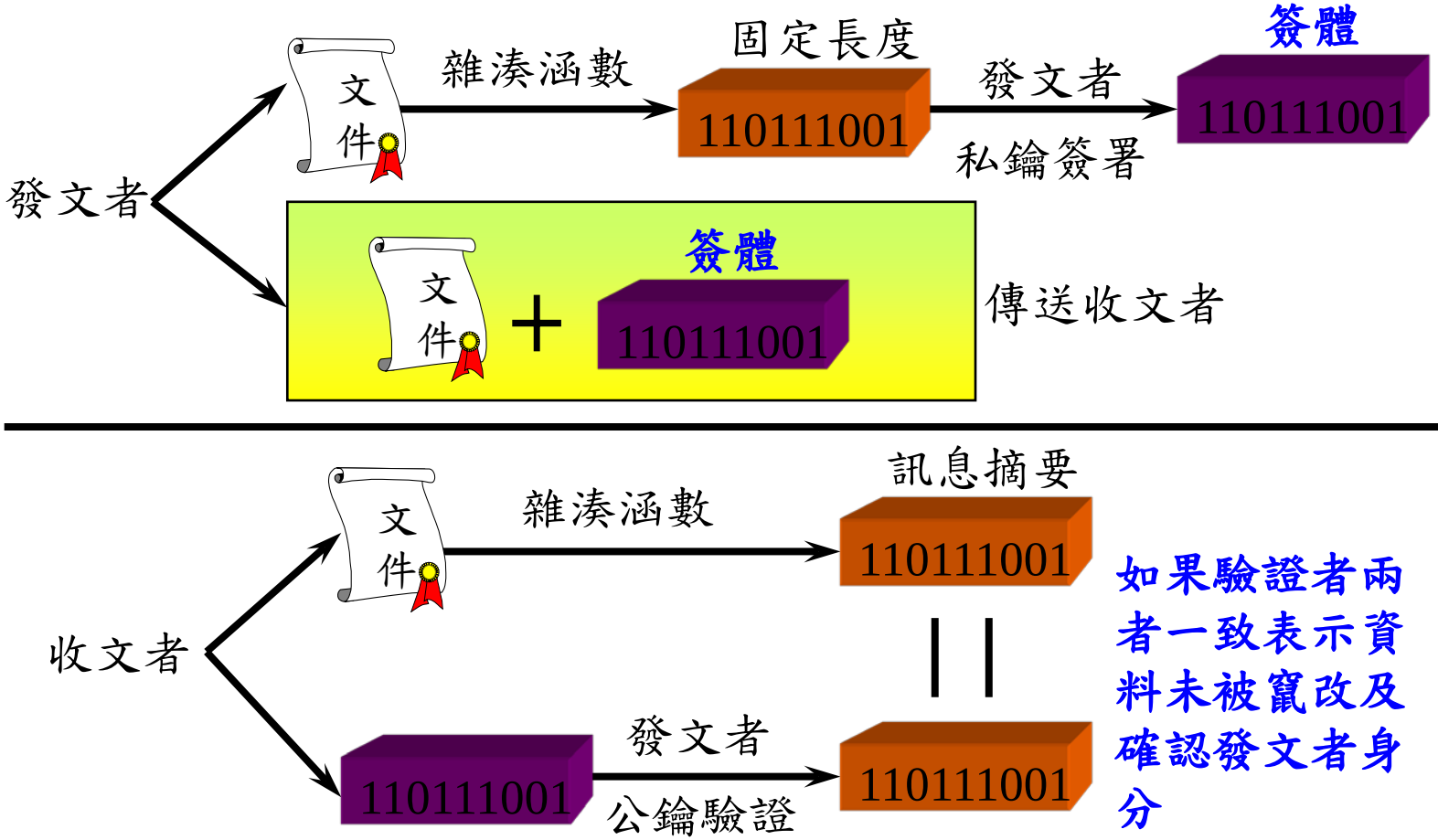


Module 12-2-4:
不可否認性

- 不可否認性是為了防止惡意的使用者否認先前所進行過的交易，其目標是產生、收集、維護以及驗證關於宣稱的事件或行動之證據，以解決關於已經發生或尚未發生事件的糾紛
- 為了達成不可否認性，通常可採取數位簽章之技術，例如：RSA數位簽章法演算法
- 數位簽章具備以下特性：
  - 鑑別性
  - 完整性
  - 不可否認性

Module 12-2-4: 不可否認性（續）

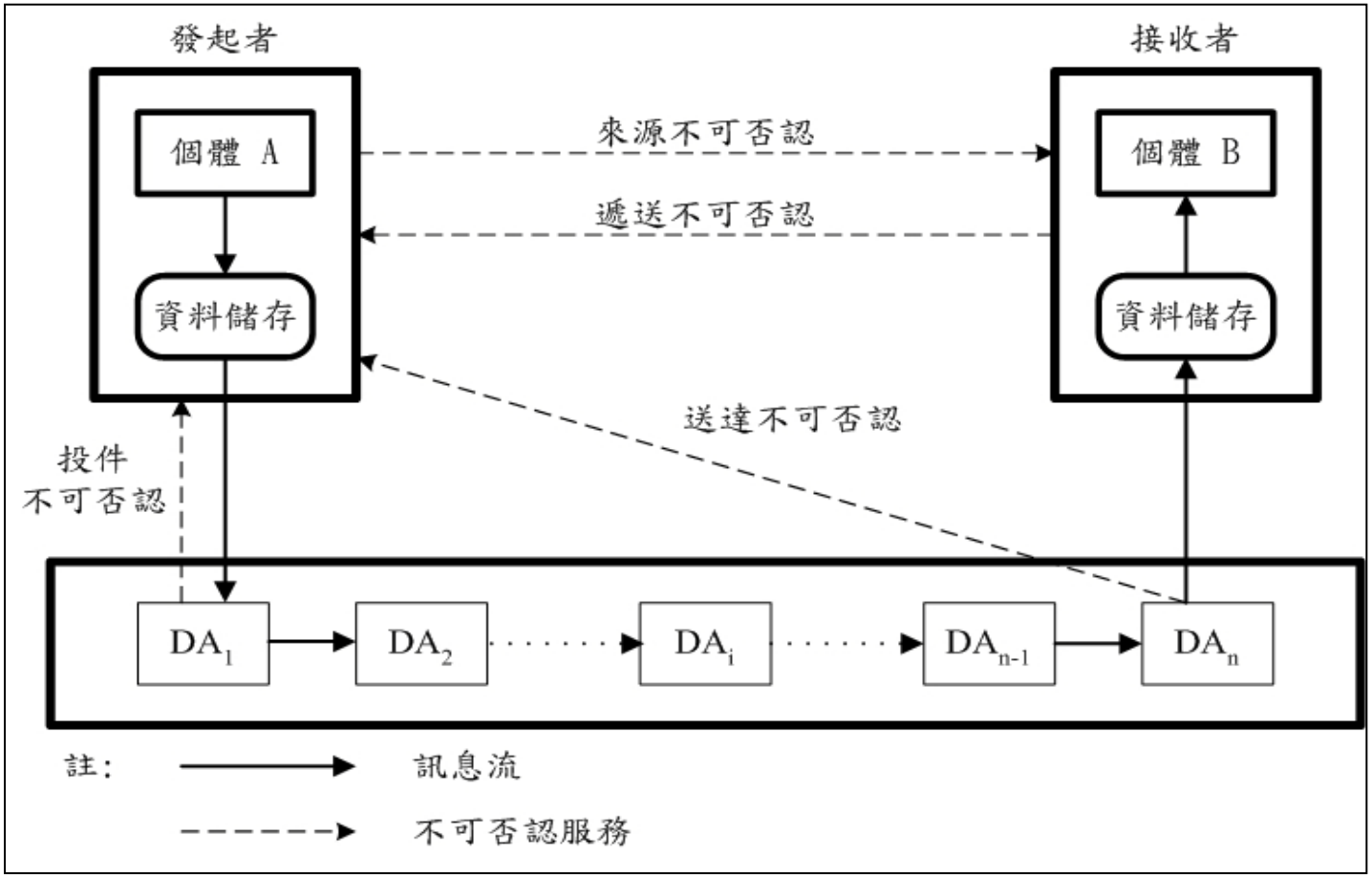
- 數位簽章之概念



來源：中華電信研究所

Module 12-2-4: 不可否認性（續）

- 不可否認機制－CNS 14510-1 Protocol



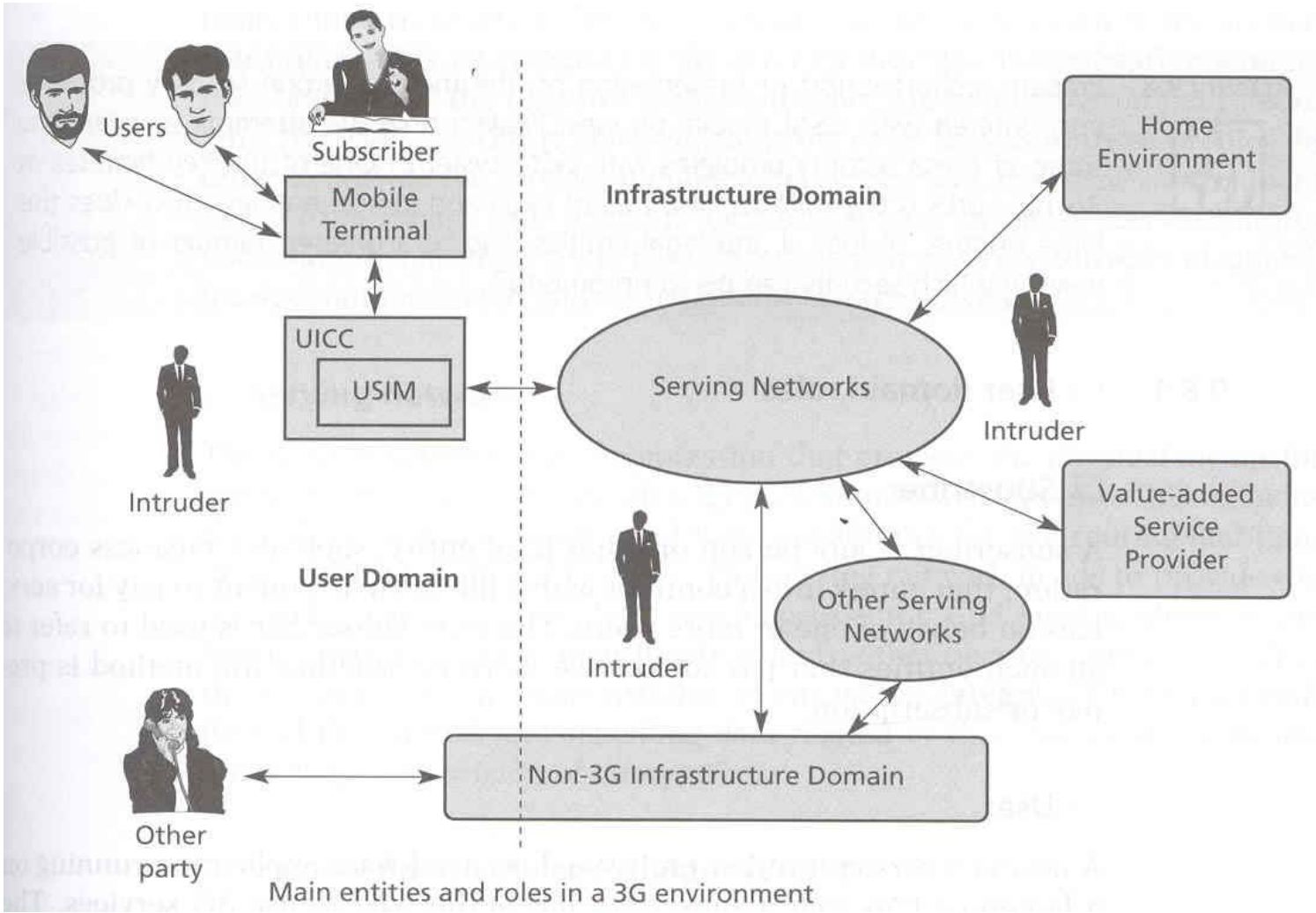
Module 12-3:
行動商務安全機制

Module 12-3:
行動商務安全機制

- 目前已經有許多適用於行動商務的安全機制提出，這些機制有些使用在GSM系統中，有些則使用在802.11無線網路中，因此本節將以WWAN、WLAN、WPAN的分類方式，各別介紹數種安全機制
  - WWAN通訊技術的安全機制
  - WLAN通訊技術的安全機制
  - WPAN通訊技術的安全機制

Module 12-3-1:
WWAN通訊技術的安全機制

- 可能安全威脅

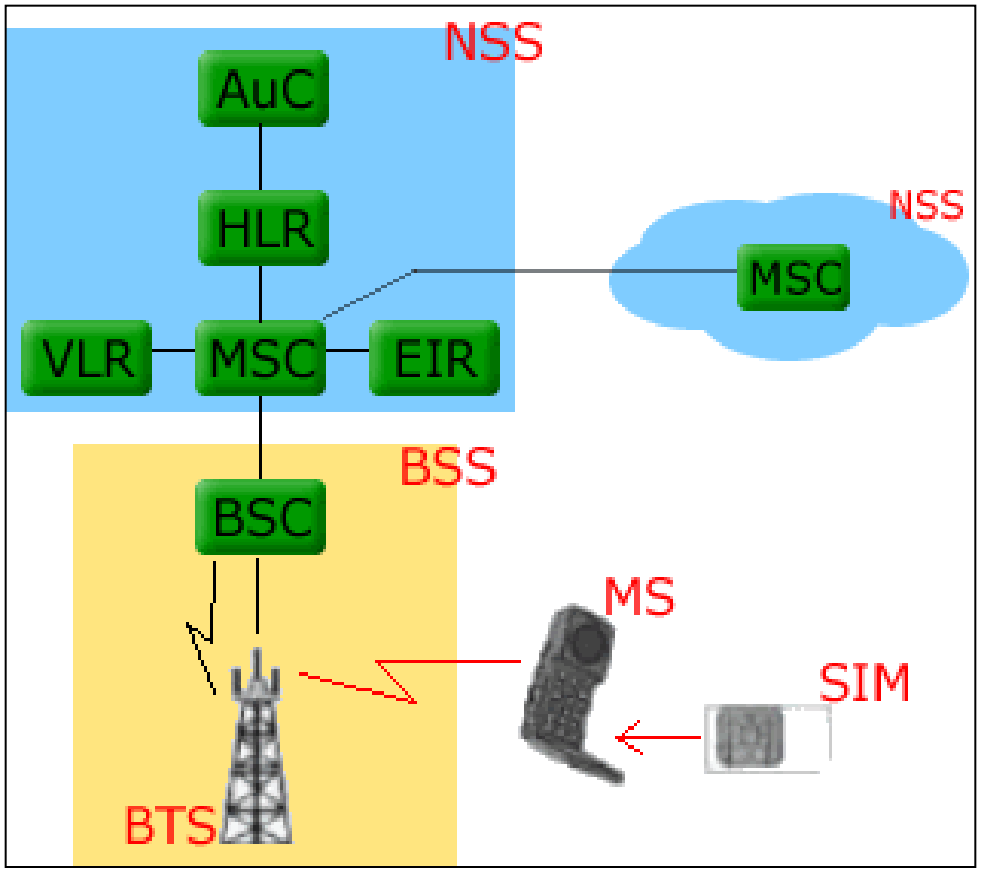


Main entities and roles in a 3G environment

Module 12-3-1:
WWAN通訊技術的安全機制

• GSM系統架構

- **MS(Mobile System)**
  - SIM(Subscriber Identity Module)
- **BSS(Base Station Subsystem)**
  - BTS(Base Transceiver Station)
  - BSC(Base Station Controller)
- **NSS(Network and Switching Subsystem)**
  - MSC(Mobile Switching Center)
  - VLR(Visitor Location Register)
  - HLR(Home Location Register)
  - AuC(Authentication Center)
  - EIR(Equipment Identity Register)



Module 12-3-1: WWAN通訊技術的安全機制（續）

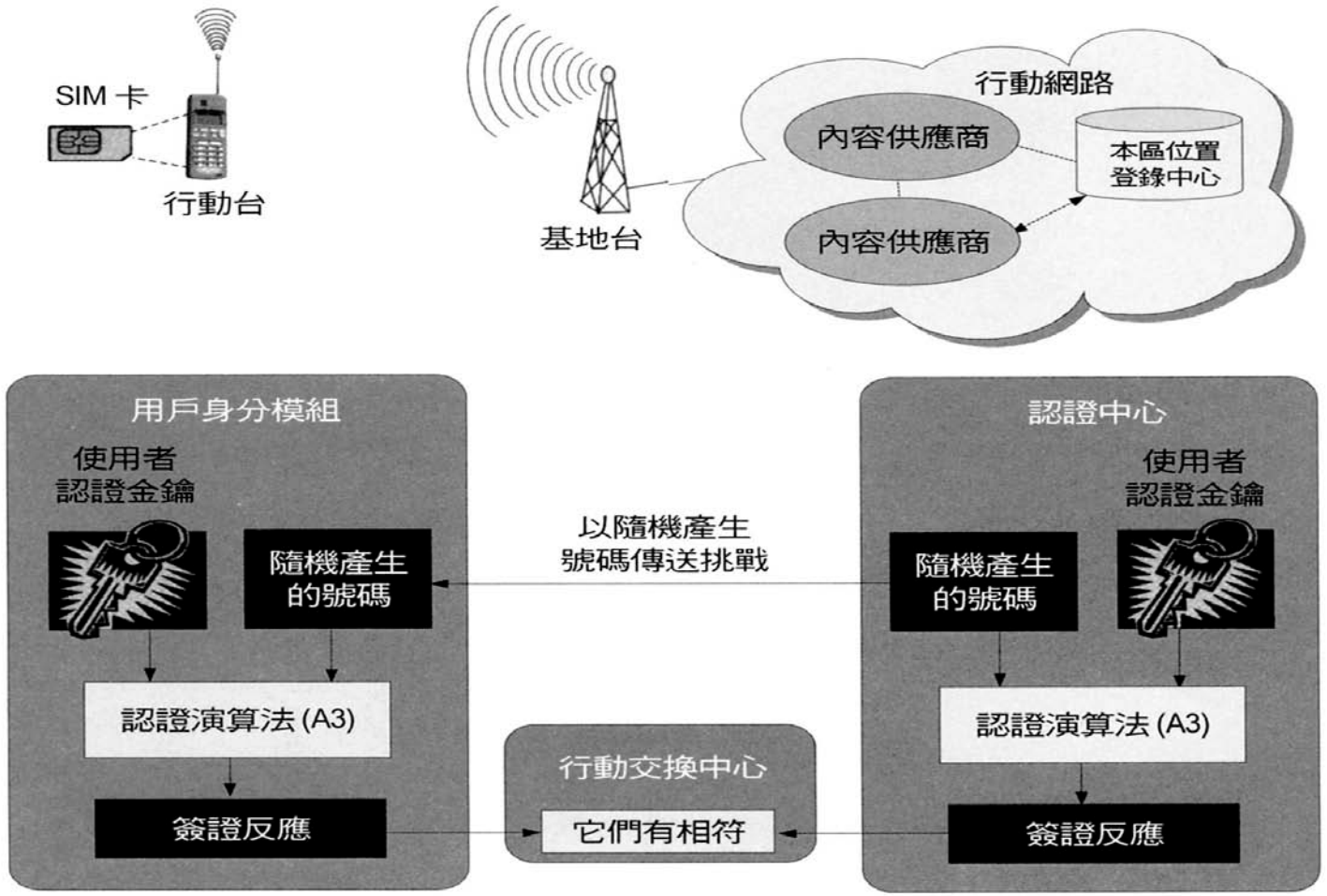
- GSM系統中有三個重要的加密演算法
  - A3
    - 身分鑑別演算法
  - A5
    - 金鑰產生演算法
  - A8
    - 通話加密演算法

Module 12-3-1: WWAN通訊技術的安全機制（續）

- GSM系統透過A3、A5、A8演算法的使用可達到安全需求中的身分鑑別以及資料機密性
  - 身分鑑別：GSM Network operator（通常為在HLR中的AuC）透過一RAND碼與MS端SIM卡中的K_i進行Authentication動作 (by A3)，以驗證MS是否為合法使用者，達到不容易被盜拷號碼的目的
  - 資料機密性：透過一RAND碼與Ki來產生加密用的Kc (by A8)，收送雙方借由Kc來進行訊息的加解密 (by A5)，以達到訊息不容易被竊聽得知內容的目的
  - 匿名性：利用TMSI (Temporary Mobile Subscriber Identity)來避免手機IMSI (International Mobile Subscriber Identification)的資訊被擷取，而獲得使用者相關的服務資訊。

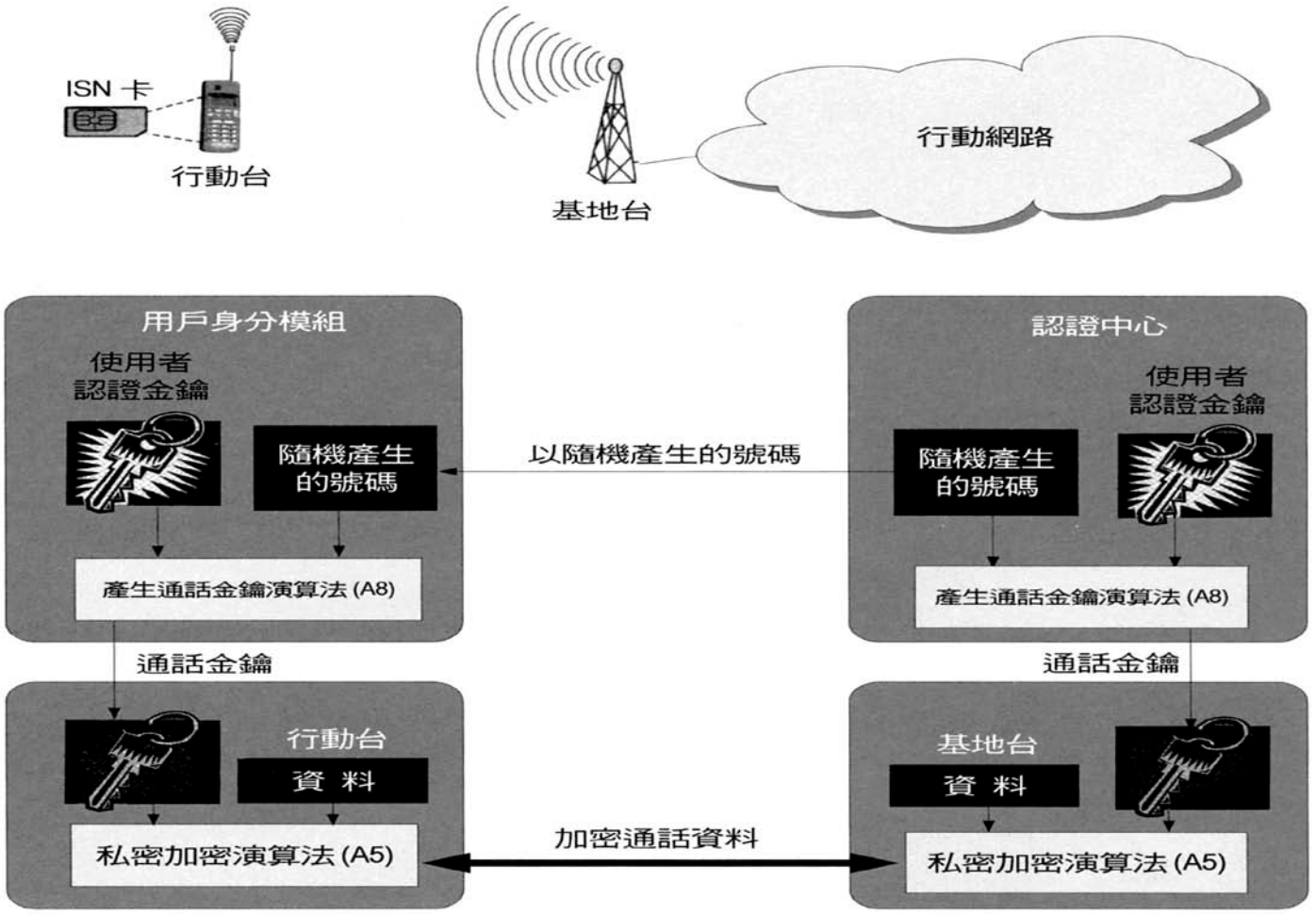
Module 12-3-1: WWAN通訊技術的安全機制（續）

- **GSM系統之身分鑑別**



Module 12-3-1:
WWAN通訊技術的安全機制（續）

- GSM系統之通話加密

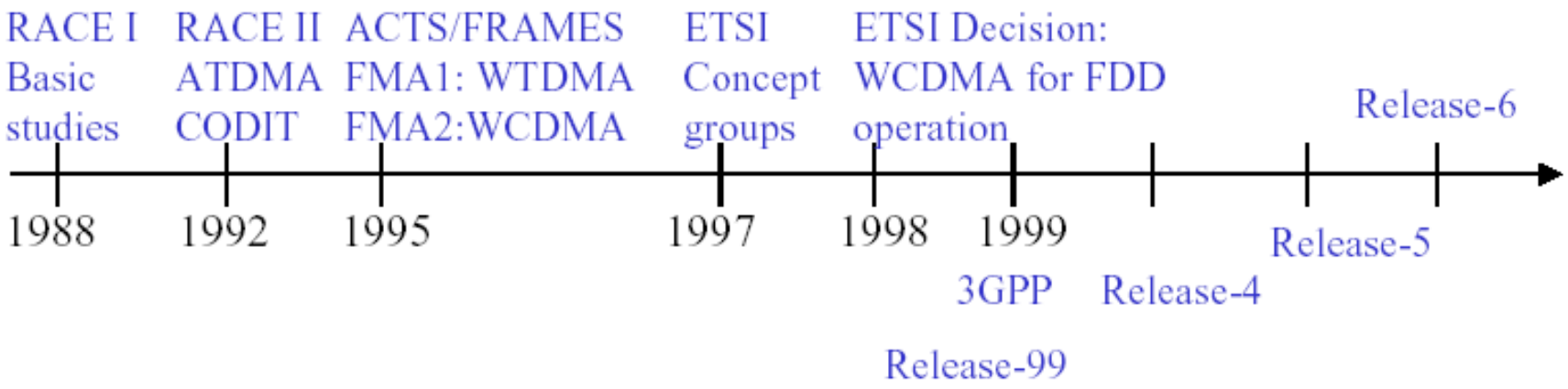


Module 12-3-1:
WWAN通訊技術的安全機制（續）

- **GSM系統之安全性**
  - GSM的加密演算法並未公開，而引起學術界的批評，A5/1與A5/2演算法後來更被Marc Briceno、Ian Goldberg和David Wagner用逆向工程法破解。
  - GSM的身分鑑別可由業者自行設計，未納進標準中；之前許多業者使用COMP-128，但已被證實該演算法會遭受攻擊，
  - GSM金鑰長度為64位元，初始前10位元還預設為0，導致真實金鑰僅54位元(後來採64位元金鑰)，且要增加金鑰長度是困難、複雜的。
  - GSM沒有明確的設計用來抵禦主動式攻擊(由網路端發起)，因為主動式攻擊需要一個fake base station，成本太高，攻擊的可行性不高。但隨著網路設備與服務越來越普及、成本越來越低、可獲得性越來越高，還是有可能透過fake base station attack取得user資訊(雖然之後GSM有提出因應對策，但仍未考量全面性的網路環境)。
  - GSM的circuit-switched service僅在MS與BS之間進行加密保護。

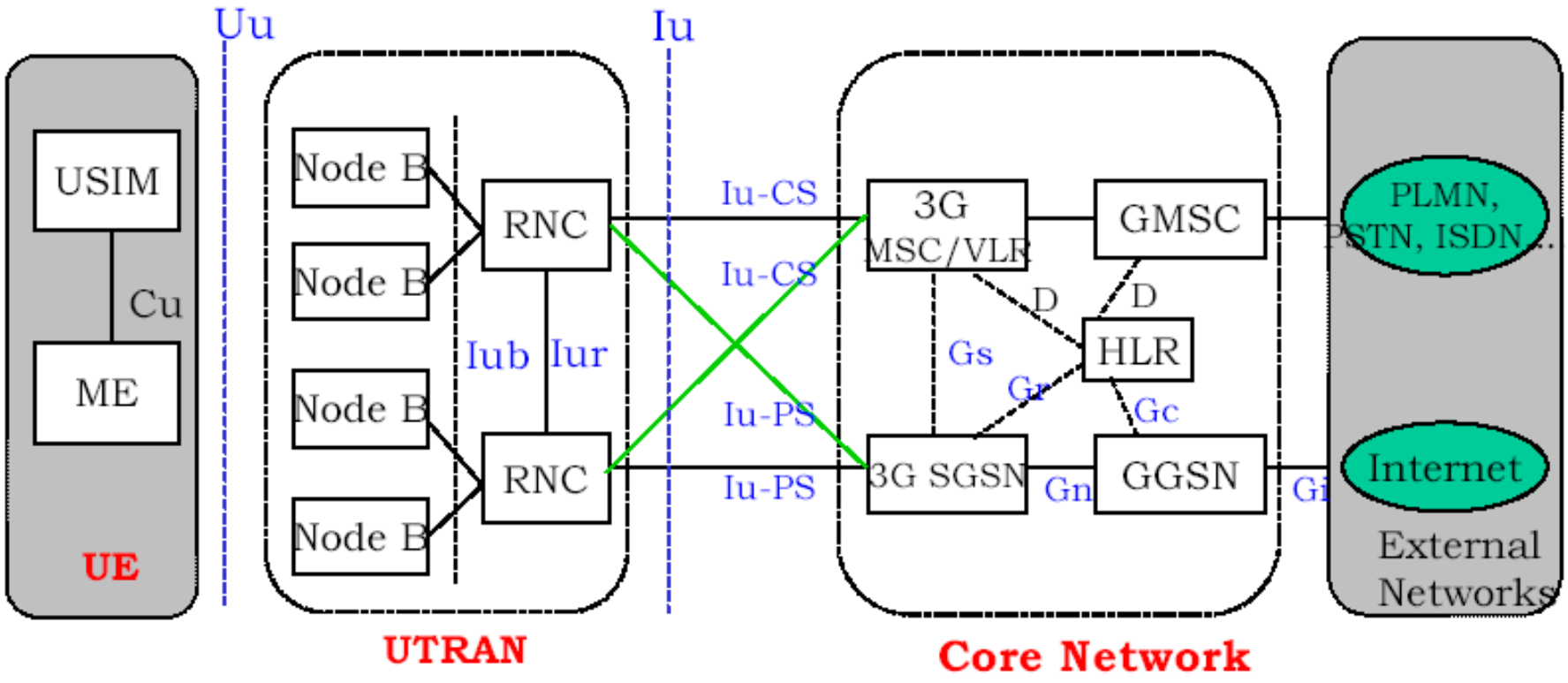
Module 12-3-1:
WWAN通訊技術的安全機制（續）

- **UMTS (Universal Mobile Telecommunication system)**



Module 12-3-1:
WWAN通訊技術的安全機制（續）

•UMTS 系統架構



System Architecture of 3GPP Release 99

Module 12-3-1: WWAN通訊技術的安全機制（續）

•UMTS安全性

- 雙向身分鑑別
  - 用戶身分鑑別：與GSM相同
  - 網路鑑別：MS端驗證所連接之網路是否經使用者主籍系統授權，並且確認該鑑別是否在有效期限
- 資料完整性
  - MS與SN可自行決定完整性之演算法
  - 個體鑑別會產生MS與SN雙方所協商的IK
  - 收方透過驗證IK的真實性來達成資料完整性
- 防制重送攻擊
  - 透過更新之資料串來達成
  - 透過一序號 (COUNT-I)來防制插入或刪除

Boman, G. Horn, P. Howard and V. Niemi, “UMTS security,” *Electronics & Communication Engineering Journal*, 2002

Module 12-3-1: WWAN通訊技術的安全機制（續）

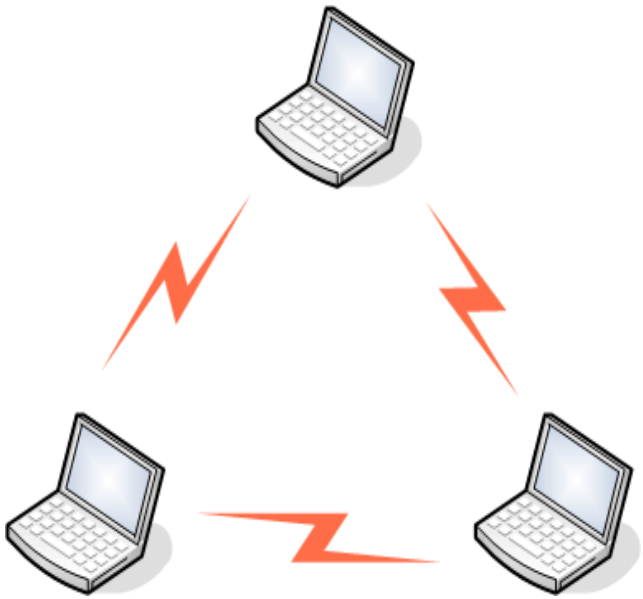
•UMTS安全性

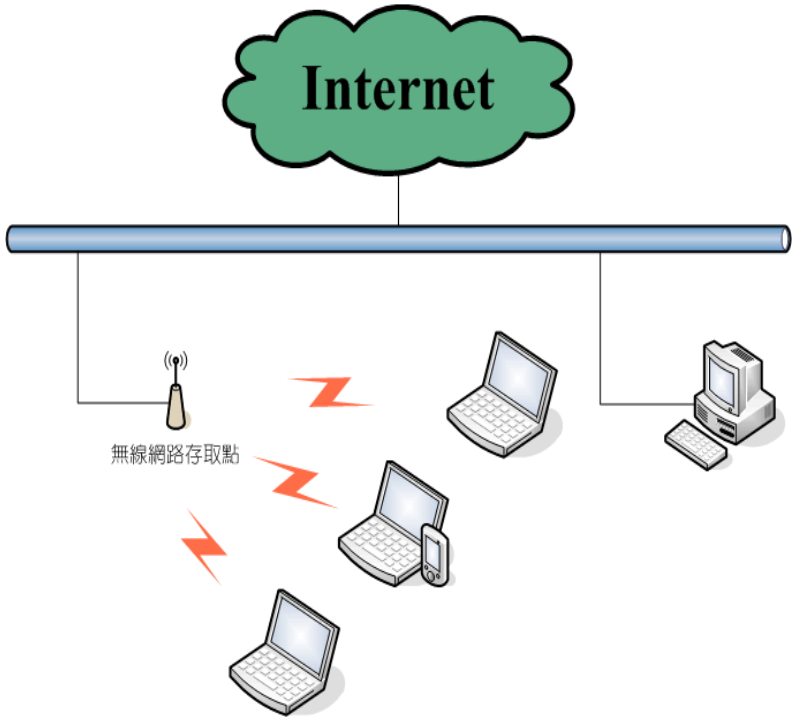
- 行動設備識別(Mobile equipment identification)
  - 每個無線通訊系統設備都有唯一的IMEI (International Mobile Equipment Identity) (無法被竄改)，業者可比對IMEI與IMSI是否配對，來確認使用者目前的行動設備是否合法
- USIM與User、terminal、network的關係
  - **User-to-USIM authentication**
    - User與USIM (Universal Subscriber Identity Module)透過共享秘密(如PIN碼)才能使用USIM
  - **USIM-terminal link**
    - USIM與Terminal透過共享秘密，來進行限制動作(如SIM-lock)
  - **USIM Application Toolkit**
    - 讓operator或third-party provider 可以在USIM上建置應用程式。Network operator則可透過網路對USIM進行訊息傳遞

Boman, G. Horn, P. Howard and V. Niemi, "UMTS security," *Electronics & Communication Engineering Journal*, 2002

Module 12-3-2: WLAN通訊技術的安全機制

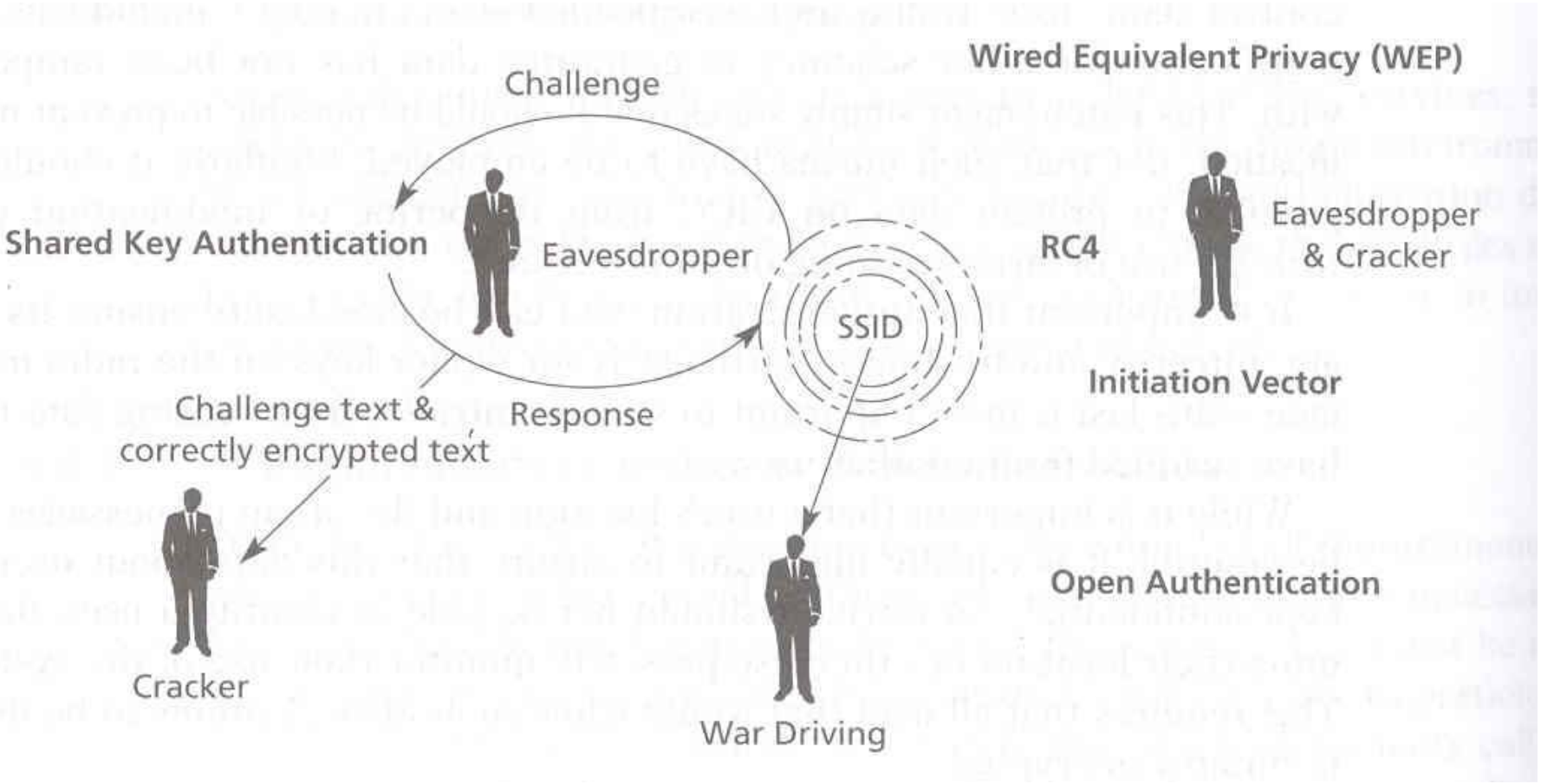
- 802.11無線網路的兩種模式
  - 左圖為簡易模式 (Ad Hoc Mode)
  - 右圖為基礎建設模式 (Infrastructure Mode)





Module 12-3-2:
WLAN通訊技術的安全機制

- 可能安全威脅



Module 12-3-2: WLAN通訊技術的安全機制

- 可能安全威脅
  - War Driving / Sniffing (Parking Lot attack)
  - Rogue Access Points
  - MAC Address
  - SSID
  - WEP

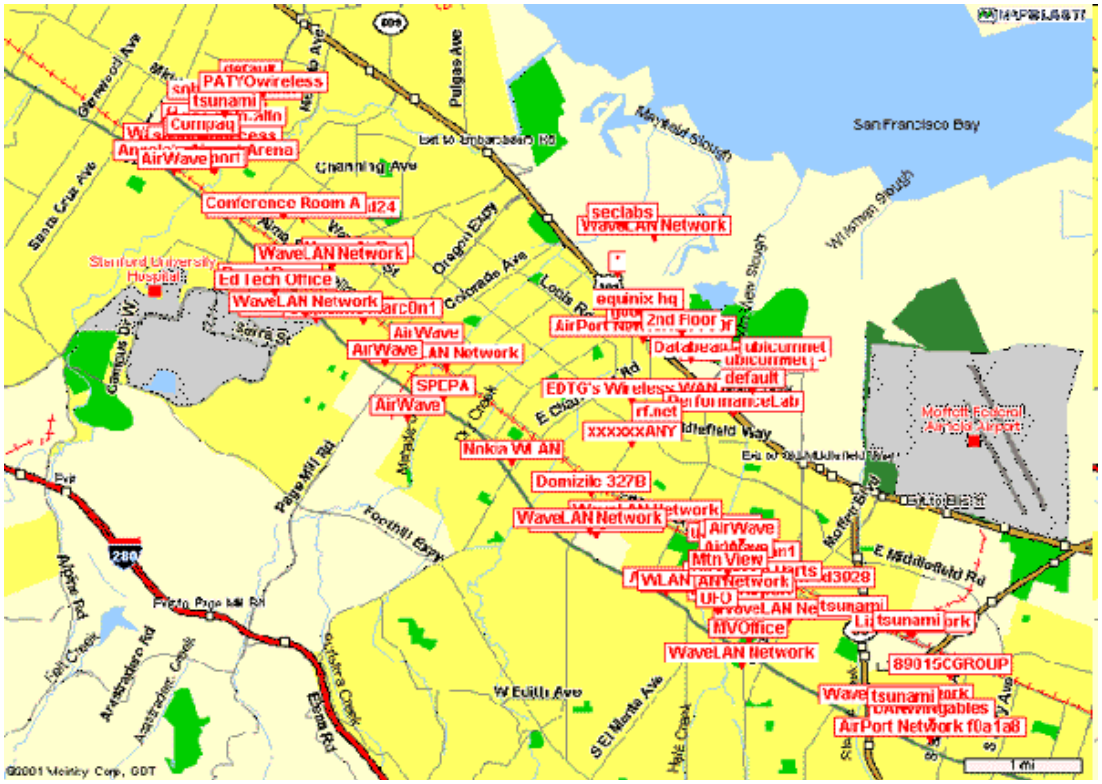
Module 12-3-2: WLAN通訊技術的安全機制

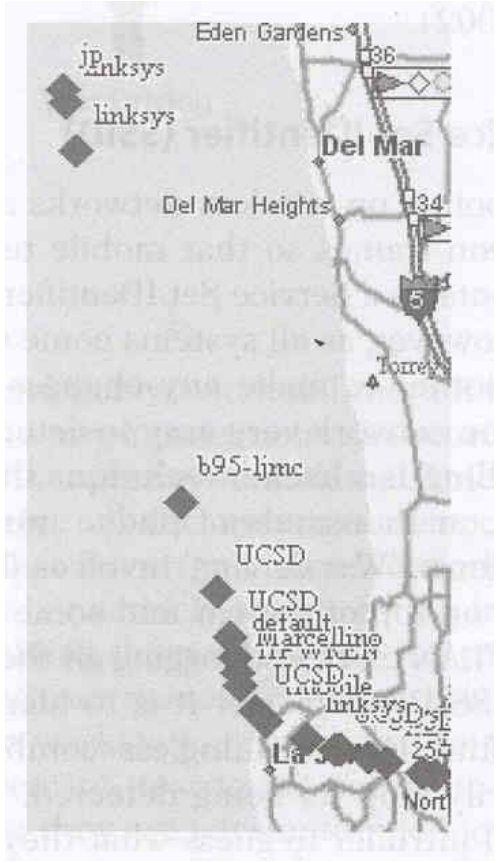
- **War Driving**

- War Driving是指駕駛車輛的同時，以行動裝置探測無線網路存取點(Access Point，AP)的行為。
  - http://www.wardriving.com/
- 常見的軟體如下：
  - NetStumbler
  - AiroPeek
  - MobileManager
  - Sniffer Wireless
  - THC-WarDrive

Module 12-3-2:
WLAN通訊技術的安全機制

- 結合GPS與地圖之War Driving攻擊手法

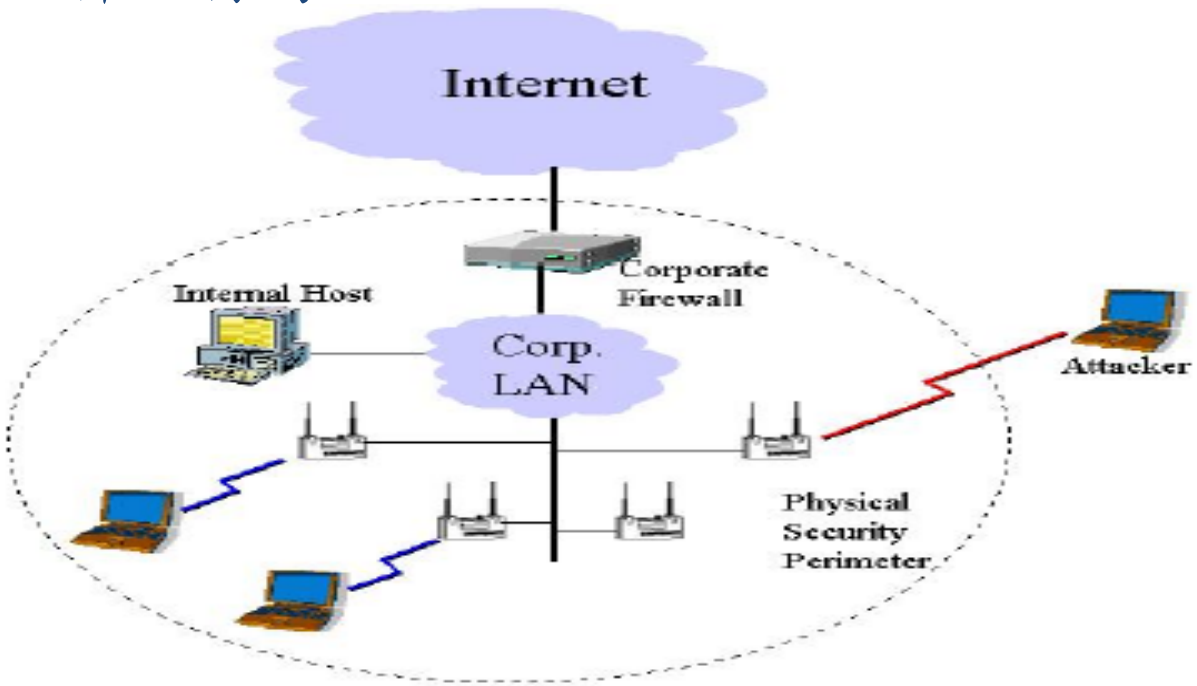




Module 12-3-2:
WLAN通訊技術的安全機制

• Parking Lot 攻擊

– 意即攻擊者可以坐在特定受害者的停車場車上，輕易地進行竊聽之 非法行為



Module 12-3-2: WLAN通訊技術的安全機制

- **未經授權的AP**
  - 未經允許的情況下，安置AP
  - 未啟動AP的安全性
  - 整個網路將易受到war driving/sniffing攻擊

Module 12-3-2: WLAN通訊技術的安全機制

- 使用MAC位址
  - 只允許合法的MAC位址才能存取無線網路
  - 合法MAC位址列表之複雜性與不易維護
  - 可使用軟體來偽造MAC位址

Module 12-3-2: WLAN通訊技術的安全機制

•Service Set ID (SSID)

- SSID是特定無線網路服務的名稱
- 可透過SSID來存取特定AP
- SSID若愈多人知道，則易導致SSID濫用或誤用之情形
- 若SSID變更，將告知所有的使用者

Module 12-3-2: WLAN通訊技術的安全機制

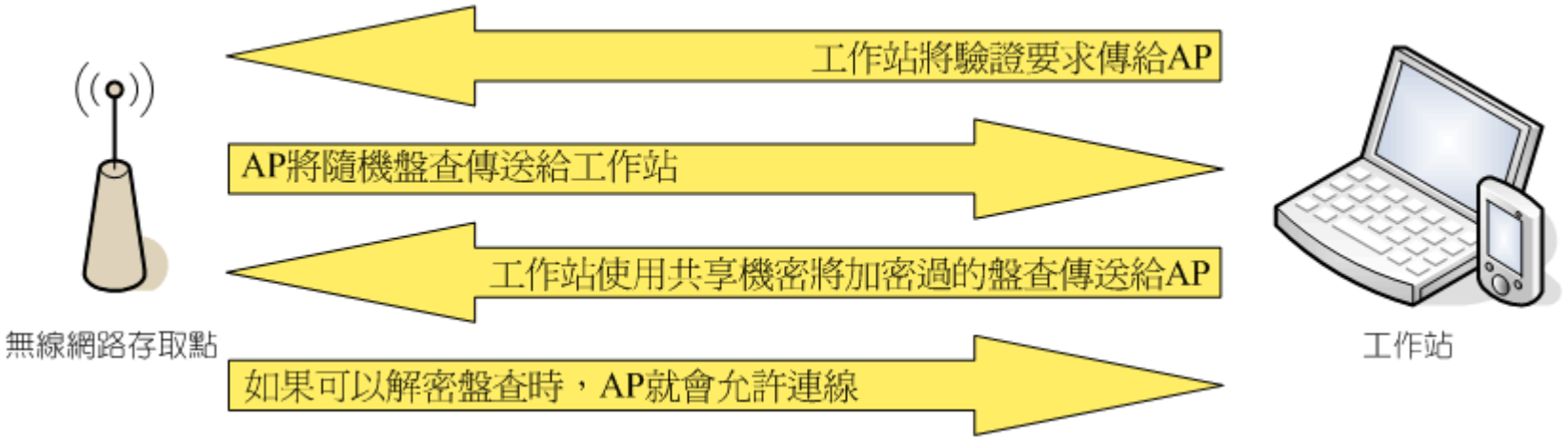
- 有線設備隱私 (Wired Equipment Privacy, WEP)
  - 目前市面上用的無線網路的認證機制，最基本的就是WEP，它是802.11定義下的一種加密方式，能夠提供以下服務
    - WEP鑑別機制
      - 身分鑑別
      - 存取控制 (Access Control)
    - WEP資料加密機制
      - 資料完整性
      - 資料機密性

Module 12-3-2: WLAN通訊技術的安全機制（續）

- WEP身分鑑別機制主要是採用擷問與回應的 (Challenge-Response) 方式，流程如下：
  - 使用者先送出使用身分驗證的鑑別給無線網路存取點 (Access Point, AP)，工作站是以服務辨識碼 (SSID) 或MAC位址做為與AP初始交換的身分鑑別回應
  - AP回應給使用者一個接受此鑑別方法的訊息，此訊息中並包含一個 128bits 的亂數作為挑戰用訊息
  - 使用者收到此訊息後，以預知的密鑰將此亂數加密並送回給AP鑑別
  - AP判斷是否為合法使用者，並決定是否讓使用者連結進入網路

Module 12-3-2: WLAN通訊技術的安全機制（續）

- WEP身分鑑別機制



Module 12-3-2: WLAN通訊技術的安全機制（續）

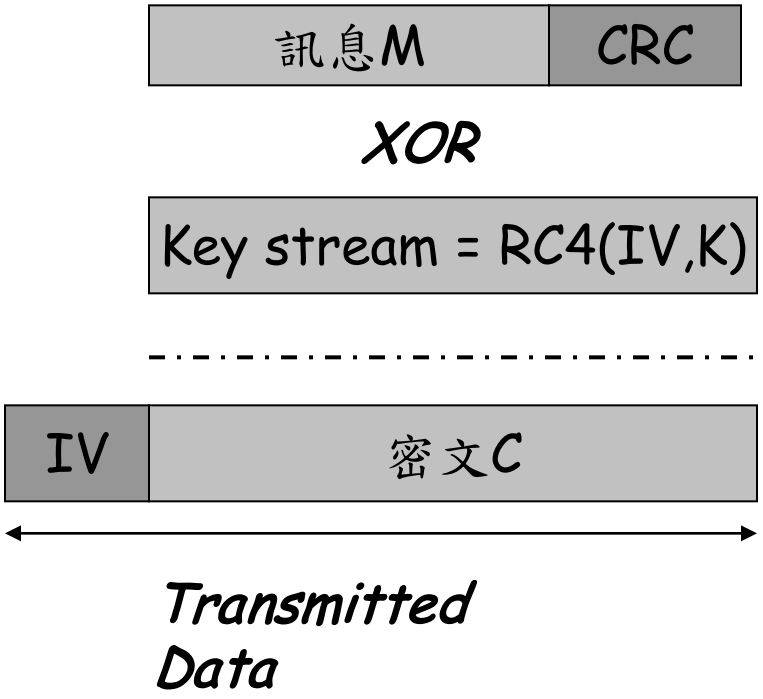
- 資料機密性
  - WEP 加密採用RC4演算法，雙方的密鑰是共享的，透過一個 24位元長度的初始向量IV (initialization Vector)，結合 40位元或104位元的密鑰來共同產生真正用來加密的密鑰串流，所有的傳輸內容與這個密鑰串流進行 XOR 運算，轉換成密文後發送
- 資料完整性
  - WEP會針對每一個傳送的封包做完整性檢查。在每一個封包加密之前會先使用CRC予以計算，之後再將資料和加密過的CRC相加並傳送給目標接收者

Module 12-3-2:
WLAN通訊技術的安全機制（續）

- **WEP資料加密機制**
  - 計算完整性檢查碼c(M)，並且附加至原始訊息 M，即

    $P = <M + c(M)>$

  - 使用RC4加密演算法、初始向量IV以及共享金鑰K，來產生金鑰串(key stream)
  - 互斥或訊息 “P”與金鑰，以產生密文$C = P \oplus RC4(IV,K)$
  - 傳送IV與密文C



Module 12-3-2: WLAN通訊技術的安全機制（續）

•WEP協定的缺點

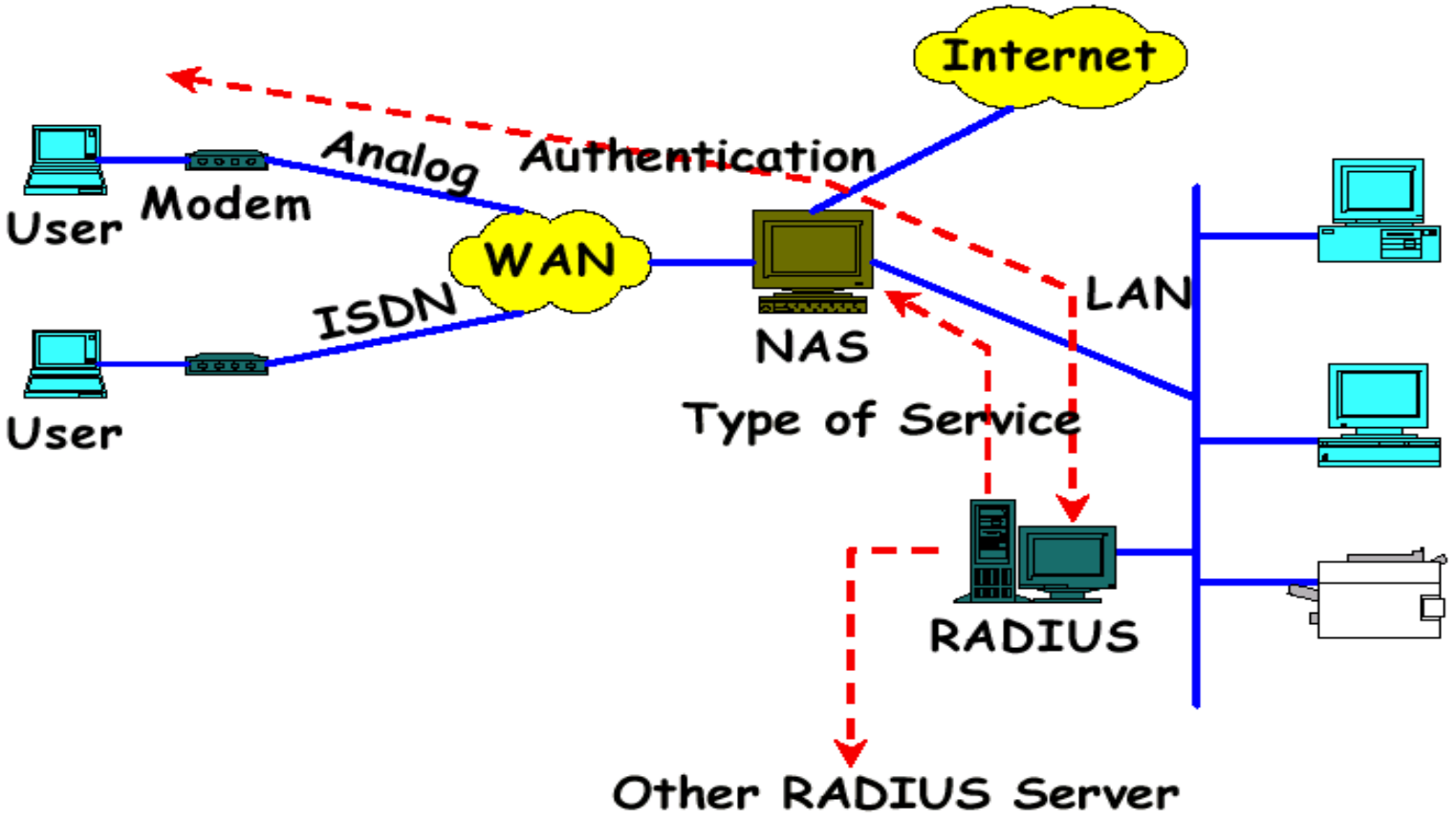
- 缺乏金鑰管理機制
- 易遭受被動攻擊以及主動攻擊
  - 被動攻擊：基於統計分析、WEP安全漏洞，企圖從竊聽之訊息中，破解加密金鑰，並解密密文
  - 主動攻擊：未經授權之行動基地台，產生新的或偽造的訊息，以達到假冒之目的
- 存取控制不完善Data headers are not encrypted
- 初始向量之濫用或誤用

Module 12-3-2: WLAN通訊技術的安全機制（續）

- **遠端認證撥接使用者服務 (Remote Access Dial In User Service, RADIUS)**
  - 部分的802.11無線網路提供RADIUS身分鑑別的機制
  - 利用使用者輸入帳號及通行碼來辨認使用者的身分，確認通過之後，經過授權 (Authorization) 的使用者便可登入網域，使用相關資源，並可提供計費 (Accounting) 機制，保存使用者的網路使用記錄
  - 在使用者和RADIUS伺服器之間的通訊是加密保護的，但RADIUS 協定並不提供資料加密

Module 12-3-2:
WLAN通訊技術的安全機制（續）

- **RADIUS**



Module 12-3-2: WLAN通訊技術的安全機制（續）

- **Kerberos**
  - Kerberos可以安全的認證使用者是否可存取網路。使用者連結到伺服器去取得數位憑證 (Digital Certificate) 和一把加密使用的金鑰，還有一把交易金鑰 (Session Key)。交易金鑰是用在要求網路服務時，而數位憑證在協定中主要的功能是讓服務可以認證正在使用的使用者身分
- **802.1x 通訊埠基網路存取控制**
  - 802.1x是IEEE發布的一個安全協定，主要提供一個較安全的使用者認證和中央控管的安全模式。它限制使用者存取網路，除非是經由認證的使用者，否則人不可以使用網路。802.1x提供對WEP金鑰管理的修正改善，不過只有認證的部分，並沒有改善加解密的演算法

Module 12-3-3: WPAN通訊技術的安全機制

- **Bluetooth安全機制**
  - 在藍芽的安全機制上涵蓋幾個主要的元件，包含金鑰管理、加密和鑑別三個部分
  - 在每一個藍芽裝置中，有四個資訊用於維護連接層的安全性：
    - 藍芽裝置位址(Bluetooth Device Address)：每一藍芽裝置都有獨一無二的藍芽裝置位址，長度48位元
    - 私有鑑別金鑰(Private Authentication Key)：用於身分鑑別，為一128位元的隨機值
    - 私有加密金鑰(Private Encryption Key)：長度從8到128位元長度都有，主要用在加密
    - 隨機亂數(RAND)：長度128位元，由藍芽裝置所產生的

Module 12-3-3: WPAN通訊技術的安全機制（續）

- **Bluetooth之金鑰管理**
  - 連結金鑰是一個128位元長度的隨機亂數，主要的應用是在鑑別過程
  - 單元金鑰是當單一裝置被安裝時所產生的金鑰
  - 組合金鑰則是當有兩個藍芽裝置必須互相交易時所產生的一對金鑰，成對產生
  - 主金鑰是一把暫時性的金鑰，用來取代目前使用的連結金鑰。由於以藍芽建立的網路中，其中一個模式是所謂的主從模式，有一個主裝置。在此模式下，主金鑰可以在主裝置必須傳送給其他裝置時，用它加密
  - 初始金鑰是用在當一開始時根本沒有組合金鑰或單元金鑰時使用的金鑰，只用在初始階段

Module 12-3-3: WPAN通訊技術的安全機制（續）

- **Bluetooth之加密機制**
  - 藍芽加密機制主要是利用E0串流加密演算法來加密封包的資料 (Payload) 部分。E0串流加密演算法包含加密資料用金鑰產生器 (Payload Key Generator)、金鑰串流產生器 (Key Stream Generator) 和加解密演算法

Module 12-3-3: WPAN通訊技術的安全機制（續）

- **Bluetooth之鑑別機制**
  - 藍芽的鑑別機制使用兩回合擷問與回應方式，雙方必須先分享一把私密金鑰，在兩回合或兩個步驟下，便可以完成認證程序
  - 認證過程中，首先驗證者傳送一個隨機值進行認證要求。

    接著，雙方利用認證演算法E1，把剛剛傳送的隨機值、被驗證者的藍芽裝置位置和目前使用的連結金鑰當成輸入，產生一個回應值 (SRES)。

    被驗證者會傳送回應給驗證者，進行比對之後，相同便表示認證通過

Module 12-4:
行動付款機制

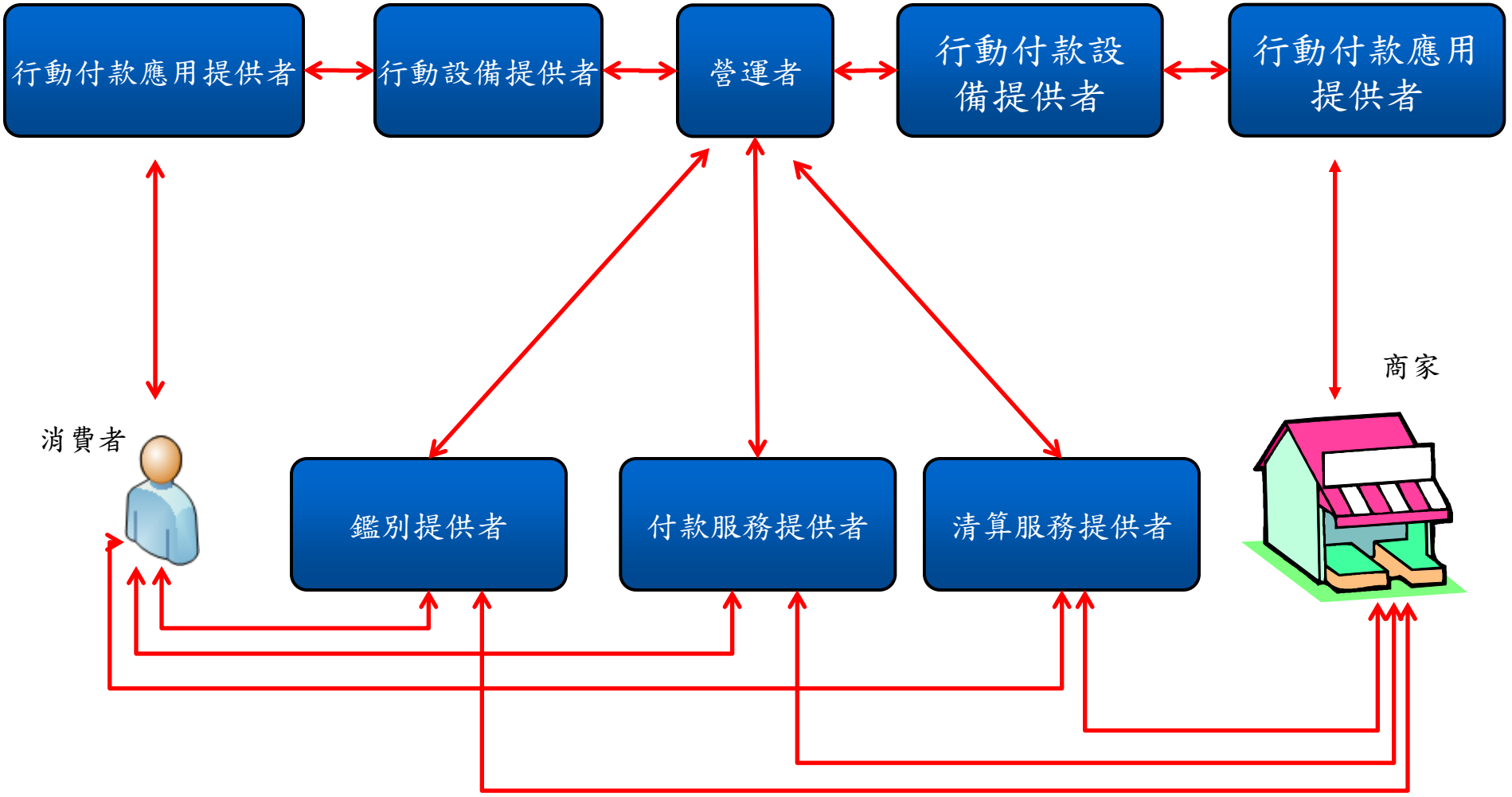
Module 12-4-1: 行動付款之定義

- 行動付款就是「透過手機或PDA 等行動通訊設備來做付款的動作」，也就是以行動裝置做為付款的工具
  - 不僅能使用於行動商務，還可以運用於電子商務及實體銷售點的付款
  - 使用者可以在任何時間、任何地點都能付款
  - 可應用在許多不同的場合，範圍由手機上的各種內容資訊，如遊戲、占卜、音樂、新聞，至飯店、餐廳消費費用，甚至是線上賭場的賭金等均可適用

Module 12-4-1: 行動付款之定義（續）

- 行動付款的主要特性如下：
  - 以行動裝置為主要付款工具
  - 可用以購買商品或是服務
  - 付款金額多寡因業者不同而有所不同
  - 可在實體世界或是虛擬的網路世界使用

Module 12-4-2:
行動付款之參與角色



Module 12-4-2: 行動付款之參與角色（續）

- 在整個行動付款中主要有以下幾個參與的角色，包含：
  - 消費者：利用行動裝置購買相關商品或服務的消費者
  - 商家：提供消費者所需的商品或服務的商家
  - 行動付款應用提供者：提供支援行動付款軟體或應用程式的業者
  - 行動設備提供者：行動裝置供應商，如Nokia、Motorola、Sony Ericsson等
  - 營運者：提供消費者行動通訊相關服務，如中華電信、台灣大哥大等

Module 12-4-2: 行動付款之參與角色（續）

- 行動付款設備提供者：提供商家處理行動付款所需之硬體設備
- 行動付款應用提供者：提供商家處理行動付款所需之軟體或應用程式
- 鑑別提供者：鑑別消費者是否為本人，也鑑別網路商家是否為真，以防止冒名的情形發生
- 付款服務提供者：將消費者的授權付款訊息傳送至相關的金融網路或機構，以幫助消費者及商家傳送付款清償訊息，完成交易，如VISA、Paypal等

Module 12-4-2:
行動付款之參與角色（續）

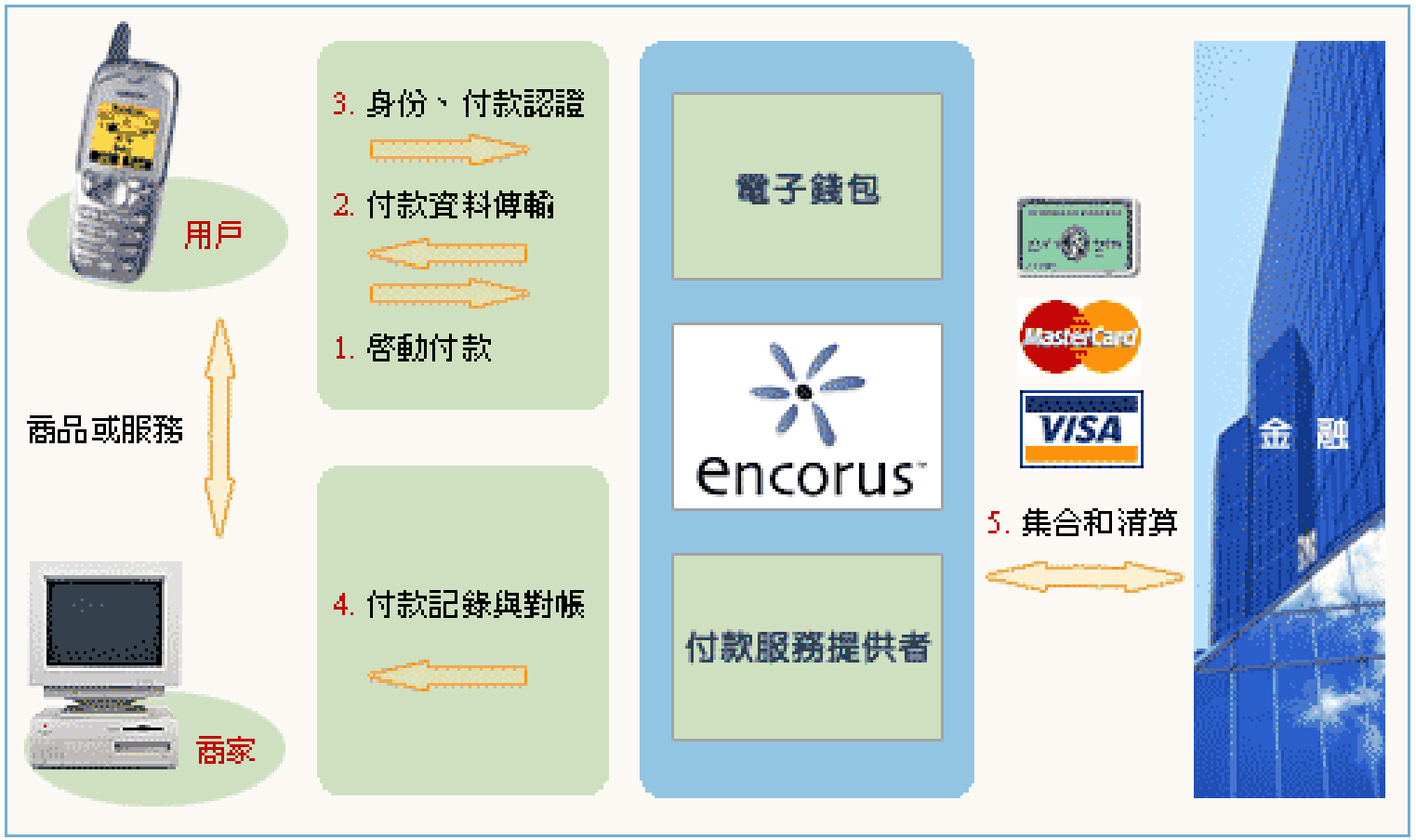
- 清算服務提供者：負責消費者與商家最後帳款的清償工作。消費者與商家會由自己的銀行機構代替其處理相關帳款事宜，其角色如同信用卡交易中收單銀行與發卡銀行的角色

Module 12-4-3: 行動付款基本流程

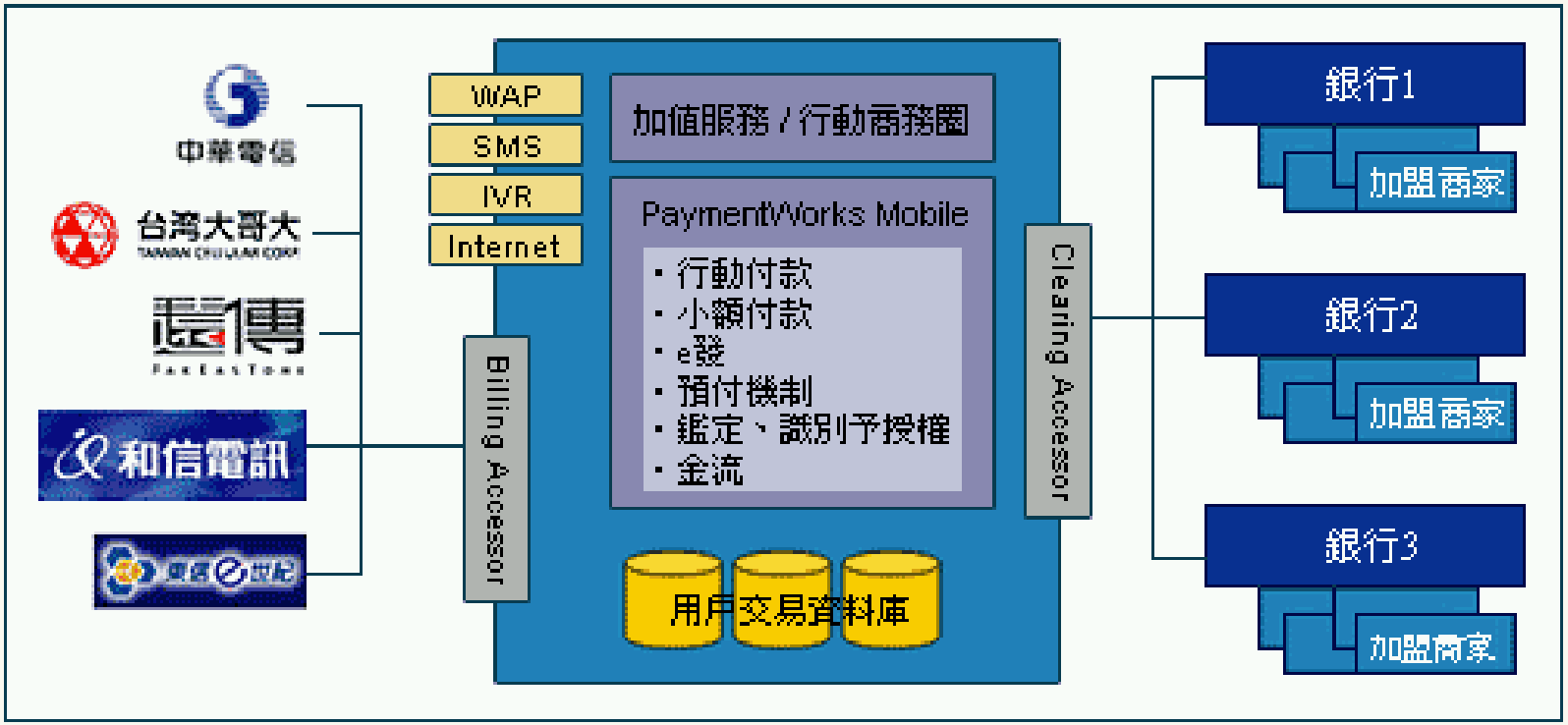
- 消費者決定要購買某個商品或服務，且利用行動付款進行結帳之動作
- 商家將消費者要購買的物品及消費者的行動電話號碼輸入傳送給鑑別提供者
- 鑑別提供者利用SMS 或是語音作確認，並要求消費者輸入PIN以作付款授權
- 消費者輸入PIN 之後，付款服務提供者會依消費者的授權向清算服務提供者要求付款之動作
- 消費者收到SMS 或語音後確認交易完成

Module 12-4-3:
行動付款基本流程（續）

- 行動付款架構與流程



Module 12-4-2:
行動付款之參與角色（續）



電　信	加　值　服　務	銀　行
• 延伸帳務方面的專業技術	• 擁有彈性化的付款系統	• 控制現有的付款基礎設施
• 開拓預付款項和小額付款的領域	• 擬定系統發展準則	• 擁有現成的企業客戶群
• 擔任中介的角色	• 開發應用程式和服務	• 擁有可靠的品牌與信譽
	• 組合內容	

Module 12-4-4:
現行的行動付款機制

- 目前國內外現行的行動付款機制可以透過使用的技術來分類，而這些技術主要有以下幾種，包含：
  - 單晶片 (Single Chip) 技術
  - 雙晶片 (Dual Chip) 技術
  - 雙插槽 (Dual Slot) 技術
  - 近端感應技術

Module 12-4-4:
現行的行動付款機制（續）

- 單晶片技術
  - 單晶片技術乃是使用單一晶片即可完成行動付款的所有流程。這個晶片可以是手機上原來的SIM 卡，有時則需向系統業者購買一張新的SIM卡，或是下載某些程式至原來的SIM 卡後才能使用
  - 使用單晶片的最大優點是消費者的轉換成本很低， 消費者需付出的成本常只是購買一張新的SIM 卡費用而已，不用更換手機，消費者接受的可能性較高，對行動付款的普及較有利

Module 12-4-4:
現行的行動付款機制（續）

- 現行單晶片技術的行動付款機制
  - 西班牙Mobipay
  - 丹麥mPay
  - Paypal

Module 12-4-4: 現行的行動付款機制（續）

- 雙晶片技術
  - 雙晶片技術乃提指除了原有的SIM 卡之外， 再加上一張與SIM 卡同樣大小的信用卡晶片 或是WIM (Wireless Identity Module)， 由銀行或是信用卡等金融機構所發行， 當消費者進行行動付款， 包含鑑別、授權及帳款消算過程均是透過第二張晶片與金融機構的後台主機相連， 因此能確保金融機構在行動付款過程中不被系統業者排除在外
  - 雙晶片技術的優點在於安全性較高，但對於消費者的轉換成本也較高，因為消費者必須申請第二張晶片卡，而且可能必須更換支援雙晶片技術之手機

Module 12-4-4:
現行的行動付款機制（續）

- 現行雙晶片技術的行動付款機制
  - 芬蘭EMPS

Module 12-4-4:
現行的行動付款機制（續）

- 雙插槽技術
  - 雙插槽技術乃指行動電話上除了原有的SIM 卡插槽之外，行動電話本身還有另一個插糟，可以插入一張含有晶片的信用卡、Debit 卡或金融卡，以進行行動付款，因此稱為雙插槽
  - 雙插槽技術亦具有安全上的優點，因與信用卡結合，因此可以直接運用信用卡的特約商店，可使用的場合及商家較多。但其缺點為消費者得購買新的雙插槽手機才能使用，轉換成本最為高昂
- 現行雙插槽技術的行動付款機制
  - 法國Paiement CB sur mobile

Module 12-4-4:
現行的行動付款機制（續）

- 近端感應技術
  - 除了使用手機作為行動付款裝置，目前近端感應技術也逐漸發展中，此技術主要是經由近距離無線感應的方式，來完成行動付款作業。常見的感應媒介有RFID、紅外線、藍芽、條碼及非接觸式智慧卡等
  - 近端感應技術也可以結合手機應用，成為另一種付款機制
- 現行近端感應技術的付款機制
  - 台北捷運悠遊卡 (RFID)
  - 香港八達通及日本Suica (FeliCa)
  - 日本NTT DoCoMo iMode FeliCa (FeliCa結合手機)

Module 12-5:
行動商務安全管理

Module 12-5-1:
無線通訊系統之風險與威脅

- 各種無線通訊技術皆存在著風險與安全威脅的問題，而此小節將介紹一般較常討論的風險與威脅

- 訊號分析 (Analysis)
  - 訊號分析指的是紀錄或監聽 (Eavesdropping) 通訊時在空中傳遞的RF訊號。通常訊號分析是無法避免的，只要在訊號傳輸範圍內的使用者皆可以監聽這些RF訊號，因此在無線通訊系統中資料傳輸的機密性變顯得非常重要

Module 12-5-1:
無線通訊系統之風險與威脅（續）

- 身分假冒 (Spoofing)
  - 所謂假冒有可能是攻擊者模仿成一個合法授權的使用者或者是行動裝置，企圖取得某些受保護的資源。例如在無線網路的環境中，攻擊者可能安裝一個惡意的AP，企圖取得使用者的鑑別資訊，然後透過此鑑別資訊，假冒成合法使用者到一合法的AP，來取得授權。這種攻擊手法又稱中間人 (Man-in-the-middle) 攻擊

Module 12-5-1:
無線通訊系統之風險與威脅（續）

- 阻斷服務 (Denial-of-Service)
  - 指的是攻擊者企圖讓某個行動裝置或者是整個網路無法進行通訊。攻擊者可能利用某些手法讓網路裝置無法回應或者是重新開機。在無線通訊系統中可透過訊號干擾 (Jamming) 的方式即可達成DoS攻擊，這種攻擊手法並不困難，有些無線網路的測試設備即具有訊號干擾的功能

Module 12-5-1:
無線通訊系統之風險與威脅（續）

- 惡意程式 (Malicious Code)
  - 所謂惡意程式的範圍包含有病毒、蠕蟲及木馬程式，可以感染網路裝置。目前已經有病毒可以感染在手機、PDA及智慧手機等行動裝置，雖然惡意程式在無線通訊系統中的發展才剛起步，但目前已經有好幾個種類的病毒產生
  - SPAM垃圾郵件也可以算是另一種惡意程式，雖然它的威脅較病毒來的小，但是其耗費的成本與資源也讓企業非常困擾

Module 12-5-1:
無線通訊系統之風險與威脅（續）

- 社交工程 (Social Engineering)
  - 社交工程通常被稱為是低階技術的駭客手法，通常是藉由人性的弱點或公司政策的漏洞來達成目的。攻擊者會誘使使用者洩漏各種資訊，包括帳號、密碼資訊等

Module 12-5-1:
無線通訊系統之風險與威脅（續）

- 行動電話的安全威脅
  - 手機要進行通話時會先廣播其行動識別號碼 (Mobile Identification Number, MIN) 以及電子序列號碼 (Electronic Number)，行動通信業者會透過這兩組號碼來比對是否為合法用戶。
    因此當這兩組號碼被攻擊者監聽到時，攻擊者便可以複製成另一支手機，以進行不法的行為
  - 透過一個指令 (Maintenance Command) 的下達，警方或政府即可在用戶不知情的狀況下監聽通話

Module 12-5-1:
無線通訊系統之風險與威脅（續）

- 無線網路的安全威脅
  - War Driving：驅車攻擊，指的是攻擊者利用開車的方式，對沿途的AP做刺探的動作，以收集AP的相關資訊，如SSID，使否使用WEP加密等
  - War Walking：概念同War Driving，但攻擊者是利用走路之方式
  - War Flying ：概念同War Driving，但攻擊者可能是駕駛私人飛機
  - War Chalking：指的是將上述刺探AP方法所收集到的資料，在地圖上做下記號，以方便他人使用的行為

Module 12-5-2: 安全管理政策（續）

- 要落實行動商務安全管理，可以透過安全政策 (Security Policy) 的制定與執行，避免安全威脅的發生，降低風險，便可以提高使用行動商務的安全性
- 安全政策的制定可以分為以下步驟：
  - 風險評估 (Risk Assessment)
  - 指導綱要 (Guideline)的建立
  - 產生Draft Policy
  - 驗證安全政策

Module 12-5-2: 安全管理政策（續）

- 風險評估
  - 風險評估是所有安全管理政策制定時的首要步驟。執行一個正確完善風險評估就可以找出目前所面臨的風險以及可以採取的風險控管，將風險降到最低
  - 執行風險評估最主要的目標有
    - 找出風險
    - 了解風險發生時可能產生的衝擊
    - 了解風險發生的頻率
  - 風險的量化分析可藉由風險係數評估法計算求得
    - 單一事件損失預期值＝資產價值*暴露因子
    - 年度損失預期值＝單一事件損失預期值*年度發生率

Module 12-5-2: 安全管理政策（續）

- 衝擊分析 (Impact Analysis)
  - 除了執行風險評估，亦必須進行衝擊分析，以了解當變異產生時所可能帶來的衝擊
- 指導綱要的建立
  - 在結束風險分析的程序後，資深管理階層(upper management) 必須建立指導綱要，羅列出各個風險並且對風險設定等級
  - 資深管理階層的參與對於安全管理政策的制定相當重要，否則制定出的政策可能無法達成目的

Module 12-5-2: 安全管理政策（續）

- 產生Draft Policy
  - Draft Policy必須藉由各個風險的測試結果以及如何控管以降低風險來產生
- 驗證安全政策
  - 產生Draft Policy後，便必須對Draft Policy進行驗證，可以讓其他的團體、部門或單位來檢驗Draft Policy，並且提供建議
  - 若大多數的團體都認可此Draft Policy，則代表此安全政策是可行的

Module 12-5-2: 安全管理政策（續）

- 無線網路安全政策領域主要可分為以下幾個：
  - 通行碼政策 (Password Policy)
    - 建立使用者通行碼的使用政策
    - 若只有單純要求使用者輸入一通行碼進行驗證，此方法可視為單因子 (One Factor)驗證，當系統要求使用者輸入的因子越多，則越可降低通行碼被破解的風險
  - 存取政策 (Access Policy)
    - 存取政策是無線網路安全政策中最重要的一環
    - 直接列出可被允許的裝置或使用者
    - 根據安全等級來建立存取機制

Module 12-5-2: 安全管理政策（續）

- 實體安全 (Physical Security)
  - 實體安全所探討的無線網路設備的實體安全，包含無線網路基礎建設以及終端設備，如AP、筆記型電腦等設備。這些設備可能遭到偷竊，造成組織的資產的損失
  - 如何管理這些設備避免偷竊即是實體政策的目標

Summary

- 行動商務概述
- 行動商務安全需求
- 行動商務安全機制
- 行動付款機制
- 行動商務安全管理

參考文獻

1. Aaron E. Earle, “Wireless Security Handbook ”, 2006.
2. Geoffrey Elliott, Nigel Phillips, “Mobile Commerce and Wireless Computing Systems”, 2003.
3. 唐正文，”802.11 無線區域網路通訊協定及應用 “，文魁資訊，民92。
4. 許建隆，長庚大學資訊管理系，行動商務課程資料。
5. 邱建清，建漢科技，”802.11無線區域網路技術回顧與展望”，民95年。
6. 廖建興，無線個人區域網路(WPAN)技術發展與應用概論。
7. 雷欽隆，范俊逸，”行動電子商務安全 “，國科會科資中心，民94 。
8. 邱榮輝，”數位憑證在行動商務之應用” ，行動商務安全與實務應用研討會，民95。
9. 尤國任，南華大學資訊管理系，行動商務課程資料。
10. 許巍瀚，”行動付款機制之分析” ，台灣大學碩士論文，民92。

References

- 教育部顧問室編輯 “電子商務安全”教材
- Turban et al., Introduction to Electronic Commerce, Third Edition, 2010, Pearson