# 安全層級

```

1.核心安全原則

1.1安全性六個基本原則

1.2目標與目的

1.3範圍

2.資訊安全

2.1資訊安全分類

2.2風險四個類別

2.3硬體安全

3.網路安全

3.1網路常見的安全性威脅

3.2防範網路詐騙

3.3InPrivate 資訊

3.4線上目錄中的隱私權

4.無線網路安全

4.1WLAN上的威脅

4.2替代方案

4.3安全使用無線網路

4.4安全措施

4.5評估安全性威脅

4.6無線網路上的安全性

4.7驗證

4.8設定管理

4.9.WEP WPA AND WPA2

4.10 SSID

```

## 1.核心安全原則

### 1.1安全性六個基本原則

```

1.識別

2.驗證

3.授權

4.機密性

5.完整性

6.不可否認性

```

### 1.2目標與目的

```

1.機密性

2.完整性

3.可用性

```

### 1.3範圍

```

1.人員安全

2.應用程式安全性

3.中介軟體安全性

4.作業系統安全性

5.硬體安全性

6.網路安全性

7.設備安全性

8.出口安全性

```

## 2.資訊安全

```

1.CAIN

2.Principle of least Privilege & Run as

3.Social Engineering

4.Attack Surface

5.Attack Surface Analyzer

```

### 2.1資訊安全分類

```

工作分類:

1.規劃

2.預防

3.偵測

4.回應

主題分類:

1.威脅和弱點減輕

2.身分和存取管理

3.安全性基礎概念

防護重點分類:

1.防毒

2.防駭

3.防災

4.防竊

```

### 2.2風險四個類別

```

1.入侵者

2.外來的威脅

3.內部威脅

4.意外及災難

```

## 2.3硬體安全

```

1.阻斷駭客進入網路

2.保護網路不受掃描

3.帳戶鎖定原則

4.安全性檢查清單

5.BitLocker

6.Access Control

7.身分和存取管理

8.Keyloggers

```

## 3.網路安全

### 3.1.網路常見的安全性威脅

```

1.偽裝

2.竄改

3.否認

4.資訊洩露

5.拒絕服務

6.提升權限

```

### 3.2防範網路詐騙

```

1.內建篩選工具

2.線上服務

3.內建舉報可以網站或詐騙的方式

4.驗證網站憑證

```

### 3.3InPrivate 資訊

```

1.資訊

2.Cookie

3.網際網路暫存檔

4.網際歷程記錄

5.表單資料和密碼

6.防網路釣魚快取

7.網址列和搜尋自動完成

8.自動損毀還原(ACR)

9.文件物件模組(DOM)存放裝置

```

### 3.4線上目錄中的隱私權

```

張貼任何資訊前

1.謹慎挑選

2.線上購物辨明來源

3.仔細閱讀網站的隱私權聲明書

4.只在知名人力網站張貼履歷表

5避免參加抽獎或其他行銷活動

6.找出自己被那些目錄列出

7.要求線上目錄移除您的名字

8.申請不列表的電話號碼

9.設立特定電子郵件地址專供線上活動使用

10.做紀錄記下您提供個資給哪些公司

```

## 4.無限網路安全

### 4.1WLAN上的威脅

```

1.竊聽

2.攔截和修改傳輸的資料

3.欺騙

4.拒絕服務

5.自由負載

6.意外的威脅

7.異常的WLAN

```

### 4.2替代方案

```

1,不部署WLAN 技術。

2,仍然使用802.11靜態WEP 安全性。

3.使用VPN保護WLAN 上的資料。

4.使用IPsec保護WLAN 傳輸。

5,使用802.1X驗證和資料加密技術來保護WLAN。

```

### 4.3安全使用無線網路

```

1.保證無線路由器或者存取點管理連接安全

2.不要廣播SSID

3.使用wpa代替wep

4.使用mac過濾入口控制

5.降低無線區域網路發射器的功率

6.進用遠程管理

```

### 4.4安全措施

```

1.密碼

2.防毒

3.Flash ROM

4.加密

5.必要的資料

```

### 4.5評估安全性威脅

```

1.竊聽

2.攔截和修改傳輸的資料

3.欺騙

4.Dos

5.自由負載

6.意外的威脅

7.異常的WLAN

```

### 4.6無線網路上的安全性

```

下列安全機制可增強無線網路的安全性:

1.Windows 防火墻

2,802.11身分確認和驗證

3.802.11有線等位私密(WEP)加密

4.Wi-Fi Protected Access ( WPA)

5.802.1X authentication 802.1X 験證

6.802.1X驗證的IAS支援

```

### 4.7驗證

```

1.眾所皆知的方法

例如:密碼

2.現有的工具

例如:智慧卡或SecurID卡中的安全憑證

3.身分識別

例如:指紋

```

### 4.8設定管理

```

1.備份檔案

2.Pc上的資料

3.網路伺服器上的資料

4.在安全的公司網頁上展示還原程序

```

### 4.9.WEP WPA WPA2

#### WEP

```

WEP 有線等效加密 (Wired Equivalent Privacy),

又稱無線加密協定(Wireless EncryptionProtocol),簡稱WEP,

是個保護無線網路(Wi-Fi)訊息安全的機制。

因為無線網路是用無線電把訊息傳播出去,它特別容易被竊聽。

WEP的設計是要提供和傳統有線的區域網路相當的機密性,而命名的。

密碼分析學家已經找出WEP好幾個弱點,

因此在2003年被實現大部分 EEE 802.11i標準的 Wi-Fi Protected Access(WPA)淘汰,

又在2004年由實現完整EEE 802.11i標準的 WPA2 所取代。

```

#### WPA

```

WPA Wi-Fi 保護存取規格(Wi-Fi Protected Access' WPA)

由Wi-Fi聯盟與EEE聯手推出的Wi-Fi強化版安全規格,

用以取代既有但安全性較差的WEP標準。Wi-Fi產品目前多採用所謂的WEP 加密機制來提供無線上網的安全性

IEEE 802.11i 標準已正式取代WEP 和原始EEE802.11標準的其他安全性功能。

Wi-Fi保護的存取2(WPA2)是透過Wi-Fi Alliance使用的產品憑證,

可以將無線設備認證為與 EEE802.11i標準相容。

```

#### WPA2

```

WPA2 憑證的目標是支援EEE802.11i標準的其他必要安全性功能,而支援WPA的產品尚未併入這些功能。

例如,WPA2需要TKIP和AES 加密支援。

WPA2 具有兩種不同的模式:

WPA2-Enterprise 使用802.1X 驗證,是針對中型和大型基礎結構模式網路所設計。

WPA2-Personal使用 PSK進行驗證,是針對SOHO基礎結構模式網路所設計。

```

### 4.10 SSID

```

服務組織別元(SSIDㆍService Set Identifier)ㆍ

32 個字元長度的字母、數字或符號所組成。

同一個服務組的設備可以使用SSID來驗證另外一個網路設備是否為同一個群組。

這個無線網路的名稱或識別碼,它可以是任何字母(可包含大小寫字母)和数字所構成的字串,最長可輸入32個字元。

無線網路基地台的製造商會在出廠時預設SSID碼,

但建議你更改這個設定來防止侵入者,或避免附近使用同型式之無線網路基地台的鄰居,意外地進入你的無線網路。

基本服務識別組(BSSID):

1.基本服務識別組(BSSID):表示AP的MAC地址

2.擴展服務識別組(ESSID):一個最長32位元組區分大小寫的字元串,表示無線網路的名稱

```