行政院所屬各機關因公出國人員出國報告書

（出國類別：專題研究）

資訊系統安全管理及維護專題研究報告

出國人　服務機關：總統府

職　　稱：分析師

姓　　名：蘇憶湘

行政院研考會編號欄

出國地點：美國

出國期間：八十八年三月二十八日至

八十八年九月二十七日

報告日期：九十年四月二日

資訊系統安全管理及維護專題研究報告

摘要

總統府在資訊應用方面，內部區域網路主要是應用於公文管理系統及辦公室自動化相關應用系統；網際網路方面，則是以提供民眾查詢總統、副總統及本府相關資訊為主要目的。內部區域網路與網際網路之間則架設一道封包過濾式防火牆，防範網路駭客侵入本府網路，及避免本府員工透過網路危害公文資訊安全。因此，如何建立一個安全及可信賴的資訊應用發展環境，確保資訊作業順利運作，維護本府公務資訊安全，為本府未來資訊業務發展最重要之課題。另，根據「政府網際服務網」統計，本府網站為政府三大熱門網站之一，因此，本府資訊安全管理工作，除保護內部資料之外，在政府機關資訊安全防護工作上，亦深具指標意義。

本報告主要內容如下：

一、心得部分：系統安全概念、威脅資訊安全的型態、安全防護技術、密碼系統、防火牆、資訊安全政策、安全維護原則等。

二、建議部分：從技術面、管理面、制度面考量本府資訊安全管理及維護策略，期於完善的資訊安全措施及合理的使用規定下，建立本府資訊應用規範，確保資訊作業順利運作，維護資訊安全。

目　次

壹. 研究目的

總統府自八十四年起開始使用區域網路，系統採主從式、小型化之開放系統架構，另為配合行政院資訊基礎建設計畫（NII），於八十五年二月由李前總統啟用「總統府全球資源網」，本府資訊網路於是走向 Internet/Intranet 架構。在資訊應用方面，內部區域網路主要是應用於公文管理系統及辦公室自動化相關應用系統；網際網路方面，則是以提供民眾查詢總統、副總統及本府相關資訊為主要目的。內部區域網路與網際網路之間則架設一道封包過濾式防火牆，防範網路駭客侵入本府網路，及避免本府員工透過網路危害公文資訊安全。

本府資訊系統建置初期是以資訊應用之方便性為主要之考量方向，然在廣泛應用各項資訊科技及數位化的同時，就分散式主從架構所引發之安全管理風險而言，單一防火牆之安全防護機制，似有不足之處。因此，如何建立一個安全及可信賴的資訊應用發展環境，確保資訊作業順利運作，維護本府公務資訊安全，為本府未來資訊業務發展最重要之課題。另，根據「政府網際服務網」統計，本府網站為政府三大熱門網站之一，因此，本府資訊安全管理工作，除保護內部資料之外，在政府機關資訊安全防護工作上，亦深具指標意義。

歐美國家早期對資訊安全相當重視，因此在相關技術方面投入了相當多的研究，有鑒於此，乃決定前往美國研究相關資訊安全防護機制，期能就本府現行安全問題，提出資訊安全管理及維護方案，以做為未來本府訂定資訊安全管理制度及推動各項應用系統之參

考。

貳. 研究過程

一. 進修部分

八十八年三月自九月參加美國西雅圖 City University 春夏季班課程，該校係以建教合作為主要教學宗旨，大西雅圖地區著名的微軟及波音公司均有員工在該校進修。在該校，我主修 client/server 有關之資訊安全課程，並請該校電子商務專案主持人 Mohan Rao 教授指導，並配合學校之電腦設備及應用環境，選定資訊安全相關技術為研究重點（研究報告如附件一）。

二. 參訪部分

透過美國農業部安排，自 88 年 9 月 14 日起至 28 日止進行為期二週之參訪行程（議程如附件二），參訪單位包括政府及民間單位，參訪行程詳如下表：

日期	地點	單位	參訪對象
9/14~ 9/15	Dallas	EDS Headquarters	Mr. Frank Liu Director of Us Marketing Support
9/16~ 9/19	Washington DC	Department of Justice The Federal Computer Incident Response Capability	Mr. Stevan D Mitchell Tria Attorney Mr. Dave Adler General Services Administration Ms. Judy L. Donsworth Telecommunications Specialist
9/20~ 9/25	New York	Information Systems Security Association	Mr. Jim Duffy Prseident

9/26~ 9/28	Minneapolis	Secure Computing Corporation	Mr. George Jelatis Professional Services Group

參. 研究心得

一. 系統安全概念

資訊安全防護範圍包括硬體、軟體、資料等，防護目標如下：

（一） 確保資料及系統資源的機密性(secrecy)、隱私性(privacy)，且限定被授權的人員才能使用。

（二） 確保資訊系統真確性(precise,accurate)、完整性(integrity)，不會被意外地或蓄意地改變或毀損；處理更改時，能維持一致(consistent)、有意義(meaningful)且正確(correct)的結果。

（三） 確保資料與系統服務之可取用性(availability)，可及時回應(timely response)、公平配置(fair allocation)、容錯(fault tolerance)等。

二. 威脅資訊安全的型態

(一) 中斷(interruption)

惡意破壞硬體設備、刪除程式或資料檔、或阻絕作業系統服務(denial of services)，使系統資源遺失、不可取用、不堪使用。

(二) 截取(interception)

未經授權接取系統資源、拷貝程式及資料、或截聽網路。

(三) 更改(modification)

未經授權更改系統資源、儲存或傳輸資料之數值、使程式執行額外運算。

(四) 仿造(fabrication)

未經授權仿造資料、插入額外的交易訊息、增加資料記錄，使得資料使用者無法分辨真偽。

三. 常見的攻擊方法

(一) 密碼被破解或偷竊

許多系統可以讓系統的一般使用者透過 Telnet、FTP 或 NIS...等服務存取系統，然而登入密碼的同時，非系統的使用者也可能獲得密碼資料。雖然大部分的密碼資料都經過加密，使得資料無法由人直接閱讀，但仍有特別的程式可以算出部分系統密碼。

(二) 人與人之間的社交活動

有些人透過電子信件溝通時，告訴自己的朋友或商業夥伴自己在某一系統使用的密碼，方便他讀取資料，而洩漏了自己的密碼。

普通的電子郵件未經加密處理，有心人很容易從中獲得侵入系統的資訊，或是藉由與他人在線上交談(Talk,Chat,IRC)，偷窺到在聊天中一些不宜公開的資料。

另外有種情況是騙取系統管理者的密碼，託故需要系統管理者使用特殊權限的帳號：例如忘記密碼，要管理者更改密碼，或製造不正常狀況...從而取得特殊權限的帳號。

(三) 程式本身的問題或被留後門(Backdoors)

這兩種情形的差別在於前者是無意，後者是有意。程式本身的問題，在網際網路上有個案例發生在 1988 年，利用 send mail 及 finger 兩個程式的問題，侵入其它在網際網路上的電腦，造成許多電腦癱瘓。留後門，是程式設計師方便自己進入系統，有名的例子是 C 語言父親 Ken Thompson：使用他寫的 C 語言編譯器來編譯 login 程式，便會造出後門，可讓 Thompson 進入系統。

(四) 確認系統問題

部分辨識使用者的確認系統，其設計可能不符合現在的環境。例如以 IP Address 做為辨別使用者的系統，自從 PC 出現便使得這種系統可靠性大大降低，因為 PC 可以很容易變更其網路位址。單是用密碼辨別使用者的系統，事實上並不安全，利用 PC 可以容易取得網路上的封包資料，進而分析出資料中的密碼。

(五) 通訊協定(Protocol)的漏洞

大部分網際網路的通訊協定設計之初,並沒有特別的保護.使得

傳遞的資料容易被人修改，然後得到控制權，獲得不應被取得的資訊。除了通訊協定被修正,許多加密系統的出現，才讓使用增加了可靠性。

(六) 資訊洩漏

有些人喜歡用生日、電話...等週遭相關的資料做設定密碼的依據，而 finger 所顯示的資訊，正好就是以上這些。因此成為猜密碼者很好的工具。同樣的在 W3 上，擺個人的首頁(Home Page)也很容易透漏以上這些訊息，成為猜密碼的人一種資訊的來源。

還有一些入侵者會透過 DNS 來查詢機器，因此除了 Gateway 的機器，最好不要把所有機器資料都放在同一 DNS。另外，建立對內 Cache 式的 DNS，也是一個辦法。

(七) 叛逆心態

有些人天性喜好破壞，就像刮汽車、砸玻璃一般。在網路上也有人以塞破別人信箱或是把 FTP site 塞滿檔案...為樂。因此最好將這些資料與系統運作的空間分開，以避免遭受破壞。另外，許多不正常的動作都會使系統的記錄檔(log)非快的增大，而影響到系統正常運作，這也是要注意的。

四. 安全防護技術

(一) 密碼系統

要確保通訊雙方在網路上傳送訊息的機密性，最基本的方法即

是使用密碼系統，讓訊息在發送之前先經過加密處理後再進行傳送，而達到接收方時再予以解密，以回復原來的內容。透過訊息鑑別碼或數位簽章機制，防制傳輸或儲存訊息遭受非授權之更改、刪除、假冒、替代。使得公正的仲裁者可以利用這些證據來解決糾紛，防制通訊雙方彼此否認曾經接收或傳送訊息。現代密碼系統的加密/解密轉換以及簽署/驗證程序大多植基於數學上的計算難題，例如排列(permutation)、分解因數(factorization)、計算離散對數(discrete logarithm)等問題。密碼系統可以依據加密過程中，加密金匙與解密金匙是否相同，分成單一金匙系統（single-key cryptography）與公開金匙（public-key cryptography），或稱「對稱性」及「非對稱性」金匙。

1. 對稱密碼系統（symmetric）

one-key 之加解密系統，加密金鑰與解密金鑰相同，加密金鑰與解密金鑰需保持秘密(密鑰)，因其速度較快，適合大量資料處理，及應用於保護個人檔案及傳輸資料。

2. 非對稱密碼系統(asymmetric)

two-key 的加解密或數位簽章系統，加密或簽章驗證金鑰為公開金鑰(public key)，簡稱公鑰，解密或簽章產生金鑰為私密金鑰(privatekey)，簡稱私鑰，公鑰與私鑰必須存在一個關係，使得由公鑰去推導私鑰是計算上不可行，因其速度較慢，適合少量資料處理，及網路系統環境。

(二) 防火牆

1. 類別

防火牆(firewall)用來分隔內部網路與外部網路(一般就指網際網路)。從外部網路要使用內部網路的機器，必須經過防火牆，使得內部機器不被外界透過網路任意連接使用，市面上防火牆可分為三類：封包過濾(packet filitering)、應用層閘道(application gateways)、電路式閘道(circuit gateways)，這三種方法並不互斥，許多人都選擇同時使用。

(1) 封包過濾(packet filitering)

這是種最便宜，而且蠻有效的方法。大部分擔任路由器的軟、硬體都提供上述功能,毋須另外花費。

內部對外溝通是透過路由器(router)傳遞封包，這種方法就是針對封包的標頭(head)加以查核，檢查封包的來源、目地以及埠址(port,可當做是服務的種類,如:telnet,ftp...)。可過濾外部到內部、內部到外部或兩者都用。

(2) 應用層閘道(application gateways)

應用層閘道是屬防火牆裡極端的設計，它並不使用原本通用的傳遞資料方式，而是特別設計過，看起來似乎是多此一舉，但比其它方法都有用，一點也不用單心外面環境如何，因為它是獨立存在。正由於它的複雜，一般只選擇幾種服務來做。

應用層閘道另一個優點是縱使在十分危險的環境，而它依然可

以記錄所有進、出系統的資料，是對抗電腦駭客十分有用的武器。

(3) 電路式閘道(circuit gateways)

電路式閘道用來傳遞 TCP 連接。當要連接內部網路某台電腦，必須透過電路式閘道，不是直接傳遞封包。這樣的設計，是必須修改使用者目前所使用的程式，才能適用這環境。

2. 防火牆功能需求

.一個 Firewall 基本上必須達到下列三方面要求，才能成為一種保護模式，確保這道防線不被突破。

(1) 防止保密性的資料被存取方面

- 認證功能：使用者在通過防火牆之前，須先行通過認證並輸入密碼，以確保合法使用。認證方法如明文靜態密碼、一次密碼、時間記號密碼、以及口令與回答式密碼等。

- 加密功能：將機密性資料加密（如 DES 演算法），在網路上以亂碼傳遞。

- 過濾功能：動態地決定在封包層裡那個網路封包允許進出內部網路和 Internet，決定使用者可以使用哪些 Internet 服務及 Web 站台。

- 代理功能：代理內部網路與公眾網路間之連接，所有活動均由防火牆代理執行。對外部網際網路的資訊需求皆透過此代理伺服器

代為處理，實際上內部網路並沒有直接與外部網際網路連接，而是透過代理伺服器間接的得到資訊。

(2) 記錄及分析可疑的資料存取方面

- 記錄功能：對所提供服務的合法及非法的使用情形都有詳細的記錄，並提供例外報告及記錄精簡的功能，以保留足夠的審計軌跡作為事後稽核之用。豐富的日誌記錄(logging)功能可以詳細追蹤任何從外面想要入侵您網路的企圖。

- 郵件複製功能：將來往的信件留存一份當副本存查以便將來稽核。

- 稽核(Auditing)功能：藉由稽核裝置檢視使用者傳送的封包數或連線時間，因每日進出防火牆所記錄下的記錄相當多，故利用紀錄分析程式來篩選出有問題的紀錄避免人為的疏失。。

- 訪客分析：可對本府全球資訊網的使用情形做分析與統計報表，使管理單位瞭解有那些網頁是外界使用者最有興趣的網頁。

- 內部使用者使用分析報表：可分析內部使用者對網際網路的使用情形，例如可知道府內同仁最常去的網站有那些，最常使用網際網路的人是誰，及某一使用者的網際網路使用情形。

⑶ 入侵行為防制及提出警告方面

- 監聽功能：隨時偵測攻擊，並針對不同的情形提供不同的反制動作，例如當外界某部主機在試圖找出系統漏洞而被拒絕 3 次後，即將此外部的主機列為拒絕往來戶，不再接受其任何的存取。以保護本府網路的安全。

- 警告功能：提供及時警告的功能，當有入侵行為發生時，能夠對系統管理者提出警告。而所提供的警告方式可由系統管理者來定義。管理者可以針對每個稽核事件設定警報，警報可直接顯示在控制台上、存入檔案、寄送電子郵件、攜帶型傳呼器等。

- 防止郵包炸彈攻擊：將郵件伺服主機與全球資訊網主機分離，避免因外界的郵包炸彈攻擊而造成全球資訊網無法使用。

- HTTP、FTP 及 SMTP 檢測功能：過濾容易入侵的 Java 小程式及 ActiveX 的活動、FTP 及 SMTP 所傳送的檔案，透過病毒碼檢測來檢視其傳輸內容。

五. 資訊安全政策

建置一完善的資訊安全防禦體系並不僅是成立安控部門、購買一些安控軟體、加解密與防火牆工具就可以完成的，其中最重要的工作也最為大家所忽略者就是資訊安全政策(Security Policy)。

一個良好的安全政策可以形成企業由上到下對安全要求的共識，區分出各種有形、無形資產需要保護的等級與優先次序，企業可將有限的資源用在最需要的地方，此外系統管理人員也有所依循而知道什麼該管制、什麼可放鬆。資訊安全政策因每個企業之業務、規模、文化、人員、都不相同，並無標準範本可供循。制訂資訊安全政策時，企業應根據自己的需求及考量下列因素：

- 成員之代表性，包括高階主管、稽核、安控人員、系統管理、使用者…等。
- 資訊分級及其保護措施，例如：一般、內部參考、機密。
- 企業可承受的風險 (Asset、Threat、Vulnerability、Loss、Safeguard)。
- 落實機制，例如：政策規定 Internet 之使用僅限於公務，而落實機制可以是每日針對防火牆 Log 產生分析報表並公佈之。
- 明訂責任。
- 政策修訂辦法及其更新頻率。

六. 安全維護原則

資訊安全指導原則如下：（OECD 1992 年訂定）

(一) 責任原則（Accountability Principle）

資訊系統擁有者、提供者、使用者及其他有關人員所應負責任應該明確。

(二) 意識原則（Awareness Principle）

為了促進資訊系統擁有者、提供者、使用者及其他有關人員對於資訊系統的信心，他們應該隨時能夠適當地了解及被告知與維護資訊系統安全相符合的安全的措施、實務應用及處理程序等知識。

(三) 倫理原則（Ethics Principle）

資訊系統及其安全應該在遵重他人的權利及合法利益的方式下被提供及使用。

(四) 多學科原則（Multidisciplinary Principle）

資訊系統安全的實務措施及處理程序應該考慮技術、商業、教育及法律等層面。

(五) 相稱原則（Proportionality Principle）

資訊安全之等級、成本、保護措施、實務應用及處理程序應該是適當的，且與資訊系統的價值及對該項系統的依賴程度是相稱的；當安全的需求隨著特定系統而改變時，應與資訊系統的重要性、受傷害的可能性及內容是相稱的。

(六) 整合原則（Integration Principle）

資訊系統安全措施、實務應用及處理程序間、組織內其他措施、實務應用及處理程序等，應該是相互協調一致及整合的，這樣才能構成一個致性及連貫性的安全系統。

(七) 及時原則（Timeliness Principle）

國內及國際上的公私部門應該及時及相互協調採取行動以防止資訊安全事件，並對於違反資訊安全的行為有所反應。

(八) 定期評估原則（Reassessment Principle）

當資訊系統及安全的需求在經過一段時間有所改變時，資訊安全系統應該定期地被重新評估。

(九) 民主原則（Democracy Principle）

資訊系統的安全應與民主社會中的合法使用資訊及資訊自由流通的原則一致。

肆. 研究建議

本研究從政府網際網路應用趨勢及本府實際使用狀況，從技術面、管理面、制度面考量本府資訊安全管理及維護策略，期於完善的資訊安全措施及合理的使用規定下，建立本府資訊應用規範，確保資訊作業順利運作，維護資訊安全。

以技術來克服安全問題是最有效的方法，因此，首先是在技術工程上建議加強現行防火牆功能，加強連線內容安全檢查機制，及新增網路防毒主機；其次是管理機制的制定，包括使用者、系統、委外、設備及突發事故的管理；在制度方面，則是檢視現今的規定，

制定有效的規範。

一. 提昇防火牆

(一) 本府現行防火牆安全防護機制

本府現行防火牆安全防護機制，係使用一道防火牆及二部路由器進行防護，安全設定方式說明如次：

1. 連線設定

藉由路由器的設定，將本府網際網路連線切割成下列三個網路區段：

- 外部網路。
- 總統府全球資訊網。
- 內部網路。

2. 進出管制

藉由防火牆之封包過濾（Packet Filtering）功能，設定進出管制：

- 「外部網路」用戶僅能查詢「總統府全球資訊網」資訊及寄送電子信件。
- 開放「內部網路」部分個人電腦於「總統府全球資訊網」及「外部網路」查詢資訊，但禁止傳送檔案至外部網路。

3. 虛擬網址

藉由防火牆之位址轉換（IP Translation）功能，設定虛擬網址：

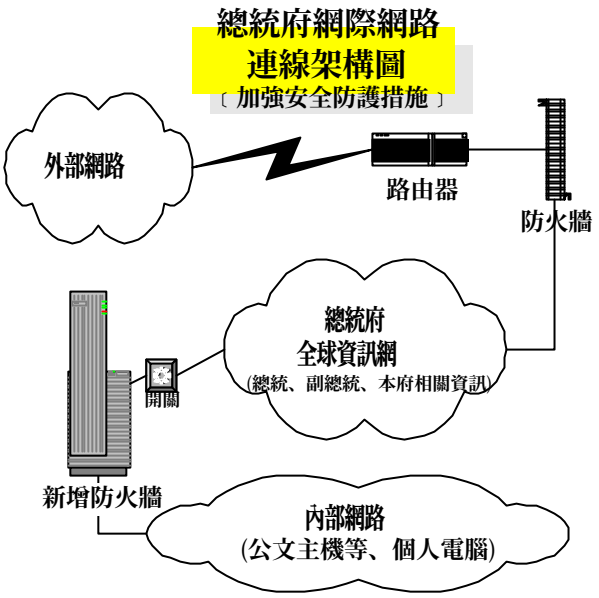
- 內部網路各主機及未開放上網之個人電腦，一律使用虛擬網址，使外界無法連結。
- 已開放上網之個人電腦查詢外部網路資料時，始由內而外單向轉換成實際網址。

(二) 現況問題

問題類別	現況問題	說明
連線設定	一、內部網路以路由器分隔，安全性不足。	路由器是以過濾網路資訊方式隔離網路，安全防護層次遠低於防火牆。本府內部網路所傳遞資訊包含重要文書資料，應以較嚴密之防護機制加強安全防護。
	二、內部網路於下班時段，仍處於連線狀態，增加安全顧慮。	本府現行防火牆防護範圍包含總統府全球資訊網及內部網路，因此，內部網路於下班時段雖無人使用，但仍然與外部相通，無人監控。
進出管制	一、無法長期追蹤外部網路用戶使用狀況，進行事前防護。	外部網路用戶連結本府全球資訊網次數，每日約一萬筆，由本科以人工檢查及研判方式，每日追蹤可疑紀錄，但因紀錄量大，只能採抽樣檢查方式，無法以全部紀錄進行完整分析，並就可能攻擊，進行事前防護措施。
	二、無法統計、追蹤府內使用狀況，以落實內部安全管理。	無法統計全府網際網路通信量，及選定特定對象，追蹤其目的地、傳輸內容等資料。
	三、現行防火牆為網址識別型防火牆，被突破機會較高。	防火牆區分為網址識別型防火牆及使用者識別型防火牆二種類別，本府目前所採用之防火牆屬於前者，儘以收發位址識別方式管制進出；而使用者識別型防火牆則是以人員識別為主要防護方法，識別項目包括密碼、來源地、目的地、使用型態，檢查項目多於現行防火牆，安全性高。
虛擬網址	一、開放連網之個人電腦，對外使用真實位址，有安全疑慮。	府內電腦向外界查詢資料時，由內而外單向轉換成實際位址後，建立連線（類似電話線點對點通信），易洩漏內部環境。

(三) 建議加強方案

本府現有防火牆機制著重於對外防護功能，防護面包含全球資訊網及內部網路，兩者以路由器區隔，防護面雖廣，然亦造成安全管理盲點。為加強本府內部網路安全，建議增設第二道防火牆（如右圖），與現有防火牆共同運作，解決現況問題，加強本府文書機密及網路的安全性，有關新增防護設施說明如下：



1. 連線設定方面：

- 內部網路與全球資訊網之間以不同廠牌防火牆隔離，加強防護。
- 兩個網域名稱伺服器：支援多重防火強架構，透過多層次(Multi-layered)安全性功能保護內部網路。分開的兩個網域名稱伺服器功能(split DNS Domain Name Server)可隱藏更多資訊，一個網域名稱伺服器負責與外部網路溝通，另一個網域名稱伺服器負責與內部網路溝通，因此，可防止外部網路主機看到或突破內部網路。
- 設定連接時限(connection time out)：限制連線時間的長短，超過

時限即自動斷線。

- 裝置定時開關：非上班時間自動切斷府內網路與網際網路之連線，以減少被攻擊的可能性。於設定時間內才建立府內網路與網際網路的連線，非上班時間則自動切斷府內網路與網際網路之連線，如此可將府內網路隔絕於 Internet，以減少被攻擊的可能性。

2. 進出管制方面：

- 於現有防火牆安裝訪客分析軟體，分析、歸納所有防火牆進出紀錄，自動提供分析報表與異常狀況報告，使防火牆的系統管理者掌握各種狀況。
- 增設府內使用網路追蹤軟體，紀錄傳輸內容、郵件備份存查、使用時間、目的地等資料，並定期自動產生稽核報表。
- 為確保合法使用，使用人應輸入密碼並定期修改。

3. 虛擬網路方面：

- 府內網路使用者均經由單一通道並透過代理人，查詢外界資料。
- 位址隱藏功能：起始主機名稱會被替換，以隱藏內部網路架構。例如，電子郵件送出前，其內部的網域名稱及使用者帳戶會被替換，以隱藏內部網路架構，避免防火牆被偵知而成為被攻擊的目標。不但保護隱藏在防火牆之後的內部系統，也保護防火牆本身。
    - 提供 MAIL HUB 功能：以防火牆之 Domain Name 為對外代表，防止洩漏內部環境。

二. 加強連線內容安全檢查機制

防火牆係以識別使用者身分方式管制網路連線，對於連線內容不作檢查，根據統計，只有約百分之三的網站使用相關安全工具偵測到非法入侵，其他約百分之九十七的網站根本不知道是否被非法入侵。因此，為避免入侵者藉由防火牆所允許之連線方式暗中進行破壞，應善用安全管理工具，增購主動式網路防衛軟體，提供反向查詢追蹤、傳輸內容稽核、主動斷線等功能。

- 加強網路安全稽核，對於網路系統管理人員的操作及通過防火牆系統之相關資訊，均應建立詳細的紀錄。同時建立網路安全警示系統，當有不明的使用者連續嘗試侵入時，系統自動發出警示訊號，讓網路系統管理人員在網路安全事件發生時，及時獲得警示性的訊號，俾利採取有效的防範措施，減少網路安全事件的發生。
- 安全稽核可偵測違反資訊安全政策的事件，以達嚇阻不法及入侵偵測的雙重目的，並可對未來稽核查詢系統加入經驗法則加強其入侵偵測的能力。建立正確完整的稽核紀錄可協助重建事件的真象，讓管理者檢視系統安全的弱點，並據以評估違反資訊安全政策事件所造成的損害。安全稽核的資訊應包括日期、時間、使用者、身分辨識確認、事件類別（如變更安全設定、重新啟動關機、程序追蹤等）、成功或失敗、物件名稱等。

- 遠端監視功能：在監視螢幕上，每一筆傳輸狀態都能一目了

然。若有人違反網路安全政策，警告標誌會顯示於此螢幕上。警告標誌通常包括了嗶嗶聲、螢光幕閃爍、或是改變 icon 的顏色。這些 icon 可以自由選擇其次序，或是依照其英文字母的順利、或是依照數字之先後順序而有不同的選擇。遠端因警告而被鎖住的檔案，也可以從螢幕上觀看其內容。警示(Alerting)功能能夠讓系統管理人員馬上知道網路是否正遭受攻擊，以便採取適當的行動。

- 管理功能：以 GUI 介面使用各種樣板(Template)來產生、修改及刪除 NameServer 之各式 records，確保 records 是以正確語法寫回 NameServer 資料庫。
- 備份及回存的設定功能：定時儲存及復原之前的設定，以回復被破壞前的狀態。
- 模擬攻擊：即模擬外界可能的攻擊行為對本府的防火牆進行安全性的測試，以測出可能的安全漏洞，並修補其漏洞，增強本府防火牆的安全性。

三. 新增網路防毒主機

由於全球資訊網瀏覽器的安全漏洞及使用者可能從網際網路下載到病毒軟體及有害程式等原因，防範電腦病毒亦為資訊安全管理重要的一環，對於電腦病毒及惡意軟體之防範，應採事前預防及保護措施，進行偵測及防制，以確保系統正常運作。本府目前並無網路掃毒機制，應於本府網際網路入口處新增網路防毒主機，掃瞄進入本府網路之封包（HTTP、FTP 及 SMTP），及早偵測及掃除電腦病毒。

四. 安全管理方面

「徒法不足以自行」，隨著資訊科技與 Internet 快速進步與更新，企業全面應用資訊系統技術於各個業務局層面，其智慧財產與營業秘密均存於電腦系統，若缺乏完善的資訊安全控管，便可能因為安全事件而衝擊整體營運因此。

(一) 使用者管理

- 有效管理每個使用者密碼，依據各項應用服務，分別訂定機關外及機關內之使用權限，密碼並定期更換。
- 訂定電腦軟體管理要點，建立軟體使用管理制度，遵守智慧財產權相關法規或契約規定。
- 使用者進入、使用、離開系統應有詳細記錄，以便查核。

(二) 系統管理

- 訂定電腦系統作業程序，以確保正確及安全地操作及使用電腦，並做為系統發展、維護及測試之依據。
- 建立日常作業之安全管理，包括：資料備份作業原則、系統作業紀錄、系統錯誤事項紀錄及電腦作業環境之監測等。
- 建立電腦媒體、系統文件、媒體處理、資料檔案之安全管理，及機密性、敏感性資料之處理程序。
- 必須注意作業系統及應用軟體是否為最新版本、系統管理者使用權限設定、系統組態檔、網路服務、目錄使用權限、帳

號管理、日誌檔管理、密碼管理等相關問題。

(三) 委外管理

- 辦理資訊業務委外作業時，應研提資訊安全相關需求，明訂廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守並定期考核。
- 在系統生命週期之初始階段，應將資訊安全需求納入考量；系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。
- 對於廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，僅核發短期性及臨時性之系統辨識及通行密碼供廠商使用，使用完畢後應立即取消其使用權限，並嚴禁核發長期性之系統辨識碼及通行密碼。

(四) 設備管理

- 嚴格控制 LAN 中的終端機、工作站的數量及位置。
- 硬體上鎖(lock)、防竊、驗證身分之設備。

(五) 成立突發事故處理小組。

針對可能的資訊安全緊急事件有所準備及建立緊急反應的機制，以收事前預防、偵測，事中監督及事後有效處理的功能。

- 在發生緊急事件之際及之後建立一套回復系統，並制定回復的優先順序。

- 不定期進行網路攻擊演習測試。
- 建立安全回報機制、建立網路與系統的 Vulnerability Database，加速電腦網路安全資訊之流通。

五. 資訊安全管理政策及制度等制度

資訊安全人人有責，必須業務、資訊及政風人員共同合作才能建立堅實的制度；業務單位管理制度建立，政風單位公務機密維護，資訊單位安全技術措施。

(一) 資訊安全政策(Security Policy)

成立資訊安全推動委員會，成員為各單位主管，並由副首長擔任召集人，負責推動、協調及督導資訊安全管理相關工作，包括：資訊安全政策之核定及督導、資訊安全責任之分配及協調、資訊資產保護事項之監督、資訊安全事件之檢討及監督等。

在資訊安全推動委員會下成立跨部門資訊安全推行小組，統籌資訊安全政策、計畫、資源調度等事項之協調研議，小組成員包括：

- 資訊單位：負責辦理資訊安全政策、計畫及技術規範之研議、建置及評估等事項。
- 業務單位：負責辦理資料及資訊系統之安全需求研議、使用管理及保護等事項。
- 政風單位：負責辦理資訊機密維護及稽核使用管理事項。

資訊系統安全需求應與資訊資產價值相稱，並考量安全措施不足，對機關可能帶來的傷害程度。依據「行政院及所屬各機關資訊

安全管理要點」、「行政院及所屬各機關資訊安全管理規範」及業務需求，訂定資訊安全政策及資訊安全水準，並告知全體人員、與機關連線作業之公私機構及提供資訊服務之廠商，共同遵守。資訊安全政策涵括下列事項：

- 資訊安全之定義、目標及範圍等。
- 資訊安全政策之解釋及說明、原則、標準，以及全體人員應遵守之規定，包括：法令及契約對資訊安全的要求及規定、資訊安全教育及訓練之要求、電腦病毒防範或偵測之要求、業務永續運作規劃之政策。
- 推動資訊安全之組織權責及分工。
- 全體人員在資訊安全上應負的一般性及特定的資訊安全責任。
- 發生資訊安全事件之緊急通報程序、處理流程、相關規定及說明。
- 需定期對各單位人員進行資訊系統及技術應用之安全評估，以反映資訊安全政策、法令、技術及機關業務之最新狀況，確保資訊安全之實務作業，確實遵守資訊安全政策，以及確保資訊安全實務作業之可行性及有效性。

(二) 管理規範

鑒於本府安全最大問題主要源至網際網路，建議訂定網際網路使用規定（草案），如下：

總統府網際網路使用規定（草案）	
訂定規定	說明

總統府網際網路使用規定（草案）	
訂定規定	說明
總則	
（目的） 一、總統府(以下簡稱本府)為有效使用網際網路資源及避免不當使用，特訂定本規定。	明定本規定之目的。
（管理單位） 二、本府網際網路系統之管理單位為第二局。	明定本府網路設施之管理單位。
（使用者限制） 三、本府網際網路之使用者以本府現職人員為限。但非本府現職人員因軟硬體維修或其他特殊需要，經管理單位同意者，不在此限。	本府網際網路於本（八十九）年十一月一日起全面開放同仁使用，非本府職員（如記者室採訪記者）不得使用本府提供之網際網路服務。
（開放服務項目） 四、本府網際網路提供之服務項目以資料查詢、電子郵件、檔案擷取及遠端登入為限。 前項所列服務項目依各單位需求而定。	本府因業務需要所需網際網路服務為本點所列四項功能。
（開放時間） 五、本府網際網路開放時間為每日六時至二十四時。 前項開放使用時間，得依實際使用情形，由本府辦公室自動化推動委員會議決定調整之。	本府現行網際網路基於公文系統安全及管理維護人力考量，僅於上班時段開放使用（目前開放時間自早上六時至下午八時，例假日不開放），超過時限即自動斷線。惟為兼顧相關單位業務需要，開放時間由本府辦公室自動化推動委員會視實際使用情形彈性調整。
網際網路服務之使用	
（使用者一般規範） 六、使用者使用網際網路資源，應注意相關法令規範，避免侵害他人權益。	使用電腦或網路時，使用者之作為可能牽涉電腦處理個人資料保護法、著作權法、專利法、商標權、營業機密保護法、電信法、公平交易法等法律，本規定無法一一列舉，只能做概括性之約束。
（禁止商業行為） 七、使用者不得利用網際網路從事非公務之相關行為。	本府網際網路服務係提供同仁公務使用，不得從事商業行為如宣傳、廣告或行銷任何商業組織、產品或服務。

總統府網際網路使用規定（草案）	
訂定規定	說明
（禁止違反公序良俗行為） 八、使用者不得利用網際網路散播不實消息、傳輸色情、猥褻或其他違反公序良俗之言論或資訊。	本府網際網路服務係提供同仁公務使用，不得有違反公序良俗之行為。
（禁止冒用名義） 九、使用者不得冒用他人名義或使用他人帳號。	擅自使用他人帳號可能觸犯刑法竊盜罪，修改他人密碼可能觸犯刑法的偽造私文書罪、偽造公文書罪或毀損罪。
（避免傳送多份大型檔案） 十、使用者應避免同時或連續於網路上傳送多份大型檔案。	同時間於網路上傳送多份大型檔案可能造成網路的壅塞，是妨礙他人使用權利之不當行為。
（機密資料傳送原則） 十一、　機密性資料及文件，不得以電子郵件或其他電子方式傳送。但依法規使用主管機關認可之加密技術傳送者，不在此限。	為加強電子郵件之安全管理，機密資料及文件不得以電子方式傳送，須以電子方式或傳送機密資料及文件者，得採用權責主管機關認可之加密技術後傳送。
（不得私自下載軟體） 十二、　使用者不得於個人電腦中私自下載或安裝非業務相關之應用程式、資料庫或系統軟體。	私自下載或安裝軟體易侵犯智慧財產權或下載到木馬程式及含有病毒之程式。
（防範電腦病毒） 十三、　使用者不得任意卸載個人電腦之防毒軟體。所有外來檔案均應於開啟前執行掃毒。	病毒之傳播與感染可能造成本身或本府其他使用人之資料毀損，故外來檔案應確實掃毒。
（設置網站限制） 十四、　未經管理單位同意，使用者不得利用本府網際網路之主機或個人電腦架設網站。	本府網路頻寬及容量係依業務需求規劃，不提供個人網頁服務。
（電子信箱容量限制） 十五、　本府網際網路提供儲存電子郵件之磁碟空間，以管理單位設定之容量為限。 前項磁碟空間之限制於本府電子布告欄公布，不另行個別通知。 使用者應自行備份重要資料。	電子郵件信箱因磁碟空間限制，必須管制使用容量，同仁應建立資料備份之正確觀念。
（連線限制）	

總統府網際網路使用規定（草案）	
訂定規定	說明
十六、　未經管理單位同意，使用者不得使用本府設定以外之連線方式，連通其他網路或電腦，以確實維護系統安全及公務機密。	以電話撥接、ISDN、ADSL 等方式連接網路，本府防火牆無法管制，造成安全管理問題。
（禁止進行或嘗試駭客行為） 十七、　使用者不得非法侵入未經授權的電腦系統，或企圖損害或更改電腦系統、網路位址（IP）、或其存放之資料。	侵入未經授權之電腦系統可能觸犯刑法之竊盜罪或詐欺罪。損害或更改電腦系統、網路系統或其置放之資料可能觸犯刑法之偽造私文書罪、偽造公文書罪或毀損罪。
稽核及查處	
（稽核單位） 十八、　資訊安全維護及稽核使用管理事項，由政風處會同相關單位負責辦理。	明定政風處負責本府網際網路稽核使用事項。
（查處） 十九、　管理單位發現使用者違反本規定者，應即通報政風處協調相關單位會同查處。 政風處接獲檢舉或通報，於查處後簽報長官，其處理方式視情節輕重得為通知改善、縮減使用權限、停止使用及行政懲處。其已涉及刑事責任者，移請司法單位處理。	通知改善含通知其一級主管督導改善。違反行政法情形如：洩漏公務機密行為。違反刑事法情形如：刑法竊盜罪、偽造私文書罪、毀損罪等。
（使用督導） 二十、　各級業務主管人員，應負責督導所屬人員正確使用網際網路，以防範不法及不當行為。	明定業務單位主管人員應負責督導及管理所屬人員之網路使用。
附則	
（定期評估原則） 二十一、　本規定應每年評估一次配合相關政府法令、技術及業務等發展，確保實際作業之有效性。	本要點應每年檢討評估其妥適性，以因應最新之需求。
（實施日期） 二十二、　本要點奉核定後實施。	本要點奉　秘書長核定後實施。

參考書目

1. Dan Blacharski, 1998, Network security in a Mixed Environment
2. Lars Klander, 1998, Hackers Proof
3. Secure Computing, 1999, Securezone
4. George Kurtz, 2000, Hacking Exposed
5. Edward Amoroso, 1998, Intranet and Internet

附件一　Research paper

Introduction

As the current business environment go distributed, it also drives the applications systems moving to distributed, client/server technologies and has dramatically changed the computing environment of many organizations. Although client/server computing do provide access to distributed information easier, it also have the problem of safeguarding corporate computing from misuse.

The complex systems that are present in mainframe environment have assured trust in their operation. Mainframe security solution have allowed strong, centralize controls to be enforced. The security of a distributed, client/world, however, is much more complex. Unlike the mainframe, the control and security functions are distributed across several platforms and are not usually under the control of any single processor. Besides, Network has also exposed corporate networks and computing systems to access by outsides.

Distributed computing security is a business problem with many complex aspects. A key issue is how can you trust the integrity of an authentication process over a untrusted network? It includes two parts:

- Securely authenticate users.
- Authorize their actions.

Data communications channels are often insecure, subjecting messages transmitted over the channels to passive and active threats. With a passive threat, an intruder intercepts messages to view the data. This intrusion is also known as eavesdropping. With an active threat, the intruder modifies the intercepted messages. An effective tool for protecting messages against the active and passive threats inherent in data communications is cryptography

Encryption can virtually eliminate many security risks and is crucial to enable technology to operate for client/server computing. Cryptography is a tool for satisfying a wide spectrum of computer security needs and requirements. It transformation of data. It provides an important tool for protecting information and is used in many aspects of computer security. For example, cryptography can help provide data confidentiality, integrity, electronic signatures, and advanced user authentication.

Drivers for computer security

Applications which adopt C/S computing require the IT infrastructure to provide a trusted services for access of applications for distributed business processes. What is really driving the need for security? In distributed business environment, the most important need for trusted service is:

- Identification: who are you.

- Authentication: Prove you are who you say you are.
- Authorization: what are you allowed to do?
- Accountability: prove you are who you say you are.
- Confidentiality: prevents disclosure of the message to unauthorized users.
- Integrity: assures the recipient that the message was not modified en route.
- Non-repudiation: Non-repudiation with proof of origin provides the recipient assurance of the identity of the sender. Non-repudiation with proof of delivery provides the sender assurance of message delivery.

Risk in client/server computing

A threat is a circumstance, condition, or event with the potential to cause harm to personnel and/or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse. The most common security threats to network systems include impersonation, eavesdropping, denial of service, packet replay, and packet modification

Eavesdropping: Eavesdropping allows a cracker to make a complete transcript of network activity. As a result, a cracker can obtain sensitive information, such as, passwords, data, and procedures for performing functions. It is possible for a cracker to eavesdrop using wiretapping, eavesdropping by radio and eavesdropping via auxiliary ports on terminals. It is also possible to eavesdrop using software that monitors packets sent over the network. In most cases, it is difficult to detect that a cracker is eavesdropping.

Many network programs, such as telnet and ftp are vulnerable to eavesdroppers obtaining passwords which are often sent across the network unencrypted. Threats associated with use of telnet and ftp are described in sections 9.2.1 and 9.2.2.

Network programs which involve file transfer are susceptible to eavesdroppers obtaining the contents of files. In particular, NFS, RPC, rcp, and ftp are vulnerable to unintended disclosure of data. Encryption can be used to prevent eavesdroppers from obtaining data traveling over unsecured networks. Section 5.1 provides information on cryptography.

Denial of Service: Multi-user, multi-tasking operating systems are subject to ``denial of service" attacks where one user can render the system unusable for legitimate users by ``hogging" a resource or damaging or destroying resources so that they cannot be used. Denial of service attacks may be caused deliberately or accidentally. Taking precautions to prevent a system against unintentional denial of service attacks will help to prevent intentional denial of service attacks.

Systems on a network are vulnerable to overload and destructive attacks as well as other types of intentional or unintentional denial of service attacks. Three common forms of

network denial of service attacks are service overloading, message flooding, and signal grounding. It is important for system administrators to protect against denial of service threats without denying access to legitimate users. In general, denial of service attacks are hard to prevent. Many denial of service attacks can be hindered by restricting access to critical accounts, resources, and files, and protecting them from unauthorized users.

Packet Replay: Packet replay refers to the recording and re-transmission of message packets in the network. Packet replay is a significant threat for programs that require authentication sequences, because an intruder could replay legitimate authentication sequence messages to gain access to a system. Packet replay is frequently undetectable, but can be prevented by using packet time-stamping and packet sequence counting.

Packet Modification: Packet modification is a significant integrity threat which involves one system intercepting and modifying a packet destined for another system. In many cases, packet information may not only be modified, but it may also be destroyed.

How encryption work

Cryptography is the science of mapping readable text, called plaintext, into an unreadable format, called ciphertext, and vice versa. Cryptography relies upon two basic components: an *algorithm* (or cryptographic methodology) and a *key*. The mathematical operations used to map between plaintext and ciphertext are identified by cryptographic algorithms. Cryptographic algorithms require the text to be mapped, and, at a minimum, require some value which controls the mapping process. This value is called a key.. The computations affect the appearance of the data, without changing its meaning.. . The resulting encrypted data is stored or transmitted is meaningless without using the correct key to decrypt the data .Given the same text and the same algorithm, different keys produce different mappings.

- The ciphertext is transmitted over the data communications channel. If the message is intercepted, the intruder only has access to the unintelligible ciphertext
- Upon receipt, the message recipient transforms the ciphertext into its original plaintext format. This process is called decryption or decipherment

Cryptography is used to provide the following services: authentication, integrity, non-repudiation, and secrecy. Two approaches have been developed to provide the authentication, integrity, and secrecy services.

private key encryption: In secret key cryptography, two (or more) parties share the same key, and that key is used to encrypt and decrypt data. As the name implies, secret key cryptography relies on keeping the key secret. If the key is compromised, the security offered by cryptography is severely reduced or eliminated. Secret key cryptography assumes that the parties who share a key rely upon each other not to disclose the key and

protect it against modification.

The best known secret key system is the Data Encryption Standard (DES), published by NIST as Federal Information Processing Standard (FIPS) 46-2. Although the adequacy of DES has at times been questioned, these claims remain unsubstantiated, and DES remains strong. It is the most widely accepted, publicly available cryptographic system today. The American National Standards Institute (ANSI) has adopted DES as the basis for encryption, integrity, access control, and key management standards.

Asymmetric or public-key cryptography differs from conventional cryptography in that key material is bound to a single user. The key material is divided into two components: a private key, to which only the user has access, and a public key, which may be published or distributed on request.

Each key generates a function used to transform text. The private key generates a private transformation function, and the public key generates a public transformation function. The functions are inversely related, i.e., if one function is used to encrypt a message, the other is used to decrypt the message. The order in which the transformation functions are invoked is irrelevant. Note that since the key material is used to generate the transformation functions, the terms private key and public key not only reference the key values, but also the transformation functions. For example, the phrase, ``the message is encrypted using the message recipient's public key'', means the recipient's public key transformation function is invoked using the recipient's public key value and the message as inputs, and a ciphertext representation of the message is generated as output.

RSA is a public keys algorithm, based on the algorithm originally developped by Diffie-Hellman. Raeher than having a single key that had to be exchanged over a secure channel , each user would have two keys. : a private keys and a public keys . no one but the user need know the private keys , and any one could know his public keys . in this way, a person sending a message can encrypt it with the recipent's public key. The recepient , using his private keys , is them the only one who can decript it.

The use of RSA algorithm is rapidly growing. Paryicually in the area of electronic messaging and electroonic mail.Secure communication between two parties can be accompolished using an exchane of public keys .

Each approach has benefit depending on the specific requirement and implementation. The advantage of a public-key system is that two users can communicate securely without exchanging secret keys. For example, assume an originator needs to send a message to a recipient, and secrecy is required for the message. The originator encrypts the message using the recipient's public key. Only the recipient's private key can be used to decrypt the message. This is due to the computational infeasibility of inverting the public key transformation function. In other words, without the recipient's private key, it is computationally infeasible for the interceptor to transform the ciphertext into its original

plaintext. Note that with a public-key system, while the secrecy of the public-key is not important (in fact, it is intended to be ``public''), the integrity of the public-key and the ability to bind a public-key to its owner is crucial to its proper functioning.

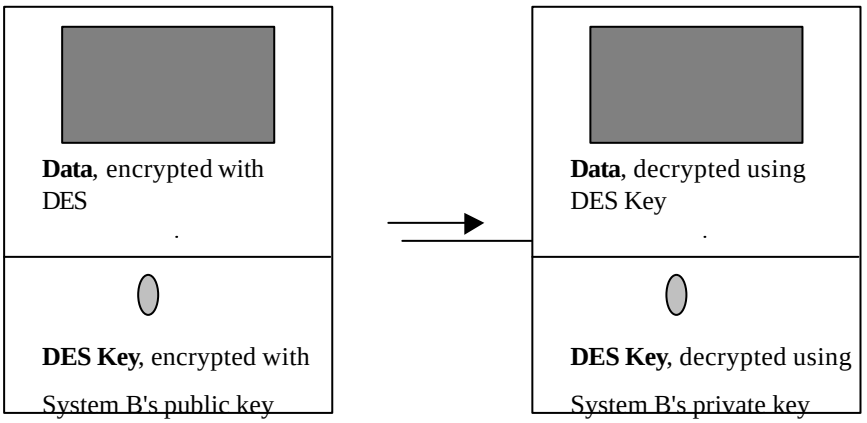
One disadvantage of a public-key system is that it is inefficient compared to its conventional counterpart. The mathematical computations used to encrypt data require more time, and depending on the algorithm, the ciphertext may be much larger than the plaintext. Thus, the current use of public-key cryptography to encrypt large messages is impractical.

A second disadvantage of a public-key system is that an encrypted message can only be sent to a single recipient. Since a recipient's public key must be used to encrypt the message, sending to a list of recipient's is not feasible using a public-key approach.

Although public-key cryptography, by itself, is inefficient for providing message secrecy, it is well suited for providing authentication, integrity, and non-repudiation services. All these services are realized by the digital signature. the downside to private key encryption is that the key is shared among two sites, one must have a secure channel to pass the encryption key. To resolve this dilemma, a combination of private keys encryption and public keys encryption is often used. the down side to RSA is that encryption with RSA takes significantly computer power and is therefore slower than DES public keys encryption circumvents the need for a secure channel for exchane keys; on;y public keys are exchanged. It is also the enabling technology for digital signatures.

Another difference between private keys and public keys encryption is in the algorithm used to encryp the data . unlike secret key encryption schemes, which use matrices called S box for encryption , public keys encryption takes advantage of the fact it is difficult to factor very large numbers.

Because public key encryption is more complex over than private keys encryption , it is also slower when compared with private keys algorithms such as DES. As a result , the two technologies are often mixed in practice , as illustrated in Figure,



The advantage of public keys encryption over private keys encryption is that the private

keys is never shared with the other principals.Another benefit of public keys encryption is that it may be used for the creation of digital signatures. A digital signatures is used to verify both the sender and contents of an electronic message.
The public keys approach is suited to situations where a user requires secure interaction with several other application or users.

Uses of Cryptography

Cryptography is used to protect data *both* inside and outside the boundaries of a computer system. Outside the computer system, cryptography is sometimes the *only* way to protect data. While in a computer system, data is normally protected with logical and physical access controls (perhaps supplemented by cryptography). However, when in transit across communications lines or resident on someone else's computer, data cannot be protected by the originator's logical or physical access controls. Cryptography provides a solution by protecting data even when the data is no longer in the control of the originator.
Encryption can be implemennted at various networking levels.Based on the EPM requirements, ESA defines the key security components and how they must work together to ensure adequate security of our IT infrastructure
Mulipupose Internet Mail Extensions (MIME) is an Internet standard for mulitimedua Encryption-mail. However, MIME lacks security. as a result, a secure version of the MIME standard (S/MIME) is under development. It involves extensions to MIME using RSA public key encryption , which also support digital signature.
Groupware
Encryption is becoming more common in commercial applications. Lotus Notes now includes encryption. Userd can encrypt a single outgoing message, specify all outbound traffic should be encryted or encrypt incoming traffic. Note's encryption capabilities support compound encryption in a document; priviliged users could read the entire document, where less privileged administrative users might only be able to read information necessary to do their work.
Another major trend is the incorporation of encryption in firewall systems. a network, such as the Internet, the message source and the physical path of the Use of a value-added network provider. If two or more parties are communicating via a third party network, the network provider may be able to provide assurance that messages originate from a given source and have not been modified.

附件二　參訪議程

A. What are current states of the market or practice on computer security?

B. How widespread are computer security incidents in USA?

C. How to detect computer security vulnerabilities and to know whether the computer system has been breached by the hackers?

D. Hoe to prevent computer criems originated within the organization, not from outside?

E. What are the steps in developing a security policy for management?