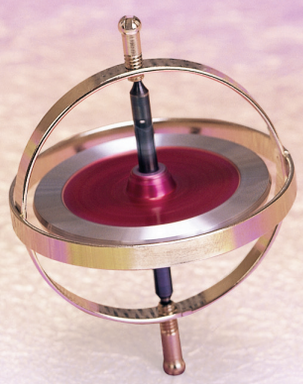
文｜許加文　圖　編輯小組
Article | Hsu Jia-wen　Photos | The Editing Team

網路環境下資訊安全的迷思

The myths surrounding data security under the networking environment



壹、前言

本署自89年1月28日成立以來，即編設通電資訊處以完善指、管、通、資、情、監、偵系統(C4ISR)之進程，期間並配合國家財政狀況及人力等負荷，迄今執行完成有無線電網路規劃與調整作業、以連結警訊、國軍及公眾等網路交換，提升各級勤務指揮及行政連絡效能，建構「海巡資訊系統」(包含海巡網際網路基礎建設、單一窗口連接政府資訊網、電子公文自動化環境、安檢資訊系統、海巡體系公開金鑰基礎建設與憑證機構(PKI&CA)與相關資訊安全強化作爲等)，以完善海巡資訊系統發展架構，而對於網路之依賴更亦形緊密而不可分。然而相對於如此眾多之通資系統，如何前瞻性的規劃本署整體資通安全防護體系亦已刻不容緩，也因此，本署自94年7月1日起調整成立資通安全科此一專責單位，以期能提供更周延之本署資通安全防護作爲。

然而相較於傳統的犯罪行爲，網路上的詐欺行爲是比較不容易追查或是定罪，也因此，在網路環境下資訊安全的防護，對於一般人而言，亦有著一定程度的困難與認知落差，「唯一」值得信賴的方法好像是：裝置適切的密碼安全設備，以獲得較高等級的資

Part 1 Foreword

Following the Administration's inception on January 28, 2000, the Communications and Information Division has been launched to perfect the progress of the Administration's command, control, communication, computer, information, intelligence, surveillance, and reconnaissance systems. Throughout the period, the state of the Treasury and manpower capacity has been taken into account, the implementation so far has yielded the wired and wireless electronic network development and adjustment operations, which are used to link to the police intelligence, armed forces and public network exchanges. It has poised to enhance various duty command and administrative contract functions. A Coast Guard information system has been instilled, encompassing Coast Guard WWW Internet infrastructure, single-window connection to the government information Web site, electronic government document automation environment, security inspection information system, Coast Guard system open gold key infrastructure and PKI&CA authentication organization, and related data security strengthening move and the like), sought to perfect the Coast Guard information system's development framework, which further showcases the inseparable networking dependency. Yet when faced with such a large volume of communications and information systems, how best to develop the Administration's overall data and communications security protection system with an innovative planning approach has emerged as an urgent matter that cannot be put off any further. And in light of which, the administration has since July 1, 2005 revamped and launched a full time unit, the data and communications security section, in a move to provide more thorough safeguard for administration data and communications security protection.

Yet when compared with conventional criminal acts, Internet

訊安全保障。但是在資訊保密與安全的作爲上，似乎仍存在著一些的迷思，使得大多數的人，陷入迷惑的困境而不自知。本文希望羅列並釐清一些共通的錯誤觀念，以期免於掉入以下的迷思中，並進而能有更正確的體會。

貳、資訊安全的迷思

一、密碼是安全的嗎？

一般人通常認爲系統需要輸入密碼方可進入才算是安全的；然而，這觀念是不正確的，因爲密碼可以很容易地被偵測及篡改，侵入者以一段較長的時間也可臆測密碼，而密碼追蹤程式又是另外一種常用的伎倆來測知密碼，使得他將來可以隨時地侵入系統，縱使密碼時時更改也無妨他後續的侵入。

所以，一個安全的存取管制系統，最佳的應該是使用隨機產生的密碼，並且只能使用一次。然而此種架構所涉及使用者的習慣與系統建置之投資等問題，恐非短期內一蹴可及的。

二、傳輸時加密就夠了嗎?

另一個普遍被誤解的觀念是只有在與外部連線進行資料傳輸時才需要安全保密，此種保密設備其實僅能提供有限的保護並且無法對付安控上某些難解的盲點。故一個安全保密的系統不僅僅是防禦外部虎視眈眈的威脅，對於蕭牆之內的禍害，更應全力釐清掃除才是上策。

有一點特別要提醒的是用於外部連線的安全保密裝置僅能提供連線兩端資料傳輸時的私密性，而對於傳送與接收端或是任何網路上經過的節點則是最大的安控盲點，它是沒有提供任何保護的。資訊安全保密應整合成系統及應用兩部份，以讓其更具效率，換句話說，什麼樣的應用就應配備什麼樣的安全保密系統才算符合效率的原則。

criminal acts are more difficult to trace and sentence the crime, and exactly because of this, when it comes to data security protection in the Internet environment, there is a certain level of difficulty and gap in recognition to most people, as most tend to believe that the only trustworthy means seems to install adequate security encryption equipment that would poise to derive a higher level of data security protection. Yet certain myths seem to linger in the move for data confidentiality and security, entrapping a majority of people to a confusing state without realizing it. The article anticipates to itemize and alleviate some of the common misconceptions in an attempt to prevent people from being entrapped in the myths, and to further provide the correct awareness of it.

Part II The myths surrounding data security

I. Are passkeys safe?

As most people tend to mistaken that it is secure when a system can only be entered by putting in a password, yet this is a misconception, for passwords can easily be detected and tempered with, where a trespasser can guess the password given a longer period of time, while password tracking program is another commonly used technique for detecting passwords, allowing a trespasser to hack a system at any time, and a password change could not prevent a hacker from subsequent hacking.

Therefore a well secured filing control system using a randomly produced password and being used only once should be the best. Yet this structure faces the problems of user's habit and construction investment and will not be easily constructed.

II. Is encryption during transmission enough?

Another commonly misunderstood concept rests on that only secure confidentiality is needed when transmitting data with outside lines, where the encryption device merely provides limited protection and can hardly tackle certain inexplicable blind spots in security monitoring. Therefore, a secure and confidential system not only needs to fend off menacing outside threats but also need to eradicate fully any potential harm hidden to make it a foolproof strategy.

三、加密的資料就一定不會被篡改嗎？

另一個常有的錯誤觀念是將資料加密就一定可以保存其私密性及完整性，實務上這並不盡然，假若，密鑰的管理已妥善地執行，資料加密只可防止某些人作不當的讀取。而只靠資料加密亦不足以防止訊息被變更，只能使其較困難些；訊息驗證碼(Message Authentication Code)也許是唯一能夠保有訊息和資料完整性的方法。

然而，要證明一個特殊的密鑰管理架構絕對安全並不容易，就好像是在證明有無反證的存在一樣。總而言之，保有訊息的私密性最好經由資料加密處理；而訊息的完整則靠訊息驗證，而要能有效地執行以上兩種技術，則非得靠一個安全的密鑰管理架構不可。

四、「專線」和「複雜的通訊協定」能保證資料的安全嗎？

許多的網路使用「專線」來連接雙方的節點，儘管選擇專線的主要理由是比起公用交換網路所花的費用來得固定而安全。然而，這個方案並不那麼單純，專線並不能提供資料保密上的助益，反而比公用交換網路更容易受到侵害。

當租用一條專線時，電信公司並不是在雙方之間直接安裝一條專用的線路，只是電信公司對所提供的線路達成一個承諾就是確保線路在任何時間都能夠保持「一定的頻寬」而已，因此「經濟實惠」應該是使用專線的唯一理由，而不是它的安全性。

五、公開金鑰能解決所有的安全問題嗎？

傳統的密碼法則爲對稱性加密法；因爲加密和解密使用相同的金鑰。而另一種新的加密法則正被廣泛地使用，稱之爲公開金鑰或是非對稱性密碼。因此，可將用於加密的金

A particular reminder is that the security confidentiality devices for outside linkup merely provides confidentiality on two ends of a data transmission, but it falls short of offering any protection when it comes to the biggest security blind spot at the transmission and receiving end and at any given nodes along a networking path. Data security confidentiality calls for integrating system and application segments, allowing them to be more efficient; in other words, an efficient principle calls for pairing a particular application with a fitting security confidentiality system in order to make it sound.

III. Would encrypted data be enough to prevent unauthorized tempering?

Another common erroneous concept lies in reckoning that data encryption would ensure confidentiality and intactness, the truth remains that it would not necessarily do so; suppose when passkey management has been securely executed, data encryption only serves to prevent certain people from unauthorized accessing. Nor relying on data encryption alone is enough to prevent the data from being tempered, but only makes it slightly more difficult; message authentication code is perhaps the only comprehensive method to ensure message and data are kept intact.

Nevertheless, it isn't easy to validate whether a unique passkey management is absolutely safe, much like trying to disprove the existence of a counterproof. In short, it is best to add data encryption to retain message confidentiality, and the intactness of messages is depend upon message authentication, and a determinant in the effective execution of the two techniques rests on securing a secure passkey management framework.

IV. Do exclusive lines and complex communications protocol help to guarantee data security?

Many networks utilize exclusive lines for connecting the nodes of two sides, given that a key reason for choosing exclusive line has been the stability and security, when compared with the cost of exchanging through public lines. However, the proposal has not been as simple, for exclusive lines do not aid to data confidentiality, and could be more susceptible to breach than using public exchanging networks.

When leasing an exclusive line, the communications provider does not install a physical exclusive line between the two end , but rather making a promise on the line provided with a certain bandwidth to be maintained at all times, thus making practicality and economical the sole reason for subscribing exclusive line, rather than its security feature.

V. Does the open gold key poise to solve all security concerns?

The conventional passkey rule is referred to as the symmetrical encryption method, for the same gold key is used in encryption and decryption processes. Yet another new encryption rule is being widely used, which is referred to as the open gold key or nonsymmetrical passkey. Therefore, it can be applied to encryption using open gold key and store it in established catalogs.

鑰公開並將其儲存於已設立之目錄中。如果使用某一固定長度的金鑰，則對稱性演算法的安全性較公開金鑰演算法爲高；因此，爲了要達成同樣等級的安全性，公開金鑰架構的金鑰及資料長度都必須加長，且在傳遞分送公開金鑰的過程中，保持金鑰的完整性將是一個主要的課題。

總而言之，公開金鑰的架構需要設計特殊的金鑰管理方式；此管理方式可能不同於傳統的加解密法，但不見得一定是比較簡易的管理模式。

六、資料加密標準已經過時了嗎？

資料加密演算法則，或一般所熟知的資料加密標準(DES)，或多或少受到一些的批評，許多聞名的數學家、學者、電腦科學專家以及密碼學家都曾多年嘗試破解資料加密標準(DES)；但換言之，就是使用比採用繁複弱勢金鑰(weak-key)，以及半弱勢密鑰(semi-weak key)外，並無出現任何重大性的突破，也就是說，資料加密標準(DES)歷經時間上的考驗和多數人的評鑑後，目前還是值得信賴的。

近年來在分解方法上已有明顯的進展並且可以產生重大的突破，因式分解已不被歸類於最困難、最難解的問題之一，即所謂的完全非定性多項式時間等級(NP-Complete)。假如快速的因式分解演算法被發現後，則以 RSA 爲主的安控系統將會完全地曝光，然而若是資料加密標準(DES)被破解，換用替代的演算法並不至於造成安控結構巨大的改變，資料加密標準(DES)經過了公開的分析，並且所獲得的評價是肯定的。很顯然地，資料加密標準(DES)是值得信賴的，並且將會繼續在商業界成爲極具占有率的演算則。

Suppose a certain length of a gold key is being used, then the security of a symmetrical computation method would be higher than that of an open gold key computation method; therefore, in order to achieve the same grade of security, the length of open gold key structure and gold key data would have to be lengthened, and how best to maintain the gold key intact during the process of transmitting an open gold key would become a critical issue.

In all, open gold key framework calls for the design of a unique gold key management mode; such management mode would likely differ from the conventional encryption methods, but does not warrant it as a relatively easier management mode.

VI. Have the data encryption criteria outdated?

Data cryptology computation method, or the generally known data encryption standard (DES) is more or less under criticism, as many renowned mathematicians, scholars, computer science experts and cryptologists have attempted, in years, to try to decode the data encryption standard (DES); yet to put it in another manner, besides suing a weak key or semi-weak key, there has not been any major breakthrough, meaning that DES remains rather trustworthy having endure the test of time and the critical assessment of many.

In recent years, as decoding methods have undergo significant progress and are able to achieve significant breakthrough, decoding contingent programs is no longer classified as one of the most difficult problems to solve, meaning the so-called non-qualitative multiple time class complete (NP-complete). Yet suppose a rapid contingent equation decoding computation method has been discovered, then RSA-based security control systems will be exposed completely, yet suppose DES has been decoded, the alternative substitution computation method does no necessary cause drastic changes to the security control structure, warranting DES's open analysis and its acclaims to be reassured. Ominously, DES remains trustworthy, and will continue to be a computational doctrine in the business sector.

VII. Can security confidentiality be achieved merely through software?

Using software to achieve encryption, signal authentication, user identity identification and other scrambling functions do provide a good incentive, being that on (one) the one hand, it is easier to design, on the other, it helps to weed out complex firmware interface and peripheral communication load. Yet when it comes to viruses hidden within, it guarantees virtually very little. For example, being that the most sensitive data on ATM machines that offer inter-bank withdrawal function has been the withdrawer's password, thus the security monitoring function an ATM machine provides would be password verification and secured transmission, and passkey decoding function will not show up. In such way, a system operator with ill intent to sabotage will not be able to do much harm as hindered by restric-

七、安全保密可以僅由軟體達成嗎?

用軟體的方式達成加密、訊息認證、使用者身份辨認及其它密碼的功能是蠻有誘因的一件事，原因在於一方面設計上較爲簡單，另一方面可避掉複雜的硬體介面及與週邊的通訊負荷；然而對於內賊，它幾乎完全無法保證什麼。舉例來說，提供跨行提款服務的ATM網路上最敏感的資料是提款人的密碼，因此自動櫃員機所提供的安控功能便應該只有密碼的確認及安全的傳輸，而密碼解密的功能就不該出現，這樣即便是系統的操作員想要做壞事但因安控功能的限制也只能徒呼莫可奈何了。

八、有了防火牆就百毒不侵了嗎？

「我們已經有防火牆」這通常都成了管理人員的擋箭牌，可是實際上大部分遭受重大資安事件損失之公司也均有防火牆；因爲現行網際網路上各類變種的惡意程式正以驚人速度成長，傳統「以病毒碼偵測病毒的防護技術」，面對這些新型態的病毒或是惡意程式也幾乎已經無能爲力了；而事實上，許多新型蠕蟲以及其變種根本就是要跟防火牆及防毒軟體一較高下，會刻意又小心的穿透防火牆並避開防毒軟體的偵查，這也導致了一般防火牆及防毒軟體根本就是沒用的。

然而防火牆與防毒軟體還是可以大大減少企業的風險。再加上網路分割、防禦主機(Bastion host) 、在網路出口之路由器設定阻擋、關閉IE瀏覽器的active scripting功能等搭配，更可以收到非常好的功效。

當然人的因素卻是科技始終沒法顧全的，因爲許多蠕蟲和病毒根本就是針對人性，而我們現在用的微軟作業系統還有應用程式的安全性又都很不健全，這當然容易長蟲中

tions of the security control.

VIII. Would the presence of firewalls enough to keep all viruses at bay?

"We've gotten the firewall" has become a safety field that every manager touts, yet in reality, a majority of firms that suffered grave security breaches have all had the firewall installed; in light that a host of vicious programming is spreading at an alarming speed through the World Wide Web Internet, the conventional virus code viral protection technology would become nearly obsolete when faced with these new types of viruses or malicious programs. The truth is that many newer forms of worms and their variations are competing head on with the firewalls and anti-virus software, as they deliberately and carefully penetrate the firewall and circumvent the anti-virus software detection, which also render the common firewalls and anti-virus software to be literally useless.

Yet it is not to discount that anti-virus software and firewalls could help to greatly reduce business risks, coupled with networking division, bastion host that serve to create resistance through the router or a network portal, coordinated with functions such as shutting down an IE browser's active scripting, all of which do serve to provide significant yields.

Naturally as human factor is something that technology cannot fully address, and many worms and viruses are gearing at human weaknesses, besides many of the Microsoft applicable programs do not come with a comprehensive security feature, all of which have contributed to the rampant running of computer virus infection. In the U.S. Enron incident, in spite that the company has had a comprehensive internal control and internal audit system, yet to tap into the bottom of the incident, the truth remains that organization culture and personnel management could be the true determinant in securing data security.

毒！以美國恩隆事件中，雖然該公司也有完整的內控內稽制度，但深究其原因，其實組織文化及人員管理很可能才是資訊安全做不好的眞正原因。

參、結論

電腦網路現今已成爲我國電子政府世代工作的必須配備，而資訊安全的重要性雖然是人人掛在嘴上，卻又對層出不窮的網路安全問題無計可施，就本署而言，仔細審視署內的各項資通安全防護設備：無論是「防火牆」、「入侵偵測」、「公開金鑰基礎建設」、「身份認證」、「單一簽入」、「資料加密」、「掃毒防毒軟體」．．．等一樣不缺，但機房人員依然疲於奔命，遑論是否落實資訊安全的目的在於確保各項線上交易具有可被信賴之品質，並建立系統遭攻擊可以應付的能力、避免系統中斷、機密資料被誤用等。

總的來說，資訊安全的範疇是相當廣泛，也沒有任何單一的廠商可以提供涵蓋全局的防護設備，不要以爲防毒、防火牆就等同於資訊安全。事實上，安全是一種多工環境，幾項必備的步驟可同步或交互進行，包括設計資訊安全管理架構、資訊安全方法與解決方案的建置，以及稽核制度的建立等。

而值此本署成立資通安全科之契機，除了彰顯本署對資通安全的重視之外，後續更當整合並統籌本署各項資訊資源，除訂立本署資訊安全政策外，更需導入資訊安全管理制度的建立與認證。其中重要的是「申請認證」是一項值得追求的目標，但更重要的是在本署的準備過程中，讓各單位或組織眞正從中學習到正視資訊安全，進而採取適當的管理程序，形成從上而下一致遵行的資訊安全文化，這才是本署後續導入資訊安全管理制度及認證的正確態度。

參考文獻

The Seven Myths of Data Security, RACAL。

（本文作者任職於海巡署通電資訊處）

Part III Recapitulation

As computer networking has become indispensable in the government's move to embrace a computerized administration era, everyone remains preoccupied with the importance of data security, yet few could come up with a viable solution for addressing the issue of networking security. As far as the Administration is concerned, a closer look of the Administration's various data and communication security protective devices, such as the firewall, trespass detection, open gold key infrastructure, identity recognition, single authentication, data encryption, anti-virus software and the like, which are all present, yet equipment room personnel are strapped in handling the demands, little else having the wits to address whether the objective of enforcing data security has been to ensure a dependable quality of various online exchanges, and the instilled system is capable of responding in the event of sabotage, in order to prevent the system from being interrupted, or confidential data from being misused and the like.

As a whole, the domain of data security remains very broad-based, and no one single vendor is capable of providing an encompassing protective device, so one shan't be mislead to believe that anti-virus program and firewalls equate to data security. In fact, safety remains a multi tasking environment, where a few essential steps can be synchronized or interacted, including the design for a data security management framework, the instilment of data security methods and solution proposals, as well as the instilment of an audit system and the like.

At the opportune time when the Administration has just launched a data and communications security section, which not only aims to showcase the Administration's emphasis on data and communications security, but it is also important to continue revamping and integrating various administration information resources, more than instilling an administration-wide data security policy but also to bring in a data security management and authentication system. Among them, application authentication remains an objective worth pursuing, and more importantly it rests on the Administration's preparation process, which would allow all units and organizations to truly discern the importance of data security, and would in turn seek adequate management procedures that would be conducive to spawn a consistent data safety culture, which would serve as a correct attitude toward the administration's pending induction of a data safety management system and authentication process.

Reference:

The Seven Myths of Data Security, RACAL

(The author is currently with Coast Guard Administration communications and information division)