Trends in IT Security

A newsletter for IT Professionals

Issue 13

I. Background

Overview

The pace of advancements in information technology is greater than ever. Today, information systems and devices have been integrated into every fibre of universities' IT environments. Thus IT security becomes the most important elements to ensure the integrity of their information systems and resources.

Recent development in information technology can be summarised into the following three main directions.

- **Mobility**

  The line between traditional computers and mobile devices has become blurred. Hand-held smartphones, laptops and tablets are taking over many computing tasks that are used to be performed by stationary desktop PCs. Seamless connection with the Internet is another great leap forward taken in mobile technologies.

- **Lower Cost**

  Under the current economic situation, improving "cost-effectiveness" is a main theme for IT expenditures. IT managers are seeking different approaches to reduce their IT budgets while sustaining the same (or even higher) level of IT service delivery. Moving IT functions into the "cloud", perhaps, is one of the most cost effective options available to organisations today.

- **Newer Standards**

  Technologies keep evolving all the time. From the fundamental infrastructure (e.g. CPU, disk storage, network protocols) to end user applications (e.g. communication software and office tools), old standards have been continuously replaced by new ones.

For each of the above direction, there are new security concerns which require relevant actions taken by universities to address the associated risks.

Reference:
http://www.ogcio.gov.hk/eng/prodev/download/g54_pub.pdf
http://news.idg.no/cw/art.cfm?id=2F201BAF-1A64-6A71-CE2C9B0C38F6E26A

I. Background (cont'd)

In this article, we will focus on the following three representative developments in information technology and introduce latest trends in the information security aspects.

- **Mobile Computing**

  Mobile computing has been a hot topic for recent years. Mobile devices such as smartphones and tablets are getting much more powerful in these few years. In addition to the conventional telephone functions, they are capable of Internet browsing, making online transactions, downloading applications and providing location services like Global Positioning Services (GPS).

  With the growing complexity of mobile devices, operating systems and applications, security threats are now more prevalent. According to a survey conducted by Juniper Network Inc. in 2010, about 72% of respondents had shared or accessed sensitive information, such as bank accounts and credit card numbers, via their mobile devices. Applications of these kinds raised the severity of sensitive data leakage or malicious attacks.

  One of the popular Open mobile platforms, Android, has suffered several attacks from hostile software in the form of viruses, worms and Trojan horses. iOS, another widely used mobile operating system for Apple's iPhones, was once known to have a security flaw that allows an application to download and execute unsigned program codes (i.e. programs without proven authenticity) from a remote source.

- **Cloud Computing**

  One of the biggest waves of technology innovation is the cloud computing. It defines a way to increase capacity or add capabilities quickly without investing in new infrastructure, training new personnel, or licensing new software.

  There are a number of security flaws associated with cloud computing, which can be categorised into:

  - **Security Flaws in Cloud Providers –** Security issues related to organisations providing the cloud services, including the underlying infrastructure, IT operational procedures and information systems deployed.

    Researchers have pointed out that multiple security vulnerabilities are found in many cloud architectures. Amazon Web Services was found to have security flaws that may allow unauthorised access to all user data and cross-site scripting attacks.

Reference:
http://www.chinadaily.com.cn/usa/business/2011-10/31/content_14005557.htm
http://www.tipb.com/2011/11/08/ios-security-exploit-exposed-released-apple-approved-app-video/
http://en.wikipedia.org/wiki/Cloud_computing_security

I. Background (cont'd)

- **Security Flaws in Customers –** Security issues that reside at client's IT environments, such as insufficient user awareness for cloud security, inappropriate cloud user account maintenance process and unsecured Internet communication protocol used for accessing cloud services.

  ~~Based on Harris Interactive's survey on cloud security in 2010, more than 65%~~ of Hong Kong firms surveyed that have not already implemented cloud security measures were planning to implement a cloud solution or purchase a cloud service in the future.

- **Internet Protocol Version 6 (IPv6)**

  With the last batch of Internet Protocol Version 4 (IPv4) assigned on 3 February 2011, organisations now need to seriously consider migrating to IPv6, the long-anticipated upgrade to the Internet's main communication protocol.

  Comparing to IPv4, IPv6 has larger address space, supports multi-cast (i.e. transmission of packets to multiple destinations in a single send action), allow more efficient processing by routers and is more compatible with mobile networks.

  However, IPv6 represents a new territory for universities and security has always been a challenge in IPv6 deployment. New features of IPv6 indicate the possible existence of unknown threats that may be leveraged by hackers. As IPv6 is still in its early stage, the solutions to these threats and proven best practices will only come after implementation experience.

Related Article

New Trends Cause Asian Firms to Review IT Security Strategies

New trends in information technology, including cloud computing and an increase in mobile devices connecting to the corporate networks, are prompting companies to review their IT security strategies.

According to a commissioned study by Fortinet, a network security provider, companies in the region are showing concern that their IT security coverage and related costs may need to be improved to guard against any security threats.

See the article:
http://news.idg.no/cw/art.cfm?id=2F201BAF-1A64-6A71-CE2C9B0C38F6E26A

Reference:
http://en.wikipedia.org/wiki/IPv6
http://www.circleid.com/posts/8_security_considerations_for_ipv6_deployment/

II. Security Concerns

- **Security Concerns in Mobile Computing**

  - **Theft or Loss of Mobile Devices**

    Despite the monetary loss to the users of mobile devices, theft / loss of mobile devices also means potential leakage of sensitive data related to personal identification, confidential material and financial information.

    In addition, by allowing staff or students to use hand-held mobile devices to conduct academic research or administrative tasks, the impact on universities due to theft / loss events will become much more significant.

  - **Viruses and Malware**

    Wherever there are information systems, the presence of viruses and malware is inevitable. Infection of viruses and malware has now become a serious topic since mobile devices can interact with the Internet and install various applications in the same way as desktops.

    According to the research by Juniper Network Inc., in a short period from July 2011 to November 2011, Google's Android operating system has had an almost sixfold increase in threats such as spyware and viruses. Once infected, users' private data will be in great danger and their communication with external parties could be hijacked without any notice.

  - **Unsecured Wireless Hot Spots**

    Comparing to the Internet services provided by mobile service providers, stationary wireless hot spots are still preferred by most of mobile device users because of higher connection speed, more stability and less service charges. Public places like coffee shops, airports and shopping malls, where unsecured wireless hot spots are offered, are the weakest links in the security chain connecting mobile devices to the Internet.

- **Security Concerns in Cloud Computing**

  - **Shared Technology Issues**

    Cloud providers deliver their services in a scalable way by sharing infrastructure (e.g. storage, CPU and network), which does not provide strong isolation properties for a multi-tenant architecture.

    Attacks have surfaced in recent years that target the cloud computing environments with weak compartmentalisation to gain unauthorised access to the data of other tenants.

Reference:
http://www.infosec.gov.hk/english/technical/files/mobilets.pdf
http://www.kansascity.com/2011/11/15/3267279/android-more-virus-prone-than.html
https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

II. Security Concerns (cont'd)

- **Data Loss or Leakage**

  Data stored in the cloud will be subject to a lower degree of control by universities. Deletion or alteration of records without backup, loss of encryption keys, physical damage of storage devices within the cloud service providers can easily result in data compromise. Insufficient authentication, authorisation and audit controls also indicate a higher risk of data leakage. Important information, such as staff / student personal information, examination records and research material, may be unrecoverable or disclosed to unauthorised parties, causing an impact on universities' reputation or even leading to potential litigations.

- **Unknown Risk Profile**

  When adopting a cloud service, universities may be well informed of the features and functionality by the cloud service provider. However, the details or compliance of the internal security measures, configuration hardening, patching, auditing and logging are usually overlooked. One of the biggest consequences is that the universities may not be able to correctly estimate their security posture and be aware of the level of security threats they may encounter.

- **Security Concerns in IPv6**

  - **Larger Network Segments**

    IPv6 supports network segments (i.e. around 18 quintillion hosts on a single segment) that are much larger than those supported by IPv4. The increase in network segment scale imposes challenges on network management practices, such as IP address administration and vulnerability scan.

  - **Extension Headers**

    IPv6 allows additional headers, also known as "Extension Headers", to follow the main headers, specifying options like destination and authentication. In presence of large number of extension headers, traditional firewalls, routers or other security gateways may suffer from performance degradation, creating a potential vector for Denial of Service (DoS) threats.

  - **Dual-stack**

    Dual-stack refers to the support of both IPv4 and IPv6 on a single network device. The co-existence of IPv4 and IPv6 dual stacks increase the potential for security vulnerabilities, because one can be subject to attacks on both IPv4 and IPv6. Users may have the firewalls well configured for IPv4 but their hosts are running IPv6, which makes them vulnerable to IPv6 attacks.

Reference:
http://www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf
http://www.infosectoday.com/Articles/Basic_IPv6_Security_Considerations.htm
http://www.cisco.com/web/SG/learning/ipv6_seminar/files/02Eric_Vyncke_Security_Best_Practices.pdf

III. Vulnerabilities and Exploitations

Mobile Computing

- **Exploitations on Application Vulnerability**

  Mobile devices usually run popular operating system and web-based applications, making them a target for application and operating system vulnerability exploitations just like laptops or desktops. For example, researchers of Privateer Labs have found a hole in Android that allows a malicious app to disable an installed anti-virus app on the user's mobile phone; Apple's iOS was vulnerable to a tool called "sslsniff", which performs "man-in-the-middle" attacks against Secure Socket Layer (SSL) / TLS (Transport Layer Security) connections made by iPhones.

- **Exploitations via Phishing Scam**

  Most of the web browsers for traditional PCs are capable of warning users when accessing phishing websites, yet such functionality is not widely deployed on mobile devices. As a result, mobile users are more susceptible to phishing scams.

  Another reason is that mobile devices usually come with smaller screens, which limit the amount of information available for users to spot phishing attempts. Take BlackBerry as an example, it is difficult for users to distinguish a phishing e-mail because the "From" field only shows sender's name, instead of the full e-mail address.

Cloud Computing

- **Exploitation on Insecure Interfaces and Application Programming Interface (API)**

  Cloud providers offer a set of software interfaces or APIs for their customers to manage and interact with the cloud services. The interfaces encompass various security areas of the cloud services, ranging from authentication and access control to encryption and activity monitoring. The security and availability of the cloud services are dependent upon the security features of these interfaces.

  Weakness in the security design of the software interfaces or APIs may cause the cloud to be vulnerable to exploitation methods such as authentication bypass or API hacks.

- **Account Hijacking**

  Phishing, pharming and e-mail based attacks, which aim at stealing cloud service account names and passwords, are one kind of typical exploitations targeting cloud users within universities. Once the user credentials are leaked, hackers can have access to personal data or proprietary information related to universities.

Reference:
http://www.enterprisemobiletoday.com/features/security/article.php/3920491/Mobile-Users-More-Susceptible-to-Phishing-Scams.htm
https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

III. Vulnerabilities and Exploitations (cont'd)

- **Cloud Service Used as Hacking Base**

  A recent disturbing trend reveals that hackers have begun to utilise the vast computing power of cloud services to carry our cyber attacks. As cloud services provide enormous processing power and storage space, they are considered an ideal platform for assaults like "brute force attacks" (e.g. sending a constant stream of passwords until the correct combination is found to crack the authentication mechanism).

  A real world case is the attack on Sony's PlayStation Network in 2011. The hacker bought time on Amazon's Elastic Compute Cloud (EC2) virtual supercomputer using a false name and launched that attack on Sony. By leveraging the EC2's massive and inexpensive processing capability, the hacker has drastically speeded up the "brute force" attacks against the encrypted passwords within the PlayStation Network.

IPv6

- **Denial of Service (DoS)**

  Extension headers of IPv6 gives rise to DoS attacks. There exists a possibility for a large amount of malicious traffic to be sent with a high priority through the manipulation of extension headers by hackers. Network devices that prioritise the malicious traffic could suffer from performance degradation and impact valid traffic on the network.

  In addition, the use of Neighbour Discovery (ND) in IPv6 allow anyone to join a local link either within minimal or no link-layer authentication. This opens the door for hackers to construct bogus ND packets and launch DoS attacks.

- **Scan Attacks**

  A first look at IPv6's large network segments may give people the idea that scan attack is not feasible in IPv6 environment, because it will cost about 5 billion years to finish the scanning using the traditional brute force method.

  Unfortunately, the reality is that there are special addresses commonly reserved for servers and routers, which can significantly narrow down the scope of scan attacks. Furthermore, the following features of IPv6 can also make the scan attacks more "efficient"

  1. Multi-cast that allow packets to be delivered to multiple destinations in a single send action; and

  2. Inner caches within IPv6 nodes that store the network status, routing data and neighbour information.

Reference:
http://www.homelandsecuritynewswire.com/hackers-using-cloud-networks-launch-powerful-attacks
http://www.securitynewsdaily.com/amazons-cloud-servers-possibly-used-sony-attack-0794/
http://www.infosectoday.com/Articles/Basic_IPv6_Security_Considerations.htm

IV. Recommendations on Security Hardening

Some hardening steps for mitigating the aforementioned IT security trends in mobile computing, cloud computing and IPv6 are listed below:

Mobile Computing

- **Use Mobile Devices with Sufficient Security Features**

  As a starting point, universities should ensure that the mobile devices used for accessing, processing and storing sensitive data must contain a minimum set of security features:

  1. Enforceable mandatory password to unlock screens
  2. Enforceable automatic device lock
  3. Password retry limit
  4. Mandatory device encryption
  5. Over-the-air remote wipe/kill capability in case of device theft / loss

- **Maintain System Integrity**

  Mobile devices, especially those installed with popular operating systems, should have anti-virus / anti-malware software / firewall installed and enabled. Periodic system scans to check for viruses or malicious codes should be performed. Users should never install applications from the Internet without a high level of assurance that the product is safe and contains no malicious contents. Universities may restrict the users' access to download applications from websites like Cydia (i.e. a popular website for applications usable on jailbroken iOS devices), or to install programs by themselves.

- **Dispose Mobile Device Properly**

  Mobile devices are evolving in terms of functionalities and usage. Proper disposal procedures should be followed if outdated or old mobile devices have been used to store sensitive university data. Prior to disposal, a thorough wipe of all data or a complete reset should be performed. For devices with hard disks, such as laptops, secure data sanitization is recommended to completely erase the previous data.

Cloud Computing

- **Data Encryption**

  Data encryption, such as Secure Socket Layer (SSL), Advanced Encryption Standard (AES) and Homomorphic Encryption, offers protection of universities' sensitive data in a shared IT environment. Encryption should be used on the following data types:

  1. Data in Transit over Networks
  2. Data at Rest (i.e. reside in the servers of cloud service providers)

Reference:
http://www.oipc.sk.ca/Resources/Helpful%20Tips%20-%20Best%20Practices%20-%20Mobile%20Device%20Security%20-%20March%202011.pdf
https://cloudsecurityalliance.org/csaguide.pdf
http://www.technologyreview.com/computing/37197/

IV. Recommendations on Security Hardening (cont'd)

3. Data on Backup Media

- **Identity and Access Management**

  To address the security issues introduced by today's aggressive adoption of an admittedly immature cloud ecosystem, universities should assess their identity and access management process within a cloud environment.

  1. Open authentication standards are generally preferred for cloud service providers. Any providers, especially Software as a Service (SaaS) providers, that implement proprietary methods to delegate authentication should be thoroughly evaluated by universities for security consideration.
  2. For Infrastructure as a Service (IaaS) cloud, dedicated VPN tunnel connected to the universities' network is recommend because it can leverage existing identity management system (e.g. Single Sign-On solutions or Lightweight Directory Access Protocol based authentication)
  3. Universities are also recommended to choose cloud service providers with support for strong authentication mechanisms, such as one-time password, biometrics, digital certificates and Kerberos.

IPv6

IPV6 security controls can be enforced in various different ways, which include:

- **Restrict Multi-cast**

  Multi-cast scope boundaries need to be enforced within IPv6 routers, packet filters, firewalls and other endpoints. Firewalls should be configured to inspect all source IPv6 addresses and filter any packets with a multi-cast source address.

- **Prevent Dual-stack Situation**

  Only allow traffic deemed as "necessary" (i.e. the so-called "default deny" policy). Universities need to implement necessary measures to monitor network and block unwanted IPv4 or IPv6 traffic. For network devices or hosts with native IPv6 support, additional care should be taken to prevent the "default" enabling of IPv6 connection.

- **Upgrade Network Protection Devices / Tools**

  Various features of IPv6, such as larger network segments, extension headers and multi-casting, would set higher requirements on the intelligence and functionalities of network protection devices / tools, such as firewalls and network vulnerability scanning tools. When migrating to IPv6, universities should proactively contact vendors for the latest security standards and hardening advice on IPv6.

Reference:
http://www.oregon.gov/DAS/EISPD/ESO/Pub/Trends/Trends_2011_01.pdf?ga=t
https://cloudsecurityalliance.org/csaguide.pdf
http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf

V. Summary

Technology innovations are emerging endlessly, which drives the current IT trends and brings enhanced system/network functionalities, simplified operational procedures and improved IT cost-effectiveness. Nevertheless, it also gives rise to more complex or unknown IT risks that impact the IT security strategy within universities.

To cope with the changing nature of IT risks, universities should adopt a more proactive approach to assess the associated security risks of IT trends and strengthen the IT security implementation by utilising the up-to-date techniques and management approaches.