CHAPTER 7
NETWORK AND COMMUNICATION SECURITY

7.1 Network Security Management

7.1.1 Recommendations for schools on building a secure network:

(a) Plan for the network security: all security issues, such as management policy, technical training and outsourcing requirements, should be considered early in the network design phase.

(b) Design physical and environmental security: put critical assets such as network communication lines, switches, routers, firewalls and network storage, e.g. network attached storage (NAS), in a locked server room.

(c) Use private Internet protocol (IP) address: schools should use private IP addressing scheme for internal networks to prevent internal networks from access by external networks.

(d) Design network security model by zoning: segregation of networks according to security requirements, e.g. the school internal network is totally isolated from the Internet, or the school's servers and computers are located behind the firewall, or set up a demilitarised zone (DMZ) network. Furthermore, unsecured or unmanaged systems should not be allowed to make connection to the internal network.

(e) Divide networks into separated network domains: schools may consider dividing their networks into separated network domains. The domains can be chosen based on trust levels, e.g. guest domain, student domain, staff domain, server domain. The segregation can be done by physical means or logical means, e.g. virtual private network (VPN). Furthermore, the perimeter of each domain should be well defined. Access between network domains is allowed, but should be controlled at the perimeter using a gateway, e.g. firewall and router. The criteria for segregation of networks into domains, and the access allowed through the gateways, should be based on an assessment of the security requirements of each domain.

(f) Configure firewall and network routers: harden the firewall and router through setting suitable access control list (ACL), by limiting the administrative access to specified locations, closing unnecessary network services for incoming and outgoing traffic or using encrypted communication channel for administration.

(g) Implement intrusion detection strategy: schools are recommended to implement intrusion detection strategy to detect abnormal activities or potential information security incidents. Installation of a network intrusion detection system (NIDS) or network intrusion prevention system (NIPS) on the network with the latest signatures so as to help to detect if there is an attack happening on the network. Schools are reminded that configuration of intrusion detection system (IDS) and intrusion prevention system (IPS) require tuning of signature and recognition patterns to reduce false alarms.

(h) Configure and secure management of information / communication systems: Schools should ensure that the information / communication systems are properly configured and securely managed, including turning off all unused services and setting security configurations properly. The configurations shall be reviewed regularly and updated if necessary.

(i) Configure servers: secure the server operating system by uninstalling unnecessary services and software, patch the system timely and disable unused accounts.

(j) Secure the applications: by means of installing security patches and hardening the configuration of the applications.

(k) Filter virus and malicious code: make sure that anti-malware software with up-to-date signature have been installed in desktop and network servers to prevent the spread of malware, e.g. virus, worm and trojan horse.

(l) Manage accounts and access privileges properly: access rights should be granted on a need basis and should be reviewed annually.

(m) Log security events and review regularly: logging and auditing functions should be provided to record network connection, especially for unauthorised access attempts. The log should be reviewed regularly.

(n) Develop security management procedures: e.g. security log monitoring procedure, change management procedure or patch management procedure.

(o) Develop a standard building of secure desktop: design a secured workstation configuration as the standard build of the school and make image backup of the build and replicate to the school's desktops. Furthermore, schools should develop backup and recovery strategies.

(p) Maintain good documentation: schools are recommended to maintain good documentation of configurations and procedures. Up-to-date system or network information, in particular, the network diagrams, internal network addresses, and configurations should be maintained to reflect the latest network environment for effective security control. Such information should be appropriately classified and securely stored.

(q) Provide training: schools should provide training to the technical support staff and users to ensure that they follow the security best practices and security policies.

7.1.2 Remote Access

(a) Remote access refers to the use of network resources from a remote location, which is not directly attached to the network.

(b) Schools are not recommended to use remote access software to connect to an internal server or user workstation directly. Such usage of remote access software can be a backdoor access by attackers to bypass firewall / router protection to the information system.

(c) To maintain the security of schools' infrastructure and information assets, schools should set up a policy to advise users on how to work remotely and securely. If use of remote access software is unavoidable, proper security controls that include logging feature should be in place. The remote access software should be enabled with idle timeout control to avoid unauthorised access. Schools should also provide secured channels, for example VPN connections, for users to connect to their internal networks. For remote access to their internal network via VPN connections, two-factor authentication is recommended.

(d) Schools should clearly identify users who would be granted with remote access privileges and what types of services could be provided to them. Schools should allow only authorised users to gain remote access to the network with proper authentication and logging.

(e) Users should properly protect those remote computers, by installation of personal firewall, anti-malware software and malware detection and repair measures, etc. All these security features should be activated at all times and with the latest malware signatures and malware definitions applied. Besides, latest security patches shall be applied to these remote computers. A full system scan should be performed to detect any malware in these remote computers before connecting to the school's internal network.

(f) To avoid information leakage, users should minimise storing school's information on remote or portable computers. Confidential information is not recommended to store in privately-owned computers, mobile devices or removable media.

(g) When working in public areas, users should avoid working on sensitive documents to reduce the risk of exposing to unauthorised parties. Users should also avoid using public printers. If printing is necessary, the printout should be picked up quickly. Furthermore, users should protect the remote computers with password-enabled screen saver and never leave the computers unattended.

7.1.3 Virtual Private Network (VPN)

(a) Setup of VPN is considered to be a viable solution to establish secure communication channel for users to work outside office. Before implementing VPN, schools should evaluate compatibility with the existing network and consider implementing the following VPN security suggestions:

- Authentication with either one-time password authentication such as a token device or public / private key system with a strong passphrase.
- Disconnect automatically from the school's internal network after a pre-defined period of inactivity. The user must then logon again to reconnect to the network.
- Disallow dual (split) tunnelling. Only one network connection is allowed.
- Protect all computers or devices connected to the school's internal networks via VPN with personal firewall, latest security patches, anti-malware and malware detection and recovery software. All these security measures should be activated all the time and with the latest malware signatures and definitions.

- Provide logging and auditing functions to record network connection, especially for failed access attempts. The log should be reviewed regularly to identify any suspicious activities.

- Remind users with VPN privileges that they are accountable for the proper use of the account.

- Educate teachers, supporting staff as well as remote users to ensure that they follow the security best practices and policies during the implementation and usage of VPN.

- Install gateway-level firewalls to control network traffic from VPN clients to authorised information systems or servers.

7.2 Wireless Network Build Up Security Concerns

7.2.1 Wireless local area network (WLAN) is generally considered as an un-trusted network that should not be used to transmit confidential / sensitive / private information without proper security controls.

7.2.2 Schools should be aware of the security risks associated with wireless networks. For examples:

(a) One characteristic of a wireless signal is that it generally fills the space within the WLAN's coverage, and can penetrate beyond building walls and windows. Thus, there is potential security risk that anyone can pick up and read such signals unless security measures have been incorporated to guard the wireless transmissions against offensive "listening".

(b) Malicious entities may gain unauthorised access to the school's internal network through wireless connections, potentially bypassing firewall protections and launch attacks.

(c) Computer malware may corrupt data on a wireless device and be subsequently introduced to a wired network.

(d) Malicious entities may deploy unauthorised equipment, e.g. client devices and access points, to surreptitiously gain access to or modify information.

(e) Information that is not encrypted (or that is encrypted with poor cryptographic techniques) and transmitted among wireless devices may be intercepted and disclosed.

(f) Denial-of-Service (DoS) attacks may be easily directed at wireless connections or devices.

(g) A fake wireless access point may be established to collect the information traveling across the WLAN.

(h) The design flaws in the security mechanism of the 802.11 standard also give rise to a number of potential attacks, both passive and active. These attacks enable intruders to eavesdrop on, or tamper with, wireless transmissions.

7.2.3 Recommendations for schools on wireless network deployment:

(a) Keep track of WiFi development standards: Since the 802.11 standard was first introduced, enhancements have continuously been made to strengthen data rates, signal range, and security of wireless networks. Therefore, it is a good idea to keep track of the development of new standards when they appear, in particular when procuring new equipment or acquiring new wireless network services. In any new purchase, protection by one of the stronger wireless security protocols such as WiFi Protected Access (WPA) / advance encryption standard (AES) or WPA2 / AES should be considered, but by no means should such wireless security protocols be solely relied upon to protect data confidentiality and integrity, as new weaknesses in protocols may be discovered in the future.

(b) Before designing the wireless network, it is important to understand the school's operational and functional requirements of the wireless solution. These requirements may affect decisions on what kind of security measures should be deployed to protect the network. For example, if guest access will be required, security best practices for guest access should be considered in the design stage.

(c) The school should develop a strong wireless security policy to address all the usage options of wireless networks and the types of information that can be transmitted. The policy should outline a framework for the development of installation, protection, management and usage procedures. Security and operation guidelines, standards and personnel roles should also be clearly defined.

(d) Perform security risk assessments and audits to identify security vulnerabilities: Security assessments and audits are essential means for checking the security status of a wireless network and identifying any corrective action necessary to maintain an acceptable level of security. These assessments can help identify loopholes in the wireless network, such as poorly configured access points using default or easily guessed passwords and Simple Network Management Protocol (SNMP) community strings, or the presence or absence of encryption. However, a security risk assessment can only give a snapshot of the risks to information systems at a given time. As a result, it is important to perform assessments and audits regularly once the wireless network is up and running.

(e) Perform site surveys: Due to the nature of radio frequency (RF) propagation, radio signal emissions cannot generally be contained within a particular building or location. Excessive coverage by the wireless signal could pose significant threat to the organisation, opening it to “Parking Lot” attacks on the network. Therefore, it is necessary to have a good understanding of the coverage requirements for the desired wireless network during the network planning phase. By performing a site survey, one can identify:

- The appropriate technologies to apply.
- Obstacles to avoid, eliminate, or work around.
- Coverage patterns to adopt.
- Amount of capacity needed.

7.2.4 It is recommended to build the WiFi network completely separated from schools’ existing network with a separate broadband line to reduce security risk. Due to the nature of wireless technology, wireless networks are relatively hard to contain within a building and it is generally considered to be an un-trusted network. As a best practice, wireless networks and wired networks should not be directly connected to each other. It is common to deploy firewalls to separate and control the traffic between different networks. For example, Address Resolution Protocol (ARP) broadcast packets should be blocked from entering a wired network from a wireless network since a malicious user could uncover internal information, such as Ethernet Media Access Control (MAC) address from these broadcasts.

7.2.5 Schools' IT personnel needs to assess, understand and eliminate the security issues and risks to schools' existing network when the WiFi network is integrated or connected to schools' existing network. Schools adopting the integration mode of WiFi networks are recommended to apply the "Defence-in-Depth" approach. The concept of "Defence-in-Depth" has been widely employed in the secure design of wired networks. The same concept can also be applied to wireless networks. By implementing multiple layers of security, the risk of intrusion via a wireless network is greatly reduced. If an attacker breaches one measure, additional measures and layers of security remain in place to protect the network. Separation of wireless and wired network segments, use of strong devices and user authentication methods, application of network filtering based on addresses and protocols, and deployment of intrusion detection systems on the wireless and wired networks are all possible measures that can be employed to build multiple layers of defence.

7.3 Security Controls to Protect Wireless Local Area Network

7.3.1 Management Control to Secure the WLAN

(a) Define a wireless security policy to address the usage of WLAN and type of information that can be transmitted over WLAN.

(b) Develop and securely keep a coverage map of the WLAN, including locations of respective access points and service set identifier (SSID) information so as to avoid excessive coverage by the wireless signal.

(c) Ensure the hardware and software are properly maintained and patched.

(d) Search regularly for rogue or unauthorised wireless access points.

(e) Perform regular IT security risk assessments and audits to identify security vulnerabilities.

(f) Keep a good inventory of all devices with wireless interface. Once a device is reported missing, consider modifying the encryption keys and SSID.

(g) Implement strong physical security controls and user authentication for complementing physical security deficiencies of wireless devices.

(h) Install access points far from a window or a door to prevent network tapping from publicly accessible area.

(i) Schools are recommended to restrict access from guest WiFi network to schools' internal network.

7.3.2 Technical Controls to Secure the WLAN

(a) Change network default name at installation; SSID should not reflect the name of the school, system name or product name / model.

(b) Change product default access point configuration settings which are considered unsecured most of the time for easy deployment.

(c) Disable all insecure and unused management protocols on access points and configure the required management protocols with the least privilege.

(d) Ensure that all access points have strong, unique administration passwords and change the passwords regularly.

(e) Enable and configure security settings including SSID, encryption keys, SNMP community strings.

(f) Deploy WPA2-Enterprise, or change encryption keys regularly if WPA2-Personal is used.

(g) Disable SSID broadcasting to prevent the access points from broadcasting the SSID so that only authorised users whose configured SSID matches that of the access point can connect to the network.

(h) Disable DHCP and assign static IP addresses to all wireless users to minimise the possibility of an unauthorised user obtaining a valid IP address.

(i) Use MAC address filtering for configuring access points so that they allow only clients with specific MAC addresses to access the network, or allow access to only a given set of MAC addresses.

(j) Activate logging features and redirect all log entries to a remote logging server if possible. The log records should be checked regularly.

(k) Install wireless intrusion detection system (WIDS) or wireless intrusion prevention system (WIPS) to monitor the WLAN.

(l) Deploy VPN on top of WLAN for connection to the school's internal network.

(m) Segment the access point's coverage areas to balance the loading and minimise the probability / impact of DoS attack.

(n) Erase all sensitive information, such as system configurations, pre-shared keys, digital certificates and passwords, on the devices upon disposal of wireless components.

(o) Disable Universal Plug and Play (uPnP) on access points to prevent malware from bypassing the firewall via the connected devices.

7.3.3 End User Controls to Secure the WLAN

(a) Install firewall and enable anti-malware protection on wireless clients, e.g. mobile devices.

(b) Turn off sharing or tethering at wireless clients.

(c) Do not attach the wireless clients to the school's internal network while it is connected to a third party WLAN.

(d) Keep strict control of the wireless interface device, e.g. USB WiFi dongle, as access credentials such as SSID and/or encryption key are commonly stored on this device.

(e) Disable wireless connection when it is not in use.

(f) Encrypt sensitive / personal data on the device.

(g) Remove your preferred network list when using public wireless services.

(h) Do not enable both wireless and wired network interface cards at the same time.

7.4 Mail Gateway Security and Email Handling

7.4.1 Mail Server Protection

(a) A mail server should be run behind a firewall system which helps to restrict the access to the mail server and provide various security protections. Also, firewalls or routers should be properly configured to block unwanted traffic, such as traffic from particular IP addresses of known spammers, into the mail server or gateway.

(b) Anti-malware protection should be adopted for filtering inbound and outbound email including any attachments that contain malware.

(c) The email system should not disclose names or IP addresses of internal networks or systems. It should be properly configured to avoid disclosing internal systems or configurations information in email headers.

(d) Use Email systems provided by reliable service providers.

7.4.2 Tips for protecting schools from email bombing, spamming and spoofing:

(a) Remove unused mail daemons such as Sendmail if not used.

(b) Keep mail gateway software up-to-date.

(c) Enable logging to record origin or header information of the spoofed email. Use intrusion detection and prevention systems (IDPS) to detect any suspicious activities such as sudden increase of incoming / outgoing emails from the same originator to assist the detection / prevention of mail bombing.

(d) Properly configure the firewall and router to allow incoming simple mail transfer protocol (SMTP) connections to a dedicated email gateway or server only to centralise the logging and traffic control.

(e) Mail relaying to and from unauthorised users or non-existence addresses should be blocked. For example, a mail server should only allow mail relay for some specified internal IP addresses or authorised internal users, but not external ones.

(f) Mail daemons or mail gateway software, which can filter out invalid messages, should be properly set up to remove junk mails or invalid messages such as from unauthorised domains or with invalid email headers.

(g) Set a limit on the maximum file size of an email, or on the maximum number of email messages that can be transmitted within a certain period of time. This can avoid flooding to eat up all available network resources or disk space.

(h) Update spammer list regularly.

(i) Set up spam blocking system before mail server to block out unwanted emails. Such spam blocking system acts as an email gateway to filter out spam emails before entering the mail server based on various criteria, such as email header, content, spam blacklist, spam whitelist, reverse domain name system (DNS) lookup, sender policy framework (SPF) and DomainKeys Identified Mail (DKIM) information.

7.4.3 Schools can implement a variety of methods to reduce the amount of incoming spam, such as protecting schools' email addresses, using filtering software and adopting well-defined security measures for workstations and email servers. The following are some tips:

(a) Schools should establish and enforce clear information security policies, and educate users not to respond to spam emails.

(b) Schools could restrict the use of school email addresses for personal messages or participation in newsgroup or chat rooms by users.

(c) When publishing the email address on school's website, the schools should consider writing it in a way that makes harvesting by spammers more difficult. For example, write the email address as "info[at]xyz.edu.hk" instead of "info@xyz.edu.hk", and consider adding a statement stating that the school do not wish to receive unsolicited emails, such as "No spam, please".

(d) Install email filter software at the server level if your school has its own email server. Filtering software can screen incoming messages before they are delivered to users.

(e) If your school use a web-based email service from an Internet service provider (ISP), they may provide the school with a number of anti-spam settings for protection. To reduce the risk of mistakenly blocking non-spam messages, schools may also consider adding a holding folder to the filtering system, so that messages can be reviewed before deletion.

(f) Adopt good security measures such as server hardening to protect the school's email server and web server from being hacked and used by third parties to send spam emails.

7.4.4 Spammers collect users' email addresses and verify that they are valid addresses before they start sending spam emails. To reduce the possibility of receiving spam emails, users must protect their email addresses / accounts and their computers. The following are some tips:

(a) Users are not recommended to disclose personal information including email addresses too readily and publish personal email address on public websites, contact directories, membership directories, or chat rooms.

(b) Users are recommended to provide separate email addresses for different purposes.

(c) Users are not recommended to use an email address that contains simple dictionary word or common names.

(d) Users should be aware of the spammers' favourite tricks, such as the use of subject headings like "Remember me?"

(e) Users should be cautious when opening emails and email attachments, especially when receiving emails from strangers.

(f) Users are recommended to simply delete emails from unknown senders or dubious sources.

(g) User should check the "sent" folder or outgoing mailbox of their email programme (or webmail account) to see if there are any outgoing messages that were not sent by them. If there are such messages, the user's computer may have been hacked and used by spammers to send emails from the user's computer. The user should disconnect from the Internet immediately and scan the computer with anti-malware software (make sure the software's signatures are up-to-date).

7.4.5 Protection against Email Scam

(a) Apart from causing annoyance to recipients, unsolicited emails can also be deceptive and deliberately fraudulent in nature, leading to infection by viruses, identity theft, or even financial loss if instructions described in the messages are followed. Such fraudulent messages are called "scam emails".

(b) The Hong Kong Police Force provides advice for avoiding the traps set by these fraudulent emails. For details, please visit:

https://www.police.gov.hk/ppp_en/04_crime_matters/ccb/fst.php?msg_id=cct_16