Hang Seng Management College Information Technology Services Centre

Title	Guidelines for Network Security
Last Update	3 March 2016

Introduction

1. This document serves as a guideline of proper protection with appropriate security measures of all college logical networks and physical network equipment. It describes the effective manner of maintaining and administrating the network addresses, configurations, equipment and information for limiting unauthorized network accesses and applications.
2. This document is updated from time to time to maintain accuracy and whenever security policy changes.

Classifications of HSMC Networks

3. In general, the college classifies the campus network into “Public Network”, “Managed Network” and “Secured Network” according to the security level of hosted services for efficiently controlling network activities.
    a. **Public Network** – The wired data nodes installed at all open areas such as corridors, lobbies, etc. are classified into “Public Network” by which any users can plug their devices into HSMC network. Besides, WiFi networks also falls into this class. However, user devices on Public Network cannot have layer 2 bi-directionally access permission of HSMC Managed and Secured Networks, except necessary services such as DHCP, DNS, Account Authentication, etc.
    b. **Managed Network** – The managed network are the data nodes which are connecting with HSMC managed equipment such as computers, copiers, servers, etc. The locations of Managed Network include classroom, computer labs and all staff offices. Normally, the proper network traffic of Managed Network equipment may access the generic servers on Secured Network.
    c. **Secured Network** – The equipment on Secured Network is strictly quarantined to ensure the pernicious network activities away from HSMC core IT services. All general purpose servers and high confidential servers are hosted in Secured Network. In addition, networks of some departments handling the confidential information are also regarded as Secured Network. According to the confidentiality of the hosted IT services, Secured Network is further derived into different sub-networks to enable flexibility of access control.

Risk Management Strategy

4. Aside from network classification, ITSC has conducted Risk Analysis on IT network for applying an appropriate level of security against the possible means of attack and vulnerability.
    a. **Low Risk** – The abnormal network activities found in the access network switches connecting to the Public network that would not disrupt the operations or cause legal or financial ramifications are classified as Low Risk.
    b. **Medium Risk** – The abnormal network activities found in the access network switches connecting to the Managed network that would cause a moderate disruption in the operations, minor legal or financial ramifications are classified as Medium Risk.
    c. **High Risk** – The abnormal network activities found in the core network equipment connecting to the Managed and Secured networks that would cause major disruption in the operations, minor legal or financial ramifications are classified as High Risk.

Local Wired Network Security

5. Local wired network is a critical IT service for HSMC users, since it provides the core IT connectivity for daily teaching, learning and college administration works. To prevent from the internal network sniffing and viruses dispersion, the following security technologies are applied to HSMC local wired network.
6. Strategies
    a. **Network Segregation**
        i. Network Segregation is a fundamental and effective strategy to harness the network traffics flowing from the Public network to the Managed and Secured Networks such that virus and network intrusions can be controlled. To efficiently segregate the networks, layer 2 VLAN technology is enabled on the core network equipment. And the networks are partitioned by the secure VLAN filters which block the undesired traffics across networks.
        ii. Aside from the generalized classification of the wired networks into Public, Managed and Secured, the specific design of sub-classification of network infrastructure is necessary for efficient segregation control.

    b. Network Port Security Control
        i. Network Port Security Control consists of different configurations to eliminate the possibility of network information being captured by the malicious users and network outage.
        ii. Switch Port Security: By network switch port security mechanism, all network switch ports were configured for restricting the unauthorized network switch plugging in.
        iii. DHCP Snooping: It is another mechanism on HSMC network to prevent the users from plugging their unauthorized routers and rogue DHCP server. iv. Spanning Tree Protocol with BPDU Guard: The protocol was enabled in all network switch to prevent from the infinitive loopback caused by inadvertent

wiring and misconfiguration of BPDU generated by other unauthorized devices on the network.

c. Monitoring Tool

i. ITSC has a fast responding network monitoring system using SNMP to proactively generate the alerts for the abnormal network activities and equipment failures. In case of abnormal network activities or equipment failure situations are identified the following risk mitigation strategies will be applied.

Risk Mitigation Guideline for Local Wired Network		
Levels	**Identification**	**Actions**
Low Risk	Invalid packets sent within 5 mins	Keep monitoring the activities by the network officer
Medium Risk	Invalid packets sent over 15 mins	Report to network team supervisor and disable the connecting network ports if necessary
High Risk	Invalid packets sent over 30 mins	Disable the connecting network ports with the malicious activities imminently and report to the Director of ITSC

Local Wired Network Security

7. There is a significant paradigm shift of teaching and learning technology, such as adopting mobile phone and tablet devices, ITSC deployed a robust and fit-for-purpose wireless system on campus. Over 400 wireless points have been installed at open areas, classrooms, computer labs and staff offices to provide over 90% single coverage on campus.
8. However, wireless radio single is a vulnerable media to sniffing. Thus, the devices on Secured network are not allowed to ride on the wireless media for data transmission. Generally, wireless network users are prohibited from accessing IT services on Secured work other than the TCP/UDP 80 and 443 ports.
9. Strategies

a. Wireless Data Transmission Encryption

i. HSMC wireless service is using a de-facto WPA2 method with AES algorithm encryption standard to alleviate the risk of being intercepted by other rouge devices.

ii. Client fingerprinting option is enabled for the purpose of collecting the wireless device identification for further security investigation if necessary.

b. Secured Authentication

i. Since 2015, HSMC wireless system has been employing the dynamic 802.1X authentication technology for the users to login on the wireless network.

ii. The technology can assign an appropriate network to the users according to their security group during the wireless service login. And layer 2 VLAN filter of local wired network is also applicable to wireless users for protecting the secured services.

c. System Monitoring and Logging

i. Aside from the proactive monitoring the wireless console, ITSC has a syslog server to capture the wireless malicious activities for further analysis if necessary.

ii. In addition, SNMP email alerts for wireless traffic will be triggered if the threshold is reached.

Internet Security

10. Internet service is an important service to HSMC users, since most of teaching and learning activities need to access the sources on Internet. Although HSMC has a redundant Internet link for contingency service, the security control of Internet access is not neglected.
11. Strategies

a. Three Tire Firewall and Web Application Firewall

i. Three tire firewall design is to protect the backend servers from being intruded through different layers of network. ii. The first tire firewalls are placed at two Internet links to secure the incoming traffics from external to backend servers.

iii. The second tire firewalls are to provide the protection for the backend physical servers accessing by the internal users on Public and Managed Networks.

iv. The third tire firewalls are virtualized firewalls which mainly control the dispersion of viruses across virtualized server subnets.

v. Nowadays, the Internet hacking activities are not just limited to network layer but also on application layer, thus ITSC deployed Web Application Firewall in front of the server farms to mitigate the attacks on the programming level. **b. SSL VPN**

i. For the authorized remote users to access internal secured server services, ITSC has SSL VPN service to provide 2048 bits encryption on data transmission to secure the data not being lacked on Internet.

ii. In addition, the SSL VPN was configured with role based access control such that the access permission of different network zones can be only reached by the specific users.

c. Security Policy Control and Public IP Zoning

i. For the outgoing traffics, ITSC enabled the restricted policies on the front end firewalls to limit the accessible external TCP/UDP ports. Normally, only TCP/UDP 80 & 443 ports are allowed for outgoing Internet access by which the rogue servers cannot be set up on the campus network.

ii. Public IP Zoning is a design to assign different source NAT IP addresses for different groups of users and servers. By this design, ITSC can trace the sources of abnormal network traffic and stopped them efficiently without affecting other users and services.