Office of the Government Chief Information Officer

INFORMATION SECURITY

Practice Guide

for

Wi-Fi Security

Version 1.1

June 2021

Amendment History				
Change Number	Revision Description	Pages Affected	Revision Number	Date
1	Update Abbreviation and Terms	1	1.1	June 2021

Table of Contents

1. Introduction

This document is intended to serve a diverse group of audience, such as management, system owners, IT Security Administrators, Local Area Network (LAN)/Systems Administrators, and information security stakeholders, who have the responsibility to setup and manage the Wi-Fi network within the government.

Some Bureaux/Departments (B/Ds) users may use mobile devices with a wide variety of communication technologies including Wi-Fi. For details of security guideline of adoption of mobile devices and related management, please refer to the Section 4 of Practice Guide for Mobile Security.

1.1 Purpose

The purpose of this document is to provide common security considerations and best practices to B/Ds on the design, management and operation of Wi-Fi network within government. The best practices are described in Section 4.

1.2 Normative References

The following referenced documents are indispensable for the application of this document.

- Baseline IT Security Policy [S17], the Government of Hong Kong Special Administrative Region
- IT Security Guidelines [G3], the Government of Hong Kong Special Administrative Region
- Information technology – Security techniques – Information security management systems – Requirements (second edition), ISO/IEC 27001:2013
- Information technology – Security techniques – Code of practice for information security controls (second edition), ISO/IEC 27002:2013

1.3 Terms and Convention

For the purposes of this document, the terms and convention given in S17, G3, and the following apply.

Abbreviation and Terms	
Wi-Fi	Wi-Fi refers to the wireless LAN technologies that utilize the IEEE 802.11 standards for communications.

5G	5G stands for the fifth generation of mobile telecommunications which is formulated by International Telecommunications Union (ITU).

1.4 Contact

This document is produced and maintained by the Office of the Government Chief Information Officer (OGCIO). For comments or suggestions, please send to:

Email: it_security@ogcio.gov.hk

Lotus Notes mail: IT Security Team/OGCIO/HKSARG@OGCIO

CMMP mail: IT Security Team/OGCIO

2. Information Security Management

Information security is about the planning, implementation and continuous enhancement of security controls and measures to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission and its associated information systems. Information security management is a set of principles relating to the functions of planning, organising, directing, controlling, and the application of these principles in harnessing physical, financial, human and informational resources efficiently and effectively to assure the safety of information assets and information systems.

Information security management involves a series of activities that require continuous monitoring and control. These activities include but not limited to the following functional areas:

- Security Management Framework and the Organisation;
- Governance, Risk Management, and Compliance;
- Security Operations;
- Security Event and Incident Management;
- Awareness Training and Capability Building; and
- Situational Awareness and Information Sharing.

Security Management Framework and Organisation

B/Ds shall establish and enforce departmental information security policies, standards, guidelines and procedures in accordance with the business needs and the government security requirements.

B/Ds shall also define the organisation structure on information security and provide clear definitions and proper assignment of security accountability and responsibility to involved parties.

Governance, Risk Management and Compliance

B/Ds shall adopt a risk-based approach to identify, prioritise and address the security risks of information systems in a consistent and effective manner.

B/Ds shall perform security risk assessments for information systems and production applications periodically and when necessary so as to identify risks and consequences associated with vulnerabilities, and to provide a basis to establish a cost-effective security program and implement appropriate security protection and safeguards.

B/Ds shall also perform security audit on information systems regularly to ensure that current security measures comply with departmental information security policies, standards, and other contractual or legal requirements.

Security Operations

To protect information assets and information systems, B/Ds should implement comprehensive security measures based on their business needs, covering different technological areas in their business, and adopt the principle of "Prevent, Detect, Respond and Recover" in their daily operations.

- Preventive measures avoid or deter the occurrence of an undesirable event;
- Detective measures identify the occurrence of an undesirable event;
- Response measures refer to coordinated actions to contain damage when an undesirable event or incident occurs; and
- Recovery measures are for restoring the confidentiality, integrity and availability of information systems to their expected state.

Security Event and Incident Management

In reality, security incidents might still occur due to unforeseeable, disruptive events. In cases where security events compromise business continuity or give rise to risk of data security, B/Ds shall activate their standing incident management plan to identifying, managing, recording, and analysing security threats, attacks, or incidents in real-time. B/Ds should also prepare to communicate appropriately with relevant parties by sharing information on response for security risks to subdue distrust or unnecessary speculation. When developing an incident management plan, B/Ds should plan and prepare the right resources as well as develop the procedures to address necessary follow-up investigations.

Awareness Training and Capability Building

As information security is everyone's business, B/Ds should continuously promote information security awareness throughout the organisations and arrange training and education to ensure that all related parties understand the risks, observe the security regulations and requirements, and conform to security best practices.

Situational Awareness and Information Sharing

As cyber threat landscape is constantly changing, B/Ds should also constantly attend to current vulnerabilities information, threat alerts, and important notices disseminated by the security industry and the GovCERT.HK. The security alerts on impending and actual threats should be disseminated to and shared with those responsible colleagues within B/Ds so that timely mitigation measures could be taken.

B/Ds could make use of the cyber risk information sharing platform to receive and share information regarding security issues, vulnerabilities, and cyber threat intelligence.

3. Overview of Wi-Fi Security

3.1 Introduction to Wi-Fi network

Wi-Fi is the type of the wireless communication technologies based on IEEE 802.11 family commonly used for IT equipment such as mobile phones, portable computers, Global Positioning System (GPS) units as well as Internet of Things (IoT) devices to access LAN or Internet.

Wi-Fi uses high-frequency radio waves (wireless signal) rather than wires to communicate between IT equipment and devices. One characteristic of a wireless signal is that it generally fills the air within the wireless LAN's coverage, and can penetrate beyond physical borders, such as building walls and windows. Thus, there is a potential security risk that anyone can read such signals outside the physical border unless security measures have been incorporated to guard the wireless transmissions against offensive "listening". Wi-Fi with connection to government internal network shall be used with sufficient authentication and transmission encryption measures, complemented by proper security management processes and practices.

3.2 A typical Wi-Fi Network

A typical Wi-Fi network is briefly introduced for reference. B/Ds should determine the configuration of their Wi-Fi network according to their business needs and operation.

A typical Wi-Fi network could have four major components: client devices, Wi-Fi Access Points (APs) and network routers/switches, a management system and an Internet gateway. Examples of client devices are notebook computers, tablets and smartphones. APs provide wireless network connectivity with client devices and connection. Network routers connect APs and the management system at the backend. A management system monitors and controls the activities on the Wi-Fi network. It typically includes wireless intrusion prevention system, wireless network management system, authentication system and anti-malware system. The management system is required to handle security threats at network and application levels, such as unauthorised access and malicious activities. The Internet gateway manages the connection with the Internet Service Providers. It also includes firewall, intrusion detection or prevention system and the router that connects the internal network to the Internet.

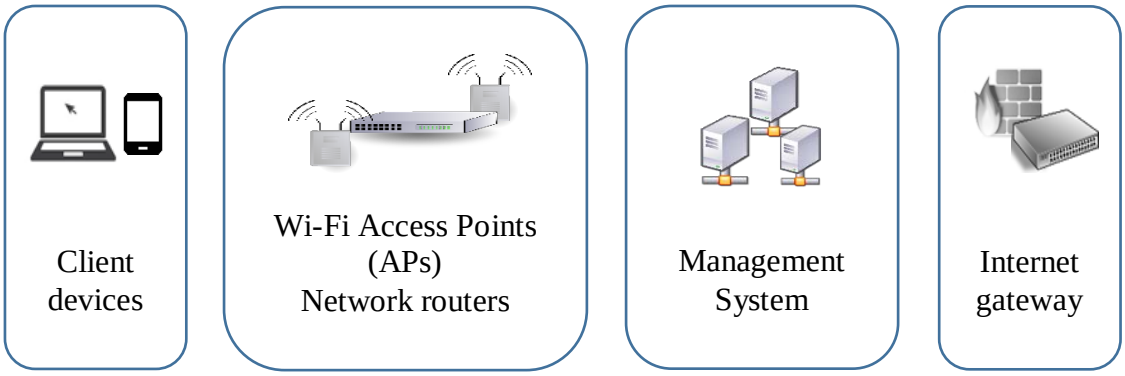

Figure 1 Four major components of a typical Wi-Fi network

4. Threats and Vulnerabilities of Wi-Fi Networks

4.1 Threats and Vulnerabilities

Nowadays, due to its wide range of advantage, the wireless connection plays important role everywhere from large organisations to individual personal use computers and networks. However, the greater availability of wireless networks means increased danger from attacks and increased challenges to an organisation, IT staff and IT security professionals. The security threat to the network can be the attacker who attempts to grasp information to exploit the network vulnerability. The security threats of a Wi-Fi network are described below.

APs

- Wired Equivalent Privacy (WEP) / Wi-Fi Protected Access (WPA) cracking

  The wireless network protected by previous version of security protocol, such as WEP or WPA are not secure as per today's technology.

- Misconfigured APs

  APs with weak or incorrect settings that allow unauthorised devices to connect or expose connection communications to sniffing and replay attacks.

- Wireless sniffing

  If APs are not properly configured and the traffic they carry is not encrypted, this can put sensitive communications or transactions at risk. If the network traffic being transmitted is clear text, malicious attackers could use sniffing tools to obtain sensitive information such as passwords or credit card numbers.

- Evil twin (spoofing)

  An evil twin is a bogus type Wi-Fi connection which fools users that believing that it is the legitimate connections to phishing attacks as well as exploitation of the data transaction purposes. In an evil twin attack, an attacker gathers information about an AP, then sets up their system to impersonate it. The attackers use a broadcast signal stronger than the one generated by the legitimate AP to let unsuspecting users connect to their AP.

- Rogue access point (unauthorised equipment)

  The rogue access point is the AP installed without explicit permission of a network administration. It creates the potential for the man-in-the-middle attack where the security of a network has breached.

Wi-Fi Signal

- Piggybacking

  The broadcast range of an AP can make wireless connections available outside building walls and windows. If a wireless network is not properly configured, anyone with a wireless-enabled computer in range of an AP can use the connection. These unintended users may be able to conduct illegal activities, monitor and capture network traffic, or steal files from the network.

- War driving

  Similarly to piggybacking, war driving refers to the practice of physically searching for unsecured wireless networks or networks that can easily be compromised.

- Denial of service (DoS)

  DoS refers to the attack with a view to depriving the service availability of an entity. Jamming makes use of intentional radio interferences to harm directly wireless connections or devices by keeping them busy.

- Eavesdropping

  Eavesdropping refers to the act of secretly listening to the communications. The unauthorised monitoring of the network traffic between the client devices and APs is susceptible to eavesdropping and with no sign of physical interception.

Mobile devices with Wi-Fi connection

- Internet Connection Sharing and Bridging Clients

  A device that shares its Internet connection or allows connectivity to multiple networks concurrently can be used to bypass network monitoring and security controls. This may result in data loss or provide an unsecured network entry point for an attacker.

- Theft of Mobile Devices

  Taking measures to protect mobile devices with Wi-Fi connection from loss or theft is important. By physically stealing mobile devices, attackers could have unrestricted access to all of its data, as well as any connected cloud accounts.

5. Security Considerations for setting up and operations of Wi-Fi Networks

In general, the security considerations for setting up and operations of a wired network are applicable to a Wi-Fi network. Specifically, B/Ds should develop a Wi-Fi security policy as well as follow the practice of protection measures described in this section for a Wi-Fi network. A plan with security considerations for the setting up and operations of Wi-Fi network is effective to reduce the network's exposure to the more common types of attacks on systems.

5.1 Security Considerations for setting up a Wi-Fi Network

The security measures and controls should be deployed to protect a Wi-Fi network. Below are some common considerations grouped by different parties, such as network owner, network administrator and end users.

Network Owner

- Purpose of Wi-Fi network

  The purposes and functional requirements of the Wi-Fi network should be clearly specified. If it is a standalone Wi-Fi network for external users to get access to Internet, the Wi-Fi network shall be physically separated from B/D's departmental networks. The access control to the Wi-Fi network should also be specified for different kinds of users and the kind of data to be transmitted and its data protection level.

- Wi-Fi Security Policy

  A Wi-Fi security policy should be developed to address all the usage options of wireless network and the types of information that can be transmitted. The policy should be reviewed regularly to cope with the latest technological and business developments. The policy should include but not limited to defining the roles and responsibilities for Wi-Fi management, the installation and usage procedures as well as the operation guidelines.

  For example, usage policy should be in place, such as disabling Wi-Fi functions when they are no longer in use and encryption key, credentials for accessing Wi-Fi network should not be shared or disclosed, and assigning a separate WLAN for guest users. Staff are also not allowed to set up their own access points.

- Data protection and configuration backup

  This measure includes data at rest encryption, secure data transmission and regular backup of all valuable information on client devices and endpoints as well as configuration files on network devices.

- IT security risk assessments and audits

  The Wi-Fi network shall be subject to regular Security Risk Assessment and Audit (SRAA). B/Ds shall take necessary remedial actions on any security vulnerabilities identified in the SRAA. In view of the rapid change of Wi-Fi technology, SRAA for the Wi-Fi network shall be conducted annually.

- Monitoring and prevention

  These measures involve logging and auditing network activities, vulnerability scanning, effective information dissemination mechanism and the provision of security awareness training to all staff on the Wi-Fi security policies. Active logging should be redirected to a remote logging server and ensure the completeness and integrity of all logs. The log records should be reviewed and checked regularly as well as analysed in case of any suspicious activities detected.

- Security Incident Handling

  B/Ds need to follow the prevailing information security incident response mechanism to report any security incidents in relation to the Wi-Fi network to the Government Information Security Incident Response Office (GIRO). The mechanism should also be updated with regard to new potential security threats. B/Ds also need to provide a contact point such that in case of emergency, the Wi-Fi network set up in the B/Ds need to be shut down with short notice.

- Keep an inventory and define hardware disposal policy

  Keep an accurate inventory for all Wi-Fi components including network switches, routers, Internet gateway, APs and other related components to make sure only authorised devices to be connected to the Wi-Fi network. Once a device is reported missing, the encryption keys and SSID should be changed immediately.

  In hardware disposal policy, it should include the requirement to erase all sensitive information, such as system configurations, pre-shared keys, digital certificates and passwords, on the devices upon disposal of all hardware, including any Wi-Fi components or devices.

- Define patch management policy

  Test and update the latest firmware and security patches of all hardware, devices and software regularly to prevent inadvertent and malicious exploits.

Network Administrator

The network administrator should consider the following security measures in various areas to protect the availability of the Wi-Fi network as well as the confidentiality of the information.

- Wi-Fi network capacity

  To ensure the availability of a Wi-Fi network, the capacity of wireless connection should be evaluated by considering the size of user population of Wi-Fi network and types of applications (e.g. voice/video conferencing, or web browsing).

- Physical protection and location of APs

  Wireless radio signal cannot generally be contained within a particular area. Excessive coverage by the Wi-Fi signal could pose significant threats and attack surfaces to malicious users. Hence, the location of APs and the strength of the wireless signal should be carefully designed such that the wireless signal should not be available outside the designed area as practically possible. For example, APs should be considered to be installed far from windows or doors to prevent network tapping from publicly accessible areas. Cross-interference with co-located wireless networks should also be avoided. A site survey is recommended to be conducted to identify the coverage map of Wi-Fi infrastructure, the number of APs, and their location and signal coverage and quality.

  The network equipment, such as APs, should be installed in facilities with strong physical security controls against thefts, sabotage or tampering, in particular for APs placed in open area. For example, APs should be considered to be installed at ceiling and wiring closets should be locked. In addition, it should consider using any locking mechanisms to physically limit access to the power buttons, reset buttons or ports (e.g. USB) of the APs.

- Network segmentation

  The network segmentation of Wi-Fi network should be adopted for guest, application development and internal network. Segmentation of the access point coverage areas can also balance the loads on a Wi-Fi network so as to minimise the availability risk. In addition, interconnection between Wi-Fi and wired networks should be restricted. The access controls between the segmented Wi-Fi networks should be adopted (e.g. firewall, port/application/MAC address filtering).

- Communication standards

  The communication standards for Wi-Fi networks are based on IEEE 802.11 standards such as 802.11g, 802.11ac, 802.11i, 802.11n and the latest standard 802.11ax. From a security perspective, the 802.11ax (Wi-Fi 6) with the Wi-Fi Protected Access 3 (WPA3) protocols introduces enhanced authentication and encryption functions.

Wi-Fi 6 is the latest standard of Wi-Fi technology. It was designed in response to the growing number of wireless devices and gadgets worldwide. Comparing with previous version, 802.11ac, it improves the functionalities and features. The latest version of communication protocol, such as the IEEE 802.11ax, should be considered to build up their Wi-Fi networks, especially for the IoT-based system that may connect up to thousands of devices to be connected.

WPA3 has two modes, namely WPA3-Enterprise and WPA3-Personal. The WPA-3 Enterprise mode is recommended as it provides enhanced security features to build up the Wi-Fi network. If WPA3-Personal mode is used, the encryption keys should be regularly changed.

- Internet gateway

Security measures in Internet gateway include firewalls, intrusion detection systems and intrusion prevention systems to detect and protect from any suspicious activities. Firewall should be installed to guard against network attacks and intrusions. B/Ds should also scan/monitor network traffic, and filter suspicious protocols, packets and content as appropriate.

- Management System

Authentication of legitimate Wi-Fi APs located in user areas should be enabled. User authentication, in particular wireless devices, should be implemented. Host-level firewall and malware protection should be installed. Intrusion prevention systems should also be installed on the Wi-Fi and wired networks to detect any suspicious activities.

- Configuration of APs

An access point is the core component of a Wi-Fi network. A baseline security configuration standard for APs is required to protect them with appropriate measures. Recommended controls include, but not limited to the following:

  - Change the default configuration settings of APs. For example, changing the default administrative account and password, disabling unnecessary or insecure services, protocols and unused management interface on the APs.
  - Ensure that all APs have strong, unique administration passwords and change the passwords regularly.
  - Change the default SSID name to a proper and inconspicuous one (e.g. WiFi.HK). The SSID name should prevent the disclosure of system details of the networks, such as product name/model.
  - Do not broadcast SSID if the stand-alone Wi-Fi network will be used by authorised pre-configured devices only. If broadcasting SSID is required, it should only be discovered within the designated coverage.
  - Authenticate legitimate APs in user areas.

- Client devices

  Individual clients should be isolated to prevent peer-to-peer communication in order to protect from malware attacks. Client-side digital certificates for mobile devices with limited Wi-Fi defences should be used so that only authorised devices are allowed to access departmental network or resources.

5.2 Security Consideration for the operation of a Wi-Fi Network

The following security measures for the operation of a Wi-Fi network should be in place in different components of the network by different parties, such as network administrators and end users.

Network Administrator

The Network administrator should implement the following technical security measures in client devices, management system and connection.

Client devices

The network administrator should put in place protection of departmental network against malware infection from the client devices, and restricting usage for authorised client devices only. Change encryption keys of APs regularly.

Management System

User activities and event monitoring should be logged to detect any malicious activities for further investigation. It should fix vulnerability that exists in network devices that may be exploited by intruders; regularly scan the Wi-Fi signal to detect whether rogue APs are installed within the coverage map of the Wi-Fi network; and detect suspicious network traffic and malicious attacks.

Client devices and connection

For client connections, end users should encrypt the data transmitted over the air to protect the confidentiality of the information. Client devices should avoid connecting to untrusted / unknown APs, and shall not share or extend Government internal network using hotspots and/or ad-hoc mode.

End Users

The followings are the best practices for end users when accessing the Wi-Fi service -

Setting

- set the default Internet connection as manual mode, instead of automatic.
- turn off peer-to-peer / ad hoc mode networking.

- enable power-on login for the client devices so that password would always be requested when accessing the device.
- install and enable personal firewall, anti-virus and anti-spyware software.

Usage

- do not leave the client devices unattended.
- turn off wireless connection when it is not in use.
- verify the certificates of captive portals to ensure that it is not a fake portal.
- do not connect to strange Wi-Fi network.
- disconnect from Wi-Fi network when there are suspicious activities.

Maintenance

- apply security patches of the applications and drivers of the client devices when they are available.
- back up data regularly.
- remove all data and sensitive configuration information, such as SSIDs or encryption keys, on the client devices before disposal.

5.3 Remote Access over Wi-Fi network

Transmission of data via Wi-Fi without protection is vulnerable to attacks. Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and transmitted among wireless devices may be intercepted and disclosed. Hence, security measures shall be adopted when transmitting sensitive information.

For access to sensitive information via wireless communications, consideration should be made to treat all wireless access as un-trusted connections. Thus, access to internal systems via wireless communications should be granted only through a designated gateway (e.g. VPN gateway) with proper authentication, encryption, user level network access control and logging implemented.

Sufficient authentication and encryption measures shall be in place for remotely accessing the internal network via Wi-Fi. B/Ds shall adopt the secured channels (e.g. Virtual Private Network (VPN), VPN over HTTPS) when connecting to government internal network with two-factor authentication. The following are some of the recommended measures:

- Update the malware protection software with latest definition in the endpoint with Wi-Fi connection (e.g. mobile device).
- Install the latest security patches.
- Enable the host-level firewall or intrusion prevention systems.
- Enable the storage encryption in the endpoint device.
- Register the endpoint device to the list of VPN client access.
- Use strong password for the VPN account.
- Enable two-factor authentication (2FA) with a token or one-time password code.

- Enable the idle timeout (e.g. 10 minutes) for disconnecting VPN connection.
- Enable the logging function for all VPN connections with Wi-Fi connection.
- Register the MAC address of the endpoint if MAC address filtering is enabled.

6. Emerging Technology

6.1 Introduction to 5G

5G stands for the fifth generation of mobile telecommunications which is formulated by International Telecommunications Union (ITU) for the development of new generations of mobile technologies. 5G enables new capabilities of mobile technologies that go beyond those of 4G. The peak data rate of 5G mobile technology can ideally reach 20 Gbps maximum while the user experienced data rates may vary depending on the environments where the mobile devices are located. As 5G networks are built on top of existing telecommunications networks, it is expected that the network infrastructures of 5G will continue to be used for providing 3G/4G services in the foreseeable future.

New capacity and characteristics of 5G

Enabler of IoT applications

The download and upload speeds are significantly increased in 5G network. The latency[1] of 5G network is also reduced. 5G would also enable massive machine-type communication which allow more devices, in particular Internet of Things (IoT) devices, to connect to the network within a small area.

Software-Based and Virtualisation Technologies

5G is designed and implemented with new software and virtualisation technologies on network management capabilities through Network Function Virtualisation (NFV), Software Defined Networking (SDN)[2], and Network Slicing[3]. These technologies enable 5G to support the coexistence as well as isolation of applications requiring different kinds of 5G network services while sharing the same infrastructure. For example, mobile broadband service requires higher speed of data transfer while smart car application requires swift response (low latency) between data communication with its sensors.

6.2 Threats and Vulnerabilities of 5G Mobile Network Service

5G mobile network service and its underlying infrastructure are provided by mobile network operators as a public communication network. Like other communication networks such as 4G, Wi-Fi, or telephone lines, 5G network is considered as an un-trusted communication network. The transmission of information over any public communication networks could be exposed to security risks because malicious attackers may capture classified information and even break into the government network by exploiting vulnerabilities of the

[1] Latency refers to the time lapse between when the cell tower sends data and when the destination device (e.g. mobile phone) receives it.

[2] SDN and NFV are deployed to deliver greater network flexibility by allowing traditional network architectures to be partitioned logically through software.

[3] Network slicing allows the network operator to provide dedicated virtual networks to the customers over a common network infrastructure. The user experience of the network slice will be the same as if it was a physically separate network.

communication networks. The threats of a public communication network are applied to 5G. In addition, some threats specific to 5G are also elaborated below.

Vulnerability of New 5G Applications and Network Technologies

As 5G network provides much wider bandwidth and high speed, it boosts the proliferated growth of innovative applications that take advantages of the technology advancements. Coming along with the new applications, some security risks are also brought upon. Moreover, 5G architecture involves various function layers and it is implemented with software-based and virtualisation technology. However, the use of these new software technologies implies vulnerable points in network operations. These new security vulnerabilities of the 5G infrastructure software may have impacts to B/Ds if not properly connected and protected.

Increased Threats Surface of 5G Devices

5G network has the capacity to support greater number of network connection and thus allow massive types of devices, in particular IoT devices, to be interconnected simultaneously. These connected devices that may have poorer security standards and capabilities due to short launch time to market and cost considerations can lead to an increased threat surface. For example, malicious attackers can intrude one of the connected devices and take control the device if there is vulnerability in the device. Furthermore, the attackers can compromise other devices in the network and perform attacks to the whole network.

Mis-configuration of Devices with 5G connectivity

Due to growing adoption of 5G in mobile devices or IoT devices, these devices may have built-in 5G connectivity. As the 5G / IoT technology can enable dynamic connection in a convenient way, users should be aware that their devices are more susceptible to various potential risks. For example, a user may connect a private IoT device to government network and unintentionally disclose sensitive data to outsiders. Moreover, attackers could take advantage of 5G features to introduce other attacks such as malware spreading, DDoS (distributed denial-of-service) attack, phishing and spam attacks.

Mobile devices, such as mobile phones, tablets and laptops, usually connect to Internet via telecommunications networks, including 5G. If security risks are not properly managed and the protection is not sufficient and effectively implemented, there would be a higher chance that data, mobile devices and related communication networks would be vulnerable to unauthorised access, modification, lost or stolen, or compromised, or even the mobile devices would become a part of botnets to launch attack.

Risk factor of 5G base stations

The density of 5G base stations operating at high frequencies would be higher when compared with that of current cellular network. Hence, mobile network operators may request for the installation of 5G base stations and antenna units in government premises in order to provide better 5G network services. As a result, it may impose security risks to the Government when the non-government owned equipment is not managed properly in the government premises while the staff or contractors of mobile operators are not managed by the Government directly.

6.3 Security Considerations for using 5G Mobile Network Services

The public 5G network deployment should have no major difference than other legacy networks, such as 4G, 3G and fixed line, which assume that all public or mobile networks are un-trusted and any government communication through public or mobile networks should be protected by additional layers of security such as encryption, authentication, access control, etc., according to data classification. Moreover, when adopting new technology, all relevant stakeholders shall pay attention to the information security threats the new technology may bring, and take effective measures in a timely manner, including adopting the latest standards or installing patches.

New 5G Applications and Network Technology

5G Network

For security consideration of connecting a public network to a departmental network, the Practice Guide for Internet Gateway Security should be referenced. For example, B/Ds should request system integrators or mobile operators to provide security controls, including but not limited to installation of security gateway or demilitarized zone (DMZ) for accessing internal network; use of encryption whenever transmission of data and network monitoring on systems and activities to prevent any malicious attack such as DDoS and man-in-the-middle attack. B/Ds should also enable security monitoring and management solutions to allow better visibility to the network and any attacks.

Regarding the 5G network virtualization technology, the deployment of application relying on new 5G network technology implies vulnerable points in network operations. Although many security responsibilities of these new technologies are borne by mobile network operators or virtualisation platform owners, B/Ds should beware of the vulnerabilities rising from these vulnerable points and request system integrators or service providers to provide security controls when 5G applications are involved. B/Ds should be well aware of the emerging security threats and associated risks of such 5G connections by subscribing to the security news, alerts, reports and other information security publications so that they can receive alerts at the earliest possible time and implement appropriate measures against such threats.

The following highlights some considerations for 5G network deployment and management:

- Disable those unnecessary 5G functionality in those network equipment with built-in features if there is no intentional connection
- Develop an operational plan on adopting 5G services in their business and operation, including but not limited to the assessment of maturity of the 5G application and network technologies, considerations of asset management, access control, physical security, operation security, communication security, cryptographic controls, log of activities with external network as well as the considerations in outsourcing, application development, business continuity, incident management and compliances, and obtain approval from Heads of B/Ds.
- Segregate those network segment connected to 5G services from other segments, which will reduce the attack surface if one of the hosts on the network segment is compromised through 5G connection.
- Sensitive and internal subnetworks can be separated from the general network to enhance the security management against risks under the dynamic network connections.
- Consider employing an independent auditor with expertise in 5G networks to review and examine the configurations and implementation of the network connected to 5G network.

5G Applications

5G enables the development of innovative applications, in particular, IoT and mobile applications. The adoption of security by design allows identification of potential risks for the application system and appropriate remediation at early stage of the project. B/Ds are recommended to make reference to the Section 5 "Mobile App Development Security" of the Practice Guide for Mobile Security that provides guidance notes in the development of mobile apps for business use as well as Practice Guide for IoT Security that highlights common security considerations and industry best practices in the adoption of IoT in various related security domains. For deploying applications with 5G connection, the general application security as stated in the government security documents should be followed with the following highlights for B/Ds' considerations:

- Keep in view the security development of the technology and conduct research to evaluate the security mechanism and features so as to choose applications that meet the security requirements.
- Only adopt necessary and secure functions; disable unwanted features, particularly for IoT devices.
- Avoid collection and storage sensitive information more than required.
- Ensure proper encryption is implemented for data in different endpoints and during transmission to protect sensitive information.
- Enable authentication and authorisation to assure that the service is accessed by authentic parties, and service is offered by an authentic source.

5G Devices

In fact, general security practices, measures and controls applicable to mobile devices are suitable and effectively to be in place to protect 5G devices. B/Ds are recommended to refer to the Section 4 Mobile Device Security of the Practice Guide for Mobile Security that guidance notes in securing the use and adoption of mobile devices in their business. Examples of these measures are unique identification of platforms and devices, counter-checking mechanism to guard against any mis-configuration of devices, device access controls, and storage and transmission encryption as well as validity of encryption keys and its renewal prior to their expiry. End users, application developers or administrators are responsible for protecting their mobile devices, data assets and related IT infrastructure respectively.

Regular trainings should be provided to increase end users' awareness on the proper use of 5G devices, in similar way as mobile devices or IoT devices. The following are some suggested contents in the trainings in order to raise their awareness:

- As the 5G / IoT technology promotes dynamic connection, users should be aware that their devices are more susceptible to various potential risks (e.g. connecting a private IoT device to a network containing sensitive Government data).
- Users should be aware that the use of vulnerable devices and devices with poor security settings would generate greater risk of cyber attacks.
- Users should deploy those devices with technical support, such as provision of security patches, so as to keep the device safe.
- Users should carefully examine the network settings of the devices or equipment and only allow connection to 5G network or devices as necessary.
- User should not connect their 5G devices directly to the departmental network without approval.

5G Base Stations

As 5G works in spectrum with higher frequency than 4G, the lower penetration capability of high frequency requires the setup of 5G stations and antenna units to be denser and closer in order to provide services with acceptable performance. If there is a need to install the base station in government premises, the following security measures should be considered:

- Ownership, and roles and responsibilities of the Government and mobile network operators should be clearly defined before installation. Proper security procedures should also be in place to manage projects and services for handling these equipment by mobile operators.
- Proper physical access controls should be in place for network equipment enabled with 5G and staff should be assigned in monitoring the physical access.
- Proper physical security procedures should be in place for controlling and logging physical access for installation, on-going maintenance, configuration changes, and inspection of all the 5G network components by staff, for examples external consultants, contractors and temporary staff.

- Clarify with the operator that the installation of the updates/patches of the 5G base stations have been approved and verified by operator' senior technical staff (such as chartered engineer).
- As the 5G base stations or related equipment are not common networking equipment available in ICT infrastructure, consult telecommunication engineers for their security advice in their expert domain before installation, if there is uncertainty.

Incident Handling

The security incident handling procedures should be reviewed with necessary modification to handle the scenarios of any suspected activities such as compromise of 5G networks due to vulnerability and base stations being compromised. Besides, the system logs and usage logs are crucial for investigation if there are any security incidents originated from both outsider attack and insider attack, the log should be under full control with adequate protection.

*** ENDS ***