GN-18/2016

Guidelines on the Security Aspects for the Design, Implementation, Management and Operation of Public Wi-Fi Service

Office of the Communications Authority

Issue 3
29 December 2016

CONTENTS

FOREWORD

In Hong Kong, the provision of public Wi-Fi service which does not cross public streets or unleased government lands is permissible under a class licence[1] created by the Communications Authority ("CA") under sections 7(5) and 7B (2) of the Telecommunications Ordinance (the "Class Licence"). For the provision of public Wi-Fi service across public streets and unleased government land, the operator should be a holder of a unified carrier licence ("UCL") granted by the CA with the appropriate provisions[2] incorporated.

2. Public Wi-Fi service operates in the licence-exempted frequency bands[3] and shares the same frequency bands with other eligible radio apparatus in an uncoordinated and unprotected manner. Security of the public Wi-Fi service therefore depends very much on the network configuration and operation provided by the respective operators. A Wi-Fi access point ("AP") without proper security measures in place would pose security risks to users where their communications through the AP may be intercepted by an unauthorised third party.

3. This document gives practical guidelines (the "Guidelines") on the security aspects for the design, implementation, management and operation of public Wi-Fi service with particular emphasis on the air interface. The Guidelines should be observed by public Wi-Fi service operators (the "Operators"), who may either be Unified Carrier Licensees with the appropriate provisions incorporated in their licences, or Licensees of the Class Licence (including those operators logically partitioning their APs for resale of service to other telecommunications operators).

4. To promote user awareness on the security of using the public Wi-Fi service, Operators should provide updated information to their subscribers from time to time about the security features of their service platforms.

---

[1] Class Licence for the Provision of Public Wireless Local Area Network Service.

[2] The carrier licensee should be authorised to provide public wireless local area network services (such as public Wi-Fi service) under the UCL.

[3] Please refers to the Telecommunications (Telecommunications Apparatus) (Exemption from Licensing) Amendment Order 2005 (http://tel_archives.ofca.gov.hk/en/ta-regulations/es22005090922.pdf).

5. In addition to the security measures, the Operators should follow the triggering criteria and reporting procedures set out in the Guidelines for reporting security violations.

6. For any further information and enquiry regarding this document or the related issues, please contact -

Office of the Communications Authority
29/F., Wu Chung House,
213 Queen's Road East,
Wanchai, Hong Kong
(Attn.: Senior Regulatory Affairs Manager (Regulatory 11))

Telephone no.: 2961 6628
Fax no.: 2803 5112
Email: wifi_security@ofca.gov.hk

SECTION 1: GENERAL PRINCIPLES

1.1 Operators should provide adequate security measures in their networks to protect user data communications using the public Wi-Fi service.

1.2 Operators should take into account the following three security objectives namely, Confidentiality, Integrity and Availability ("CIA"), when they design and operate their networks and services -

- **Confidentiality** refers to the protection of user data against unauthorised access, viewing, diverted or intercepted as it flows via the public Wi-Fi APs;

- **Integrity** refers to the protection of user data against unauthorised modification, deletion, creation and replication; and

- **Availability** refers to the service provisioning to minimise downtime due to security attacks by hackers, if any.

1.3 As user awareness is crucial for any security measures to be effective, Operators should promote user awareness and provide on-going education to their customers for secure use of the public Wi-Fi service. This would include for example advice to the customers on the user best practice.

SECTION 2: CONSIDERATIONS

2.1 From the technical perspective, Operators should bear in mind the CIA objectives to tackle potential security threats inherited in their networks. According to the International Telecommunication Union ("ITU"), security threats associated with public Wi-Fi networks can be classified into five categories -

(i) denial of service ("DOS");

(ii) eavesdropping;

(iii) loss/corruption of information;

(iv) masquerade; and

(v) unauthorised access.

A summary of threats is given in **Appendix 1**.

2.2 In addition to the security considerations, Operators should also take into account the following issues in designing proper security measures for their networks -

(a) apart from the popular notebook computers, which are equipped with adequate security tools to protect user access to the APs, there are other less sophisticated devices (such as personal digital assistants, smartphones and legacy devices) that, even if equipped with a Wi-Fi interface, may not support advanced security features; and

(b) any security measures to be introduced should not deter user from accessing the public Wi-Fi service. Operators should strike a reasonable balance between security and user convenience.

SECTION 3: SECURITY MEASURES

3.1 The security measures set out in the Guidelines can be classified into management, operational and technical measures. Operators should comply with the basic technical measures as well as the management and operational measures. Operators are also encouraged to implement the advanced technical measures as far as possible.

Management Measures

3.2 Each of the Operators should take into account the following measures in the overall management of its network -

(a) implement security policies and measures for the network and review such security aspects regularly in order to cope with the latest technological and business developments;

(b) implement business continuity plan if the network supports the Operator's critical business activities[4];

(c) perform security risk assessments regularly to fully explore the risk areas and maintain a good security posture of the network;

(d) perform independent security audit to verify the compliance of the security posture of the network with the security policy. Staff in the same organisation but not involving in the Wi-Fi operation can also act as the independent auditor; and

(e) develop a set of in-house procedures on incident response and remedy as well as update such procedures with regard to new potential security threats.

Operational Measures

3.3 Both the Operators and the Office of the Communications Authority

[4] Please refer to the Government Infosec website at http://www.infosec.gov.hk/english/business/planning.html.

("OFCA") should play their respective roles in advising the users and the public on security violations or outages. The Operators, having first-hand information about the operational status of their networks and services, should be responsible for providing prompt information and advice to their customers on security violations or outages. Where the incident falls within the reporting criteria, the Operator concerned should, in addition to providing information and advice to its customers, report to OFCA within the specified timeframe. OFCA, upon receiving such information, should promptly inform the public and provide guidance where necessary if it is assessed to have significant and territory-wide implications.

3.4 Some Operators may wish to offer free services for causal users that might not require user login or implementation of any security measures. Under such arrangement, if an Operator cannot comply with the Basic Security Measures as detailed in paragraph 3.6 below, the Operator concerned should explicitly alert the users concerned to the lack of a certain security protection and the potential risks that they might be exposed to when accessing the service.

3.5 Each of the Operators should also take into account the following measures in the daily operation of its networks -

(a) ensure that strong security measures are in place for any remote administration of the APs;

(b) ensure that all factory default parameters of APs, including Service Set Identifier ("SSID"), administration passwords, encryption key, Internet Protocol ("IP") address range to be allocated to Wi-Fi clients are properly configured;

(c) maintain the firmware of the APs and the network components up-to-date as far as possible;

(d) implement appropriate patch management mechanisms for the proper update of security patches and software applications;

(e) keep records of configuration change logs;

(f) implement access controls and carry out regular system/application/data backup;

(g) keep proper inventory records (including firmware and patch version

information) of the APs and the associated network components;

(h) implement physical security controls to safeguard any modifications to the hardware, software and network facilities by any unauthorised parties;

(i) use non-suggestive SSID naming convention to prevent the disclosure of system details of the networks;

(j) develop procedures for immediate disabling of any connections of confirmed improper usage;

(k) publish coverage information of the public Wi-Fi service including locations of the respective APs and the associated SSIDs; and

(l) inform users of the proper use of the public Wi-Fi service and their responsibilities.

Basic Technical Measures

3.6 Each of the Operators should implement the following technical measures in its network -

(a) install the server certificate signed by a trusted Certification Authority to confirm the authenticity of the APs concerned, and display it to the end users wherever possible;

(b) employ strong encryption (such as Secure Sockets Layer ("SSL") or Transport Layer Security ("TLS")) when users are asked to input their own accounts and passwords in order to ensure the confidentiality of user data;

(c) keep record of the login identity (such as login ID and pre-paid card numbers), the Media Access Control ("MAC") address of the device and the allocated IP address for a particular user as well as other relevant information for a minimum period of 6 months in order to facilitate future investigation work, if any;

(d) prohibit peer-to-peer attack through the same AP;

(e) allow users to deploy their own virtual private network ("VPN")

connections; and

(f) separate Wi-Fi network from other public service provisions with firewall or other means.

Advanced Technical Measures

3.7 In addition to the basic technical measures, each of the Operators is encouraged to develop and implement the following technical measures in its networks -

(a) implement secure authentication methodology (such as IEEE 802.1x) to ensure that only the authorised users can access the service;

(b) direct log record entries to a remote audit server in order to protect the integrity of logging data;

(c) implement secure air interfaces where user data is encrypted for communication between the APs and client devices. For instance, Wi-Fi Protected Access ("WPA") or Wi-Fi Protected Access 2 ("WPA2") can be used to protect users' data transmission over its network. The Operator should change the encryption keys as often as necessary[5];

(d) implement firewall in its network to protect end-users from malicious attacks through the APs;

(e) deploy anti-virus and anti-spyware systems with up-to-date definitions to help stop any wide spreading of virus, worms, and malicious code through the networks;

(f) deploy intrusion detection system ("IDS") and/or intrusion prevention system ("IPS") to detect the inbound and outbound network traffic as well as detect and log any suspicious activities and network attacks, in particular to block those attacks originated from the associated devices within the Operator's Wi-Fi networks;

[5] As Wired Equivalent Privacy ("WEP") requires all users in the same network to share the same encryption key, it is not considered as a secured encryption method.

(g) deploy wireless IPS ("WIPS") to detect wireless attacks and provide real-time alert with a view to preventing users from mis-associating with a rogue AP;

(h) segment the service coverage areas to balance traffic loading of the wireless network so as to minimize any adverse impact that might be caused by malicious attacks;

(i) configure the APs to enable layer 2 isolation; and

(j) implement measures to tackle the problem of exhaustion of all available IP addresses assigned for the Operator's public Wi-Fi service.

User Best Practices

3.8 Operators should inform and advise their customers from time to time of the risks associated with the public Wi-Fi service. They should provide recommendations to their customers for accessing their networks and inform their customers of the availability of the security measures implemented. A set of recommended "User Best Practices" is given in **Appendix 2**. Operators are also encouraged to make reference to "Tips on Wireless Security for End-users" at the Government's one-stop information security portal (www.infosec.gov.hk).

SECTION 4: INCIDENT REPORTING

4.1 The Operators should report to OFCA whenever a security violation occurs that meets the triggering criteria mentioned in paragraph 4.2 below. Notwithstanding the above, the Operators are encouraged to share information with the Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT") on the daily operation of the Wi-Fi network as detailed in paragraph 4.7. If the situation warrants, OFCA might consider issuing warning alerts to the public and liaising with the Internet Infrastructure Liaison Group ("IILG")[6] for better coordination amongst the relevant stakeholders regarding the incident.

Incidents of Severe Security Violation

4.2 If there is an outbreak of security violation which meets either of the criteria specified in the table below, the Operator concerned should report the case to OFCA in accordance with the following reporting timeframe -

(a) Triggering Criteria

- More than 200 APs of the Operator concerned are exposed to a particular malicious attack, such as DOS, hacking, etc. for more than 2 hours.
- An AP experiences sustained malicious attacks for more than 24 hours.

[6] The IILG was established in 2005 aiming to facilitate the Internet infrastructure stakeholders to formulate coordinated response in case of major incidents that will affect the smooth operation of the Internet infrastructure of Hong Kong. Its members include government departments (i.e. Office of the Government Chief Information Officer ("OGCIO"), Hong Kong Police Force and OFCA) and the major local Internet stakeholders. IILG serves as a liaison channel for sharing intelligence, experience and best practices with a view to ensuring the stability, security, availability and resilience of the local Internet infrastructure.

(b) Reporting Time Frame

Occurrence Time	**Initial Report**	**Restoration of Service**
Time Zone 1 (Between 08:30 and 21:00)	The Operator concerned should report the security incident to OFCA within one hour after the triggering criteria for reporting the incident is met	The Operator concerned should report to OFCA within two hours after rectification of the security loophole.
Time Zone 2 (Between 21:00 and 08:30 of next day)	The Operator concerned should report the security incident to OFCA within one hour or by 08:30, whichever is later.	The Operator concerned should report to OFCA within two hours or by 08:30, whichever is later.

(c) OFCA's Contacts for Reporting Severe Security Breach

	Telephone No.	**Email Address**
First Contact	6392 9536	outage@ofca.gov.hk
Second Contact	6392 9157	outage@ofca.gov.hk

4.3 When reporting an outage to OFCA, the Operator concerned should provide OFCA with the following information, whenever possible -

(a) name of operator;
(b) description of incident;
(c) date and time of onset of the incident;
(d) types and estimated number of customers/end-users affected;
(e) affected areas;
(f) action taken; and
(g) contact information: name of contact person as well as the person's fixed and mobile telephone numbers and email address.

4.4 OFCA will assess the significance of impact on the territory and

determine whether public alert is warranted. Prior to the complete restoration, the Operator concerned should regularly update the responsible parties on the status of the affected network/service.

Submission of Incident Report

4.5 The Operator concerned should submit a preliminary report to OFCA within three working days of the incident on severe security violation. The preliminary report should give a detailed account of the incident, the security violation in question, the impact caused by the incident and the remedial action taken.

4.6 Where requested by OFCA, a full report should be submitted to OFCA within 14 working days of the incident or other deadline as specified by OFCA. The full report should give a detailed account of the measures which have been taken (or will be taken) in order to prevent recurrence of similar incidents.

Internet Service Outage

4.7 OFCA has implemented a mechanism for reporting Internet outage or service degradation since early 2007[7]. Where such outage or service degradation falls within the pre-defined reporting criteria, the relevant Internet Service Providers and Operators should, in addition to alerting its customers, report the incident to OFCA within the specified timeframes. The said outage reporting mechanism should be applicable to any severe security violation causing outage and/or service degradation in the public Wi-Fi network that provides access to the Internet services.

[7] Please refer to the "Guidelines for Cable-based External Fixed Telecommunications Network Services Operators and Internet Service Providers for Reporting Network and Service Outages" (http://www.coms-auth.hk/filemanager/statement/en/upload/286/gn_201403e.pdf).

Other Security Issues

4.8 Since 2001, HKCERT has provided service to the community to help resolve technical issues including virus control and other security issues. HKCERT publishes alerts through their service portal at http://www.hkcert.org. Operators are encouraged to share information with HKCERT in respect of the other security issues that have occurred in their networks. If the incident is suspected to involve criminal offences, the affected party should report the incident to the Hong Kong Police Force and the Customs and Excise Department, as appropriate.

SECTION 5: REFERENCES

5.1 The following is a list of useful resources on network security, including the public Wi-Fi networks -

- IT Security Guidelines published by OGCIO
- Security Risk Assessment & Audit Guidelines published by OGCIO
- Wireless Network Security for IT Professional from the government one-stop information security website 'InfoSec'
- Guideline for Safety Using Wireless LAN published by HKCERT
- Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, November 2002 (800-48) published by NIST
- Wireless Security in TISN's Information for CIOs
- Overview of Security for the Management Plane of ITU-T Recommendation M.3016.0
- Security Architecture for Systems Providing End-to-End Communications of ITU-T Recommendation X.805

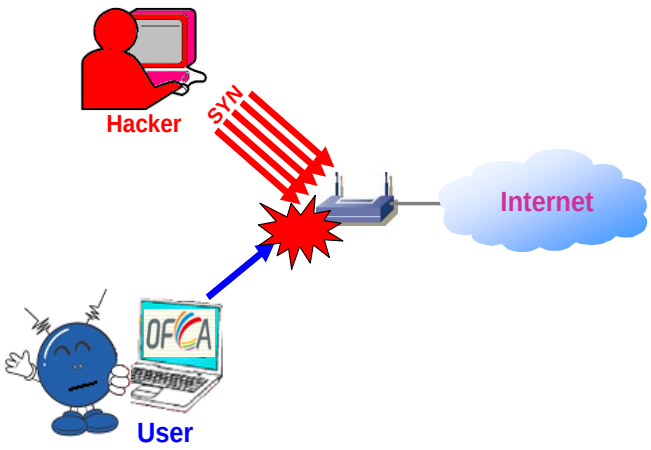
Appendix 1

Security Threats against Public Wi-Fi Service

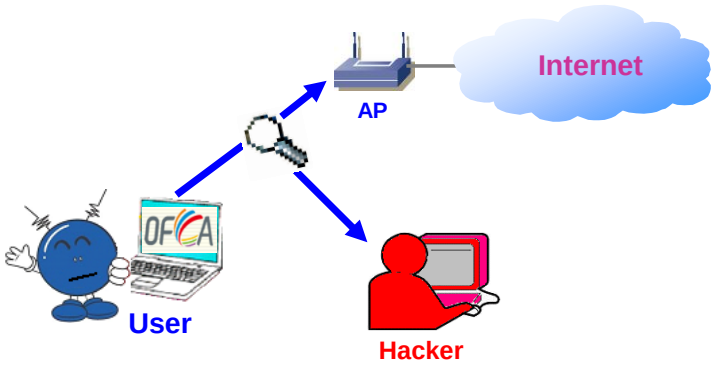
The table below summarises the threats to Wi-Fi security.

Threat	Confidentiality	Integrity	Availability
Denial of service			X
Eavesdropping	X		
Loss/corruption of information	X	X	X
Masquerade	X	X	X
Unauthorised access	X	X	X

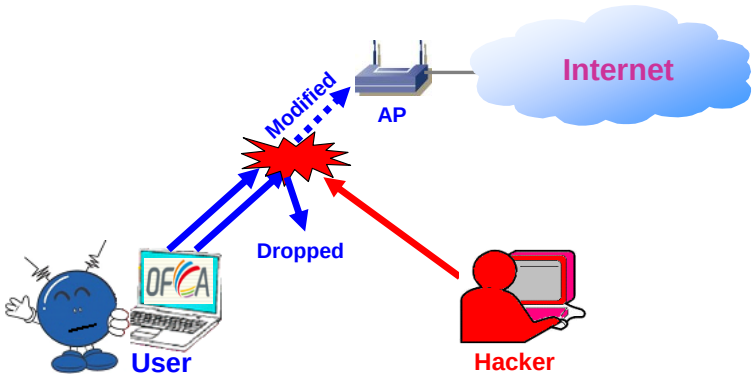
- **Denial of service ("DOS"):** an attack with a view to depriving the service availability of an entity.



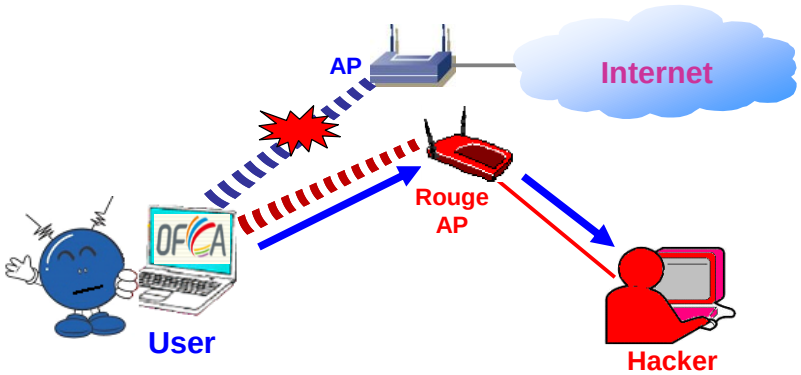
- **Eavesdropping**: unauthorised monitoring of third party's communication, e.g. man-in-the-middle attack.



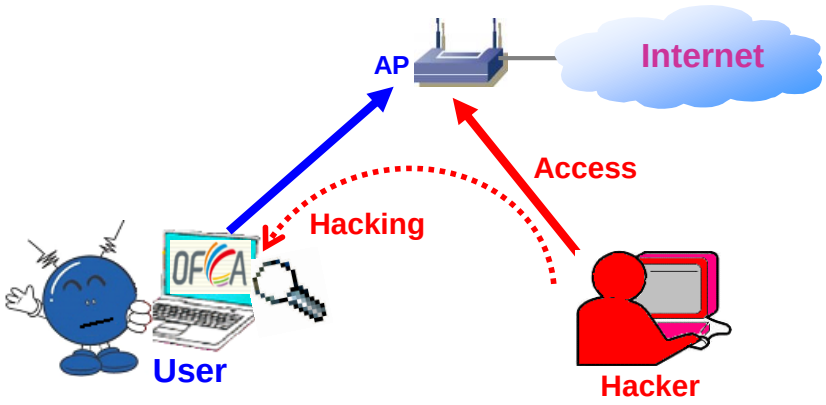
- **Loss or corruption of information**: compromise the integrity during data transfer, such as unauthorised deletion, insertion, modification, re-ordering, replay or delay, e.g. man-in-the-middle attack, peer-to-peer attack.



- **Masquerade ("spoofing")**: pretence of authorised status by an impostor, e.g. rogue AP.



- **Unauthorised access**: an attempt to access data in violation of the security policy in force, e.g. peer-to-peer attack, unauthorised access of Wi-Fi service.



Appendix 2

User Best Practices for Accessing Public Wi-Fi Service

Users are encouraged to follow the best practices below when accessing the public Wi-Fi service -

- set Internet connection default to "manual" mode instead of "automatic" mode;
- do not leave the wireless device unattended and turn off wireless connection when it is not in use, activate only appropriate mode of data connection when needed;
- do not enable both wireless and wired network interface card at the same time;
- do not connect to uncertain / strange network and disconnect from accessing network when suspicious activities observed;
- do not send sensitive / personal information when using public Wi-Fi service;
- employ Virtual Private Network ("VPN") technologies for enhanced end-to-end transmission protection;
- turn off peer-to-peer / ad hoc mode networking, disable resource sharing, shut down split tunnels on VPNs, and configure the personal firewall to prevent exposure of client ports;
- remove your preferred network list when using public Wi-Fi service;
- remove all sensitive configuration information, such as SSIDs or encryption keys, on the discarded devices when disposing wireless components;
- keep security patches and wireless network interface card drivers installed on the wireless device up-to-date as well as back up data regularly;
- install and enable personal firewall, anti-virus and anti-spyware software and keep the associated definition files and security patches up-to-date;
- enable the wireless device's power-on login, system login authentication, and password-protected screen saver;
- check the authenticity of captive portal by verifying the certificate of the website when accessing a public Wi-Fi service;

- encrypt those sensitive data stored on the device accessing public Wi-Fi service; and
- if the wireless device supports wireless encryption, use the encrypted connection if it is available from the relevant Operator.

- End -