

**Security Guidelines for
Next Generation Networks**

Office of the Telecommunications Authority

1 April 2010

FOREWORD

In Hong Kong, public telecommunications operators (hereafter referred to as “operators”) have established next generation networks (NGNs) or are in the process of replacing their traditional service platform with NGNs for the provision of public telecommunications services. NGN usually refers to a platform that has the capability to carry voice, data and video information by using one single service platform based on the Internet Protocol (IP)¹. It enables operators to have greater flexibility of introducing innovative services and benefits customers with new user experience that has not been possible over traditional service platforms.

2. While enjoying the benefits, operators and customers may face the security issues brought about by NGNs. As the architecture of NGN is moving from a closed platform to an open platform that run everything over IP technologies, it would increase the chance of intrusion. Therefore, a NGN without proper security measures in place would be highly vulnerable to malicious attacks and pose security threats to its users.

3. This document gives practical guidance on the provision of security measures for proper operation of NGNs and protection of the users’ proper use of the telecommunications services. It should be observed by all the operators which operate NGNs (facility based operators) or provide services with the use of NGN provided by others (service based operators).

4. To promote user awareness on the security of using the public telecommunications services, operators should from time to time provide updated information to their subscribers about the security capability of their NGNs.

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

¹ For the purpose of this document, the NGN definition introduced by the Telecommunication Standardization Sector of International Telecommunication Union (ITU-T) is adopted.

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

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

Telephone no.: 2961 6628
Fax no.: 2591 0316
E-mail: net_security@ofta.gov.hk

SECTION 1: GENERAL PRINCIPLES

1.1 The operators should take into account the following security objectives, namely confidentiality, integrity, and availability, when building their network and providing their services.

- **Confidentiality** refers to the protection of network and user data against unauthorized access, viewing, diverted or intercepted;
- **Integrity** refers to the protection of network and user data against unauthorized modification, deletion, creation and replication;
- **Availability** refers to the network and service provisioning to minimize downtime due to security attacks by hackers, if any.

1.2 These objectives provide a foundation upon which a more consistent and structured approach to the design, development, and implementation of network security capabilities can be constructed. The security measures for fulfilling these objectives should not just solely focus on the technical controls. Consideration on non-technical issues, such as policy and operational procedures should also be taken.

1.3 While providing adequate levels of protection, the security measures should allow certain flexibility in order to accommodate the rapid change of the telecommunications environment.

SECTION 2: SECURITY FRAMEWORK

2.1 A comprehensive protection of the NGN shall comprise measures from different perspectives which can effectively counter all possible threats and attacks that may happen in the network.

2.2 A threat is a potential violation of security. Threats may be accidental or intentional and may be active or passive. An accidental threat is one with no premeditated intent such as a system or software malfunction or a physical failure. An intentional threat is one that is realized by someone committing a deliberate act. When an intentional threat is realized, it is called an attack. Threats associated with NGNs may be classified into (i) destruction, (ii) corruption, (iii) removal, (iv) disclosure, and (v) interruption. The illustration of these security threats is given in Annex 1.

2.3 To safeguard NGNs from malicious attacks, a set of security measures should be in place. These measures should address particular aspects of the network security from different dimensions which may include (i) access control, (ii) authentication, (iii) non-repudiation, (iv) data confidentiality, (v) communication security, (vi) data integrity, (vii) availability, and (viii) privacy. These dimensions represent the classes of actions which can be employed to combat the security threats and attacks. The details of these security dimensions are shown in Annex 2.

2.4 Apart from protecting the operator's network, user protection and awareness is also a critical element in network security. The operators concerned should provide sufficient measures to protect the users' proper use of their network services and to promote the users' awareness of potential threats. The ultimate goal is to enable users to adopt appropriate measures available to them in accessing to NGN services.

2.5 In order to ensure that a security incident can be tackled and managed in a control manner, an effective reporting mechanism is required that the government and the relevant parties can be well aware of the latest development and impact of the incident. This would enable

the government and relevant parties to take appropriate action/coordination to safeguard the overall interest of the community.

2.6 In addition to above security considerations, operators should be mindful that any security measures to be introduced should not deter users from accessing the telecommunications services. Any measures should strike a reasonable balance between security and user convenience.

SECTION 3: SECURITY MEASURES

3.1 The practical security measures can be classified into the following three categories, namely management measures, operational measures, and technical measures. The security measures listed below are not exhaustive. The operators should implement other relevant measures to fulfil the principles as set out in Section 1.

Management Measures

3.2 Operators should take into account the following measures when formulating the policies for the proper management of their networks and the provision of network services:

- (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) 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;
- (c) assign clear responsibility to the each personnel involved in relation to network security;
- (d) implement effective information dissemination mechanism to ensure that network security information, including the security policies, procedures, incident reporting, can be effectively delivered;
- (e) perform security risk assessments regularly to fully explore the security posture of their network;
- (f) perform independent security audit to verify the compliance of the security posture of the network with the security policy. Staff in the same organization but not involving in the network operation can also act as the independent auditor;
- (g) implement business continuity plan if the network supports the operator's critical business activities;

- (h) implement adequate security control on external consultants, contractors and temporary staff for their access to the network infrastructure; and
- (i) ensure proper security process in place to manage outsourcing projects/services.

Operational Measures

3.3 Operators should take into account the following measures in the daily operation of their networks:

- (a) ensure updated operational and procedural manuals are available for relevant staff to access and follow. When a security violation is detected, they should be handled in a controlled way in accordance with a pre-defined plan to minimize potential damage and to restore to the normal security level;
- (b) ensure that all factory default parameters of network equipment, including login name, administration passwords, IP address range to be allocated to network equipment are properly configured;
- (c) ensure that strong security measures are in place for any remote administration of the network equipment;
- (d) ensure public domain software and freeware are fully tested and verified before putting in operational use;
- (e) ensure proper counter-checking mechanism is in place to guard against any mis-configuration;
- (f) maintain the firmware of the network components up-to-date as far as possible;
- (g) implement an appropriate change control and patch management mechanism for the proper update of network configuration, security patches and software applications;
- (h) keep proper documentation on network architecture and inventory records (including firmware and patch version information) of the network components;

- (i) keep record of configuration change logs;
- (j) carry out regular system/application/data backup;
- (k) select proper location for housing the network equipment so that they are well protected against fire, water flood, etc.;
- (l) implement physical security controls to safeguard any unauthorized access and modifications to the hardware, software and network facilities by any unauthorised parties;
- (m) ensure sufficient and uninterruptible power supply and air conditioning/ventilation are available to the network facilities;
- (n) implement appropriate security measures to prevent the disclosure of system details of the network;
- (o) develop procedures for immediate disabling of any connections of confirmed improper usage;
- (p) prevent the security issues occurred in own network from propagation to other networks;
- (q) ensure that customer and secured network information is properly erased and unrecoverable before the disposal; and
- (r) ensure copyright law restrictions must be respected at all times. Only approved software and hardware with proper licences are allowed to be set-up and installed following the corresponding licensing agreements and procedures.

Technical Measures

3.4 Operators should implement the following technical measures to protect their networks:

- (a) design and build the network infrastructure and facilitates to prevent single point of failure, at the core network and, as far as possible, at the edge network connecting to the user's device through an appropriate combination of resilience, redundancy, restoration and repair;
- (b) separate the service networks from the operator's corporate

networks;

- (c) assign different login name and password for both operational and test systems to reduce the risk of accidental log-on and other errors;
- (d) make the best effort to avoid conducting development and testing activities in the production environment;
- (e) employ network management tools and procedures to ensure controls are consistently applied and services are optimized;
- (f) deploy anti-virus and anti-spyware systems to help stop any wide spreading of virus, worms, and malicious code through the networks. The definitions should be up-to-date as far as possible;
- (g) deploy intrusion detection system (IDS), intrusion prevention system (IPS) or alike 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 their networks;
- (h) implement monitoring system or alike to monitor relevant security activities and examine monitoring records on a regular basis;
- (i) execute regular system backup and store the backup data in the secured location;
- (j) implement secure authentication methodology to ensure that only the authorized staff can access to the network and the authorized users can access to the services they subscribe;
- (k) implement firewalls or alike to protect their networks and prevent the security issues occur in the network from affecting the users; and
- (l) disable unnecessary services embedded in the network facilities.

SECTION 4: USER PROTECTION

4.1 Operators should protect the users' proper use of the network services and implement the following measures to safeguard their interests:

- (a) ensure customers' information is collected and used in a proper way as well as in compliance with the Person Data (Privacy) Ordinance;
- (b) implement secure network connectivity to protect the wireline and wireless communications between end-devices and the service networks, including but not limited to, the prevention of eavesdropping and altering the communication contents;
- (c) employ secured connection like Secure Sockets Layer (SSL) when users are asked to input their own account and password in order to ensure the confidentiality of user data;
- (d) allow users to establish their own virtual private network (VPN) connections;
- (e) inform users about the proper use of the network services and their responsibilities;
- (f) inform and advise their customers from time to time about the risks associated with the network services that the customers subscribe;
- (g) provide prompt information and advice to their customers on security violations or outages that may affect their network services; and
- (h) provide recommendations to their customers for accessing their networks and inform their customers about the availability of the security measures implemented. A set of recommended "User Best Practice" is given in Annex 3. The operators are also encouraged to make reference to the Government's one-stop information security portal (www.infosec.gov.hk) to obtain the updated user best practices.

SECTION 5: INCIDENT REPORTING

5.1 Telecommunications is one of the essential facilities supporting the economy and people's activities in Hong Kong. The outbreak of security violation may result in the degradation or outage of the telecommunications services. It is the operators' responsibility to advise the government on the occurrence of any severe security incident and to provide accurate update of the latest development so that the government can carry out necessary coordination and arrangement to minimize the impact of the incident to the community.

5.2 If there is outbreak of security violations which meets any of the triggering criteria specified below, the operators concerned should report the case to the Office of the Telecommunications Authority (OFTA) in accordance with the following reporting timeframe.

Triggering Criteria

Event	Duration of the Incident
A security violation results in degradation of service or failure of network components that would affect 10,000 or more users	> 30 minutes
A network element experiences sustained malicious attacks	> 24 hours
A severe network incident from the overseas counterparts that may affect the network services in Hong Kong	Report immediately when the incident has been confirmed

Reporting Timeframe

Initial Report	Restoration of Service
The operator concerned should report the security incident to OFTA within 1 hour after a triggering criterion for reporting the incident is met	The operator concerned should report to OFTA within 2 hours after security violation has been resolved

5.3 OFTA will assess the significance of impact on the territory and determine whether public alert is warranted.

Information to be Provided by the Operator When Reporting an Outage

5.4 When reporting an outage to OFTA, the operator concerned should provide OFTA with the following information, whenever possible:

- (a) Name of the operator;
- (b) Description of the incident;
- (c) Date and time of onset of the incident;
- (d) Types and estimated number of customers/users affected;
- (e) Affected areas;
- (f) Actions taken; and
- (g) Contact information (name of contact person, the person's fixed and mobile telephone numbers, and email address).

Updates on Network and Service Status

5.5 During the recovery stage, the operator concerned should inform OFTA of the status of the affected network/service. Under critical circumstances, OFTA may specify the update frequency and the information to be provided by the operator concerned to facilitate the assessment on the impact of the outage and the progress of recovery of the affected service.

Submission of Incident Report

5.6 The operator concerned should submit a preliminary report to OFTA within 3 working days from the close 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.

5.7 Where requested by OFTA, a full report should be submitted to OFTA within 14 working days from the close of the incident or other

deadline as specified by OFTA. The full report should give a detailed account of the measures which have been taken (or will be taken) in order to prevent similar incidents from reoccurrence.

Contact Points

5.8 OFTA's contact points for reporting severe security violation are as follows:

	Tel. No.	Email
First Contact	2961 6221 (office hours) 9107 5918 (outside office hours)	outage@ofta.gov.hk
Second Contact	2961 6635 (office hours) 9613 0231 (outside office hours)	outage@ofta.gov.hk

5.9 Each operator is required to provide OFTA with the contact information of its focal point responsible for reporting severe security violation to OFTA, including the names, fixed and mobile telephone numbers and email addresses of the first and second contact persons. Whenever there is any update on the contact information, the operator should inform OFTA of the change at least 5 days before the effective date.

5.10 The main steps for reporting severe network security violation are depicted in the flowchart in Annex 4.

Internet Service Outage and Wi-Fi Security Violation

5.11 OFTA has published the guidelines for reporting Internet outage/service degradation and the guidelines for public Wi-Fi security in 2007². Where incidents fall within the pre-defined reporting criteria stipulated in those guidelines, the relevant Internet service providers and

² "Guidelines for Cable-based External Fixed Telecommunications Network Services Operators and Internet Service Providers for Reporting Network and Service Outages" can be downloaded at www.ofta.gov.hk/en/report-paper-guide/guidance-notes/gn_200702.pdf and "Guidelines on the Security Aspects for the Design, Implementation, Management and Operation of Public Wi-Fi Service" can be downloaded at www.ofta.gov.hk/en/report-paper-guide/guidance-notes/gn_200817.pdf.

operators should, in addition to alerting its customers, report the incidents to OFTA within the specified timeframes. The said incident reporting mechanisms should be applicable to any severe security violation causing outage and/or service degradation in the NGN that provides telecommunications services.

Other Security Issues

5.12 If the incident is suspected to involve criminal offences, the operator concerned should report the incident to the Hong Kong Police Force and the Customs and Excise Department, as appropriate.

SECTION 6: REFERENCES

- ITU-T: Recommendation X.800: Security Architecture for Open Systems Interconnection CCITT Applications (03/1991)
- ITU-T: Recommendation X.805: Security Architecture for Systems Providing End-to-end Communications (10/2003)
- ITU-T: Recommendation Y.2701: Security Requirements for NGN (04/2007)
- ITU-T: Recommendation E.408: Telecommunication networks security requirements (05/2004)
- ITU-T: Security In Telecommunications and Information Technology (06/2006)
- OGCIO: Baseline IT Security Policy (S17), Version 3.1 (November 2008)
- OGCIO: IT Security Guidelines (G3), Version 5.1 (November 2008)
- CERT: Home Network Security (27 February 2006)
- 3GPP: Security Principles and Objectives, 3G TS 33.120 Version 3.0.0 (March 1999)
- 3GPP: Security Threats and Requirements, 3G TS 21.133 Version 3.1.0 (December 1999)
- 3GPP: A Guide to 3rd Generation Security, 3G TR 33.900 Version 1.2.0 (January 2000)
- 3GPP: Security Architecture, 3G TS 33.102 Version 3.7.0 (December 2000)
- NIST: Federal Information Technology Security Assessment

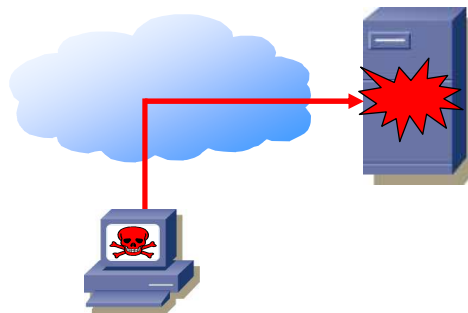
Framework (28 November 2000)

- NIST: Telecommunications Security Guidelines for Telecommunications Management Network (Special Publication 800-13)
- NIST: Minimum Security Requirements for Federal Information and Information Systems (FIPS PUB 200, March 2006)
- NIST: Recommended Security Controls for Federal Information Systems (Special Publication 800-53 Rev 3, August 2009)
- NIST: Engineering Principles for Information Technology Security (A Baseline for Achieving Security) (Special Publication 800-27 Rev A, June 2004)
- NIST: Underlying Technical Models for Information Technology Security (Special Publication 800-33, December 2001)
- TISPAN: NGN Security (NGN_SEC) Requirements, Release 1
- TISPAN: NGN Security architecture, Version 0.015
- OECD: Guidelines for the Security of Information Systems and Networks (25 July 2002)

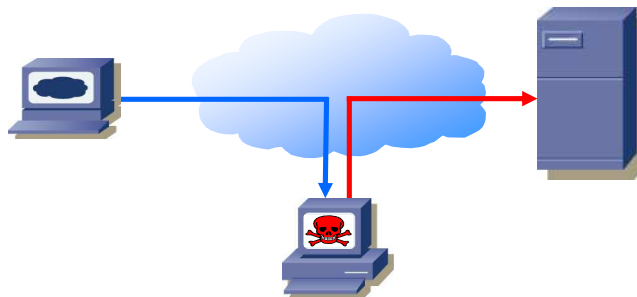
ANNEX 1 – SECURITY THREATS AGAINST NGN

The architecture identifies security issues that need to be addressed in order to prevent both intentional and accidental threats.

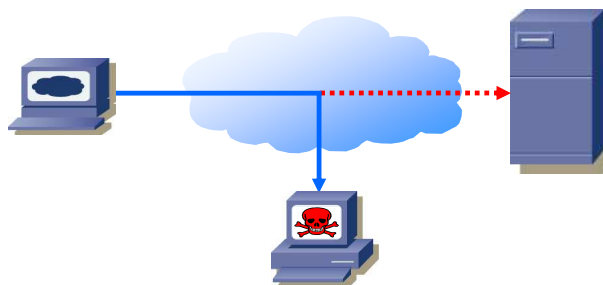
- Destruction – an attack on availability refers to the destruction of information and/or network resources



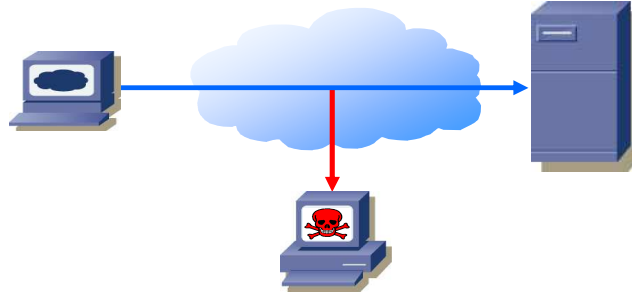
- Corruption – an attack on integrity refers to unauthorized tampering with an asset



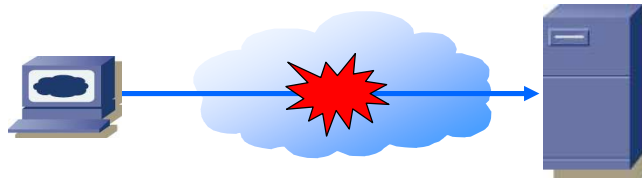
- Removal – an attack on availability refers to theft, removal or loss of information and/or other resources



- Disclosure – an attack on confidentiality refers to unauthorized access to an asset



- Interruption – an attack on availability refers to network becomes unavailable or unusable



ANNEX 2 – SECURITY DIMENSIONS FOR PROTECTION OF NGN

The security dimensions shown below outline the security protections that can be deployed to counter security threats/attacks.

1. **Access Control** – It protects against unauthorized use of network resources. Access control ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications. Examples of access control include the implementation of password, access control list (ACL), and firewall.
2. **Authentication** – It serves to confirm the identities of communicating entities. Authentication ensures the validity of the claimed identities of the entities participating in communication (e.g., person, device, service or application) and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication. Examples of authentication are the use of shared secret, Public Key Infrastructure (PKI), digital signature, and digital certificate.
3. **Non-repudiation** – It provides means for preventing an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions such as proof of obligation, intent, or commitment; proof of data origin, proof of ownership, proof of resource use. It ensures the availability of evidence that can be presented to a third party and used to prove that some kind of event or action has taken place. Examples of non-repudiation are the introduction of system logs and digital signatures.
4. **Data Confidentiality** – It protects data from unauthorized disclosure. Data confidentiality ensures that the data content cannot be understood

by unauthorized entities. Encryption, access control lists, and file permissions are methods often used to provide data confidentiality.

5. **Communication Security** – It ensures that information flows only between the authorized end points. The information is not diverted or intercepted as it flows between these end points. Examples of communication security are the support of virtual private network (VPN), multiprotocol label switching (MPLS), and Layer 2 Tunneling Protocol (L2TP).
6. **Data Integrity** – It ensures the correctness or accuracy of data. The data is protected against unauthorized modification, deletion, creation, and replication and provides an indication of these unauthorized activities. Examples of data integrity are the employment of Message-Digest algorithm 5 (MD5), digital signature, and anti-virus software.
7. **Availability** – It ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to events impacting the network. Examples of availability are the implementation of intrusion detection/protection system, network redundancy and business continuity/disaster recovery plan.
8. **Privacy** – It provides for the protection of information that might be derived from the observation of network activities. The information may include websites that a user has visited, a user's geographic location, and the IP addresses and domain names of devices in a service provider network. Examples of privacy are the use of network address translation (NAT) and encryption.

ANNEX 3 – USER BEST PRACTICES FOR ACCESSING NGN

Users are encouraged to follow the best practices below when accessing the public telecommunications services:

- keep security patches and network interface card drivers installed on the device up-to-date;
- backup all personal data on a regular basis;
- make a boot disk to aid in recovering from a security breach or hard disk failure;
- install and enable personal firewall, anti-virus and anti-spyware software and keep the associated definition files and security patches up-to-date;
- perform virus scan on removable disk and the files downloaded from Internet before using them;
- encrypt those sensitive data stored on the device accessing public telecommunications services;
- pack information or information backup in separate bag from laptop in case of theft if travelling with confidential information;
- turn off the computer/notebook or disconnect from the network when not in use;
- set Internet connection default to ‘manual’ mode instead of ‘automatic’ mode;
- employ VPN technologies for enhanced end-to-end transmission protection;
- use a password that is difficult to guess but easy to remember and change the password frequently;
- use different sets of login names and passwords for different services. Change the passwords on a regular basis;
- report abnormal behaviour to your service provider or ISP immediately;
- disable Java, JavaScript, and ActiveX if possible;

- disable scripting features in email programs;
- disable hidden filename extensions;
- do not use any device which is infected by virus/malicious code;
- do not open any suspicious email and unknown email attachments;
- do not store any personal or sensitive information on a computer that is shared with others;
- do not cache the login name and password; and
- do not download or accept programs and contents from unknown or untrusted sources.

ANNEX 4 – INCIDENT REPORTING FLOWCHART

