International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 30

(09/2017)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.805 – Supplement on security guidelines for mobile virtual network operators

ITU-T X-series Recommendations – Supplement 30

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed legder technology security	X.1400–X.1429
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Supplement 30 to ITU-T X-series Recommendations

ITU-T X.805 – Supplement on security guidelines for mobile virtual network operators

Summary

Supplement 30 to ITU-T X-series Recommendations provides security guidelines for mobile virtual network operators (MVNOs). Security is very important to MVNOs and most MVNOs have a lot of security similarities. This Supplement analyses the main features of MVNOs and the typical security threats that they face. Based on the structure of MVNOs, this Supplement provides a security framework for MVNOs, including security objectives and security requirements.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X Suppl. 30	2017-09-06	17	11.1002/1000/13410

Keywords

Mobile virtual network operator, MVNO, security guide.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

A mobile virtual network operator (MVNO) is a mobile communication services provider that does not own the wireless network infrastructure over which the MVNO provides services to its customers. An MVNO enters into a business agreement with a mobile network operator (MNO) to obtain bulk access to network services at wholesale rates and then sets retail prices independently. An MVNO usually uses its own customer service, billing support systems, marketing and sales personnel, or employs the services of a mobile virtual network enabler (MVNE). Different from traditional network operators, who own relatively independent telecommunication networks, an MVNO can only manage part of telecommunication networks and services. The service resellers of MVNOs are scattered in different places and connect to the MVNOs through different connections. It is inevitable that MVNOs face serious security threats due to inadequate security practices and requirements, which are very different from the security requirements of traditional network operators. Generally, the security capabilities of MVNOs are weaker than those of traditional network operators. MVNOs are becoming the main targets of security exploits; therefore, it is very important to develop security guidelines for MVNOs.

Supplement 30 to ITU-T X-series Recommendations

ITU-T X.805 – Supplement on security guidelines for mobile virtual network operators

1 Scope

This Supplement provides security guidelines for mobile virtual network operators (MVNOs) on how to take action against common security threats. This Supplement analyses the requirements and categories of security measures for MVNOs. It defines a set of detailed security requirements and measures for MVNOs' daily operation and maintenance. This Supplement will be helpful in reducing the security risks to MVNOs. The target audience of this Supplement is MVNOs.

2 References

[ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications.*

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 authentication [b-ITU-T X.800]: The corroboration that the source of data received is as claimed.

3.1.3 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.2 Terms defined in this Supplement

This Supplement defines the following term:

3.2.1 mobile virtual network operator (MVNO): A wireless communication services provider that does not own the wireless network infrastructure over which it provides services to its customers.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

CRM Customer Relationship Management

CSRF Cross-Site Request Forgery

DDoS Distributed Denial of Service

DLP Data Loss Prevention

DoS Denial of Service

DMZ Demilitarized Zone

HLR Home Location Register

HSS Home Subscriber Server

IAM Identity and Authorization Management

IPS Intrusion Prevention System

ISP Internet Service Provider

IPSec Internet Protocol Security

IT Information Technology

L2TP Layer 2 Tunnelling Protocol

MNO Mobile Network Operator

MVNE Mobile Virtual Network Enabler

MVNO Mobile Virtual Network Operator

RPO Recovery Point Objective

RTO Recovery Time Objective

SSL Secure Socket Layer

SQL Structured Query Language

VPN Virtual Private Network

WAF Web Application Firewall

XSS Cross-Site Scripting

5 Conventions

None.

6 Background

A mobile virtual network operator (MVNO) is a mobile communication services provider that does not own the wireless network infrastructure over which the MVNO provides services to its customers. An MVNO leases the wireless capacity from traditional network operators and packages it for a specific application. Typically, an MVNO owns its customer base, sales channel and specific brand, while providing competitive billing policies. An MVNO conventionally covers a range of different business approaches to providing mobile services. There are four common operating models of MVNOs: reseller, service operator, full MVNO and mobile virtual network enabler (MVNE), as illustrated in Figure 1.

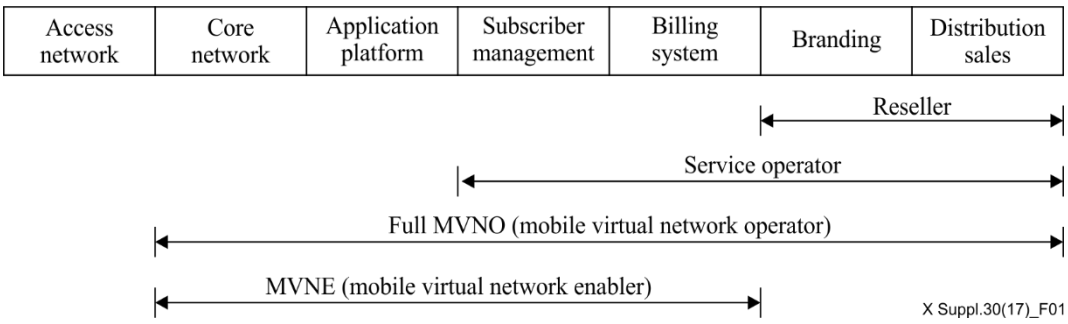

Figure 1 – Common operating models of MVNO

The four operating models of MVNOs are as follows:

1) The reseller model suits an organization that can leverage its existing distribution channels to sell mobile services, but has little need to innovate the services it provides or differentiate itself from other players. Typically, this means selling no-frills voice and messaging services.

2) The service operator model suits those organizations that wish to gain control over the services they provide, both in terms of pricing and service innovation. This means the service operator model suits players that seek to address specific customer segments, by differentiating themselves from other players in those segments through innovation in pricing and/or service content.

3) The full MVNO suits players aiming to achieve additional differentiation from service operators and mobile network operators (MNOs), by offering leading edge products and services, and achieving a high degree of independence at the outset. The full MVNO model may be the best approach for some players who would otherwise select the reseller or service operator models and introduce differentiating services into their offerings at a later date. This is because the control provided by the full MVNO model may offer better short-and long-term opportunities.

4) The MVNE model acts as an interface between a reseller or service operator and a host MNO.

Traditional network operators own relatively independent telecommunication networks, whereas MVNOs can only manage part of telecommunication networks and services. MVNOs' service resellers are scattered in various places and connect to the MVNOs through assorted connections. It is evitable that an MVNO will face serious security threats due to inadequate security practices and weak fundamental security requirements. Generally, the security capabilities of MVNOs are weaker than those of traditional network operators. This weakness causes MVNOs to become the main targets of security exploits, thus it is very important to produce a security guide for MVNOs. This Supplement mainly focuses on full MVNOs and MVNEs. Security documents for other models may also refer to this Supplement.

7 Security threats for operation

Generally, an MNO has a complete infrastructure chain including radio access, switches and other network elements, customer relationship management (CRM) and billing systems, services and content systems, and user management systems like SIM cards, home location register (HLR) and home subscriber server (HSS) offerings. In comparison, an MVNO would have some, but not all, network elements, an independent CRM and billing system, and its own user management systems which may or may not include SIM cards, but it would not have its own radio access infrastructure.

Unlike an MNO with a huge network infrastructure, an MVNO's information assets may mainly include generic equipment/systems such as databases, clusters of servers, PCs and network security equipment. An MVNO's complexity and diversity, and the inevitable vulnerabilities of its information systems and any existing flaws in administrative, logical or physical security design could be exploited and could lead to a variety of security threats. The security threats faced by MVNOs could be summarized in the following aspects. See [ITU-T X.805]:

– Destruction of information and/or other resources

The daily operations of an MVNO rely heavily on the Internet, which inevitably brings about traditional Internet security threats. Illegal intruders could utilize various kinds of vulnerabilities in security mechanisms such as access control, authentication and authorization, to execute malicious activities, which may result in information/system damage.

– Corruption or modification of information

Like all other information technology (IT) organizations, the accuracy of electronic data is a prerequisite to ensure the smooth operation of an MVNO. However, there are many factors which could provide opportunities for corruption or modification of information, such as: unreasonable role definition, loose access control, unforeseen system vulnerabilities.

– Theft, removal or loss of information and/or other resources

  Data are the core assets of MVNOs which face security threats from external attackers and/or malicious internal employees. Besides technical issues, flaws in administrative operations are often exploited, such as a lack of separation of duties and imperfect data backup processes. As with any other organization, MVNOs should also consider physical security threats including personnel, environment, fire control, etc.

– Disclosure of information

  Like MNOs, MVNOs have a huge amount of sensitive user data such as user names, ID numbers, bank accounts, call records, etc., which are high-value targets for illegal attackers. During the entire life cycle of a user's information including collection, transmission, testing, application and even destruction, existing vulnerabilities could certainly increase the probability of data leakage which may be caused by illegal attacks or internal workers' false operations.

– Interruption of services.

  To prevent unforeseen disasters or serious security incidents, MVNOs need to consider sufficient redundancy and countermeasures of availability protection, such as data backup of billing systems, network load-balancing of MVNOs connecting to MNOs, distributed denial of service (DDoS)-protection of online business systems, etc. Existing shortcomings could bring about security threats to business continuity.

8 Security requirements

Generally, the security requirements of MVNOs can be regarded as a subset of MNOs, but with two unique aspects. First, an MVNO may have to build a guaranteed response-time security mechanism in response to security events needing more processing fields that span across MVNOs and MNOs. Second, the security operations of MVNOs that have few assets, would focus on their own IT assets, while MNOs' security operations would focus much more broadly on their widespread network infrastructure.

To cope with various security threats, it is necessary for MVNOs to consider security design from six aspects including: physical, network, system, application, data, and terminal, to achieve security goals which could be understood as different levels of protection. The security goals should cover three security capability including: detection and recognition, protection, and audit and recovery, illustrated as follows:

1) Detection and recognition

   The discovery of threats is the basis for taking measures to eliminate the threats. In the security architecture of MVNOs, detection and recognition should consist of authentication, authorization, evaluation of security vulnerabilities, monitoring and warning of network attacks.

2) Protection

   Countermeasures should be integrated as an entire solution to construct an in-depth defence. The protection methods of MVNOs should not only be focused on technical issues, but should also take protection management seriously, to promote the effectiveness and efficiency of technical methods such as access control, redundancy, backup, encryption, etc.

3) Security audit and recovery

   Security audits help security specialists to verify the reliability and security status of systems and can even detect some advanced threats, while recovery is a corrective measure to ensure business continuity of MVNOs. Security incidents are hard to predict, so audit and recovery could be treated as the last line of defence.

These security goals can be further developed into detailed security requirements to achieve different levels of protection. Regarding MVNOs, security requirements mainly include the following six aspects:

1) Physical security

   For all organizations, physical security is the premise to construct a complete security architecture of information systems. Physical security requirements should not be limited to physical issues only, but should involve administrative and technical measures, which could consist of biometric authentication schemes, environment monitoring, power supply protection, crime prevention through environment design, etc.

2) Network security

   It is vital for MVNOs to maintain a reliable network even in the face of accidental disasters, malicious attacks and incorrect operations by employees. Network security requirements should consist of boundary protection, intrusion prevention, network redundancy, DDoS protection, encrypted communication, etc.

3) System security

   As the basic platform for all kinds of application systems in MVNOs, system software mainly includes operating systems and database systems. To provide a safe and stable computing environment, the security requirements of systems should consider identification, authentication, authorization, access control, intrusion prevention, operation audit, etc.

4) Application security

   The business of MVNOs is mainly built on application systems, which are software systems that provide internal and/or external services. The security requirements of application systems protect information processing processes via security tools or strategies to eliminate hidden dangers like SQL injection, cross-site scripting and Web Trojans.

5) Terminal security

   Nowadays, terminal types are abundant and include PCs and a growing number of mobile devices, which have introduced further security challenges to MVNOs and other organizations. The security requirements of terminals should comprise patch management, virus protection, intrusion detection, data protection, etc.

6) Data security

   Data are the most important assets of MVNOs. Data asset attributes can usually be described by confidentiality, integrity and availability. The security requirements of data should include encryption, key management, key escrow, data backup and recovery, etc.

9 Security countermeasures

It is necessary for MVNOs to take appropriate measures to improve their security capabilities including: detection and recognition, protection, and audit and recovery, which could build an in-depth defence. As physical security countermeasures are the same for MNOs and MVNOs, they are not discussed here. These security measures and activities include, but are not limited to, the following:

– Detection and recognition. Implementing some detection measures are required to provide basic capabilities and facilities to estimate the security status of an MVNO.
  a) network intrusion detection is specified in clause 9.1.1.
  b) scan of vulnerabilities is specified in clause 9.1.2.

– Protection. It is vital for an MVNO to take the necessary protective measures to reduce or eliminate both internal and external security threats.
  a) identity and authorization management is specified in clause 9.2.1.
  b) network access control is specified in clause 9.2.2.

c) network intrusion prevention is specified in clause 9.2.3.
d) defence of DDoS is specified in clause 9.2.4.
e) defence of malicious code/software is specified in clause 9.2.5.
f) database security is specified in clause 9.2.6.
g) Web application security is specified in clause 9.2.7.
h) data loss prevention is specified in clause 9.2.8.
i) terminal security is specified in clause 9.2.9.

– Security audit and recovery. MVNOs could implement security audits as a key method to detect unknown security threats, and not only to satisfy compliance requirements. MVNOs should also pay appropriate attention to backup and recovery procedures because they have always been regarded as the last defence of data loss.
a) security audit is specified in clause 9.3.1.
b) data backup and recovery is specified in clause 9.3.2.

Furthermore, security implementations of an MVNO should observe the following two principles:

1) Cost/benefit

Before implementation, a risk assessment should be completed, which may be based on qualitative and/or quantitative methods. High risks should be prioritized as matters to avoid, mitigate, accept or transfer.

2) Centralization

To reduce the cost of security management and improve return on investment, network security domains should be divided, protection devices at network boundaries should be deployed, identity and authorization management (IAM) should be implemented, and anti-virus systems and firewalls, among others should be installed.

9.1 Detection and recognition

9.1.1 Network intrusion detection

An MVNO should deploy network intrusion detection systems at the network boundaries of essential systems, managed and maintained by a unified console. The network intrusion detection systems should update the rules' library in a timely manner. Most importantly, security personnel must keep optimizing the detection rules in accordance with the characteristics of the MNVO's assets, which are essential to improve detection accuracy and decrease the rate of false alarms generated by the network intrusion detection systems.

9.1.2 Scan of vulnerabilities

Vulnerability scanners could be divided into two types: system vulnerability scanners and Web vulnerability scanners. An MVNO should periodically perform security scans of its hosts, servers, databases, web application systems, etc.

Once security vulnerabilities are detected, security patches or security reinforcement configurations should be implemented in a timely manner. The vulnerability scanners should also keep up-to-date the vulnerability library in a timely manner.

9.2 Protection

9.2.1 Identity and authorization management

Identity and authorization management is needed between users and hosts, and also among hosts. An MVNO should implement a well-designed IAM to ensure that its access policies are carried out

reliably and effectively, as the IAM system could prevent an attacker masquerading as a legitimate user, and guarantee legal users' legitimate interests.

For an MVNO, the implementation of IAM should meet the following capabilities:

– Reasonable centralization. In a small-scale scenario or a scenario with a small number of users and resources, the implementation could be decentralized; while in a large-scale scenario or a scenario with a large number of users and resources, the implementation should be centralized, which would obviously reduce the difficulty of security management.

– Wide variety of interfaces. The interfaces of IAM systems should support most operating systems, databases, middleware, etc.

– Adequate intensity of authentication. For important systems containing sensitive data or systems in a high-security area, a strong authentication, like two-factor authentication, should be chosen.

9.2.2 Network access control

Network access control aims to control and manage connections between trusted and untrusted zones using various measures in the network layer. It should be deployed at the network boundaries of different security zones.

As an important technical means, virtual private networks (VPNs) should be deployed at the network boundary of an MVNO's important systems; the type of VPN could be a layer 2 tunnelling protocol (L2TP) VPN, an Internet protocol security (IPSec) VPN, a secure socket layer (SSL) VPN or a combination of these. Ideally, users of VPNs should be granted different access rights according to their specific roles. In addition, in scenarios requiring high availability, the network access control components, despite of hardware or software, should be redundant.

9.2.3 Network intrusion prevention

Compared to network intrusion systems, network intrusion prevention systems extend further into block functions, which results in a diverse manner of deployment. Usually, network intrusion prevention systems are deployed in series, while network intrusion systems are deployed in parallel. Network intrusion prevention systems should be deployed at the network boundaries of an MVNO's critical systems, but with simple and limited service types, which would lead to simple but effective rules, as false blocks may cause fatal errors in services.

9.2.4 Defence of DDoS

Defence of DDoS is a systemic project. Firstly, redundant network equipment and network traffic cleaning equipment should be deployed at the network's boundaries, while the hosts of MVNO's important service systems should be deployed redundantly with a load balancer in front, or the hosts could be deployed in cluster to achieve high availability. Secondly, unnecessary network ports of an MVNO's systems should be closed, and a scanning of the MVNO's service's status should be periodically executed. Lastly, an MVNO could purchase a defence service of DDoS service from an Internet service provider (ISP) or a professional defence service provider.

9.2.5 Defence of malicious code/software

Defence of malicious code/software is needed for a system's hosts and terminal devices. Anti-virus gateway equipment could be deployed in front of an MVNO's service systems such as their e-mail system, while anti-virus software should be installed in related terminal devices. Most importantly, regardless of the anti-virus hardware or software installed, a virus database should be managed centrally and updated regularly.

9.2.6 Database security

Database systems, database security has always been an essential security target for MVNOs. Firstly, access control of database systems, including hosts and databases should be enforced. Account privileges should be minimized according to user roles. Database backup mechanisms are also important when unpredicted incidents occur. Secondly, some security countermeasures are needed including network firewalls and IDS/intrusion prevention system (IPS) systems deployed at the network boundary and anti-virus and vulnerability management software deployed in the hosts. Most importantly, a database security audit component may be needed to check each operation in the database.

9.2.7 Web application security

Generally, Web application security reinforcements should contain all the above mentioned countermeasures. Further, MVNOs should deploy web application firewalls (WAFs) at the border of demilitarized zones (DMZs).

For MVNOs, the implementation of WAFs should meet the following capabilities:

– Detection of anomaly protocol. WAFs should detect anomaly IP packets which violate the requests or responses of the HTTP standard.

– Validation of users' input. WAFs could block brute force DDoS and effectively prevent DDoS at the application layer, which would not impact Web server's performance.

– Rule-based protection. Based on detection of the anomaly protocol, WAFs should detect various attacks according to a regularly updated rules library, which includes structured query language (SQL) injection, cross-site scripting (XSS), cross-site request forgery (CSRF), etc.

Session state management. WAFs should detect abnormal events (e.g., logging failures) of a session and make suitable responses like limiting creation rates or concurrency requests.

9.2.8 Data loss prevention

Data loss prevention (DLP), using various measures, aims to prevent sensitive data leakage. An MVNO should deploy DLP in specific network security domains.

For MVNOs, the implementation of DLP should meet the following capabilities:

– Data encryption and non-repudiation

  Generally, data encryption mechanisms are based on symmetric cryptography, while non-repudiation mechanisms are based on asymmetric cryptography.

– Permission control based on users' roles

  For documents identified with a high-security level, DLP should ensure that the users have the specified access permission and roles, while other users should be blocked from accessing such documents.

– Transmission control based on a unified policy

  DLP should detect and block the transmission of sensitive information.

9.2.9 Terminal security

Terminal security aims to ensure that users' devices follow a definite level of security compliance and meet the correct standards. In MVNOs, devices could be PCs, laptops, tablets and even mobile devices. For MVNOs, the implementation of terminal security should meet the capabilities including network access control, patch management, users' behaviour management, anti-virus and update of virus libraries, asset management, etc.

9.3 Security audit and recovery

9.3.1 Security audit

Security audits are necessary to help maintain the security level of MVNOs, as they can be used for a variety of purposes, including: forensic analysis, regulatory compliance, monitoring of user activity, and troubleshooting. Regularly scheduled security audits should be carried out for all assets and services, which could be executed by an MVNO's independent internal audit team or a third-party auditor. The audit trail (such as system logs, activity reports, system configurations) should be properly collected, stored and protected to avoid unauthorized changes.

9.3.2 Data backup and recovery

In the event of a disaster or major security incident, backup and recovery is vital for MVNOs. Firstly, MVNOs should set a reasonable recovery point objective (RPO) and recovery time objective (RTO) for different systems. Secondly, the system architecture (e.g., local or distributed server clusters) and backup strategies should be designed to meet both the RPO and RTO. Lastly, the backup data should be regularly checked and the data validated and protected as the original data.

Appendix I

A practice of MVNO security

A typical MVNO is shown in Figure I.1.

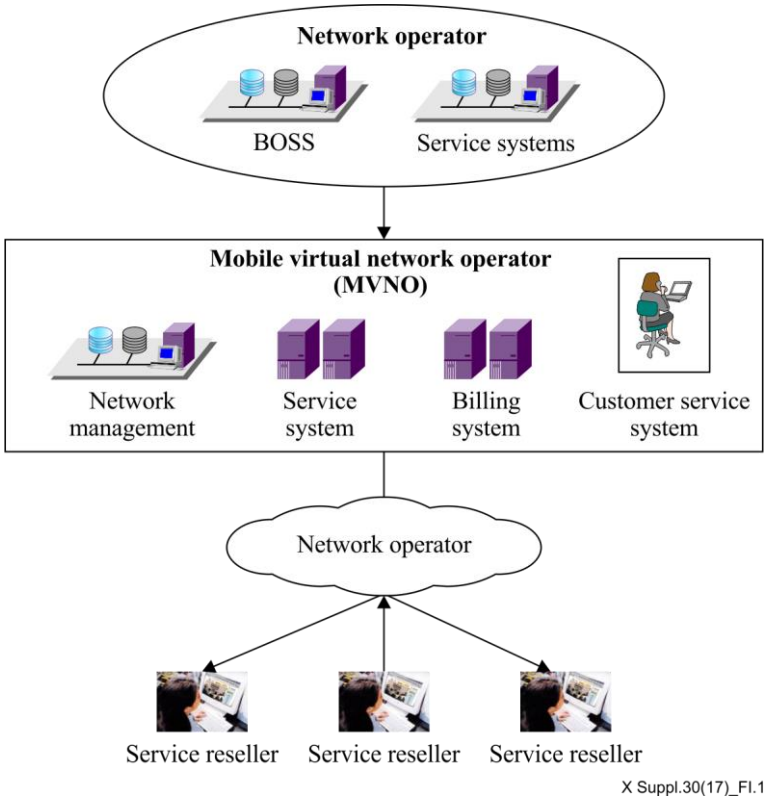

Figure I.1 – Illustration of mobile virtual network operators

A practice implementing the security measures including boundary protection, internal protection and security management is illustrated in Figure I.2.

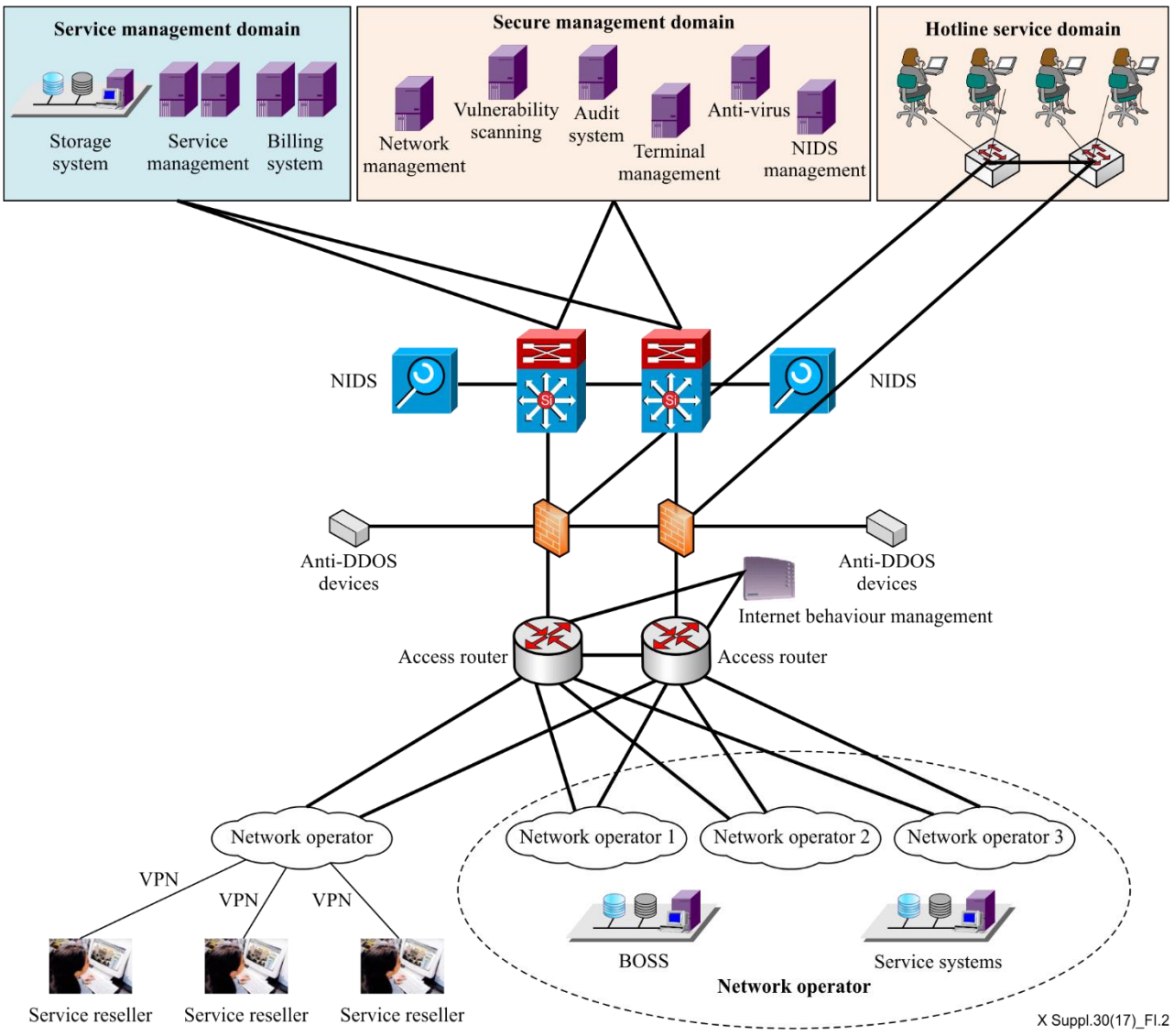

Figure I.2 – A technical security practice of MVNO

Bibliography

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*

[b-ITU-T X.1031] Recommendation ITU-T X.1031 (2008), *Roles of end users and telecommunications networks within security architecture.*

[b-ITU-T X.1032] Recommendation ITU-T X.1032 (2010), *Architecture of external interrelationships for a telecommunication IP-based network security system.*

[b-ITU-T X.1051] Recommendation ITU-T X.1051 | ISO/IEC 27011 (2016), *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations.*

[b-ITU-T X.1052] Recommendation ITU-T X.1052 (2011), *Information security management framework.*

[b-ITU-T X.1054] Recommendation ITU-T X.1054 (2012), *Information technology – Security techniques – Governance of information security.*

[b-ITU-T X.1055] Recommendation ITU-T X.1055 (2008), *Risk management and risk profile guidelines for telecommunication organizations.*

[b-ITU-T X.1056] Recommendation ITU-T X.1056 (2009), *Security incident management guidelines for telecommunications organizations.*

[b-ITU-T X.1057] Recommendation ITU-T X.1057 (2011), *Asset management guidelines in telecommunication organizations.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019