International Telecommunication Union

ITU-T X.1126

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03/2017)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services – Mobile security

Guidelines on mitigating the negative effects of infected terminals in mobile networks

Recommendation ITU-T X.1126

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	
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	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	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1379
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.

Recommendation ITU-T X.1126

Guidelines on mitigating the negative effects of infected terminals in mobile networks

Summary

Recommendation ITU-T X.1126 provides guidelines to mobile operators to restrain the infected terminals by utilizing technologies in the mobile network to protect both subscribers and mobile operators. This Recommendation describes the characteristics and effects of malicious software caused by unhealthy ecosystems in the mobile environment. Based on network-side technologies, this Recommendation focuses on mitigating the vicious effects caused by infected terminals. This Recommendation defines and organizes the mitigating measures and corresponding technologies.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1126	2017-03-30	17	11.1002/1000/13194

Keywords

Infection, malicious software, mobile network, terminal.

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

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation 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 Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation 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 Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. 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

The rapid expansion and development of operating systems for mobile devices has created a large and vibrant market for the mobile industry. Around this valuable market, many ecosystems have grown to in order to take advantage of its benefits. However, the powerful capabilities of current mobiles could also be abused by malicious software to hack the vulnerabilities of terminals, as well as networks and services, causing great damage.

Note that a healthy ecosystem should be promoted over a "closed garden" in legacy mobile systems, to secure the mobile market and protect the benefits of all relevant partners. Healthy ecosystems have been successful in some countries.

Note also that mobile market ecosystems are highly diversified in some countries, although some of them are irresponsible, unhealthy or even dangerous. The negative effects of irresponsible ecosystems could cause great damage to mobile subscribers and networks, in addition to malicious software. Sometimes, even mobile subscribers and networks in a healthy ecosystem can be affected by infected terminals, as most mobile Internet services are currently global.

The potential risks of malicious software spreading primarily in irresponsible ecosystems are listed as follows.

For subscribers:

- privacy theft, e.g., eavesdropping and location tracking;
- asset loss, e.g., system malfunction and data destruction;
- malicious transaction and consumption, e.g., sending expensive messages and dialling international call centres;
- malicious software propagation to attack other terminals;
- sending spam to annoy other subscribers;
- fraud and blackmail.

For operators, attacks on network entities, mobile services and other terminals, include:

- occupation of massive resources of networks or mobile services, resulting in their compromise and subscriber complaints about quality of service;
- hijacking service hosts and even network entities.

Malicious software brings more damaging effects to the mobile Internet than to the traditional wired Internet for following reasons.

- The mobile Internet is an emerging market, with a relatively slow development of the corresponding security mechanisms.
- Mobile terminals are often the carriers of private and confidential business deals, which are highly attractive targets to the hackers.
- Mobile networks have fewer resources, and a flood-style attack consumes them more easily and heavily.
- Many mobile terminals are strongly coupled with their networks. Malicious service and privacy theft could lead to operator revenue loss, subscriber complaints and legal issues.
- Open or cracked mobile operating systems provide breeding grounds that are out of operator control for malicious software.
- Mobile terminals often have numerous data exchange interfaces, e.g., universal serial bus (USB), secure digital (SD) card slot, and Bluetooth, many of which operators cannot secure.

In order to mitigate the damage from malicious software and to trace the sources of threats, it is vital to manage infected terminals on the network side, a responsibility and obligation of mobile operators.

Recommendation ITU-T X.1126

Guidelines on mitigating the negative effects of infected terminals in mobile networks

1 Scope

This Recommendation provides guidelines on mitigating the negative effects of infected terminals on the network side in mobile networks. This Recommendation introduces a framework that organizes the guidelines according to processes. Furthermore, this Recommendation discusses the principles, policies and technologies in these processes.

Conformance with this Recommendation is not to be taken as any proof of evidence for claiming compliance with any national or regional law, regulation or policy. The technical, organizational and procedural means described in this Recommendation do not in any way guarantee the constitution of any level of security that may be put upon certain correspondence by specific national or regional law, regulation or policy.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 blacklist [b-ITU-T X.1245]: An identification list of persons or sources in communication services, where the identifications of the list are denied to access particular communication resources.

3.1.2 malware [b-ITU-T X.1211]: Malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability.

NOTE – Examples include: viruses, ransomware, spyware, adware and scareware.

3.1.3 mobile network [b-ITU-T X.1121]: A network that provides wireless network access points to mobile terminals.

3.1.4 mobile terminal [b-ITU-T X.1121]: An entity that has wireless network access function and connects a mobile network for data communication with application servers or other mobile terminals.

3.1.5 spamming [b-ITU-T X.1244]: A chain of activities carried out by spammers to send spam, such as collection of target lists, creation of spam, delivery of spam, etc.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 botnet: A group of compromised computer systems that are infected with malicious software and connected in a coordinated fashion for malicious purposes without the owner's knowledge, e.g., to transmit malicious software or spam, or to launch attacks.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

App Application running on mobile terminals

API	Application Programming Interface
C&C	Command and Control
DDoS	Distributed Denial of Service
GGSN	Gateway General packet radio service Support Node
IP	Internet Protocol
MMS	Multimedia Messaging Service
MMSC	Multimedia Messaging Service Centre
SD	Secure Digita
SIM	Subscriber Identity Module
SMS	Short Message Service
SMSC	Short Message Service Centre
URL	Uniform Resource Locator
USB	Universal Serial Bus
VAS	Value-Added Service
WAP	Wireless Application Protocol

5 Conventions

None.

6 Framework and processes

In most cases, after being infected by malicious software, most mobile terminals can still access the network and use as usual all kinds of services, as well as starting to unleash negative effects on networks and services, which subscribers may be unaware of. The mobile operator is bound to be aware of the infection and restrain the infected terminal properly to keep its network and service capabilities in a stable condition and to maintain its credibility by protecting subscriber benefits. Figure 1 depicts a framework for mitigating the negative effects of infected terminals in which there are three types of role: of operators, subscribers and other organizations. Operators play the key role in the framework and their work can be divided into three processes: discovery, governing and information sharing. In order to support all three processes, malicious software and source database are involved in the framework. Operators undertake the processes in this framework taking into account the national legal and regulatory obligations in individual member states in which they operate.

There are relationships among the three roles: Operators discover and govern anomalies of subscriber terminals on the network side, and then inform subscribers about the threats that these anomalies pose. Furthermore, operators can also share malicious software information with collaborative operators and organizations.

In the discovery process, sample applications (Apps) running on mobile terminals and attack reports can be collected and analysed to discover anomalies in the mobile network. Anomalies and affected terminals are reported during the governing process. In the governing process, anomalies are validated and specific measures taken to mitigate negative effects on subscribers and operators. In order to provide timely information to counter or handle mobile malicious software, an information-sharing process should be established. In the information-sharing process, malicious software information is shared with collaborating operators and organizations, to enhance the security of the whole industry.

Malicious software and source database: Running through all processes, there is a database of malicious software and sources to store and provide knowledge about such code including its behaviour patterns and sources. The knowledge supports the identification of anomalies, control of infected terminals and publication of malicious software information in the three processes. In addition, new knowledge of malicious software from the discovery and information-sharing processes can be uploaded to the database to implement "always-up-to-date" protection.

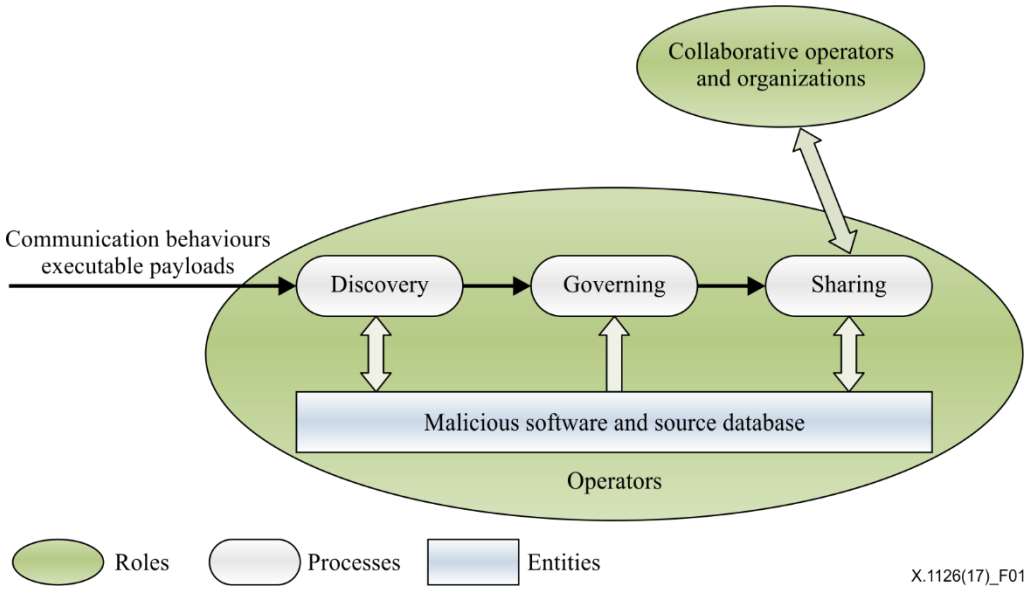

Figure 1 – Framework of mitigating the negative effects of infected terminals

7 Discovery

In the discovery process, sample Apps in App stores and attack reports from both terminals and network elements are collected to analyse anomalies in the mobile network that may be indicators or clues of infected terminals and malicious sources. Figure 2 depicts the workflow of the discovery process.

All data used in this clause and those following can be collected from sample Apps in App stores and attack reports from subscriber terminals or network elements. Any use of data can be related to subscriber privacy in the discovery process and can need subscriber agreement or authorization according to local legislation. Data use should be strictly limited to the analysis of malicious software and related activities, and nothing else.

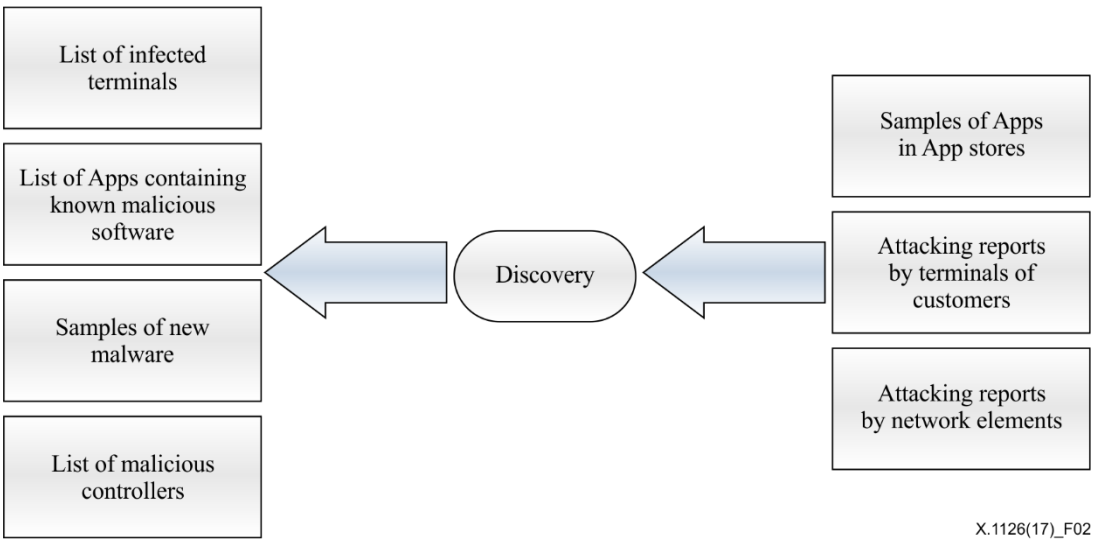

Figure 2 – Interactive relationships for the discovery process

7.1 Collection of applications and attack reports

In the discovery process, two kinds of data can be collected to characterize network anomalies:

- attack reports from subscriber terminals and network elements;
- samples of Apps from App stores or markets.

7.2 Analysis of infected terminals and known malicious software

Some infected terminals can be identified from attack reports. Additional signature matching can assist in finding some new Apps that contain known malicious software.

Analysis of infected terminals and known malicious software is used to locate malicious controllers hiding in the network.

The Internet protocol (IP) addresses in the controlling packets of infected terminals require analysis to identify IP sources that command infected terminals or collect the status of infected terminals.

Dynamic analysis shall be adopted for known malicious software found in Apps to check whether there is any update by malicious controllers.

7.3 Analysis of new malicious software

Based on the Apps obtained from App stores, new malicious software can be discovered by behaviour, static and dynamic analyses.

7.3.1 Malicious codes and executables analysis

Static analysis: This approach is used to understand suspected malicious software at a syntactic level. For example, a mobile application can be disassembled by reverse-engineering techniques to get its manifest file (containing information about permissions that the application accesses) and source codes. By examining the manifest file and scanning the application programming interface (API) invoking characteristics, a number of malicious attempts can be recognized in terms of some typical detection policies:

- if any unnecessary and sensitive access privilege is permitted;
- if the network API is invoked to access malicious Internet sources;
- if the process API is invoked to terminate an application;
- if the process API is invoked to export contact information to a specific location;

- if the behaviour of the reading secure digital (SD) (memory) card or the subscriber identity module (SIM) card is abnormal;
- if there is an exchange of data with known malicious uniform resource locators (URLs);
- if there is a service subscription short message service (SMS) not requested by the subscriber;
- If there are some instructions to control the mobile terminal remotely.

Dynamic analysis: The approach runs and monitors suspicious mobile malicious software in a controlled (and even virtualized) environment (such as sandboxes). The following are some typical detection policies.

a) Botnet communication:

   i) Description: The bot has to report its existence to a command and control (C&C) server to join the botnet, and the C&C server instructs the botnet to conduct malicious activities. The C&C server can be a web server or a terminal in the mobile network, and the instruction can be issued through the Internet, SMS and multimedia messaging service (MMS) services.

   ii) Detection policies:

      1) A large number of terminals connect to a known malicious host.
      2) A terminal connects to a known malicious host regularly for a long time.
      3) A terminal sends binary SMS messages to a large number of terminals.

b) Propagation and spamming:

   i) Description: The malicious software spreads itself or sends spam to other subscribers through various services (Internet, MMS, SMS, etc.) as widely as possible.

   ii) Detection policies:

      1) A large number of terminals send the same MMS or SMS messages (the messages are compared with a one-way hash), and their geographical distribution is arbitrary.
      2) The volume of a service surges dramatically in an idle time.
      3) Making triple calls.
      4) Sending SMS messages.
      5) Sending MMS messages.
      6) If a spooned call is invoked by software.
      7) If the information in the SIM card is exported to a server by software.
      8) If a malicious call is invoked after a short period by software.
      9) If there is any induction of additional download unnecessarily.
      10) Accessing known malicious controllers.

c) Malicious subscription and consumption:

   i) Description: The infected terminals will subscribe to value-added services (VASs), and to triple call services, to make premium rate calls or international calls and send a large number of messages. The subscriber will not be aware of these charges.

   ii) Detection policies:

      1) Unexplained rise in the subscriber's bill.
      2) The infected terminal frequently makes premium rate calls or international calls at specific time periods.
      3) Numerous terminals constantly send the same messages many times at specific time periods.

4) The terminal subscribes to the triple call services and uses them frequently and even all the time.

d) Distributed denial of service (DDoS) attack:

i) Description: A crowd of terminals flood the radio and other resources in the mobile network to compromise quality of service.

ii) Detection policies:

1) The traffic in gateway general packet radio service support node (GGSN) or other network entities surges dramatically and most traffic has the same destination.

Static analysis is not appropriate for suspicious malicious software that is concealed or obfuscated and dynamic analysis cannot cover the complete program code. Therefore, both static and dynamic analysis should be performed to gain a complete understanding about how that particular malicious software functions.

Abnormal attempts or behaviours captured and recognized by static and dynamic analysis are useful in updating policies in behaviour analysis for the latest anomaly scenarios. Furthermore, these recognized characteristics can help the operator to find unknown malicious URLs or IP addresses.

7.3.2 Combination approach

A combination of the two analytical approaches to improve the performance and reduce false positives in the discovery process is therefore suggested.

In the discovery process, various outputs can be generated to support the following governing process. The output of the discovery process should include, but is not limited to:

- list of infected terminals;
- samples of Apps containing known malicious software;
- samples of new malicious software;
- list of malicious controllers.

The above information is vital for operators to take appropriate measures in the processes described in clauses 8 and 9.

8 Governing

In the governing process, discovery process outputs are analysed and validated automatically or semi-automatically. Governing measures are then carried out according to the severity of anomalies. Figure 3 depicts the interactive relationships between the governing process and other network and service entities.

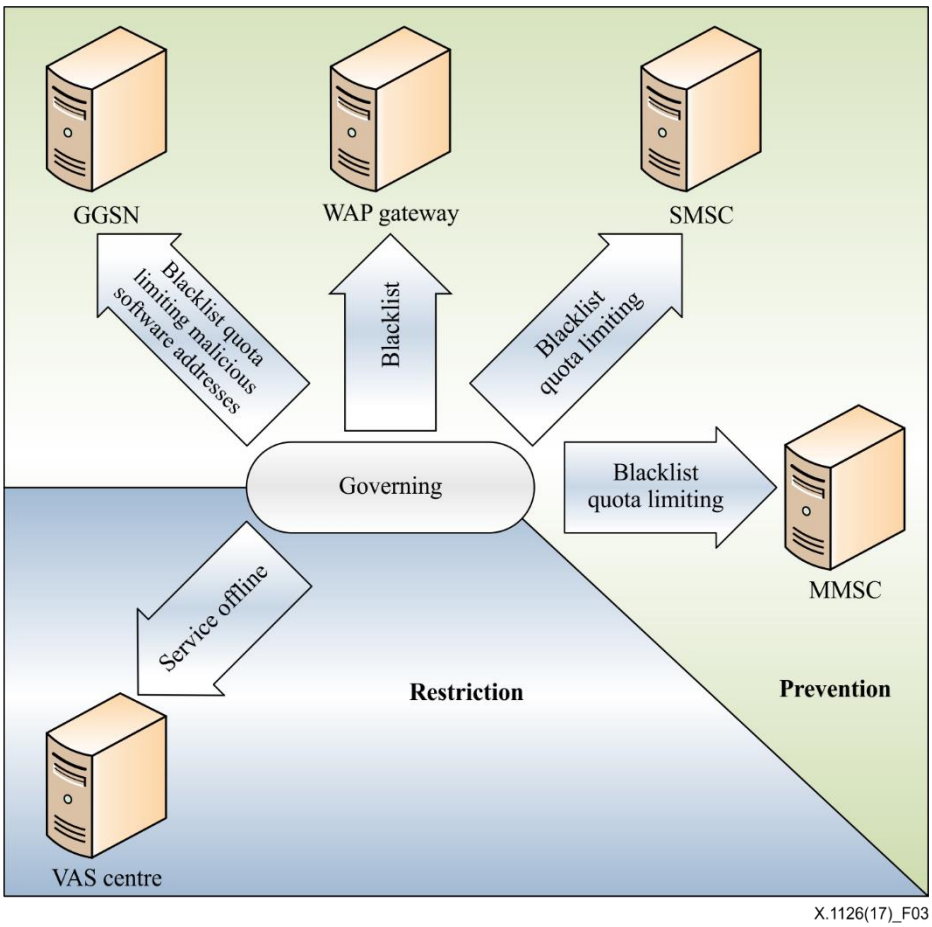

Figure 3 – Interactive relationships for the governing process

8.1 Governing measures

There are two kinds of measure associated with different severity of anomalies: prevention and restriction, both of which only utilize the capabilities of network entities and service-supporting platforms.

- Prevention: If the anomaly is moderate and can be controlled without interrupting services offered to subscribers, the prevention method can be adopted to handle the problem.
- Restriction: If the prevention approach has failed and the subscriber has already suffered a great loss of money, restriction is employed to selectively or completely suspend the affected service.

8.2 Prevention

8.2.1 Blacklist

When an anomaly is triggered by a malicious controller, the controller can be added to a blacklist. Any subsequent requests to or from that controller are then blocked. There are many network entities, e.g., GGSN, wireless application protocol (WAP) gateway and multimedia messaging service centre (MMSC), that support the blacklist function. Multiple blacklists can be kept to block different kinds of malicious controllers, e.g., domain names of malicious websites and IP addresses of C&C servers. Note that the sources in the blacklist will be confirmed and updated regularly in order to avoid blocking legitimate sources.

Any addresses that linked to the download of any App containing malicious software can be blocked by the GGSN.

8.2.2 Quota limiting

When spamming activity is the main cause of an anomaly in the network, e.g., a DDoS attack, the quota-limiting approach can be employed to mitigate spread speed. Quota limiting defines a threshold for the maximum number of messages that can be sent in a certain time period (e.g., a month) with full guarantee of the fundamental or emergency communication capability of any terminal. When the message number exceeds the threshold, no more messages are allowed to be sent.

8.3 Restriction

8.3.1 Operator's service offline

If a malicious controller lies in the service of an operator, which is caused by hacking maybe, the operator can wield the right and obligation to offline its own service temporarily and use the backup service if necessary with the obligation of emergency communication.

9 Information sharing

Governing cannot be the final goal, as it just tries to minimize the negative impact on subscribers and networks. The final goal is to get things back to normal and to try to prevent wider infection. Therefore, the information-sharing process is important for the perfection of the whole framework.

To enhance the welfare of the industry, only malicious software samples should be shared between operators.

Note that the information-sharing process should comply with local legislation and subscription contracts.

Bibliography

[b-ITU-T X.1121] Recommendation ITU-T X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

[b-ITU-T X.1211] Recommendation ITU-T X.1211 (2014), *Techniques for preventing web-based attacks*.

[b-ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications.*

[b-ITU-T X.1245] Recommendation ITU-T X.1245 (2010), *Framework for countering spam in IP-based multimedia applications*.

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, 2017