[2017 TopN Security Threats and Preventive Measures for Mobile Networks]

2017.10

HUAWEI

Contents

Foreword

Today, we are living in a globally connected world. Mobile Internet has become one of our daily basic requirements. Mobile Internet of Things (IoT) is growing exponentially. In future, mobile communications will face thousand-fold proliferation of data traffic and hundreds of billions of networked devices. Fortunately, MBB networks have not encountered large-scale targeted attacks so far. Against the explosive growth of mobile Internet, we are living in one of the best ages.

Are the MBB networks really immune to security attacks that would occur? Are we prepared to address them? Of billions of new IoT devices connected to enterprise networks, a huge proportion cannot stay immune to attacks, and therefore more new services simply would mean more victims. The Dyn cyberattack in October 2016 reminded us of the fragileness and proneness of our IoT networks to cyber attackers. From this perspective, we may also live in one of the worst ages.

This document identifies TopN security threats for mobile communications based on Huawei understanding of security challenges on mobile communications networks, aiming at helping customers build secure networks.

In the long run, we also hope to increase the industry-wide importance attached to security issues and promote sharing and cooperation in security across the industry. We believe that cooperation among suppliers, operators, and all those in this industry chain is indispensable to constructing secure, fully connected societies.

1 Overview

Welcome to TopN Security Threats and Preventive Measures for 2017 Mobile Networks drafted by Huawei Wireless Product Line. In 2012, Huawei established the dedicated Product Security Incident Response Team (PSIRT) to collect security vulnerabilities in conjunction with the computer emergency response team (CERT) groups, industry organizations, and vulnerability databases. Huawei has been a continuous contributor to the best practices in vulnerability processing.

Huawei PSIRT explores vulnerability information from diverse sources, such as subscriptions to security websites, cooperation with other organizations, security conferences, and various CERT groups. In 2016, PSIRT subscribed to over 200 security websites via RSS or email and received 200–300 mails on average per day. PSIRT has also set up VulnCenter to obtain vulnerability information from professional vulnerability information providers, such as VulnDB. Furthermore, PSIRT has been closely following and attending industry security conferences, for example, Hack In The Box, Black Hat, and FIRST Conference. As an active contributor to open source communities, PSIRT reports discovered vulnerabilities to these communities. Huawei actively analyzes the root cause of each vulnerability, extracts their common features, and summarizes TopN security threats based on Huawei understanding on the newest vulnerabilities in the industry.

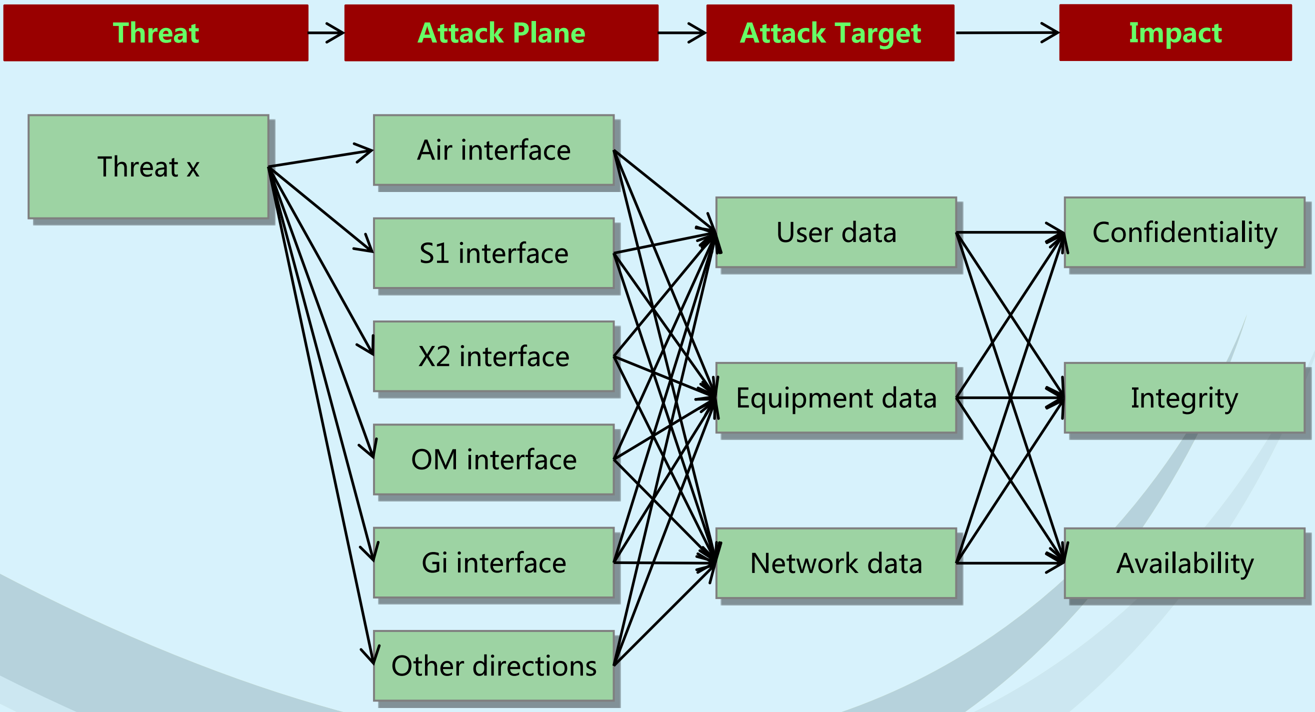
These security threats possibly undermine services on mobile networks. For each type of security threat, this document uses a base score from Common Vulnerability Scoring System v3.0 for risk assessment, analyzes the root cause, and offers suggestions based on Huawei mobile communications products, hoping that these preventive measures can help the customers against security loss caused by security vulnerabilities.

The TopN security threats will be subject to constant updates in response to changes in internal and external environments

2 Mobile Networks Security Threats

1. What Are Mobile Networks Security Threats?

There are many paths attackers can find to gain access to and potentially do harm to services provided over a mobile communications network. Each one represents a type of threat that may, or may not, be serious enough to warrant attention.



Some paths can be easily found and exploited, but some others are not. Similarly, the threats may damage none or all of the services. The security risks need to be assessed by taking into considerations both service conditions and impacts, such as the threat likelihood, possible attack surfaces, possible attack vectors, and impact on confidentiality, integrity, and availability. Together, these factors determine the overall risks.

2. What Are Our Security Threats?

This document focuses on the TopN security threats, the ones which may cause the most severe damage, or which are the most likely to affect networks. A base score from Common Vulnerability Scoring System v3.0 is used for risk assessment regarding each type of threat.

Threat	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact
Threat Description	Network	High	High	Not Required	Changed	High	High	High
	Adjacent Network	Low	Low	Required	Not Changed	Low	Low	Low
	Local		None			None	None	None
	Physical							

Only you know the specifics of your own system's environment. Depending on the actual situation and network configuration, certain security threats may not be relevant to your network, but some may have severe impact on your system. Therefore, you must evaluate each risk yourself. In this document, the risk assessment is based on a base score from Common Vulnerability Scoring System v3.0.

The TopN security threats are named after the type of attack, vulnerability, or impact they represent. We chose names that accurately reflect the threats and, where possible, align with common terminology most likely to raise awareness.

3. References

https://www.first.org/cvss/specification-document

https://www.first.org/cvss/calculator/3.0

https://www.first.org/cvss/user-guide

3 TopN Mobile Networks Security Threats

T1 - SS7/IPX/Diameter threats

SS7 was originally designed for closed telecom networks. Security depends on the network closeness, but these days networks are increasingly opened. On an SS7 network, an attacker can track users, intercept messages, or launch DoS or fraud attacks. The threats facing SS7 networks problems are also present on 3G and 4G IPX/GRX/Diameter networks.

T2 – IoT security threats

The advent of IoT terminals poses new security risks to mobile communications networks. Insecure IoT terminals may spread malicious traffic such as viruses, and massive numbers of IoT terminals may cause DoS attacks

T3 – False GSM base stations

Lack of mutual authentication mechanisms is a fatal flaw in GSM. Which can be exploited by setting up a false GSM BS to launch attacks on attached UEs. The UEs can be tracked, eavesdropped on, spoofed, or subjected to SMS scams. Sending junk or smishing messages from a false GSM BS has become an important part of the telecom fraud chain, intensifying the security threats.

T4 – Air interface protocol-based user tracking

Location tracking violates user privacy, yet attackers can never get bored in doing it. It is true that existing mobile communications protocols can use a temporary identity that constantly changes to prevent passive listening. It is also true that attackers can find a way to actively locate users, for example by using IMSI catcher, proved by the disclosure that even a temporary identity is no longer safe

T5 – DoS attacks over air interface

The mobile network safeguards transmission over the air interface via measures such as authentication, encryption, and integrity protection, which start through a security activation procedure. However, prior to this procedure, UEs and the network communicate in plain text, which can be forged or tampered with by attackers to launch DoS attacks

T6 – Forced 3G/4G-to-2G fallback

A mobile communications network comprises multiple access technologies, such as GSM, UMTS, and LTE. GSM is prone to security vulnerabilities, represented by one-way authentication, lack of integrity protection, and unreliable encryption algorithms. Many attackers attempt to force UMTS/LTE UEs to fall back to GSM networks and then attack the UEs while they are there

T7 – NFV security threats

Virtualization of functions used on mobile system not only broadens the attack surface, but also poses new challenges to security management due to its flexibility and scalability. An attacker can look for security vulnerabilities at different NFV layers, intercept or tamper with service NE data, and interfere with other normal services, sabotaging the confidentiality, integrity, and availability of NFV data

T1 SS7/IPX/Diameter Threats

1. Risk Assessment

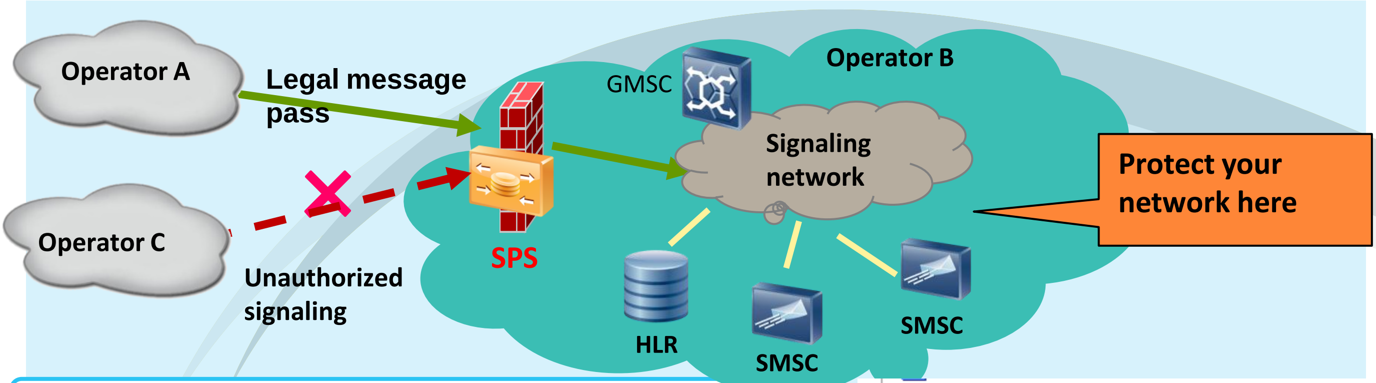
Threat	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact
SS7/IPX/Diameter threats	Network	Low	Low	Not Required	Changed	High	High	High
	Attackers can remotely access SS7/IPX/Diameter networks to track users, intercept messages of users, or launch DoS and fraud attacks. Currently, attack tools can be exploited to reduce the attack complexity. Attackers may access the SS7/IPX/Diameter network without requiring any privilege, and can initiate attacks without users knowing. Security flaws in an SS7 node can be abused to degrade the security of the entire network.					Attackers can track users, intercept messages of users, or launch DoS or fraud attacks to ruin the communication confidentiality, integrity, and availability		

2. Root Cause

- SS7 treats all nodes on an SS7 network as trusted. Given the multitude of SS7 nodes from global operators and interconnection operators, however, it is actually difficult to ensure that all the nodes are trustable. Once an attacker controls an SS7 node, the attacker can exploit the node to track users, intercept messages of users, or launch DoS or fraud attacks through SS7 signaling.
- SS7 vulnerabilities are also present on GRX/IPX and Diameter networks
- Hackers have already devised some tools to facilitate exploitation of SS7 vulnerabilities

3. Preventive Measures

- Deploy SS7/Diameter signaling firewalls on the operator networks to enable category-based signaling filtering, as recommended by GSMA[1][2].
- Enable location check for the signaling firewalls. For example, upon the reception of a location update request sourcing from a new MSC/VLR, a signaling firewall checks whether the UE has left the previously serving MSC/VLR or determines the possibility of the UE traveling to the new MSC/VLR. If the UE stays served by the original MAC/VLR or is unlikely to move to the new MSC/VLR, the signaling firewall performs error handling, such as rejecting the location update request or logging the error
- Figure T1.1 shows the Huawei SS7 Security Solution



The supported signaling screening types:

Direction - Linkset

MTP - OPC/DPC

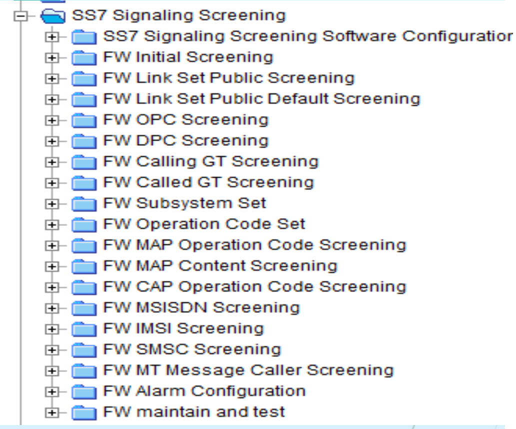
SCCP - calling/called GT, SSN, translation type

MAP/CAP - Operation Code

SMS - IMSI, MSISDN and SMSC address

IMSI/MSISDN – user number of Category 2 and 3 MAP messages

…



- SS7 Signaling Screening
  - SS7 Signaling Screening Software Configuratior
  - FW Initial Screening
  - FW Link Set Public Screening
  - FW Link Set Public Default Screening
  - FW OPC Screening
  - FW DPC Screening
  - FW Calling GT Screening
  - FW Called GT Screening
  - FW Subsystem Set
  - FW Operation Code Set
  - FW MAP Operation Code Screening
  - FW MAP Content Screening
  - FW CAP Operation Code Screening
  - FW MSISDN Screening
  - FW IMSI Screening
  - FW SMSC Screening
  - FW MT Message Caller Screening
  - FW Alarm Configuration
  - FW maintain and test

FigureT1.1 SS7 Screening to Prevent Unauthorized Access

4. Attack Case

In May 2017, many bank accounts were drained in Germany. The attacked banks used two-factor authentication for key transaction acts such as payment. This authentication mode requires a user to input the account password and an SMS verification code sent by a bank. Attackers first installed malware on the victims' computers, and stole the victim account passwords and information such as the mobile number. Then the attackers exploited the SS7 vulnerabilities to intercept SMS verification codes sent by the bank to crack the two-factor authentication

More Information refer to:

https://www.theregister.co.uk/2017/05/03/hackers_fire_up_ss7_flaw/

5. References

[1] GSMA FS.07 SS7 and SIGTRAN Network Security

[2] GSMA IR.82 Security SS7 implementation on SS7 network guidelines

T2 IoT Security Threats

1. Risk Assessment

Threat	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact
IoT security threats	Network	Low	Low	Not Required	Changed	High	High	High
	Attackers can remotely attack IoT devices, networks, and applications. IoT devices have inadequate security protection. Often located within the reach of attackers, IoT devices are prone to attacks. Attackers can launch attacks without requiring any privilege. Attacks can be launched without user awareness. After cracking an IoT device, an attacker can exploit the IoT device to attack the network and IoT applications.					Attackers can track users, launch DoS or fraud attacks, or exploit IoT devices to attack the network, harming the confidentiality, integrity, and availability of IoT communication.		

2. Root Cause

- IoT device suppliers come with insufficient security capabilities. Forrester's global organization survey shows that 47% business organizations using or planning to use IoT have been exposed to security risks. 27% of the control systems are damaged or infected. 80% of the devices use simple passwords. 70% of the communications are not encrypted. 90% of the firmware upgrades do not check the signature.
- IoT device security varies greatly. Some devices with low power consumption, low storage, and low computing capability have a low device security protection level. Some devices are deployed in unattended areas. Therefore, IoT devices are vulnerable to attacks. In addition, remote management of massive terminals is a demanding task. Vulnerability repair and upgrades may not be performed in a timely manner.
- The design of IoT access protocols and application layer attaches importance to the function implementation but lacks consideration of security mechanisms.

3. Preventive Measures

The operators must address IoT security from multiple angles, covering the sensing layer, network layer, and application layer.

- The sensing layer involves the sensing devices, identification devices such as radio frequency identification (RFID), GPS positioning devices, and smart devices with part or all of such functions.
  The sensing layer is the source of IoT data. Sensing layer security must be designed based on the device capabilities. Operators should evaluate the security assurance of attached IoT devices to reduce the chance that they are hacked.
- The network layer encompasses the access network and core network. The access network allows wireless access over a short or long distance.
  The network layer is the transport layer of IoT information and data and sends the data collected by the sensing layer to the application layer for further processing. When deploying the network layer security, operators must comply with the local data privacy protection regulations and international security standards, support protection against DoS attacks, and use firewalls to identify and filter malformed packets and block traffic attacks.
- The application layer analyzes and processes data transmitted from the network layer, to provision users with a variety of services such as a smart grid, intelligent logistics, and smart transportation.
  In terms of application layer security, it is recommended that operators implement threat modeling, vulnerability detection, and attack defense by using big data analysis and machine learning to identify IoT network security postures and unknown security threats, and achieve second-level notification and coordinating, helping timely discover and intercept malicious behavior and avoiding negative impact to the overall network and service operation.

4. Attack Case

In July, at Black Hat USA 2017, hackers disclosed vulnerabilities inherent to the insecure MQTT communication protocol used by IoT devices. The protocol is widely used on IoT devices in the power and other industries, allowing attackers to detect and attack IoT devices and servers, making them malfunction

More Information refer to: https://www.blackhat.com/us-17/briefings/schedule/#taking-over-the-world-through-mqtt---aftermath-6462

T3 False GSM Base Stations

1. Risk Assessment

Threat	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact
False GSM Base Stations	Adjacent Network	Low	Low	Not Required	Unchanged	High	High	High
	Rogue base stations attract nearby UEs and launch attacks on the UEs that attach. There are already false GSM base stations mature enough to initiate attacks. Attacks do not require any specific privilege. Some attacks such as eavesdropping do not require user involvement. Extra permissions are beyond the reach of attacks, such as the permission to tamper with SIM card files in OTA mode.					A false GSM base station can track users, eavesdrop on users, or launch spoofing or SMS scam attacks. Sending junk or smishing messages by using a false GSM base station has become an important part in the telecommunication fraud chain, intensifying the security threats.		

2. Root Cause

- Lack of mutual authentication is a fatal GSM defect. This defect can be exploited by an attacker to set up a false GSM base station, attract UEs to access this base station by means of high power and special cell selection and reselection parameters, derive UE IMSIs or IMEIs from location update signaling, and then track users, eavesdrop on users, or launch spoofing or SMS scam attacks. Sending junk or smishing messages by using a false GSM base station has become an important part in the telecom fraud chain, intensifying the security threats

3. Preventive Measures

- Operators can deploy the false base station detection solution on the network side, which checks the signaling procedures (such as abnormal Location Update signaling) for the presence of false base stations. This solution can help the operators locate in-network false base stations but cannot prevent UEs from accessing such base stations.
- UEs capable of false base station detection can avoid them, effectively reducing the hazards they represent. Such UEs can identify and block false base stations based on inherent characteristics such as cell selection and reselection parameters. Also, based on malicious SMS messages reported by applications, such UEs can identify whether the base station sending the malicious SMS messages is false after double checking the signaling exchanged with the base station.

4. Attack Case

2016 China False Base Station SMS Research Report of 360 Mobile Security

- In March, 2016, 360 Mobile Security intercepted 11 million SMS messages from false base stations, on average about 3.548 million per day. The top three sources included a fake CMB 95555 hotline, a fake ICBC 95588 hotline, and a fake China Mobile 10086 hotline.
- Among the SMS messages sent by false base stations, advertisements ranked first with 41.3% of the total; Law violation accounted for 33.8% and smishing made up 24.0%. Among the advertising SMS messages, advertisements for financial services ranked first, accounting for 47.5% of the messages.

2016 China False Base Station Report of Tencent Mobile Manager

- In February to May 2016, about 4, 618,455 SMS messages received by UEs were sourced from false base stations.
- Smishing, law violation, and advertisements are the top three contributors to such messages, accounting for 72.59%, 15.26%, and 12.13%, respectively. This means that, almost 90% of such messages are associated with various illegal activities, potentially posing security threats to users.

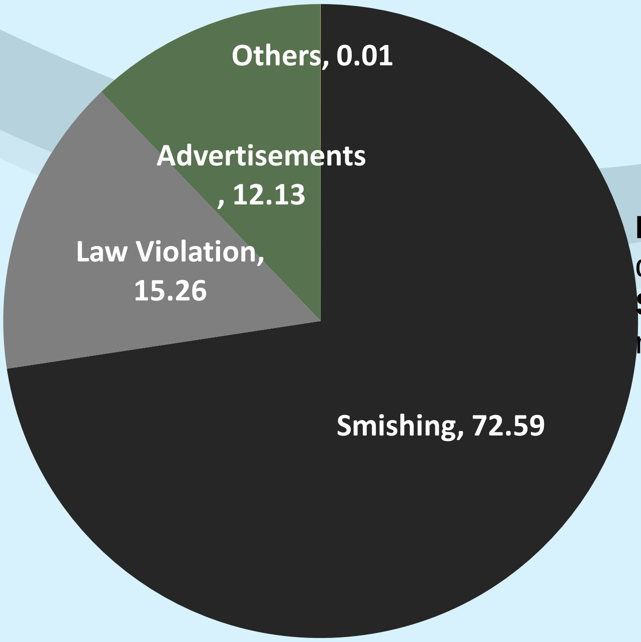


Figure T3.1 The ratio of different type of fraudulent SMS
Source: Tencent mobile phone manager

T4 Air Interface Protocol-based User Tracking

1. Risk Assessment

Threat	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact
Air interface protocol-based user tracking	Adjacent Network	Low	Low	Not Required	Unchanged	High	None	None
	Nearby attackers can listen in on signaling exchanged between the network and the users. Some open-source projects can make building a false base station easier. Attackers can launch attacks without requiring any privilege. Attacks can be launched without user involvement. Attackers can trace user locations					Attackers can locate users (cell granularity) without users knowing.		

2. Root Cause

- An IMSI is a permanent user identity that can be transmitted over the air interface in plaintext. An attacker can launch attacks, such as building a false base station, to request the IMSI of a user and then locate the user.
- Currently, 3GPP specifications embrace temporary identities to counteract passive user tracking like eavesdropping. The temporary identity needs to be updated frequently. However, 3GPP specifications do not define the update frequency. They but leave it up to the operator-desired configuration. In actual scenarios, temporary identities are not upgraded frequently enough, and attackers can exploit this defect to identify a given user, and then track that user.
- Existing LTE specifications confine the network-side paging to the entire tracking area (TA). To reduce the signaling load, some operators and equipment manufacturers use Smart Paging technology, which initiates paging first in the last served cell of a UE and only after that, if no response is received in this cell, in the entire TA. The cell that is currently serving a particular UE can be identified (generally an area of approximately two square kilometers).

3. Preventive Measures

- Reallocate GUTI in the attach and TAU procedures.
- After a UE is in the RRC_CONNECTED state for a specified duration, allocate a new GUTI to the UE through the GUTI relocation procedure. The duration has certain randomness (for example, between 30 minutes and 1 hour) so that GUTI allocation rules cannot be predicted, further enhancing the user identity confidentiality
- The 5G system will use public keys in USIM cards to encrypt IMSIs

4. Attack Case

In November 2015, researchers in Black Hat Europe demonstrated how to exploit infrequently updated TMSIs to locate users. Attackers can use Facebook or Whatsapp to page UEs and eavesdrop in areas where users are likely to visit, then successfully locating the users.

More Information refer to: https://www.blackhat.com/docs/eu-15/materials/eu-15-Borgaonkar-LTE-And-IMSI-Catcher-Myths.pdf

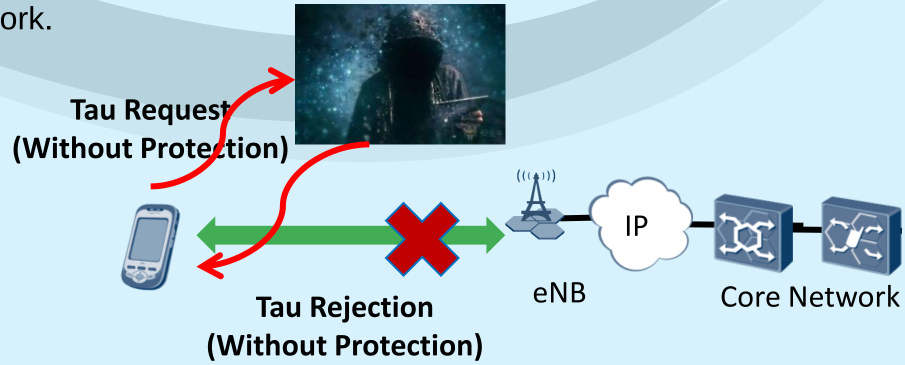
T5 DoS Attacks over Air Interface

1. Risk Assessment

Threat	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact
DoS Attacks over the Air Interface	Adjacent Network	Low	Low	Not Required	Not Changed	None	Low	High
	Nearby attackers can build a false base station to attract UEs and then tamper with or forge signaling exchanged between the network and any of the UEs attached to the false station, to launch DoS attacks. Some open-source make building a false base station easier. Attackers can launch attacks without requiring any privilege. Attacks can be launched without user involvement. Attackers can launch DoS attacks to users or the network.					Attackers can tamper with or forge signaling, affecting the integrity of signaling. Attackers can launch DoS attacks against the availability of users and the network.		

2. Root Cause

- ➢ Although systems such as UMTS and LTE can protect security of most signaling and data. However, security protection is started only posterior to the security activation procedure. Messages transmitted prior to this procedure are void of security protection and can be abused by attackers to initiate DoS attacks to users and the network. For example, an attacker can forge messages to deny access, causing UEs to become disconnected from the network.



- ➢ Attackers can also send a large number of messages to the network prior to the security activation procedure, causing DoS attacks to the network.

3. Preventive Measures

- Operators can use the following 3GPP-defined security mechanisms to mitigate risks:
  - 3GPP TS 24.301[1] has redefined the way UEs process unprotected NAS reject messages. The new processing mechanism can protect the UEs against DoS attacks.
  - 3GPP specifications also define the mechanism that performs integrity check on the unprotected initial uplink NAS messages. This mechanism prevents attackers from modifying capability information in unprotected initial uplink NAS messages to launch downgrade attacks to UEs.
- Operators should deploy anti-DoS-attack mechanisms such as congestion control on network devices.

4. Attack Case

In 2016 and 2017, 3GPP work groups work on the methods of attacks using unprotected NAS messages and countermeasures, with the emphasis on the following two attacks:

- Attack 1[2]: The UE can send a TAU Request message, which is integrity-protected using the existing NAS security context but not encrypted. As a result, a rogue eNodeB can decode it and respond with a "TAU Reject" message including the cause #7 "LTE services not allowed" without the integrity protection. This reject message will be processed by the UE, which reacts on the indicated rejection cause by deleting all existing EPS context. Furthermore, the UE updates the status to "EU3 ROAMING NOT ALLOWED" and considers the USIM (and hence the UE) as invalid for EPS services until it is rebooted or USIM is reinserted.
- Attack 2[3]: An attacker modifies the IEs included by the UE in Attach/TAU Requests, which results in the UE ending up attached to the network in ways the UE had not requested, e.g. for SMS only

5. References

[1] 3GPP TS 24.301

[2] 3GPP TDoc: C1-161448

[3] 3GPP TDoc: C1-171951

T6 Forced 3G/4G-to-2G Fallback

1. Risk Assessment

Threat	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact
Forced UMTS/LTE-to-GSM fallback	Adjacent Network	Low	Low	Not Required	Changed	High	High	High
	Nearby attackers trick UEs into accessing GSM networks. Open-source projects significantly reduce the difficulty of these attacks. Attackers can launch attacks without requiring any privilege. Attacks can be launched without user involvement. After UEs access a GSM network, attackers can eavesdrop on users or launch spoofing or DoS attacks.					After deceiving UEs into accessing GSM networks, attackers can exploit GSM security vulnerabilities to eavesdrop on users or launch spoofing or DoS attacks.		

2. Root Cause

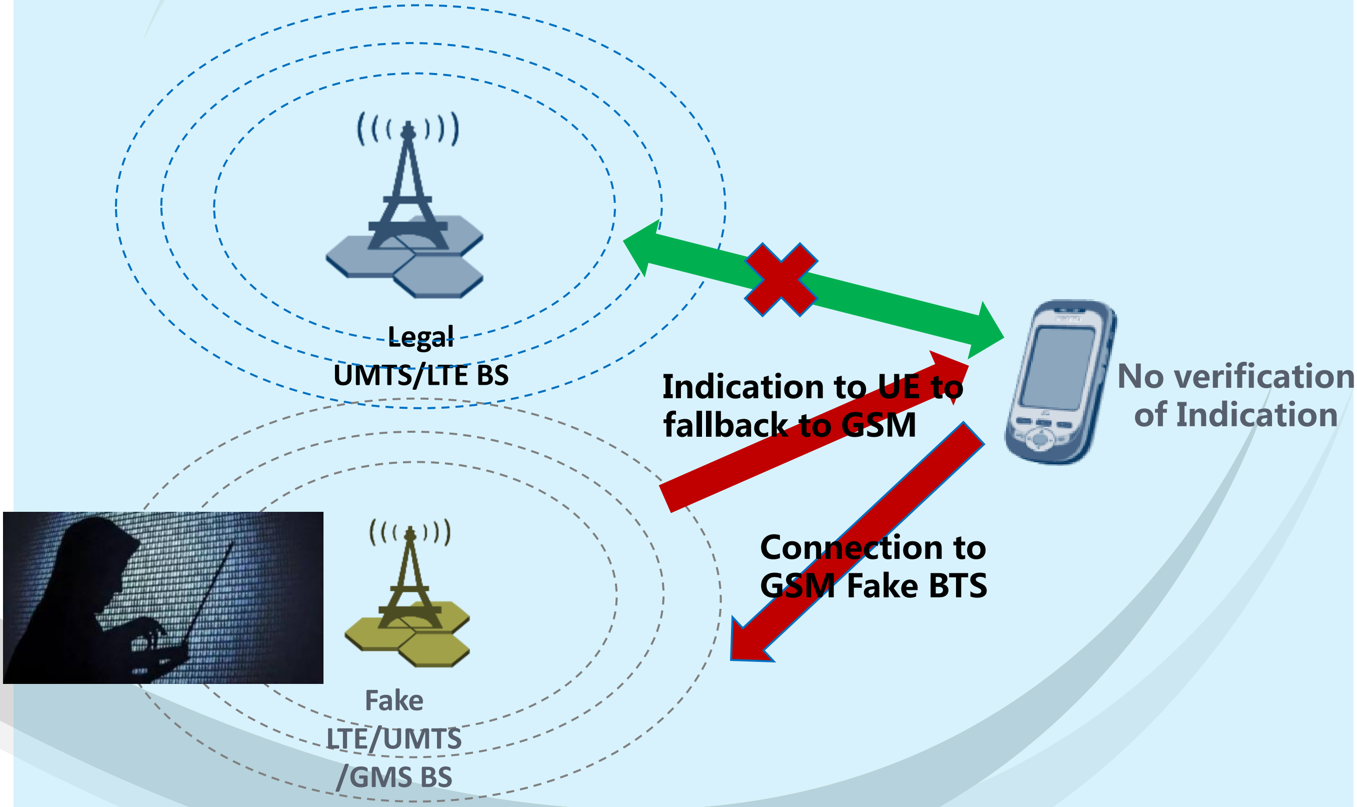
- Currently, GSM, UMTS, LTE systems all exist together on mobile communications networks. UEs usually support all the three systems. The GSM system has security flaws, such as a lack of mutual authentication or integrity protection for signaling, and defective encryption algorithms. Attackers can force UEs to fall back the GSM system in multiple ways, by masking UMTS and LTE signals for example, and then exploit the GSM security flaws to attack the UEs. Recently, mobile communications networks are subject to more efficient and hidden ways to force the fallback

3. Preventive Measures

- Operators should try their best to enhance the GSM network security so that attackers cannot launch attacks even if UEs are forced to fall back to the GSM network. To this end, measures such as increasing the authentication frequency and adopting the standard A5/4 cipher algorithm can be taken.
- Integrity protection is imperative for messages that the network signals UEs to fall back from the LTE/UMTS network to the GSM network. 3GPP groups are discussing the possible solutions

4. Attack Case

Near the end of 2016, researchers of 360 Security disclosed an LTE vulnerability in DEFCON[1]. An attacker could build a false LTE base station to forge RRC Release messages containing specially designed redirection data. The data instructed UEs to fall back to a false GSM base station built by the attacker



5. References

[1] https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Zhang-Shan-Forcing-Targeted-Lte-Cellphone-Into-Unsafe-Network.pdf

T7 NFV Security Threats

1. Risk Assessment

Threat	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact
NFV security threats	**Network**	**Low**	**Low**	**Not Required**	**Changed**	**High**	**High**	**High**
	Attackers can remotely attack virtualized NEs. The virtualization technology makes this type of attack easier. Attackers may launch attacks without requiring privilege. Attacks can be launched without user involvement. The attack scope can be enlarged.					An attacker can attack security vulnerabilities at different NFV layers, intercept or tamper with service NE data, and interfere with other normal services, sabotaging the confidentiality, integrity, and availability of service network data carried by NFV		

2. Root Cause

Network function virtualization of the mobile communications system not only increases the attack surface, but also creates new challenges to security management due to its flexibility and scalability. NFV has the following security challenges:

- Platform layer: The NFV underlying layer uses the cloud-based data center pools and leverages the virtualization technology to provide a service hosting environment. Due to the absence of physical borders, NFV inherits all of the security threats intrinsic to cloud computing and virtualization technologies, for example, attacks launched by malicious VMs both internal and external to the virtualized network. There are backdoors and hijacking attempts arising from virtualization layer vulnerabilities, attacks launched by malicious VMs to the platform layer, and then to authorized VMs, unauthorized access due to storage sharing, and unauthorized access to residual data. Decoupling of software from hardware and the utilization of white box trend servers contribute to improving resource efficiency but also expand the attack surface of underlying services compared with traditional hardware products.
- Management plane: NFV adds new management functions to dynamically orchestrate network services and resources, which extends the trust chain. Attacks can control a management function to maliciously configure NEs or abuse resources, or tamper with the management channel to cause a management function to work improperly, affecting normal services and resource arrangement. Security policies are difficult to coordinate in cross-layer multi-vendor management scenarios, resulting in poor performance and low security efficiency.

- Dynamic service orchestration: The security environment is continuously changing due to dynamic orchestration of NFV services. Service migration, scale-up, or scale-down arouses changes in the VM quantity, resource occupation, geographical location, service status, and network configuration. In response to such changes, security policies must be updated promptly to ensure that the new VMs are in a secure environment. Compared with the traditional fixed network structure, the NFV architecture requires dynamic adjustment of security NEs and their configurations, which cannot be achieved by using static security policies

3. Preventive Measures

Operators should enhance the following aspects security of NFV NE security.

- Platform layer
  - Detection and response: Provide unified user, log, and vulnerability management and operations audits. Ensure that user behavior is controllable, manageable, and traceable. Enable trusted computing and remote verification to form a secure execution environment for the platform layer.
  - Virtual storage security: Isolate and control access to upper-layer application data. Delete VM data completely when necessary, and store key data in an encrypted manner, preventing information from being intercepted or tampered with.
  - Virtual computing security: Leverage strong access control and use intrusion and escape detection mechanisms to provide a secure virtualization execution environment for upper-layer applications.
  - Virtual network security: Provide a multi-faceted isolation mechanism covering resource isolation, traffic isolation, virtual firewall (VFW), disk file write (DFW), and security group.
  - System hardening: Use default system hardening to eliminate known security threats.
- Management plane
  - Embrace trusted technologies and construct a trust chain from the platform layer to the MANO domain, and improve the verification mechanism to achieve trusted management.
  - Use a unified IAM authentication technology, establish a flexible access control model, and support fine-grained access control, flexible implementation mechanism, and centralized management of network device authentication credentials.
  - Perform security hardening for interfaces and introduce anti-fraud, non-repudiation, and anti-eavesdropping security protocols to ensure the security of the management interfaces.

- Automatic orchestration of security policies
  - Implement unified orchestration of service-oriented policies and policy-driven security through abstraction and modeling of security and service policies.
  - Develop automatic O&M tools to implement functions such as automatic patch upgrades and weak password detection given the multitude of VMs.
  - Identify known and unknown threats by using big data and machine learning to analyze massive security events and information collected by system agents

4 Conclusion

2017 has witnessed wider application of mobile communications, but there have also been increasingly difficult challenges to network security. Cyber security will undoubtedly become a fundamental issue of for the 5G system.

This document is written based on Huawei own understanding. Huawei believes that the entire ecosystem, including the industry, operators, and end users must make joint efforts to cope with network security problems and challenges, and better enjoy the benefits and conveniences of a secure, fully-connected word

This document is provided “as-is” without warranty of any kind, express or implied. All warranties are expressly disclaimed. Without limitation, there is no warranty of non-infringement, no warranty of merchantability, and no warranty of fitness for a particular purpose. Huawei assumes no responsibility for the accuracy of the information presented. Any information provided in this document is subject to correction, revision and change without notice. Your use of, or reliance on, the information provided in this document is at your sole risk. All information provided in this document on third parties is provided from public sources or through their published reports and accounts.
HUAWEI and HUAWEI are trademarks or registered trademarks of Huawei Technologies Co., Ltd.
All other company names, trademarks mentioned in this document are the property of their respective owners.