THREATS TO PACKET CORE SECURITY OF 4G NETWORK

2017

POSITIVE TECHNOLOGIES

CONTENTS

TERMS AND ABBREVIATIONS

3GPP—The 3rd Generation Partnership Project

AUC—Authentication Center

CDR—Charging Data Record

CGF—Charging Gateway Function

Diameter—An authentication, authorization, and accounting protocol for computer networks

DPI—Deep Packet Inspection

EIR—Equipment Identification Register

eNodeB—Evolved Node B is the element in air interface of 3GPP LTE

GRX—GPRS Roaming Exchange

GTP-C—GTP control protocol is the control section of the GTP standard

GTP-U—GTP user data tunneling is in effect a relatively simple IP-based tunneling protocol which permits many tunnels between each set of endpoints

HLR—Home Location Register

HSS—Home Subscriber Server

IMS—IP Multimedia Core Network Subsystem

IMSI—International Mobile Subscriber Identity

LTE—Long Term Evolution

MME—Mobility Management Entity

OCS—Online Charging System

OFCS—Offline Charging System

MSISDN—Mobile Station ISDN Number

PCEF—Policy and Charging Enforcement Function

PCRF—Policy and Charging Rules Function

P-GW—Packet Data Network Gateway

S1AP—S1 Application Protocol

SCTP—Stream Control Transmission Protocol

S-GW—Serving Gateway

SS7—Signaling System No. 7

TEID—Tunnel Endpoint Identifier

TMSI—Temporary Mobile Subscriber Identity

UDP—User Datagram Protocol

UE—User Equipment

VLR—Visitor Location Register

Broad adoption of 4G mobile networks has simplified access to high-speed Internet for billions of users. However, more than smartphones, tablets, and computers are connecting to 4G en masse. The high speeds and minimum latency of LTE networks allow using them for building out the infrastructure of the Internet of Things. Analysts estimate that by 2022, the number of IoT devices connected to mobile networks will increase from 400 million to 1.5 billion.[1] Thus the security of Smart City systems, self-driving connected cars, and other IoT technologies will partially depend on the security of today's (4G) and tomorrow's (5G and LTE-M) mobile networks.

In 2016, Positive Technologies experts analyzed the security of 4G signaling networks. On all the tested networks, the experts found vulnerabilities caused by fundamental deficiencies in the Evolved Packet Core. The issues detected allow disconnecting one or more subscribers, intercepting Internet traffic and text messages, causing operator equipment malfunction, and carrying out other illegitimate actions. To exploit vulnerabilities in 4G networks, an attacker does not need hard-to-obtain tools or considerable skill.

This report details possible attack scenarios and lists the measures necessary to improve security.

EVOLVED PACKET CORE: MAIN COMPONENTS AND PROTOCOLS

For 4G networks, the 3GGP consortium developed a new architecture for the network core—the System Architecture Evolution (SAE)—which is designed around the Evolved Packet Core (EPC). Compared to previous-generation networks, the structure of the EPC is simpler (Figure 1), with increased bandwidth and reduced signal delays in the transmission of user data and service information. One important component in prior generations, the circuit-switched network, has disappeared entirely. Instead, 4G networks are built as an All IP Network, in which data and voice calls are transmitted in a packet environment. However, not all operators have implemented the necessary technologies (for example, IMS for VoIP) for voice transmission via 4G. In such cases, when a call is made, the subscriber's connection is downgraded to 2G/3G and may be subject to the vulnerabilities that we have described on numerous occasions in our previous research.[2]

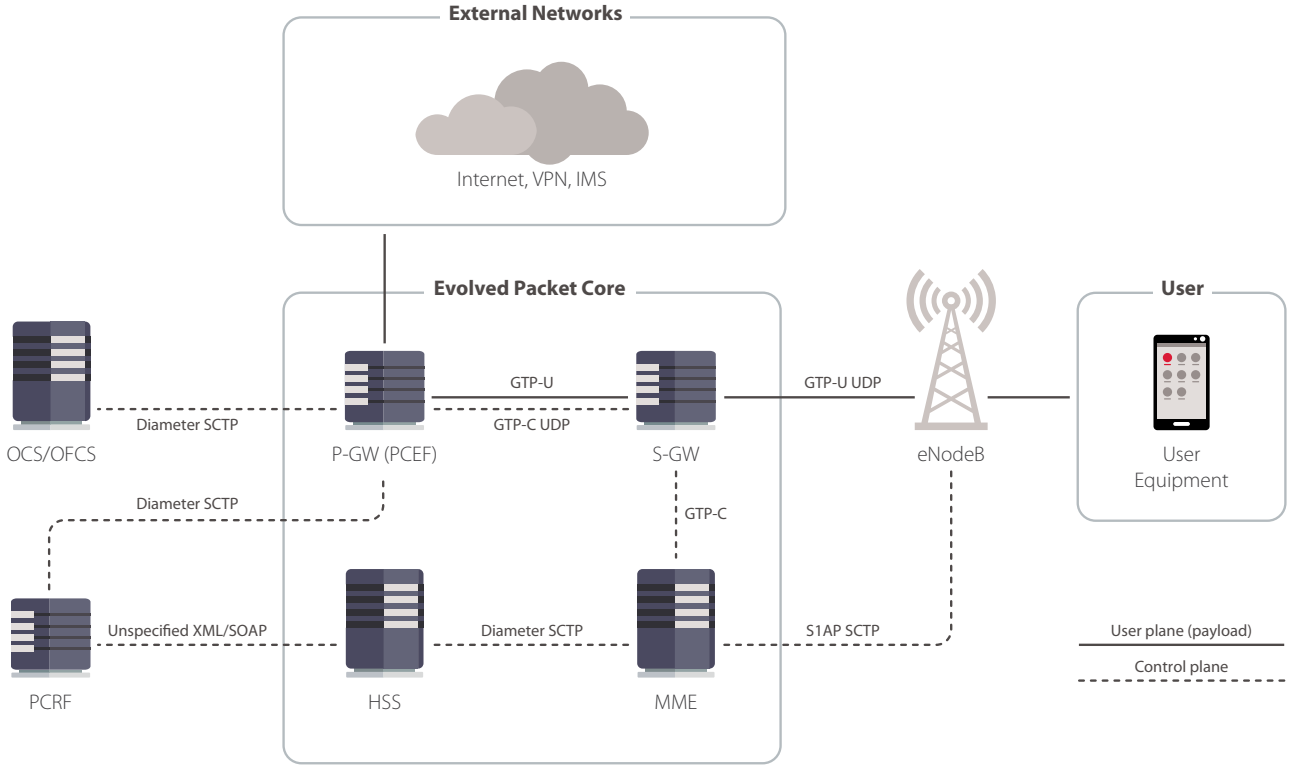

Figure 1. Evolved Packet Core (EPC) structure

1 Ericsson Mobility Report 2016:
www.ericsson.com/assets/local/mobility-report/documents/2016/ericsson-mobility-report-november-2016.pdf

2 Primary security threats for SS7 cellular networks (2016):
www.ptsecurity.com/upload/corporate/ww-en/analytics/SS7-Vulnerabilities-2016-eng.pdf

The following elements are the main components of the packet core:

Home Subscriber Server (HSS) is a large database for storing information about subscribers. In effect, the HSS replaces the VLR, HLR, AUC, and EIR databases used in 2G/3G networks.

Serving Gateway (S-GW) handles transmission and processing of user data between user equipment (UE) and the base station subsystem of the operator's LTE network (eNodeB).

Packet Data Network Gateway (P-GW) manages data streams transmitted to external packet networks, and in essence acts as the entry and exit point for user traffic on the operator's network. When combined with the PCEF (a network element responsible for applying charging rules), it ensures the correct operation of billing systems and the application of charging rules.

Mobility Management Entity (MME) enables switching between base stations and roaming. In addition, the MME is responsible for authenticating user equipment (UE) by interacting with the HSS, as well as for selecting the S-GW.

Each EPC node can, in addition to checking and filtering network packets by their content (DPI), implement lawful interception functions used by law enforcement agencies.

For interaction, EPC nodes use the GPRS Tunneling Protocol (GTP), S1 Application Protocol (S1AP), Diameter, and other protocols. The main threats to the Diameter protocol are detailed in our previous report.[3] The attacks analyzed in this report are aimed at nodes that interact via the GTP protocol.

ATTACK SCENARIOS

Of particular interest to attackers are special interfaces for exchanging information between EPC components. These interfaces are rich with signaling traffic, which consists of both service and user information. None of these interfaces have built-in data encryption mechanisms, due to which attackers can conduct the following attacks:

+ Interception of user MSISDN and IMSI
+ Subscriber location discovery
+ Man-in-the-middle attacks for unencrypted traffic (interception of access to unencrypted mail, browsing history, etc.)
+ Interception of text messages
+ Eavesdropping on VoLTE calls via packet interception
+ Identity spoofing for fraudulent purposes
+ Denial-of-service attacks on subscribers causing loss of user data during transmission, and call interruptions on VoLTE networks
+ Denial-of-service attacks on equipment causing network disruptions

The majority of possible attack scenarios are possible because of how roaming is implemented and deficiencies in inter-operator interaction via the GRX network (GPRS Roaming Exchange). Signal and user traffic crosses the network boundary of one operator and is transmitted both over the GRX transit packet network and over the guest operator network. To ensure user authentication and the application of charging rules, the participants of inter-operator exchange interact via open interfaces. An attacker can take advantage of these interfaces to attack subscribers or the operator's equipment.[4]

WHAT IS NECESSARY FOR A SUCCESSFUL ATTACK

Such attacks via the GRX global roaming exchange network can be conducted by employees of almost any mobile operator as well as by external attackers who have access to the operator's infrastructure. An external attacker could gain such access by taking advantage of dictionary passwords or the simplest vulnerabilities on the network perimeter.

Before LTE, voice call interception required that the attacker have special equipment and in-depth knowledge of the specific protocols used for voice calls. But since 4G networks are built on the principle of All IP Network, the attacker can use all currently available hacking tools, which are largely automated and do not require a deep understanding of the nature of the attack. It is enough for an attacker to have a laptop, public-domain software for penetration

3 Next-generation networks, next-level cybersecurity problems: www.ptsecurity.com/upload/iblock/a8e/diameter_research.pdf
4 www.ptsecurity.com/upload/corporate/ww-en/analytics/GPRS-Vulnerabilities-eng.pdf

testing, and basic programming skills. Real operator GGSNs are often available on the Internet with real APNs and subscribers, which reduces the time to prepare the simplest attack—a DoS attack on a subscriber—to just several hours, including preparation of the necessary tools.

The data needed to start an attack depends on the protocols involved and the required message parameters. Initially, the attacker needs to have the Temporary Mobile Subscriber Identity (TMSI), International Mobile Subscriber Identity (IMSI), and Tunnel Endpoint Identifier (TEID).

The attacker can obtain the correct TEID by bruteforcing, that is, sending GTP-U messages with arbitrary TEID values to the P-GW. If the TEID is incorrect, the P-GW responds with a GTP-C "Error Indication" message; if no error message is received, the TEID is correct (Figure 2). Although a full search can take several hours, the range of TEID values can be predicted for most devices, which allows reducing this time to several minutes.

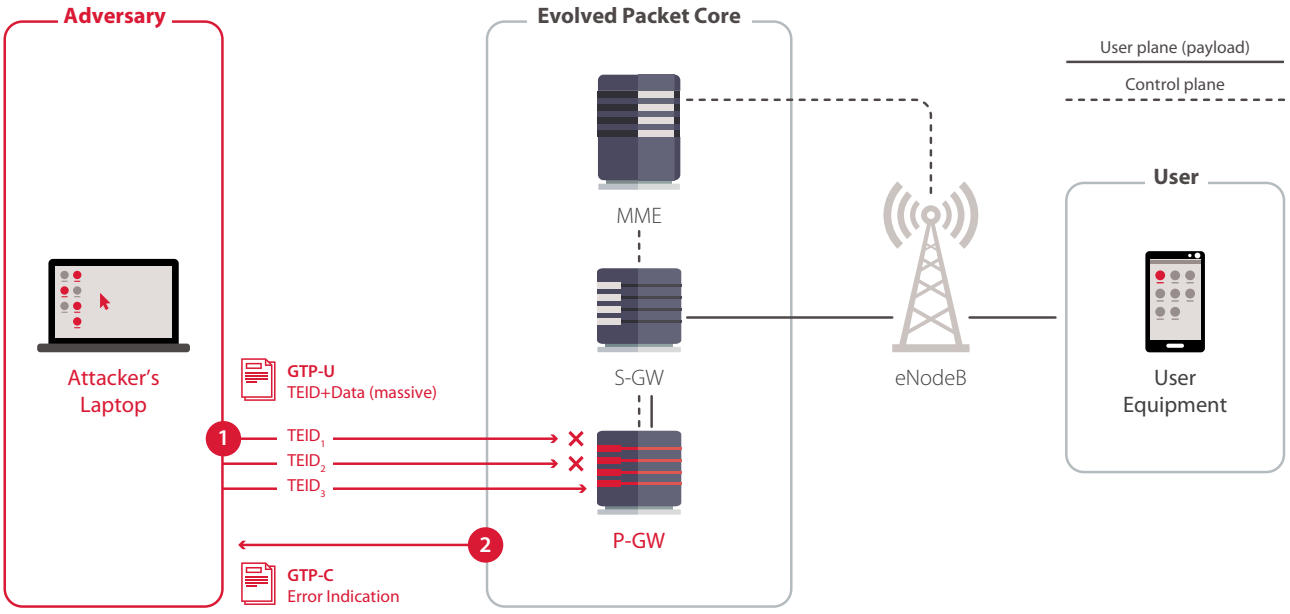

Figure 2. Bruteforcing the Tunnel Endpoint Identifier (TEID)

To successfully conduct some of the described attacks, the attacker needs to specify the victim's TMSI in the generated requests. The TMSI can be obtained by bruteforcing, passive radio scanning with the help of a fake base station (FakeBTS) or an IMSI catcher.

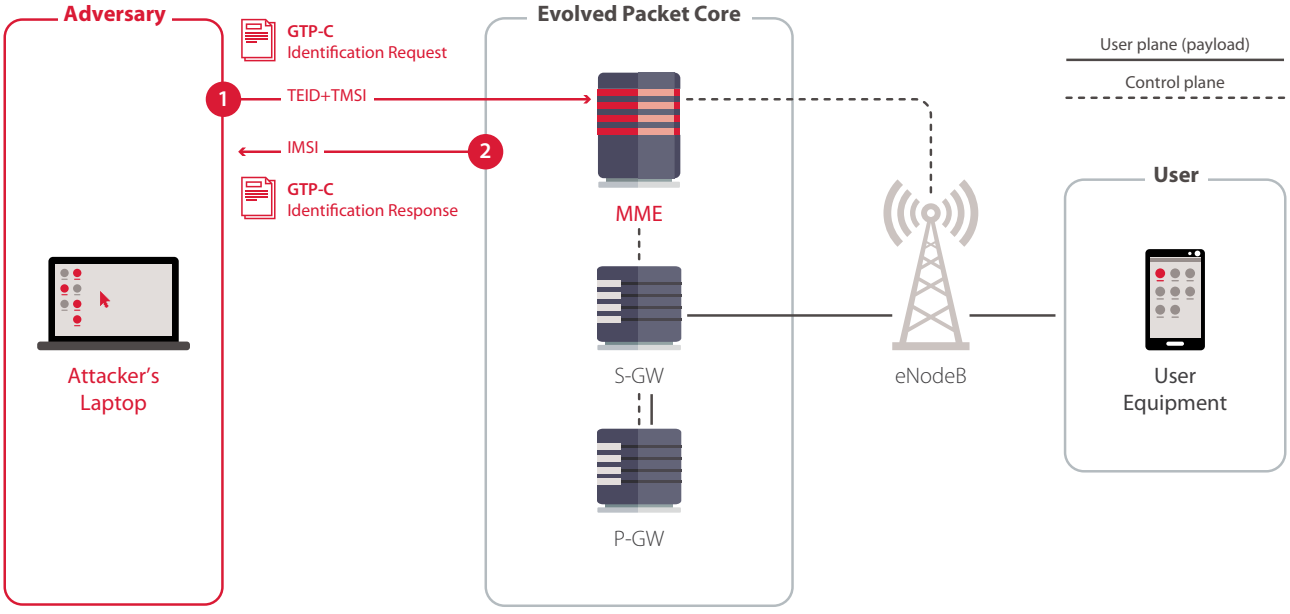

Figure 3. Determining the subscriber's IMSI

With the TEID and TMSI, an attacker can then determine the subscriber's IMSI (Figure 3). For this, the attacker needs to send a GTP-C "Identification requests" message to the MME. If the request succeeds, an "Identification Response" message containing the IMSI of the victim subscriber is received in response.

The IMSI is the basic ID used for attacking SS7 and Diameter. In addition, this attack allows bypassing the radio interface protection that masks real IMSIs by replacing them with TMSIs, and tracking subscriber location by passive radio scanning.

THREATS TO EPC SECURITY

The EPC is the basis of 4G networks, but it contains protocols and mechanisms for backward compatibility with previous-generation networks (2G/3G). For example, the S-GW and P-GW must support the older GTPv1 protocol for normal switching from 4G to 2G/3G when LTE becomes unavailable.

In some cases, even if a device can handle GTPv2 packets, equipment manufacturers may overlook GTPv1 packet validation: work on obsolete technologies usually stops when new ones appear, and it is often impossible to simply disable support for the old protocol. As a result, the attacker can conduct attacks on subscribers and the operator's equipment via the GTPv1 protocol, which is easier and faster. For example, to intercept a subscriber's Internet session, the parameters of the GTPv2 "Context Request" message must contain the reason for sending this message (location update), switching parameters, encryption types supported by the mobile device, etc. By contrast, its GTPv1 equivalent, the "SGSN Context Request" message, must contain only the TMSI.

The attack scenarios detailed in this report involve GTPv2 messages.

1. Fraud

Insufficient protection of EPC components allows the attacker to gain access to the operator's services and resources bypassing the charging system or at the expense of other subscribers. As a result, the operator may suffer direct financial losses, while subscribers may receive huge bills for services that they did not actually use. Such situations may occur if IP addresses of devices that send requests to operator's equipment are not verified.

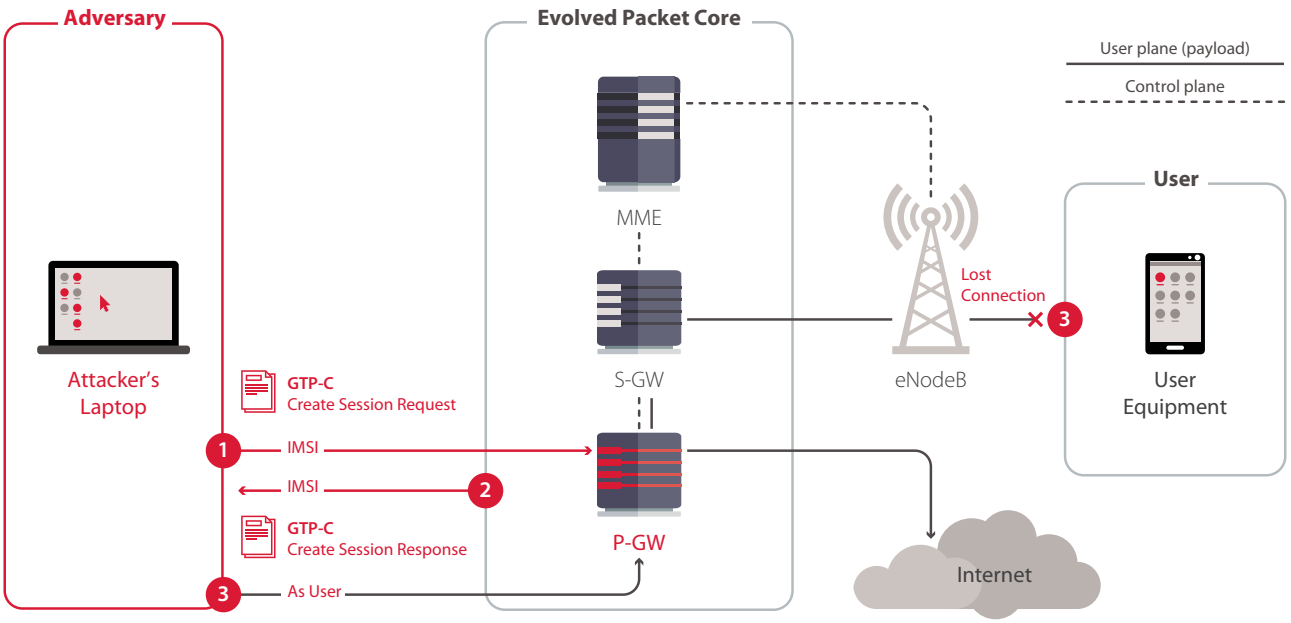

Figure 4. Using services at the expense of the operator or another subscriber by sending a GTP-C request

An attacker can spoof another subscriber's identity to gain unauthorized Internet access by sending a specially generated GTP-C "Create Session Request" service message to the P-GW (Figure 4). If the request contains an IMSI belonging to an actual subscriber, the charging system will charge this subscriber for all traffic used by the attacker. Otherwise, when the IMSI is not assigned to an actual subscriber, data transmission costs will be incurred by the operator (Figure 4).

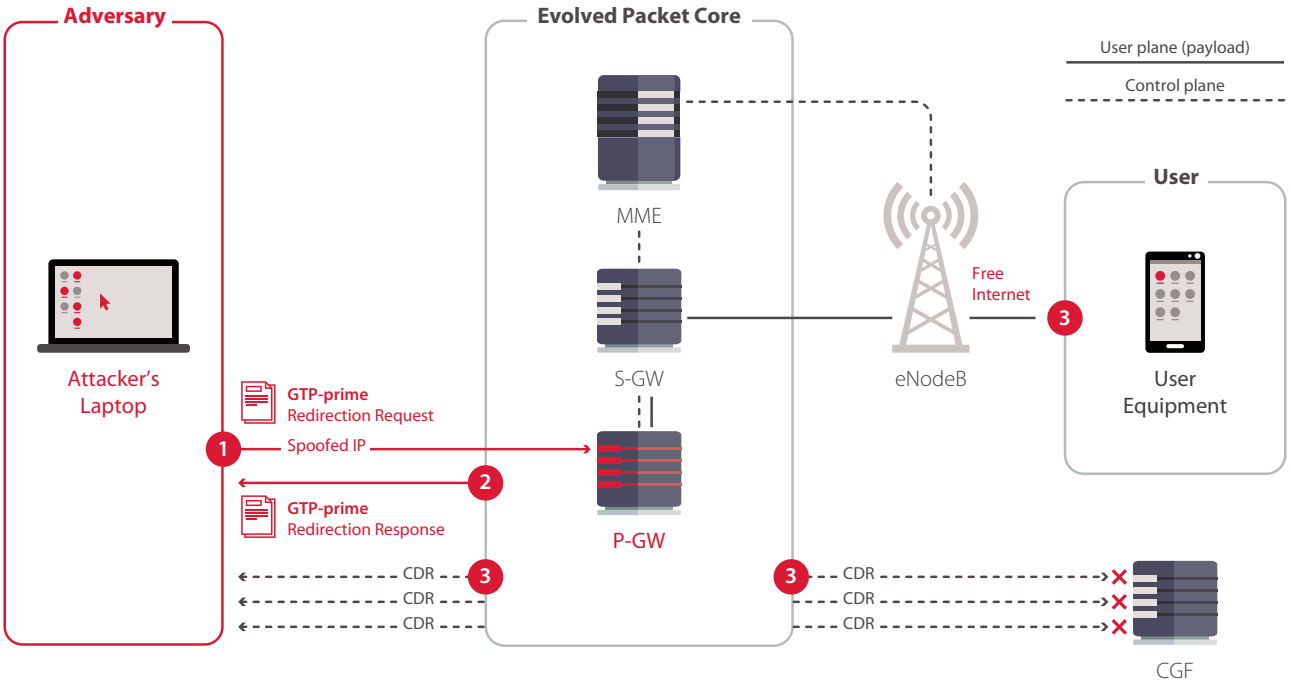

Figure 5. Using the CGF buffer to bypass the CGF

Another variant of this attack (Figure 5) uses the CGF (Charging Gateway Function) failover mechanism. This component is responsible for receiving and verifying detailed data on the service provided—CDR (Charging Data Record)—in the billing system. When the CGF buffer is overflowed or overloaded, data on the service provided can be rejected by a "Redirection Request" message that contains the IP address of a backup gateway. By exploiting this fact, attackers can send such requests to the P-GW indicating their IP addresses as free CGF addresses, which allows bypassing the CGF.

The described attack scenarios can potentially give attackers unauthorized unlimited access to resources, for example to services that are not included in the attackers' rate plan, which will inflict direct financial losses on the mobile operator.

2. Connection hijacking

This type of attack threatens to leak sensitive subscriber data and compromise important resources. The attacker can continue spoofing the subscriber's identity, and when the connection is handed over to the subscriber, the subscriber will be denied further service.

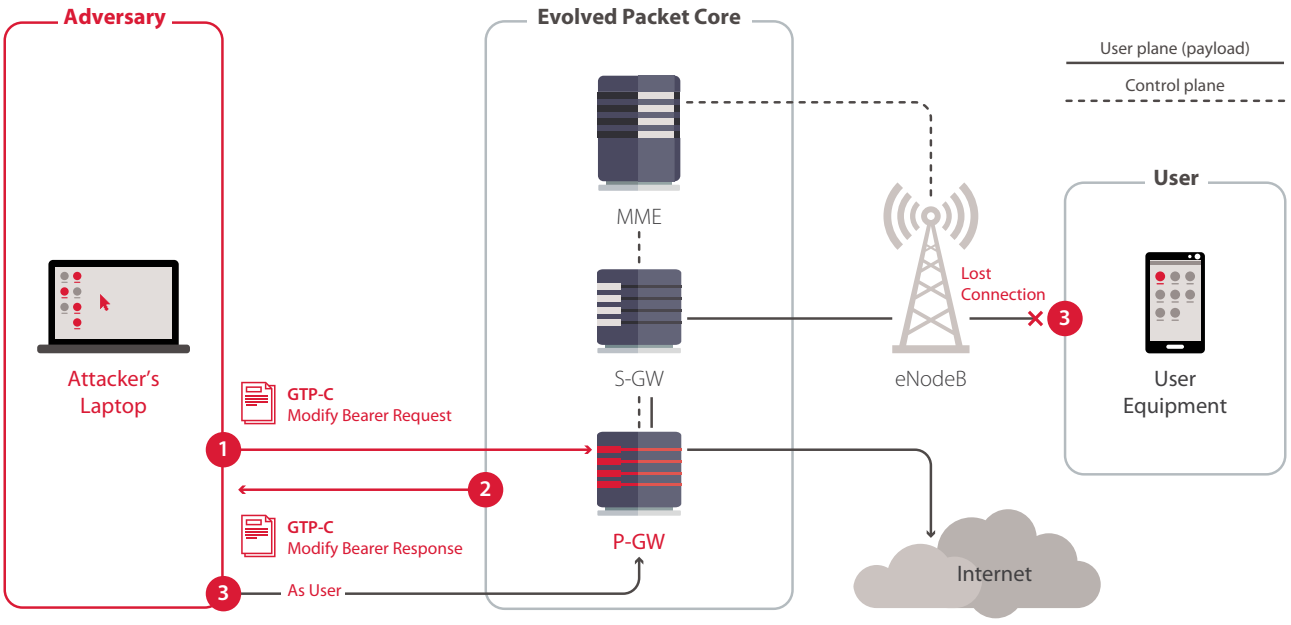

Figure 6. Hijacking the Internet connection by sending a "Modify Bearer Request" message

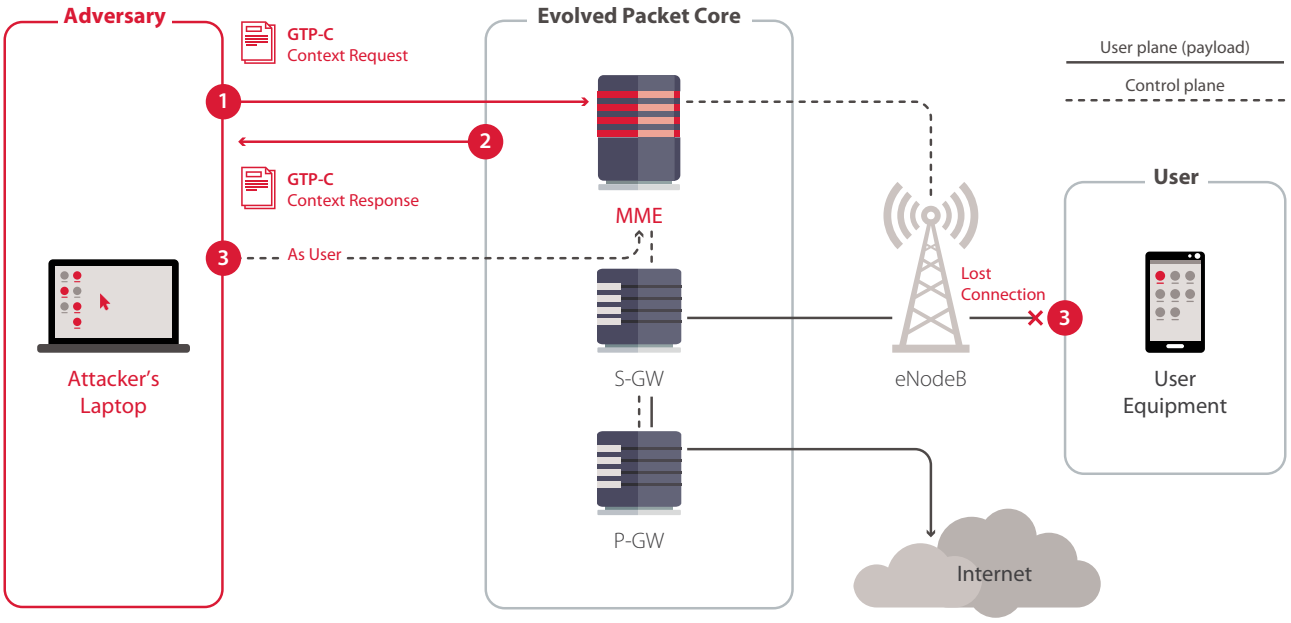

Figure 7. Hijacking the Internet connection by sending a "Context Request" message

The same attack can be conducted on the MME by using a specially generated GTP-C "Context Request" message in which the TEID and TMSI of the subscriber being attacked are specified among other parameters (Figure 7).

The described scenario, which is made possible due to a vulnerability in the GTP protocol and failure to verify the sender's IP addresses, allows the attacker to access the Internet as a subscriber. This method can be used for bypassing lawful interception systems, for example by fugitives hiding from law enforcement agencies.

3. DoS attacks on subscribers

In the EPC, several scenarios for conducting a denial-of-service attack blocking the subscriber's Internet connection are possible. If the connection is lost once, the user can restart the smartphone to restore it. But if the attacker is conducting such an attack continuously, the subscriber will be blocked completely. By bruteforcing TEIDs, the attacker can disconnect multiple users at once. Such actions significantly affect the overall quality of services provided and subscribers' loyalty to the operator.

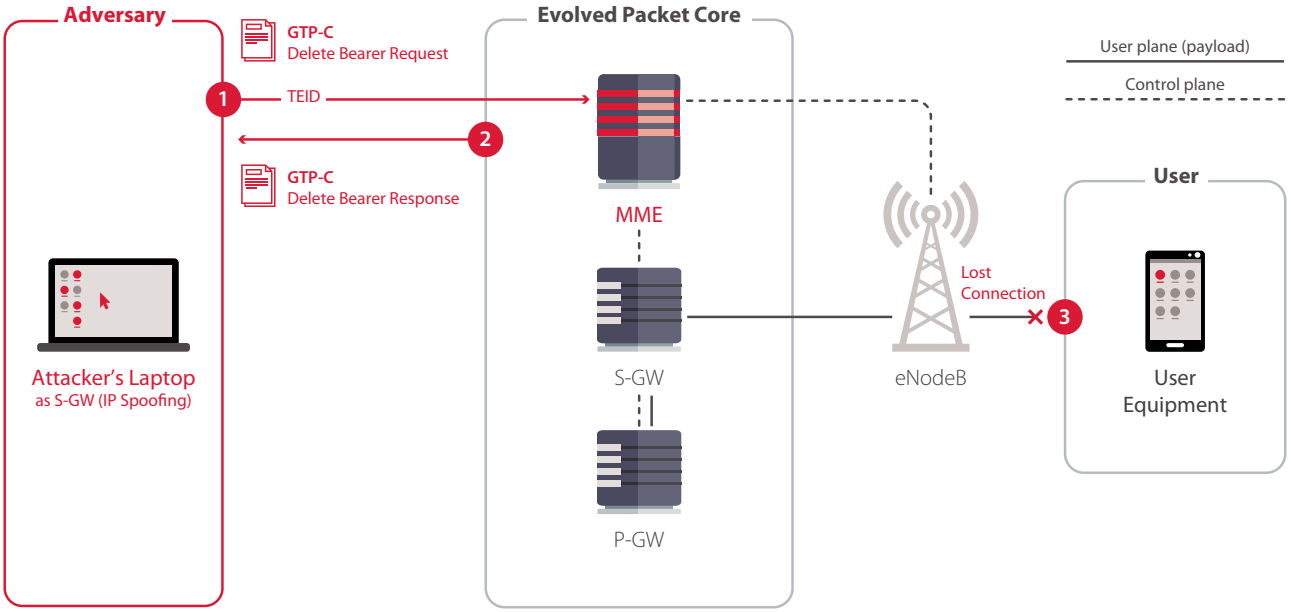

Figure 8. DoS attack on a subscriber via a "Delete Bearer Request" message

This attack (Figure 8) is successful if the sender's address is not verified on the operator's equipment when the attacker sends a GTP-C "Delete Bearer Request" message, posing as the S-GW, to the MME containing the subscriber's TEID; the sender's IP address is replaced with the IP address of the S-GW. After this, the subscriber's device is disconnected until it is reconnected to the network or restarted.

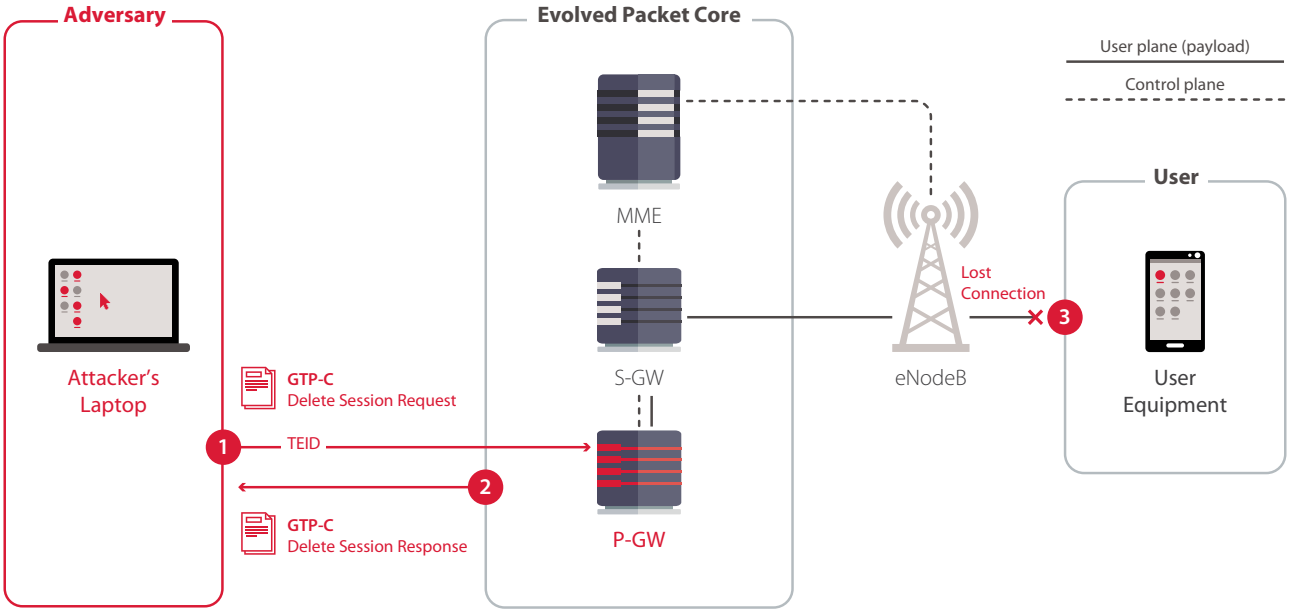

Figure 9. DoS attack on a subscriber via a "Delete Session Request" message

The attacker can also disconnect the subscriber from the Internet by obtaining the TEID of the subscriber's current session and sending a GTP-C "Delete Session Request" message to the P-GW (Figure 9).

4. DoS attacks on the operator's equipment

Manufacturers of telecommunications equipment do not always scrutinize the "worst-case scenarios" of how interfaces and protocols may be abused, preferring to assume that all network elements will comply with standards. Our experience shows that several specially crafted incorrect packets can cause elements of the operator's signaling network to malfunction (Figure 10).

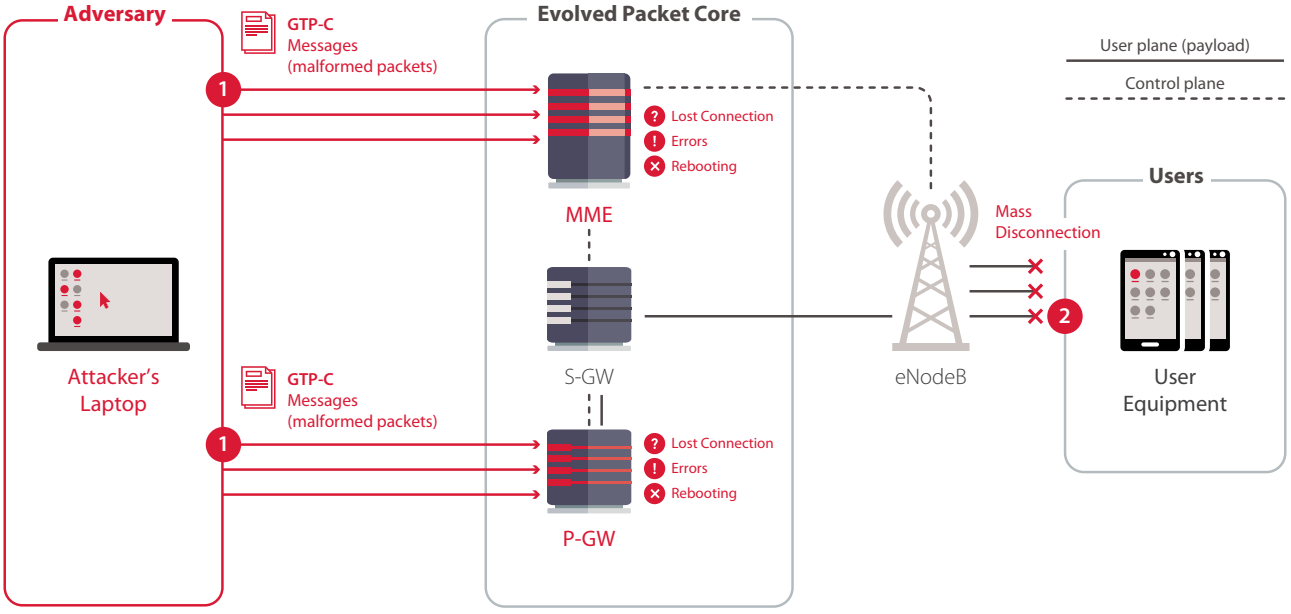

Figure 10. DoS attack on an operator via incorrect packets

Such vulnerabilities must be promptly eliminated in accordance with the recommendations detailed in the Conclusion section of this report. Equipment errors during message processing can lead to network disruptions, degradation of quality, or denial of service for multiple subscribers.

5. Control packets inside a user tunnel: GTP-in-GTP

Another major security problem is caused by GTP-U tunnels, containing user data, that terminate at the P-GW. Only their payload is transmitted to external networks. If an authorized mobile Internet user encapsulates a service packet (GTP-C) as payload in a GTP-U packet, the P-GW may treat this as a control signal packet, instead of sending them along together down the network. Thus, if GTP-in-GTP attacks are not blocked on the network, all attacks described in this report are possible not only from inside the network but also from a subscriber LTE modem or mobile phone (Figure 11).

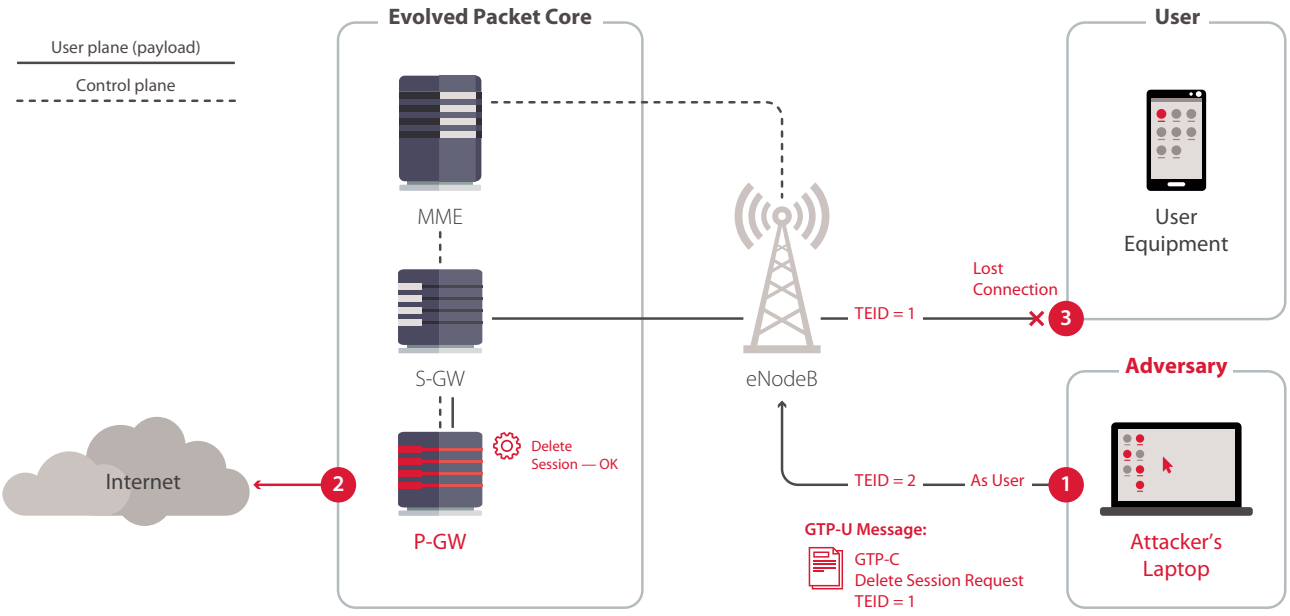

Figure 11. Attacks possible not only from inside a network but also from a mobile phone

For example, a DoS attack on a specific user can be conducted by sending GTP-C "Delete Session Request" subscriber disconnection service messages to the P-GW, posing as another user via GTP-U.

CONCLUSION

This report demonstrates the main security threats related to the centerpiece of 4G (LTE) networks, the EPC. With interfaces available to attackers from external networks and manufacturers of telecommunications equipment paying little attention to security, mobile operators are poorly prepared for attacks.

The simplified packet core structure and the transition to the All IP Network model enable potential attackers to use a wide range of already-existing tools to conduct attacks such as identity spoofing for fraudulent purposes, interception of text and email messages, eavesdropping on VoLTE calls, and blocking connections.

Some of these threats are caused by deficiencies in operator's equipment configuration, for example failure to verify the sender's IP address and device port. Attackers can therefore spoof the sender's address or create, intercept, and terminate sessions as another subscriber. Other problems arise from the lack of encryption on device interfaces, which enables attackers to exploit the operator's service information.

It is necessary to keep in mind that lax or absent protection mechanisms are a deliberate choice made by industry, who shortchanged security in favor of reducing network delays and increasing data processing speeds. In today's competitive telecom market, mobile operators are forced to immediately absorb new technologies with minimal consideration of subscribers' security. Attempts to add protection mechanisms, such as the Security Gateway, can only add to delays.

However, with the rise of the Internet of Things (IoT) and the Industrial Internet of Things (IIoT), the security of 4G networks will rise higher on the agenda in coming years than ever before. For example, as estimated by the Global Agenda Council for the Future of Software and Society and announced during the World Economic Forum, by 2026 10 percent of all cars in the world will be self-driving.[5] By this time, the first smart city is expected to appear, with automated management of energy, logistics, and traffic, and AI will be involved in making business decisions at the board level. Exploitation of poorly protected communication channels and malicious disruptions in the operation of such systems can lead to serious consequences for city infrastructure, disasters at industrial facilities, and transport disruptions. That is why the first mobile operators to build a secure ecosystem to connect IoT infrastructure will gain a strong competitive advantage.

Mobile operators must ensure protection of communications and equipment from unauthorized access, and regularly assess the security of their infrastructure, especially in and around interconnects with other operators (GRX, in the case of the EPC). To develop adequate measures, operators should start by assessing the security of the packet core and signaling network equipment. It is necessary to analyze the potential attack vectors available to attackers and assess the risks associated with them. Based on this testing, recommendations can include measures at both the level of equipment (to prevent physical access to hardware and communications) and software (logical security measures to protect data from unauthorized access, for example using IPSec).

Any changes to the quantity or quality of equipment affect network configuration, and therefore can degrade network security. Keeping security settings up to date requires special tools for monitoring, analyzing, and filtering messages that cross network boundaries.

Implementation of these measures is a network-by-network task. Responsibility for the completeness and promptness of security measures lies entirely with individual mobile operators and the contractors maintaining networks on their behalf.

5 www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com