NEXT-GENERATION NETWORKS, NEXT-LEVEL CYBERSECURITY PROBLEMS

2017

POSITIVE TECHNOLOGIES

Contents

Introduction and methodology

In preparation for the brave new world of 5G and IoT, the last few years have seen operators make significant CapEx investments in their next-generation networks. However, despite spending billions upgrading from a protocol developed in the 70's (ss7) to Diameter (4G and 5G), flaws exist that allow an attacker to carry out eavesdropping, tracking, fraud, theft, and worse.

This research report draws on the experience we have gained whilst working on real mobile network infrastructure to outline how Diameter is equally vulnerable to many of the attacks that plagued its predecessor for years. More pressingly, we highlight techniques that could allow DoS attacks directly on operator equipment, which could cause wide-scale network outages. This is particularly important, given the central role such equipment is set to play in enabling the connection of everything—from cars to industrial devices.

On every one of the Diameter-based 4G networks on which Positive Technologies performed security audits in 2016, we found vulnerabilities that could enable attacks for locating users, intercepting SMS messages, instigating denial of service, and performing other illegitimate actions. The attack techniques outlined in this report are either ones which we have observed taking place, or have discovered are possible in the course of testing on the networks we work with.

It's not just new attacks that work, either. Almost all users of 4G networks are, perhaps without even knowing it, users of previous-generation networks as well. While a mobile operator can provide only data transfer over LTE, for example, making phone calls and exchanging SMS messages requires technology for temporarily falling back to older networks (circuit-switched fallback). Therefore, 4G subscribers are still susceptible to the threats associated with previous-generation networks.[1]

Attack scenarios for Diameter-based networks

"Diameter" itself is a bit of a play on words—judging by the name, Diameter should be twice the protocol of its predecessor, RADIUS. Although the standard for the protocol originally envisioned both network-level and transport-level security, most operators do a poor job of implementing these measures. Moreover, these measures by themselves are often insufficient for blocking the actions of a range of actors: unscrupulous employees, intelligence agencies and companies, and groups that stay within the formal limits of the law, while using their knowledge and access to signaling systems to perform surveillance and cyberespionage.

As with SS7, the attacks outlined rely on an attacker having access to the Diameter network. This deep level access to the underlying telecoms interconnect has been, in our opinion, responsible for a false sense of security to operators the world over for many years. As with SS7 networks, there are a number of well-established ways for gaining access to the underlying mobile protocol. These range from corrupt employees in lesser regulated countries to access offered anonymously on the dark web and even legitimate access offered by companies which is then abused. With the introduction of Diameter, a purely IP-based protocol, the possibility of an intruder gaining access through direct hacking is also now an increased risk. More software and more connectivity only ever means more attack vectors.

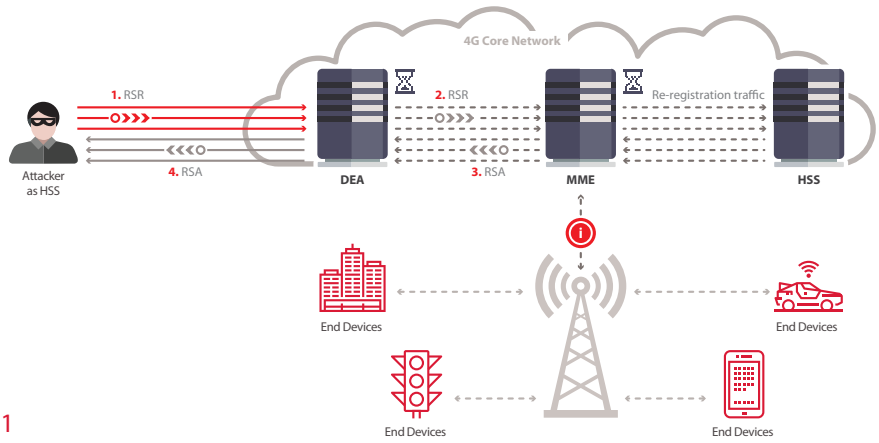
[1] https://www.ptsecurity.com/upload/corporate/ww-en/analytics/SS7-Vulnerabilities-2016-eng.pdf

New equipment, new attack vectors

The equipment itself used to enable the next generation of Diameter networks provides an attacker with opportunities to create widespread downtime for any device connected to it. Considering the push for such networks to support the burgeoning 'internet of things' market, and with LTE-M and 5G being integrated into everyday devices of the future, objects in the 'smart cities' of tomorrow could become a victim of attacks, which could realistically paralyze entire cities. For example, if the notion of fleets of connected cars takes off as the industry is hoping, a city-wide DoS attack on the supporting Diameter network could, at best, cause mass inconvenience. Telecom operators will take the blame for the consequences in such a scenario.

The network equipment used to build Diameter is susceptible to Denial of Service (DoS) and other attacks typical of IP networks. Based on the security audits performed in 2016 by Positive Technologies on Diameter signaling networks, one out of every two components on the networks tested is susceptible, being just one wrong byte away from being taken offline by a well-aimed packet[2].

Several techniques are possible for performing DoS attacks against Diameter networks. The simplest one is to send many CER (Capabilities-Exchange-Request) connection requests in order to deplete the capacity of a network node.



Pic. 1

Another way is to send, as HSS, a large number of RSR (Reset-Request) messages to an MME that services subscribers from a known range of subscriber IMSIs (Pic. 1). A large number of such messages could snowball into an enormous amount of signal traffic between the MME and actual HSS, degrading the performance of the HSS and overall network.

Other causes of a spontaneous increase in signal traffic could be simpler, for example, a poorly designed or maliciously altered app on IoT or user devices.

Such flaws may be down to the fact that, since the mobile sector has historically been a relatively closed market, the equipment deployed often does not undergo full security testing. As a result, it is open to the possibility of vulnerabilities.

Overloading and bringing Diameter servers offline can also have consequences beyond the direct impact of taking down connected devices, such as:

1. Customer churn—both individual subscribers, but also the manufacturers who pay networks to connect their devices wholesale
2. The relative ease with which an attacker can hide, means attribution is difficult
3. Legal action against the operator from the impact of failing to secure their network

[2] Based on data on less than 10 projects

These consequences, beyond compromising a company's reputation as a reliable telecom operator, include direct financial losses. Given the above facts, the Diameter protocol is not adequately protected from overloads.

Attacks on subscribers using Diameter

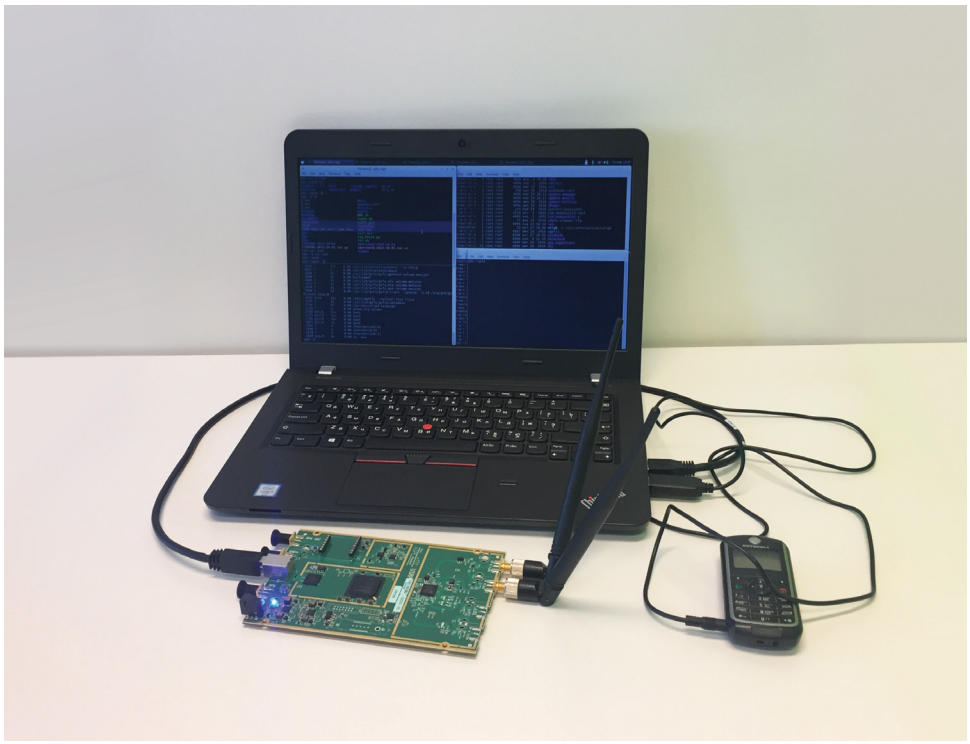
Intelligence gathering

Before performing virtually any kind of attack, the attacker must first perform reconnaissance to learn about the targeted network and subscriber. Since usually the attacker poses as a roaming partner, the following information is necessary before attacking:

1. IP addresses of the Diameter edge nodes to be attacked, including Diameter Edge Agents (DEA) and Diameter Routing Agents (DRA), together with their identifying information.
2. Identifying information for the network nodes of other operators with which the attacked operator may interact, in order to disguise itself as a legitimate roaming partner.

An attack directed at a specific subscriber generally requires knowing their International Mobile Subscriber Identity (IMSI). The IMSI is an identifier unique to a specific mobile subscriber worldwide. With the IMSI, it is possible to determine in which country and on which operator's network the subscriber is located.

There are several ways of learning a subscriber's IMSI. The most common way is to leverage vulnerabilities in the SS7 signaling protocol. As noted above, this attack is possible because for various reasons virtually all 4G subscribers are also de facto subscribers of previous-generation networks.

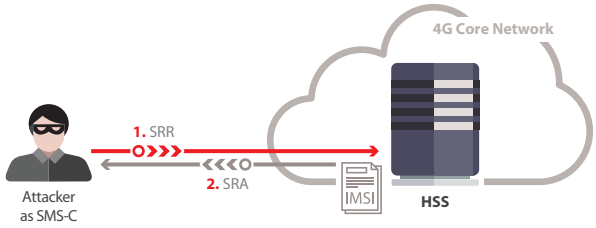


Pic. 2

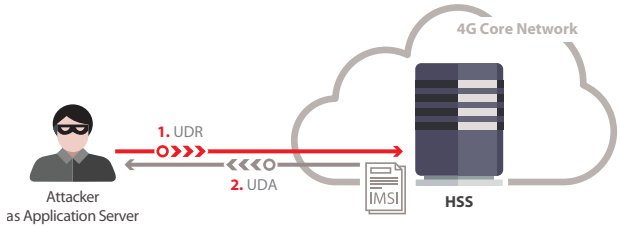
An IMSI can also be obtained using special equipment (IMSI catchers). This device spoofs a mobile base station and allows the attacker to intercept information about the users of the mobile phone connected to the base station, including their IMSI identifiers (Pic. 2).

Some operators allow subscribers to make calls via Wi-Fi networks[3], in which case any Wi-Fi hotspot owner can use the hotspot as a cheap IMSI catcher. In addition, there are now free and paid[4] services online for using a subscriber's phone number to look up their IMSI.

Pic. 3



Pic. 4

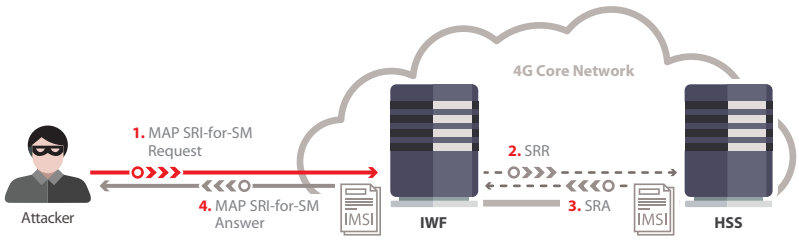


There are also ways of getting a subscriber's IMSI via a Diameter network. This requires the mobile subscriber's number (MSISDN) and address of an edge node on the Diameter signaling network.

One attack scenario using a known vulnerability is as follows. An attacker, acting as SMS center (SMS-C), sends a specially crafted SSR (Send-Routing-Info-for-SM-Request) message to the Home Subscriber Server (HSS). If successful, the attacker receives the IMSI of the relevant user in response (Pic. 3).

In a second scenario, with a new vulnerability discovered in the course of our recent work, the attacker can pose as an application server and send a specially crafted UDR (User-Data-Request) message to the HSS. The data received in response from the HSS will contain the IMSI of the relevant user (Pic. 4).

Pic. 5



Another way of forcing IMSI disclosure is to attack the Interworking Function (IWF) node responsible for compatibility between the Diameter network and the networks of previous generations. In this case, an SRI4SM request from MAP SS7 is translated into the equivalent Diameter SRR request. In response, the attacker receives the requested IMSI (Pic. 5).

Once the attacker obtains a subscriber's IMSI plus addresses of the mobile network nodes servicing the subscriber, they have the relevant targeting information they need to launch the attacks outlined below.

[3] WiFi-Based IMSI Catcher – https://www.blackhat.com/docs/eu-16/materials/eu-16-OHanlon-WiFi-IMSI-Catcher.pdf
[4] HLR Number Lookup – http://www.txtnation.com/mobile-messaging/hlr-number-lookup/

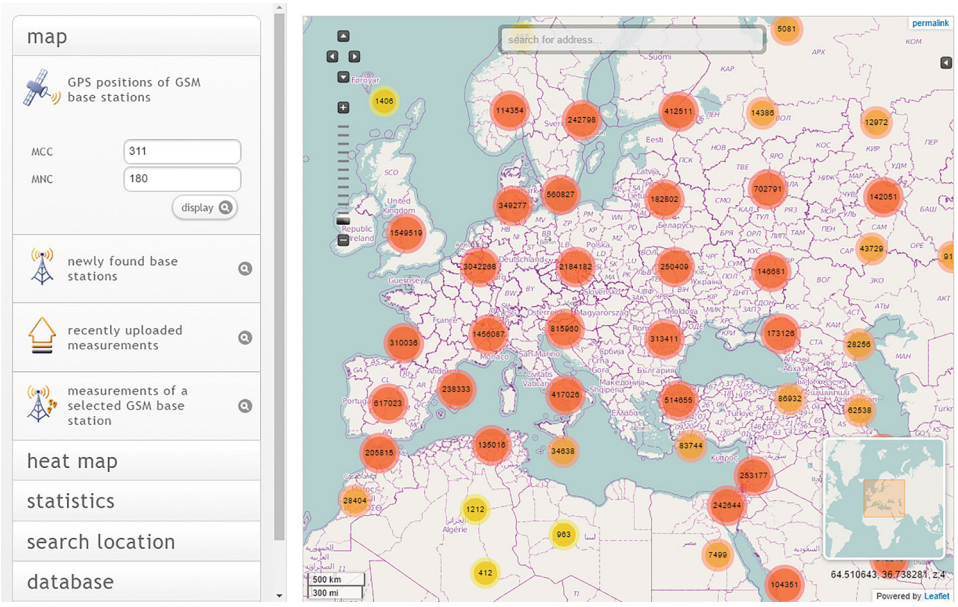
Same old attacks, just on a new protocol

As previously mentioned, the shift to Diameter could have heralded a new level of security for mobile subscribers. However, our experience with numerous networks shows that Diameter is still unfortunately open to the same types of attack that the predecessor SS7 was, if somewhat altered to take into account some technical differences. The types of attack this allows on subscribers are highlighted below.

1. Subscriber location discovery

Perhaps the "classic" attack on Diameter networks is the one for determining a subscriber's current location.

Attackers could use this technique to discover compromising information about a politician or business leader, making public where, when, and with whom the subscriber has met. In such cases, forensic investigation will show that the leaked information was obtained from the telecom operator.



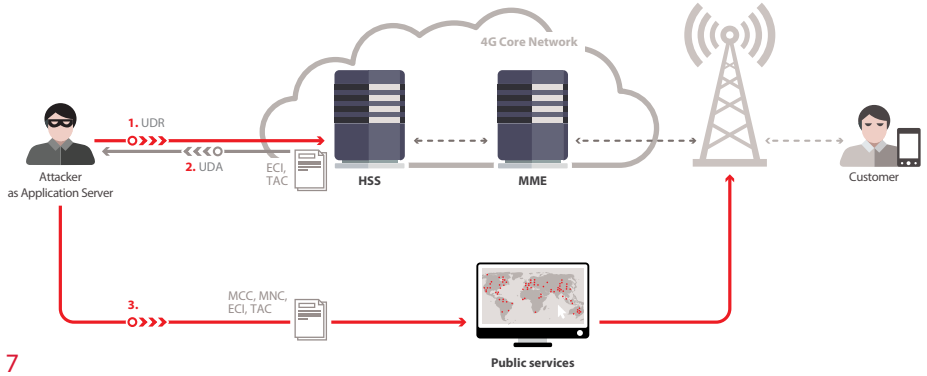
Pic. 6

The main goal of the attacker is to get the cell identifiers (CID or ECI) and location codes (TAC and LAC). With this data, services such as Google, Mozilla Location Services, and OpenCellId offer ways of approximating a user's location (Pic. 6). Any internet site can use the APIs for those services to request the location coordinates of the user or base station servicing the user, and even show the results on a map[5, 6].

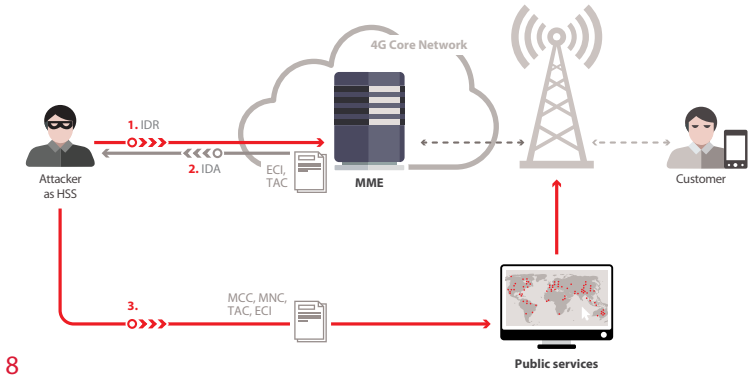
Several methods exist for obtaining information about a subscriber's location. The following scenarios outline these.

In the first scenario, the attacker acts as an application server and sends a specially crafted UDR message to an HSS (Pic. 7). If the request is accepted, the response contains the ECI cell identifier and TAC location code. This information is sufficient to calculate the user's location to within several hundred meters with the help of the publicly available services mentioned above. Then, using any online map service[7], these coordinates can be matched to a point on the map.

[5] Find GSM base station cell id coordinates – http://cellidfinder.com/
[6] CellTower Locator – http://www.cell2gps.com/
[7] Google Maps https://www.google.co.uk/maps



Pic. 7



Pic. 8

In another approach, the attacker, poses as an HSS and sends IDR (Insert-Subscriber-Data-Request) messages to the Mobility Management Entity (MME), to obtain data to determine the cell and location codes (Pic. 8). Then, as previously described, the attacker can input this into any of a number of websites to discern location.

In conclusion, determining a user's location, with all its attendant opportunities for surveillance and blackmail, is trivial for any attacker who has access to a Diameter-based signaling network. Moreover, the subscriber has no way of knowing their location and movements have been compromised.

2. Interception of SMS messages

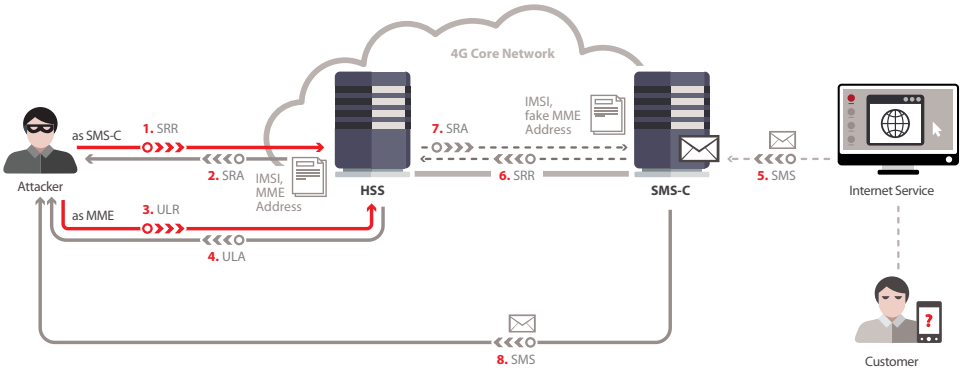
This attack is particularly dangerous for any online service, which relies on SMS-based two-factor authentication, such as online banking sites. With this vulnerability, an attacker can steal money straight from a bank account, with the organization believing the transaction to be legitimately authorized. This makes it practically impossible for the user to claim fraud and dispute the transaction.

Interception of SMS messages on a Diameter network is similar to the equivalent attack on SS7 networks, and can be carried out using the following approach:

Armed with the MSISDN, the attacker acts as an SMS center and sends an SRR request to an HSS, receiving information including the subscriber's IMSI and the MME currently servicing them.

Then, in the role of MME, the attacker sends a ULR (Update-Location-Request) request to the HSS and, if successful, receives the corresponding ULA (Update-Location-Answer) response. From that point on, the HSS will store updated information that the attacked subscriber is serviced by that (fake) MME and associated with the attacker's SMS center.

One important aspect of the Diameter protocol facilitates this attack: the response to a request is always returned to the originating node, regardless of any information indicated in the Origin-Host pair.



Pic. 9

The attacker can then request a password reset by SMS (for a social network, chat program, etc.) or confirm an online banking transfer from the subscriber's account.

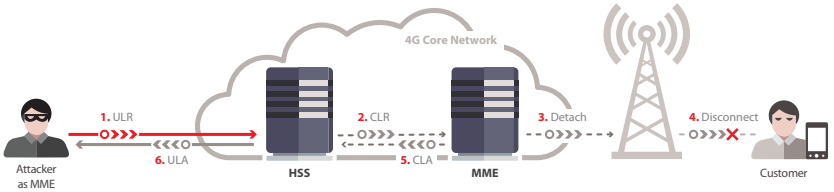
The operator's SMS center then requests information from the HSS about the MME that is servicing the attacked subscriber, which replies that the user is being serviced by the fake MME and SMS center (Pic. 9). From that point forward, all SMS messages with confidential user information are sent to the fake SMS center controlled by the attacker.

With confirmation codes from these SMS messages, the attacker can then obtain full access to online services, change passwords, and have full control over the user's accounts. In the case of a bank account, an attacker can control the user's bank account and transfer money.

Subscribers will only know they have been attacked when they see the impact of the attacker's actions, such as money being stolen, unauthorized posts to social media accounts, or other unauthorized account access.

3. DoS attack against a subscriber

Several key aspects of implementation of the Diameter protocol make it easy to perform simple but effective denial-of-service (DoS) attacks against one or numerous subscribers. On a small scale, targeted downtime can be forced upon unsuspecting high value targets. On a larger scale, large groups of individuals can be denied access to their mobile devices.



Pic. 10

To carry out such attacks on a Diameter network, the attacker must force an HSS to think that it is servicing (as MME) the subscriber with a given IMSI (Pic. 10). Then the HSS initiates the procedures for disconnecting the subscriber from the old MME, after which the user loses his or her connection to the 4G network.

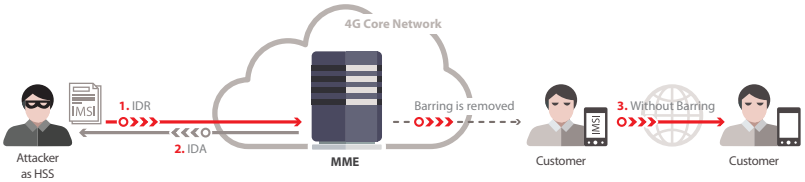
To do so, the attacker (acting as the MME) sends a counterfeit ULR to the HSS requesting an update of the corresponding identification information, and notifies (as itself) that currently the attacker is the MME servicing the given subscriber device. When the HSS updates the database, it sends a CLR (Cancel-Location-Request) message to the genuine MME node that previously serviced the subscriber; then the MME initiates the procedure for disconnecting them from the data network. In addition, if the Diameter protocol is used on the subscriber network for calling (VoLTE) and SMS messaging, these services will become unavailable.

Of course, the user will probably try to reconnect to the network. So the user signs on to the network again by restarting his or her 4G device. However, the attacker can flood the session with fake requests, completely blocking the reconnection attempt and overloading the HSS with junk traffic.

4. Fraud

Diameter networks are also at risk of attacks enabling free access to calls, SMS, and data at the expense of the operator or subscribers, causing them financial loss.

Such attacks require an exceptional degree of knowledge about the internal processes and network of the operator, especially when attempting to change the rules applied to a particular subscriber. However, some attacks require rather less information: the subscriber's IMSI and addresses of several nodes on the Diameter network are all that is required. This includes redirecting billing-related traffic to a non-existent or hacked billing server, as well as disabling prohibitions applied to some or all services (barring).



Pic. 11

Barring can be removed by sending a specially crafted IDR message to an MME (Pic. 11). The attacker acts as HSS. Information in the IDR about barring is removed, enabling the subscriber with the indicated IMSI or MSISDN to potentially obtain unlimited access to resources that are not usually provided to the subscriber (such as services not available under the subscriber's rate plan).

Conclusion

Diameter is the chosen bedrock for the brave new connected world. However, it appears similar vulnerabilities, which have existed in SS7 for many years, still provide attackers with too many opportunities. Thinking of operators in their current terms, as a way of connecting a small personal computer, this means subscriber fraud, and theft of data, and other ongoing criminal operations will continue. However, fast forward a few years to a world where operators connect and service all the moving parts in urban areas, and it opens up a new level of problems for the mobile industry, as well as the people living in these connected areas. Steps must be taken to safeguard against potential doomsday scenarios.

Such frightening consequences are only the tip of the iceberg. Configuration errors and vulnerabilities in networks allow a creative attacker free reign to experiment with what is possible from compromising the services and equipment on the signaling networks of telecom operators.

To minimize risk, we urge mobile operators to transition into an increasingly IP-based world in a way which is fitting of the medium. This means regularly performing security testing of their signaling network in a way similar to that of IT networks the world over. Since introduction of new equipment or configuration changes to existing equipment may affect network security, this testing should take place at least quarterly.

To mitigate these threats and keep security settings up to date, telecom operators must also consistently monitor, test, and filter the messages that cross their network boundaries. These tasks are ably handled by specially designed attack detection systems and equipment with firewall functionality for signaling traffic.

Key abbreviations

DEA—Diameter Edge Agent. Usually on the edge of the operator's signaling network, acting as a proxy agent for signal traffic from the networks of other operators.

DRA—Diameter Routing Agent. Routes Diameter traffic.

HSS—Home Subscriber Server. One of the most important elements on LTE network infrastructure. Stores user information and information about subscriber actions.

IMSI—International Mobile Subscriber Identity. Used to uniquely identify each mobile subscriber worldwide.

IWF—Interworking Function. Converts the MAP SS7 protocol to Diameter for compatibility with previous-generation networks.

MME—Mobility Management Entity. Enables switching between base stations, roaming, and authentication of user devices in cooperation with the HSS. Also responsible for selection of the S-GW gateway for a user.

MSISDN—Mobile Station ISDN.

S-GW—Serving Gateway. Transfers and processes user data from user devices from/to the operator's base station subsystem.

SMS-C—SMS Service Center. Responsible for text messaging on mobile networks.

SS7—Signaling System 7. Common-channel signaling system used in international and local phone networks worldwide.

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