Diameter Security: An Auditor's Viewpoint

Sergey Mashukov

Positive Technologies, Russia
E-mail: smashukov@ptsecurity.com

Received 8 September 2017;
Accepted 7 November 2017

Abstract

In this paper we share our experience in conducting security audits for several different mobile network operators and discuss the difficulties encountered in the process. We also describe successful attacks performed by us on Diameter equipment in these environments. Some of these attacks have not been published previously.

Keywords: Diameter, Security, 4G.

1 Introduction

Security research clearly shows that SS7 protocols are vulnerable to a plethora of attacks. But what about 4G and other modern mobile networks, which do not use SS7?

Instead, such networks use the Diameter protocol. Diameter is often regarded as a successor to SS7 on all-IP 4G LTE networks, since it now handles most SS7 signaling procedures, including mobility management for roaming.

It should be noted that Diameter was not specifically created for these purposes, but simply chosen as "good enough" during development of 4G standards. As a result, the protocol contains several flaws that attackers may exploit.

Journal of ICT, Vol. 5_1, 53–68.
doi: 10.13052/jicts2245-800X.513

One flaw is the spoofing-friendly nature of the protocol. All responses to a request return by the same path with which the request was received, so an attacker will always receive the results of an attacker-initiated operation, even if the attack involved spoofing a node of another network operator.

Another flaw is a lack of end-to-end authentication, integrity checks, and encryption. Thus, it is not possible to confirm the true sender of a Diameter message, nor that its contents were not modified in transit. As a result, security of the network is largely based on trust between all roaming operators and can be compromised by a single "weak link". This model has come under increased pressure due to the growing number of virtual mobile network operators and lower barriers to entry for attackers on IP-based 4G networks.

Current research on Diameter security shows that it is possible to gather information about subscribers [1–3], locate and track them [1, 2], and perform denial of service (DoS) attacks on them [1, 2].

In this paper we will show which attacks have been successful in our audits of mobile network operators, and also describe some attacks that have not been published previously.

The attacks described here are divided into two groups: protocol attacks and vendor-specific issues. Protocol attacks are generally applicable to any mobile network operator (MNO) and include International Mobile Subscriber Identity (IMSI) retrieval, subscriber DoS, and subscriber location attacks. Vendor-specific issues, on the other hand, are caused by flaws in implementation of the Diameter protocol on a specific vendor node, which enable attackers to cause DoS of network elements and bypass filtering.

In some cases, even protocol attacks may require different combinations of flags and informational elements in a message, or may be unsuccessful entirely, due to different configurations of network equipment or other circumstances. We encountered cases in which the success of an attack depended on the precise order of Attribute–Value Pairs (AVPs) in a message, although normally the order of most AVPs is not fixed.

2 Tools Used

We have written our own scripts to code and decode Diameter messages, as well as emulate Diameter Client and Diameter Server behavior. Development of such tools is not an obstacle for would-be attackers, however, because of the ease of adapting existing open-source or commercial solutions to perform Diameter attacks.

For sending messages via Stream Control Transmission Protocol (SCTP), we used Python bindings to the Linux Kernel SCTP module [4]. Wireshark was used to monitor the results. We also asked MNO personnel to provide us with notifications and alarms from the management interfaces of the nodes under test.

3 Network Configuration

The PC containing our software was connected to the test network on the MNO premises. The node acting as point of entry to the Diameter network (ideally, Diameter Edge Agent [DEA] or Diameter Routing Agent [DRA]) was reconfigured to maintain a Diameter connection with the auditor's PC. This way it is possible to simulate a situation in which an intruder has access to the IPX network.

All tests were performed using test SIM cards or emulated User Equipment.

4 Protocol Issues

4.1 IMSI Retrieval

In essence, an IMSI Retrieval attack consists of obtaining a subscriber's International Mobile Subscriber Identity from a network node with prior knowledge of only the subscriber's mobile phone number (MSISDN). The IMSI is an internal network identifier used in most signaling procedures to identify a subscriber. Knowing this identifier, the attacker can perform other Diameter attacks targeting that subscriber.

4.1.1 IMSI retrieval via Sh User-Data-Request

Please note, that Sh is an internal interface used between services of the same MNO, however, in case no interface separation is done on the network's edge, it is left open for attacks.

We discovered that, in the environments where IMS is used, it is possible to perform IMSI retrieval with an Sh User-Data-Request (UDR) message.

During normal operation, Sh UDR (described in [5]) messages are used by Application Server (AS) to get subscriber-related information from a Home Subscriber Server (HSS). We found that in some cases it is possible to send this type of message from the international interconnect to the HSS.

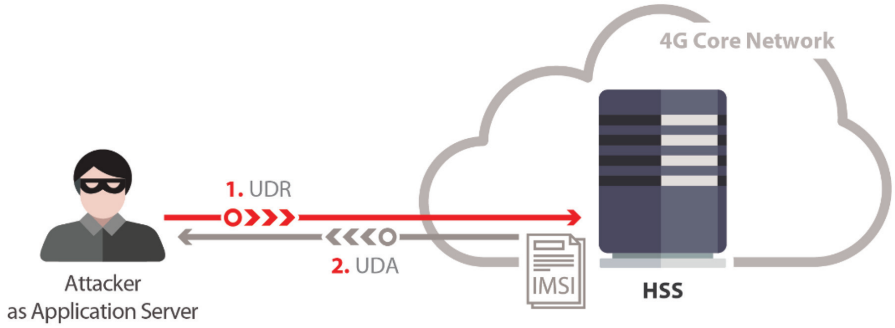

Figure 1 IMSI retrieval via Sh UDR.

To perform the attack, we need to send an Sh UDR message with:

- Destination-Realm AVP containing Host-Id of the MNO's HSS
- Spoofed values for MNO's Application Server in the Origin-Host and Origin-Realm AVPs
- Data-Reference AVP set to 32 (IMSI)
- User-Identity AVP containing MSISDN of the target subscriber

If the message is successfully processed by the HSS, the response is sent back to the attacker instead of the AS, due to the way routing works in Diameter. The response will contain Sh-User-Data AVP, with XML containing the IMSI of the subscriber.

From the intruder point of view, the greatest difficulty in this process is to obtain the AS Diameter Host-Id. However, naming of nodes on an MNO's network is usually predictable. An attacker can send different realm-routed messages to get the values in the Origin-Host AVP from the responses. Because the names of nodes most likely contain repeated elements (e.g., site name prefix or postfix, network element name, and number of this network element in a certain format), it is easy to guess or bruteforce the AS name.

4.2 DoS on Subscriber

This group of attacks pursues the simple goal of disrupting services provided to a subscriber by an MNO. In most cases, a successful attack will disconnect the subscriber from the 4G network or prevent access to 4G Internet.

In this context, "subscriber" refers to a SIM card, meaning that these attacks are also applicable to Internet of Things (IoT) devices.

4.2.1 DoS on subscriber via S6a Insert-Subscriber-Data-Request

We were able to conduct three different versions of a DoS attack on a subscriber by using different fields in S6a Insert-Subscriber-Data-Request (IDR) messages.

Using Access-Restriction-Data AVP. This attack has not been published previously.

To conduct this attack, an S6a IDR message is sent to the Mobility Management Entity (MME) that is currently serving the user, containing:

- MME Host-Id in Destination-Host AVP
- IMSI of the target
- Subscription-Data AVP containing Access-Restriction-Data AVP with value 127

Access-Restriction-Data AVP is of type Unsigned32 and, according to [6], contains a bit mask:

Table 1 Access-Restriction-Data AVP values

Bit	Description
0	UTRAN Not Allowed
1	GERAN Not Allowed
2	GAN Not Allowed
3	I-HSPA-Evolution Not Allowed
4	WB-E-UTRAN Not Allowed
5	HO-To-Non-3GPP-Access Not Allowed
6	NB-IoT Not Allowed

Thus, by setting all flags to 1, it is possible to restrict usage of all radio access technologies.

Changing APN Configuration for the Subscriber. This attack has not been published previously. Somewhat similar attack was described for SS7 earlier in [7].

To conduct this attack, an S6a IDR message is sent to the MME that is currently serving the user, containing:

- MME Host-Id in Destination-Host AVP
- IMSI of the target
- APN-Configuration-Profile AVP containing:
  - Correct Context-Identifier AVP value
  - APN-Configuration AVP with wrong APN name inside of Service-Selection AVP

- All-APN-Configurations-Included-Indicator AVP set to 1 (MODIFIED/ADDED_APN_CONFIGURATIONS_INCLUDED)

Because the Context-Identifier value of the current APN-Configuration is not known to the intruder, the intruder must bruteforce through all possible values of this AVP (type is Unsigned32). If the attack is successful, the node should answer all subsequent IDR requests for the same user with Experimental-Result-Code DIAMETER_ERROR_USER_UNKNOWN (5001).

Note that according to [6], if interworking with MAP is needed, the Context-Identifier will be between 1 and 50.

Using Operator-Determined-Barring AVP. This attack has been previously described in [1].

To conduct this attack, an S6a IDR message is sent to the MME that is currently serving the user, containing:

- MME Host-Id in Destination-Host AVP
- IMSI of the target
- Subscription-Data AVP containing:
  - Operator-Determined-Barring AVP with first bit set to 1
  - Subscriber-Status AVP set to 1 (OPERATOR_DETERMINED_BARRING)

Operator-Determined-Barring AVP is of type Unsigned32 and, according to [6], contains a bit mask:

Table 2 Operator-Determined-Barring AVP values

Bit	Description
0	All Packet Oriented Services Barred
1	Roamer Access HPLMN-AP Barred
2	Roamer Access to VPLMN-AP Barred
3	Barring of all outgoing calls
4	Barring of all outgoing international calls
5	Barring of all outgoing international calls except those directed to the home PLMN country
6	Barring of all outgoing inter-zonal calls
7	Barring of all outgoing inter-zonal calls except those directed to the home PLMN country
8	Barring of all outgoing international calls except those directed to the home PLMN country and Barring of all outgoing inter-zonal calls

Thus, setting all first bits to 1, it is possible to bar all packet-oriented services, which results in subscriber DoS on a VoLTE network.

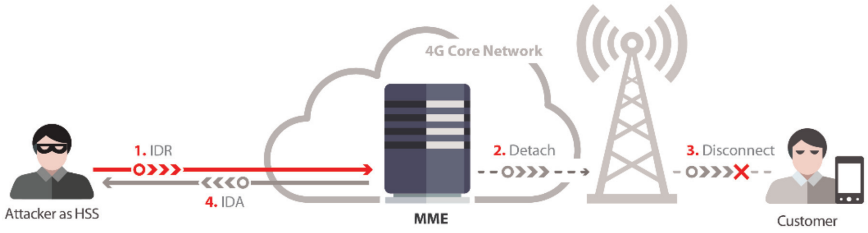

Figure 2 DoS on subscriber via S6a IDR.

4.2.2 DoS on subscriber via S6a Cancel-Location-Request

This attack has been previously described in [1, 2].

To conduct this attack, an S6a Cancel-Location-Request (CLR) message is sent to the MME that is currently serving the user, containing the IMSI of the target.

The MME interprets this as a message from the legitimate HSS, which results in disconnection from the network.

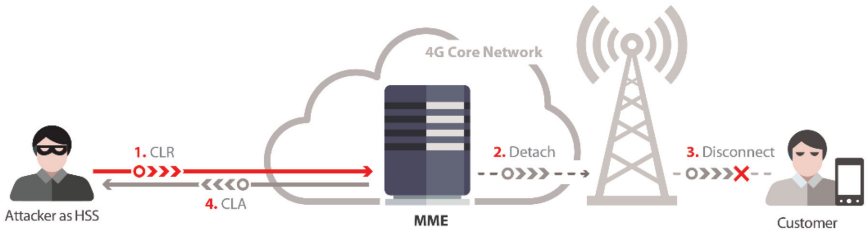

Figure 3 DoS on subscriber via S6a CLR.

4.2.3 DoS on subscriber via S6a Update-Location-Request

This attack has been previously described in [1, 2].

To conduct this attack, an S6a Update-Location-Request (ULR) message is sent to the MNO's HSS (realm routing may be used), containing:

- IMSI of the target
- Destination-Realm should contain MNO's HSS realm

The HSS interprets this as a switch over to a new MME due to change of the user's location and sends S6a CLR to the MME that is currently serving the user, which results in disconnection from the network and overwrites the MME name in the database with the value from Origin-Host AVP.

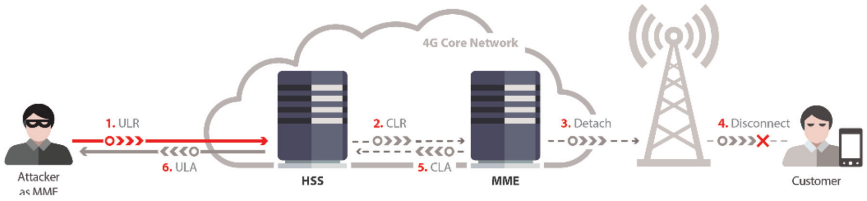

Figure 4 DoS on subscriber via S6a ULR.

4.2.4 DoS on subscriber via S6a Delete-Subscriber Data-Request

To conduct this attack, an S6a Delete-Subscriber Data-Request (DSR) message should be sent to the MME that is currently serving the user, containing:

- IMSI of the target
- Correct Context-Identifier AVP value

It appears that in some cases such a message triggers deletion of all subscriber-related data on the MME.

Because the Context-Identifier value of the current APN-Configuration is not known to the intruder, the intruder must bruteforce through all possible values of this AVP (type is Unsigned32). If the attack is successful, the node will answer all subsequent DSR requests for the same user with Experimental-Result-Code DIAMETER_ERROR_USER_UNKNOWN (5001).

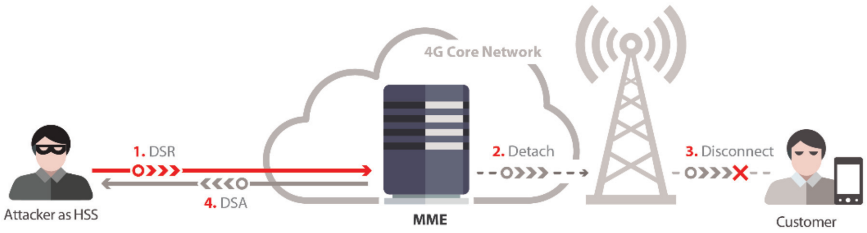

Figure 5 DoS on subscriber via S6a DSR.

4.2.5 DoS on subscriber via S6a Purge-UE-Request

This attack has been previously described in [2].

To conduct this attack, an S6a Purge-UE-Request (PUR) message is sent to an MNO's HSS (realm routing may be used), containing:

- IMSI of the target
- Origin-Host should contain Host-Id of MME currently serving the subscriber

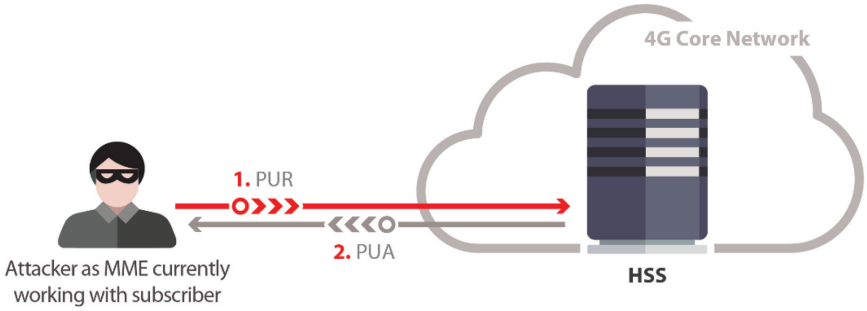

Figure 6 DoS on subscriber via S6a PUR.

The HSS interprets this as an indication of user inactivity from the MME, meaning that the current MME is no longer serving the user. As a result, the MME name is removed from the database and incoming SMS and VoLTE calls cannot be routed to the subscriber.

4.3 Location Tracking

All location tracking attacks below use the same concept as SS7 location tracking attacks. The attacker sends a request for the current cell-id and tracking area of the subscriber and receives information in the response. Then this information, together with the MCC and MNC of the subscriber's current network, is used to obtain the location of the subscriber with the help of cell-id databases publicly available online. Repeating these actions allows for tracking the subscriber over time.

4.3.1 Location tracking via S6a Insert-Subscriber-Data-Request

This attack has been previously described in [1, 2].

To conduct this attack, an S6a IDR message is sent to the MME that is currently serving the user, containing:

- IMSI of the target
- Empty Subscription-Data AVP
- IDR-Flags AVP set to 0xbf

IDR-Flags AVP is of type Unsigned32 and, according to [6], it contains a bit mask:

Table 3 IDR-Flags AVP value

Bit	Name
0	UE Reachability Request
1	T-ADS Data Request
2	EPS User State Request
3	EPS Location Information Request
4	Current Location Request
5	Local Time Zone Request
6	Remove SMS Registration
7	RAT-Type Requested
8	P-CSCF Restoration Request

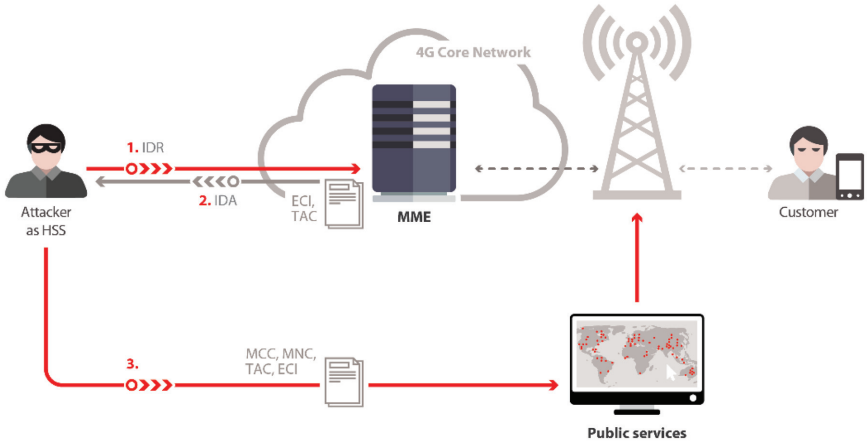

Figure 7 Location tracking via S6a IDR.

If the "EPS Location Information Request," "Current Location Request," and "UE Reachability Request" bits are set, User equipment (UE) will be paged and the received information will be sent by the MME in the IDA inside of EPS-Location-Information AVP. In the case of 4G, E-UTRAN-Cell-Global-Identity and Tracking-Area-Identity AVPs allow getting the location of a mobile device via public services.

4.3.2 Location tracking via Sh User-Data-Request

This attack has been previously described in [2].

To conduct this attack, a Sh UDR message is sent to an MNO's HSS (realm routing may be used), containing:

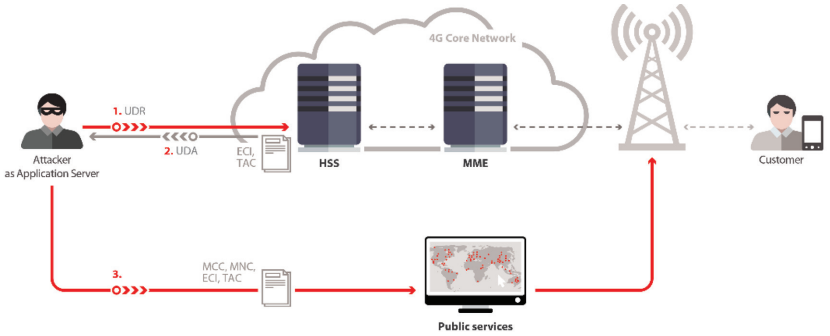

Figure 8 Location tracking via Sh UDR.

- Destination-Realm AVP containing Host-Id of MNO's HSS
- Spoofed values for MNO's Application Server in the Origin-Host and Origin-Realm AVPs
- Data-Reference AVP set to 14 (LocationInformation)
- User-Identity AVP containing MSISDN of the target subscriber
- Requested-Domain AVP set to 1 (PS-Domain)
- Current-Location AVP set to 1 (InitiateActiveLocationRetrieval)
- Requested-Nodes AVP set to 1 (MME)

As a result, the HSS sends IDR to the MME and then answers with the requested information in UDA in Sh-User-Data AVP. The response contains E_UTRANCellGlobalId, TrackingAreaId, MMEName, CurrentLocationRetrieved, and AgeOfLocationInformation. This information is enough to get the device location using public services.

5 Vendor-Specific Issues

5.1 No Filtering Based on Advertised Application Ids on DEA

We found that some DEAs advertise support only for a certain Diameter interface that is used for interconnection, but they still freely route messages from unsupported interfaces. For example, if support only for S6a is advertised for the connection, it is still possible to reach nodes inside of the MNO's network using Sh and conduct successful attacks using the same connection.

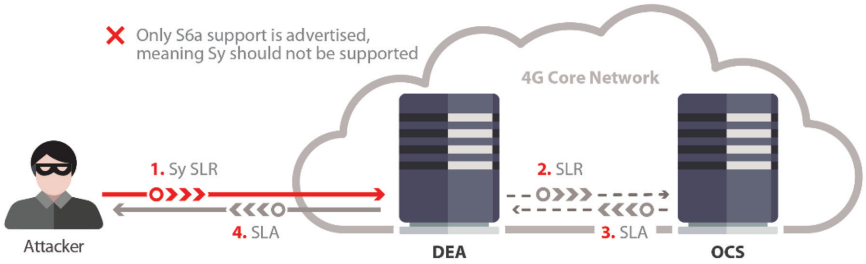

Figure 9 No filtering based on advertised Application Ids on DEA.

5.2 Wrong Handling of Optional Fields in AVP Header on Some MME Nodes

It is possible to cause reboot of MME nodes of a certain vendor by continuously sending the same message with one bit flipped in the header of an AVP.

This bit, called a V-bit, is used to determine whether the 4-byte Vendor-Id field should be present in the AVP header.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           AVP Code                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|V M P r r r r r|                  AVP Length                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Vendor-ID (opt)                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Data ...
+-+-+-+-+-+-+-+-+
```

Figure 10 Diameter AVP structure according to [8].

To reproduce the issue, we needed to send a message with V-bit set in the header of a non-vendor-specific AVP. This seems to cause incorrect interpretation of the message length and reading of the wrong chunk of memory, because the process restarts after several thousand such messages are received. If more such messages are sent, this leads to a node reboot.

6 Telecom Security Audits: Real-World Considerations

We would like to discuss several difficulties and issues encountered while working with MNOs.

For all operators we have worked with, telecom security audits are possible only on test networks. We found that often these networks are configured differently than the real network used by subscribers. Therefore, it may not be possible to assess some attack scenarios that would be possible on production networks.

In addition, in our experience, it is usually a challenge for operator personnel to prepare the network for testing (such as by configuring a Diameter connection for the auditor's equipment) beforehand. Much of the time allocated for testing is actually used to configure equipment, taking up to a week in some cases. As a result, the duration and quality of testing are impacted.

Speaking of the human factor, MNO awareness of security issues is often poor. It seems that currently there is very low awareness of SS7-related vulnerabilities, and virtually no awareness of vulnerabilities in Diameter and other telecom-specific protocols, among MNO security personnel. It is also our experience that many operators do not see any value in securing and testing their SS7 network. They appear to downplay the importance of SS7 network security, despite being provided with all the relevant information. Because older technologies are still widely in use for roaming and as temporary solutions (CSFB), quite a few attack vectors take advantage of interworking between the technologies (see [3] for one example).

Our experience also shows that operators are much more concerned by fraud or network DoS than ensuring privacy and quality of service for individual subscribers. While this can be expected due to immediate monetary and reputational risks for the operator, we think that MNOs should not underestimate the similar harm of subscriber DoS or location tracking attacks, particularly when aimed at VIP subscribers.

Another difficulty in communicating the severity of problems to a client is due to limitations in rating methodologies. CVSSv3, for example, does not adequately capture differences between some attacks.

7 Short-Term and Long-Term Solutions for Diameter Security

Our view is that Diameter security must start with education and awareness-raising among MNOs. Many operators seem oblivious to Diameter threats and are reluctant to think about protection or even security audits. Even diligent MNOs that perform audits lack the necessary information about vulnerabilities and their consequences.

Currently, the best protection against Diameter attacks is a combination of IDS + firewall. However, this combination offers only limited protection against attacks that use roaming protocols (mainly S6a), due to the difficulty of distinguishing between attacks and legitimate roaming traffic.

Ultimately, to ensure robust security for Diameter networks, end-to-end encryption, authentication and integrity protection must be implemented. While an IETF draft on these topics was prepared, it is no longer active and an RFC with scenarios and requirements [9] has been proposed instead. We also believe that the same end-to-end approach to security is essential for any protocols that may replace Diameter in 5G networks.

References

[1] Kotte, B. T. (2016). *Analysis and Experimental Verification of Diameter Attacks in Long Term Evolution Networks.* Master's thesis, Aalto University, Espoo.

[2] De Oliveira, A. (2016). "Assaulting IPX Diameter Roaming Network," in *Proceedings of the Troopers IT-Security Conference*, Heidelberg.

[3] Rao, S., Holtmanns, S., Oliver, I., and Aura, T. (2016). *The Known Unknowns of SS7 and Beyond.* Espoo: Aalto University.

[4] SCTP Stack for Python (2017). Available at: https://github.com/philpraxis/pysctp

[5] ETSI (2012). *3GPP Specification: 29.329; Sh Interface Based on the Diameter Protocol; Protocol Details. Version 14.0.0 by 3rd Generation Partnership Project.* Sophia Antipolis: ETSI.

[6] European Committee for Standardization (2013). *3GPP Specification: TS29.272 Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) Related Interfaces Based on Diameter Protocol Version 14.0.0 by 3rd Generation Partnership Project*. Brussels: European Commission.

[7] Nohl, K., and Melette, L. (2015). *Advanced Interconnect Attacks. Chasing GRX and SS7 Vulns.* Available at: https://www.youtube.com/watch?v=2oCOdGpXvZY

[8] Fajardo, V. (Ed.), Arkko, J., Loughney, J., and Zorn, G. (Ed.). (2012). *RFC6733 Diameter Base Protocol.* Available at: https://www.rfc-editor.org/rfc/rfc6733.txt

[9] Tschofenig, H., Korhonen, J. (Ed.), Zorn, G., and Pillay, K. (2016). *RFC7966 Security at the Attribute-Value Pair (AVP) Level for Non-neighboring Diameter Nodes: Scenarios and Requirements*. Available at: https://www.rfc-editor.org/info/rfc7966

Biography

S. Mashukov attended Lobachevsky State University of Nizhny Novgorod, Russian Federation, receiving his B.Sc. and M.Sc. degrees in Computer Science in 2010 and 2012, respectively. Before joining Positive Technologies in 2016, he worked for 6 years on maintenance and development of a Diameter Base implementation for the one of the most deployed telecom platforms in the world.

As a telecom security specialist, his main point of interest is security of the Diameter protocol. He performs Diameter security audits for international MNOs and conducts research on the protocol weaknesses.

Sergey is also the general developer of the Diameter Vulnerability Scanner tool and member of the Telecom Attack Discovery development team.