Ericsson white paper
GFMC-18:000011 Uen
April 2018

ERICSSON

How to achieve adaptive security in the signaling network

Introduction

According to Ericsson Mobility Report, November 2017 [1], communication services have become an integrated part of daily life, with billions of subscribers worldwide counting on operators to protect their privacy. To maintain a high level of trust with their subscriber base, operators must be able to ensure confidentiality, data integrity, accountability and availability with their service offerings. Further, investing in secure network solutions enables them to gain a commercial advantage through the reduction of subscriber churn and the accelerated transition toward new and innovative services on account of a higher level of customer acceptance.

Securing connectivity for the Internet of Things (IoT) is another important aspect for operators to consider. There will be strong growth in IoT in the years ahead with multiple opportunities for ecosystems, each with different requirements and capabilities. Secure connectivity is a basic requirement that is described further in the Ericsson white paper IOT Security [2].

Operators need a robust strategy to protect their networks from known security risks. A typical protection strategy first addresses central routing functions at the network edge. It then broadens to become a defense-in-depth strategy that extends to the target nodes inside the network to provide multi-layer protection. While this is a good start, we recommend that operators use advanced analytics as well to raise the level of security protection still further.

Modern security monitoring and analytics tools are able to reveal known and new security risks, giving operators the opportunity to take preemptive action and implement the necessary countermeasures before their networks become subjected to attacks. Regular security risk assessments make it possible to continuously identify potential security risks and verify the measures that protect against them. The results from security analytics should be integrated in the security risk assessment to turn unknown security risks into known ones.

The introduction of Network Functions Virtualization increases flexibility, making it easy to add or remove network elements based on operators' needs. Achieving effective threat management in a rapidly changing environment requires a high level of process automation to assess vulnerability and address security risks.

The challenge

The vulnerabilities of today's telecommunication networks drive the need for innovative threat management solutions at network level. There are typically no security mechanisms built into the signaling protocols used in networks, including protocols based on the international Signaling System 7 (SS7) standard, including Mobile Application Part (MAP) and IP-based protocols such as Session Initiation Protocol (SIP), Diameter and GPRS Tunneling Protocol (GTP). The reason for this is that the network architecture was designed based on the assumption that only trusted parties communicate with each other through a trusted signaling network. This assumption can however no longer be made because in today's networks, connectivity to signaling networks is provided to third parties, making it possible to inject malicious signals through user-to-network interfaces as well as through network-to-network interfaces. The procedures used to manipulate signaling sequences are widespread.

As a result of the security flaws in today's telecommunication networks, operators and users are facing a diverse range of security risks including the threat of privacy violations, identity theft, fraud, service interference, and denial-of-service attacks. These threats were made public to broad audiences at the Chaos Communications Congress conference in Hamburg in both 2014 [3] and 2015 [4]. Further, CBS News provided a live demonstration of SS7 vulnerabilities and how they affect mobile phone users in one of its 60 Minutes features: Hacking your Phone (April 17, 2016) [5].

The solution

Establishing an adaptive security strategy

To protect their networks from signaling security threats, operators should follow a three-step strategy as depicted in **Figure 1** that includes adopting a signaling security framework, employing analytics and process automation, and carrying out regular security assessments.

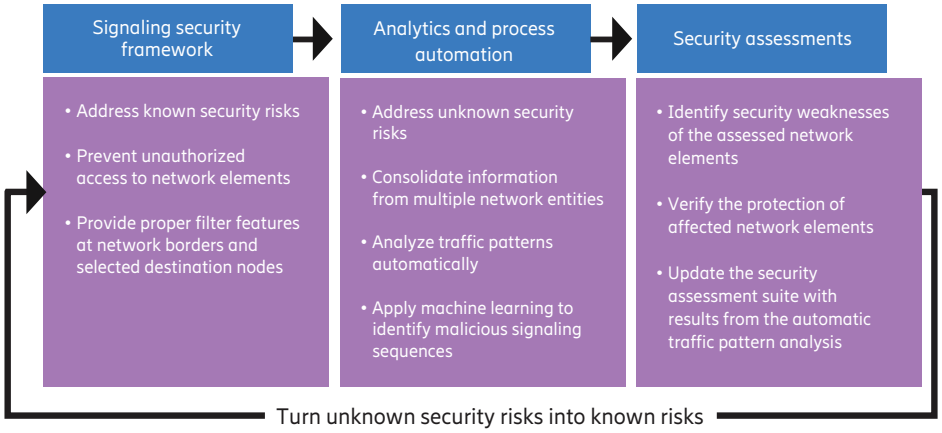

Figure 1: Signaling network – security protection strategy

A signaling security framework makes it easier to address known security risks by preventing unauthorized access to network elements and providing proper filter features at network borders as well as at selected destination nodes. Analytics and process automation extend the protection to include unknown security risks by consolidating data from multiple network entities and interpreting traffic patterns automatically. Analytics and machine learning should also be used to identify malicious signaling sequences.

Performing security assessments on network elements on a regular basis enables the identification of known vulnerabilities as well as verification of the protection of these elements. An analytics and process automation suite carries out an automatic traffic pattern analysis of services, evaluating the risk status of these elements, providing feedback and turning unknown vulnerabilities into known ones.

The signaling security framework

To establish a basis for a secure signaling network, an operator must protect network equipment from unauthorized access in the following ways:

– Apply proper node hardening methods to all network elements so that unused interfaces are closed and only authorized network interfaces can be used to establish communication links with the network elements.

– Protect IP connectivity with the network elements with an IP firewall, so that only authorized network elements can establish connections.

– Perform authorization and authentication of operations and maintenance (O&M) accounts, so that only well-known users can modify the configuration of a node in line with a given permission. Any changes to the node configuration are logged so that they are traceable.

– Configure dedicated network elements to deal with external network signaling traffic, keeping them segregated from the network elements that deal with internal network traffic. In this way, if an operator's network faces a denial-of-service attack from the outside, internal network traffic will not be affected.

– Define the services that can be triggered by third parties with access to the signaling network to protect it from harmful ingress signaling traffic.

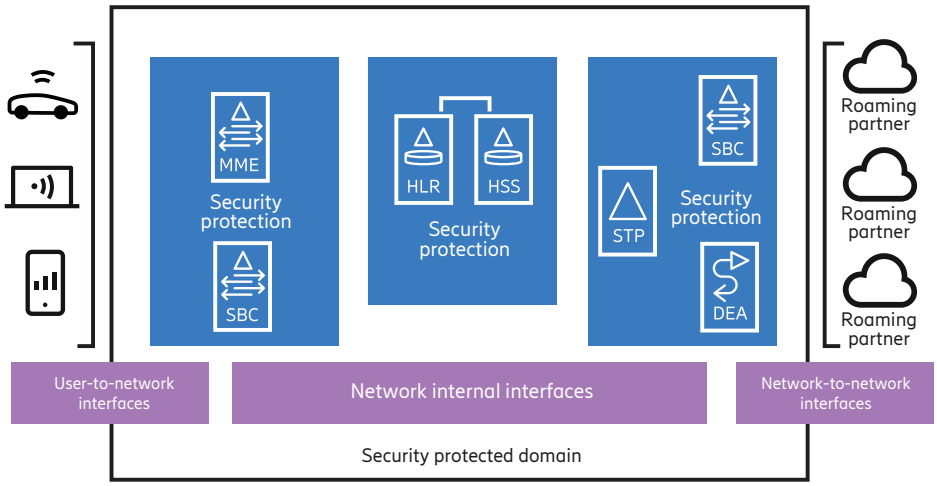

Figure 2: Signaling security framework

Following the above recommendations typically prevents the operator's own network from being used as a source of malicious signaling traffic. Nevertheless, the signaling network remains exposed to signaling security risks that can be injected on both user-to-network and network-to-network interfaces. **Figure 2** shows how to set up a signaling security framework to protect the operator's network from known signaling security risks.

User terminals need to be authenticated and authorized before they can access the network through a user-to-network interface. The authentication and authorization can be based on the subscriber identity module (SIM) or the universal subscriber identity module (USIM) in the user terminal. Other means of authentication are user name and password combinations and certificate-based credentials.

Verifying the injected signaling procedures is also recommended when users are correctly authenticated and authorized. For instance, in the case of IMS, the session border controller (SBC) located at the edge of the network performs signaling and media rate control, and SIP requests validation and encryption to protect the subscribers' privacy and integrity from eavesdroppers.

On network-to-network interfaces, operators need to verify the trustworthiness of incoming signaling procedures in their own administrative domain. This is typically done in nodes acting as the first point of contact at the edge of the signaling network. The signaling transfer point (STP) acts as first point of contact for SS7 signaling.

The Diameter Edge Agent (DEA) takes on this role for Diameter signaling. SIP signaling from interfacing networks is terminated first in an SBC before it is propagated into the own network.

The defense-in-depth principal can be applied in the signaling network as well, introducing an additional layer of security checks in case the first layer is bypassed. Consequently, target nodes such as the HLR or HSS perform sanity checks on the signaling messages as well to filter out any that are obviously wrong.

Recommended security checks on network-to-network interfaces can be separated into two types: stateless and stateful. Stateless security checks only take into consideration the message contents and internal configuration data. Stateful security checks involve more sophisticated handling processes. A stateful security check is designed to prevent location-based fraud, where voice calls or text messages are redirected, resulting in unlawful interception or impersonation of subscriber identities.

In large network deployments, there are multiple interconnection points to roaming networks. Stateful security checks have to be executed in all these interconnection points so the signaling firewall will need an efficient mechanism to synchronize location information on subscribers network-wide. New location information can be received on any of the interconnect points for a dedicated subscriber. Information about the last trusted location must be the same in all the signaling firewalls.

Using encrypted signaling transport is a complementary strategy providing additional security in signaling networks. IPsec, TLS or DTLS provide confidentiality, integrity, authentication and replay protection for a signaling connection between two peers. External parties cannot read or modify the signaling information. Neighboring peers can be authenticated in a more trustful way, and attackers cannot replay recorded signaling streams to harm the network.

Secure signaling connections can be established between two peers. This works fine on user-to-network interfaces where the communication from a user terminal to a trusted network node can be encrypted. Certain limitations will however become apparent when extending this concept to an end-to-end session involving multiple operator networks. End-to-end encryption is not possible when intermediate network nodes must read and modify certain information elements of a signaling message to facilitate routing decisions. Operators can agree on a secure signaling connection at their interconnection links, but none of these operators can influence how the signaling is treated behind the agreed security endpoints, so that it is possible to continue with an unprotected signaling connection. Another issue that counteracts secure signaling transport is the fact that attacks on the signaling infrastructure are launched from trusted network elements. This is possible because the business model is based on selling connectivity to the signaling network to third parties.

Considering these limitations, the added value of encrypted signaling transport is quite limited. It can be used for user-to-network interfaces or to bridge security zones, but it cannot yet be considered a solution that provides end-to-end signaling transport security; further agreements on the standardization level are still needed.

Analytics and process automation

In today's networks, signaling network protection involves security measures being taken at the network boundary protecting individual signaling interfaces. While this approach increases the overall level of security, it is still not sufficient for the detection of all types of threats. For highly secure operations, boundary protection should evolve toward in-depth protection with a unified security and fraud governance solution, as illustrated in **Figure 3**. Such a solution provides end-to-end network knowledge for securing assets across different layers and for facilitating remediation across all relevant assets.

Unified security analytics is evolving toward the aggregation of information elements from different points in the network. The consumed security feeds can be signaling packets, message flows, events, signaling configuration information, and so on. Data collection from multiple sources enables nodal information to be combined and thus increases situational awareness at the network level.

Sophisticated methods of attack such as camouflaging or distributed denial-of-service type attacks are a concern for signaling networks, since these methods are hard to detect at the network boundary. Big data analytics techniques such as sequence analysis and behavioral analytics can extract advanced security indicators from correlated event feeds. Predictive analytics working on those indicators can even detect threats where individual signaling events appear harmless.

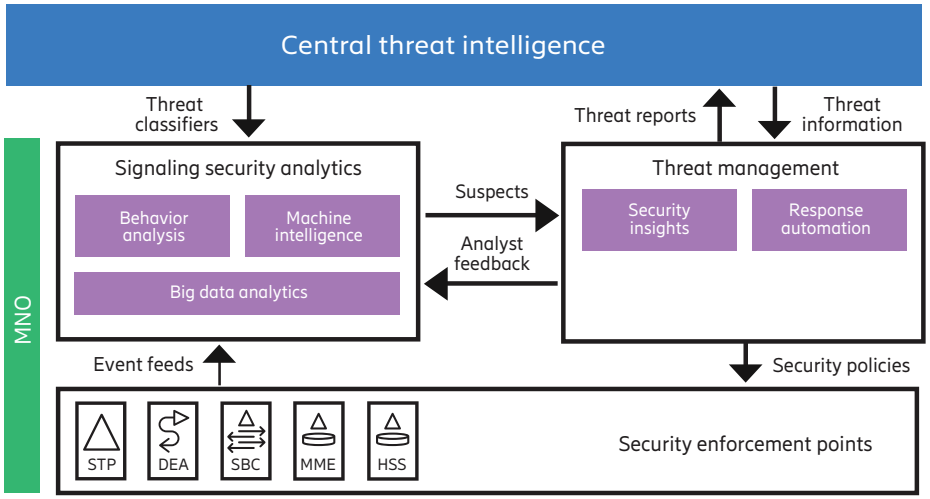

Figure 3: Signaling security analytics and process automations

The emergence of new types of threats creates new challenges in keeping threat information databases up to date. With the help of machine intelligence, input from security analysts as well as from central threat intelligence can be rapidly incorporated into predictive analytics. In this way, threat detection becomes significantly more adaptive compared with a traditional programmatic approach.

Operators need a way to ensure that new threat types are detected and mitigated rapidly. Modern security analytics can provide pre-emptive information about known as well as new security risks. Anomaly detection techniques can identify signaling abnormalities, drawing security analysts' attention to suspects at an early stage.

We recommend that network operators select a consolidated signaling security analytics solution with the combined power of big data analytics, machine intelligence and anomaly detection. This proactive security approach provides the benefits of end-to-end security risk awareness, sophisticated threat detection capabilities and significantly shortened mitigation time.

For enhanced protection, operators should subscribe to central threat intelligence information, which can alert them to globally affected threats and in some cases even targeted threats applicable to their realm. Threat intelligence facilitates an understanding of risks, and allows threat information to be turned into deployable mitigation actions. Operators can also decide to share threat information by submitting threat reports to the central threat intelligence.

A high degree of automation is needed to ensure a speedy response to any threat identified. Security process automation and policy orchestration should deploy and adjust security controls dynamically. The process can act upon threats and anomalies that signaling security analytics have identified or the central threat intelligence has reported, and decisions can be made based on confidence level and impact.

Security assessment

Security assessment is an essential procedure carried out to gain an understanding of the risk level a signaling network is exposed to, and to what extent known security issues are mitigated by the network functions. Two different strategies can be applied: passive monitoring and active attack initiation.

As shown in **Figure 4**, passive monitoring is based on observance of actual network traffic and reports of known attack scenarios, which make an operator aware of the actual security risks observed in the network and what countermeasures to take to prevent them.

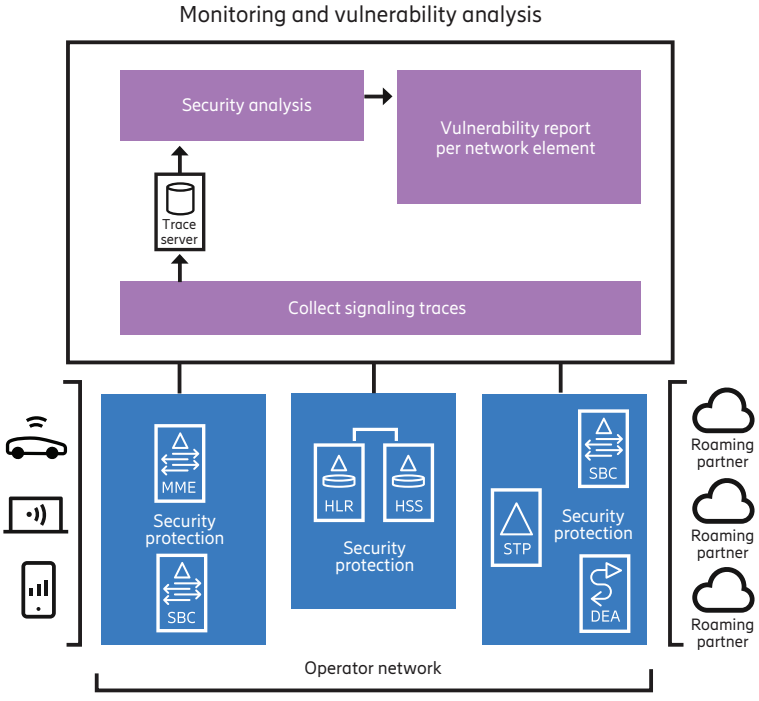

Figure 4: Passive monitoring

The passive monitoring approach can be enhanced with an assessment of the node hardening and privacy protection of the network elements involved, covering the following points:

– security policy set definition (at network level), including policies about access control, data masking, hardening, audit logging and so on

– policy compliance monitoring

– threat analytics (detection of security policy breaches).

Applying the strategy of active attack initiation goes a step further, as Figure 5 illustrates. Known attack scenarios are targeted toward network nodes from special equipment – either network internally in a kind of lab environment, or network externally in a realistic end-to-end environment. The advantage of this approach is that it is possible to systematically target attack scenarios against the different network entities and to verify protection mechanisms against them. Thus an operator gets a verified security configuration at the node and network level that can mitigate the injection attack scenarios.

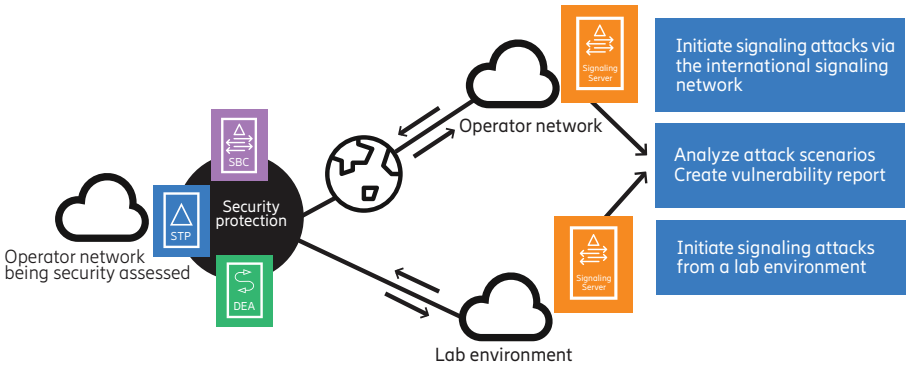

Figure 5: Active attack initiation

Over time, security assessments need to be adapted to the latest known security risk level. Once updated, a security assessment can be reapplied to an operator network, verifying that the security measures are sufficient to protect the network from the newly identified security risks.

Conclusion

An innovative adaptive security strategy is required to protect operator assets from a diverse range of security threats to the signaling network, from the interception of private communications or location information, to the takeover of user accounts to initiate money transfer, to denial-of-service attacks. The approach we recommend consists of three steps: adopting a signaling security framework; employing analytics and process automation; and performing regular security assessments.

The first priority for an operator is to prevent unauthorized access to the network entities and to block all known security attacks either at the network border or at targeted destination nodes. Unknown and more sophisticated attacks can be detected by a unified security and fraud governance solution that provides end-to-end network knowledge to secure the operator's assets by consolidating information from different network elements. Big data analytics and machine intelligence can extract threat signatures from the data collected. This process allows a high level of automation and is highly relevant given the increased flexibility of operators' telecommunication networks and their migration to virtual network solutions. Finally, carrying out security assessments on a regular basis ensures that the protection mechanisms for the threat signatures identified remain in place.

References

1. Ericsson, Ericsson Mobility Report, November 2017, available at: https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-november-2017.pdf

2. Ericsson, IoT Security – Protecting the Networked Society, February 2017, available at:https://www.ericsson.com/assets/local/publications/white-papers/wp-iot-security-february-2017.pdf

3. 31st Chaos Communication Congress, Hamburg, December 27-30, 2014, available at: https://events.ccc.de/congress/2014/wiki/Static:Main_Page

4. 32nd Chaos Communication Congress, Hamburg, December 2015, available at: https://events.ccc.de/congress/2015/wiki/Static:Main_Page

5. CBS News, 60 Minutes, Hacking your Phone, April 17, 2016, available at: https://www.cbsnews.com/news/60-minutes-hacking-your-phone/

Glossary

DEA	Diameter Edge Agent
DTLS	Datagram Transport Layer Security
GPRS	General Packet Radio Service
HLR	Home Location Register
HSS	Home Subscriber Server
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPsec	Internet Protocol Security
MAP	Mobile Application Part
MME	Mobility Management Entity
MNO	Mobile Network Operator
O&M	Operations and Maintenance
SBC	Session Border Controller
SBG	Session Border Gateway
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SS7	Signaling System 7
STP	Signaling Transfer Point
TLS	Transport Layer Security
USIM	Universal Subscriber Identity Module

Contributors

The contributors to Ericsson's opinion on this topic are Gergely Matefi and Michael Stief.

Gergely Matefi
is a system architect at Security Solutions within Business Area Emerging Business. He has gained 18 years of experience at Ericsson ranging from packet QoS, media processing, over-the-air synchronization and cloud technologies, through his various system architecture design, technology exploration and standardization assignments. In his current position, he is responsible for the evolution of telecom security analytics architecture. His focus is on end-to-end automation of threat detection and mitigation loops. Matefi holds an M.Sc. in information technology from Budapest University of Technology and Economics, Hungary.

Michael Stief
joined Ericsson in 1994 and has worked with system management and product management assignments for various wireless and wireline circuit switched applications over the years. He is currently working as technical product manager for signaling within Product Line Communication Services, where he is technically responsible for Diameter, SS7 and SIP signaling products, including Diameter Signaling Controller (DSC) and IP-Signaling Transfer Point (IP-STP). Stief graduated from the Technical University of Dortmund, Germany with a degree in electronic engineering.