PRESS RELEASE

Stockholm, Sweden
December 7, 2021

AdaptiveMobile Security Publishes Blueprint for Securing 5G SMS

AdaptiveMobile Security, an Enea company and the world leader in mobile network security, today published a comprehensive blueprint on how to secure SMS on 5G Networks. The research outlines how SMS operates on the next generation of networks, identifying the emerging security risks and attack scenarios that exist on 5G networks. It also sets out the principles for securing 5G networks against malicious attacks via SMS, including the need for attack correlation across both legacy 2G, 3G, 4G and new 5G protocols and between different interfaces to identify the real threats. The full research paper, *Messaging for the Future: Securing SMS in 5G*, is available for download from here.

The research details how the security of SMS communication in 5G is more important than ever and the key aspects mobile operators must consider when protecting their subscribers from attacks. There are new security considerations as SMS usage increasingly moves from user-centric messaging towards Application-to-Person (A2P) and Machine-to-Machine (M2M) SMS-based messaging. A growing number of enterprises are dependent on SMS for direct communication with their customers, and the market is witnessing huge expansion in the Communications Platform as a Service (CPaaS) sector which in turn is driving the unstoppable momentum witnessed in A2P SMS. Meanwhile, the growth of IoT devices and the subsequent increase in M2M SMS means that messaging must be secured at the network level due to the lack of any human supervision that could detect a security breach and raise an alert.

SMS on 5G networks also retains legacy technology which must be integrated with the new technologies 5G brings to the mobile network, with attackers able to use an extensive toolkit of techniques to penetrate networks at various entry points until they succeed. Even with new standards and specifications, 5G is not completely secure, and lessons from the vulnerabilities of previous mobile network generations must be learned and applied to secure the future of SMS mobile messaging in 5G. The mistakes of 3G and 4G must not be repeated.

The research paper also includes:

- Information to mobile operators on implementing legacy support for SMS traversing both 4G and 5G networks
- SMS Subscriber roaming methods, how messages are sent through and the various delivery approaches
- A detailed comparison of 2G, 3G, 4G and 5G SMS-related nodes and interfaces, and a breakdown of the mechanisms of SMS delivery using Rich Communication Suite (RCS) in a 5G environment

Enea AB, P.O. Box 1033
164 21 Kista

Phone: +46 8 507 140 00
Fax: +46 8 507 140 40

E-mail: info@enea.com
Website:
www.enea.com

- An overview of the current misuse of SMS and the various attack types that are possible and that AdaptiveMobile Security believes will continue when sending SMS through the 5G core network, including: Unsolicited SMS Messaging, SMS Phishing, Premium SMS Fraud, Mobile Malware, Surveillance, Information Retrieval, Denial of Service, SMS Interception and Grey Routes abuse
- Highlights of new potential SMS risks and attacks that may arise in the next generation of mobile networks
- An outline of how to mitigate threats and best practices for securing SMS in 5G, such as protecting various attacker entry points, implementing efficient filtering approaches, complemented with ongoing threat intelligence to defend against new and evolving attacker tactics, techniques, and procedures

“Rumours of the demise of SMS have been greatly exaggerated, in particular in the A2P market where we continue to see strong growth. SMS holds and will continue to hold significant and considerable advantages to Over-the-Top messaging services. Despite all the new features of 5G, SMS’s ability to reach every mobile device in the world makes it a powerful tool for mobile operators and brands, both today but also for the foreseeable future,” said Cathal McDaid, CTO of AdaptiveMobile Security. “However, securing SMS over 5G is a complex combination of dealing with legacy technology, while also integrating with the new demands and network designs that 5G brings. Mobile network operators must ensure they are fully aware of the potential threats and how to best to mitigate them both today and in the future as they migrate to 5G.”

This research is the latest in a series of groundbreaking work done by AdaptiveMobile Security into new 5G network technologies, use-cases and the associated security challenges these create. The AdaptiveMobile Security research team has published analysis on general 5G security challenges, specifically on securing the core network migration from 4G to 5G and most recently on Slicing Security in 5G Core Network. In this latest 5G Security research, AdaptiveMobile Security determines if there are any security implications to consider for SMS as mobile operators roll out 5G networks and migrate subscribers to the next generation of mobile networks. The full report is available for download here

Contact

Erik Larsson, Senior Vice President Marketing and Communication
E-mail: erik.larsson@enea.com

Máirín O’Sullivan, Head of Marketing, AdaptiveMobile Security
Email: mairin.osullivan@adaptivemobile.com

PRESS RELEASE

About Enea

Enea is one of the world's leading specialists in software for telecommunications and cybersecurity. The company's cloud-native products are used to enable and protect services for mobile subscribers, enterprise customers, and the Internet of Things. More than 3 billion people rely on Enea technologies in their daily lives.

Enea is headquartered in Stockholm, Sweden, and is listed on Nasdaq Stockholm.

For more information: www.enea.com

About AdaptiveMobile Security

AdaptiveMobile Security, an Enea company, is a world leader in mobile network security, protecting more than 2.2 billion subscribers worldwide. With deep expertise and a unique focus on network security, AdaptiveMobile Security award-winning innovative security solutions and services provide its customers with advanced threat detection, response, and actionable intelligence, combined with the most comprehensive security product-set in the market today, predicting and protecting against multiprotocol mobile security attacks.

AdaptiveMobile Security provides its customers with the unique combination of technology, analyst input and intelligence to ensure their subscribers, data and networks remain protected from cyber warfare.

AdaptiveMobile Security was founded in 2006. The Company counts some of the world's largest carriers, Governments and Regulators as customers. The Company is headquartered in Dublin with offices in North America, Europe, South Africa, the Middle East, and Asia Pacific region.

For more information: www.adaptivemobile.com

Enea AB, P.O. Box 1033
164 21 Kista

Phone: +46 8 507 140 00
Fax: +46 8 507 140 40

E-mail: info@enea.com
Website:
www.enea.com