Abstract

Mobile Network Operators interconnect their networks to provide roaming services based on Service Level Agreements (SLAs) directly with peers or through roaming intermediaries. The SLAs include security clauses that are translated into security requirements in the interconnection links. Whilst the security architecture in the fifth generation of mobile networks (5G), in comparison with previous generations, has introduced significant advancements towards a new end-to-end security paradigm, the security posture in the interconnection of mobile networks cannot be considered static and solely dependent on policies part of contractual documents. On the contrary, the security posture in this context requires a continuous adaption to the ever-growing interconnection ecosystem and threat landscape, considering the unavoidable coexistence of the three protocol stacks since the beginning of the mobile networks, i.e., SS7 (2G/3G), Diameter (4G) and HTTP/2 (5G).

The primary aim of this research was to build a risk-based security framework capable of anticipating major security issues and reacting to changes in the security level of the interconnection links established between peer Mobile Network Operators and/or roaming intermediaries. To achieve this, I have developed four building blocks, connected to form a comprehensive security lifecycle. Firstly, I have designed a dynamic risk evaluation mechanism at both message and sequence levels using expert knowledge and data mining techniques applied to data streams. As a baseline for computing the risk, I have adopted the Common Vulnerability Scoring System. Secondly, I have proposed a novel approach to determine a trust score for Mobile Networks in roaming context, with risk measurement as the main input. Thirdly, I have introduced the concept of security profiling in 5G interconnection as a catalyzer to implement the new security end-to-end paradigm in 5G. Finally, I have designed a new method to dynamically create and enforce the security policies in the interconnection gateways, acting as enforcement points, by enhancing the current 5G Policy Control framework, making security an actual quality element of the network.

The security framework has been validated with a theoretical key use case such as location tracking, as well as with an anonymized trace of real Diameter signaling traffic between two operators in Asia. Several procedures following the actual 5G-Advanced standardization are provided to demonstrate the adequacy of the novel methods in the 5G system, even when privacy and security

concerns to access the signaling data in interconnection hinder wide academic experimentation in this field.

Keywords: mobile networks, security, roaming, interconnection, signaling, SLA, 3GPP, 5G, 4G, Diameter, HTTP/2, IPX, risk management, data mining, security enforcement, trust score, security profiling.