Mobile Network Threat Analysis and MNO Positioning

George Lyberopoulos, Helen Theodoropoulou and Konstantinos Filis

Abstract The dramatic increase of smart mobile devices and applications, the advent of Android OS, the increased number of wireless radios (incl. NFC) the support and the low awareness about security and privacy risks on the one hand, and the flatter, IP-based network architecture, the introduction of new radio technologies (femtocells, WiFi, LTE) and applications (M2M, NFC) on the other, have changed the mobile threats landscape and will change the way security will be dealt in the coming years. Mobile Network Operators (MNOs) have started to investigate the possibility to introduce additional measures to secure their networks, providing thus a defense before security threats materialize.

1 Introduction

The wide adoption of smart mobile devices (smartphones, tablets) encompassing personal data such as, contacts' list, photos, notes, financial data, credentials for online banking, while offering always-on capability to social networks, e-mail accounts and possibly access to corporate networks, has augmented the interest of cyber-criminals, not only due to possible financial gains, but because these devices could be utilized as stepping stones for launching attacks towards the mobile core network and other connected networks or for industrial espionage. In addition,as mobile networks become

G. Lyberopoulos · H. Theodoropoulou · K. Filis (✉)
COSMOTE-Mobile Telecommunications SA, Ikarou 1 and Ag, 19002Louka, Attica, Greece
e-mail: glimperop@cosmote.gr

H. Theodoropoulou
e-mail: etheodorop@cosmote.gr

K. Filis
e-mail: cfilis@cosmote.gr

E. Gelenbe and R. Lent (eds.), *Information Sciences and Systems 2013*,
Lecture Notes in Electrical Engineering 264, DOI: 10.1007/978-3-319-01604-7_41,

central part of our daily lives, they comprise attractive, high-profile, targets for hacktivists, whose aim is to promote a political or social agenda through disruption.

The support of multiple communication technologies such as Bluetooth, Wi-Fi, 2G, 3G, Long Term Evolution (LTE), along with the user's capability to install applications from "untrusted" sources and the extensive use of outdated operating system versions—esp. for Android devices [17]—have increased the vulnerability of smart devices by exposing them to heterogeneous attack vectors [18]. In addition, the introduction of new radio access technologies, such as femtocells, Mobile Network Operator (MNO)-operated WiFi, and LTE (4G), the transition to flatter and more open network IP-based architectures, the upcoming M2M and NFC applications and the exponential growth traffic, introduce additional vulnerabilities for both the mobile devices/users and the core network.

It is envisaged that security attacks will become more aggressive both in terms of frequency and severity. As such, MNOs, to prevent potential mobile cyber-attacks and protect its brand name, are investigating the possibility to introduce additional measures to secure their networks, providing thus a defense before security threats materialize. Currently, the research interest is focusing on the specification and development of an infrastructure based on honeypots being capable of collecting and analyzing attack traces coming from mobile devices, in order to understand the attack strategies and build appropriate countermeasures [15, 16, 20].

The material included in this paper is organized as follows: Sect. 2 sheds some light on the mobile telecommunications threats landscape. In Sect. 3 we present the currently available security techniques for the 3G and LTE mobile networks and for the femtocells. In Sect. 4 we elaborate on the MNO's role/strategy in addressing the emerging security threats, while in Sect. 5 we draw some concluding remarks.

2 Mobile Environment Threats Landscape

The proliferation of powerful smart devices, the dramatic increase in the number of applications (from "trusted" and "untrusted" sources), the advent of Android OS—which is more susceptible to malware due to its openness-, the increased number of wireless radios (incl. NFC) and the low awareness of users about security and privacy risks on the one hand, and the flatter, IP-based network architecture, the introduction of new radio technologies (femtocells, WiFi, LTE) and applications (M2M, NFC) on the other, have changed the mobile threats landscape and will change the way security will be dealt in the coming years.

Figure 1 illustrates the security threats landscape in a mobile telecommunications environment. Obviously, mobile devices play a crucial role since hackers may not only benefit from the information stored in the terminal, but because they may be utilized as enablers/facilitators to launch attacks towards the mobile core networks and/or other external networks. The most common method for spreading malware to

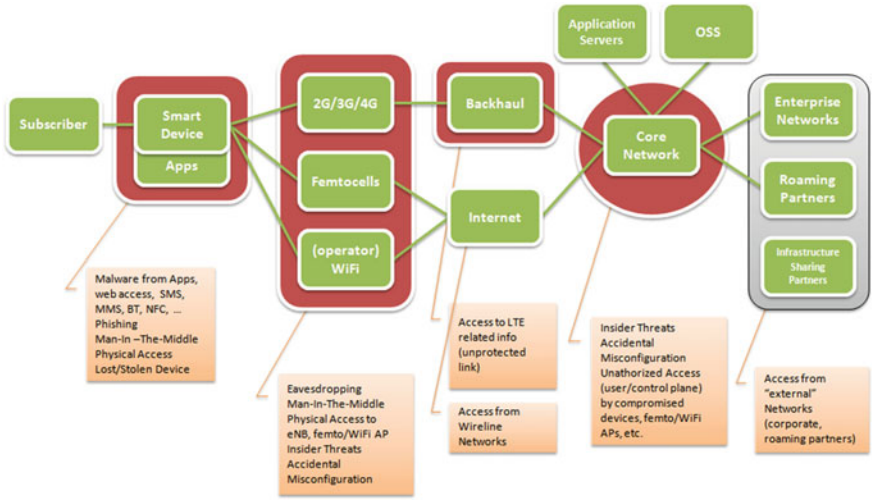

Fig. 1 Threats landscape in a mobile telecommunications environment

mobile devices is through the installation of an application (by the user's full consent), via SMS, MMS, Bluetooth, e-mail, the Internet, trusted and untrusted markets, etc.

By granting permission to collect and transmit information from the device, the hacker, may initiate voice calls and/or SMSs to premium numbers (that cost extra money), send e-mails and/or block incoming calls/SMSs, record conversations and send them to 3rd parties, steal and send personal info to 3rd parties, monitor the phone "status" (off-hook, ringing), take over control of the smartphone, turn the phone into mobile botnets so others can execute commands remotely, initiate attacks to mobile core/corporate network(s), (such as DDoS), reduce smartphone utility e.g., battery discharging, unusable smartphone (repeated reboots).

As far as the security threats towards the mobile core network are concerned (see Fig.1), these may originate from: (a) Compromised smart mobile devices, (b) The access network, (c) The backhaul network, (d) The core network and (e) External or 3rd party networks such as, the Internet, corporate networks, roaming partners' networks, other connected PLMNs, shared RAN, non-3GPP access network, external transport network, etc.

Note: Access to access/backhaul/core network necessitates physical access to the respective network nodes (by a "malicious" employee or a 3rd party) or the use of special equipment.

The security issues/challenges in 3G mobile core networks have been extensively discussed in the literature [7–10]. However, the evolution of the mobile networks towards the provision of higher Quality of Experience (QoE) to the end-users, as well as the simplification of the network architecture, has raised new security concerns for MNOs. More specifically:

- The proliferation of femtocells has introduced new points of attacks, including the air-interface, the FAP itself (which may reside at untrusted locations) and the backhaul [11, 12]. Third-party attacks may include man-in-the-middle (MITM), traffic snooping/redirection, fake base station attacks, authentication snooping, service disruption, and billing fraud.
- The incorporation of non-3GPP WiFi(s) owned by the MNO may necessitate access to LTE core network elements depending on the level of integration. As such, as in the case of femtocells, for a hacker it's easy to gain physical access to a WiFi access point that is now part of the MNO infrastructure.
- The introduction of the LTE (due to the new interfaces—such as X2, the Diameter protocol, the flatter architectures as well as the application related control plane traffic), is expected to have a tremendous impact on the signaling traffic that the network will have to cope with which may be leveraged for malicious activity.
- The transition of mobile networks to IP brings additional security threats, such as DoS and DDoS attacks, ping floods, SYN floods, replay attacks, DNS hijacking, IP port scanning [6], which may result in the interception of subscriber data, limit subscriber access (causing congestion), and/or compromise the overall network security of the network, since some of the core elements' functionality may be lost.[1]
- Apart from the upcoming VoLTE and the mandated introduction of IMS, it is envisaged that the trend toward virtualization and sw-defined networks will create new vulnerability sources, as both user and control plane traffic becomes more distributed across network and has to cross untrusted portions of it [6].

3 MNO Security Architecture

A threat and risk analysis for mobile communication networks in a qualitative way—see estimation of the likelihood of attacks, overall vulnerability of the assets, impact of successful attacks on the network—is presented in [14]. According to this study, the following threat categories can be identified:

(1) Flooding an interface (radio, backhaul), (2) Crashing a network element via a protocol or application flaw, (3) Eavesdropping (radio interface, backhaul, control plane, user plane), (4) Unauthorized data access to sensitive data on a network element via leakage, (5) Traffic modification (radio interface, backhaul, c-plane, u-plane), (6) Data modification on a network element, (7) Compromise of a network element via a protocol or application implementation flaw, (8) Compromise of a network element via management interface, (9) Malicious insider, (10) Theft of service.

MNO's security techniques include: advanced firewall and intrusion prevention systems, the addition of IPsec termination capabilities on platforms, and standardized features of network security architecture, including advanced message and entity

[1] In Japan, NTT DoCoMo experienced a signaling flood that disrupted network access in Jan/2012, caused by a VoIP OTT application running on Android phones [13].

authentication for both user and network, by using strong key-based cryptography, advanced encryption methods, mobile equipment identification, security gateways, ciphering mechanisms for signalling messages, location verification, prevention of unauthorized access, etc. However, the protection of the mobile core network from an attack coming from a user device still remains a challenge to be investigated and addressed, so that MNOs can protect their networks and provide their subscribers with a safe environment and advanced quality of service.

3.1 3G Security Architecture

Security protection in 3G-networks requires the consideration of several aspects and issues, such as the wireless access, the end-user mobility, the particular security threats, the type of information to be protected, and the complexity of the network architecture. The radio transmission is by nature more susceptible to eavesdropping than wired transmission. The user mobility and the universal network access certainly imply security treats. The different types of data, such as user data, charging and billing data, customer information data, and network management data, which are conveyed or are resident in mobile networks, require different types and levels of protection. Furthermore, the complex network topologies and the heterogeneity of the involved technologies increase the dependability challenge. Figure 2 presents an overview of the complete 3G security architecture [2].

There are 5 different sets of features that are part of the architecture:

(1) Network access security: Provides secure access to 3G services and protects against attacks on the radio interface link. (2) Network domain security: Allows nodes in the operator's network to securely exchange signaling data and protects

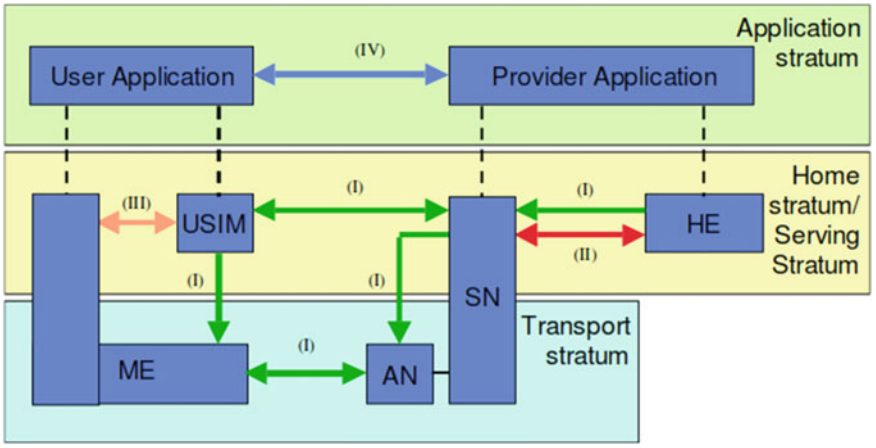

Fig. 2 Overview of the 3G network security architecture

against attacks on the wireline network. (3) User domain security: Secures access to mobile stations. (4) Application domain security: Enables applications in the user and in the provider domain to securely exchange messages and (5) Visibility and configurability of security: Allows the user to get information about the security features in operation and whether a service provision depends on the activation or not of a security feature.

Network access security features can be further classified into:

(1) User authentication: The property that the network that provides the service (serving network) corroborates the identity of the user. (2) Network authentication: The property that the user corroborates that he is connected to a serving network that is authorized by the user's home network. (3) Cipher algorithm agreement: The property that the terminal and the serving network can securely negotiate the algorithm that they shall use subsequently. (4) Cipher key agreement: The property that the terminal and the serving network agree on a cipher key that they may use subsequently. (5) Confidentiality of user data: The property that user data cannot be overheard on the radio interface. (6) Confidentiality of signaling data: The property that signaling data cannot be overheard on the radio interface. (7) Integrity algorithm agreement: The property that the terminal and the serving network can securely negotiate the integrity algorithm that they shall use subsequently. (8) Integrity key agreement: The property that the terminal and the serving network agree on an integrity key they may use subsequently. (9) Data integrity and origin authentication of signaling data: The property that the receiving entity (terminal or serving network) is able to verify that signaling and/or its origin has not been modified in an unauthorized way.

3.2 LTE Security Architecture

The LTE/SAE (System Architecture Evolution) network consists of only two nodes: (1) The MME/S-GW (Mobility Management Entity/SAE gateway), which is a multi-standard access system behaving as the anchor point for the mobility between different access systems, and (2) The eNB, which gathers all the purely radio-oriented functionalities. Most of the security requirements for 3G networks hold also for the LTE, so as at least the same level of security (as in 3G) shall be guaranteed (Fig. 3).

The main changes that have been adopted to fulfill the required level of LTE security are summarized below:

- A new hierarchical key system has been introduced in which keys can be changed for different purposes.
- The LTE security functions for the Non-Access Stratum (NAS) and the Access Stratum (AS) have been separated. The NAS functions are responsible for the communications between the core network and the mobile terminal, while the AS functions encompass the communications between the network edges, i.e. the eNB and the terminal.
- The concept of forward security has been introduced for LTE.

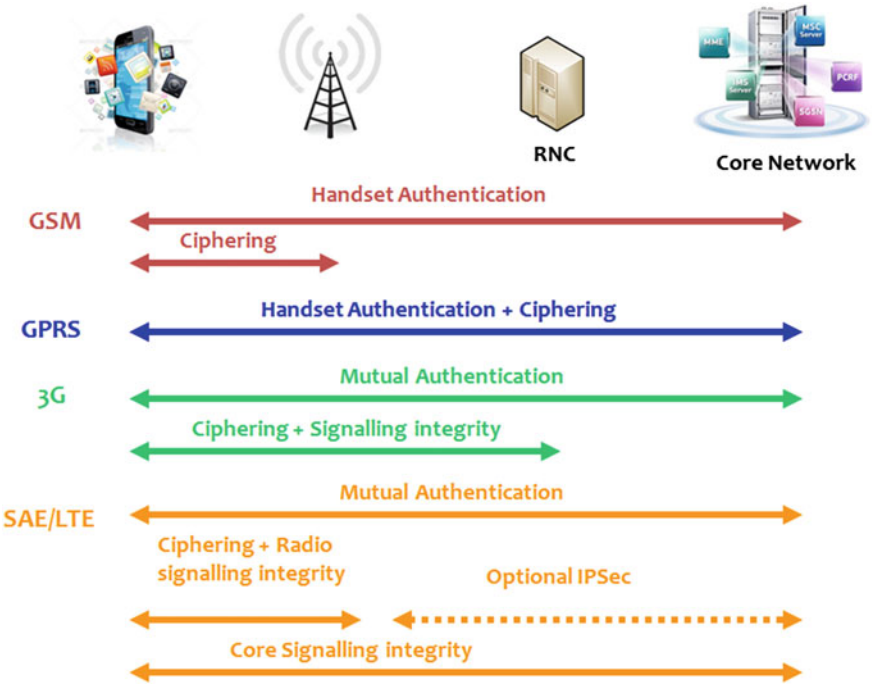

Fig. 3 Evolving security architecture towards LTE [19]

- LTE security functions have been introduced between the existing 3G network and the LTE.

In addition, since in LTE the mandated encryption from the mobile device terminates at the eNB, MNOs should secure the IP-based control/user plane transport to the core network using IPsec; although not mandatory according to the standards.

3.3 Femtocell Security Architecture

Femtocell Access Points (FAPs) are close-range, limited-capacity base stations that utilize residential broadband connections to connect to carrier networks [4]. The use of such distributed base station architecture, although it improves reception and allows the operators to deliver fast, seamless, high-bandwidth cellular coverage indoors, introduces new security concerns classified into three main categories: (1) Device and network authentication, (2) Data privacy and (3) Data integrity.

The security mechanisms designed to fulfill these concerns are the following [5]:

(1) FAP Physical Security, (2) FAP and Core Network mutual authentication and IPSec tunnel establishment, (3) Location Verification, (4) Access Control,

(5) Protection of traffic between FMS and FAP and (6) Measures for Clock Protection.

4 MNO Positioning

The mobile industry (equipment manufacturers, security systems vendors, etc.) is oriented towards a strict compliance approach aligned with the 3GPP specifications for securing networks' operation. In order for the MNOs to cope with the emerging security threats, they should develop a holistic, proactive, defensive and affordable security strategy (incl. policies, security processes, security risk management, business continuity, etc.), so as to secure both their networks and their subscribers. It is obvious that this objective is a real challenge, since the mobile network infrastructure is massive and extremely complex with multiple entities coordinating together. In case of a successful attack (e.g. DDoS attack) affecting part or the whole mobile network, the impact on the operator business will be negative, and therefore such incidents are highly undesirable.

Even in case the attack is directed to the user terminal, the impact could be significant if this happens on a large scale. In such cases, the customers' experience will be degraded and even if the "problem" originated by the customer itself (phone jailbreaking/rooting, installation of applications from untrusted sources, careless acceptance of application permissions), it is envisaged that the customers will blame the operator; especially if they have purchased their smartphones from the particular MNO. In the long term, if fraud via mobile malware gets out of control, it may lead to a trust loss which may slow down the growth of the overall mobile business. Towards this direction, the MNOs should:

- Apply all the latest security features (upon availability) to protect their networks end-to-end from possible malicious and/or accidental attacks.
- Facilitate the public awareness regarding the existence of malware and their impact as well as to inform the public on how they could be protected.
- Participate in R&D security-related activities, so as to be capable of setting the requirements from their own perspective, being informed on the latest developments on the security aspects and/or exploiting security research results.
- Closely cooperate with infrastructure and security vendors, security analysts, etc. to specify/develop new security features and toolsets.
- Establish a dedicated team to deal with network and terminal security, in terms of: identification of possible security gaps, conduction of specific experiments to reveal network vulnerabilities, monitoring how malicious attacks are evolving with time, disseminating the findings especially to those responsible for protecting the availability and integrity of the mobile network, coordination/decision making for actions required at the event of a successful DDoS signalling attack (e.g., load balancing, policy enforcement, validation of legitimate signalling traffic to minimize disruption, etc. [6]).

5 Conclusions

While current security techniques provide an adequate level of protection, MNOs need to take further actions to protect their networks from emerging threats, which may be caused either by malicious activity explicitly directed at the mobile network, or accidentally occurred. On the other hand, compromised mobile devices may constitute a quite substantial threat for the affected user, while when acting as mobile botnets, can easily endanger a whole mobile network operation. Therefore, MNOs should focus on building an effective proactive security strategy to protect both their network and subscribers, while in case of an attack, the MNOs should be prepared to respond immediately to defend their reputation and ensure the viability of mobile business.

Acknowledgments The current study is part of the Project NEMESYS (Enhanced Network Security for Seamless Service Provisioning in the Smart Mobile Ecosystem) which has received funding from the European Union Seventh Framework Programme (FP7) under grant agreement 317888. Disclaimer: The views expressed in this article are those of the authors and do not necessarily represent the views of the company.

References

1. http://www.lucent.com/enrich/v1i12007/article_c4a4.html
2. ETSI TS 133 102 V11.5.0 (2013–02) Digital cellular telecommunications system (Phase 2+); UMTS; LTE; 3G security; Security architecture (3GPP TS 33.102 v11.5.0 Rel. 11)
3. LTE; E-UTRA; E-UTRAN; Overall description; Stage 2 (3GPP TS 36.300 v11.4.0 Rel. 11).
4. Chen J, Wong M (2012) Security implications and considerations for femtocells. J Cyber Security Mobility 21(35)
5. ETSI TS 133 320 V11.6.0 (2012–11) UMTS; LTE; Security of Home Node B (HNB)/Home evolved Node B (HeNB) (3GPP TS 33.320 v11.6.0 Rel. 11)
6. Monica Paolini. Wireless Security in LTE Networks
7. Peng X, Wen Y, Zhao H (2011) Security issues and solutions in 3G core network. J Networks 6(5):823–830
8. Ahmed F et al. (2011) A data mining framework for securing 3g core network from GTP fuzzing attacks. Proceedings of the 7th International Conference on Information Systems Security
9. Checkpoint White Paper, Next Generation Security for 3G and 4G LTE Networks
10. Peng X et al. (2010) GTP security in 3G core network. 2010 2nd international conference on networks security, wireless communications and trusted computing
11. Bilogrevic I, Jadliwala M, Hubaux J.-P (2010) Security issues in next generation mobile networks: LTE and femtocells
12. Security of H(e)NB. Technical Report TR 33.820 v8.3.0, 3GPP, Dec. 2009
13. http://www.reuters.com/article/2012/01/27/us-docomo-idUSTRE80Q1YU20120127
14. ASMONIA Project: D5.1 - Threat and Risk Analysis for Mobile Communication Networks and Mobile Terminals, http://www.asmonia.de/deliverables/D5.1_II_ThreatAnd RiskAnalysisMobileCommunicationNetworksAndTerminals.pdf
15. NEMESYS Project, http://www.nemesys-project.eu/nemesys/
16. C. Dimitriadis Improving Mobile Core Network Security with Honeynets
17. Android Dashboard. https://developer.android.com/about/dashboards/index.html, Dec 2012
18. La Polla M et al. A survey on security for mobile devices

19. Cisco LTE Security Architecture—Session 2
20. Gelenbe E, Gorbil G, Tzovaras D, Liebergeld S, Garcia D, Baltatu M, Lyberopoulos G (2013) NEMESYS: Enhanced network security for seamless service provisioning in the smart mobile ecosystem. Proceedings of 28th International Symposium on computer and information sciences (ISCIS13), Paris, Oct 2013