A Review of Security Risks in the Mobile Telecommunication Packet Core Network

Varin Khera[1,2], Chun Che Fung[1], and Sivadon Chaisiri[3]

[1] School of Engineering and Information Technology, Murdoch University, Australia
[2] Nokia Solution Network (NSN)
varin.khera@nsn.com, l.fung@murdoch.edu.au
[3] School of Information Technology, Shinawatra University, Thailand
sivadon@siu.ac.th

Abstract. Advances in information technology depend on the availability of telecommunication, network and mobile technologies. With the rapid increasing number of mobile devices being used as essential terminals or platforms for communication, security threats now target the whole telecommunication infrastructure that includes mobile devices, radio access network, and the core network operated by the mobile operators. In particular, the mobile core network is the most important part of the mobile communication system because different access networks are consolidated at the core network. Therefore, any risks associated with the core network would have a significant impact on the mobile network regardless of technologies of access networks are in use. This paper reviews the security risks in the mobile core network for data services by considering the confidentiality, integrity and availability (CIA) aspects, and then relates them to the ITU-T X.805 reference framework. Finally, this paper provides a recommendation on how to address these risks using the ITU-T X.805 reference framework. This paper will benefit mobile operators and network designers looking to secure the mobile packet core system.

Keywords: telecommunication, network security, ITU-T Recommendation X.805, risks mitigation.

1 Introduction

With the advancement of mobile telecommunication technologies, wireless data access is on the rise with mobile users accessing telecommunications services (e.g., Internet and cloud services) from anywhere at anytime. Such technologies are essential to the stability and future development of a nation's economy. They form the backbone supporting the communication and value-added services for individuals and organizations. In addition, they enable effective operations of government agencies and private sectors. Disruption of the telecommunication systems have serious impacts and implications to the public safety and security of the country [1].

B. Papasratorn et al. (Eds.): IAIT 2013, CCIS 409, pp. 93–103, 2013.

A mobile telecommunication system consists of two layered networks, namely access and core networks. Access networks are edge networks where mobile devices (i.e., mobile users) connect to the telecommunication system. In particular, the mobile core network plays the most important role of the mobile telecommunication system since every access network is attached to the core. Hence, vulnerabilities in the core network could tremendously affect the entire telecommunication network [2].

In a mobile telecommunication system, core networks are classified into circuit and packet core networks. The circuit and packet core networks are deployed for voice services (e.g., services in the public switched telephone network) and data services (e.g., services in the Internet), respectively. In this paper, we mainly review the security risks on the packet core network which is highly vulnerable to security attacks. The main objectives of this paper can be summarized as follows:

- This paper reviews the risks associated with the mobile core network regardless of the technologies applied for the access networks. Then, we classify the risks into specific domains using the confidentiality, integrity, and availability (CIA) triad which is a widely used model for designing information security policies.
- We provide a recommendation on how the reviewed risks can be mitigated using the X.805 security framework defined by the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) [3]. Specifically, we propose a design of secured mobile packet core which is able to protect itself against the risks.

This review will be useful to mobile telecommunication operator and network designers since the risks can be considered as the benchmark to assess the operators' core networks. Furthermore, the proposed mobile packet core network design based on the ITU-T X.805 framework will be a guideline for improving the core networks. As a result, the secured core network will be able to protect invaluable information and assets belonging to the mobile users and operators.

The rest of this paper is organized as follows. Related works conducted in this area are discussed in Section 2. Section 3 describes the mobile network architecture. Then, risks associated with the mobile packet core network are presented in Section 4. The proposed improvement of the core network is presented in Section 5. Finally, Section 6 gives a conclusion and suggestion for future work on this topic.

2 Related Work

A number of studies have been conducted on the security implication of the user equipment (e.g., cellular phones) and the radio access network without focusing much on the mobile packet core network e.g., [4–7]. In [7], the infrastructure security of 3GPP relating to universal mobile telecommunications system (UMTS) network was discussed but did not investigate how risks could be associated with

the core network. As the mobile core network is essentially the most important part of the mobile telecommunication system, this core network therefore forms the main focus of this paper.

Security issues on the core network were studied. Security issues in GPRS tunnel protocol (GTP) and a solution to address the issues were presented in [8]. The study in [9] proposed a honeynet solution to secure a 3G core network. In [10], a review of security for a 3G network was presented, and then a security enhancement model was proposed with primarily focus on the access domain security. In [11], some security treats on a femtocell-enabled cellular network were reviewed. A study in [2] focused on security risks on a 4G network using the X.805 framework with short explanation on how the framework could be used to understand and mitigate risks on the mobile core network as a whole.

It was also noted from the mentioned literature that security standards have not been applied to the mobile core network with an objective to correlate between standards and the risks. In addition, the literature did not discuss how to protect against different risks using recommended standards.

3 Mobile Network Architecture

Fig. 1 shows a typical mobile network consisting of three main parts, namely user equipment (UE), radio access network (RAN), and the core network. The UE is the closest to the users, for example, the user cellular phone. The UE has a radio connection to the RAN (also called the NodeB in a typical GSM network). An access network is an edge network where the UE accesses the core network. The RAN is then connected into the core network via a radio network controller (RNC) and into either the circuit-switched domain for voice services or the packet-switched domain for data services.

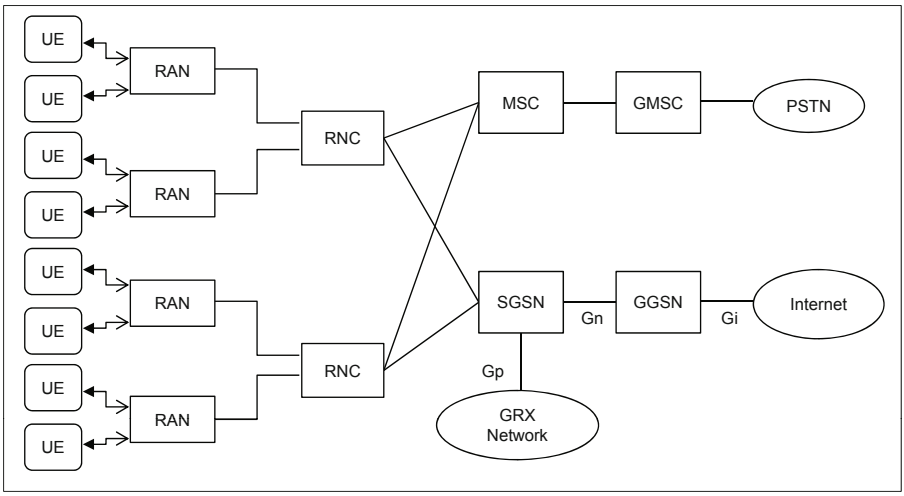

Fig. 1. Overview of the mobile communication system

In a typical 3G core network, the most important elements in the circuit-switched domain are the mobile switching center (MSC) and the gateway MSC (GMSC) which provide an external connection to an external circuit-switched network such as the public switched telephone network (PSTN). In the packet-switched domain, the serving GPRS support node (SGSN) and the gateway GPRS support node (GGSN) provide an external connection for the packet-switched network, i.e., the packet core network for data services [6]. The SGSN connects the global roaming exchange (GRX) network being a hub for GPRS connections for mobile devices. Again, this paper mainly reviews the risks on the packet core network or the packet-switched domain.

When the mobile packet core network is discussed, it is important to understand the different type of interface used at each location. We only focus three interfaces that are relevant to our work, namely Gi, Gp, and Gn. The Gi interface is the connection between the GGSN and the external network such as the Internet or the partner network. The Gp interface is the connection between the SGSN with the external GGSN for roaming partners. The Gn interface is the connection between the internal SGSN and GGSN. At the Gi interface, the protocol is purely IP based whereas the Gp and Gn protocols are carried inside the GPRS tunnelling protocol (GTP).

Mobile operators are now moving towards deploying 4G networks, commonly referred to as Long Term Evolution (LTE) [12]. LTE networks contain only the packet-switched domain and offer a large data transmission rate (over 100 Mbps). LTE introduces a significant change at the radio access network. At the core network, the system still shares many characteristics of the 3G network but without the circuit switch connection [2]. Most operators also concurrently provide the 2G, 3G, and 4G networks in which 2G and 3G networks share the same core network while a 4G network deploys a new element to the existing core network.

4 Risks on the Mobile Core Network

The mobile core network is where the different access networks are consolidated. Therefore, any risks on the core network would have a significant impact on the mobile telecommunication system regardless of technologies used for the access networks. As mobile operators concurrently provide different generations of telecommunication networks (e.g., 2G, 3G and 4G) at the packet-switched domain to their customers, any successful attacks at the core network could compromise the entire networks. In general, we classify attacks at the packet core network into three domains based on the CIA triad as follows:

4.1 Confidentiality

A confidentiality attack is usually carried out to steal information traversing the packet network [1]. This type of attack commonly utilizes a method known as a man-in-the-middle (MitM) [14]. This type of attack allows an attacker to

intercept and change data traversing the network in real time. The attack can be accomplished this using the following techniques.

- *Spoofed Update PDP Context Request Attack* – An attacker can use his or her own SGSN or a compromised SGSN to send an update PDP context request to an SGSN, which is handling an existing GTP session. The attacker can then insert his or her own SGSN into the GTP session and hijack the data connection of the subscriber. This will give the attacker full view of the data and allow modification of data compromising data integrity as well.
- *Capturing Subscriber's Data Session Attack* – Since GTP are not encrypted, an attacker who has access to the path between the GGSN and SGSN such as a malicious employee or a cracker who has compromised access to the GRX can potentially capture a subscriber's data session.
- *Internal Access Attack* – Most packet switching core networks of mobile operators are not properly protected especially the internal connection through the operators access network such as the GPRS/EDGE/3G and LTE networks. This weakness opens a potential for an attacker to compromise the core network and take full control over the operator network. Then, the attack can result in disruption to a level that could lead to significant losses for the operators.

4.2 Integrity

Another common form of attack is related to integrity. In this form of attacks, data is changed or modified without the consent of the users [1]. At the mobile packet core level integrity attacks is generally accomplished by manipulating the billing information of the subscriber. This type of attacks allows an attacker to target individual subscribers and potentially exploit them for fun or bring them into an extensive social engineering scheme.

- *GPRS Overbilling Attack* – This attack can overcharge fake phone bills to mobile users. With this attack, the attacker first connects to a server on the Internet. Then, this malicious server starts sending UDP packets (e.g., packets for video/audio streaming service). The attacker then changes his IP address, but as the connection from Internet side remains opens. Once the victim connects to the Internet and is assigned an IP address previously assigned to the attacker, the server continues sending the UDP packets (i.e., the GGSN resumes packet forwarding) and the victim is charged the malicious traffic even though the victim has not generated any traffic.
- *Billing Bypass for Free Internet Usage Attack* – Based on the MitM attack, this attack allows an attacker to use an Internet connection for free and possibly offering free or low cost of a VoIP connection.

4.3 Availability

A common type of attacks on the packet core network is the denial of service (DoS) attack causing network resources to be unavailable. The attacks could

result in prominent damage to the operator's network [13]. A DoS attack on the core network can be accomplished using the following techniques.

- *Border Gateway Bandwidth Saturation Attack* – In this attack, a malicious operator that is also connected to the same GRX network may have the ability to generate a sufficient amount of network traffic directed at the operators border gateway such that legitimate traffic is starved for bandwidth in and out of the operators network, thus denying roaming access to or from the operators network.
- *Domain Name System (DNS) Flooding Attack* – The DNS servers on the operator network can be flooded with either correctly or malformed DNS queries denying subscribers' the ability to locate the proper GGSN to use as an external gateway.
- *GTP Flood Disabling Roaming Users Attack* – SGSNs and GGSNs may be flooded with GTP traffic that causes them to spend their CPU cycles processing illegitimate data. This may prevent subscribers from being able to roam, to pass data out to external networks, or from being able to attach to the packet network..
- *Spoofed GTP Packet Data Protocol (PDP) Context Delete Attack* – In this attack, an attacker with the appropriate information can potentially craft a GTP PDP context delete message, which will remove the GPRS tunnel between the SGSN and GGSN for a subscriber. Crafting these types of attack will require that the attacker has certain information about the victim. The attacker can send many PDP context delete messages for every tunnel ID that are being used to deny multiple victims' services.
- *Bad BGP Routing Information Denying Access into Roaming Partners Attack* – An attacker who has control of a GRXs router or who can inject routing information into a GRX operators route tables, can cause an operator to lose routes for roaming partners thereby denying roaming access to and from those roaming partners.
- *DNS Cache Poisoning for Man in the Middle Attack* – It is possible for an attacker to forge DNS queries and/or responses that causes a given user's APN to resolve to the wrong GGSN or even none at all. If a long time-to-live (TTL) is given, this attack can prevent subscribers from being able to pass any data at all.
- *Spoofed Create PDP Context Request Attack* – It is well known that GTP inherently provides no authentication for the SGSNs and GGSNs themselves. As a result, the appropriate information of a subscriber, an attacker with access to the GRX, another operator attached to the GRX network, or a malicious insider can potentially create his or her own bogus SGSN, a GTP tunnel to the GGSN of a subscriber, and a false charging or distributed DoS (DDoS) attacks on the subscriber.
- *Gi Bandwidth Saturation Attack* An attacker may be able to flood the link from the Internet to the mobile operator with network traffic thereby prohibiting legitimate traffic to pass through causing a massive DoS.

– *Flooding Mobile System Attack* – If a flood of traffic is targeted towards the network (IP) address of a particular mobile system, that system will most likely be unable to use the GPRS network.

5 Addressing Risks with ITU-T X.805

To improve the security of the mobile telecommunication packet core network from the risks outlined in the previous section, we apply the ITU X.805 framework as the reference architecture [3]. As depicted in Fig. 2, the ITU X.805 network security model provides a set of principles including three layers (i.e., application, services, and infrastructure), three planes (i.e., end user, control, and management planes), eight security dimensions (i.e., access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability, and privacy), and five threats/attacks (i.e., destruction, corruption, removal, disclosure, and interruption) which can be mapped to the mobile core network in order to determine if a network is vulnerable to any attacks listed in the risk domains discussed in Section 4, and to pinpoint where such weaknesses exist and how to mitigate the detected risks.

Table 1 reviews the risks outlined in Section 4 and associates them with the threats in the ITU X.805. This mapping will help identify how the risks are associated with the recommended framework. Then, we apply the eight security dimensions of the ITU X.805 recommendation to identify suggested technologies to mitigate the threats as presented in Table 2.

Finally, we present a topological view of the mobile packet core network with the recommended protection that we have derived by using the X.805 reference model and provided the description of each recommended component.

As illustrated in Fig. 3, to protect the eight security dimensions in the X.805 framework, we propose the design of secured mobile packet core network. This

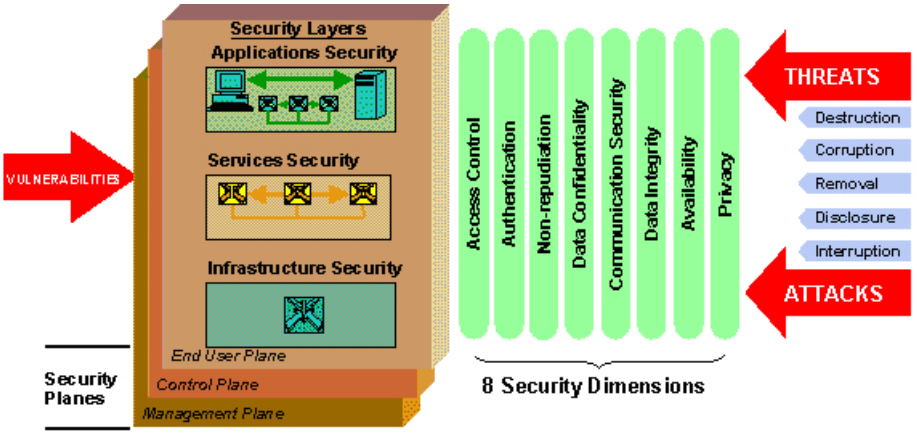

Fig. 2. ITU-T Recommendation X.805 [3]

Table 1. Mapping the Risk Domains into X.805 Threats Model

Threat	Description	Risk Domain
Destruction	Destruction of information and/or network resources	Availability
Corruption	Unauthorized tampering with an asset	Integrity
Removal	Removal or loss information or other resources	Availability
Disclosure	Unauthorized access to an asset	Confidentiality
Interruption	Network become unavailable or unusable	Availability

Table 2. Security Dimensions and Risk Mitigations

Dimension	Description	Mitigation	Threats Solved
Access Control	Only allow access to authorize system	Firewall	Destruction, Interruption
Authentication	Verifying the identity of the person or device observing or modifying data	Network Access Control system with single sign on service	Disclosure, Disruption
Non-repudiation	Provide a record that identify each individual or device that observed on modify the data	Certificate authority, identity management system	Destruction, Corruption
Data confidentiality	Data is confidential and only readable by whom it is intended	Encryption such as SSL/VPN	Disclosure
Communication Security	Data access and communication is secured	VPN / IPSec Tunnel	Interruption
Data Integrity	Data is no changed or modified	Digital certificate	Corruption
Availability	Data or access is available as needed	DDoS protection system and backup links	Destruction, Removal, Interruption
Privacy	Privacy	Encryption	Disclosure

design requires the deployment of technologies including firewall, intrusion detection and prevention (IDP) system, virtual private network (VPN) server, and network access control server.

A firewall is a device that controls incoming and outgoing traffic by analyzing the data packets based on a predefined set of rules. In the mobile packet core network, the firewall should be presented on the external boundary such as the Gi, Gi, and the internal network such as the charging, application and operations, administration and management (OAM) domain, in a form of high availability clusters. The Gi firewall protects against external attacks including DDoS attacks that originate from the Internet, while the Gp firewall must provide GTP inspection capabilities to filter traffic travelling into the mobile core

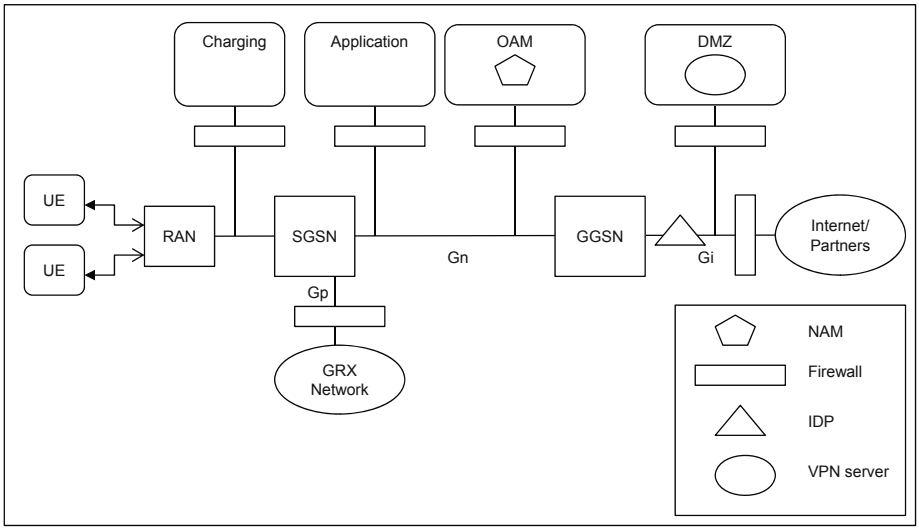

Fig. 3. Proposed secured mobile packet core network design

network from the roaming partners. Basically, the Gi and Gp firewalls act as an external defence to block against any threats coming into the packet core network. In the case of the DMZ zone (i.e., a perimeter network), the firewall for this zone can be shared with the Gi firewall. At the internal network zone (e.g., the operations support system (OSS), application, and the charging domains), a firewall must be available as the second line of defence to protect these internal systems.

The IDP system is normally the next line of defence for the mobile packet core network. The IDP system utilizes signature and entropy-based behaviour to block against attacks managing to bypass the firewall filters. This system provides the second line of defence in the most critical zone of the mobile core network. In the mobile packet network, we recommend that an IDP system should be placed behind the firewall at the Gi domain. This placement will allow the IDP system to filter any threats coming into the network from the Gi including the DMZ zone which could be compromised.

A network access management (NAM) server allows administrators to implement a single user interface to securely control every access to the network element in the mobile network. Since the mobile core network contains a large number of network elements, it is important that the access to these elements can be controlled and audited in a timely fashion. We recommend that a NAM server should be placed in the OAM domain. In addition, the NAM server must be enforced as a single interface for logging into any network elements on the mobile core network.

A VPN server allows secure remote access into the internal network by using an encrypted protocol. Every access should be passed through a dedicated VPN server since encryption and decryption can be performed at the VPN server. Therefore, the server must be placed in the DMZ zone for maximum protection.

6 Conclusion

We have mainly reviewed the security risks on the mobile telecommunication packet core network. This core network is the most important part of the mobile telecommunication system since different access networks are consolidated at the core network. Therefore, vulnerabilities in the core network could have the major impact on both mobile operators and users.

In this paper, we have identified a number of security risks in the mobile core network. Then, we have grouped the risks into three classes by using the widely used CIA triad including confidentiality, integrity, and availability classes. Then, we have related the classes to the ITU-T X.805 reference framework. Next, we have recommended the technologies which could be deployed along the framework with the objective to safeguard against the risks in the eight security domains. Finally, we have proposed the secured mobile packet core network design which is able to mitigate the risks.

This review will be useful to mobile telecommunication operators and network designers. The risks outlined in the review can be considered by the operators as the benchmark to assess their packet core networks in order to safeguard data services. Furthermore, our proposed mobile packet core network design could be applied as a guideline for improving the security of the mobile telecommunication systems. A secure telecommunication system will be able to safeguard invaluable information belonged to the mobile users and operators against the risks.

For future work, we will study a hypothetical mobile telecommunication packet core network and evaluate how attacks can be carried out on the network. Countermeasures to address the risks using the three dimensions of people, process, and technology will also be investigated and proposed.

References

1. Harmantzis, F., Malek, M.: Security Risk Analysis and Evaluation. In: IEEE International Conference on Communications, vol. 4, pp. 1897–1901 (2004)
2. Chouhan, S., Gaikwad, R.B., Sharma, N.: A Study on 4G Network and Its Security. International Journal of Computer Architecture and Mobility 1(9) (2013)
3. ITU-T Recommendation X.805: Security Architect for Systems Providing End-to-End Communication (2003)
4. Ahmadian, Z., Salimi, S., Salahi, A.: Security Enhancement against UMTS-GSM Internetworking Attacks. Elsevier Computer Network Journal 54, 2256–2270 (2010)
5. Xenakis, C., Merakos, L.: Security in third Generation Mobile Network. Elsevier Computer Communication Journal 27, 638–650 (2004)
6. Vriendt, J.D., Laine, P., Lerouge, C., Xu, X.: Alcatel: Mobile Network Evolution: A Revolution on the Move. IEEE Communication Magazine, 104–111 (April 2002)

7. Prasad, A., Wang, H., Schoo, P.: Infrastructure Security for Future Mobile Communication System. In: WPMC 2003, Yokosuka, Japan (2003)
8. Peng, X., Wen, Y., Zhao, H.: Security Issues and Solutions in 3G Core Net-work. Journal of Networks 6(5), 823–830 (2011)
9. Dimitriadis, C.K.: Improving Mobile Core Network Security with Honeynets. IEEE Security & Privacy 5(4), 40–47 (2007)
10. Xenakis, C.: Security Measures and Weaknesses of the GPRS Security Architecture. International Journal of Network Security 6(2), 158–169 (2008)
11. Bilogrevic, I., Jadliwala, M., Hubaux, J.-P.: Security Issues in Next Generation Mobile Networks: LTE and Femtocells. In: 2nd International Femtocell Workshop, Luton, UK (2010)
12. Astely, D., Dahlman, E., Furuskar, A., Jading, Y., Lindstrom, M., Parkvall, S.: LTE: The Evolution of Mobile Broadband. IEEE Communications Magazine 47(4), 44–51 (2009)
13. Ricciatoa, F., Colucciaa, A., D'Alconzo, A.: A Review of DoS Attack Models for 3G Cellular Networks from a System-design Perspective. Elsevier Computer Communications Journal 33, 551–558 (2010)
14. Meyer, U., Wetzel, S.: A Man-in-the-Middle Attack on UMTS. In: Proceedings of the 3rd ACM Workshop on Wireless Security (2004)