Scientific Research

Security Architecture and Defence Strategy of 3G Mobile Communication System*

Xinhe HU[1], Boxiong YANG[2], Ling LV[1], Ying CHEN[1]

[1]*Computer Department, Xianning Profession Technology College, Xianning, China*

[2]*State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, Wuhan, China*

Email: hxhhb999@163.com, ybxemail@163.com, lvling123@163.com, chenying2000@163.com

Abstract: Higher requirement for security of mobile communication system is put forward with the development of 3G. The threatening origin of 3G mobile communication system has been introduced, and the security architecture of 3G is set forth in the paper. Meanwhile, the security strategy of dignity secrecy, entity authentication and data integrity adopting in the 3G system have been deep researched and discussed in order to provide reference for the security technology development of 3G mobile communication system.

Keywords: 3G mobile communication system; security architecture; defence strategy; entity authentication; dignity secrecy; data integrity

1 Introduction

Third-generation mobile communication system (3G) in the security technology is based on GSM. When the mobile communication has become a favorite mean of communication step by step, 3G will provide users and servicers more reliable security mechanism [1].

3G system dues to integration of wireless communications and internet technology, and thus its security system also will be the integration of a variety of different security methods. 3G security will be applied to the internet in a variety of sophisticated encryption technology, various international organizations (such as the WAP Forum and the IETF, etc.) will also be in the 3G-security solutions to make contribution more [2].

2 Mobile Communication System Security Threats

3G networks from the core network perspective are actually IP networks. From 2G networks to 3G networks, is actually from a closed, based on circuit-switched systems to open IP-based network transformation. 3G networks which control signaling and data transmission have become increasingly dependent on IP networks. Thus, 3G networks and mobile communication network than the previous, more of the characteristics of IP networks, mobile communication IP networks are being transformed into a special application. The openness of IP network security issues arising from 3G networks is the main security issues to be faced [3].

1) IP network vulnerabilities Obviously, for the purpose of exploits increasingly strong, and time is short, enterprises are faced with an increasing risk that these changes to the telecom operators increasing the risks of

2) IP Internet, the spread of the virus attack that time is short, how to protect networks from virus 3G has become the operators to 3G transition must be addressed [4].

3) 3G users are using more and more IP-based mobile terminals. From the functional point of view, 3G mobile phone is actually a data terminal, with the basic characteristics of the data terminal, and then access to the IP-technology as the core of the 3G network, will have more chances of contracting the virus or hacker intrusion programs. Terminals more intelligent, more complex functions, the more inevitable its security vulnerabilities, hackers or virus infected the greater the possibility of capture. These terminals are dangerous in themselves, while the threat to the 3G network is growing.

4) An important feature of 3G networks is the 3G terminal is always online. This will inevitably face a direct security threat, virus or hacker attack is less likely to be discovered and, after treatment, even if the deal will also be a long, huge project. Such terminal equipment hidden security vulnerabilities on a more sustained and longer harm [5].

5) 3G can provide users with more than 2Mbps access speed, while the signal coverage area to achieve soft switching, access speed improved and access sites, applications, leading to constantly changing network of various parameters are constantly changing, making the security of the mobile terminal monitoring and management more difficult. Once the mobile terminal to become the birthplace of viruses and hacking programs or relay stations, access network and core networks and 3G networks carry the business system will directly face security threats.

6) As for the 3G security objectives and related work norms lag, 3G network security management and related systems are also relatively short, 3G specification de-

*Granted specially by key project of education science "Eleventh Five-Year" plan in Hubei province. Code: 2009A101

978-1-935068-12-9 © 2010 SciRes.

scription and requirements for security is clearly insufficient. For the 3G networks, the lack of security requirements for the future operation of the network will be leaving a number of hidden dangers.

7) With network convergence (triple play) trend to deepen, the increasing complexity of telecom services, 3G networks will face more than ever the threat of severe [6].

3 3G Security Goals

For carrying the mass application of telecommunications networks, any one network and information security vulnerabilities and attacks being used, are likely to carry a devastating impact on businesses. As telecommunications development impact society as a whole growing, the role of universal service from the point of view, through the telecommunications network to ensure the safety of the state and society and thus to guarantee the security and stability is undoubtedly the basis of the obligations incumbent telecom operators.

According to CDMA network infrastructure, 3G Network security level can be divided into the network layer and application layer two main parts (**Figure 1**): pairs of 3G in the user equipment (UE), Radio Access Network (RAN), Core Network (CN) and business networks (Service) protection can be included in these two levels, respectively. In 3G systems, they have their different effect on the network security implications and requirements vary [7].

From the perspective of understanding of telecom operators, 3G network security work at least to include the following:

1) Ensure the 3G network and its hosted business systems to provide continuous services; guarantee constitutes a telecommunications network to all facilities, systems, and the data processing system in normal working condition [8].

2) 3G applications on the network security information (user information, data, a variety of transactions) in the context of controlled transmission, that is, effective control of the scope and means of dissemination of information to prevent the unauthorized disclosure of important information to the telecommunications companies outside the organization or personnel to protect the information assets confidentiality, integrity, available [9].

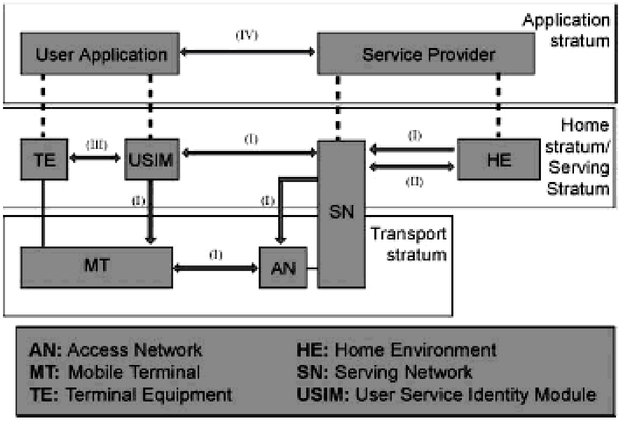

Figure 1. 3G security architecture

4 Thinking of Building 3G Security System

1) Improve the robustness of the network itself to ensure network security incidents having adequate disaster recovery capability.

Development of the Internet is based on a flexible and open IP protocol IP protocol based network and communications equipment produced as well as related applications, for today's rapidly growing popularity of the Internet business foundation. But it was precisely this openness, making it a carrier-class operation network, security and reliability is weak and can not guarantee the quality of service problems are gradually emerged at the same time due to lack of technical standards for Internet security, many Internet systems and equipment, difficult to achieve the traditional telecom level stability.

The robustness of the network itself is the operator's network to provide continuous service basis. For the Internet network security, than any other traditional network of technical standards, the current IP network security technology standards in a relatively primitive state of operability is not very good, technical prevention system is not perfect, there is no unified and standardized device management, security domain there is no uniform principles of classification. Operators, equipment reliability, how to start a network to improve network stability and the ability to prevent risks are to become the first 3G network security issues.

2) Good terminal access management, risk control terminal to a certain extent

Operational experience from the Internet, 80% of network security risks from the business end, the business management is a 3G terminal in the important part of the security system. Using terminal equipment in 3G network security system is a protected object and an important information asset. It is also the source of the virus and attacking the source of the object is a need to focus on prevention.

In 3G networks, the face of hundreds of millions of terminals, according to traditional methods, with limited intrusion detection and traffic, protocol filtering equipment for protection, no doubt drop in the bucket. 3G user terminal equipment, safety and security, will depend largely on the terminal itself, the security features, which is divided into the basic objectives of security domains. And certification of user terminals similar to 2G, for 3G terminals must carry safety certification through the state of online security surveys and assessments, to meet the requirements of the terminal to allow access terminals that do not meet the requirements restricting the use of function, only allows access to given limited resources, and try to perfect the security, may pose a threat to the network terminal in the 3G network access layer to be controlled in order to achieve proactive security defense.

3) Doing a good job on the application layer isolation and protection

In 3G systems, in addition to providing traditional voice business, e-commerce, e-commerce, network services and other new 3G services will become an important business development point, so 3G will give more consideration to the application layer to provide security protection mechanisms.

In 3G systems, the focus of security has been transferred from the physical layer to the network layer and application layer, from the traditional voice communication security as the core transferred to the IP network and application security as the core. In accordance with the contents of business applications into logical private network is a 3G network, the basic requirements for security management, but also an inevitable requirement.

Demarcation of the logical private network is based on different business special network SLA requirements, encryption, authentication, border protection and the means for the deployment of application-layer security. In the robust and flexible security system, the deployment of security measures to achieve centralized management, ease of SOC (Security Center) to quickly grasp a variety of events, vulnerability, rapid and effective deployment of security measures and early warning to ensure that arise due to security incidents the consequences can be effectively controlled level of the affected areas. Logical private network (security domain) division is “the edge of deployment, centralized management” approach for the best basis.

5 Conclusions

Relative to the second-generation mobile communication system, for the 3G system’s security should be given adequate attention. Conducting 3G system security system, not only to inherit the second-generation mobile communication system in the security management concepts and have been shown to be necessary and robust means of security, but also according to IP-based 3G networks the actual technical requirements, and continuously targeted to increase security measures to compensate for the current IP network security system defects. With the advent of 3G networks large-scale construction, all operators must at the same design, simultaneous construction, synchronous operation 3G network security system to ensure network quality, efficient, safe operation, business and timely and smooth launch.

References

[1] 3GPP Technical Specification 33.102, 2000. 3G security architecture[S].

[2] 3GPP Technical Specification 33.103, 2000. 3G security: Integration Guidelines[S].

[3] 3GPP Technical Specification 25.401 (v3. 10.0). UTRAN Overall Description J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., Vol. 2. Oxford: Clarendon, 1892, pp. 68-73.

[4] Deswarte, Y., Blain, L., Fabre, J. C.: Intrusion tolerance in distributed computing systems. In: Proceedings of the 1991 IEEE Symposium on Research in Security and Privacy. (1991) 110-121.

[5] Amir, Y., Kim, Y., Nita-Rotaru, C., Schultz, J., Stanton, J., Tsudik, G.: Exploringrobustness in group key agreement. In: Proceedings of the 21th IEEE International Conference on Distributed Computing Systems. (2001) 399-408

[6] Ateniese, G., Steiner, M., Tsudik, G.: New multi-party authentication services and key agreement protocols. IEEE J. of Selected Areas on Communications 18 (2000) 42.

[7] 3GPP Technical Specification 33.900, 2000. 3G secrutiy: A guide to 3rd Generation Security [S].

[8] Xenakis C, Merakos L.Secruity in third generation mobile networks. Computer Communications, 2004: 27(7): 638-650.

[9] Akyildiz I F, Su W Wireless Sensor Networks: a Survey. Computer Networks, 2002, 38(4): 393-422.