International Journal of Future Generation Communication and Networking
Vol. 8, No. 2 (2015), pp. 317-330
http://dx.doi.org/10.14257/ijfgcn.2015.8.2.26

Research on Users' Privacy Protection in Mobile Communication

Ganqiang Lu[1], Caixia Liu[2] and Qing Zhang[3]

National Digital Switching System Engineering & Technological Research Center
Zhengzhou, Henan 450000, China
[1]luganqiang@163.com, [2]lcxtxr@163.com, [3]feiying910103@163.com

Abstract

With the rapid development of communication technology, mobile communication network integrates with internet constantly and forms mobile internet. The mobile communication system tend to be IP-based, mobile terminals tend to be intelligent, application of APP becomes more and more popular, intelligent applications make people's life more convenient. But, there are huge security threats hidden in current mobile communication, the security of users' privacy information in mobile communication, such as users' identity, location information, business routing, arouse more and more widely attention. This paper introduces related researches and problems of users' privacy protection in current mobile communication, and discusses to apply the idea of active defense to the security mechanism for better protection of users' privacy information.

Keywords: *privacy data, security protection, active defense, mobile communication*

1. Introduction

As is shown in the latest report about the development of china mobile internet, the number of cell phone netizen has been reached 500 million by the end of 2013, and continue to be the leading internet terminal. The continuous growth of cellphone netizen promotes the development of various kinds of cellphone application. Cellphone is still the major growth power of netizen in china. With the further popularization of 3G network, the commercialization of 4G networks, and the development of smart phone and wireless network, social network platform have been developing rapidly and mobile terminal applications, such as shopping online and group purchase, also have an obvious growth.

Modern communication technologies change the way of traditional life, the possibility of people directly involved in the information interaction has been greatly enhanced, people's life become more convenient. But, there are lots of privacy information interacted in the process of mobile communication. Reference [1-6] shows that it's very important to ensure its security and how to protect the security of users' privacy information has attracted widespread attention. Virus in cellphone has been emerging endlessly, since the world's first cellphone virus appeared in 2004. Its hazards involved malicious deduction, stealing privacy, and mad message. The undercover software appeared in 2010 can send communication record and confidential information that stored of cellphone users to specified monitoring site. These malicious events threatened the communication security of users' privacy. Meanwhile, it not only destroyed the social harmony and stability, but also posed a threat to national security. Reference [7] the popularity of intelligent terminals and the maturity of mobile application environment bring a bright prospect for mobile P2P networks. In recent years, the security of cellphone users' privacy tend to be more severe with the widely use of mobile applications, and we are facing with the risk of privacy disclosure whenever and wherever you are. For example, the navigation software need to share our location information in real-time when we use it, which reflect the users' behavior path. If the software are attacked, the user will

ISSN: 2233-7857 IJFGCN

be followed, which cause the leak of users' location privacy.

Currently, the mobile internet environment has been deteriorating, the upstream links, such as cellphone shops, BBS and download site have been polluted, which speed the infection of downstream users. There are more than 703 thousands new mobile internet malicious programs in 2013, increased 3.3% compared to 2012. In addition, new technologies and internet business, such as cloud computing, mobile internet and social network, change the way of collecting and using personal information, which makes the security of personal information less controllable and the potential threat of personal privacy information leak intensified. For example, the use of cellphone number as the unique identifier account in applications becomes more and more common. Reference [8] shows that researches carried out by Schrittwieser showed that it will bring a lot of security problems.

The security mechanism of mobile communication has been improved after several generations development, and to some extent, it can protect users privacy. But, it still is a passive defense mechanism, and reference [9] shows that there are a lot of security vulnerabilities which can’t ensure absolute safety of users’ privacy information. Therefore, a new security mechanism is needed to adapt to the rapid development of mobile communication technology, the defender need to game with the attacker actively so that users’ privacy information can have a better protection. This paper makes an overview of the existing security mechanism of privacy protection, and introduces the active protection technology, and discusses the application of dynamic defense mechanism to privacy protection in the mobile communication.

2. Privacy Data in Mobile Communication

Privacy data is very important information related to users’ identity, including mobile station integrated services digital network number(MSISDN), international mobile subscriber identification number(IMSI), user's location, and so on, which is transparent associated storage and use in multiple equipment in mobile communication network.

Nowadays, with the development of communication technology, mobile communication can provide value-added personalized service basing on user's privacy information，such as identity information, location information, and so on. As the credentials for users to access and use network resource, the privacy information must be well protected by the system.

However, the current reality is not optimistic. The communication systems are facing many conflicts and contradictions, such as content supervision and content diversity, user’s convenience and privacy data security. If lacking of effective supervision, greater security threat will be brought to user. Therefore, the security of user’s privacy data existing in mobile communication network arouses more and more widely attention, it is necessary to take measures to protect the security of privacy information better.

3. Hidden Danger of Privacy Data Security in Mobile Communication

Great changes have taken place in the way of our life, with the rapid development of mobile communication technology, the mobile terminal become intelligent, the mobile application platforms become diversity. Nowadays, people almost can't live without cellphone in daily life. Cellphone has taken up much of people’s time and energy. More importantly, there is a huge hidden risk of privacy information security, while user enjoying the convenience of intelligent terminal. Security events disrupt the security environment of global information, and network space, as the fifth dimension of the world today, its security is the greatest security issue human facing today. Therefore, it’s imminent to solve the security problem of users' personal privacy information in mobile communication. There are many reasons that caused the leak of users’ privacy information in mobile communication, which can be basically divided into two categories.

One is passive information leak, the other one is active information leak, which caused by people's personal behaviors.

3.1. Information Leakage in Mobile Communication

Nowadays, the applications of mobile terminal become more and more popular, with the rapid development of APP. However, many mobile applications are not credible or less credible, which make a lot of threat hidden in the process of mobile communication. Reference [10] shows that these threats cause the leakage of user privacy in mobile applications.

Mobile users sometimes also unconsciously leak personal privacy information actively, in addition to the security problem of mobile application platforms and malicious attacks. Figure 1 shows that we like to share our personal privacy information, such as our location information in real-time, when we use some chat software or social platforms on mobile terminal, such as QQ, Twitter, Facebook, *etc.*, which leak our personal information virtually. With the benefit of the convenience of mobile application platforms, some APP platforms even require user to bind their personal privacy information, such as mobile phone number or others, when registering on it, which increases the possibility of privacy information leakage virtually. It will cause greater harm to users, if these data is utilized by criminals. At present, people pay more and more attention to information of identity and location. With the help of big data platform and data mining technology, the information of personal privacy, such as users' identity, users' behaviors and social relation network, can be analyzed dynamically, by collecting and analyzing the vast amounts of data of mobile users on social platforms. Therefore, consciousness should be strengthened to protect personal information from being leaked.

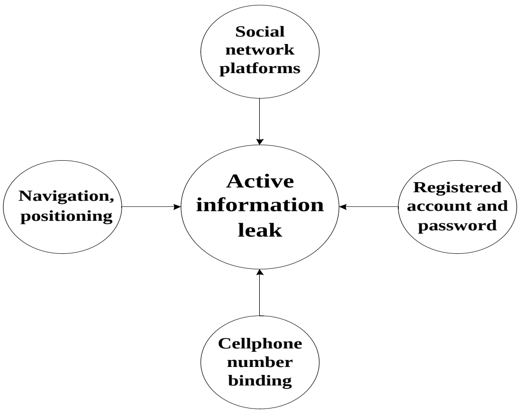

Figure 1. Active Information Leak

In terms of the mobile communication network, there are several security vulnerabilities in the storage, management and use of private data, which causes the leakage of mobile user's privacy data. These privacy data is transparent associated storage and use in the core network equipment of mobile communication, and is associated binding when transmitting signaling on mobile transmission route, which is easy to be obtained by some technique, such as backdoor, Trojans, route intercept, and so on.

Therefore, privacy information can be checked, if attackers obtain user's mobile phone number, as they are bare associated storage, and can be seized easily by attackers for correlation analysis, as they are transparent associated transmission. Moreover, it's difficult to ensure the securities and controls of users' private data, as they are widely binding distributed. More importantly, as the multinational operations in mobile communication network, mobile users' privacy data will be transmitted on the international signaling pathways and stored or used in the overseas operator networks, if user roaming abroad, which makes the security of private data more severe to be guaranteed.

4. Related Research Work of Privacy Data Security in Mobile Communication

The main security threats of mobile communication systems come from the weakness of network protocol and system. The attackers can take advantage of these weaknesses for unauthorized access to sensitive data and interference or abuse of network services, which cause losses to the resources of user and network.

How to identity users' identify effectively and not leak users' privacy information to other irrelevant networks, has been received extensive attention in mobile communication. As early as 1994, IBM has applied for a patent that a method and device for mobile users' secret identity in communication network, which put forward a camouflage international mobile subscriber identification number to avoid IMSI privacy leaking, which show that United States has already make a deep research into the information protection of users' sensitive privacy security in mobile communication network. Reference [11-13] shows that over the years, scholars have invested a lot of energy in IMSI confidentiality of air interface in mobile communication network. For example, southeast university proposes a protection method for IMSI privacy information in 3G access in 2013, with key ID and key groups. Users' IMSI privacy information will be output in the form of cipher text after being encrypted to avoid IMSI privacy information leaking in air interface. Reference [14] shows that railway university of Shijiazhuang proposes a method that location privacy preserving for semi-honest users in location based services (IBS), to seek a better protection for users' privacy information of location. Reference [15] shows that, several measures have been taken to protect the security of users' privacy information from different angles in mobile communication in nowadays, such as authentication, encryption, *etc*.

4.1. Security Mechanism of GSM

The developments of mobile communication systems have experienced from analog communication to digital communication, of which the most striking one is GSM. GSM is the first generation of digital communication system. Figure 2 shows the typical structure of GSM system.

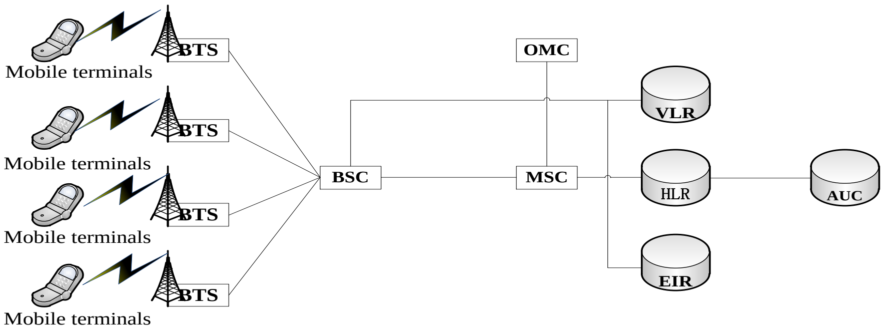

Figure 2. The Structure of GSM System

GSM system has realized two security goals. One is preventing the unauthorized user from accessing to network the other is protecting users' privacy. In order to prevent the attacker from disguising as a legitimate user to carry out attacks, authentication mechanism is used to authenticate users' identity in GSM. Figure 3 shows the process of authentication in GSM network, only the networks authenticate on mobile stations and mobile stations can't authenticate on networks, due to the one-way authentication mechanism in GSM network. Whether to open the encryption function or not is decided by the network. Therefore, attackers can use a fake base station as a legal network for terminals, to implement the middle attacks.

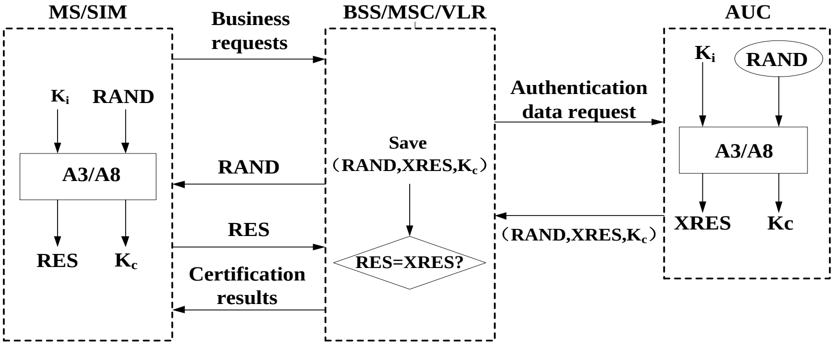

Figure 3. The Process of Authentication in GSM Network

In order to protect the privacy of mobile user, temporary mobile subscriber identity (TMSI) is used to mark users in the access network of 2G, just like GSM, IMSI information isn't leaked to unauthorized individuals, entities and procedures. TMSI updates and changes constantly, and will be encrypted when transmitted, which have been protected the security of users' IMSI and location information to some extent. Although IMSI is protected by TMSI, it also will be transmitted in plaintext in the air interface when first access to the network or the visitor location register (VLR) lost user's information. Therefore, the hidden danger of privacy information leakage can't be eliminated in GSM. In the core network of 2G, there is no authentication mechanism between devices and no protection mechanism of information confidentiality and integrity. Therefore, the one-way authentication mechanism of GSM can't prevent middle attack and fake base station from attacking. In addition, the system itself does not provide end-to-end encryption, user's data and signaling lack integrity protection mechanism.

4.2. Security Mechanism of 3G

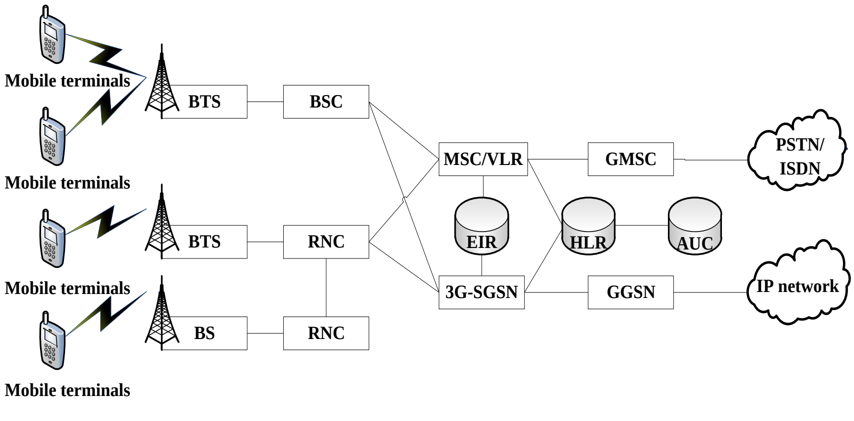

Figure 4. The Architecture of 3G Systems Network

The mainly business of 2G is to provide voice services, and the security design of 2G is mainly aiming at voice business, which makes the security mechanism lack consideration of protection for data confidentiality and integrity in 2G. According to the security characteristics and weaknesses of 2G, the security design of 3G is enhanced, and provides some new security services. Figure 5 shows the security structure of 3G systems. According to 3GPP standard, 3G is divided into five security domain, such as access security, network security, user security, application security and visibility and configuration of security, to guarantee the security of user's privacy information from every aspect.

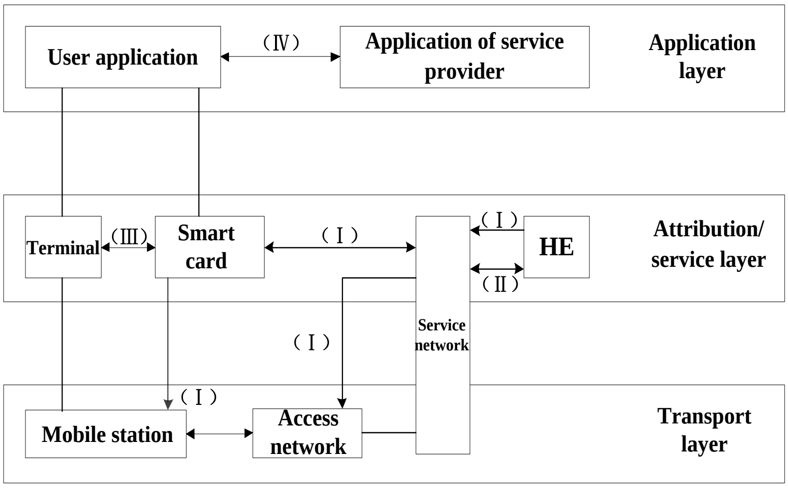

Figure 5. The Security Structure of 3G Systems Network

In order to overcome the security weaknesses of 2G, bidirectional authentication is adopted in 3G. Figure 6 shows the authentication and key agreement (AKA) mechanism of 3Gsystems.

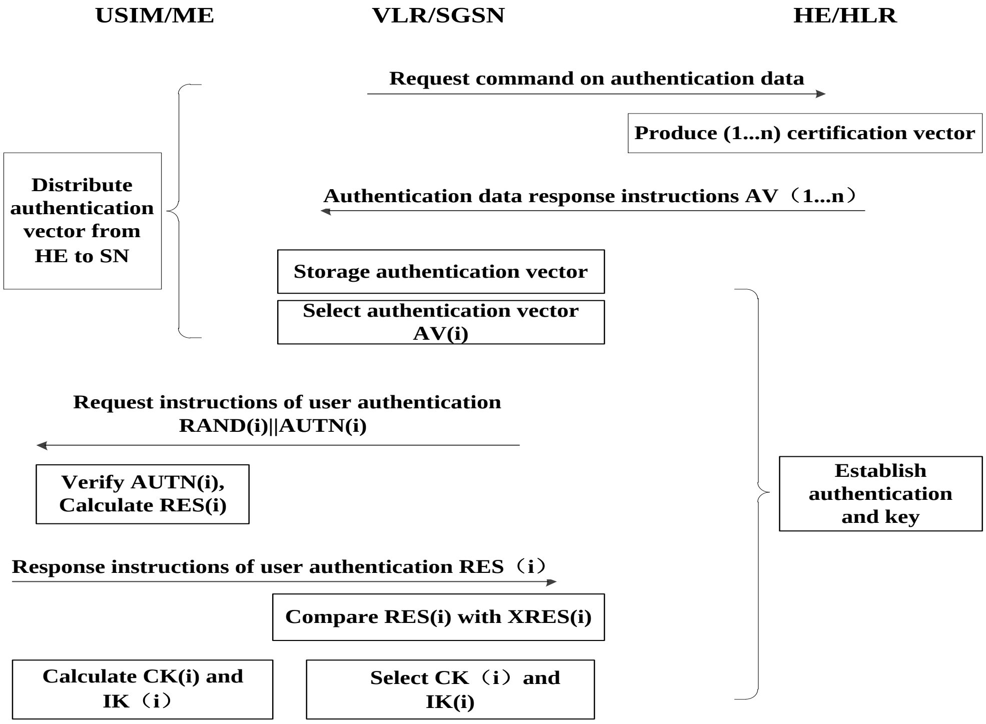
USIM/ME
VLR/SGSN
HE/HLR
Request command on authentication data
Produce (1...n) certification vector
Distribute authentication vector from HE to SN
Authentication data response instructions AV（1...n）
Storage authentication vector
Select authentication vector AV(i)
Request instructions of user authentication RAND(i)||AUTN(i)
Verify AUTN(i), Calculate RES(i)
Establish authentication and key
Response instructions of user authentication RES（i）
Compare RES(i) with XRES(i)
Calculate CK(i) and IK（i）
Select CK（i）and IK(i)

Figure 6. The Authentication and Key Agreement (AKA) Mechanism of 3G

AKA realized the bidirectional authentication between user and network, and will provide the encryption key and integrity key after authenticated, to prevent attacks from fake base station. As SQN can leak users' location and identity information, AK or is used to hidden SQN.

Figure 7 shows the encryption mechanism of 3G systems in air interface, and Figure 8 shows the integrity protection mechanism of 3G systems in air interface.

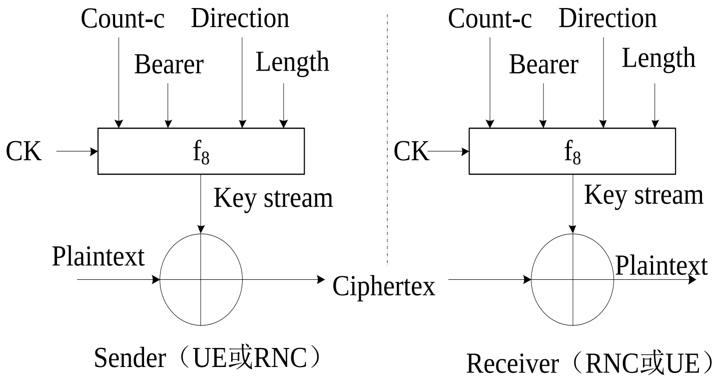

Figure 7. The Encryption Mechanism of 3G in Air Interface

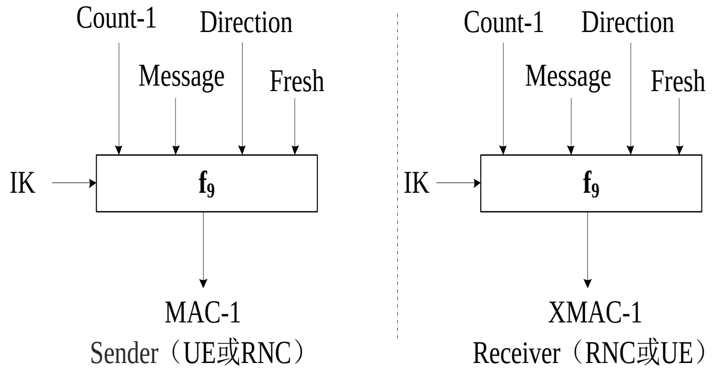

Figure 8. The Integrity Protection Mechanism of 3G in Air Interface

In air interface of 3G, the length of the key is extended. The data transmitted will be encrypted using encryption key CK, and the integrity of data will be protected using integrity key IK. 3GPP defines f8 algorithm to implement encryption mechanism of air interface, and f9 algorithm to implement data integrity of air interface. What's more, reference [16] shows that the encryption range is extended from base station to core network in 3G, and security mechanisms, such as MAPSec, TCAPSec and IPSec is added in core network. Compared to 2G network, IMSI isn't transmitted in plaintext in the wireless link, and the confidentiality protection of user's identity has been improved greatly. Due to 2G and 3G networks coexists with each other, 3G is still likely to transmit IMSI in plaintext in air interface in order to compatible with 2G, which makes some safety measures in 3G network difficult to play a role. Therefore, many safety problems still exist for a long time. Although the protection for user's privacy information has been enhanced in the air interface of Long Term Evolution (LTE), but, the problem that IMSI may be accessed in plaintext still haven't been solved.

4.3. Security Mechanism of 4G

Global unique temporary identity(GUTI) assigned by mobility management entity(MME) to users, is used as user temporary identity in the 4G system, which is effective only within the scope of its MME. Similar to TMSI, GUTI is also binding with user's IMSI. However, the correlation matching between IMSI and TMSI will not exist in communication network and IMSI will be used to indicate user's identity when UE starting up, during which IMSI is transmitted in the plaintext in the air interface and IMSI may be leaked in this process.

In order to achieve the smooth upgrade of communication system, AKA is continue to be used in 4G security mechanism. More attention, reference [17] shows that the protection for signaling integrity only stays on the control layer, and protection for privacy data in user layer will not be provided.

4.4. Analysis of Security Mechanism in Mobile Communication

The security problems of mobile users' privacy exist in each link of the communication process. From the prospective of security mechanism in mobile communication system, measures are adopted to protect users' privacy in order to ensure the safety in GSM, such as authentication, encryption and TMSI. Authentication can prevent the unauthorized illegal users and terminals from accessing to network, encryption can resist the hacking attacks in air interface, TMSI can prevent the leakage of users' identity information and location information through constantly updates. The security mechanism of GSM has played an important role in the protection for users' privacy information, while its security vulnerabilities are also clearly. For example, an attacker can disguise as a legitimate member of the network to steal user's information, an attacker could also carry out attacks by replaying, deleting and tampering as the lack of data integrity protection. Due to the fact that there is no key update mechanism in GSM, encryption is easy to be cracked, so the security of algorithm is low. Moreover, the encryption function is not extended to the core network, the system lacks security predictability and IMSI may be leaked.

In view of the security defects in 2G, 3G enhances the security mechanism and improves many security vulnerabilities existing in 2G. The authentication technology is promoted from one-way to two-way in 3G, which makes the protection of users' confidentiality being improved large. The integrity protection of signaling data is increased, which makes the data transferred have a better protection. Moreover, the encryption algorithm is enhanced and operation with safety and visibility is also provided in 3G. User can always check your own security model and security level. Although the security mechanism of 3G has been improve greatly compared to 2G, but there are still many safety risks. For example, the two-way authentication in AKA is incomplete that it only happened from service network to terminals and from terminal to home location. There is no authentication from terminals to service network, which make the system suffer redirection attack easily. The integrity protection of data is only for signaling data and not for user's data. More importantly, the plaintext transfer of IMSI is still exists in 3G when users' VLR can't gain user's data.

LTE is a flat network architecture based on IP, which reduces the nodes in the access network that there are only eNB (Evolved Node B) Node and the eNB area is not considered completely credible. Therefore, the security of LTE is divided into access layer and non-access layer. In the mechanism of LTE, mark of service network will also be transferred when users sending request of authentication to HSS, which makes the authentication from service network to terminals come true indirectly. Moreover, the resynchronization faults of SQN are improved, the levels and length of key are increased, the protection for user data in air interface is enhanced and the ZUC algorithm is increased in LTE, which makes the security of optional encryption algorithm higher. Although, the security system of LTE has been very perfect, but problems that IMSI may be access clearly and root key fixed still be unresolved. As LTE considering base station node unsafe and the compatibility and coexistence of various access ways, such as 2G and 3G, so the potential security threats to users' privacy data is still very great.

According to current security mechanism, there is almost no any security mechanism in 2G core network, and security mechanisms, such as MAPSec, TCAPSec and IPSec is added in core network of 3G and 4G. But, mechanisms, such as MAPSec and TCAPSec, are rarely deployed in the existing mobile communication, because of the complexity of implementation. Therefore, the existing security mechanisms can't compensate the security weakness of mobile data in storage, management and use. The security threat to user's privacy information will be more and more heavily, as the deeply fusion of mobile and internet, the multinational operation and the cross-communications operators operation. Moreover, the systems are facing inherent security issues of IP with the introduction of IP technology. Thus, the traditional passive defense mechanisms, that implementation of signal detection and access control are based on anomaly characteristics, are unable to protect the security of users' privacy data effectively.

5. New Research Thought on Privacy Data Security Mobile Communication

The privacy data security of mobile communication is not only personal information security, but also national security to some content. A smartphone always operates general operating system with open interface, which can install new applications freely. The emergence of smartphones has enriched the types of mobile applications greatly, which also create favorable conditions to cellphone virus breeding. To some content, the spread of cellphone virus is a derivative of cellphone intelligent, which is a serious threat to mobile communication security.

As personal items in people's lives, mobile terminals carry too much personal privacy. If the mobile terminals are lost or infected by malwares, it can lead to the leakage of privacy and sensitive information. In order to protect the privacy information of mobile user, the existing mobile terminals have taken some safety measures, such as antivirus software, privacy encryption and firewall and so on. For example, antivirus software detects and blocks malwares and malicious mobile codes, and performs automatic and real-time elimination to malware. In addition, the virus can be upgraded through loophole mining technology.

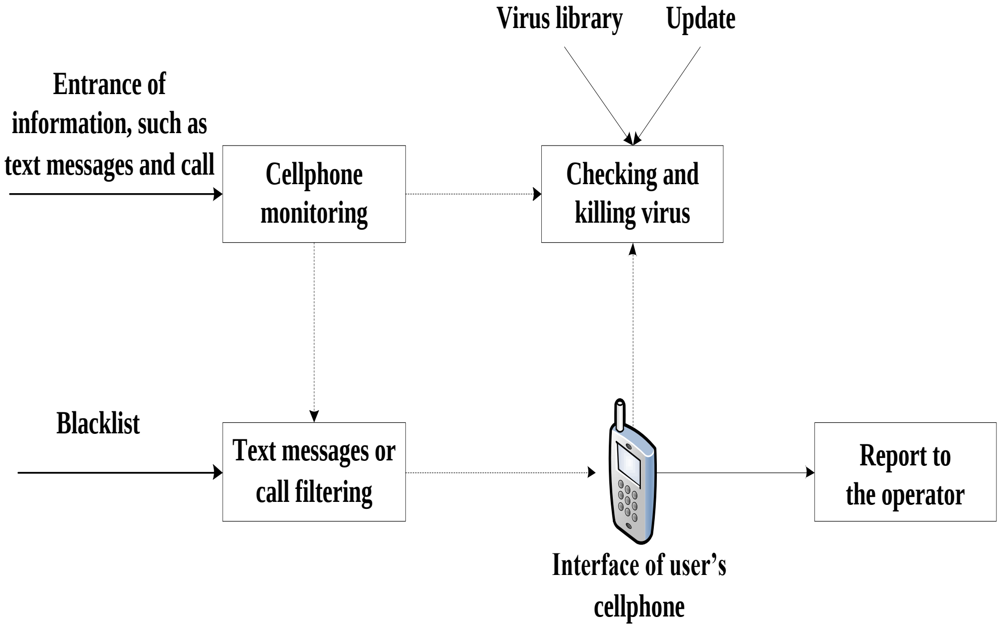
Virus library
Update
Entrance of information, such as text messages and call
Cellphone monitoring
Checking and killing virus
Blacklist
Text messages or call filtering
Report to the operator
Interface of user's cellphone

Figure 9. The Structure of Traditional Cellphone Security Defense

The ideal goal of vulnerability discovery technology is to detect the vulnerabilities totally automatically and to adjust adaptively and scholars have proposed many methods to achieve it. Reference [18-19] shows a new fuzzy method using multi data samples combination and a model-based vulnerability analysis of IMS network. But, the protection of traditional security defense system for user's privacy information is passive and there are still many weaknesses. The limitations of the existing security measures are shown in Table 1.

Table 1. Limitations of the Existing Security Measures

Characteristics of attack recognition	Unable to cope with continuous dynamic attacks
Patch	Ensure timeliness is difficult
Remove vulnerability or backdoor	Engineering is difficult

The passive protection technology can't meet the security needs of user's personal privacy, with the severe security situation. Therefore, revolutionary technology of mobile security defense is needed, and it's imminent to research active protection technique, method and related technology.

5.1. Proactive Protection Technology

Proactive protection technology makes the attacker can't complete attacks to booking targets, with the existence of some mechanism. Proactive protection isn't dependent on prior knowledge, and has been developed rapidly in computer network security in recent years. Reference [20] shows that the main idea of proactive protection in computer security field is that, it isn't judge a virus according to characteristics of virus code, but from the original definition of virus that based on independent analysis of program behavior to protect in real-time directly. Proactive protection technology take all kinds of protection measures to make attackers not achieve the desired purpose, while enhancing and guaranteeing the security of local computer network. Reference [21] shows that proactive protection makes security protection of computer information network enter a new era, and is also considered to be the future development direction of network security protection. Reference [22] shows that proactive protection technology includes machine learning, neural network, genetic algorithm, and so on. Moreover, game theory is introduced in information security field, to research on attack and defense. These intelligent algorithms provide optimum paths of strategy adjustment.

Proactive protection technology is composed of multiple technologies that can realize network security active defense function, and realizes perfect network security defense system through reasonable organic combination. The Moving targets defense (MTD) putted forward by United States and mimicry security defense (MSD) proposed by china represents the new direction current computer network active defense field. If the thought of proactive protection technology is applied to privacy data protection in mobile communication, the existing security mechanism will be improved greatly.

5.2. Moving Targets Defense

As a revolutionary technology of cyber space, that will change the rules of game, MTD is completely different from previous research idea on network security, which doesn't seek to establish a perfect system to against attack. Instead, MTD is dedicated to build a dynamic, heterogeneous, uncertain network to increase the attack difficulty greatly. Reference [23-26] shows that the present specific techniques of MTD mainly include variable of channel number, routing and IP security protocol channel, the randomization of host identity, address space, instruction set and Store data. Reference [27-30] shows lots of new progress about MTD technology. Figure 10 shows several new progress of MTD in recent years.

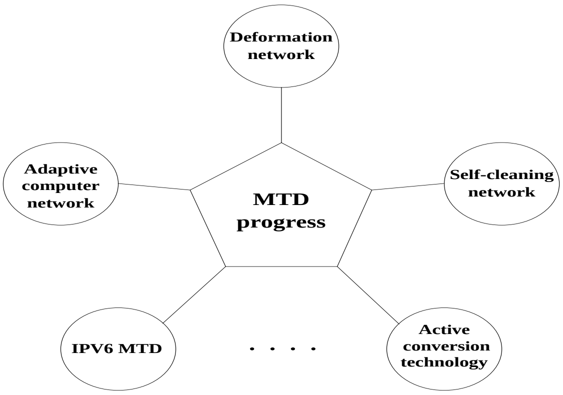

Figure 10. New Progress of MTD

5.3. Mimicry Security Defense

Mimicry security technology utilizes bionics. Figure 11 shows the structure of mimicry environment establishment.

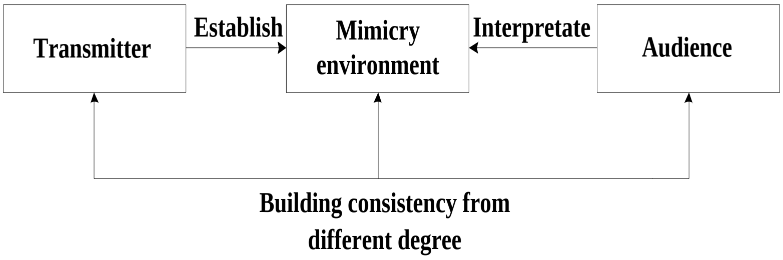

Figure 11. The Structure of Mimicry Environment

The concept of mimicry security defense is based on mimicry calculation, and the essence of mimicry calculation is the functional calculation structure. Mimicry computer designed according to mimicry calculation, relies on dynamic variable structure and the combination of hardware and software to realize the calculation based on efficiency, which changes the theory of classical computer that the perform structure is fixed and calculates by software programming. MSD aims to enhance the uncertainty of running environment or perform structure and implements mimicry environment by active jumping or migrating with functional equivalence condition of computation or processing structure, and changes the system architecture randomly in the way that defender can control. Therefore, MSD makes it difficult to observe and forecast for attacker. MSD don't try to eliminate all loopholes, backdoors, Trojans or viruses, but reducing the security risk in term of architecture technology level, so as to double the attack difficulties. The essence of MSD is to change the static, deterministic and similarity of environment that system performing or running.

6. Conclusion and Prospect

With the rapid development of mobile internet technology, many security problems of internet is brought into mobile communication network, while mobile internet bringing us conveniences. In addition, new security mechanism is needed although there are many security mechanisms in the existing mobile communication, as the security threats is changing. The security of users' privacy information has aroused widespread concerns, with the widely application of APP. At present, the research methods of mobile internet leak protection is almost all concentrated on the find and repairs of leak in intelligent terminal, and very little from aspects of network protection.

Passive defense technology is based on prior knowledge and can't against being attacked timely that utilizing unknown vulnerabilities or backdoors. In term of proactive protection technology, the main development direction is to build a dynamic, uncertain system architecture, which can enhance the attack difficulties and defense capabilities of network or system. Referencing to the core idea of proactive protection technology, especially the latest MTD and MSD, we can try to implement the combination of proactive protection technology and security mechanism in mobile communication in the future, and build a more secure protection mechanism to realize the active defense of user’s privacy data.

Acknowledgements

This work was supported in part by a grant from a project numbered 2013ZX03006002.

References

[1] Z. Dai, Y. Peng and T. Zhao, “Security of LBS System,” Journal of Tsinghua University (Natural Science), vol. 1, no. 10, **(2011)** May, pp. 1246-1253.

[2] Z. Peng and S. Li, “LBS Location Privacy Protection in Mobile Environment,” Journal of Electronics & Information Technology, vol. 33, no. 5, **(2011)** May, pp. 1211-1217.

[3] Y. Che, “Key Technologies Research On User's Location Privacy Protection in Location-based Services,” Ph.D.thesis, Zhejiang University, **(2013)**.

[4] C. Chow, Y. Mokbel and M. F. Aref, “Query Processing for Location Services without Compromising Privacy,” ACM Transactions on Database Systems (TODS), vol. 34, no. 4, **(2009)**, pp. 763-774.

[5] T. Xu and Y. Cai, “Exploring Historical Location Data for Anonymity Preservation in Location-based Services,” INFOCOM proceedings, IEEE Press, **(2008)**, pp. 1220-1228.

[6] M. Y. Jang and J. W. Chang, “A New K-NN Query Processing Algorithm Enhancing Privacy Protection in Location-Based Services,” Proceedings of the 2011 IEEE 11th International Conference on Computer and Information Technology , IEEE Press, **(2011)**, pp. 421-428.

[7] Z. Ou, M. N. Song, X. S. ZHAN, et al., “Key Techniques for Mobile Peer to Peer Networks,” Journal of Software, vol. 19, no. 2, **(2008)**, pp. 404-418.

[8] S. Schrittwieser, P. Fruehwirt, P. Kieseberg, et al., “Guess who is texting you, evaluating the security of smartphone messageing,” Proceeding of the Network and Distributed System Security Symposium (NDSS 2012), **(2012)**, San Diego, USA.

[9] Z. Pan, C. Liu, S. Liu, et al., “Vulnerability Discovery Technology and Its Applications,” Journal of Software, vol. 8, no. 8, **(2013)** August, pp. 2000-2007.

[10] Y. Cheng, L. Ying, S. Jiao, et.al., “Research on User Privacy Leakage in Mobile Social Messaging Applications,” Chinese Journal of Computers, vol. 37, no. 1, **(2014)** January, pp. 87-100.

[11] H. W. Curtis, “Subscriber Authentication and Security in Digital Cellular Networks and Under the Mobile Internet Protocol,” Ph. D. thesis, The University of Texas at Austin, **(2001)** May.

[12] G. M. Køien, T. Haslestad, R. Telenor and D. Norway, “Security Aspects of 3G-WLAN Interworking,” IEEE Communications Magazine, **(2003)**, pp. 82-88.

[13] W. B. Lee, C. K. Yeh, “A New Delegation-based Authentication Protocol for Use in the Portable Communication Systems,” IEEE Transactions on Wireless Communications, **(2005)**, pp. 57-61.

[14] L. Wu, X. Pan, Z. Peng, “Location Privacy Preserving for Semi-honest Users in LBS,” Journal of Shi Jia Zhuang Tie Dao University (Natural Science), vol. 27 no. 1, **(2014)** March, pp.99-105.

[15] Q. Si-Han, “Twenty Years Development of Security Protocols Research,” Journal of Software, vol. 14, no. 10, **(2003)**, pp.1740-1752.

[16] R. Perlman, C. Kaufman, “Analysis of the IPSec Key Exchange Standard,” Proceedings of the 10th IEEE International Workshops on Enabling Technologies Infrastructure for Collaborative Enterprises, IEEE, **(200l)**, Massachusetts, USA.

[17] N. Li, S. Wang, O. Li, “Analysis of Security Flaw in Cooperative Communication of 4G Mobile System,” Telecommunication Engineering, vol. 53 no. 11, **(2013)** November, pp. 1500-1505.

[18] D. Wang, and C. Liu, “Model-based Vulnerability Analysis of IMS Network.” Journal of Networks, vol. 4, no. 4, **(2009)** June, pp. 254-262.

[19] X. Zhu, Z. Wu, and J. W. Atwood, “A New Fuzzing Method Using Multi Data Samples Combination,” Journal of Computers, vol. 6, no. 5, **(2011)** May, pp. 881-888.

[20] M. D. Compton, “Improving the Quality of Service and Security of Military Networks with A Network Tasking Order process”, Ph. D. thesis, Air Force Institute of Technology, **(2009)**.

[21] D. Gerry, B. Douglas, H. John, et al., “Vulnerability Analysis of AIS-based Intrusion Detection Systems Via Genetic and Particle Swarm Red Teams,” Evolutionary Computation, CEC2004, vol. 1, **(2004)** June, pp.111-116.

[22] H. Zhou, Z. Qiu, J. Xiao, “Security Model and Sytem Structure for Network Active Defense,” Jiangsu University of Science and Technology, vol. 6 no. 1, **(2005)**, pp. 40-43.

[23] Q. Zhu, A. Clark, R. Poovendran and T. Basar, “Deceptive Routing Games," Proc. 51st IEEE Conference on Decision and Control, CDC12, Maui, Hawaii, **(2012)** December 10-13.

[24] S. Antonatos, P. Akritidis, E. Markatos, K. Anagnostakis, “Defending Against Hit List Worms Using Network Address Space Randomization,” Computer. Network, vol. 5, no.12, pp. 3471–3490, Aug 2007.

[25] G. S. Kc, A. D. Keromytis and V. Prevelakis, “Countering Code-injection Attacks With Instruction-set Randomization,” In Proceedings of the 10th ACM conference on Computer and communications security (CCS’ 03), New York, NY, USA, pp. 272-280.

[26] J. Sushil, K. G. Anup, S. Vipin, et.al., “Moving Target Defense—Creating Asymmetric Uncertainty for Cyber Threats,” Springer Press, **(2011)** January.

[27] E. Al-Shaer, S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, and X. S. Wang, “Toward Network Configuration Randomizationfor Moving Target Defense,” In Moving Target Defense, ser. Advances in Information Security, Springer , New York, vol. 54, **(2011)**, pp.153–159.

[28] N. Poolsappasit, R. Dewri and I. Ray, “Dynamic Security Risk Management Using Bayesian Attack Graphs,” IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 1, January/ February **(2012)**, pp. 61-74.

[29] D. Matthew, G. Stephen, U. William, et.al., “MT6D: A Moving Target IPv6 Defense,” MILCOM. U.S: IEEE Communication Committee, **(2011)**, pp. 1321-1326.

[30] H. J. Jafar, A. Ehab, Q. Duan, “Open flow Random Host Mutation: Transparent Moving Target Defense Using Software Defined Networking,” Hot SDN, no. 12, **(2012)**, pp. 127-132.

Authors

Ganqiang Lu, he was born in 1990 in Jining, Shandong provience. In 2013, he got the Bachelor's Degree of communication engineering from Shenyang University of Science and Technology. Now, he is studying for master's degree of information and communication engineering in Zhengzhou University. The main research interests are wireless communication networks, mobile communication and novel network architecture.

Caixia Liu, she was born in 1974 in Yantai, Shandong providence. In 1997, she got the Bachelor's Degree in communication engineering from Zhengzhou University. She received the M.S and Ph.D degree of information and communication engineering in Zhengzhou University in 2000 and 2004. Now, she is a Associate Professor in Zhengzhou University. Her main research interests are mobile communication, social networks and wireless communication networks. She has published more than 30 technical papers in refereed international journals and conference proceedings.

Qing Zhang, he was born in 1991 in dongying, Shandong povience. In 2013, he got the Bachelor's Degree of communication engineering from Najing University. Now, he is studying for master's degree of information and communication engineering in Zhengzhou University. The main research interests are wireless communication networks, mobile communication and novel network architecture.