Research on the Mobile Internet Security

Yue lei
China Criminal Police College,Shenyang, China
Email:863748603@qq.com

Keywords: mobile communication, mobile Internet, security

Abstract. With the development of economy, the level of science and technology has improved greatly. People's demand of the Internet information is increasing in their daily work and life, so people's demand of the Internet technology is even higher. The current mobile Internet technology is developing, as a result of which people are faced with various potential security risks. This article starts from the network access security and terminal application security and analyzes the security status of the mobile Internet. What's more, it studies the security problems in the mobile Internet development, concludes the damage resulting from some safe leakages by simulation experiments and reproduces how the attackers make use of the leakages to attack the Internet. Finally this article makes a summary and outlook for the safety of the mobile Internet.

Introduction

Along with the wide application of the computer network technology and wireless communications terminal equipment, the mobile Internet technology is developing greatly, which brings great convenience to people's life. At present, as the 2G, 3G, 4G and other related technology are improving, the development of mobile Internet technology is more comprehensive, leading to the use of the tablets and apple mobile phones. By further combing with the network information technology, the mobile Internet technology will become the major direction of the mobile communication terminal products, the wireless communication and the information technology. Until January, 2012, 356 million Chinese use the mobile Internet, increasing by 17.5% compared with the earlier year. In 2011, the percentage of the Internet users who use desktops was 73.4%, while the percentage of using mobile phones was 69.3% and that of using laptops was slightly increasing to 46.8%. So we can see it clearly that with the usage of desktops decreasing , the mobile phone terminal usage was close to traditional desktop computers, so the mobile Internet users have gradually become the main Internet users in China nowadays. The mobile Internet not only combines the mobile communication network and the Internet, but also derived a new form of business and business models. Traditional Internet enterprises, communications, consumer electronics manufacturing and other industries are combined with their own advantages, infiltrating positively to the field of the mobile Internet. With the development of mobile Internet technology, the mobile network will be everywhere and people will become more and more dependent on the mobile network and access to information, so people's dependency on the dissemination information of the mobile Internet is more and more strong. One of the most important ways that people have access to information, especially the information closely related to their own interest, is through the mobile Internet. The mobile Internet is born with openness, interactivity, dispersion, privacy, convenience, the diversity of information content , the complexity of numbers and the characteristics of due arrival, which make people's requirements of sharing information, flexibility and convenience met . These features also make supervision complicated and at the same time bring new potential security risks to national security, social stability and user protection, especially the user privacy protection. This article starts from the mobile Internet access security and the terminal application security to study the potential security risks.

Network Access Security

The mobile Internet from the Internet technology and the mobile communication technology

derived from traditional technology and detached from traditional technology. But it inevitably inherited the safe leakages of them. In addition, it produces a lot of security problems due to its own characteristics.

1.1 Identity Authentication Security

In the 3GPP standard the authentication process involves three entities: VLR/SGSN (network service)， HLR/HE (Home Realm) and ME(mobile terminal users), which need mutual authentication between the three entities to identify each other. Ideal authentication model is as shown. These three entities have the actual link between them. Identity authentication doesn't go through other entities.

In the actual network operations, according to the 3GPP standards the geographical position between HLR/HE and VLR/SGSN has certain physical interval for the identity authentication relationship between VLR/SGSN. The interactions information between them need to exchange through a large number of nodes and the external network. Moreover, the network authenticates the terminal ME. But ME only certificate HLR/HE and doesn't authenticate the network VLR/SGSN， which may cause the following four serious problems: (1) the leakages of the mobile terminal user identity (2) the phishing attacks of the fake VLR/SGSN (3)the information gathering of false VLR/SGSN (4)the active communication of unknown VLR/SGSN

1.2 Wireless Access Security

The mobile WIFI is connected to the computer network, which also makes the inherent defects of the computer network affect the mobile terminal. APR protocol vulnerabilities is one of the APR protocol that is used to establish and maintain the seven layers of the network protocol address mapping of the second and third layer. Mapping table is stored with each computer and the data link layer address (MAC) mobile of the mobile terminal, the network layer address and the corresponding relationship of IP address. The source host sends APR request in a broadcast way. Reply packets are unicast packets. Any host agreement shall have the right to send APR response packet. But it is a pity that deal has not received APR response package for security verification. That's to say, it unconditionally receives APR reply packets. Then it inserts the response data to own APR address cache table. Under such an agreement loophole, the attackers can not only cheat mobile terminal users, but can deceive the gateway, which is shown in figure.On this basis, the attacker can a variety of forms of attacking the terminal.

(1) block and DOS attacks

Attackers send a lot of mistakes LAN APP data to the mobile phone terminal or gateway at a faster speed than the frequency of updates and the real APR cache data can not be saved. In the attack equipment, all the data from the equipment that was attacked will be sent to the wrong MAC address, which makes the attacked host can't send information and the mobile terminal host or gateway can't work normally.

(2) man-in-middle attack

The attackers send fake data to the ARP host and gateway respectively at a faster speed than the frequency of updates. Meanwhile, the attackers commit spoofing attack to the host and gateway APR and make the data between the host and gateway go through the attackers, which is transmitted by the attackers. The interaction of packets between the host and gateway are taken by the attackers unwittingly.

(3) the phishing attack

On the basis of the middle attack, when the target's access involves visiting shopping sites or bank account operation, the attacker who monitors the target data sends the target the prepared fishing website to obtain the target's account and even steal the target's fund unwittingly.

(4) the counterfeit attack

After gaining the user's information, the cheating gateway disguises as the original target for rapid operation and blocks the target, which makes it unable to connect to the Internet to seek illegal interests and does serious damage to the user's self-interest and information security. In addition, the attackers can also combine several attacks for more large-scale attacks.

Terminal Application Security

As the process of using smart mobile phones, users are able to experience that the functions of smart phones also show the characteristics of diversification and intelligence. The openness of mobile applications at the same time also caused criminals to take advantages of the machines, the intelligent terminal under the mobile Internet is faced with various security threats, which can be divided into charges loss and privacy leakage.

2.1Charges Loss

2.1.1 Malware

Inside mobile applications and even mobile terminals, because users cannot understand its operation mechanism, the users' charges may be secretly consumed. Or the hidden trouble existing in the mobile applications may cause the user's charges loss, which belongs to the current existing hidden trouble of the mobile terminal.

Smart phone software, which can deduct the user's expenses, can be spread by group messaging channel. If the group message is send to 1 million persons each time and 5% of them click on the software , then 10,000 mobile phones can be infected each group massage. If every person is deducted 2 yuan a month, it can bring the criminals an income of more than 100,000 yuan. Because the message group line price is 1 to 2 fen , sending 1 million messages only needs 10.000 to 20,000 yuan. But from the perspective of the users, the amount of the expenses deducted by the software is small, it is hard to find it timely.

2.1.2 Malicious Attacks

Recently we've studied NFC (the near field communication) mobile phones. We found when NFC identifies near-field tags, the title of the lable will be displayed before the content. So we have such attack experiment to add Space, Enter to the title to make the showing title disguised as the one that should be originally displayed "title + content", letting the near field communication users mistakenly assume that showing URI is the interaction address which id due to.

Similarly, the near field telephone calls and short massages have the same format. This way is also suitable for the attacking of the near field calls and short messages, as a result of which the trade of user's near field communication losses.

2.2 Privacy Leakage

In the digital age citizens' privacy is an old topic. No matter which direction the digital society develops in, we can agree on a consensus: that is in the mobile Internet era personal privacy has become even more vulnerable than ever and to protect individual privacy is a difficult thing. In 2014 new mobile phone virus malware can steal user privacy in which malware can steal user location privacy information.

Location based service is a value-added service that is provide to the mobile users. Location information is naturally sensitive. Preventing the leakage of user's location information has become a problem to be solved although the authentication mechanism of current NED in the system is perfect and can be transmitted through the encryption in the process of each server install firewall and other measures to ensure the user's location information. Identity authentication and content security are two key problems of communication security, which are also two important hot topics of the field of 3G network security. In addition to the traditional voice services, the main characteristic of 3G networks also provides rich multimedia data. Therefore, it is also called mobile Internet. The diversification of business of 3G network access security and the safety of the business data content puts forward the new demand for 3G network. One of the core technology of the network access security is identity authentication and key agreement, because they are essential to achieve secure communication and protect the interests of the users and operators. As part of the call setup, identity authentication and key agreement protocols play an important role in it. Therefore, the security analysis and improvement of them have been an important topic in the field of 3G security research. The security of 3G network multimedia data service content is the major research field in recent years. There have been many successes. The open features of 3G networks and multimedia content, multimedia data is easy to copy, distribute and so on, which make the research in protection and management technology more practical and valuable. The digital

watermark technology has developed in recent years, which is an important technology in the field of multimedia information security, the main application fields of which are to mark the digital content copyright and copyright protection, content authentication and integrity checking, etc.

Summary and Outlook

In a word, this article starts from two aspects—the mobile Internet network access and terminal application security, analyzes the security status of the mobile Internet. Besides, by studying some potential security risks this article imagines multiple attacks that malicious attackers can make by using some defense leakages and confirms some attacks by some experiments.

The current mobile Internet terminal security needs joint efforts. First of all,whether operators, mobile phone manufactures, distributors or security software vendors should strengthen the propaganda of safety. With the development of science and technology ,the mobile Internet technology is developing rapidly, the potential security risks that are brought o the residents and the country are more and more serious, which should be paid enough attention to . We manage it from two aspects of terminal security and operation safety and we practice all kinds of effective safety mechanism and technical means so as to protect user privacy and maintain national security and ensure the safety of the mobile Internet network.

References

[1] 29 times China Internet network development state statistics report [R]. Beijing: China Internet network information center, 2012.Ding in
[2], the 3G network vulnerability analysis and research. Beijing: Beijing University of Post And Telecommunicatio, 2011.
[3] zhong-hua dai, peng yong, terry. LBS system security. Journal of tsinghua university (natural science edition). 2011 ploidy (10) : 1246-1251.
[4] Hongbo Chen, Hui. Sun. Mobile Internet technology production and the content of the mode of shallow ground [J], China media technology, 2010 (9).
[5] Hongwei Yuan xiu-lin hu, Yunyu, Zhang mobile IP and its information security [J], 2011 (01) information security and communications confidential