Mobile Internet Information Security Analysis and Countermeasures

Yongbin Zhu\textsuperscript{a}, Li Yan, Junsheng Li\textsuperscript{b}
Computer Science of Engineering College, Honghe University, Mengzi, Yunnan, 661199, P. R. China
*Corresponding author, e-mail: abel.chu@foxmail.com\textsuperscript{a}, 122143275@qq.com\textsuperscript{b}

Abstract

The influence of mobile Internet on people's daily life is increasing day by day. In the constantly changing people's lives, at the same time, the mobile Internet information security is also facing a huge challenge, and concerned by more and more information security practitioners. According to the characteristics of the mobile Internet, this paper analyzes the factors that affect the security of the mobile Internet, and expounds the current security situation of the mobile Internet.

Keywords: mobile internet, information security, intelligent terminal, measures

Copyright © 2016 Universitas Ahmad Dahlan. All rights reserved.

1. Introduction

Mobile Internet is a revolutionary advance in technology; it not only changed the way of communication between people, but also brought a new revolution to many industries and business [1]. Mobile internet terminals have features of mobility and personalization different to internet terminals. With the rapid development of mobile broadband technology and services, as well as the increasing of the user, the global mobile Internet market is developing with each passing day [2]. The mobile intelligent terminal is becoming more intelligent and more open, and its property is closer to the user's demand. These mobile intelligent terminal devices with Internet access, Office, telecommunications, gaming, entertainment and other features, are gradually developing into a user's counseling centers, office centers, trade centers and entertainment centers. As more and more users prefer to use mobile intelligent terminal devices to access the network, and enjoy personalized services brought by mobile Internet, while cybercriminals also eyeing the huge gains in mobile Internet, mobile Internet and intelligent terminals are also becoming a new target of cyber attacks [3]. In addition to the risk of economic losses and leakage of privacy, mobile Internet users also faced with the threat of communication barriers. Furthermore, mobile Internet also has many security problems; hundreds of millions of users have been plagued by a variety of security issues.

2. Mobile Internet Features and Security Risks

2.1. Mobile Internet Features

Mobile Internet has the features of convenience, personalization, privacy, integration and InteliSense and other characteristics. With different to traditional Internet access methods, the mobile Internet can be accessed through mobile communication networks anywhere and anytime, and can keep the real-time online state [4]. With the development of intelligent terminal devices become smaller, increasing capacity, processing power is growing, to a great extent to meet the convenience needs of people to access the network. This convenience has spawned a huge market for location-based services, such as mobile electronic maps, taxi software, etc. In the access terminal, network and APP applications, mobile Internet will better reflect the individual needs of users. Individual terminals and network personalization combined with each other to make a personalized effect great release [5]. Integration of mobile voice services and mobile Internet services has led to business integration, and features more integrated, smart phones are becoming the only electronic equipment to carry. Future mobile devices will have
intelligent perception, for example, the future watch can detect your blood pressure and heart rate, and before the physical health problems will be able to remind you of timely treatment.

2.2. Mobile Internet Information Security Risks

With the popularity of smart phones, different manufacturers provide different systems; the wide variety terminal types increase the security flaw possibility. Because of the close relationship between the mobile terminal and its user, personal information is more valuable, and the continuous expansion of the business functions, such as office and payment, carry a huge business value, so the threat of intelligent terminal users is more serious than PC users. From the intelligent terminal, the security issues include malicious deductions, tampering destruction, loss of privacy, identity theft and mobile phone viruses. From an operational platform, the security issues include denial of service and information theft, etc. From a service provider perspective, the problems include adverse information dissemination, unsafe and malicious chargeback service [6]. Therefore, the characteristics of the mobile Internet determine its network will face more serious security threat than traditional.

3. Mobile Internet Security Status

3.1. The Security Threat to the Development of Intelligent Terminal

The gradual popularization of 4G high speed mobile network has brought a broad space for development. The original social networks, search applications, micro blogging, micro letter, LBS (mobile maps and route optimization) and so will be more popular. The original functions such as online video viewing and video chat can not be fluent in the 3G mobile phone network in 4G high-speed network will be used by more people. As the mobile intelligent terminal is becoming more and more intelligent and opening, the user terminal properties are more close to individual. Expanding office, payment and other business functions carries great commercial value, so that the mobile terminal more vulnerable to attack. A large number of users and users lack security awareness, so that the mobile network is facing serious security threats [7].

3.2. Network IP Brings New Security Challenges

Network infrastructure as an important mobile Internet, hosting a large number of application data, operators will increase the confidentiality of communications services, integrity and availability of building a more rapid, reliable and intelligent pipeline. With the increase of data traffic carried 4G, IP-based underlying network inevitable. IP-based telecommunications network makes over a closed network to an open Internet, and also the various security threats and attacks, the vulnerability of the Internet and other telecommunications networks is introduced, greatly increasing the security risks (such as anonymous telephone calls flood, etc). LTE has become mobile Internet IP pipeline, but the safety of LTE/SAE is still issues; while WLAN is gradually as mobile internet primary access mode, the network security problems are still difficult to solve; IPv4 address was exhausted in 2011.2, address safety planning, safety supervision and other issues of popularized IPv6 need attention [8].

3.3. Security Threats Faced by Business Diversification

The rapid development of communication services, from traditional voice services to data and media development, diversified business is facing a variety of security threats [9]. As bad information service information for dissemination of sensitive information leakage, the Trojan back door for business support, Web attacks, the business model for business abuse, malicious ordering, operators will assume more responsibility for information security, the need to increase content security, safety, security building business processes, safeguard green, convenient and secure business applications.

3.4. Security Threats Caused by Platform Diverse

Cloud computing and the Internet of Things bring new security risks. Mobile Internet era, business services side gradually evolve to cloud computing platform, features of cloud computing virtualization, multi-tenancy, dynamic scheduling bring a huge change to the business model, but also introduce new security issues for mobile Internet applications [10]. Things mode proposed new security requirements [11]: 1) Distributed terminal make centralized
protection mode may not be available, such as traditional firewall centralized protection can not be achieved; 2) M2M terminals (such as smart meters, fire alarm, room monitor, etc.) in IOT are not mobile or mobile within a fixed range, illegal mobile nodes must be monitored; 3) Things will contain a large number of private data, such as personal identity, location information, water and electricity data, transmission of private information requires effective protection; 4) Equipment in Things become the focus of network communications, equipments need to focus on their own safety issues, such as certification for device identification.

3.5. Users Lack Security Awareness
DCCI released “China Mobile Security Status Survey” data: 94.9% of mobile phone users lack a sense of security, 45.4% of mobile phone users do not have to install security software, and more than half of mobile users are lack of mobile security protection [12]. The loss of the phone is 15 times as much as a laptop computer. The value of the consumer’s data assets stored in phones is huge, but there are more than 1/3 of the information is lack of protection; 52% of consumers use mobile phones as mobile wallet; therefore, how to carry out the safe shopping through mobile devices becomes more and more important. More than half of smart phone users are not using any password protection to prevent unauthorized access to their devices. Mobile phone threat is becoming more and more complex; users need to enhance security awareness.

4. Results and Discussion
In view of these above security situations, it is recommended to take hierarchical and sub domain ideas for the mobile Internet security, respectively, from the mobile terminal security, core network security, application security and security assessment of four levels to take measures.

4.1. Improve the Security of Terminal Equipment
Terminal security is a problem that must be solved in the development of mobile Internet, and is also the most concerned by users. Mobile internet terminal securities include the traditional terminal protection means, mobile terminal security management, terminal access control and other [13].

(1) Strengthen the management of mobile intelligent terminal access. The mobile communication terminal manufacturers in the network license application, the mobile intelligent terminal equipment must first comply with the certification requirements, and must be responsible for the safety and legitimacy of application software pre-installed. (2) It needs to improve the mobile Internet malware monitoring and disposal capacity, to build and improve the relevant technology platforms. Mobile operators should have the ability and liability to deal covering the monitoring of the enterprise network, and to promote users about the intelligent terminal safety knowledge, to encourage users to install security software, timely to upgrade the operating system and security configuration [14, 15].

4.2. Strengthen the Core Integrated Network Security
Core integrated network security is the central link of the entire mobile Internet for safe operation. Mobile Internet is composed of access network, IP bearer network and Internet. We can learn from the experience of traditional Internet and mobile Internet features into account, from the network equipment security, network security, access network security, network security, security and information security, information security, information security these levels to study its security measures to further strengthen safety identification in the key links of information identification, filtering and blocking. For example, using the better recognition and disseminate ability of the Internet to enhance the safety monitoring of some blind spots; in the process of multi system access to users, a unified security management policy must be provided; in new business development, inspection and monitoring of new business must be carried out, so that new business security technology and existing basic standards can be merged.
4.3 Mobile Internet Security requires more Effective Integrated Management

Maintenance of mobile Internet security should be made a global perspective complete integrated solution, which needs users, mobile operators, network security vendors, handset manufacturers, software developers and Internet information providers to put forward higher requirements, at the same time, government regulators need to improve the corresponding regulatory system, strengthen the construction of relevant laws and regulations.

(1) Handset users need to further improve the safety awareness and the knowledge of network security to identify problem sites, malicious software and various network frauds. (2) Operators, network security providers, handset manufacturers, software developers need to build a scientific, comprehensive security system from starting construction of the mobile Internet as a whole at all levels of network security vendors, to focus on the development of mobile Internet viruses and malicious software, to take the work in a timely manner of network security, mobile devices and operating platforms. (3) Network Information providers should further improve the information content of the pre-trial management mechanism, strengthen the monitoring means of information dissemination of content, blocking information from a source of insecurity spread. (4) Government regulatory departments should establish and improve the mobile Internet-related regulatory mechanisms to accelerate relevant laws and regulations, strengthen law enforcement, and severely punish criminal conduct mobile Internet network, at the same time, government regulators should carry out the mobile Internet-related safety knowledge publicity and education activities to enhance network security awareness of the whole society.

5. Conclusion

The rapid development of the Internet is often ahead of legislation, when the problem has emerged, but the corresponding law does not develop, the network security is a great threat. Internet industry itself must strengthen the moral construction. Information provided by individuals should be timely reviewed to avoid some of the harm to society content. Some network practitioners for their own interests wantonly spread malicious information contained pornographic, reactionary and cults like. This requires network providers for further screening and filtering against illegal information to ensure cyberspace content consistent with national laws and regulations.

Acknowledgments

This paper belongs to projects of the “Basic Applications Research in Yunnan” (No.2013fz127) and the “Yunnan Education Fund for Scientific Research” (No.2014C136Y).

References


