Security Framework of Mobile Internet

Wei Liang
(China Academy of Telecommunication Research of MIIT, Beijing 100045, P. R. China)

Abstract:
The article describes the layered model of physical network and information security, and the establishment of the mobile Internet's security framework based on its network architecture. The mobile Internet has three parts, i.e. terminal, network and service system, each of which can be studied in four layers of the network and information security, namely, the equipment/environment security layer, the service and application security layer, the information security layer and the information content security layer.

Thanks to the advancement of information technology, people are increasingly dependent on Internet in their work and life, bringing the higher requirement on Internet use. Besides access to the Internet from home and workplaces, people also need the mobile connectivity anywhere and anytime, for instance, when they are moving in the public transportation or away from the city area. The fast developing wireless technologies are helping support all these needs. These technologies include 3G mobile communication technologies such as WCDMA, CDMA2000 EV/DO, Time Division Synchronous Code Division Multiple Access (TD-SCDMA) and World Interoperability for Microwave Access (WiMAX), besides Wireless Local Area Networks (WLANs) like Wireless Fidelity (Wi-Fi). According to the statistic results of China Internet Network Information Centre (CNNIC), there had been 117 million mobile Internet users in Chinese by the end of 2008, almost the same as the number of Internet users in 2005, with a growing rate of more than 100% for two years in a row. Along with the launch of 3G Internet access packages by China Mobile, China Telecom and China Unicom, the mobile Internet has embarked on a fast track of development in China.

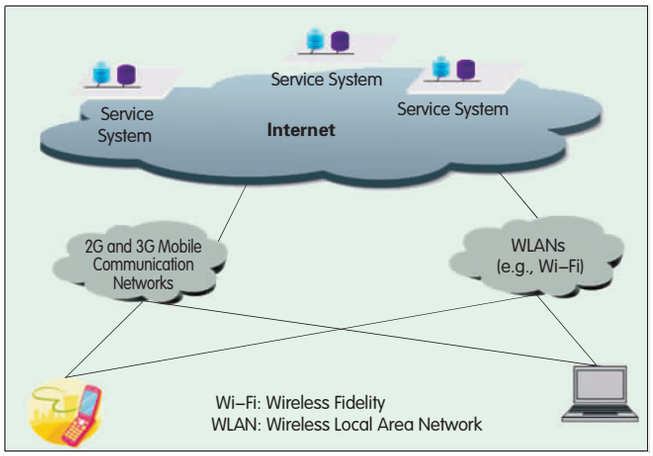
Nevertheless, security problems of the mobile Internet are also emerging. Attacks occur in large quantities to threat the Internet security, such as GPRS Tunnelling Protocol (GTP) Overbilling attack, Distribution Denial of service (DDoS) attack, Dynamic Host Configuration Protocol (DHCP) exhaustion attack, malicious block of context with fake address, "Curse of the Silent" service refusal attack, junk information sending by groups, private information theft, and mobile phone viruses. By the end of 2008, nearly 400 viruses had been able to run on smart phone platforms. The mobile Internet has inherited the vulnerability of traditional Internet technology and mobile communication network, and is now faced with double risks from both the problem-ridden Internet and the mobile network that is becoming more dependent on IP technology. It is predictable that the mobile Internet security is being seriously threatened.

This work was supported by the National High Technology Research and Development Program of China ("863" Program) under Grant No. 2008AA01A204.

1 Mobile Internet

As opposed to the traditional Internet, the concept of mobile Internet emphasizes the capability to access the Internet and use the services anywhere and anytime when the user is in a mobile status. Another similar concept is radio Internet, which is featured by the radio access mode, instead of coaxial cable, twisted pair and optical fibre through which the Internet is accessed and its services be used. Generally speaking, the two concepts are not exactly the same as mobile Internet is supported by the cellular mobile communication network (2G, 3G and Evolutional 3G, namely E3G) and usually accessed by the mobile phone; while radio Internet emphasizes the radio access modes, namely, by way of the cellular network and other various radio access technologies, for example, the 802.11 (Wi-Fi) technology, which is adopted by laptop PCs.

Anyway, the differences between mobile Internet and radio Internet are becoming more unnoticeable now due to the technological and service integrations between the telecommunication network and computer network. Specifically, the mobile phone can access Internet through either mobile telecommunication network or Wi-Fi, and the laptop PC can access Internet through either Wi-Fi (radio LAN) or data card (mobile telecommunication network). In other



◀Figure 1. Structure of mobile Internet.

words, by mobile Internet it means that people use the mobile phone, Personal Digital Assistant (PDA), laptop PC and other special mobile Internet terminals to access Internet and use Internet services by way of the mobile telecommunication network (2G, 3G, E3G, for instance) or radio LAN and in this process, the Wireless Application Protocol (WAP) is employed or not. Figure 1 depicts the structure of mobile Internet.

Consequently, the security studies of mobile Internet focus on cases that people use the mobile phone, PDA, laptop PC and other special mobile Internet terminals to access Internet and use Internet services by way of the mobile telecommunication network (2G, 3G, E3G, for instance) or radio LAN and in this process, the Wireless Application Protocol (WAP) is employed or not.

2 Security Architecture of Mobile Internet

2.1 Layers of Network and Information Security

The mobile Internet works not only on the traditional mobile telecommunication network (currently including circuit domain and packet domain) but also on Internet reputed as suffering serious security problems. This results in necessarily layered studies of network and information security, which usually are as shown in Figure 2.

(1) Equipment/Environment Security

The temperature, humidity, electromagnetic radiation, dust–proof, fireproof, and access control of the environment where the network, hosts and terminals are located should be conformant with related standards. The operating system, database, middleware and basic protocol stacks should be capable to resist attacks and invasions. Equipment should be ensured to work reliably in a stable status.

(2) Service and Application Security

For communication networks, a service usually refers to that provided directly by the network to users, while an application is a service provided to users through the network that works as a channel. The service and application security covers normal provisioning of services and applications, reliable access of users, security of management information (such as charging information), security of control information (such as signaling), prevention of unauthorized use, misuse of services, theft of services, DDoS attack, service denial and signaling disturbance, and more.

(3) Security of Information Itself

The security of information itself covers information integrity, confidentiality and non–repudiation. Information integrity can be guaranteed through packet identification mechanism, such as Hash algorithm. Information confidentiality can be protected by encryption mechanism and key distribution. Information non–repudiation can be ensured by digital signature technology.

(4) Information Content Security

Information content security usually refers to the exclusion of information that is forbidden by local laws, the information not conformant with social ethics, the information that exposes personal privacies, the junk information and viruses.

2.2 Security of Mobile Internet

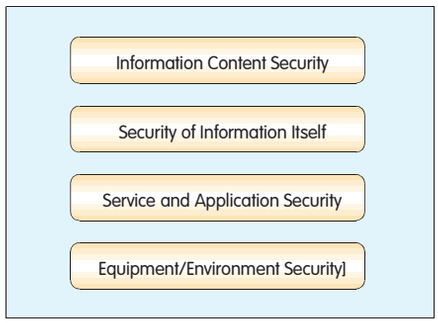
Based on the Internet architecture and layering of network and information security, the security of mobile Internet can be studied in three parts: terminal security, network security and service security, as shown in Figure 3.

2.2.1 Terminal Security

Mobile Internet terminals include mobile phones, Personal Digital Assistants (PDAs), netbooks, laptop PCs, and more. Terminal security is studied in the following four aspects: equipment/environment security, service and application security, security of information itself and information content security.

(1) Equipment/Environment Security

First, mobile Internet terminals belong



▲Figure 2. Layers of network and information security.

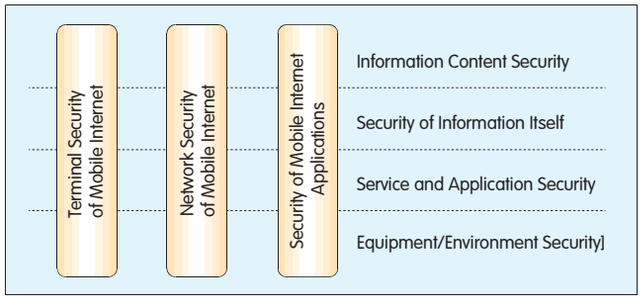


Figure 3.▶ Security architecture of mobile Internet.

to information technology equipment and telecom terminal equipment as well. They should meet the requirements of the China Compulsory Certification (CCC) that includes Electro Magnetic Compatibility (EMC) and electrical appliance security.

Second, the terminals use radio technology, so they should have the Type Approval Certification (TYC) of the State Radio Regulation Committee (SRRC) of China.

Third, telecom terminal equipment like mobile phones should have the Network Access License (NAL) granted by Ministry of Industry and Information Technology (MIIT) of China.

Moreover, because the mobile Internet terminal is intelligent equipment that often has an operating system, it is supposed to be able to protect itself from the common viruses, wooden horse, fishing software as well as attacks targeted at loopholes in operating system and applications.

(2) Service and Application Security

The terminal service and application security is to guarantee valid users' normal use of services and applications, to prevent services from being used with stolen identity, to prevent leakage of users' privacy including user passwords, to make sure of service use at any time within valid scope, to resist DDoS attacks, and to guarantee communication secrecy through encryption and isolation approaches. When a mobile communication network is employed as the access media, the terminal–related access security is considered from equipment/environment security (network access requirements for telecom terminal equipment) and network security of the mobile Internet. To put it simple, the service and application security is mainly concerned with the application security that is unrelated with access.

(3) Security of Information Itself

The security of information itself means that users' privacy and personal information stored in the terminals are protected from illegal acquisition. Such information includes contact information, record of calls, short messages and multimedia messages received and sent, International Mobile Equipment Identity (IMEI), SIM card information, user documents, photos and pictures. The confidentiality, integrity and availability of user information during the transmission process are considered as a part of network security and service/application security of the Internet. The security of terminal information itself covers aspects such as authorized access to the information in the terminal, invasion protection and encrypted storage.

(4) Information Content Security

The information content security of the mobile Internet is mainly concerned with protecting youngsters from porn and violent content.

2.2.2 Network Security

The mobile Internet is made up of the access network and the IP bearer network/Internet.

The access network, in the case that the mobile communication network is employed, consists of Base Transceiver Station (BTS), NodeB, Base Station Controller (BSC), Radio Network Controller (RNC), Mobile Switching Center (MSC), Media Gateway (MGW), Serving General Packet Radio Service Support Node (SGSN), Gateway General Packet Radio Service Supporting Node (GGSN) and related links. If the Wi–Fi mode is deployed however, the Access Point (AP) equipment will be involved instead.

The IP bearer network/Internet involves the router, switch, access server and related links. The network security is also studied in the abovementioned four aspects.

(1) Equipment/Environment Security

This refers to the security of network equipment such as a router and that of the environment where the equipment is located are conformant with standard requirements. Equipment security includes conforming to the security requirements as defined by the MIIT of China for network access. Environment security requires that the temperature, humidity, electro–magnetic radiation, dust–proof, fireproof, and access control of the environment where the network equipment is located are conformant with related standards. Moreover, equipment/environment security also requires that the operating system, database, middleware and basic protocol stacks resist attacks and invasions so that the equipment can work reliably in a stable status.

(2) Service and Application Security

The network service and application security refers to the security of access service, that is, to guarantee valid users' use of services and applications through authentication and other technical methods, and to prevent services from being used with stolen identity. One–way authentication is executed in the 2G GSM network and A3/A8 algorithms deployed to carry out authentication and key agreement. Taking 3GPP specifications as an example for 3G networks, the 3GPP R99 version introduces a two–way authentication and new authorization algorithm: Advanced Encryption Standard (AES). With AES, the encryption algorithm is moved backward to RNC, the new password algorithm Kasumi is employed and signaling integrity protection is added. The 3GPP R4 version adds the Mobile Application Part Security (MAPSec) protocol to protect the signaling security of MAP. The 3GPP R5 version uses the Internet Protocol Security (IPSec) to protect the packet domain, and uses IP Multimedia Subsystem (IMS) for access security protection. The 3GPP R6 version adds the general authorization architecture. If Wi–Fi access is adopted, access security will be protected with the 802.11i standard and Wireless Authentication and Privacy Infrastructure (WAPI).

(3) Security of Information Itself

The security of information itself mainly covers the necessary isolation and secrecy protection provided by the network when information is transmitted via the air interface or through the IP bearer network/Internet, as well as the user's registration information security involved in the access network. Although the air interface encryption algorithm has been defined for the mobile communication network, in China, it has been carried out in China in neither the 2G nor 3G networks that are now being deployed. Most Wi–Fi access networks do not deploy encryption either. That is to say, the security of information itself is fulfilled by end–to–end deployment.

(4) Information Content Security

A large proportion of services on mobile Internet are from the traditional Internet and the information content

being transmitted is public rather than for end–to–end purposes. Therefore the network information content security of mobile Internet should cover necessary screening and detection procedures for harmful information.

2.2.3 Security of Mobile Internet Applications

The mobile Internet services come in three categories:

- Services duplicated from the traditional Internet to mobile Internet;
- Services transplanted from mobile communication networks to the mobile Internet;
- New services adaptive to mobile Internet terminals, which integrate services in mobile communication networks and the Internet.

The currently predictable mobile Internet services are mobile browsing, mobile Web2.0, mobile search, mobile Email, mobile instant messaging, mobile e–commerce, mobile online games, telephone calls, short message service, color ring back tone, multimedia message service, mobile location, mobile navigation, mobile payment, mobile Voice over IP (VoIP), mobile map, mobile audio, mobile advertisement, mobile Mashup, and mobile Software–as–a–Service (SaaS).

(1) Equipment/Environment Security

This refers to the security of the application server, Web server, database server, mail server, gateway and storage media, as well as the environment status that is conformant with standard requirements. Equipment Security follows the requirements of CCC that include electrical appliance security. Environment security requires that the temperature, humidity, electro–magnetic radiation, dust–proof, fireproof, and access control of the environment where the abovementioned equipment is located are conformant with related standards. Moreover, the operating system, database, middleware, and basic protocol stacks should be capable to resist attacks and invasions.

(2) Service and Application Security

The service and application security is to guarantee valid users' use of services and applications through authentication and other technical methods, and to prevent services from being used with stolen identity. Most current application security mechanisms are unrelated with the security mechanism of network layer access, but are carried out end to end between mobile Internet terminals and mobile Internet service equipment.

(3) Security of Information Itself

The security covers application–related information integrity, confidentiality and non–repudiation. Although information security can be protected by encryption and isolation mechanisms, it is in most cases carried out end to end.

(4) Information Content Security

Most service–related information is for public purpose rather than for end–to–end communication, such as mobile browsing, mobile Web2.0, mobile search, mobile map, mobile audio, mobile video, mobile advertisement, and mobile Mashup. This means adequate measures should be taken for the mobile Internet applications to make sure that no illegal, harmful information or personal privacies are included in the application–related information.

3 Future of Mobile Internet Security

The mobile Internet is the newborn that integrates the mobile communication network and Internet, and is consequently endowed with the advantages of both. It starts booming along with the 3G deployment and maturation of smart phones and netbooks. Its security problems, however, are also emerging, including viruses, wooden horses and junk information from the Internet, as well as illegal location and mobile Internet identity theft as the results of the combination of mobile networks and the Internet. As the 3G network construction is moving forward, the smart phone becomes more popularized, and people's dependency and demand on the Internet grow, the subscribers and network scale of the mobile Internet are both expected to increase by leaps and bounds, which means the security problem of the mobile Internet is also becoming a pressing issue to be solved.

Compared to the traditional Internet, the mobile Internet still has many advantages because of its limited terminal bandwidth, limited computation capability, small screen, very few content sources and poor input method. Such a situation will be put to an end eventually with the help of technology advancement, and people will someday no longer tell the mobile Internet from traditional Internet, or to select whether to access the Internet through wired or mobile networks. Currently, at the early stage of the mobile Internet development, there is a good chance to make the mobile Internet, even the entire Internet in the future, safer by overall considering the security requirements and technologies based on the security framework of the mobile Internet. It's predictable that the security issues of mobile Internet will stay hot for a long term in the field of security studies.

References

[1] Mobile working needs a security rethink [EB/OL]. 2009–04–07. http://www.zdnetasia.com/insight/security/0,39044829,62052863,00.htm.
[2] **陈灿峰. 宽带移动互联网** [M]. **北京: 北京邮电大学出版社**, 2005.
[3] **张惠媛. 移动互联网与**WAP**技术** [M]. **北京: 电子工业出版社**, 2003.
[4] Mobiles to come under attack from "bad guys" [EB/OL]. 2008–04–25. http://www.zdnetasia.com/news/communications/0,39044192,62040620,00.htm.
[5] Mobile security technology fights fraud [EB/OL]. 2008–06–20. http:/www.zdnetasia.com/news/security/0,39044215,62042941,00.htm.
[6] Botnets on cell phones in 2009 [EB/OL]. 2008–10–17. http://news.cnet.com/8301–1009_3–10067994–83.html.

Biography

Wei Liang

Wei Liang is a vice chief engineer of the Research Institute of Telecommunications Transmission (RITT) of MIIT of China, and the director of the Network and Information Security Center of RITT. He has been engaged in the research of network architectures, next generation Internet and network and information security. He is now the reporter of ITU–T SG17 Q8, and has chaired and participated in three projects supported by the National High Technology Research and Development Programs of China ("863" program). He has published eight technical papers.