Security Service Technology for Mobile Networks

Abstract: As mobile networks become high speed and attain an all-IP structure, more services are possible. This brings about many new security requirements that traditional security programs cannot handle. This paper analyzes security threats and the needs of 3G/4G mobile networks, and then proposes a novel protection scheme for them based on their whole structure. In this scheme, a trusted computing environment is constructed on the mobile terminal side by combining software validity verification with access control. At the security management center, security services such as validity verification and integrity check are provided to mobile terminals. In this way, terminals and the network as a whole are secured to a much greater extent. This paper also highlights problems to be addressed in future research and development.

Keywords: mobile network security; security service; trusted computing; access control

Aiqun Hu
Tao Li
Mingfu Xue
(Information Security Research Center of Southeast University, Nanjing 210096, P. R. China)

1 Security Architecture and Threats in Mobile Telecommunication Systems

1.1 Security Mechanism Proposed by 3GPP

To secure 3G mobile telecommunication systems, 3GPP has developed a a security architecture with five feature groups [1] in three strata, as shown in Fig. 1.

These five feature groups and their functions are:

Group 1: network access security. This provides users with secure access to 3G services and protects against attacks on the radio access link.

Group 2: network domain security. This enables nodes in the provider domain to securely exchange signaling data and protects against attacks on the wireline network.

Group 3: user domain security. This secures access to mobile stations.

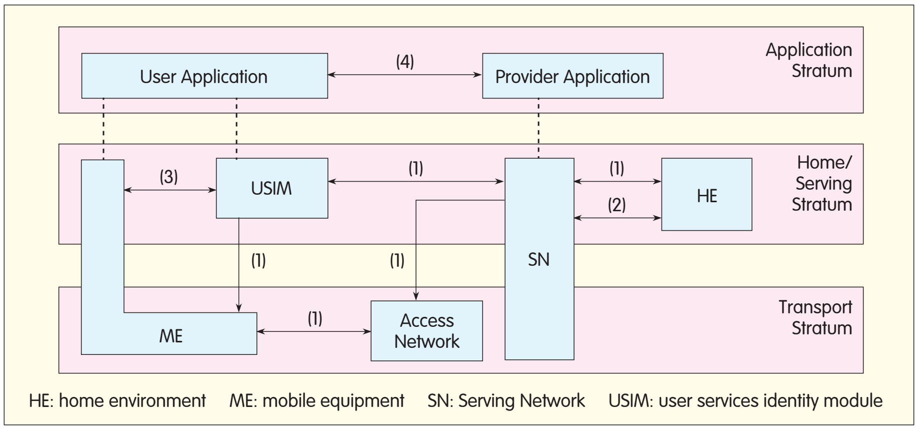
Group 4: application domain security. This enables applications in the user domain and provider domain to securely exchange messages.

Group 5: visibility and configurability of security. This enables users to determine whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

In 3GPP's security architecture, the emphasis is on the network access security mechanism, including mutual authentication, universal terrestrial radio access network (UTRAN) ciphering, and integrity protection of signaling data. Network access security mechanisms mainly fall into three categories:

- identification by temporary identities such as Temporary Mobile Subscriber Identity (TMSI)
- identification by a permanent identity such as International Mobile Subscriber Identity (IMSI)
- authentication and key agreement (AKA).

Among these, AKA is important and



▲Figure 1. 3G security architecture by 3GPP.

This work is funded by the National High-Technology Research and Development Program of China ("863" Program) under Grant No. 2009AA01Z427.

is a hot topic in research on 3G network security mechanisms. AKA mutually authenticates the mobile station and network, creating a new cipher key and integrity key. Other security mechanisms of 3G networks include data ciphering and integrity mechanisms. The data ciphering mechanism uses F8 ciphering algorithm to encrypt information between mobile equipment (ME) and the radio network controller (RNC). The data integrity mechanism applies F9 ciphering algorithm to authenticate data integrity and validity of a signaling message.

Protection measures such as mutual authentication, long secret keys, high-density ciphering, integrity algorithms, and signaling integrity protection mechanism are already used in 3G systems. A mechanism to protect core nodes in the telecommunication network is also used [2]. However, new services, open IP networks, and enhanced attack technologies still threaten the security of mobile networks.

1.2 Security Mechanism for 4G Networks

The security requirements of 4G networks fall roughly into four categories [3]:

- network access security. This provides access to 4G services that is secured against attacks on the radio access link.
- network area security. This enables nodes in the provider domain to securely exchange data and protects against attacks on the wired network and network entities.
- user user area security. This enables secure access to ME/user services identity module (USIM) and provides a security environment in the ME/USIM.
- application security. This enables applications in the user and provider domains to securely exchange messages.

The security architecture of 4G networks therefore includes these four feature groups, and functions of these groups are similar to those in 3G networks.

In terms of security requirements, the difference between 3G and 4G networks is that in 4G networks, the integrity of the hardware, software, and operating system in the mobile platform on ME/USIM needs to be protected. A trusted computing environment for mobile entities is created. Only with a secure mobile platform can the security of user information be guaranteed. Research shows that the security of a mobile platform depends on mobile terminals themselves and also security management and services of the security servers in the mobile network.

1.3 Security Threats Faced by Mobile Telecommunication Networks

3G mobile telecommunication networks are developing into all-IP networks. As a result, they are facing more security threats from viruses, trojans, junk e-mails, spam SMS, and eavesdropping. These will also affect future 4G networks.

Unlike legacy mobile telecommunications, 3G mobile telecommunications is oriented toward network application services. The mobile terminal is both a platform for users to enjoy services and an Internet terminal. Security problems in mobile terminals have a great impact on the entire 3G network. This is reflected in two ways. First, high-speed 3G mobile phones access to the Internet significantly increases the amount of sensitive data being transmitted over the air interface. Second, viruses and baleful information are transferred from mobile phones to other terminals or nodes in the network. Currently, 3G specifications on terminal data security are incomplete. Except for user authentication, they do not provide effective protection for data coming from the user side. The openness of the Internet is also a great threat to mobile terminal security. Easy access to the Internet increases the possibility that mobile phones will pick up viruses or be hacked. Security problems arising from network openness are a great challenge to 3G networks. With a large number of protocols being adopted, 3G systems are prone to certain security risks [4].

2 Research on the Security of Mobile Telecommunication Networks

To address threats to 3G and 4G mobile telecommunication networks, much research has been conducted on the security of mobile telecommunication networks.

2.1 Technologies for Architecture Security

Researchers from Anglia Ruskin University in the U.K. have proposed a new hybrid approach using symmetric/asymmetric authentication protocol for future mobile networks [5]. To overcome the defects of existing authentication schemes of 3G mobile systems—including leaking of mobile terminal identities and high update overhead of temporary identities—this approach uses a secure authentication mechanism. With this mechanism, the number of messages between authentication entities is reduced from five to four in the initial authentication procedure. The subsequent authentication procedure only contains two message exchanges. The number of messages between the mobile terminal and authentication center is reduced, and information congestion and slow processing at the authentication center is avoided. Moreover, authentication time delay, call setup time, and signaling traffic are minimized. This mechanism can also be used to counter network attacks such as replay attacks and guessing attacks. The mechanism meets the security requirements of 3G communication systems.

Researchers at the University of Illinois at Urbana-Champaign have proposed a lightweight, component-based, reconfigurable security mechanism [6]. This mechanism applies Tiny SESAME architecture to mobile networks in order to improve authentication and IP-based multimedia security services. This enhances the security functions of mobile devices. SESAME architecture, first introduced in Europe, is designed for distributed systems. The mechanism adopts asymmetric encryption and a special attribute certificate to verify security attributes such as identity and privilege.

Researchers at the University of Florida have proposed an enhanced AKA protocol (called AP–AKA) so that 3GPP AKA protocol is not vulnerable to false base station attacks [7]. In a false base station attack, user traffic is redirected from one network to another, and authentication vectors are used to impersonate other networks. AP–AKA protocol resists such attacks.

In [8], an IPSec–based virtual private network (VPN) is used to secure multimedia services over 3G networks. The IP multimedia subsystem (IMS) defined by 3GPP is an open network and vulnerable to attack. So security and quality of service (QoS) have become major issues. The IPSec–based VPN solution provides end–to–end security for real–time multimedia transmission while guaranteeing QoS.

AKA protocol–related problems in 3G mobile networks—including authentication vector attacks—were analyzed in [9]. For emerging 4G telecommunication systems, the AKA protocol is enhanced with Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocol, which has been proven secure and effective.

Security challenges in 4G systems were studied in [10], and the X.805 standard was used to analyze the Y–Comm framework of 4G systems. Y–Comm is a 4G security architecture with an integrated security module and has a specific security model for protecting data, servers, and users.

The AKA protocol used by 3GPP System Architecture Evolution (SAE) release 8 was analyzed in [11], and outstanding security problems were detailed. Security defects in the AKA protocol include user identity disclosure, compromised authentication vectors, and shared key leakage. In [11], a novel 3GPP SAE AKA protocol is proposed. A public key cryptosystem is used to encrypt user identities and authentication vectors in the network domain, and random numbers are used for public keys and local authentication.

Researchers at Beijing University of Posts and Telecommunications (BUPT) studied the security of 3GPP AKA and analyzed four attacks that affect the protocol [12]. They proposed a public cryptology–based AKA protocol that can be applied to two cases: location update and location immovability. Results showed that this protocol is secure. Compared with existing protocols, this protocol improves security to a certain degree.

Researchers at Tongji University of China proposed a terminal system scheme for establishing an IPSec VPN connection in a mobile network [13]. This system uses the Network Driver Interface Specification (NDIS) intermediate driver to traverse the firewall and ensure normal transmission of IPSec data packets. The system also uses secure intelligent cards to store X.509 certificates for identity verification. This prevents unauthorized users.

2.2 Technologies for Terminal Security

The terminal is the source of data and storage and is where most attacks are initiated. If each terminal in a mobile system is authenticated and authorized and its operations comply with security policies, security of the entire network system can be guaranteed [14]. Therefore, research on terminal security is attracting greater attention. Terminal security can be divided into two types: protection by antivirus and trusted terminal–based security.

A trusted computing based security architecture for 4G mobile terminals was proposed in [3]. Based on Trusted Mobile Platform (TMP) and Public Key Infrastructure (PKI), this architecture provides a robust platform for users to access sensitive services and data in 4G systems. A hybrid AKA scheme is also introduced in [3].

It was suggested in [15] that antivirus software be installed on the terminal; and on the network side, bypass detectors and filters be added to scan and kill viruses that threaten intelligent terminals.

In [16], multilayer security control means were suggested to be taken from network access layer to application service layer On the terminal side, security applications were developed; and on the network side, strategies for controlling secure network access and application service access were applied. These security control means work with security servers to guarantee security in mobile networks.

Both [14] and [17] advocate a trusted computing–based terminal security architecture so that there is consistency between trusted terminals and trusted network as well as security in the system. In [14], trusted computing based architectures and their effectiveness in terminal security protection was summarized. Future research directions were also given. However, [14] does not take into account system efficiency in actual situations nor does it show how to set up a unified security architecture within a network.

In short, the two approaches to terminal security are important for security in mobile networks. The first approach focuses on securing the air interface, and the second approach prevents viruses from invading the terminal. The first approach is relatively mature, while the second has attracted great attention in the past two years because of the emergence of mobile viruses. This paper focuses on the second approach.

3 Service–Based Security Architecture for Mobile Networks

As previously discussed, there are two main methods of protecting mobile terminals from viruses: scanning terminals and killing viruses, and creating a trusted computing environment for terminals. Neither is independent of security service architecture. In the first method, an updatable virus library and virus–killing service center is needed in the mobile network so that mobile terminals are provided with periodic and online antivirus services. In the second method, a trust check is needed for setting up and maintaining the trusted environment for terminals. Unlike computer users, mobile users often lack technical knowledge. So security in mobile networks is hard to guarantee if there is no security service.

Supposing identity authentication, data integrity, and confidentiality are guaranteed between the mobile terminals and the access network, security threats to mobile terminals will come mainly from the Internet, similar to a computer accessing the Internet. People expect that a trusted terminal can resist attacks from the Internet. If a terminal is trusted, its performance should satisfy expectations, and there should be no unlicensed software on the terminal. In other words, all software installed or executed on the terminal must be licensed by the security server. In this way, a virus on the Internet will not be transplanted to the terminal.

3.1 Trusted Service-Based Security Architecture

We propose a trusted service-based security architecture in which a mobile trusted module (MTM) [18] is added to the mobile terminal. This module is independent and secure, has computing capability, and can communicate securely with the security service provider (SSP). It calculates the integrity of all software installed on a mobile terminal and reports it to the SSP. It also checks the validity of software that is to be installed and executed on a mobile terminal. If the software is not authorized by the SSP, the module forbids its installation or execution. SSP is also added to the mobile network. The main function of the SSP is to provide software validity to the mobile terminal. Before software is installed or run on a mobile terminal, the software provider (SWP) must provide a validation certificate for the software issued by the SSP. That is, the software must hold the digital certificate issued by the SSP. Fig. 2 illustrates the trusted service-based mobile network security architecture.

In Fig. 2, the SSP server is connected to the access network (AN) server. To establish this architecture, only small changes need to be made to the existing system. Once a mobile terminal is authenticated and granted access to the network, the SSP checks its integrity. If the integrity of the terminal's software is found to be compromised, the terminal may have a virus. In this case, the terminal is forbidden to access the network in order to avoid the viruses spreading to other terminals. If the integrity has not been compromised, the SSP monitors the installation and running processes of the software and provides the mobile terminal with dynamic security services.

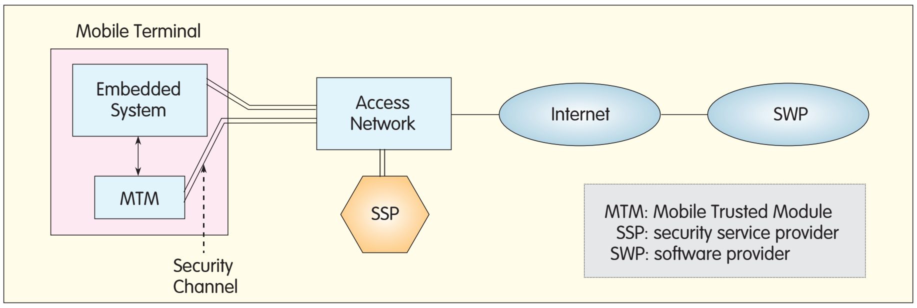
3.2 Trusted Computing Environment for Mobile Terminals

The key to an efficient service-based security architecture is a trusted computing environment for mobile terminals. For the purpose of this paper, the mobile terminal has two states: startup and started. A trusted computing environment established in the startup state is called static trusted environment, and that established in the started state is called dynamic trusted environment.

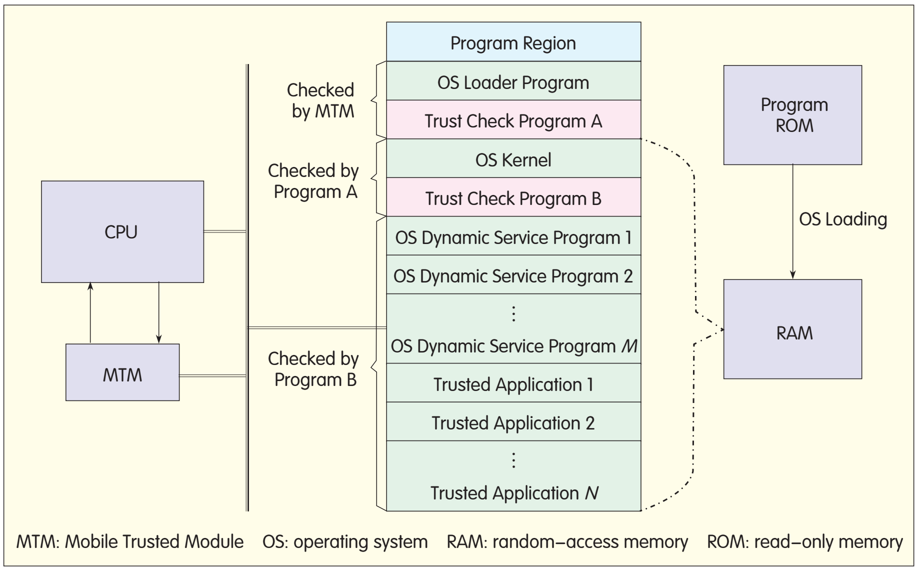
The method of creating a static trusted environment has already been widely discussed, and here we only intend to give a brief description. Once the power to a mobile terminal has been switched on, the trusted codes fixed in the trusted module are run. There are hardware features to ensure the codes cannot be modified. First, the trusted codes check the integrity of the system's loader codes. If the loader codes are complete, the trusted codes hand control over to the loader codes. The loader codes then check the integrity of the kernel of the operating system. If the kernel is complete, it is loaded. Next, the OS kernel checks the integrity of other parts of the OS. If all parts pass the integrity check, the OS is enabled. Finally, the integrity of upper-layer applications is checked. The terminal cannot be used until the integrity of all applications has been verified. If any integrity check fails in any of the above steps, the old configuration must be restored or the system must be re-installed. If the chain of trust is transferred away from trusted codes; that is, from the OS to applications by means of integrity check, a static trusted environment is established for the entire system. Fig. 3 illustrates the resource structure when the system starts. The trust check program is attached to the end of each program and is responsible for checking the integrity of the program that follows.

As shown in Fig. 3, to ensure system security, the OS kernel and trust check program B cannot be damaged after the static trust chain has been established. These two programs need to be protected by the MTM because after the system has started, the kernel program runs and trust check program B dynamically checks all applications that are to be run (or gathers integrity information of mobile terminals for SSP).

Once a system is started, protection relies on the dynamic trusted mechanism because the system's integrity changes dynamically with applications that are enabled by users. For example, when a browser is opened, the browser software is executed. The system has to run browser-related programs, so its integrity changes. If integrity information of the system cannot be updated correctly and in a timely



▲Figure 2. Trusted service-based security architecture for mobile networks.



▲Figure 3. System resource structure in startup state.

manner, malicious software may have an opportunity to damage the system. Dynamic integrity computing consumes computing resources. This is unavoidable. Therefore, implementing security over a running system is still a difficult problem for trusted computing. Trusted computing should

- periodically determine the integrity of a program or resources in a specified area and report it to the SSP
- check the validity of the program to be installed, and if the program is found invalid, forbid its installation
- check the validity of the program to be executed, and if the program is found to be invalid, forbid its execution
- ensure the security mechanism itself is secure
- ensure the security mechanism does not significantly decrease system efficiency.

It must first be determined whether the running system software or software resources have been modified. A common method for determining the integrity of a segment of codes is to compute the abstract value of the codes and then compare it with the existing abstract value (provided by the SSP). Another method is to select a random number of code bits and compute the abstract value. If the codes are long, the second method is advantageous.

When a program is to be executed on a mobile terminal, its integrity and validity must be checked. Verifying the validity of a program is often done by checking whether the program is licensed by the SSP. A validity certificate is provided by the SSP. The SSP signs contracts with SWPs and saves version and abstract information of legal software in the SSP server so that mobile terminals can query it. This process is illustrated in Fig. 4.

To ensure the security mechanism itself is secure, the key is to protect the trust check program B (Fig. 3) from being damaged. This often requires special hardware. An effective protection method is to use a hardware circuit to ensure the address space of trust check program B is not re-written, unless the writing is authorized by the MTM. Such a hardware circuit can be integrated into the MTM.

3.3 Security Server

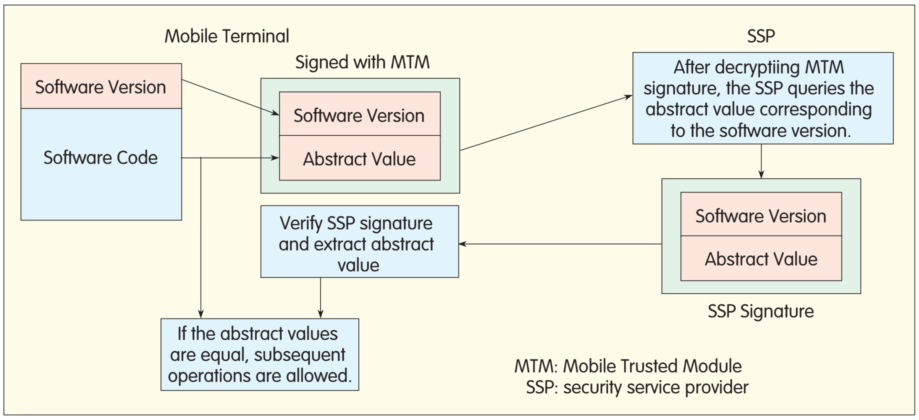
The two main functions of a security server are:

- to check the integrity of software on the mobile terminal. If integrity has been compromised, the terminal may have a virus and it is not allowed to access the network. If the mobile terminal were to access the network, it may spread a virus to other terminals or network devices.
- to provide validity query service for the mobile terminal. When a mobile terminal wants to install or execute software, it first queries the validity of the software in the local MTM. If no result is returned, it sends a query request to the security server. Upon receiving the request, the security server verifies the identity of the terminal and returns a result.

Other functions of the security server include interacting with SWPs (to audit the security of software and gather validity information); interacting with the authentication, authorization and accounting (AAA) server of the mobile network operator (to authenticate identity and to bill); and interacting with the access network server of the operation network (to control access based on the integrity of mobile terminals).

4 Future Research Direction

With network architecture and transmission protocols being mature,


Mobile Terminal
Software Version
Software Code
Signed with MTM
Software Version
Abstract Value
Verify SSP signature and extract abstract value
If the abstract values are equal, subsequent operations are allowed.
SSP
After decryptiing MTM signature, the SSP queries the abstract value corresponding to the software version.
Software Version
Abstract Value
SSP Signature
MTM: Mobile Trusted Module
SSP: security service provider

▲Figure 4. Integrity check and validity verification process of software.

the focus of future mobile security will be on terminals. Existing embedded platforms and operating systems on mobile terminals were not originally designed for mobile telecommunication, so their security problems are more serious than others. Integrated program and data space in the embedded OS makes it difficult to protect critical programs. An area of interest in mobile terminal security is the development of an embedded system architecture that protects critical programs.

Domain separation technology such as TrustZone [19], is a good way to implement read/write protection in critical locations in the memory. Once the OS and applications are loaded in the memory, the technology monitors the memory address accessed by the CPU and controls read/write operations for those critical locations. If the read/write operation is controlled with hardware, the impact on the system's running efficiency is almost negligible. Domain separation is an effective approach to real–time protection of the system. However, it requires the assistance of the embedded OS to provide, for instance, complete address information managed by the memory. For the sake of security, the architecture of the embedded OS must be studied and improved.

The key to software platform security lies in the OS. Access control is an effective means; but so far, it lacks theoretical support and security measurement methods. This is also a problem that trusted computing technologies have to handle. In research on OS security, the focus is often on how to construct a security model using theoretical knowledge.

Determining the integrity of system software and applications is critical in constructing a secure architecture. But this requires a great deal of computing. It is most pragmatic to design an effective integrity measurement algorithm with small computing burden. For example, the computing burden dramatically decreases if only bits of information are extracted from software codes and an abstract value is computed. How to extract such information and how to synchronize with the verification entity requires further study.

5 Conclusions

It is expected that mobile phones will become genuine Internet terminals in the near future. A mobile phone can be used in the same way as a PC for e–commerce, e–mails, and mobile wallet. However, if mobile phone security problems cannot be solved, mobile phones will be a bottleneck for these applications.

Security in mobile networks should be solved from the perspective of the entire network. The traditional approach, where users assume responsibility for antivirus functions, should be replaced by security services provided by the network operator. Network operators have advantages over individual users in terms of technology, facilities, and management and can more effectively guarantee mobile network security.

Before a good solution to mobile network security is worked out, security events will occur from time to time. Whether an operator can provide high quality security service will be a critical factor for their commercial success. Service–based security solutions will become mainstream in the development of information security technologies for future networks.

References

[1] Min Lei, Hai Bi, and Zhengjin Feng, "Security architecture and mechanism of third generation mobile communication," in *2002 IEEE Region 10 Conf. Comput., Commun, Control and Power Eng. (TENCON'02), Beijing, vol.2,* pp. 813–816.

[2] H. Yang, F. Ricciato, *S. Lu, and* L. Zhang, "Securing a wireless world," in *Proc. IEEE*, vol. 94, no. 2, pp. 442–454, 2006.

[3] Y. Zheng, D. He, W. Yu, and X. Tang, "Trusted computing–based security architecture for 4G mobile networks, " in *6th Int. Conf. Parallel and Distr. Comput. Applicat. and Tech. (PDCAT'05)*, Dalian, 2005, pp. 251–255.

[4] Q. Dai and Y. Wang, "Network security ushering in the era of 3G mobile communication," *China Inform. Security*, no. 5, pp. 34–39, 2010.

[5] M. Al–Fayoumi, S. Nashwan, S. Yousef, and A. R. Alzoubaidi, "A new hybrid approach of symmetric/asymmetric authentication protocol for future mobile networks," in *3rd IEEE Int. Conf. Wireless and Mobile Comput., Networking and Commun. (WIMOB'07)*, White Plains, 2007, p.29.

[6] J. Al–Muhtadi, D. Mickunas, and R. Campbell, "A lightweight reconfigurable security mechanism for 3G/4G mobile devices," *IEEE Trans. Wireless Commun.*, vol. 9, no. 2, pp. 60–65, 2002.

[7] M. Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," *IEEE Trans. Wireless Commun.*, vol. 4, no. 2, pp. 734–743, 2005.

[8] W. B. Diab and S. Prism, "VPN solution for securing voice over third generation networks," in *2nd Int. Conf. Internet Multimedia Services, Architecture and Applicat. (IMSAA'08)*, Bangalore, pp. 6.

[9] G. Kambourakis, A. Rouskas, and S. Gritzalis, "Using SSL/TLS in authentication and key agreement procedures of future mobile networks," in *4th Int. Workshop on Mobile and Wireless Commun. Networks (MWCN'02)*, Stockholm, 2002, pp. 152–156.

[10] M. Aiash, G. Mapp, A. Lasebae, and R. Phan, "Providing security in 4G systems: unveiling the challenges," in *6th Adv. Int. Conf. on Telecommun. (AICT'10)*, Barcelona, 2010, pp. 439–445.

[11] Y. Deng, H. Fu, X. Xie, J. Zhou, Y. Zhang, and J. Shi, "A novel 3GPP SAE authentication and key agreement protocol," in *2009 IEEE Int. Conf. on Network Infrastructure and Digital Content (IC–NIDC'09)*, Beijing, pp. 557–561.

[12] F. Lu, K. Zheng, X. Niu, Y. Yang, and Zhongxian Li, "Security analysis of 3GPP authentication and key agreement protocol," *Journal of Software*, vol. 21, no. 7, pp. 1768–1782, 2010.

[13] X. Wang, "Research on cellphone security system based on IPSec VPN," *Network and Computer Security*, no.1, pp. 52–54, 2009.

[14] W. Liu, J. Hu, Y. Fang, and Changxiang Chen, "Research and Development on the secure architecture of terminal based on trusted computing," *Computer Science*, vol.34, no. 10, pp. 257–269, 2007.

[15] H. Lv, Q. Chen, and X. Wu, "Research on development and countermeasures of virus in smart phone," *Information Security and Communications Privacy*, vol. 30, no. 1, pp. 80–82, 2008.

[16] D. Huang and Z. Sang, "Analysis of anti–virus method in mobile communication networks," *Study on Optical Communications*, no. 2, pp. 39–43, 2008.

[17] Zhenqiang Wu and J. Ma, "Research on TPM–based mobile Internet trusted architecture," *Network Security Technology and Application*, no. 11, pp. 18–20, 2007.

[18] NTT, DoCoMo, IBM, and Intel Corp. (2005, Jun). "Trusted mobile platform: hardware architecture description," [Online]. Available: http://xml.coverpages.org/TMP–HWADv10.pdf

[19] T. R. Halfhil, "ARM Dons Armor – TrustZone security extensions strengthen ARMv6 architecture," Microprocessor Report. [Online]. Available: http://www.mdronline.com/mpr/p/2003/0825/173401.pdf

Biographies

Aiqun Hu (aqhu@seu.edu.cn) is director of the Information Security Research Centre of Southeast University, China. He is also a professor and doctoral advisor. His research interests include wireless networks and their security technologies.

Tao Li (leotao1984@hotmail.com) is studying for his doctoral degree at the School of Information Science and Engineering of Southeast University, China. His research direction is trusted computing technologies for mobile networks.

Mingfu Xue (57233806@163.com) is studying for his doctoral degree at the School of Information Science and Engineering of Southeast University, China. His research direction is trusted computing technologies for mobile networks.