Development Analysis of Trusted Computing Technology of Smart Mobile Terminal

Ge Zhao and Jinming Hu
The Third Research Institute of the Ministry of Public Security, Shanghai 200031, China
Email: zhaoge@mctc.org.cn; hujm@mctc.org.cn

Abstract. With the continuous development of mobile communication technology, the market scale of smart mobile terminal industry is expanding rapidly. At the same time, due to the open characteristics of the software ecosystem and usage scenarios of smart mobile terminal, its security is facing great risks. Based on this, this paper first summarizes and classifies the security risks faced by smart mobile terminals according to the risk sources, then studies the current development status of trusted computing technology, and finally analyses the feasibility of introducing trusted computing technology into smart mobile terminals.

Keywords. Mobile communication technology; smart mobile terminal; trusted computing technology.

1. Introduction
With the development of wireless communication technique, the market scale of smart mobile terminal industry is growing rapidly. In 2020, the output of smart phones reach 1.3 billion. It is expected that the industrial scale of smart mobile terminals will continue to expand in future [1]. Compared with traditional mobile terminals, smart mobile terminals have more powerful processing capacity and larger storage space, which have gradually become a platform for all kinds of business systems. Furthermore, smart mobile terminals are gradually replacing desktop computers to become an important channel for users to access the Internet with the support of third-party software [2].

However, smart mobile terminals are more complex than traditional computer platforms in terms of terminal complexity, function diversity, use environment complexity and quantity scale. Therefore, smart mobile terminals face higher security risks. If the smart mobile terminal is invaded, the damage is more serious, including the disclosure of personal privacy information and commercial data, the abnormal use of the terminal, etc. [3]. For example, the Skulls series of viruses will cause the terminal to have only call function by disabling all system applications; the Android.Skullkey malware can read data from an infected terminal and sends a text message to the phone for a hefty service fee.

In order to ensure the security of smart mobile terminals, this paper first analyses the security risks faced by smart mobile terminals. Then, the current development status of trusted computing technology is studied. Finally, we analyse the feasibility of introducing trusted computing technology into smart mobile terminals.

2. Classification of Smart Mobile Terminal Security Risk
As the ecological environment of mobile Internet becomes increasingly complex, the new type of network crime related to the mobile Internet has become increasingly prominent. Its malicious behaviours have changed to the forced promotion of risk transmission, unauthorized collection instead
of system destruction, malicious deduction and consumption of fees. According to risk sources, the security risks of smart mobile terminals can be classified into the following categories [4].

- **Security risks caused by user behaviours**: Security risks caused by user behaviours mainly come from two situations: The first is that users are tricked into installing malicious software or accessing malicious links. Malicious software can invade mobile terminals through firmware implantation, application bundling implantation and other means for remote Trojan control and privacy theft. Because malicious software and trojans can be camouflages through packaging, users’ smart terminals can not avoid the possibility of infection even if they choose download content and links carefully. The second is that the terminal security policy is not configured, such as the start-up password. Smart mobile terminals provide basic security policy configuration mechanisms, such as passwords, face recognition, fingerprints, and other measures. However, if the user does not set a password or sets a very low security password, the security policies provided by the terminal manufacturer may fail to take effect, which will introduce security risks to smart mobile terminals.

- **Security vulnerabilities of the terminal itself**: Terminal’s own security vulnerabilities mainly include hardware security vulnerabilities, system security vulnerabilities, application security vulnerabilities and so on. Although terminal systems provide basic security mechanisms to ensure terminal security, such as Google’s application signature protection mechanism for Android applications, Android operating system can scan all Android applications that contain encrypted signatures to determine whether an application is legitimate. However, insurance company BlueBox found a way to make changes of the application code without affecting the encrypted signature. This technology can be used to install trojans on Android devices to read any data on the device, steal passwords, copy phone numbers, take photos and perform other functions.

- **Risks caused by network environment**: Risks of smart mobile terminals caused by the network environment mainly include network attacks. For example, when smart mobile terminals access high-risk WIFI networks, attackers will disguise themselves as legitimate network access points to deceive users to access. By intercepting the plaintext data on the wireless communication link, the attackers can obtain or tamper user privacy data.

3. **Trusted Computing Technology**

The overall goal of trusted computing is to improve the security of computer system. At present, the main goal is to ensure the integrity of system data, secure data storage and remote proof of platform credibility.

Trusted computing is a new type of self-immune computing mode with both operation and protection, which makes the results of operation and process behaviour always consistent with expectations under any conditions. The basic idea of trusted computing is to build a relatively independent trusted computing environment from the hardware chip to monitor and protect the computing environment from the impact of malicious code, so as to improve the fatal security defects in the modern computer system architecture [5]. The basic principle of trusted computing technology is shown in figure 1.

Firstly, trusted computing technology should build a trusted root based on the underlying trusted chip. Starting from the power-on of the device, build a trust chain from the hardware trusted chip to the motherboard platform, the basic input output system (Basic Input Output System, BIOS), the operating system booter, and the operating system kernel and applications. Starting from the underlying trusted root, one level of measurement and one level of trust, and then extends this trust to the whole computing system. Secondly, trusted computing technology should build a trusted network environment through trusted network connection (TNC) and extend trust relationship to the whole network by using trusted reporting and remote certification functions [6].

4. **Smart Mobile Terminal Trusted Computing Technology**

At present, network security level protection standards have been released and implemented, which put forward specific requirements for the construction of active immune security system using trusted
computing technology. Therefore, it is necessary to improve the security system of smart mobile terminal according to national policies and standards.

Figure 1. Basic principle of trusted computing technology.

However, due to the particularity of mobile platforms, it is difficult to copy the trusted computing technologies applicable to computers to mobile platforms directly. This paper considers to build a trusted system on the mobile terminal platform based on the idea of trusted computing 3.0. It is necessary to build a trusted root and dual architecture on the mobile platform, and establish a trusted verification mechanism based on measurement technology [7-9].

4.1. Trusted Root Build
As the source point of the whole active immune defence system, the trusted root has hardware and software resources independent of the host, which can proactively access all resources of the host to support the implementation of the trusted authentication mechanism.

For mobile terminals, Peripheral Component Interconnect (PCI) board cannot be used to build the trusted root due to the high degree of device integration and the lack of relevant bus interfaces. Meanwhile, the hardware transformation of mobile terminals is difficult and the cost is high, so it is not suitable to integrate the password chip. Therefore, the CPU of mobile terminals should be used to build the trusted root.

At present, most mobile terminals use ARM-based CPU and integrate the Trust Zone function, which provides the foundation for transformation and construction of trusted roots. Therefore, through the customization of the CPU basic firmware, we can select the computing core with start-up priority and memory access privilege in the CPU computing core to establish the trusted root.

4.2. Dual Architecture Build
The dual architecture is the infrastructure guarantee of the whole active immune defence system, and the core feature of trusted computing 3.0 which is different from other security protection mechanisms.

To build a dual architecture of computing components and protection components in mobile terminals, each component needs to meet certain characteristics. It is necessary to ensure the security isolation of the computing component, that is, it is unable to access the relevant resources of the protection component. The protection component needs to have the corresponding ability to access all the resources of the computing component. The protection component takes the trusted platform control module (TPCM) as the core and source of trust, which starts before the computing component and initializes the computing component resources and bus. The protection component accesses the computing component resources through the direct bus sharing mechanism, and uses static and dynamic measurement methods to verify the trustworthiness of the computing component. According to the trusted security strategy, the protection component takes the password as the gene to protect the reliable operation of the computing component and actively resist the intrusion behaviour through a series of means such as identity recognition, state measurement, state analysis, dynamic perception, response control, confidential storage and security control.

Through the customized transformation of the authority control mechanism and memory call mechanism of the CPU core of the mobile terminal based on the arm architecture, the TPCM function is realized based on a fixed CPU core, and the trusted computing 3.0 system is realized by using the
multi-core architecture of the CPU. Based on the security core, we can build a dual active immune architecture with parallel computing and protection by invoking the local physical resources, accessing and scheduling the computing environment resources and TCM resources. The dual active immune architecture can realize the active defence ability against viruses, implant "immune system" for mobile terminals and escort the stable operation of smart mobile terminal.

4.3. Measurement Mechanism
The measurement mechanism measures the measurement object according to the measurement strategy. Measurement strategy consists of measurement object, measurement method, etc. Measurement objects include programs, data and behaviour. The measurement methods include the setting of moderate measurement points in the measurement object, the timing of measurement, the algorithm of measurement, etc. The measurement process includes measuring the relevant subject, object, operation, environment and other information transmitted by the control mechanism according to the measurement strategy, and sending the measurement results to the decision mechanism.

The trusted static measurement object in the mobile terminal environment mainly includes the feature collection of the system executable program. Specifically, the collection content includes format files such as binary executable files (ELF, script), dynamic library and kernel module (driver). After information collection, a strategy benchmark library is formed. The programs existing in the benchmark library can be executed normally, the dynamic library can be linked normally, and the driver module can be loaded normally. The static measurement mechanism realizes the effect of controlling the minimum permission of users, preventing malicious code and software operation. Dynamic measurement mainly includes the monitoring of all key processes, modules, execution codes, data structures and important jump tables in the real-time system. Corresponding measurement methods are configured for different measurement objects to comprehensively check the operation of the system to ensure the safety and credibility of the system. Dynamic measurement is the core guarantee of the system. It is the key to monitor the running state of the system, measure the process behaviour and analyse the credibility of the system. The operation mechanism of dynamic measurement realizes the monitoring of important nodes of the system and blocks the intrusion of malicious code into the system effectively.

4.4. Establishment of Trusted Verification Mechanism
The trusted verification mechanism consists of the basic trust base and trusted software base built in the mobile terminal. The most obvious advantage of smart mobile terminal is openness. At the same time, update third-party applications and system images can be update, which increases the risk of smart mobile terminal applications. Although the APK file of Android smart mobile terminal application needs to be signed before release, this signature is only used to identify the application developer. The signature does not need the authentication of a third-party certification authority without control.

Trusted verification operations can ensure dynamic trust during system operation including identity verification, state measurement verification, data encryption and decryption, etc. At the same time, it also includes controlling the computing node in the start-up phase and runtime, recording the measurement results, evaluating the trusted state, generating trusted logs, credentials and reports. Under the support of trusted root and dual architecture, the trusted verification mechanism constructs an all-round trusted verification system from firmware to application. The trusted verification mechanism can make viruses and Trojans "kill themselves without killing", which is equivalent to cultivating the immune ability for the mobile terminal system. Even if there are loopholes in the system or application, the immune mobile terminal is not easy to be used, resulting in the destruction of the system or data.

5. Conclusions
With the development of mobile communication technology, smart mobile terminal has gradually replaced the traditional computer system and penetrated into various industries. The traditional passive defence technology of “blocking and killing” shows technical deficiencies in dealing with the security
problems of smart mobile terminal platform. To solve the security problem of mobile terminal, this paper analyses the trusted computing technology of smart mobile terminal. Based on the analysis of current development status of trusted computing technology, the feasibility of introducing trusted computing technology into smart mobile terminals is proposed.

Acknowledgments
This work was supported by the Technical Research Program of the Ministry of Public Security under Grant 2020JSYJJC16.

References
[1] Wijayanto E and Suyoto S 2020 Development of smart workshop mobile application as information 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), pp 98-102.
[2] Lu G, Zhou Z and Wang S 2012 Overview in the principles of smart mobile devices 2012 International Conference on Computer Science and Information Processing (CSIP) pp 486-488.
[3] Smith N A, Camacho A C, Escobedo E J and Contreras J M 2020 A safety index for smart mobility using real-time crowdsourced data 2020 IEEE International Smart Cities Conference (ISC2) pp 1-8.
[4] Chen M, Li R, Li N and Chen L 2017 A mobile terminal operating environment security measurement framework 2017 10th International Conference on Intelligent Computation Technology and Automation (ICICTA) pp 241-244.
[5] Akram R N and Ko R K L 2014 Digital trust - trusted computing and beyond: A position paper 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications pp 884-892.
[6] Das P and Debnath S 2020 A trust computing model for future generation networks 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) pp 1-4.
[7] Xue M and Hu A 2011 A security framework for mobile network based on security services and trusted terminals 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing pp 1-4.
[8] Kim M, Kim Y and Ju H 2010 Design and implementation of mobile trusted module for trusted mobile computing IEEE Transactions on Consumer Electronics 56 (1) 134-140.
[9] Willink T 2020 Possibility-based trust for mobile wireless networks IEEE Transactions on Mobile Computing 19 (8) 1896-1909.