Advances in Intelligent Systems Research, volume 147

International Conference on Network, Communication, Computer Engineering (NCCE 2018)

Mobile Intelligent Terminal Based on SD Card Trusted Module Credibility Enhancement and Application Mode Research

Fei Wang[1, a)], Jie Qiang[2, b)] and Xinlai Dang[3, c)]

[1]*School of Space Engineering University, Beijing 101400, China.*
[2] *School of Space Engineering University, Beijing 101400, China.*
[3] *School of Space Engineering University, Beijing 101400, China.*

[a)] wangfei791009@163.com, [b)] easyravan@163.com, [c)] 296869149@qq.com

Abstract. Based on the security threats faced by mobile intelligent terminals in the Internet of Things, this paper proposes a trusted enhancement framework for Android mobile intelligent terminals based on the SD card trusted module. A trustworthy computing environment including Trusted Security Management Center Trust border and trusted network "one center, three layers of protection" credible security system, and put forward the system in the Internet of Things environment mode of use.

Key words: Trusted module, Mobile Intelligent Terminal, Trusted enhancement, SD Card.

INTRODUCTION

In recent years, with the continuous advancement of information construction, the Internet of Things system has been initially applied in the field of measuring and measuring and has realized the application of real-time monitoring of the tower structure and intelligent power monitoring. Due to its small size, rich functions and convenient use, mobile intelligent terminals have broad prospects in the management and application of the Internet of Things. However, the security issues faced by mobile intelligent terminals are more complicated than PC systems and are getting more and more attention from attackers.

Mobile intelligent terminal directly applied to the Internet of Things system will face the following threats, as shown in Figure 1.

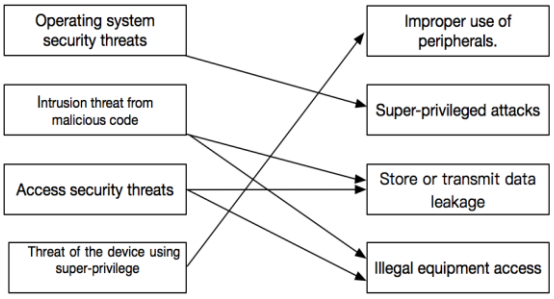

FIG. 1. Mobile intelligent terminal is facing the threat

(1) Mobile intelligent terminal operating system security threats

The mainstream operating system of the mobile intelligent terminal includes Android and iOS. Which iOS is a mobile operating system developed by the United States Apple is a private system is not open; Android operating system is based on the Linux kernel open operating system. No matter what kind of operating system is faced with the PC operating system similar vulnerabilities and other security issues, there is a vulnerability exploited by the attacker's risk.

The existing mobile intelligent terminal OS lacks mandatory access control measures and can't restrict App access to system resources according to a preset rule, which can easily lead to storage or transmission data leakage.

(2) Invasion threat of malicious code in smart terminal

Intelligent mobile terminals support rich peripheral interfaces and communication protocols, including infrared, Bluetooth, USB, WIFI, RFID, bar code scanning and GPRS, mobile network interfaces, etc., which may exist in the aspects of chip design, interface protocol and transmission protocol Security loopholes; and PC operating system as the same virus, Trojans and other malicious code threat. In recent years, with the popularization of smart mobile terminals, malicious code for smart mobile terminals has exploded.

Existing mobile intelligent terminal App without unified security detection and integrity protection, nor the installation of the App control, can't guarantee the security of the source of the App; In addition, although more or less for each App rights management and behavior monitoring means, but can't detect and control whether the App is subject to malicious code tampering.

(3) Terminal access security threats

Mobile intelligent terminals can access the Internet of Things through WIFI or SIM card networking. Relying solely on the 802.1X protocol and the access support of telecom operators are not enough to support IoT (Internet of Things) secure access, which is similar to WIFI cracking and pseudo-base station attack Ways to make it easier for attackers to access the Internet of Things, which in turn can pose a serious threat to IoT security.

In order to ensure the security application requirements of mobile intelligent devices in the IoT environment, the problems of lack of integrity protection of operating systems and APPs, lack of mandatory access control mechanisms, and proprietary security access control methods are faced in ordinary mobile smart devices.

(4) Threat of the device using super-privilege

Mobile smart devices include cameras, Bluetooth, wireless and microphones. Some malicious programs will force users to request permission to use the device. Malicious monitoring, recording and photographing may occur during the use of the Internet of Things, which may result in the threat of information leakage.

SD CARD-BASED MOBILE INTELLIGENT TERMINAL CREDIBLE ENHANCED ARCHITECTURE

In view of the threat to the use of mobile intelligent terminal in IoT environment, the paper proposes a credible enhanced architecture of mobile intelligent terminal based on SD card as shown in FIG. 2, including a trusted security management center and a credible enhanced system of mobile intelligent terminal.

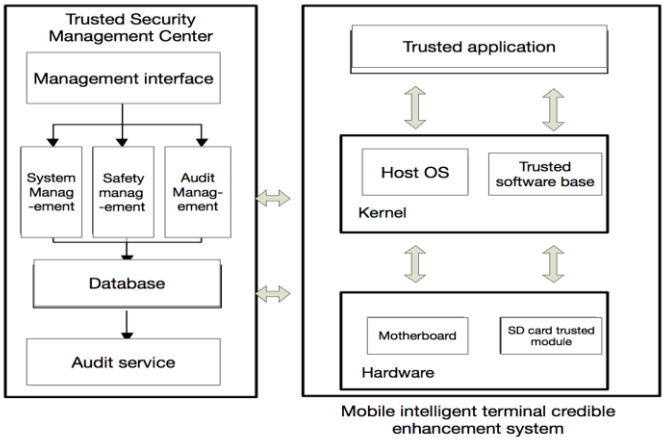

FIG. 2. SD card-based mobile intelligent terminal credible enhanced architecture

In view of the threat to the use of mobile intelligent terminal in IoT environment, the paper proposes a credible enhanced architecture of mobile intelligent terminal based on SD card as shown in FIG. 1, including a trusted security management center and a credible enhanced system of mobile intelligent terminal.

(1) Trusted Security Management Center is responsible for system management, security management and audit management of mobile smart trusted enhancement devices.

System Management is responsible for equipment user identity management, resource management, trusted hardware and software libraries and emergency response;

Security management is responsible for equipment benchmarking, tagging, policy management, authorization management and trusted connection management;

Audit management is responsible for equipment audit information strategy formulation, as well as audit information collection, summary, visual presentation.

(2) The mobile intelligent terminal credible enhancement system is composed of the SD card credible module and the credible software base:

SD Card Trusted Module connects with mobile intelligent devices via Micro SD / SD card slot to provide security services like certificate storage, digest value storage and encryption and decryption. It is the credible root of the entire chain of trust.

Trusted software base consists of 6 modules, including trusted boot, device control, software control, trusted connection, trusted authentication and trusted management agent. With the support of the SD card trusted module, a three-layer security protection system such as trusted computing environment, trusted border and trusted network is built for the mobile intelligent terminal.

Trusted Computing Environment: Building a trust chain that includes OS Loader, operating system, trusted software base and applications to enhance the terminal's ability to defend against viruses and Trojans; at the same time, dynamically measure the system and process to detect the integrity of the system and process space Whether or not sexuality has been tampered with, and proactively guarding against the security risk of exploiting system vulnerabilities to inject malicious code into the system and process space to penetrate the system infiltrate.

Trusted boundary: The security defense of the border is realized through mechanisms such as user identity authentication of the network access device, platform identity authentication, trusted status assessment of the platform, and network-based mandatory access control based on security policies.

Trusted Network: Creates a trusted and controllable network that meets the characteristics of "high real-time, high-reliability" services through trusted network connections that control the separation of traffic from data traffic.

MOBILE INTELLIGENT TERMINAL CREDIBLE ENHANCEMENT SYSTEM

The mobile intelligent terminal credible enhancement system mainly consists of the SD card credible module and the credible software base. The trusted software base consists of such modules as trusted boot, device control, software control, trusted connection, trusted authentication and trusted management agent, as shown in FIG.3.

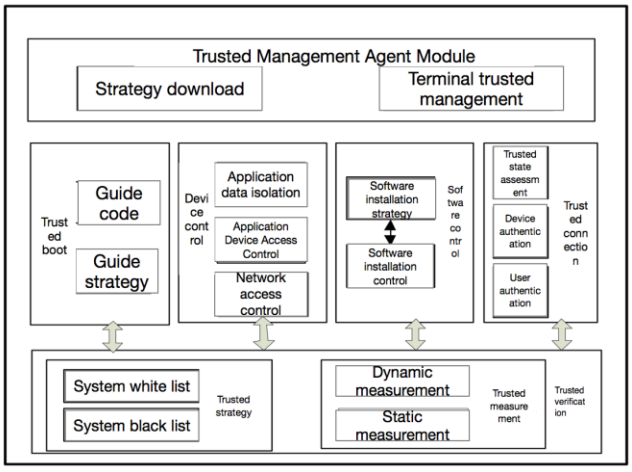

FIG. 3. Trusted software base composed

(1) Trusted software base composed

Trusted boot module is responsible for building the trust chain of the startup process. The trusted boot module is loaded during the OS loader loading phase. After the kernel is started to load, the master boot partition and the loaded kernel driver section are reversely measured first, and then the metrics are measured step by step so that the trust chain can be smoothly and smoothly delivered to the system. stage. The workflow shown in the figure.

(2) Equipment control module

The device control module is responsible for controlling application access behavior and restricting its unauthorized access to system devices. Its main features include:

a) Application data isolation

Device control provides isolated operating environment, application of configuration files, resource files and other private data resources are isolated as a unit, running applications can't resources outside strategy to read, write, delete and other operations.

b) Application Device Access Control

With no camera enabled, no camera, and audio recording are forbidden during the call.

c) Network access control

For applications to control TCP, UDP protocol network access capabilities, through policy control applications to access part of the network address or prohibit access to the network.

(3) Software control module

The software control module is responsible for the installation and maintenance of trusted applications of the mobile intelligent terminal, preventing the installation of malicious or unauthorized applications, and is also responsible for the software upgrade management. Its main features include:

Software Installation Policy It is responsible for communicating with Trusted Security Management Center for the latest policy information.

Software Installation Control is responsible for controlling software installation and updating based on policies.

(4) Trusted connection module

The Trusted Connection Module is responsible for building trusted and trusted network environments for trusted computing devices. Its main features include:

Device Authentication: Authenticates the identity of the device that is connected and refuses to allow unauthorized devices to connect to the network.

User Authentication: Based on the device authentication, user identity is authenticated, and non-authorized users are denied access to the network using authorized devices.

Trusted status assessment: Evaluate the trusted status of connected devices, determine whether the current status is trustworthy, and allow or deny access to the network according to whether the device status is trusted or not.

(5) Trusted verification module

Trusted authentication module based on credible strategies for mobile intelligent terminals for static and dynamic credible measurement, to provide support for the construction of trusted computing environment. Its main features include:

a) Trusted strategy

Including the system white list and application white list. The system whitelist consists of kernel trustworthiness metrics that allow for legal enforcement, such as the confidence metrics for kernel image files, kernel module files, system images, and system-important files; whitelists for application whitelists by application trust metrics that allow for legitimate enforcement Value composition.

b) Trusted measurement

Responsible for trusting all executable code against trustworthy policies, including static metrics of kernel files, system files, and applications prior to loading, preventing unauthorized executables from running, preventing system from being maliciously tampered with, or alien intrusive Illegal system applications, to ensure that the operating environment is credible; and process code segment, the kernel code segment, the module code segment, the system call table, interrupt call table, file system and network protocol stack dynamic measurement to ensure the credibility of the operation process.

(6) Trusted Management Agent Module

The Trusted Management Agent manages and configures the Trusted Enhancement Subsystem configuration management of the mobile intelligent terminal through the management interface, communicates with the Trusted Management Center, and forwards the instruction from the Trusted Management Center. Its main features include:

a) Terminal trusted management

Provide services such as application software for mobile intelligent terminals, white list policies, device control policies and trusted connection policies, and trusted status information of terminals to view and inquire.

b) Strategy Download / Audit Report

Update and download trusted policies and access control policies from the Trusted Security Management Center and report the collected trusted status information of the mobile intelligent terminal to the Trusted Security Management Center.

APPLICATION MODE AND EFFECT ANALYSIS

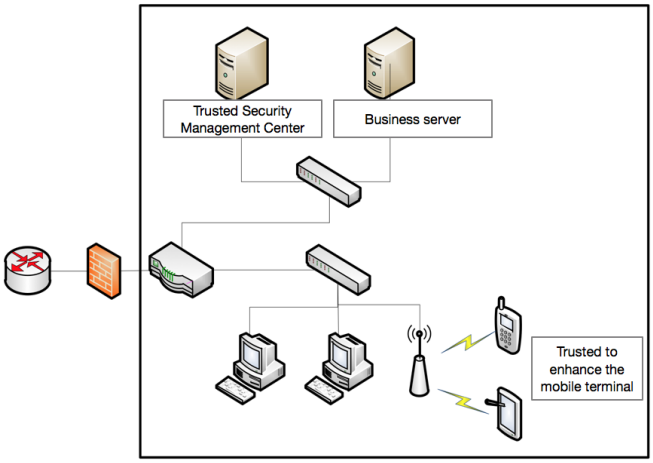

FIG. 4. Mobile intelligent terminal credible system to enhance application patterns

Mobile intelligent terminal credible system to enhance the application in the Internet of things as shown in Figure 4. Deploy Trusted Security Management Center servers in the backbone network. Mobile intelligent terminals (mobile phones and tablets) are required to install the trusted enhancement system of mobile intelligent terminals, with a trusted SD card module, access to the Internet of Things through the WIFI network, Business Management App implements device monitoring in the Internet of Things environment, as well as business access and other operations.

Mobile Intelligent Terminal Trusted Enhancement System can provide the following support for IoT security:

(1) Effectively prevent malicious code and operating system vulnerabilities caused by security threats

The use of SD trusted card and trusted software base to achieve the credible enhancement of the mobile intelligent terminal to ensure that the mobile intelligent terminal boot process credible to ensure that only legitimate and compliant application software to run and timely detection of " Known or unknown threat of malicious code intrusion and to control security issues caused by operating system vulnerabilities to a limited extent to provide a trusted computing environment for mobile terminals in the Internet of Things.

(2) Effective control of unauthorized terminals and untrusted terminals illegal connection threat

Through the device authentication of access equipment, user authentication and trusted status assessment, under the open access environment in the Internet of things to ensure that only legitimate, trusted mobile intelligent terminal access, denied IoT authorization and untrusted mobile intelligent terminal illegal connection.

(3) Effectively prevent information leakage threats due to the use of hyper-privileged devices

Through the application of data isolation, application access control and network access control, to achieve the IoT mobile intelligent terminal camera, Bluetooth, wireless, microphones and other equipment, effective management and control, effectively prevent the equipment due to super-use malicious monitoring, recording, photographing Other information leakage threats.

Based on SD Trusted Module Mobile Intelligent Terminal Trusted to enhance the framework and application mode for mobile intelligent terminals from the kernel, systems, applications to the network of trusted solutions, the establishment of a system of active defense security protection system, and it’s the application mode in the Internet

of Things gives suggestions, which are versatile, easy to deploy, and low in management complexity. It can provide effective theoretical and technical support for security construction in Internet of Things.

REFERENCES

1. Wei Xiong. Research on Android Mobile Intelligent Terminal Security Reinforcement Technology Based on Trusted Computing[J]. Wireless Communication and Mobile Internet Security,2017,41(5):84-85.
2. Zhen-dao Wang. A Trusted Security Solution for Embedded Terminals[J]. Computer Applications and Software,2016,33(1):230-234.
3. Shi-cai Zhan. Behavior-based remote certification scheme for mobile intelligent terminal platforms[J]. Computer System Application,2016,25(9):35-42.