High Secure Mobile Operating System Based on a New Mobile Internet Device Hardware Architecture

Gengxin Sun and Sheng Bin

International College of Qingdao University, Qingdao, China
sungengxin@qdu.edu.cn
Software Technical College of Qingdao University, Qingdao, China
icewine@126.com

Abstract

Mobile Internet as a new information and communication technology is growing fast. The security challenges facing from the Mobile Internet come from the mobile devices and access networks. A new Mobile Internet device architecture is proposed in this paper. Focusing on the characteristics of the new architecture, a high secure operating system with internal network structure is designed. There are two sub-kernels in the secure operating system, an inter-kernel data transmission protocol is implemented for communicating between two sub-kernels, which is connection-oriented and can provide reliable peer-to-peer connectivity. In this paper, we proposed the data transmission protocol implementation procedure and analyze protocol transmission efficiency.

Keywords: Mobile Internet, Operating System, Data transmission Protocol.

1. Introduction

The Mobile Internet refers to access to the World Wide Web from a mobile internet device, such as a smartphone or a feature phone, connected to a mobile network or other wireless network [1]. A mobile internet device (MID) is a multimedia-capable mobile device providing wireless internet access. They are usually designed to provide communication, information, entertainment and location-based services for personal use. The function of mobile internet device is always inferior to general computer.

The Mobile Internet device architecture is different from general computer. It usually uses MicroProcessor Unit (MPU), such as an ARM Cortex CPU, wireless radio and a touchscreen. Aiming to the special architecture, Mobile Operating System is needed.

Mobile Operating System is an operating system that operates a smartphone, tablet, PDA, or other mobile device. Modern mobile operating systems combine the features of a personal computer operating system with other features, including a touchscreen, cellular, Bluetooth, Wi-Fi, GPS mobile navigation, camera, video camera, speech recognition, voice recorder, music player, near field communication and infrared blaster [2]. The class of mobile operating system mainly included Windows CE, IOS, Android, Ubuntu Touch OS and Windows 7.

Due to the characteristics of the mobile internet device, security issues of Mobile Internet device compared to traditional general computer, there are some differences between them as following: (1) Due to the limited computing and storage capacity of Mobile Internet device, there is serious technology limitations for some security protection technique develop, for example, sophisticated encryption algorithm can not be used, large virus libraries cannot be stored. (2) Transmission method of malicious software is more diverse, whose concealment is
higher. (3) Mobile Internet is wireless access to the Internet via a cellular telephone service provider, which causes more easily to eavesdropping, surveillance and aggressive behavior. Currently, malicious software (such as viruses, Trojans, etc.) has constituted a major threat to the security of Mobile Internet device, continuously enhance of memory and chip processing capabilities give malicious software more living space, open operating system and application programming interfaces greatly facilitate the development and intrusion of malicious software, at the same time, the increasing Mobile Internet users create the environment for the spread of malicious software, so how to detect and protect from malicious software is essential to ensure security and privacy protection of Mobile Internet device.


Although above methods have enhanced the security of Mobile Internet device, they could not solve the fundamental security problem due to Mobile Internet device hardware architecture.

2. New Mobile Internet Device Architecture and Operating System

A new high secure hardware architecture of Mobile Internet device has been proposed by Fengjing Shao [7]. There are a CPU and two physically isolated system buses in new high secure architecture, which can ensure only one bus to be connected to CPU at the same time through Bus Bridge [8].

Mobile Internet device system is divided into two subsystems according to local bus and network bus. All network devices mounted on the network bus form network subsystem which connects to Internet. All storage devices and peripheral mounted on the local bus make up local subsystem which is isolated from Internet. Hardware-level isolation can effectively ensure the security of privacy data in local subsystem.

![Figure 1. The Secure Mobile Internet Device Hardware Architecture](image-url)
The new secure Mobile Internet device hardware architecture is shown in Figure 1. In order to support the new hardware architecture, a high secure dual-kernel operating system with internal network structure is designed in this paper. There are two sub-kernels in the operating system, local kernel and network kernel run individually in two subsystems. The two sub-kernels communicate with each other by shared transit cache mounted on the shared bus.

Inter-process communication of operating system is similar to inter-computer of network [9]. A sub-kernel is like a local area network; in each sub-kernel there is only a gateway process, which acts the role of gateway in local area network. The other processes except gateway process are named as user process. User process can only communicate with user process of another sub-kernel through gateway process, which is the data transfer interface between the sub-kernels, of the same sub-kernel. The topological structure of dual-kernel operating system is shown in Figure 2.

According to the characteristics of new Mobile Internet device hardware architecture, only one subsystem can use the CPU at any time, in other words, only one sub-kernel is active at the same time. So the two gateway process can’t directly communicate with each other, they must use the shared transit cache to transfer messages indirectly. The procedure of inter-kernel data transfer is shown in Figure 3.

3. Communication Mechanism of Dual-Kernel

The new Mobile Internet device hardware architecture combined with the high secure mobile operating system can effectively prevent from malicious software intrusion to local subsystem, but it also prevents the data getting from Internet. Therefore, there should be a secure communication mechanism of dual-kernel, which not only can prevent from network intrusion, but also can implement communication between two kernels. An inter-kernel data
transfer protocol is proposed and implemented for communicating between two sub-kernels securely.

3.1. Hardware Mechanism

There is a cache mounted on the shared bus, it plays a role of bridge and can be operated by the two gateway processes when transferring data between gateway processes.

The shared cache is divided into three parts: cache state block, head area and transit block area. The cache structure is shown in Figure 4.

![Figure 4. Shared Cache Structure](image)

In the initialization process, cache state block is allocated in the low-end of shared cache, their corresponding transit block are allocated in the high-end of shared cache, every head links its corresponding transit block to form head area which is made up heads pointing to transit block. A transit unit consists of a head and its transit block. There into, head is used to descript transit unit attributes; transit block is used to store data.

There are two kinds of transit unit: network transit unit and local transit unit. All the same type of transit units is linked to be a doubly linked circular list. So there are network linked list and local linked list in the shared cache. Transit cache state block contains a transit cache state structure which has three fields: network linked list head pointer, local linked list head pointer and residual count. Network and local linked list head pointer individually points to the first idle transit unit of the network and local doubly linked circular list, residual count indicates number of free transit unit in shared cache.

Transit units which are divided into idle transit unit and non-idle transit unit are also linked in a doubly circular list. In the beginning, every transit unit is idle transit unit, when data transmission happens between sub-kernels, idle transit unit would be obtained from head of doubly circular list and become a non-idle transit unit, which would be inserted into tail of the list. Therefore, idle transit units would be in the front of the list while non-idle transit units would be in the end of the list. The doubly circular list of transit units is shown in the Figure 5.
A pair of transit units which have the same ID is needed to finish data transmission between sub-kernels. Network transit unit receives data which is sent by gateway process of local sub-kernel. Similarly, Local transit unit receives data which is sent by gateway process of network sub-kernel. When data transmission between sub-kernels finished, the two units would be released.

3.2. Data Transfer Protocol Between Dual-kernel

In order to prevent from network intrusions via shared transit cache, a inter-subsystem data transfer protocol is designed. It is a connection-oriented protocol, which it can provide reliable peer-to-peer connectivity and ensure data transmission safely and inerrably between dual-kernel.

In data transmission process, data is in manner of packets stream. When data is written into or read from shared transit cache, data is in manner of file. The protocol format is shown in Figure 6.

<table>
<thead>
<tr>
<th>...</th>
<th>FSI</th>
<th>FBT</th>
<th>FS</th>
<th>FD</th>
<th>FET</th>
<th>ET</th>
<th>...</th>
</tr>
</thead>
</table>


**Figure 6. Data Transfer Protocol Format**

When using transfer protocol, gateway process of one sub-kernel acts as sender, gateway process of another sub-kernel acts as receiver at the same time.

As a connection-oriented protocol, data transfer protocol between dual-kernel must set up peer-to-peer connection before beginning data transmission. For meeting the security needs of high secure mobile operating system, the data transfer protocol uses four-way handshake based on signature verification to establish connection. In data transfer connection, the data transfer process which is used to send data is named sender gateway process, and the process which is used to receive data is called receiver gateway process.
Begin of creating a data transfer connection, the sender gateway process obtains a private key, and then connection request message with signature through the private key is generated. Receiver gateway process sends validation message with signature to sender gateway process after receiving connection request message, sequence number of validation message is the sequence number of request message adds to 1. Thus, sender gateway process would validate signature of validation message. Then, receiver gateway process randomly generates a initial sequence number and sends connection request message with signature to sender gateway process, sender gateway process receives connection request message, which would also send validation message with signature to receiver gateway process, sequence number of validation message is equal to the sequence number of request message adds to 1. The connection between two gateway processes would be completely established if receiver gateway process validates signature successfully. The above creating connection procedure of data transfer is shown in Figure 7.

![Figure 7. The Creating Connection Procedure](image)

Connection of gateway process in individual sub-kernel has been established, the dual-kernel can communicate with each other, when communication completed, the connection needs to be closed, which also needs four-way handshake signal. For closing data transfer connection, the sender gateway process sends a connection close message, whose sequence number is the next sequence number of sent message. After receiving connection close message, receiver gateway process sends validation message to sender gateway process, whose sequence number is that the sequence number of close message adds to 1. Then, receiver gateway process sends connection close message to sender gateway process, whose sequence number is also the next sequence number of sent message. Sender gateway process receives connection close message, it would also send validation message to receiver gateway process, whose close message sequence number is that receiver gateway process adds to 1. After completion of these procedures, the connection can be closed licitly. The procedure of closing connection is shown in Figure 8.
4. Protocol Performance Evaluation

According to concrete realization of data transfer protocol between dual-kernel, whose performance is analyzed in this Section.

Protocol transmission efficiency $E$ is the ratio of the requested effective data quantity and the total transfer data quantity. With increase or decrease of data transmission quantity, transmission efficiency $E$ increases or decreases consequently.

Supposing data transmission includes $n$ files, and every file size is $S$ bytes, thus, size of requested data $D$ is

$$D = n \times S \quad (1)$$

Connection request message size is $R_1$ bytes, relevant validation message size is $R_2$ bytes. Data quantity of creating connection size $C_{message}$ is defined as,

$$C_{message} = 2(R_1 + R_2) \quad (2)$$

Data stream prefix size is $Pf$, size of actual data transmission quantity through protocol $P_{data}$ is defined as,

$$P_{data} = n(Pf + S) \quad (3)$$

The total data transmission quantity $T_{data}$ is defined as,

$$T_{data} = C_{message} + P_{data} \quad (4)$$

According to Equation (1) ~ Equation (4), Transfer efficiency $E$ is defined as,
\[ E = \frac{D}{T_{data}} = \frac{1}{1 + \frac{Pf}{S} + \frac{2 \times (R_1 + R_2)}{n \times S}} \] (5)

Because of connection request message size, relevant validation message, and value of \( Pf \) are constant, from Equation (5) we can know, transfer efficiency \( E \) would change along with data transmission quantity (file size \( S \) or number of file \( n \)), and whose max is 1.

5. Conclusion

In the Mobile Internet device hardware architecture, in order to prevent from network intrusions via shared transit cache, in the high secure mobile operating system, a inter-subkernel data transmission protocol is implemented and used to control the inter-subkernel data transmission safety. The high secure mobile operating system can ensure security of the new Mobile Internet device architecture and be widely used other Mobile Internet device very well.

References


Authors

Gengxin Sun received his Ph.D. degree in Computer Science from Qingdao University, China in 2013. He is currently an Associate Professor in the School of Computer Science and Engineering at Qingdao University. His main research interests include embedded system, operating system, complex networks, web information retrieval and data mining.
Sheng Bin received her Ph.D. degree in Computer Science from Shandong University of Science and Technology, China in 2009. She is currently a lecturer in the School of Software Technology at Qingdao University, China. Her main research interests include embedded system, operating system, complex networks, cloud computing and data mining.