Mobile Ticketing System Employing TrustZone Technology

Wan Huzaini Wan Hussin, Paul Coulton, and Reuben Edwards

Department of Communication Systems, Lancaster University, LA1 4WA, UK

E-mails: (w.wanhussin, p.coulton, r.edwards)@lancaster.ac.uk

Abstract

Security in mobile commerce is becoming more important due to increasing demand from users wishing to perform online transactions over mobile devices. Security is one of the critical issues for successful adoption of mobile commerce both from an operator and user perspective. Although there are many aspects relating to security in this paper we concentrate on one of the current difficulties concerned with the provision of mobile receipt. Current systems depend entirely on the merchant providing the proof of purchase relating to a particular item or service and many users can experience difficulty if the system fails. Further, as current mobile devices do not offer any verifiable security over the data stored means that merchants can have little confidence in receipts stored on the device. In this paper we present a simple mobile receipt system that offers security both for customer and merchant based on the new TrustZone Architecture for ARM devices.

1. Introduction

Mobile commerce refers to the use of mobile handheld devices to conduct any electronic transaction or information interaction that leads to transfer of value in exchange for information, services or goods over wireless networks [1]. Examples of m-commerce application include mobile financial services, mobile context services, on-line games, tickets and mobile shopping. M-commerce enables consumers to play on-line games, trading stocks and get the latest sports results using mobile phones. It provides convenient, localization and personalized services to customers, employees and businesses. Indeed, m-commerce revolutionizes the way businesses interact with consumers and with each other resulting in the creation

of new business opportunities and the improvement of the efficiency of business processes and quality of services to consumers.

It is anticipated that the growth of m-commerce is dependent on the increasing confidence of wired Internet users to conduct transaction online. In 2004, the global m-commerce market was worth \$200 billion with 130 million customers generating approximately 14 billion transactions per year [2]. The convergence of mobile technology and the Internet has encouraged the development of more sophisticated mobile phones with greater capabilities, offering a range of services and functionalities. To date, worldwide mobile subscribers are about 1.5 billion [3]. This figure is expected to rise 33 percent by 2007 to two billion. Due to the fact that mobile phones outnumber personal computers, m-commerce industry should take advantage to offer better services to consumers.

Despite generating billions in revenue especially in countries with high levels of wireless adoption, there are still issues and challenges to be addressed. M-commerce will become a commercial success only when the services offered are easy and convenient for consumers to use. The complexity of the payment infrastructure should be made invisible to avoid unnecessary confusion. It is also vital to develop mobile payments based on existing methods and standards in order to be easily accepted and adopted.

Perhaps, the most important factor to consider when conducting monetary transactions is security. More value of a transaction, the higher security protection should be. Security covers two main elements: channel security and content security [4]. Channel security is how secure the channel when transaction is being conducted particularly when passing the sensitive information from one end to another. On the other hand, content security is primarily concerned with the information that has been received. According to Group Inc. it is predicted that in 2005, 85 percent of wireless security incidents will be

device related rather than over-the-air related [4]. Therefore content security can be considered as the most important area of handheld security.

This paper discusses a simple mobile receipt system in mobile phones that employs TrustZone technology. It describes the TrustZone architecture for ARM devices and explains a typical mobile ticketing system. Then, it introduces the mobile ticketing system using TrustZone technology developed for this paper. Finally, it draws conclusions on the benefits of such system.

2. TrustZone technology

Operating systems are by their very nature open and complex system and very difficult to secure. This makes the devices used as part of the mobile commerce infrastructure vulnerable to many forms of attack. TrustZone introduces security structure by providing a separate secure domain to provide on-device security protection to ensure data integrity. To systemize the implementation of secure systems, it uses a hardware-enforced security domain to the core architecture and memory system, in other words it isolates part of the chip architecture purely for secure information. It also disassociates system security from complex non-secure applications as illustrated in Figure 1 [5]. This means devices are capable of storing non-secure data and sensitive information separately within the secure domain in the structure. This can be deployed in the mobile ticketing system. The later part of this paper will explain how TrustZone technology can be deployed in the mobile ticketing system which enhances the security measures in mobile commerce.

Figure 1. TrustZone architecture

3. Mobile ticketing system

Mobile ticketing is one of the m-commerce services currently being offered by wireless network operators. To purchase a cinema ticket, for example, the user needs to receive an electronic receipt as prove of purchase in order to get the cinema ticket. The production of such electronic receipt must satisfy a list of requirements: it needs to be recognized by the delivery entity; it can be used as proof showing that the holder of the receipt has made the purchase and goods can be delivered; it cannot be falsified and it cannot be duplicated or used twice [6]. These characteristics are to ensure the originality of the ticket purchased by user. However, a typical receipt system relies on the reliability of the merchant's system in getting the correct code and information about the wanted tickets. It is lacking the on-device security protection. Once the tickets information is stored in the mobile phone it is vulnerable to attacks and information can be falsified. Figure 2 illustrates a typical receipt model.

Figure 2. Typical structure of m-ticketing system

Therefore, there is a requirement to secure the information on the physical devices so that information received during the process is genuine and verifiable without relying solely upon the merchant. Therefore,

this paper suggests such a solution for a mobile ticketing system using TrustZone.

4. M-ticketing with TrustZone

This section defines the stages of operation for a new model of mobile ticketing system to purchase a movie ticket by using the TrustZone technology for on-device security protection. This solution secures content of the data stored on physical devices within the mobile phone core-hardware.

4.1 System implementation

Figure 3. Structure of m-ticketing system with TrustZone

4.1.1 Purchasing ticket

A user browses the internet using a mobile phone and selects the movie to watch and the preferred time. This ticket is considered as time-based, as it is only valid during the time of the movie is shown and

therefore a proof of purchase must be easily identified for both user and cinema operator.

4.1.2 Payment process

Once the user agreed with the terms and conditions, the user then makes a payment using mobile phone. The process of sending the user's information is done based on standard Internet security protocol Secure Socket Layer (SSL) which applies standard 128-bit decryption over a wireless line. At this stage, the user sends the details to purchase the ticket to the operator's terminal. The user can make the payment directly to his credit/debit card or billing the amount of the ticket purchased on user's network provider or deduct user's prepaid amount.

4.1.3 Encryption process

Upon receiving the request of ticket(s) from the user, the operator then sends an encrypted ticket electronically to the user. Then, the encryption key is sent to the operator by the user's mobile phone.

The operator sends an encryption key to TrustZone on the user's mobile phone to enable the user to open ticket details. The operator should have a list of "trusted digital tickets" which is processed using mobile phones with TrustZone technology. This enables the protection of on and off-chip memory and peripherals from software attack. Since the security elements of the system are designed into the core hardware, therefore there is no issue of ticket being tampered [5].

4.1.4 Ticket details and confirmation

By using the encryption key stored in TrustZone, the user can open and check the ticket details including unique ticket number, time of purchased, movie title, show time and amount paid. Once the user satisfies and agrees with the information, the user sends acknowledgement to the operator. The ticket details would be used as part of the encryption process so that a new encryption key could be created by the merchant if required to validate a ticket.

4.1.5 Cinema entrance using e-ticket

The user then passes the encrypted ticket to get access to the appropriate movie entrance by connecting their mobile phone to the terminal available at the counter via infrared or Bluetooth. This verifies the

digital ticket stored in the TrustZone. The operator then prints out the physical ticket/receipt to the user or provides an instant access to the “e-ticketer”.

There should be no dispute of the originality of the ticket as it is maintained encrypted within the user’s mobile phone. The ticket details are still available and accessible and will enable the merchant to verify the encrypted ticket should they have lost the information from their system.

In addition, the operator has less liability and responsibility. If the operator’s system fails during or after the user purchased the ticket, the user has no problem in entering the cinema because the proof of ticket details are genuine as it is stored in the TrustZone.

4.2 Benefits of proposed system

With the deployment of the TrustZone technology within a mobile phone, it is expected that the security of mobile commerce services will improve significantly particularly in the mobile ticketing system.

At the moment, the only security that protects the mobile commerce transactions is solely dependent on the gateway or tunnel security encryption when information is passed through from one end to another. By introducing the embedded TrustZone technology within mobile phone hardware, it adds another layer of security that gives on-device protection. This solution protects sensitive data within the mobile phone to secure the content of information on top of the existing security channel in mobile commerce infrastructure.

Data stored in TrustZone technology within a mobile phone is reliable and is not alterable by the user or anyone because the way it is secured within the hardware itself. Unlike many encryptions security software in the market, TrustZone will not allow information kept in a mobile phone to be attacked by viruses and intruders to falsify the information.

This mobile ticketing solution not only adds another layer of security but also remains transparent to the end user because the data is stored in a secure domain within the operating system [4]. As this security protection happens in the background, user never sees the add-on security and gives no different whatsoever from user’s point of view. In addition, it will have no effect on the performance because the TrustZone works within the core hardware level.

5. Conclusion

M-commerce offers a wide range of new mobile applications to consumers making life more convenient and providing easy access to information from a mobile phone. In order to increase the adoption of m-commerce, it is vital to provide more secure environment for mobile transactions. Therefore, this paper has introduced the deployment of TrustZone technology in a mobile phone that will add another level of security within the core hardware architecture. This would increase the level of confidence of the consumers and benefit the wireless network providers, application developers and manufacturers as they are able to offer better secure services to consumers. As a result, more consumers are expected to engage in mobile commerce transactions which will contribute to a wider adoption of mobile commerce services.

6. References

- [1] “Connecting Mobile Consumers and Merchants”, NOKIA White Papers, <http://whitepapers.zdnet.co.uk/0,39025945,60082474p-39000516q,00.htm>, 03/01/2005
- [2] Mobilocity.net, “The m-Business Builder for the New Era: Understanding the Fundamentals of M-Commerce - A Mobile Internet 101”, <http://whitepapers.zdnet.co.uk/0,39025945,60010321p-39000514q,00.htm>, 12/01/2005
- [3] cnews, “Nokia:Two Billion Mobile Phone Users by 2007”, <http://cnews.canoe.ca/CNEWS/TechNews/TechAtHome/2004/06/14/pf-499181.html>, 16/12/2004
- [4] F-Secure Corporation, “Content Security at Hand: A White Paper on Handheld Device Security”, www.f-secure.com/products/white-papers/hhsecurity021122.pdf, 17/01/2005
- [5] York, Richard, “A New Foundation for CPU Systems Security: Security Extensions to the ARM Architecture”, ARM Limited, May 2003
- [6] Ee-Peng Lim and Keng Siau, *Advances in Mobile Commerce Technologies*, IDEA Group Publishing, London, 2003, pp. 34-40