Mobile Commerce: Security Challenges and Technologies

Dr. Manish Shrimali
Department of Computer Science & IT, JRN Rajasthan Vidyapeeth (D) University, Udaipur 313001, India

Abstract - Mobile commerce is a major application domain for mobile devices, enabling users to perform commercial transactions wherever they go. However, these applications require a high level of security. In this paper, we identify the special characteristics of m-commerce and reflect on some important security issues and technologies.

Keywords: M-Commerce, e-commerce, PC, Security, Mobile, m-commerce, Security Challenges, Internet

I. INTRODUCTION

The term e-commerce (electronic commerce) denotes business processes on the Internet, such as the buying and selling of goods. There is a distinction between B2B (business-to-business) and B2C (business-to-consumer) markets. In the first case, the business processes are carried out between businesses; in the latter case, they are carried out between businesses and end consumers. This general definition of e-commerce does not say anything about the kind of device that the end user employs to gain access to the Internet. The underlying technology could be wire line (e.g. using a home PC as end user device) or wireless (e.g. using a mobile phone as end user device). The term m-commerce (mobile commerce) is all about wireless e-commerce, that is, where mobile devices are used to do business on the Internet, either in the B2B or B2C market. As such, m-commerce is a subset of e-commerce. With the omnipresent availability of mobile phones (and other mobile devices), m-commerce services have a promising future, especially in the B2C market. Future applications include buying over the phone, purchase and redemption of ticket and reward schemes, travel and weather information, and writing contracts on the move. However, the success of m- commerce very much depends on the security of the underlying technologies.

As such, security can be regarded as an enabling factor for the success of m- commerce applications. In this paper, we discuss the main areas of m-commerce that are relevant to security, namely:

- *Network Technology* – In m-commerce, all data is transmitted via a mobile telecommunication network. Here, we consider existing network and service technologies for 2G (2nd Generation), 3G (3rd Generation) and other wireless systems.

II. M-COMMERCE AND ITS DIFFERENCES TO E-COMMERCE:

In comparison to e-commerce, m-commerce offers both advantages and disadvantages. The following list summarizes the advantages of m-commerce:

- *Ubiquity* – the end user device is mobile, that is, the user can access m-commerce applications in real time at any place.
- *Accessibility* – accessibility is related to ubiquity and means that the end user is accessible anywhere at any time. Accessibility is probably the major advantage by comparison with e-commerce applications involving a wired end user device.
- *Security* – depending on the specific end user device, the device offers a certain level of inherent security. For example, the SIM card commonly employed in mobile phones is a smart card that stores confidential user information, such as the user's secret authentication key. As such, the mobile phone can be regarded as a smart card reader with smart card.
- *Localization* – a network operator can localise registered users by using a positioning systems, such as GPS, or via GSM or UMTS network technology, and offer location- dependent services. Those services include local information services about hotels, restaurants, and amenities, travel information, emergency calls, and mobile office facilities.
- *Convenience* – the size and weight of mobile devices and their ubiquity and accessibility makes them an ideal tool for performing personal tasks.
- *Personalization* – mobile devices are usually not shared between users. This makes it possible to adjust a mobile device to the user's needs and wishes (starting with the mobile phone housing and ringtones). On the other hand, a mobile operator can offer personalised services to its users, depending on specified user characteristics.

The following list summarizes the main disadvantages of m-commerce:

- Mobile devices offer limited capabilities. Between mobile devices these capabilities vary so much that end user services will need to be customized accordingly.
- The heterogeneity of devices, operating systems, and network technologies is a challenge for a uniform end user platform. For this reason, standardization bodies consisting of telecommunication companies, device manufacturers, and value-added service providers integrate their work (see Section 4.5). For example, many current mobile devices implement an IP stack to provide standard network connectivity. At the application level, the Java 2 Micro Edition (J2ME) offers a standardized application platform for heterogeneous devices.
- Mobile devices are more prone to theft and destruction. According to a government report, more than 700000 mobile phones are stolen in the UK each year. Since mobile phones are highly personalized and contain confidential user information, they need to be protected according to the highest security standards.
- The communication over the air interface between mobile device and network introduces additional security threats (e.g. eavesdropping.).

2.1 Security challenges

As mentioned earlier, m-commerce is not possible without a secure environment, especially for those transactions involving monetary value. Depending on the point of views of the different participants in an m-commerce scenario, there are different security challenges. These security challenges relate to:

- the mobile device – confidential user data on the mobile device as well as the device itself should be protected from unauthorised use. The security mechanisms employed here include user authentication (e.g. PIN or password authentication), secure storage of confidential data (e.g. SIM card in mobile phones) and security of the operating system.
- the radio interface – access to a telecommunication network requires the protection of transmitted data in terms of confidentiality, integrity, and authenticity. In particular, the user's personal data should be protected from eavesdropping.
- the network operator infrastructure – security mechanisms for the end user often terminate in the access network. This raises questions regarding the security of the user's data within and beyond the access network. Moreover, the user receives certain services for which he/she has to pay. This often involves the network operator and he/she will want to be assured about correct charging and billing.
- the kind of m-commerce application – m-commerce applications, especially those involving payment, need to be secured to assure customers, merchants, and network operators. For example, in a payment scenario both sides will want to authenticate each other before committing to a payment. Also, the customer will want assurance about the delivery of goods or services. In addition to the authenticity, confidentiality and integrity of sent payment information, non-repudiation is important.

III. SECURITY TECHNOLOGIES RELEVANT FOR M-COMMERCE

In this section, we give an overview of the technologies, which are relevant to secure m-commerce transactions. We focus on those network and service technologies that are specific to mobile devices.

3.1 Transport Layer Security

The above technologies provide security for the wireless link between mobile customer and access network or access device. If the access network is considered secure and the m- commerce transaction is completely handled within the access network, this may be sufficient. But often, an m-commerce transaction involves parties outside the access network (merchant, payment service provider etc.). In this section, we discuss end-to-end security for mobile devices.

SSL/TLS

The SSL/TLS (Internet Secure Socket Layer) protocol is by far the most widely used internet security protocol. Its main application is the HTTPS protocol (HTTP over SSL), but it may also be used as a standalone protocol. SSL requires a bidirectional byte stream service (i.e. TCP). SUN has implemented a client side version of SSL for limited devices, called KSSL (Kilobyte SSL). KSSL does not offer client side authentication and only implements certain commonly used cipher suites, but it has a very small footprint and runs on small devices using the J2ME platform.

WTLS

The WAP forum has standardized a transport layer security protocol (WTLS) as part of the WAP 1 stack. WTLS provides transport security between a WAP device (e.g. a mobile phone) and a WAP gateway which performs the protocol transformation to SSL/TLS. Hence, no real end-to-end security is provided and the WAP

Gateway needs to be trusted. Note that the WAP Forum now proposes a WAP 2 stack which is a classical TCP/IP stack on a wireless bearer medium. This permits end-to-end SSL/TLS sessions.

3.2 Service Security

Here, we discuss the security of network services which can be used for m-commerce transactions.

Intelligent Network

With the introduction of the IN (Intelligent Network) technology to GSM networks, additional services could be realized. The IN architecture for GSM (called CAMEL, Customized Application for Mobile Enhanced network Logic) was adapted from the fixed network standard ETSI Core INAP, and was originally designed for circuit switched calls. The IN platform provides some flexibility for the generation of m-commerce services. IN handling can e.g. be triggered by a specific called party, a calling party, an USSD string (requiring CAMEL phase 2), mobile originating SMS (requiring CAMEL phase 3) or mobile terminating SMS (requiring CAMEL phase 4). The security of an IN service depends on the underlying GSM or UMTS network security and on the specific characteristics of the service application.

Parlay/OSA

Parlay/OSA (Open Service Access) is an initiative of the industry (Parlay group), ETSI and 3GPP and aims at introducing standard interfaces to network services. The IN platform and their SS7 based protocols like INAP and CAP are relatively complex and generation of services is reserved to operators and manufactures. Now Parlay offers standard application programming interfaces which allows service provisioning on IT platforms using standard middleware (e.g. CORBA). The Parlay/OSA framework then provides gateway functionality between applications and Service Capability Features (SCF's) of the IN. M- Commerce applications can then access core network functionality, e.g. inquire status and location of a mobile user, send messages or place calls. Parlay/OSA applications are portable among networks which is usually not possible with IN services. Security is an important issue, since Parlay/OSA potentially opens the core network to intruders. Parlay/OSA specifies authentication and encryption on the application layer. But the security also depends on the underlying network architecture, e.g. firewalls and strict policies should protect core network components.

SMS

SMS (short message service) is a very popular data service for GSM networks. Although SMS messages are limited to 160 characters, a considerable number of m-commerce scenarios are based on this service. The sender and receiver of an SMS is identified by its IMSI which an attacker cannot forge without breaking the GSM/UMTS security mechanisms (e.g. by cloning a SIM card). Hence SMS messages can be used for authentication (at least towards the network). Furthermore, SMS data is transmitted in the GSM (UMTS) signaling plane, which ensures the confidentiality of messages. However, the protection ends in the GSM or UMTS network, there is no end-to-end security, and the network operator and its infrastructure (e.g. SMSC, Short Message Service Centre) must be trusted (when no other security mechanisms are applied to the SMS message, confer section on SIM/USIM Applications below).

USSD

The GSM Unstructured Supplementary Service Data (USSD) service allows data communication between a mobile station and either the HLR, VLR, MSC or SCP in a way transparent to the other network entities. Unlike the asynchronous SMS service, an USSD request opens a session which may induce other network operations or an USSD response before releasing the connection. Mobile originated USSD may be thought as a trigger for a network operation. USSD works with any mobile phone since the coded commands are entered in the same way as a phone number (e.g. *123#1234567890#).

With USSD, roaming can be offered for prepaid GSM customers before IN services (CAMEL) are implemented in a network. Another USSD application (requiring CAMEL phase 2) is replenishing a prepaid account by incorporating the voucher number in an USSD string. In principle, any transaction, e.g. a payment operation, could be triggered by USSD data. USSD possesses no separate security properties; instead it relies on the GSM/UMTS signaling plane security mechanisms.

SIM/USIM Application Toolkit

The SIM and USIM Application Toolkits (SAT and USAT respectively) allow operators and other providers to create applications which reside in the SIM/USIM. These applications can e.g. send, receive and interpret SMS.

IV. CONCLUSIONS

There will be no m-commerce without security of the underlying technologies. In this paper we discussed security issues relating to network and service technologies. One of the main future challenges will be to unify payment solutions, providing the highest possible level of security.

REFERENCES

[1] GSM 02.09 version 7.0.1 Release 1998. Digital cellular telecommunication system (Phase 2+); Security Aspects.

[2] 3GPP TS 33.102 3.9.0 Release 1999, 3rd Generation Partnership Project.

[3] S. Kent, R. Atkinson. Security Architecture for the Internet Protocol. RFC 2401.

[4] M. Walker, T. Wright, Security Aspects. In: F. Hillebrand, GSM and UMTS: The Creation of Global Mobile Communication, John Wiley and Sons Ltd.

[5] WAP Forum, Wireless Transport Layer Security, Version 06-Apr-2001.