IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol-6, Special Issue-5, Jun 2018 E-ISSN: 2347-2693

Secure Mobile Transactions Processing System

Narinder Bali[1*], Raghav Mehra[2], Arvinder Bali[3]

[1*]Research Scholar: Department of Computer Sciences, Bhagwant University. Ajmer, Rajasthan
[2]Associate Professor: Department of Computer Sciences, Bhagwant University. Ajmer, Rajasthan
[3]Student: IK Gujral Punjab Technical University Punjab

*Corresponding Author: email: balinarinder7@gmail.com Tel:9419262571

Available online at: www.ijcseonline.org

***Abstract*:** Due to the advent of the Internet, electronic business transactions have exploded around the globe. The radical evolution of computers and advancement of technology in the area of hardware (smaller size, weight, low power consumption and cost, high performance) and communications has introduced the notion of mobile computing .Mobile wireless market is increasing by leaps and bounds. Today, new technologies that allow cellular (mobile) phones and other handheld devices to access the Internet have made wireless business transactions possible. This phenomenon is known as mobile commerce or M-Commerce. Mobile payments (m-payments) are increasingly being adopted by organisations as a new way of doing business in the 21st century. Recently, more and more people have begun using their mobile phones as a method of payment for online shopping and banking. Mobile payments have become easier than ever. Present security issues of mobiles, payments however, still require improvement. Mobile Commerce is an evolving area of e-commerce, where users can interact with service providers through a mobile and wireless network using mobile device for information retrieval and transaction processing .The challenge for mobile network lie in providing very large footprint of mobile services with high speed and security. Online transactions using mobile devices must ensure high security for user credentials and it should not be possible for misuse. the principal drivers of a resurgent and increased interest in mobile payments. In addition, advances in software and hardware security techniques have made trusted financial transactions possible from these devices. This white paper examines the current state and nature of the mobile payments market, some of the relevant enabling technologies, and looks at the relevant risk, security and assurance issues that security and audit professionals will want to consider when developing and evaluating mobile. Payment services. (TPS) is an information processing system for business transactions involving the collection, modification and retrieval of all transaction data. Characteristics of a TPS include performance, reliability and consistency. TPS is also known as transaction processing or real-time processing.

Key word: Bluetooth, Cryptographic operations, M-Commerce, Micropayment protocol, M-payment, Wireless security, WLAN security

1. Introduction:

Mobile devices with minimal computing capability, such as the most basic cell phones, are also out of scope because of the limited security options available and the limited threats they face. This section discusses the features of mobile devices, focusing on what makes mobile devices different from other computing devices, particularly in terms of security risk. This section also presents high-level recommendations for mitigating the risks that these mobile devices currently face.M-payment is a point of sale payment made through a mobile device such as cellular telephone, a Smartphone or a personal digital assistant (PDA) Mobile payment system provides attractive opportunities to, merchants financial and users. These opportunities were simplicity and ease of a-payment transaction for the user and they also enable merchants to access customer information and target specific customer through various incentive programs such as discount coupons and reward programs. The growth of mobile payment transactions over the last decade has been largely enabled by increasing speeds of mobile network connections. The rapid proliferation of portable devices and the world wide penetration of mobile cellular subscription..Using m-payment a person with a wireless device could pay for items in a store or settle a restaurant bill without interacting with any staff members. According to orange Mobile Payment (Danish Company) the entire transaction should take not more than 10 seconds.In order to provide a secure and comprehensive m-payment, the payment scenario should be designed so that it performs fast and simple for the end-use , but secure and comprehensive for the provider. An efficient payment scenario takes efficient steps in performance. The critical items in each step are the payment messages containing critical information being transferred between participating parties. These messages are objects to which security should be applied.

2. Defining Mobile Device Characteristics

Two main areas in which e-commerce grew significantly in recent years are Internet banking and conducting business on the Internet. With Internet banking, the way customers make use of banking services has changed. They do not have to go to ATM (Automatic Teller Machine) terminals or stay in-line at a bank branch to withdraw or transfer money between accounts, but simply log on to a bank's website which provides. Internet technology offers extensive ranges of services such as electronic mails, file transfers, etc., and one of the most popular services offered on the Internet is "Electronic Commerce" (or e-commerce). E-commerce is becoming bigger technological wave that has changed the way by which business is being conducted. According to business transactions, many e-commerce websites enable their customers to browse for goods and services offered in their virtual stores remotely from the customers' personal computers. Not only physical goods, such as books (e.g. www.amazon.com) or laptop computers (e.g. www.dell.com), are offered, but electronic goods, such as music, digital images, video clips, or electronic novels, are also available. Customers simply select desired products or services and pay for them by credit-cards or electronic cash cards. More importantly, these virtual stores are open 24 hours a day, 7 days a week. Mobile device features are constantly changing, so it is difficult to define the term "mobile device". However, as features change, so do threats and security controls, so it is important to establish a baseline of mobile device features. The following hardware and software characteristics collectively define the baseline

- A small form factor
- At least one wireless network interface for network access (data communications). This interface uses Wi-Fi, cellular networking, or other technologies that connect the mobile device to network infrastructures with connectivity to the Internet or other data networks.[1]
- Local built-in (non-removable) data storage
- An operating system that is not a full-fledged desktop or laptop operating system1
- Applications available through multiple methods (provided with the mobile device, accessed through web browser, acquired and installed from third parties) The list below details other common, but optional, characteristics of mobile devices. These features do not define the scope of devices included in the publication, but rather indicate features that are particularly important in terms of security risk. This list is not intended to be exhaustive, and is merely illustrative of common features of interest as of this writing.
- Network services: o One or more wireless personal area network interfaces, such as Bluetooth or near-field communications o One or more wireless network interfaces for voice communications, such as cellular o Global Positioning System (GPS), which enables location services
- One or more digital cameras/video recording devices
- Microphone

Guidelines For Managing The Security Of Mobile Devices

- **Storage:**

Support for removable media o Support for using the device itself as removable storage for another computing device Built-in features for synchronizing local data with a different location (desktop or laptop computer, organization servers, telecommunications provider servers, other third party servers, etc.[2]

2.1 High-Level Threats and Vulnerabilities

Mobile devices typically need to support multiple security objectives. These can be accomplished through a combination of security features built into the mobile devices and additional security controls applied to the mobile devices and other components of the enterprise IT infrastructure. The most common security objectives for mobile devices are as follows:

- Confidentiality—ensure that transmitted and stored data cannot be read by unauthorized parties

- Integrity—detect any intentional or unintentional changes to transmitted and stored data

- Availability—ensure that users can access resources using mobile devices whenever needed. To achieve these objectives, mobile devices should be secured against a variety of threats.

Mobile devices often need additional protection because their nature generally places them at higher exposure to threats than other client devices (e.g., desktop and laptop devices only used within the organization's facilities and on the organization's networks). Threat modeling helps organizations to identify security requirements and to design the mobile device solution to incorporate the controls needed to meet the security requirements. Major security concerns for these technologies that would be included in most mobile device threat models are listed below. [3]

2.2 Use of Untrusted Applications

Mobile devices are designed to make it easy to find, acquire, install, and use third-party applications from mobile device application stores. This poses obvious security risks, especially for mobile device platforms and

application stores that do not place security restrictions or other limitations on third-party application publishing.

2.3Limitations of Wireless Environments

Performing payment transactions in wireless environments mainly suffers from resource limitations of mobile devices and characteristics of wireless networks
Resource Limitations of Mobile Devices

Mobile devices have the following limitations:
Computational capability of their processors is comparatively lower than that of personal computer (PCs).

They have limited storage which affects available cryptographic algorithms applied to them .A mobile device with the above limitations is not capable of performing high computational cryptographic operations such as public-key operations which are used in a fixed-network device such as a PC. Due to the low computational capability of mobile devices, completing a payment transaction on a mobile device takes longer period of time than that on a PC which has higher processing capability. [4]

3. Technologies for Mobile Device Management

Centralized mobile device management technologies are a growing solution for controlling the use of both organization-issued and personally-owned mobile devices by enterprise users. In addition to managing the configuration and security of mobile devices, these technologies offer other features, such as providing secure access to enterprise computing resources. This section provides an overview of the current state of these technologies, focusing on the technologies' components, architectures, and capabilities. [5]

3.1 Components and Architectures

There are two basic approaches to centralized mobile device management: use a messaging server's management capabilities (often from the same vendor that makes a particular brand of mobile device operating system), or use a product from a third party, which is designed to manage one or more brands of mobile device operating systems. It may be possible with the latter approach to have a single product that can manage multiple brands of mobile device operating systems desired for use within an enterprise. However, a product provided by a mobile device manufacturer may have more robust support for the mobile devices than third party products [6]

3.2 Additional information.

If there is not a centralized management solution, or certain mobile devices cannot use it, then mobile devices have to be managed individually and manually. In addition to the additional resources expended, there are two major security problems with this: The security controls provided by a mobile device often lack the rigor of those provided by a centralized mobile device management client application. For example, a mobile device often supports only a short passcode for authentication and may not support strong storage encryption. This will necessitate acquiring, installing, configuring, and maintaining a variety of third-party security controls that provide the missing functionality. It may not be possible to manage the security of the device when it is not physically present within the enterprise. It is possible to install utilities that manage devices remotely, but it will require significantly more effort to use such utilities to manually apply updates and perform other maintenance and management tasks with out-of-office mobile devices.

3.3 Capabilities

This section describes security services commonly needed for security management of mobile devices. These services may be provided by the mobile device operating system, enterprise mobile device management (MDM) software, or other security controls. These services apply to the entire mobile device (if it is fully managed) or to the mobile device's secure sandbox/secure container , unless explicitly noted otherwise. These services are equally relevant for centrally managed or individually managed mobile devices Designing the architecture includes the selection of mobile device management server and client software, the placement of the mobile device management server and other centralized elements, and the architecture of any virtual private network (VPN) solutions.[7]

 Authentication.

Authentication involves selecting device and/or user authentication methods, including determining procedures for issuing and resetting authenticators and for provisioning users and/or client devices with authenticators. Authentication includes access to or integration with existing enterprise authentication systems.

 Cryptography.

Decisions related to cryptography include selecting the algorithms for encryption and integrity protection of mobile device communications, and setting the key strength for algorithms that support multiple key lengths.

 Configuration requirements.

This involves setting minimum security standards for mobile devices, such as mandatory host hardening measures and patch levels, and specifying additional

security controls that must be employed on the mobile device, such as a VPN client.

Device provisioning.

It is important to determine how both new and existing devices will be provisioned with client software, authenticators, configuration settings, etc.

Protection.

Information stored on the mobile device and communications between the mobile device and the organization are protected in accordance with the established requirements.

Authentication.

Authentication is required and cannot be readily compromised or circumvented. All device, user, and domain authentication policies are enforced.

Applications.

The applications to be supported by the mobile device solution function properly. All restrictions on installing applications are enforced. All restrictions on uninstalling applications (such as enterprise mobile device management software) are enforced.[8]

Management.

Administrators can configure and manage all components of the solution effectively and securely. The ease of deployment and configuration is particularly important. Another concern is the ability of users to alter device/client software settings, which could weaken mobile device security. [9]

Performance.

All components of the solution provide adequate performance during normal and peak usage. It is important to also consider the performance of intermediate devices, such as routers and firewalls.

4. Technology of Mobile Payment

We studied and assessed technologies in mobile payment systems from the existing researches as described below P. Pukkasenung and R. Chokngamwong

- SMS—Short Messaging Service is a text messaging service used to send and receive short text messages. The maximum length of messages is less than 160 alphanumeric characters, to and from mobile phones.
- WAP—Wireless Application Protocol is a technology which provides a mech-anism for displaying internet information on a mobile phone.
- NFC—Near Field Communication is the communication between contactless smart cards and mobile phones.
- RFID—Radio Frequency Identification is a method of identifying an item wirelessly using radio waves
- Smart Card—Smart cards and plastic cards normally appear in the same shape as credit cards are embedded with a chip or microprocessor that can handle and store 10–100 times more information than traditional magnetic-stripe cards.[10]
- Internet—the internet is a publicly accessible, globally interconnected network. It uses the internet protocol to enable the exchanging and sharing of data among computers in the network
- USSD—Unstructured Supplementary Services Data is a mechanism of trans-mitting information via a GSM network. Unlike SMS, it offers a real-time connection during a session
- IVR—Interactive Voice Response is a telephony technology where the users can interact with the database of a system without any human interaction
- Magnetic—Data is stored in a magnetic stripe on a plastic card. It is read by swiping the card in a magnetic card reader.

4.1 Cryptography Concept

Cryptography is a technique used to secure data protection from the hacker, which can be classified into the following three groups:[11]

- Symmetric Key Cryptography—It is the encryption methods in which both the sender and receiver share the same key. The algorithms, in general, consist of DES (Data Encryption Standard), 3DES (Triple DES) and AES (Advance Encryption Standard)[12]

- Asymmetric Key Cryptography—It is also known as public key cryptography, a class of cryptographic algorithms which requires two separate keys. One key is secret and the other key is public. The algorithms are RSA (Rivets, Shamir and Adelman) and ECC (Elliptic Curve Cryptography).[13]

- Hash Function—It is a public one-way function that maps a message of any length into a fixed-length, which serves as the authenticator. A variety of ways of a hash code can be used to provide message authentication.[14]

5. Conclusion

As a conclusion, to discover the best secure mobile payment protocol, the protocol standard must be the same all over the world and the communities and industries must be adopting the standard., it also provides the transaction security level and non repudiation property that is necessary for macro payments. [15]. Although the proposed technique has been optimized for the current GSM network, but its modular design enables it to accept future improvements of the mobile network technology and infrastructure, such as EMS and MMS, with minimum change in the protocol structure

References

1. McKitterick D, Dowlin J State of the art review of mobile payment technology. https://www. scss.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-24.pdf

2. Fun TS, Beng LY, Roslan R, Habeeb HS (2008) Privacy in new mobile payment protocol. World Acad Sci Eng Technol 2:198–202

3. Fun TS, Beng LY, Razali MN (2013) Review of mobile macro-payments schemes. J Adv Comput Netw 1(4)

4. A. Basaure "Preliminary research on existing and planned mobile data service solutions and value systems in leading markets", Helsinki University of Technology HUT, 2004

5. Singh A, Shahazad KS (2012) A review: secure payment system for electronic transaction. Int J Adv Res Comput Sci Softw Eng 2(3)

6. Ahamad SS, Udgata SK, Nair M (2014) A secure lightweight and scalable mobile payment framework. In: FICTA 2013. Advances in intelligent system and computing, vol 247. Springer International Publishing, Switzerland

7. Mathew M, Balakrishnan N, Pratheeba S (2010) A study on the success potential of multiple mobile payment technologies. In: Technology management for global economic growth (PICMET), Proceedings of PICMET '10

8. Smart Card Alliance (2008) Proximity mobile payments business scenario: research report.

9. Li Y, Wang Y Secure electronic transaction. http://people.dsv.su.se/*matei/courses/ IK2001SJE/li-wang_SET.pdf

10. Fun TS, Beng LY, Likoh J, Roslan R (2008) A lightweight and private mobile payment protocol by using mobile network operator. In: Proceedings of the international conference on computer and communication engineering 2008 May 13–15, Kuala Lumpur, Malaysia, 2008

11. Isaac JT, Zeadally S (2012) An anonymous secure payment protocol in a payment gateway centric model. In: The 9th international conference on mobile web information system (MobiWIS). Elsevier12.Sekhar VC, Sarvabhatla M (2012) Secure lightweight mobile payment protocol using symmetric key techniques. In: International conference on computer communication and informatics (ICCCI), pp 1–6, 10–12 Jan 2012

12. Tripathi DM, Ojha A (2012) LPMP: an efficient lightweight protocol for mobile payment. In: 3rd national conference on emerging trends and applications in computer science (NCETACS)

13. "certicom," [Online]. Available: http://www.certicom.com/index.php/an-introduction-to-the-uses-of-eccbased-certificates. [Accessed 01 01 2013].

14. "RSA Laboratories," RSA, [Online].Available:http://www.rsa.co/rsalabs/node.asp?id=2129. [Accessed 10 12 2012].

