Secure Mobile Finance Application (MFA) in Bluetooth Technology using SSL

Azni Haslizan, Dayang Hanani, Kartinah Zen, Seleviawati Tarmizi
Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak

ABSTRACT

Mobile commerce is a major application domain for mobile devices, which enabling user to perform commercial transactions wherever they go. However, these applications require a high level of security. This paper describes how Mobile Financial Application (MFA) performs in Bluetooth technology and identifies some important security issues. One of important security issues in Bluetooth is user authentication. It can only authenticate devices and not users. We use Secure Socket Layer (SSL) as a user authentication solution to be incorporated at the application-level security to provide encryption and build secure tunnels between the Bluetooth device and the network. This paper also describes implementation of user authentication in Bluetooth technology using SSL.

1.0 INTRODUCTION

Mobile commerce was proclaimed as the next technological revolution and opportunity for companies to provide a new distribution channel for customers. According to a new research paper prepared by analysts at the Gartner Group [Sanchez, J. 1999], the large number of mobile phone users, combined with emerging technologies, including wireless application protocol and Bluetooth, means that at least 40 percent of consumer e-commerce transactions outside of North America will take place from mobile devices by 2004. This shows that mobile commerce is growing rapidly as a handy business tools and is fast becoming one of the most important technology in consumer commerce in very near future.

Mobile commerce can be defined as “any transaction with a monetary value that is conducted via a mobile telecommunication network”. There are myriad of potential mobile commerce applications around such as mobile banking and brokerage service, mobile money transfer and mobile micro-payments. These services could turn a mobile device into a business tool, replacing bank, ATM and credit cards by letting a user conduct financial transaction with mobile money. With the use of Bluetooth technology, a consumer could purchase something like a can of drink from a vending machine without ever taking out a card or cash. Using Bluetooth, a small charge could be deducted from a smartcard included in the phone. Bluetooth would send signals from the machine to the smartcard, deducting the cost from the user's account. These applications somehow could improve services to customers and enhance customer satisfaction. However, there are issues such that could arise from this technology, is that a mobile or user's devices are open to attack from passers-by is a real threat. For example, hackers could create applications that would withdraw money from a user's smartcard and place it in their accounts without the user knowing, since physical contact is not necessary. Besides that the problem is also on the devices which infecting each other with viruses. Therefore, secure transactions are required before any of these applications are widely deployed.

Existing Bluetooth application only limited to non-secure application such as downloading pictures from PDA. Bluetooth enable device is not very popular in mobile commerce application because there is lack of implementation in high-level security application. Bluetooth’s own security scheme at the link layer does not meet the requirements of mobile commerce applications [Paul, 2002]. In addition, security is a crucial requirement of mobile commerce system because the sensitive financial information could not travel over untrusted networks. Due to above problem, there is a need to find a solution to provide user with the essential level of security. If the problem solved, Bluetooth enable device will become more usable and widely used especially in Mobile commerce application.

2.0 BLUETOOTH TECHNOLOGY

Bluetooth [Bluetooth SIG, 2003] is a specification for a low-cost, low-power, short-range wireless communication technology that provides wireless connectivity between mobile devices such as cellphones, personal digital assistants (PDA) and portable computers. Not only can it be used as a cable replacement on point-to-point bases but can also form ad hoc networks in a master-slave formation called Piconets, which allow users to create Personal Area Networks (PAN) between devices. Bluetooth network system is relatively secure, but there are still a number of weaknesses in the standard. One of the weaknesses of the general Bluetooth protocols comes from the device address scheme.

Bluetooth can only authenticate devices and not users. Normally the user does not have to authenticate himself to the device. When devices go missing, unauthorised third parties will thus normally be able to use them immediately. Device authentication is based on the share of the same link key between the two units in the process. This link key could be the initialization key, or a previous link key. If this link key was the initialization key, everything relies on the PIN shared by the two units. Since it is the only information used to create the initialization key, and therefore, the PIN also used for devices

authentication purposes. To achieve better Bluetooth security, the process of selecting long and random PIN codes is not the best solution to secure the connection. Additional local protective measures such as user authentication should be implemented where Bluetooth devices are used.

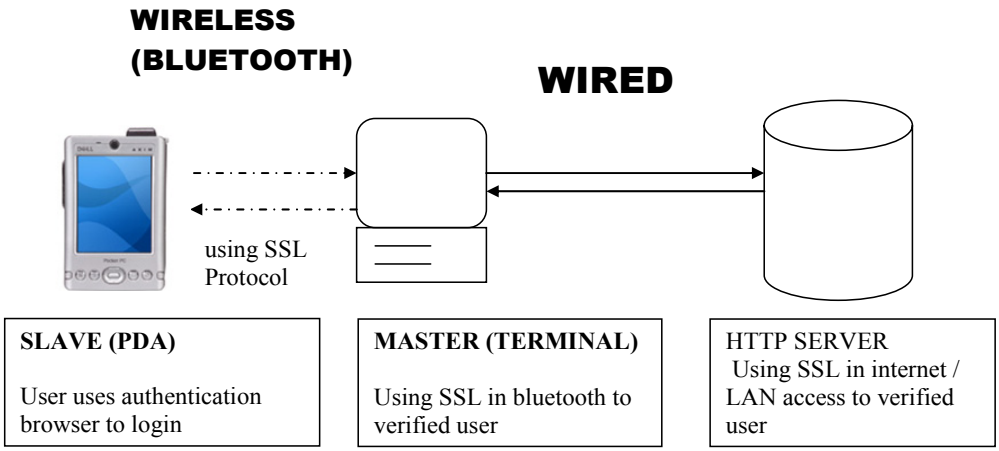
3.0 USER AUTHENTICATION USING SSL

User authentication is the means by which the device determines the identity of a user. It allows the device to verify that the user is entitled to use the service. In wired application, SSL protocol is mostly used to authenticate user especially web servers and browser based applications. It provides a reliable end-to-end service. As an added security measure, SSL can be employed at the application level in Bluetooth protocol. SSL provides communications privacy through symmetric encryption and integrity through message authentication Code (MAC) [Kambourakis,2004]. The successful use of the SSL protocol in the wired Internet has proved its usability and effectiveness. A bluetooth device that supports SSL protocol can be used for various applications, like electronic transactions, including those which require the exchange of private information like passwords, PINs, or credit card numbers. It can ensure their secure transport through the network, and providing the user with the essential level of confidence and certainty.

SSL protocol in Bluetooth technology is used to ensure that the mobile device only signs data from the right terminal and conversely that the terminal only accepts data from the right mobile. It uses public key certificates to protect information during authentication. The purpose of public key certificates is to bind public key values to identities. Identities unambiguously designate persons or systems. The binding is asserted by trusted third parties, named certificate authorities (CAs). A CA signs this binding and thereby guarantees that a certain public key belongs to a certain identity. The CA signature also protects the certificate against modification. Therefore certificates can be sent across unsecured channels and stored in unsecured storage. Entities can simply check the validity of a certificate by verifying the CA signature. Certificates typically have a limited lifetime, which is included in the certificate attributes. Certificate authorities can be organized hierarchically, which means that a certificate of a CA is signed by its parent-CA. The origin of the hierarchy is called a *root CA*. The path from a client certificate up to a root CA is called a *certification path*. Root CAs are unique within organizations that act as trusted third parties, like Swisskey, VeriSign, Thawte ,or Entrust. Invalidated certificates are placed on public certificate revocation lists (CRLs).

This protocol makes attacks like mention above impossible. This can be done when the client proves its identity by signing a hash value that is computed from all the handshake messages exchanged between client and server. After hash value has been computed by the terminal, it is sent to the mobile via Bluetooth link. The hash value is secured by appending the MAC that is parameterized with the authentication keys that was established before. After the signing operation is performed, the signature of the hash value is sent back to the terminal. From there it is passed on to the SSL server as the content of a certificate verify message.

Below is an overview of all components involved in implementing this project:



4.0 CONCLUSION

There will be no mobile commerce without security of underlying technologies. Many applications are

still relying on third-party implementations of SSL. SSL will remain a transport layer security protocol, that is, it will provide a secure channel for confidential and authenticated communication. In this form, it will be a basic security building block. Additional security features will not be added to the protocol itself, but should be added within the application. Although user authentication is an option within SSL, it is an example of a critical security feature which is typically provided on top of SSL.

This paper describe user authentication using SSL in Bluetooth environment. The objective of this project is to design an authentication framework in auto configuration environment for Bluetooth communication based on SSL security concept. Besides, the project will evaluate the effectiveness of adapting SSL based authentication protocol and tailor an appropriate protocol according to the specific requirements. This project is at the preliminary stage and expected to be completed in year 2005.

REFERENCE

Bluetooth Special Interest Group, www.bluetooth.org,2003

C. Allen and T. Dierks. The TLS Protocol, Version 1.0. Internet RFC 2246, Jan.1999.

Corner,Mark, "Transient Authentication for Mobile Device",University of Michigan, 2003

Gregory Lamm Et Al, "Bluetooth Wireless Networks Security Features", Proceedings of the 2001 IEEE

Juha, "Bluetooth Security", 2000, Helsinki University of Technology

Jun-Zhao Sun Et Al, "Design, Implementation, And Evaluation Of Bluetooth Security", 2001, University of Oulu, Finland.

Kambourakis, Georgios Et Al, "Performance Evaluation of Public Key-Based Authentication in FutureMobile Communication Systems" Journal on Wireless Communications and Networking 2004:1

Nathan, "Bluetooth Demystified", 2001, McGrawHill

Nikhil, "An Overview of Bluetooth Security", 22 February 2001, SANS Institute

O. Freier, P. Karlton, and P. C. Kocher. The SSL Protocol, Version 3.0. home. netscape.com/eng/ssl3/draft302.txt, Nov. 1996.

Paul, "Knowing Bluetooth Has Security Vulnerabilities,Why Talk About It?",Washington DC,www.TDISecurity.com, 2002.

Sanchez, J. Mobile technologies like Bluetooth to push e-commerce. Available at: http://www.infoworld.com/cgi-bin/displayStory.pl?99112.enbluetooth.htm , (1999).