Trust Management by Making a Comparative Analysis of Wireless Devices and Web

Kamini
Department of Computer Applications
Chandigarh Group of Colleges, Landran
Kamini_girdhar08@hotmail.com

Krishan Tuli
Department of Computer Applications
Chandigarh Group of Colleges, Landran
mca.krishantuli@gmail.com

Abstract

The security plays an important role in today world for wireless networks and for wired network. When we are using the mobile phone for accessing the internet from the web server all the wireless communication protocols are transferred to the web server. Two Different protocol s are used for providing a communication through the mobile phones to www server. Protocols used for wireless devices are different from the protocol used at wired devices. There can be communication mismatch problem can be occur in between if two different protocols are used. To solve this problem gateway is place in between the wireless devices and www server. The gateway acts as intermediate between the two different protocols .This paper focuses on the how the communication take place between the two different devices and what kind of problem can be occur and how to solve that problem. This paper focuses on implementing an authentication method in between the gateway so that end to end security can be improved .This paper also emphasis on the comparison of all the layers used for wireless devices with the wired devices.

Keywords: Protocol, Devices, Networks

Introduction

The mobile phones in today life become important for doing all kind of e-commerce transaction. The WAP protocol is used for making all the communication possible through the mobile phone. The TCP /IP protocols are used for making all the communication possible through the web server. Security plays an important role in computer networks. All the communication which is passed from client to server it should be very secure. For security reasons different protocols are used at different end. One protocol is required at client side and other protocol is used at server side. Two way authentications is become necessary for making a communication through wireless and wired networks. When any communication take place from mobile phones to www server then one protocol is called WTLS is used by WAP and another TLS is used by www server. The WTLS protocol is derived from TLS only difference is that WTLS is used for the mobile phones. The structure of paper is as Follows .Section 2 discusses about the review of literature. Section 3 discuss about the comparison analysis of wireless and wired devices. Section 4 discuss about the trust management between the client and server.

Review Of Literature

Discuss about the two end-to-end security supported protocols. An industry implemented security protocol, Wireless Transfer Layer Security (WTLS), and an academic proposed security protocol, Integrated Transfer Layer Security (ITLS) will be introduced. The current specification of WTLS does not provide total end-to-end security because WTLS-enabled gateway will leak plaintext during data transmission to the server. ITLS was created based on fixing WTLS security holes. A comparison of ITLS and WTLS demonstrates that ITLS provides stronger protection in gateway and offers a more secure channel than WTLS. Unlike in WTLS, where server trusts gateway, clients is the ITLS security partner of server in ITLS. All the encryption and decryption will be doubled on the client-side. Due to the limited resource on the client side (mobile devices), ITLS will perform slower than WTLS. They proposed a modified ITLS that will increase ITLS performance in addition to providing the same security level as current ITLS.

Discussed about the More and more applications are being accessed through wireless systems, including commerce, medical, manufacturing, and others. Wireless devices have become an extension of corporate databases and individuals. Their security compromises are as serious as any attack to the corporate database and may have damaging effects on the privacy of individuals and the protection of assets of an enterprise. Wireless devices include cellular phones, two-way radios, PDAs, laptop computers, and similar. These are normally portable devices with limitations of weight, size, memory, and power.

Discussed about the trade-off is security versus processing and transmission time. In this paper, an analytical performance model for public-key cryptosystem operations in WTLS protocol is developed. Different handshake protocols, different cryptosystems and key sizes are considered. Public-key cryptosystems are implemented using state-of-the–art performance improvement techniques, yielding actual performance figures for individual cryptosystems. These figures and the analytical model are used to calculate the cost of using public-key cryptosystems in WTLS. Results for different cryptosystems and handshake protocols are comparatively depicted and interpreted. It has been observed that ECC (Elliptic Curve Cryptography) performs better than its rival RSA cryptosystem in WTLS. Performance of some stronger ECC curves, which are not considered in WTLS standard, is also analyzed in this paper.

Discussed about the cryptographic protocols are designed for entity authentication and key establishment. The WTLS handshake protocol is a cryptographic protocol that performs authentication and key establishment for secure WAP communication, and an AKC protocol including key authentication and confirmation of key possession. But it has weakness in active attack because it uses variable key exchange mechanism through hello messages.

Discussed about the Wireless Application Protocol (WAP) is a protocol stack for wireless communication networks. WAP uses WTLS, a wireless variant of the SSL/TLS protocol, to secure the communication between the mobile phone and other parts of the WAP architecture. This paper describes the security architecture of WAP and some important properties of the WTLS protocol. There are however some security problems with WAP and the WTLS protocol. Privacy, data

Comparison Analysis Of Wireless And Wired Devices

Type	Wireless Devices	Wired Devices
User interface	The user interface used for WAP is through the built in mini browser in mobile phone.	The user interface used for wired devices is through the internet explorer, Mozilla, opera etc used by web.
Security Protocol	The security protocol used for wireless devices is called WTLS.	The security protocol used for wireless devices is called TLS.
Capacity	The mobile phones limited bandwidth and less memory .Due to this heavy computations does not performed by security devices	The wired devices has more capacity as compare to mobile phones .Due to this heavy computations is performed by security devices
Use of Gateway	The WAP communication is passing through the gateway to web server.	All the encrypted data of wired devices is passed directly to server.
Language	The WML language is used by wireless devices.	The HTML language is used by wired devices.
Transport layer protocol	The protocol used by transport layer is called WDP.	The protocol used by the transport layer is called UDP.
Session layer protocol	The protocol used for maintaining the session is called WSP.	The protocol used for maintaining the session is called HTTP.
Transaction Layer protocol	The WTP protocol is used at transport layer.	The TCP/IP is used at transport layer.

WAP WIRELESS COMMUNICATION

WAP stands for wireless application protocol which provides the internet facilities and various telephonic services to digital mobile phones and wireless terminals. This protocol works for various wireless network environment and provide web page available on low resolution device.WAP devices are used for various web application, internet browsing, email and searching purpose.

WAP is the worldwide standard for providing Internet communications and advanced telephony services on digital mobile phones, pagers, personal digital assistants and other Wireless terminal.WAP means Wireless Application Protocol. Wireless means Lacking or not requiring a wire or wires: pertaining to radio transmission. Application means a computer program or piece of computer software that is designed to do a specific task. Protocols mean a set of technical rules about how information should be transmitted and received using computers. WAP is the set of rules governing the transmission and reception of data by computer applications on, or via, wireless devices like mobile phones. WAP allows wireless devices to view specifically Designed pages from the Internet, using only plain text [6]. Wireless devices provide the computing device with limited CPU, memory and battery life and a simple user interface. The WAP specification addresses these issues by using the best of existing standards and developing new extensions when needed. The WAP solution leverages the tremendous investment in web servers, web development tools, web programmers and web applications while solving the unique problems associated with the wireless domain.

The basic structure of WAP is as follows.

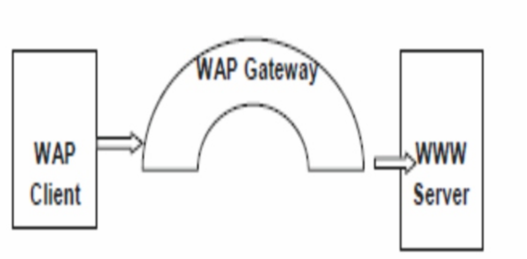

Figure 1. WAP structure

In the above diagram 1 the WAP client wants to connect to the Internet, all the communication passes through the WAP gateway[7]. This WAP gateway translates all the protocols used in WAP to the protocols used on the Internet. The Wireless transport layer security protocol is used by WAP Gateway to provide communication between the WAP client and WAP gateway[8]. The Transport layer security protocol is used to communicate between the gateway and www server.

Pros & Cons Of Wtls

Pros

- The protocols works in conjunction with PKI (public key infrastructure) and wireless cookies for providing the security solution.PKI uses digital certificates to secure application platform and browsers.
- The WTLS provide data security, integrity, privacy, authentication of WAP devices.

Cons

- Wireless devices consume less CPU power, less memory and more battery life when we used encryption techniques normally it consume a great deal of CPU usage, memory and bandwidth.

- Wireless networks provide less bandwidth, stability and reliability then the wired networks.

TLS Protocol Stack

The TLS is used to provide data integrity and security for network communication[9]. They use cryptographic methods to encrypt the data at the transport layer from end to end. The application layer used HTTP, FTP, Telnet and others. The SSL/TLS operates on a layer between the transport layer and application layer. In this position it can support multiple application layer protocols by securing the application data before sending it to transport layer.

The TLS security protocol is divided into four specialized protocol

The Handshake protocol is responsible for the cipher suite negotiation, the initial key exchange and the authentication of the two sides. The alert protocol offers some signalling to the other protocols. It can help informing the peer for the cause of failures and other error conditions the record protocol offers symmetric encryption, data authenticity and optionally compression.

Trust Management

Trust is important factor in security which provides relationship among the security protocols. When communication take place between client and server, Trust is required at both sides. The trust management is used for managing whether client is connecting to correct server and server is connected with trusted client. Both parties exchange the certificates with each other. This certificate is called trusted certificate which exchange by the client and server machine. The WTLS security protocol is based on TLS which is used for providing the data security and integrity between the two parties when they are communicate through the intrenet.The following three types of authentication is provided by security protocol.

1. Anonymous: This type of authentication is made between the client and server without exchanging certificates between them
2. Server side authentication: In this authentication method the server is authenticated by sending a security certificate to client. This is called one way authentication because no certificate is send from client side.
3. Client side authentication: In this authentication both client and server authenticate each other by sending a security

Conclusion

The paper focuses on the literature study of various protocols used for wireless devices and wired devices. Trust management between the client and server becomes a important factor in today date. This trust management is providing the information regarding whether the correct client is connected to correct server. Two parties exchanges certificates with each other to maintain trust. In future trusty path would be created for providing a communication between the client and server.

References

[1] Albert Levi, Erkay Savas." Performance Evaluation of Public-Key Cryptosystem Operations in WTLS Protocol".

[2] Complete WAP Security from Certicom.Available : www.certicom.com pages 5-12 Website link http://www.tutorialspoint.com/wap/wap_introduction.htm"

[3] Dave Singel´ee, Bart Preneel." The Wireless Application Protocol (WAP)". September 2003.

[4] Eduardo B. Fernandez, Imad Jawhar, Maria M. Larrondo-Petrie, and Michael VanHilst." An overview of the security of wireless networks" November 19, 2004".

[5] Jongcheol Moon*, Bonghwan Kim*, Sokjoon Lee*, Yoojae Won." A HANDSHAKE PROTOCOL ANALYSIS OF WAP WTLS".

[6] Karygiannis, Tom, and Les Owens. "Wireless network security." NIST special publication 800 (2002): 48.

[7] Security Issues in WAP and WAP Enabled Devices link http://www.users.cs.umn.edu/~htalkad/files/wap.pdf.Pages 34

[8] Younhee Kim, Chun-kit Wong, *George Mason University."* Comparison of WTLS and ITLS in Wireless end-to-end secure network (December 2002)".