Key Resolution of Reencryption by Providing Paging in Between the Gateway

Kamini
Research Scholar (PHD)
Punjab Technical University,
Jalandhar- Kapurthala.

Rajiv Mahajan, PhD.
Professor and Head
Global Institute of Management,
And Emerging Tech, Amritsar

Parteek Sharma
RIMT Institute of and
Technology,
Mandi Gobindgarh, India.

ABSTRACT

The Internet use in mobile has increased day by day .Every user want to access the Internet through mobile phones instead of laptop because of its feature like small in size and portable. When mobile user wants to access the Internet on mobile then all the request goes to the wireless gateway .The gateway acts as intermediate between the two points either it can be from wireless to wired or vice versa. The request of mobile phone is transferred from WAP device to web server through the gateway .The gateway is also a protocol translator which translate all the protocols used by wireless device to wired network. The problem of existing system was hole in the gateway .This paper has discussed about the problem of the WAP gateway .This paper focused on implementation of hashing technique in between the networking gateway to provide a solution of Re-encryption.

General Terms

Protocol Translator, Wireless Client, Hashing

Keywords

WAP, Security, Client, Server, gateway

1. INTRODUCTION

The number of users who use the Internet on their personal computer or laptops is decreased day by day because of mobility increased very fast. The mobile has low cost and price is less as compare to laptop PC and desktop computer. Most of Internet plans are available in today for mobile is very low cost and every middle class family people can make the use of Internet. The WAP enabled mobile phones is available today for using the Internet on mobiles. WAP browser is available for mobiles for using the Internet services like tickets booking, food order, and e-banking at any time.WAP browser is available with full graphic display and it include a micro browser. The main function of WAP is to communication with web server installed in the mobile phone networks [1].The security protocols are used in between when there is communication required between client and server for accessing the Internet from web server. The WTLS protocol is designed for wireless application which is required for client and the server to authenticate for wireless transaction. The TLS Protocol is used for providing a communication between the client and server to authenticate with each other for wired transaction. In between the gateway two way encryption and decryption is used between the client and server for wireless networks and wired networks. The problem was that when wireless client was to communicate with wired server all the request for communication goes to gateway .The gateway encrypts all the wireless traffic and decrypt by the client for wireless transactions. The gateway then converts all the wireless protocols in to wired protocols when communication has to pass through wireless client to wired server.Re-enryption us required in between the gateway for transferring all the packets from wireless client to wired server. The problem of Re-encryption is that the data of wireless networks can be hacked by any one because data is in air. To solving the problem of Re-encryption one new security protocol has been introduced which will work in between the gateway. This new introduced protocol will work for providing the common security for wireless network and wired networks.

The remaining structure of paper is as follows. Section II describes the review of literature for security protocol used in wireless and wired server. Section III describes the Re-encryption problem what is Re-encryption, how it take place. Section IV describes the solution of Re-encryption. Section V discuss about the use of paging in between the gateway so that end to end security problem is improved. Section VI concludes the paper.

2. REVIEW OF LITRATURE FOR SECURITY PROTOCOL USED IN WIRLESS AND WIRED SERVER

The literature has study for protocol used by wireless client and wired server. The WTLS protocol is based on the transport Layer security protocol (TLS). The main idea behind the WTLS and TLS is same which provide the communication between the mobile client and web server [2].The WAP gateway is a act as bridge between the WTLS and TLS security protocol. When the WAP client and web server exchanges the data between the TLS and WTLS protocol and all the communication held between them is unencrypted for a small fraction of time inside the WAP gateway [3]. From the SSL and TLS security protocol provides a security on Internet when transaction take place .In the similar way WTLS is working for mobile phones for any kind of e-commerce transaction over the wireless Internet [4]. The main difference between the TLS and WTLS is on the base of performance evaluation is that the client side activity is performed on WTLS rather than TLS .The use of mobile phone for Internet is low processing power and low data transfer rate of wireless transaction ,in that case some precautions are required from the side of WTLS[5]. WAP devices use WTLS instead of SSL, due to the assumed WAP client resource constraint, the basic WAP configuration involves a WAP gateway that translates between the various WAP protocol and the corresponding Internet protocol [6]. . WTLS is based on TLS, but there are a few differences in the wireless version that specifically relate to the low bandwidth and memory requirements of current mobile data communications [7]. Future versions of the WAP specification may address shortcomings in WTLS. The transport layer used E-commerce to E-commerce security specification which is used for the elimination of the decryption and re-encryption in the WAP gateway is called WAP Forum draft. Here, a WAP client's request would be redirected using an XML document [8]. WTLS is getting popular day by day for providing privacy, data integrity, authentication for application used by mobile phones and for other wireless devices like PDA and cellular phones. Millions of devices using WTLS are expected to be worldwide before the end of the year 2000 [9].

A web service used for the mobile phones is increasingly day by day but still there is one problem of mobile security [10]. Secure communication is an intrinsic requirement of today's world of on-line transactions. Whether exchanging financial, business or personal information, people want to know with whom they are communicating (authentication) and they wish to ensure that the information is neither modified (data integrity) nor disclosed (confidentiality) in transit[11]. Most of the text in the WTLS specification has been adopted word to word, from the TLS specification. However, many of the changes that were made by WAP Forum have led to security problems [12]. Both side authentications in web services the certificate is used for the identification of valid user and valid server. This authentication is required to determine whether valid user is connected to valid web site [13]. The effectiveness of this protection depends on a variety of mostly unrelated issues such as cryptographic key size, protocol design, and password selection [14].

Gateway is necessary for the transfer of from one protocol to another protocol .Without gateway it is not possible to communicate between the wireless client and web server when different language is used [15]. The goal of the WAP Forum is to develop an open, freely licensed specification that is not tied to any network technology, or to any specific device [16]. The WAP standard specifies both a protocol and a format, named Wireless Markup Language (WML) being the WAP analogy to HTML used by HTTP [17]. WAP was designed to work not only with GSM but most other digital wireless telephone networks [18]. Due to the consequent separation of the wireless world from the wired world within WAP, a complete protocol conversion is performed in the WAP gateway. As a consequence, a decryption and reencryption between WTLS and SSL/TLS and vice-versa takes place, and data is available in clear text [19].

3. REENCRYPTION PROBLEM

The Re-encryption problem occurs in between the gateway because of two encryption techniques are required in between the wireless client and wired server. A WAP client use mobile phone for accessing the information on Internet. At one end wireless client is used and at the other end wired server is used. In between these two communication, the gateway is used which acts as intermediate between the wireless client and www server. The gateway acts as request and response between the wireless client and www server. The first request goes to gateway through WAP client using WML (wireless markup language).The gateway pass all the WAP traffic to www server which use HTML (Hypertext Markup Language).The security protocols are used by WAP and WWW server are WTLS and TLS. The first security protocol is used named as WTLS for wireless client who use mobile phone for accessing the data on the Internet. The second protocol is used named as TLS for www server. One encryption algorithm works for WAP in gateway which encrypts all the wireless traffic and send it back to WAP client for Decryption. Again for the next time encryption is done by wired server. When two encryption are used then there is reason for end to end security problem. These two time encryption problem cause a reason for hacking the data because data is in air when next encryption take place after decryption .The end to end security problem also occurs because there is no end to end security directly from WAP client to www server.

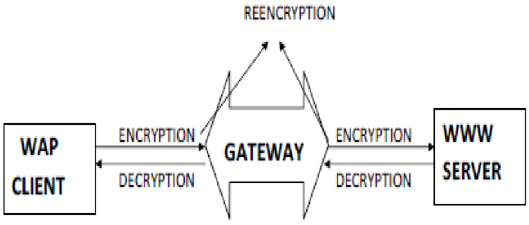

Fig 1: Gateway Re-encryption

The above diagram has shown the concept of Re-encryption. This problem occurs in between the gateway when two security protocols are used.

4. SOLUTION OF RE-ENCRYPTION

The problem of re-encryption is solved by changing the route of gateway encryption directly from WAP client to www server. The flowchart of solution of re-encryption is as follows.

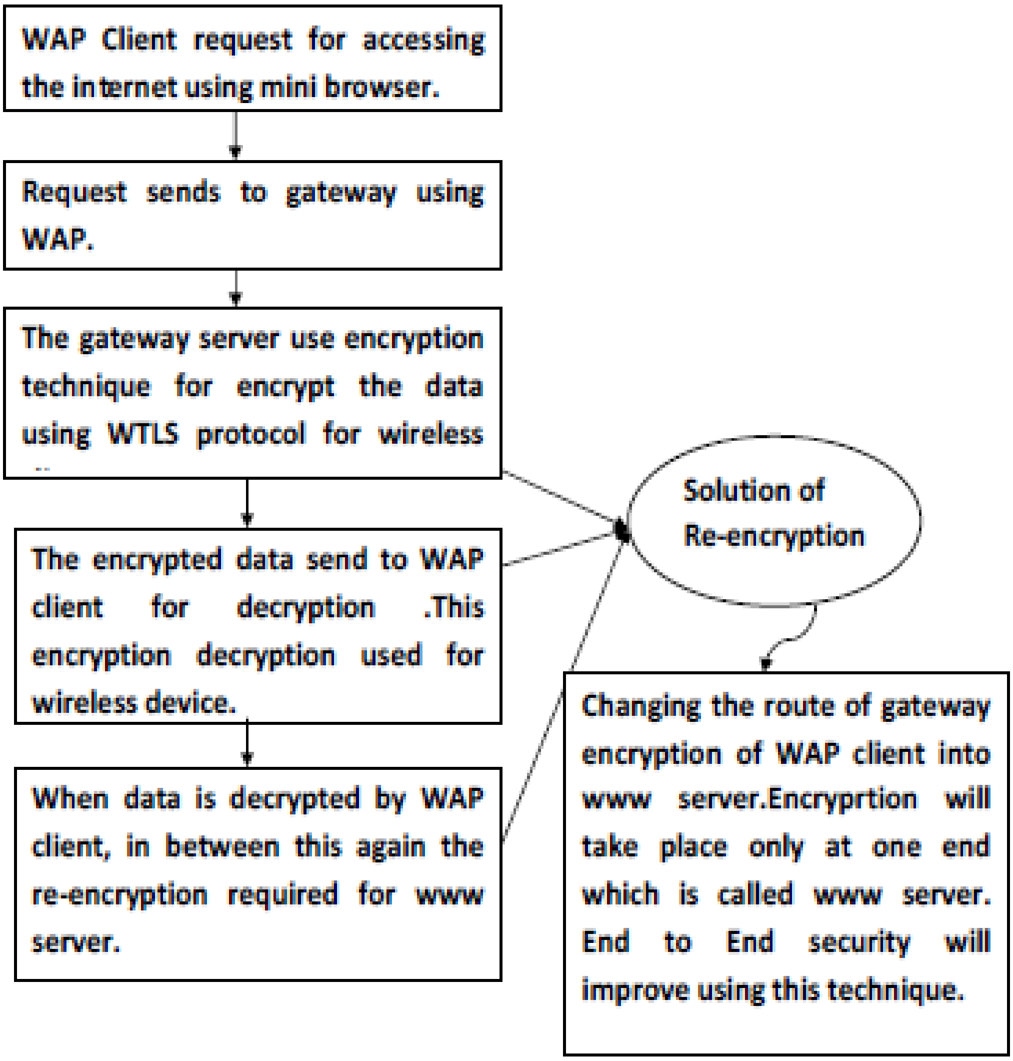
WAP Client request for accessing the internet using mini browser.
Request sends to gateway using WAP.
The gateway server use encryption technique for encrypt the data using WTLS protocol for wireless
The encrypted data send to WAP client for decryption .This encryption decryption used for wireless device.
When data is decrypted by WAP client, in between this again the re-encryption required for www server.
Solution of Re-encryption
Changing the route of gateway encryption of WAP client into www server.Encryprtion will take place only at one end which is called www server. End to End security will improve using this technique.

Fig 2: Flowchart of Re-encryption solution

The gateway is used in between wireless client and www server to provide a communication from client to server. The gateway communication is like two way pathway in which one pathway is used for sending the request and other pathway is used for requesting the request. Two protocols are used for request and response from WAP client to www server. If two protocols are used for security purpose, the problem of end to end security and re-encryption problem occurs.

Instead of using two protocols only one would be used which works for both wireless and wired device. In the review of literature most of the authors have discussed about the WAP gap which means data can be hacked by unauthorized user when data is in the air. My contribution here is to provide the solution for re-encryption and also for the solution for providing end to end security. All the WAP devices communicate with www server not directly but through a common intermediate which is called gateway.

5. USE OF PAGING IN THE GATEWAY

Paging is used for fast retrieval and for storing the data. When any of WAP clients want to access the pages from the Internet then the entire request pass from gateway to server. If the requested page available in server then the browser will open that particular requested page otherwise it gives an error of page not found on mini browser of mobile phones .paging is done by searching a particular page in page look up table. The structure of paging is as follows.

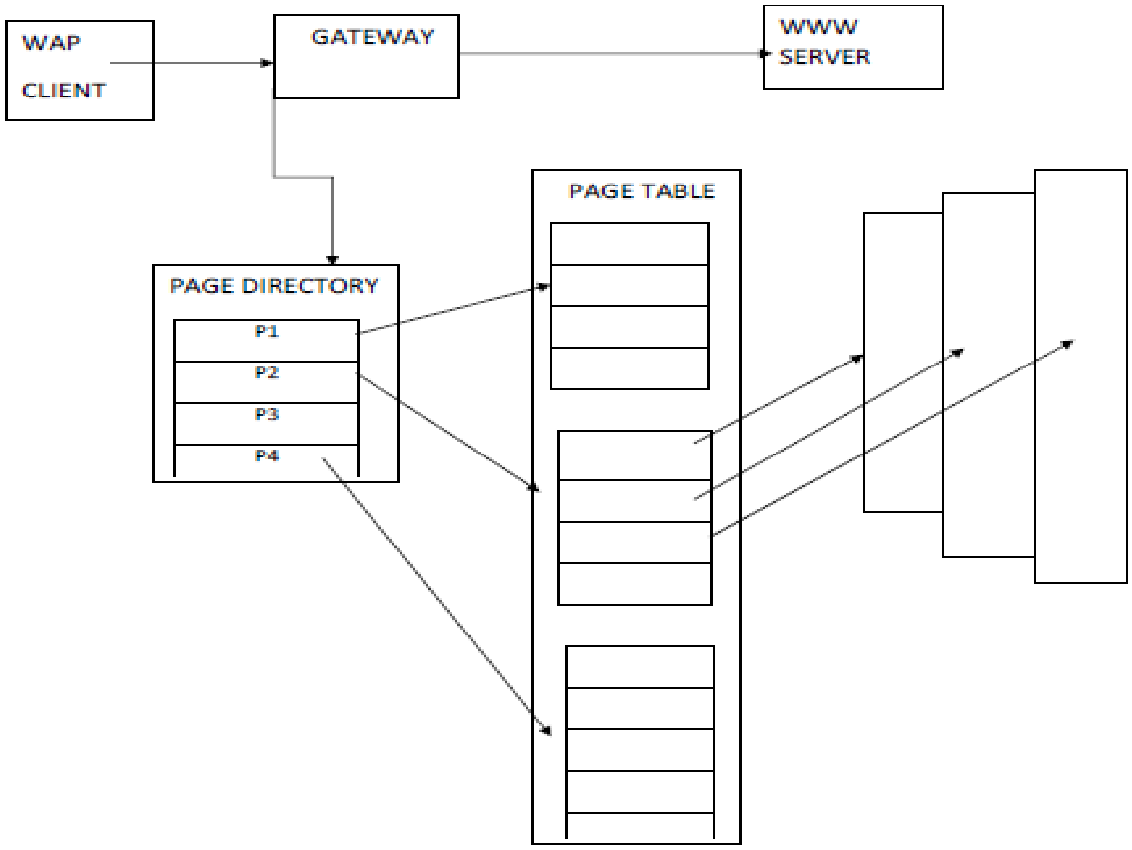

Fig 3: Implementation of Paging

In the above diagram the paging represent how the pages are store on server. The WAP client receives all the data from gateway .Now the gateway act as server for WAP client. In actual the data arrives from www server. But for the wireless devices it seems to like that the data is arriving from gateway. Two way handshaking is used for accessing the data from server. It seems that the data is arriving from gateway. Two way handshaking is used for accessing the data from server. When client use Internet on their mobile phone for accessing any website, the direct path should be from mobile client to main server. When there is no point to point accessibility then the problem of end to end security and man in middle attacks can occur. My contribution here is to change the root of encryption technique from gateway to direct server. Now the encryption algorithm takes place in main server. Instead of using two security protocol one for wired and another for wireless a common security protocol is used for solving the problem of re-encryption. Now WAP client is acting as actual client and www server is acting as actual server

Both client and server authenticate each other by sending certificate for originality. The authentication can be one way where only client send the request to server without knowing which server is actually replying. Second way of authentication is two way authentications where client and server agreed upon by sending a certificate of originality.

6. CONCLUSION

The paper has discussed about the use of paging as database for storing the WAP data. This paper focused on Re-encryption problem which occurs in the WAP gateway. The review of the literature for both security protocols like wireless and wired device have already discussed in this paper. In future new solution can be provided for the fast retrieval of data from the web server. The entire problem related to gateway security can be improved in future. This paper focuses on resolution of Re-encryption by providing the paging in between the gateway. Two encryption and decryption cause a problem of security in between the gateway. Instead of using two encryption and decryption it would be possible to use one common encryption and decryption in the both end of network.

7. REFERENCES

[1] Available in the link "http://www.lovelysms.com/mobile-phone-wap-technology.htm"

[2] Philip J Mikal,"An introduction to WAP security at the network protocol layer-WTLS" ,Nov 1,2001

[3] Eun-Kyeong Kwon, Yong-Gu Cho, Ki-Joon Chae,"Integrated Transport Layer Security :End to End security model between WTLS and TLS", Kaywon School of Art and Design, Youngdong University, Ewha Womans University

[4] Thanh V.Do," WAP Security:WTLS" .INFT 931,May 4,2001 Professor Kris Gaj,Secure Telecommunication System.

[5] Albert Levi, Erkay Savas," Performance Evaluation of Public-Key Cryptosystem Operations in WTLS Protocol" Sabanci University,Istanbul, Turkey.

[6] Eduardo B. Fernandez, Imad Jawhar, Maria M. Larrondo-Petrie, and Michael VanHilst," An overview of the security of wireless networks" Dept. of Computer Science and Engineering,Florida Atlantic University

[7] Thanh V. Do," Project Specification for Analyzing of theWireless Transport Layer Security(WTLS) Applications". March 15, 2001, INFT 931

[8] PHILIP J MIKAL"An Introduction to WAP Security at the Network Protocol Layer — WTLS"2001.

[9] Markku-Juhani Saarinen "ATTACKS AGAINST THEWAP WTLS PROTOCOL" University of finland

[10] Eduardo B. Fernandez" Two patterns for web services security" Florida Atlantic University,Boca Raton, FL 33431, USA

[11] Vipul Gupta, Douglas Stebila_, Stephen Fung," Speeding up Secure Web Transactions using Elliptic Curve Cryptography" 2600 Casey Avenue Mountain View, CA 94043.

[12] Enhancing Security and Trust on WAP in Mobile Commerce Part 2, Singapore, Fri November 10 2000.

[13] Available at this website "http://cryptodox.com/WTLS"

[14] Arjen K. Lenstra1, Eric R. Verheul2." Selecting Cryptographic Key Sizes" GRMS Crypto Group, Goudsbloemstraat 14, 5644 KE Eindhoven, The Netherlands.

[15] Thomas Pettersson "WAP Gateway", 2000-03-03.

[16] Lars Wirzenius "Kannel Architecture and Design", Gateway architect Wapit Ltd.

[17] Anders Hessel and Paul Pettersson," Model-Based Testing of a WAP Gateway: an Industrial Case-Study" Department of Information Technology, Uppsala University, P.O. Box 337.

[18] Niels Christian Juul," Niels Christian Juul" Roskilde University, Department of Computer Science, Bled, Slovenia, June 17 - 19, 2002.

[19] Michael Schmidt," Consistent M-Commerce Security on Top of GSM-based Data Protocols –A Security Analysis" University of Siegen, Institute for Data Communications Systems,57068 Siegen, Germany.