ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 8(30), DOI:10.17485/ijst/2015/v8i30/72068, November 2015* ISSN (Online) : 0974-5645

A Survey on Recently Proposed Key Exchange Protocols for Mobile Environment

Pranav Vyas[1*], Bhushan Trivedi[2] and Atul Patel[1]

[1]Smt. Chandaben Mohanbhai Patel Institute of Computer Applications, Charotar University of Science and Technology, Anand - 388421, Gujarat, India; pranavvyas.mca@charusat.ac.in; atulpatel.mca@charusat.ac.in
[2]GLS Institute of Computer Technology, GLS University, Ahmedabad - 388421, Gujarat, India; bhtrivedi@yahoo.com

Abstract

Background/Objectives: Cryptographic protocols are used for securing information when transmitting it over insecure network such as Internet. This paper's objective is to study recently proposed key exchange protocols for mobile environment. **Methods/Statistical Analysis:** In this paper we do a literature survey of recently proposed key exchange protocols for mobile environment. We analyze execution of protocol in three phases i.e. initialization, communication, renewal/termination phase. In initialization protocol prepares for key exchange process. Next, protocol actually communicates with others to exchange secret key. Third protocol may terminate or renew connection for further communication. We also study activities done by protocols that define characteristics of protocol. **Findings:** In this paper we find that there are many parameters to consider when designing a key exchange protocols for mobile environment. However, significance of parameters is different, based on the security requirement of application for which protocol is being developed. Strength of a protocol is in the encryption technique that it uses. Hence, stronger encryption techniques results in better security of protocol. Speed of protocol is another important parameter. Length of steps in algorithm of protocol is directly proportional to its speed. A protocol must be able to withstand various attacks on it. A protocol should have high reliability if it is to be used in handling critical data. We found that modern key exchange protocols are not properly analyzed and tested before being proposed. Instead of working on already proposed protocols and solve their vulnerabilities and strengthening them researchers are proposing new protocols without testing them properly for vulnerabilities which are later exploited by malicious users. **Applications/Improvements:** This research paper will help researchers and protocol designers. It will give them idea about design parameters when designing key exchange protocol. It will enable them to take better decisions.

Keywords: Data Security, Key Agreement, Key Exchange, Key Management, Mobile Communication, Wireless Communication

1. Introduction

Key exchange protocols have been highly researched area in recent time with various techniques proposed by researchers[1-4]. Technology has come a long way starting with development of key exchange protocols for traditional computers with protocols such as Diffie-Hellman[5] to protocols working on wireless and hand held devices and wireless sensor network6 to vehicular networks[7].

However with freedom of wireless devices there are some constraints. Wireless devices have limited range of communication, limited battery power, processing power and memory capacity.

The limitations mentioned above required to have customized protocols which are designed considering these limitations. In last few years, large numbers of customized protocols for wireless devices considering its limitations have been proposed8-11. Some of the notable key exchange protocols proposed for wireless network

* *Author for correspondence*

recently are Yi-June's[12], Liaw's[13] and Saeed's[14] protocols.

In their paper, Yi-June[12] addresses weakness of existing protocols. They propose an improved version of MAKEP protocols. They call this version EC-MAKEP. Authors claim that their modified version supports user anonymity and forward security among other characteristics that are not supported by traditional key exchange protocols. They also claim that their protocol is more efficient in terms of computation and communication costs. According to authors protocol also supports authentication to server and dual authentication to client.

Second protocol we review is by Liaw et al[13]. In their paper, authors discuss wireless mobile ad-hoc network. In their paper authors propose identity based key exchange protocol that works in environment where public key infrastructure is not present. They propose protocol that is without certification authority for mobile ad-hoc networks. By this protocols authors claims to have solved problem of having certification authority in mobile ad-hoc network.

Third protocol we review is by Saeed et al[14]. Their protocol is designed with smart card in mind. However the technique they use can be applied to traditional wireless network key exchange protocols as well. In this paper authors propose two protocols which are based on cards and are efficient and smart as claimed by authors. Authors combine their protocol with CAPTCHA. Authors claim that their protocols are efficient in terms of communication costs and computational complexities as compared to Fen et al's protocol[15].

2. Analysis Methodology

In this paper we have compared various phases they pass through during their execution life cycle. We evaluated protocols initialization process and tried to find out differences among them. Second phase of a protocol is central to its functionality that describes communication. This phase is for reviewing techniques to provide mutual authentication and user anonymity of these protocols. Nodes also exchange their session keys during communication phase. During third phase nodes can either end current session or update session to continue communication or some protocol have ability to update set of session keys generated in order to service newly joined nodes.

In this paper we review recently proposed session key exchange algorithms. We describe their working. We divide these algorithms in various phases they pass through during execution. We compare their working in these phases and derive conclusion.

This paper is divided into 4 sections. We begin with introduction to topic, and discuss some of the recently

3. Analyzing Protocol

Execution of key exchange protocols can be divided into 3 phases. First phase is initialization phase. In this phase nodes prepare for beginning of communication session. This phase starts before secure communication is about to take place. It prepares nodes for process of key exchange in next phase. Second phase of execution can be categorized as communication phase or key exchange phase. This phase may also include techniques to achieve mutual authentication, user anonymity and forward security. Third phase of execution consists of termination or renewal of session. Some protocols in this phase terminate their sessions where as there are other protocols that renew existing sessions.

3.1 Initialization Phase

Function of initialization phase is to prepare client and server side of the protocol for further communication with each other. In this phase both sides initialize variables that are required for secure communication. These variables may get exchanged during communication and key exchange phase that is then used to calculate and exchange session key.

Yi-June's protocol works with prime numbers. It also selects two large prime numbers that are used for further communication. It also selects a number as starting point. Server also announces public key and private key during this phase.

At the same time, client calculates two variables by using 3 random prime numbers. These two variables are sent to server once they are calculated.

Both sides of this protocol are highly dependent on selection of prime numbers. For this protocol to function in efficiently, selection of prime number is very important. If prime numbers selected are small then it is easy to guess and thus break. It makes whole protocol

vulnerable. However, calculation of large prime number is time consuming and not feasible to calculate in wireless environment.

Liew's protocol[13] also begins with selection of three large prime numbers randomly. Public and private key of both server and client are calculated based on these prime numbers. The server also makes seed and hash function public making them publically accessible for its clients.

Registration of client node to server is also performed in this phase. For this purpose each client sends its identification to server. Once identification is received an acknowledgement message is sent from server to each client. After all the clients in network have identified themselves, the server can exit from network and clients can communicate themselves.

However problem with this technique is the case where node encounters fatal error during communication and requires restarting. In this case the acknowledgement received by node is lost due to restart and in absence of it node cannot communicate securely with other nodes. It cannot get acknowledgement information again as server has already exited the network.

Saeed's protocol uses random numbers and time stamp to maintain freshness of message. In this protocol initialization process is performed on client side. In this protocol client calculates 3 values based on two random numbers.

It sends these values to server with its ID and current time as timestamp. This message also serves as registration message that registers node to server that helps server identify individual node in network.

However problem with this scheme is in freshness of message. This technique uses timestamps for maintaining freshness of message but for timestamps to be effective both the nodes need to have synchronized. In this protocol authors do not specify any synchronization step. In this case if times on both node and server are different, then freshness of message cannot be maintained. This vulnerability can be exploited by a malicious user.

3.2 Communication Phase

This phase consists of communication between clients and server after initialization phase. In this phase session key is calculated either by client or server and is sent to other party. In this phase protocols could also perform processes required for mutual authentication, user anonymity.

In Yi-June's protocol after initialization phase where client announces public key and generates private key. The protocol then generates a message from a random number and its identity information to server. This process is considered as initiation of new communication session. On receiving message from client, server selects one random number and using one random number from client and one of its own, it calculates session key. It then sends the second random number to client.

Upon receiving message from server, client can calculate session key with help from random number received from server. It can also authenticate server by checking contents of its own message and comparing it with message from server. If that matches then it means that message is indeed from sever and that authenticates server.

Lastly client sends an acknowledgement message to server that contains a value that server can use to authenticate client. Server fetches this value and compares calculated value to value received from message, it that matches it means that client is also authenticated. Thus mutual authentication is performed in Yi-June's protocol.

In Liaw's protocol user verification is necessary before key can be exchanged. In this protocol to verify two parties, both users select a random number and compute two public keys. They pass this information to each other encrypted their public keys. Both parties compute variable based on message they have received from other party and compare with the value they have sent. If the calculated value matches their value then mutual authentication is complete and now the key can be exchanged.

After both sides are mutually authenticated, key is generated on both sides. Seed for key generation is the value that they have calculated based on messages they have sent to each other. Since mutual authentication process is successful, the value calculated by them is same. So the key generated by both of them will be same too. Thus it will eliminate need for key exchange.

In Saeed's protocol user has to verify himself and answer a puzzle or a question presented to him/her for generation of session key. However session key is not sent to client node unless that node is mutually authenticated.

Once the client has sent it's identification to server, it generates 3 messages and calculates session key sk2. It sends its identifier and all 3 messages to client. Now to authenticate that client is human, he/she is presented with a puzzle or question. If user answers it correctly, then client calculates session key. However this session

key is not valid for communication session until server is verified. It verifies server by matching contents of message from server with key it has calculated. If it matches then a new messages is sent to server form client with acknowledgement and its identity information. Sever also authenticates client by checking value of its message and comparing that value with value it has calculated. If both values are matched, then client is verified by server. After this process the calculated session key is considered valid for that communication session and can be used to securely communicate over the network.

3.3 Session Renewal/Termination Phase

Session renewal or resumption of paused session is a feature that is not found in most of session key exchange protocols. Very few protocols such as Jing's protocol[16] have these features. This feature is useful especially when the signal is poor. In case if the communication is disrupted by poor signal then instead of letting existing session expire, it is possible to freeze current session and resume it when signal is available again.

However this feature carries very high security risk with it, in case during the freeze time if the client is compromised or a malicious user is able to guess the secret key, then whole communication when it resumes would be vulnerable. Also there are very few sophisticated and safe techniques developed for session renewal[17-19].

It is for this reason that none of the protocols that we have discussed supports techniques for session renewal or resumption.

In session termination phase, once the data is exchanged between two computers, after the acknowledge for last message is received the sender sends a message saying that there is no more data to transfer and ends communication session.

Table 1. Comparison of protocols based in criteria

Protocol Name	Initialization Phase	Communication Phase		Session Termination/Renewal/Resumption Phase		
		Key Exchange	Mutual Authentication	Termination	Renewal	Resumption
Yi-June	Using prime numbers	Based on mutual authentication	Message based	Through Mutual Agreement	No	No
Liaw	Using prime numbers and acknowledgement from server.	Based on mutual authentication	Message based	Through Mutual Agreement	No	No
Saeed	Using random numbers and time stamps.	Based on authentication of human user and mutual authentication	Message based	Through Mutual Agreement	No	No

4. Conclusion

From our review we conclude that while designing a protocol for mobile devices, protocol designers should aim for a protocol with right amount of security, speed and reliability. Here, security of protocol depends on encryption techniques that are used. Stronger the encryption technique better the security of protocol. Speed of protocol is directly proportional to number of steps protocol has or number of operation it has to perform. Reliability of a protocol is its ability to withstand various attempts to exploit weakness of protocol.

Also conclude that key exchange protocols should be properly analyzed for existing vulnerabilities before being released. We also suggest that authors should focus on developing solution to vulnerabilities by modifying existing protocols rather than coming up with new protocols that could introduce new vulnerabilities.

5. References

1. Tan Z. An enhanced three-party authentication key exchange protocol for mobile commerce environments. Journal of communications. 2010; 5(5):436–43.
2. Wu T-Y. An efficient user authentication and key exchange protocol for mobile client–server environment.Computer Networks. 2010; 54 (9):1520–30.
3. Chang T-Y, Hwang M-S, Yang W-P. A communication-efficient three-party password authenticated key exchange protocol.Information Sciences. 2011; 181(1): 217–26.
4. Jianjie Zhao DG, Gu D. Provably secure three-party password-based authenticated key exchange protocol. Information Sciences. 2012; 184(1):310–23.

5. Hellman ME, Diffie W. New Directioins in Cryptography. IEEE Transactions on Information Theory. 1976; 22(6):644–54.
6. Lin Q, Wang Y. Novel Three-Party Password-Based Authenticated Key Exchange Protocol for Wireless Sensor Networks. Advances in Wireless Sensor Networks. 2013; 334:263–70.
7. Eric G, Chachati M.Analyzing Routing Protocol Performance with Nctuns for Vehicular Networks. Indian Journal of Science and Technology. 2014 Sep; 7(9):3191–1402.
8. Pervaiz MO, Cardei M, Wu J. Routing security in ad hoc wireless networks. Network Security. Springer , US. 2010. p. 117–42.
9. Ballardin F.A calculus for the analysis of wireless network security protocols. Formal Aspects of Security and Trust. Springer: Berlin Heidelberg. 2011.p. 206–22.
10. Carmen R. Wireless Network Security. Ovidius University. Annals Economic Science Series; 2012.
11. Chen L. Applications, Technologies, and Standards in Secure Wireless Networks and Communications. Wireless Network Security. Springer: Berlin Heidelberg; 2013. p. 1–8.
12. He Y-H, Lee M-C. Towards a secure mutual authentication and key exchange protocol for mobile communications. In: 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops. Berlin. 2008. p. 225–31.
13. Liaw S-H, Su P-C, Chang H-C, Lu E-H, Pon S-F. Secured key exchange protocol in wireless mobile ad hoc networks. In: 39th Annual 2005 International Carnahan Conference on Security Technology. 2005. p. 171–3.
14. Saeed M, Shahriar Shahhoseini H. Security analysis and improvement of Smart Card-Based Authenticated Key Exchange protocol with CAPTCHAs for wireless mobile network. IEEE Symposium on Computers and Communications (ISCC), Kerkyra. 2011. p. 652–7.
15. Fan YJ, Wen Q, Zhang H. Smart card-based authenticated key exchange protocol with CAPTCHA for wireless mobile network. 2nd International Conference on Future Computer and Communication (ICFCC) 2010. p. 119–23.
16. Xu J, Zhu W-T, Feng D-G. An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks. Computer Communications. 2011; 34 (3):319–25.
17. Ali ST, Sivaraman V, Ostry D.Eliminating Reconciliation Cost in Secret Key Generation for Body-Worn Health Monitoring Devices. IEEE Transactions on Mobile Computing. 2013; 13(12):2763–76.
18. He X, Niedermeier M, de Meer H. Dynamic key management in wireless sensor networks: A survey. Journal of Network and Computer Applications. 2013; 36(2):611–22.
19. Mosca M, Stebila D, Ustagolu B. Quantum key distribution in the classical authenticated key exchange framework. Post-Quantum Cryptography. 2013; 7932:136–54.