A REVIEW OF RECENT MOBILE BASED KEY EXCHANGE PROTOCOLS

[1]Pranav Vyas, [2]Dr. Bhushan Trivedi, [3]Dr. Atul Patel

Charotar University of Science & Technology, GLS Institute of Computer Technology,
Charotar University of Science & Technology
Email:[1]Pranavvyas.mca@charusat.ac.in, [2]bhtrivedi@yahoo.com,
[3]atulpatel.mca@charusat.ac.in

Abstract— In this paper we analyze 3 key exchange protocols proposed in recent years. We focus on protocols developed particularly for mobile environment. We begin with a brief study of past work done on key exchange protocols for mobile environment. We then divide protocol execution in different phases. We divide each phase in several activities. These activities are not mandatory to follow for all the protocols examined here. The protocols analyzed here can perform activities out of order as well. We also specify the protocol's function under each phase of execution. Protocols are examined based on the activities that they perform under each phase during execution. We also point out a number of weaknesses of protocols under different activities in different stages of execution. We also point out how these weaknesses can be exploited in a mobile environment.

Index Terms— Data security, Key exchange, Key management, Mobile communication, Wireless communication

I. INTRODUCTION

A critical issue in today's mobile devices is the security of user's information. The requirement of security is common among all the digital devices and also common in all types of digital communication; mobile devices have special characteristics such as limited memory, processing power and limited battery life that require special attention. Once the communication channel is established by following various security protocols, the problem is reduced to executing cryptographic algorithm to encrypt or decrypt messages. However the most important factor is designing a protocol for key exchange as part of activity of setting up communication channels. If a security related critical error is made in this part, it could affect current communication session and following sessions as well.

Proposing a design of secure key exchange protocol for all platforms is hard to achieve. The proof of that is clearly apparent from different key exchange protocols proposed over the years on a variety of platforms. It is also not surprising that many of these protocols remain vulnerable for many years after publication. Due to a wide variety of protocols and keenness required for analysis of such protocols. It is hard for designers of mobile de-vices to compare and select protocol best suited for their needs [1] [2]. In this paper we present a survey popular key exchange protocols developed for mobile devices to perform key exchange process.

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 the differences among them. The 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 the current session or update session to continue communication or some protocol have the ability to update the set of session keys generated in order to service newly joined nodes.

By doing this comparative study we want to find out different techniques used by different protocols for providing security, for mutual authentication and user anonymity. We will examine protocols and compare them to allow designers of applications for mobile computers and other wireless devices to choose the protocol as per their requirement.

This paper is divided into 4 sections. In this section we have introduced the topic at hand. In the next section we discuss related work. In section 3, we describe our comparison of protocols for different phases and techniques they use to provide various features. In section 4, we present our conclusion based on comparison.

II. RELATED WORK

A lot of research has been going on in key exchange protocols, recently a lot many protocols have been proposed. [3] [4] [5] [6] Key exchange protocols have been developed for traditional computers from a Diffie-Hellman [7] to protocols for wireless sensor networks described by Lin and Wang [8].

However, wireless devices come with several limitations unlike traditional wired devices. Some of deficiencies include limited range, battery power, processing power and limited memory capacity.

Such limitations drive wireless devices to have customized protocols that are designed to compensate for limitations mentioned above. There is a sudden surge of such protocol designed to overcome limitations of wireless network security. [9] [10] [11] [12] Some of the key ex-change protocols that are proposed for mobile devices are Yoon's [13], Jing's [14] and J. Nam's [15]. These protocols have been selected for study because of the variety of solutions they offer in solving key exchange problem. Each of the selected protocol offers different solution to the problem of key exchange and also offers other services such as mutual authentication and support for user anonymity.

In his paper Yoon et al [13] proposes a new protocol considering mobile devices that have low power computing capacity. The authors suggested an environment where there exists a powerful server with enough computing power and a number of clients with low computing capability where the server can provide several different services. These clients can access server through the internet, cellular network or wireless network.

Yoon et al. proposed an ID based public key system with bilinear pairing defined on elliptic curves for management of certificates. In this paper authors have analyzed the efficiency of the protocol proposed by Wu et al. [16]. The authors then proposed a more efficient protocol improving protocol that they have studied.

The proposed protocol is a two phased protocol with the first phase consisting of key extraction and the second phase of user authentication and key exchange phase.

Second protocol by Jing et al. [14] propose aims to solve problem of user anonymity in mobile networks. The authors propose that their protocol addresses problems present in Lee & Hwang's protocol [17] and Zhu and Ma's protocol [18] before them. Authors points out that there are problems such as flow in implementing anonymity, unfairness in deciding key and user unfriendliness. The authors also point out that there are inefficiencies involved in above mentioned protocol by Lee and Hwang. This protocol is divided into three phases.

A third protocol in the list is by J. Nam et al. [19]. This presents a group key agreement protocol that according to the authors is secure against powerful active adversary who controls all communication flows in a network and executes unlimited number of concurrent instances of that protocol. The authors provide proof of security under Decisional Diffie-Hellman assumption in Bresson [20]. The authors also claim that their protocol provides forward secrecy, so disclosure of long term secret key does not compromise the security of previously established session keys.

III. ANALYZING PROTOCOLS

The work of key exchange protocols can be broadly divided into three phases. The first phase is called an initialization phase. Initialization phase deals with beginning of the communication and preparing nodes for key

exchange for the next phase. The second phase is called communication phase here, nodes receive session key from the server using a variety of techniques proposed by various protocols. In this phase, a protocol executes mutual authentication and handle user anonymity characteristics. The third phase of protocol execution consists of techniques of renewal or termination of existing communication session. Some group communication protocols provide techniques for updating session to include newly added nodes in the group in this phase

A. Initialization Phase

The initialization process of each protocol we discussed in paper starts with a type of registration of a mobile node with the server. This communication is initiated by mobile device and involves, mobile device providing identity information to server that will help it to identify a mobile device uniquely.

In Yoon's protocol its node sends identity information IDC to the server. The server then generates a unique ID to identify the particular mobile node. It is done by calculating QIDC.

Also on this protocol, the identities of all nodes are kept with the server. This takes place in this phase of the protocol. Later, every time a communication needs to be done, server is referred. Due to this technique user anonymity is also achieved. Also at the end, server matches QIDC with a value V sent by the client. Using this technique mutual authentication is also achieved.

On Jing's protocol value of the key depends on password that the user selects. In this protocol user has to submit a password with identity information. This information is passed to the server. This information is used with a secret key to computers new identity for a particular node. This identity is then encrypted by the use of a hash function . Once encrypted, delivery of this key is secure.

J. Nam's protocol has two variants one with two round initialization and with three round initialization. In both the protocol variants initialization process is different, rest of steps remain same.

In two rounds protocol, process begins with the device choosing a random number from a given set of numbers. This set us usually very large so numbers are not repeated for a long time. At the same time a random number is selected from the same set by the server as well. Both device and server then apply a common hash function and generates a secret key.

In three round protocol variant the device is initialized with the long term key, also long term key is signed with public and private key of the server. Signing is done by executing a key generation algorithm. Each user also selects an instance identifier that is valid to identify the user for the particular instance. This instance is broadcasted by user so in a group of n users, each user has set of n-1 instances each belonging to a member of the group. Later, these instances are used to identify members uniquely.

B. Communication Phase

This phase is related to communication between server and mobile nodes. This phase starts once initialization phase for all mobile nodes is over. Mainly this phase is used for mutually authenticating each other and exchanging keys for main communication.

Once all nodes are initialized, in Yoon's protocol nodes send their identity information to sever. Here sever can verify nodes and authenticate them. However for nodes be able to authenticate the server and other nodes, a secret key is given to each node by the server. This key is preserved by the particular node and the server. Whenever a node needs to authenticate the server, it can send messages and encrypt message using this secret key. Sever and decrypt and reply to it and authenticating itself to the mobile node. In order to authenticate other mobile nodes, after receiving the message, they forward it to server encrypting already encrypted message again by its own secret key. The server decrypts this message and responds to request of authentication. Based on the response the mobile node authenticates or rejects authentication request form other mobile node.

For Yoon's protocol key exchange also takes place in this phase. The node generates a key and is sent to another node that wants to communicate with nodes. This process takes place once the authentication is successfully done by both the sides. The key is only valid if the mutual authentication process is performed and both nodes have authenticated themselves to each other.

In this phase, Jing's protocol implements a system to mutually authenticate nodes with one another. In this protocol both server and device share common hash function that is used to encrypt or decrypt key generated by server. In this protocol device selects a pass-word that is sent to the server. At the time of sending this password is encrypted with the public key of the server. This password and public key of the server are passed to a hash function and the session key is generated. This session key is then encrypted using a common hash function that is present on both device and server. After encryption of a session key, exchange of it on insecure network is safe.

Using this technique, a node, does not need to forward each and every request to the server. Resources of server are saved. Also because they are using above mentioned techniques to identify other nodes, identities not revealed. So user anonymity achieved.

Jing's protocol also performs mutual authentication in this phase. When a node is in foreign network it can send messages asking for secure key to the home network. This message is first received by foreign agent, but because this message is encrypted with a public key of home agent, it cannot be decrypted by the foreign agent. Home agent then issues a random number to node and a secret key with the same random number to foreign agent. The mobile node sends this random number it received from the home agent to the foreign agent. The foreign agent then compares this number with the one it received from a home agent, if the match is found then mobile node is authenticated. A similar process is done by mobile to authenticate the foreign agent.

J. Nam's protocol in this phase tries to achieve user anonymity and mutual authentication. There are two variants of the protocol, a two round key exchange protocol and a three round key exchange protocol. Both the variants of this protocol follow the same technique to achieve user anonymity and mutual authentication. In this protocol user anonymity is achieved by having a trust based relationship between all the nodes and server. After the registration process is completed, a security certificate is issued by the server to all the nodes. In this technique, no node needs to send identity information to other node. Presenting a certificate from server will serve the purpose. This certificate based technique is used to achieve user authentication.

Now whenever a node wants to initiate communication, they will ask for a security certificate issued by server to validate other nodes. Using this technique they will create a trust based relationship for data exchange. These steps will be repeated by both sides resulting in mutual authentication of each other.

Once the nodes are authenticated and verified key exchange takes place. Key ex-change technique is different for both protocols namely two round key exchange protocol and three round key exchange protocol.

In two rounds key exchange protocol, once the secret number is assigned to a node, that node calculates a secret key by passing this number to a one way hash function H. It then encrypts the result of the hash function with the certificate key of node it wants to communicate and send it to that node. The only recipient node has key to decrypt data.

In three round protocol variant the device is initialized with the long term key, also it is signed with public and private key of the server. Signing is done by executing a key generation algorithm. Each user also selects an instance identifier that is valid to identify the user for the particular instance. This instance is broadcasted by user so in a group of n users, each user has set of n-1 instances each belonging to a member of the group. Later, these instances are used to identify members uniquely.

C. Renewal/Update Phase

There are three possibilities after the first two phases are successfully executed. A node can end communication or renew communication session or update the nodes involved in communication group.

One possibility is that after the message exchange there is no more need for further communication. In this case both nodes agree to terminate the current session and the session ends with mutual agreement.

Another possibility is that there is more data to be exchanged and the session is ending, in this case a new key is generated and distributed. Before this process communication is paused once session is expired. Once, a new key is distributed, communication is resumed using the

new key.

A third possibility is updating information in the group; it is possible that since last session initialization more nodes have been added in the group. In this case, newly added nodes cannot securely communicate due to lack of keys. In this case, the server generates new keys and updates previously generated keys.

There is no room for renewal or update of session to happen in the design of Yoon's protocol. If a session expires with Yoon's protocol, one needs to start from initialization and start communication from all over. Jing's protocol lets user renew session, this is done by using existing session keys and processing them to generate new session keys. The previous key is passed in a one way hash function H () to get a new key. Authors of Jing's protocol also assume that after a communication session, devices may go into hibernation mode. In this case when the device wakes up and there is the need to communicate, the device can take old session key and perform one way hash function, to get a new session key.

In J. Nam's protocol there is no specification that states if protocols have the functionality of renewal, or updating current session.

IV. CONCLUSION

A lot many protocols are proposed in recent years target mobile and wireless environ-ment [3] [4] [5] [6]. They have different goals and use different cryptographic techniques. A large number of protocols are flawed in one way or the other [21]. The new trend that we see is where authors are providing newer solutions to the problem rather than address con-cerns of old solution [21]. This result in a large number of protocols but not many these newly proposed protocols are properly analyzed for vulnerabilities. The aim of these proto-cols should be to provide proper security properties for new generation mobile system and be highly reliable.

As we can see from table, the protocol by Jing [14] is the only protocol that is con-cerned with securing the interface between two hosts. All other protocols are concerned with details of providing security for complete Lifecycle of the message. All protocols have tried to maintain confidentiality of messages, and all the protocols are concerned with user anonymity.

In protocols that support user anonymity, mobile's identity is secured by encrypting it with a secure cryptographic key. This identity may be disclosed to trusted server inside its home network or could be shared by servers on foreign networks when a mobile node mi-grates geographically. We find that it is very difficult to manage user anonymity.

Based on results, we conclude that the

TABLE 1. PROTOCOL COMPARISION

Protocol Name	**Initialization Phase**	**Communication Phase**			**Session Termination/Renewal/Update Phase**		
		Key Exchange	***Mutual Authentication***	***User Anonymity***	***Termination***	***Renewal***	***Update***
Yoon	Unique number based ID	Based on authentication	Nonce based	Identity authentication by server	Through Mutual Agreement	No	No
Jing	Password based ID	Based on Public key and hash function	Nonce based	Identity authentication by server	Through Mutual Agreement	Using old session keys	No
J.Nam	**2 Round:** Unique number from client **3 Round:** Long term initialization and Instance identifier	**2 Round:** Based on unique ID and hash function **3 Round:** Based on Instance identifier and certificate signing	Nonce based	Trust based relationship	Through Mutual Agreement	No	No

initialization phase is of importance to the core function of the protocol. From protocols that we have analyzed we conclude that in all protocol initialization phase provides a platform to prepare clients and server for the key exchange process. In all the protocols we have analyzed, the initialization process provides unique identification to each node. This identification is then used for further communication with nodes. In some protocols, this process is done by a server assigning unique number of node, in other protocols it is done by client by taking a password from the user and applying a hash function to it. Some protocol variants also use long term initialization that is valid identification for multiple sessions for predefined time span.

All the protocols we discussed serve multiple mobile nodes. However, most of these protocols can communicate with the server only once to register themselves. Once they are registered they do not need to communicate with the server again in order to communi-cate with others.

We find that the problem with these protocols is that they eliminates the need to com-municate with server frequently, however downside of this solution is that if one of the cli-ent is compromised after authentication process and its key is revealed, it can be used for malicious purpose. A protocol need to be designed in such a way that this weakness is also addressed, one need to take care so that the frequent communication between server and the mobile node is efficient.

The key exchange process varies widely in the protocols we have analyzed. While one protocol exchanges key only after authentication process is completed another protocol that we discuss relies on long term authentication and certificate signing for key exchange. One way hash functions are used by third protocol to generate public key before to encrypt message carrying key before it is sent across the network.

We found that in the last phase of protocol most protocols do not provide functionality to renew or update session and chooses to end current session and begin a new session if required. Some protocols however provide the service of session renewal and updating.

We also found that some protocols that provides with the session renewal facility uses old session keys and a random number to calculate a new session key with help of hash function. This functionality could be exploited if old session key is leaked. In process of updating nodes, a new id will be generated to assign new node in order to identify it. This new id is usually a random number. If this number is leaked a malicious user could impersonate as a valid user. From our analysis of protocols we conclude that aim of new key exchange protocols is to provide proper security properties of new generation mobile systems with high reliability. Protocol designer should strive to achieve the right balance of speed and reliability. The speed of protocols depends on a number of steps that they have to go through to make communication secure. More steps results in more calculation and thus require more time for execution. Reliability of protocol depends on the security that protocol can provide during the key exchange process.

At the time of designing a key exchange protocol one should not become biased towards either of two characteristics of speed and reliability. If the designer is based towards speed then the resultant protocol is fast but not secure. On the other hand, if a designer is biased on designing reliable protocol then the resultant protocol may be very reliable and secure but very slow in execution. It is also equally important to analyze key exchange protocol for potential vulnerabilities. We also conclude that instead of developing new solution existing problem of key exchange, designers should concentrate on developing solutions to vulnerabilities present in existing protocols.

REFERENCES

[1] Canetti, Ran, and Hugo Krawczyk, "Analysi of key-exchange protocols and their use for building secure channels," Advances in cryptology EUROCRYPT'01, Springer Berlin Heidelberg, 2001. 453-474.

[2] Bellare, Mihir, Ran Canetti, and Hugo Krawczyk, "A modular approach to the design and analysis of authentication and key exchange protocols," In Proceedings of the thirtieth annual ACM symposium on Theory of computing, pp. 419-428. ACM, 1998.

[3] Tan, Zuowen. "An enhanced three-party authentication key exchange protocol for mobile commerce environments." Journal of communications vol.5 2010 pp. 436-443..

[4] Wu, Tsu-Yang, and Yuh-Min Tseng. "An efficient user authentication and key exchange protocol for mobile client–server environment." Computer Networks vol.54 2010 pp. 1520-1530.
[5] Chang, Ting-Yi, Min-Shiang Hwang, and Wei-Pang Yang. "A communication-efficient three-party password authenticated key exchange protocol." Information Sciences vol. 181 2011 pp.217-226.
[6] Zhao, Jianjie, and Dawu Gu. "Provably secure three-party password-based authenticated key exchange protocol." Information Sciences vol.184 2012 pp.310-323.
[7] Diffie, Whitfield, and Martin E. Hellman. "New directions in cryptography." Information Theory, IEEE Transactions on vol.22 1976: pp. 644-654.
[8] Lin, Qiaomin, Yangjunxiong Wang, Xing Shao, Faxin Yang, and Ruchuan Wang. "Novel Three-Party Password-Based Authenticated Key Exchange Protocol for Wireless Sensor Networks." Advances in Wireless Sensor Networks, pp. 263-270. Springer Berlin Heidelberg, 2013.
[9] Pervaiz, Mohammad O., Mihaela Cardei, and Jie Wu. "Routing security in ad hoc wireless networks." Network Security. Springer US, 2010. pp.117-142.
[10]Ballardin, Francesco, and Massimo Merro. "A calculus for the analysis of wireless network security protocols." Formal Aspects of Security and Trust. Springer Berlin Heidelberg, 2011. pp.206-222.
[11]Carmen, Rãduþ. "Wireless Network Security." Ovidius University Annals, Economic Sciences Series vol.12 2012 pp.502-506.
[12]Chen, Lei. "Applications, Technologies, and Standards in Secure Wireless Networks and Communications." Wireless Network Security. Springer Berlin Heidelberg, 2013. pp.1-8.
[13]Yoon, E-J., and K-Y. Yoo. "A new efficient ID-based user authentication and key exchange protocol for mobile client-server environment." IEEE International Conference on Wireless Information Technology and Systems (ICWITS), 2010.
[14]Xu, Jing, Wen-Tao Zhu, and Deng-Guo Feng. "An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks" ,Computer Communications vol. 34, 2011, pp. 319-325.
[15]Nam, Junghyun, et al. "Security enhancement to a password-authenticated group key exchange protocol for mobile ad-hoc networks." IEEE Communications Letters, vol.12 ,2008,pp.127-129.
[16]Wu, Tsu-Yang, and Yuh-Min Tseng. "An efficient user authentication and key exchange protocol for mobile client–server environment." Computer Networks vol.54, 2010, pp.1520-1530.
[17]Lee, Cheng-Chi, Min-Shiang Hwang, and I-En Liao. "Security enhancement on a new authentication scheme with anonymity for wireless environments." IEEE Transactions on Industrial Electronics, vol. 53,2006,pp.1683-1687.
[18]Zhu, Jianming, and Jianfeng Ma. "A new authentication scheme with anonymity for wireless environments." IEEE Transactions on Consumer Electronics, vol.50, 2004, pp.231-235.
[19]Nam, Junghyun, Juryon Paik, Ung Mo Kim, and Dongho Won "Resource-aware protocols for authenticated group key exchange in integrated wired and wireless networks." Information Sciences, vol.177,2007 pp.5441-5467.
[20]Bresson, Emmanuel, Olivier Chevassut, and David Pointcheval. "Provably authenticated group Diffie-Hellman key exchange—the dynamic case." Advances in Cryptology—ASIACRYPT 2001. Springer Berlin Heidelberg, 2001, pp. 290-309.
[21]Boyd, Colin, and Anish Mathuria. "Key establishment protocols for secure mobile communications: a critical survey." Computer Communications, vol.23, 2000, pp.575-587.