Journal of Information Security, 2015, 6, 51-58
Published Online January 2015 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2015.61006

Scientific Research Publishing

Authenticated Key Agreement Protocols: A Comparative Study

Areej Omar Baalghusun[1], Olfa Fahad Abusalem[1], Zahra Abbas Al Abbas[1], Jayaprakash Kar[2]

[1]Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, KSA
[2]Department of Information Systems, Information Security Research Group, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, KSA
Email: jayaprakashkar@yahoo.com

Received 30 November 2014; accepted 15 December 2014; published 13 January 2015

Abstract

One of the most important and challenging cryptographic primitives in Public Key Cryptography is Key Agreement Protocol where two or more parties share secret values and establish the session key. Many authors have proposed key agreement protocols. In this article, we have viewed some authenticated Key Agreement Protocols and presented a comparative study. We have also described the design principle, security requirement and various attacks on Key Agreement Protocol.

Keywords

Impersonation Resilience, Prime Factorization, ECDLP, Trapdoor Function

1. Introduction

Cryptography is the basic technology used to secure information that travel over Internet communication and may expose by attacker (third parties). Key Establishment (KE) is one of the basic concepts in this context and the first step to set up secure, complex and higher level communication [1] which is defined as a method or protocol that make two or more parties sharing a secret value for getting secure information transition [2] [3]. KE is subdivided into two kinds: Key Transport Protocol (KTP) and Key Agreement Protocol (KAP). In KTP one party is created or gets a secret value and transmitted securely to the other party, more details found in [2] [3]. Where in KAP two or more parties create a shared secret value by contributing information and combining them to obtain the result. The KE protocol is traditionally known as the hardest one to design, several challenges are associated with KE listed below as [3] stated:

• Ensuring that the parties (sender and receiver) are exchanging keys to achieve communication encryption/decryption.

• Preventing the disclosure of the key by eavesdropper.

• Giving evidence that a message was encrypted by the party who claims having the sent message for the receiver.

This survey is presented to give a brief review; clear understanding about KAP which has important role in cryptography and it is a part of data security in any system. KAP is one of the hardest protocols to design, the reason for that as long as many attacks are discovered, protocols need to be verified again and there is a need to develop new one that can defend against the new attacks. The method that will be used in surveying is literature study and the most KAP topics that the survey discusses are present in **Figure 1**. The next section will examine what does a KAP mean and give a brief history. Security requirements of KAP are presented in second section. The third section introduces attacks that exposed to the system. The fourth section discusses the knowledge needed to design a new protocol that meets the security requirements respectively.

2. Key Agreement Protocol: An Overview

KAP is one of the basic cryptography concepts, two or more parties be in agreement on a key to be used for confirming the communication privacy and authentication between them [4]. In 1976 W. Diffie and M. Hellman suggested the initial protocol that is taken as building block for most of the new protocols [5]. However, this protocol does not offer verification between the two parties of communication. Therefore, it is disposed to man in middle attack. Many of protocols have been proposed to resolve this trouble [2] by offering authentication. The authentication can be performed by several methods, such as using the public key infrastructure [6].

2.1. Security Requirement of Key Agreement Protocol

Security Requirements are related to confidentially, integrity, authentication and availability. So a KAP must hold the following set of required properties [3] [6] [7].

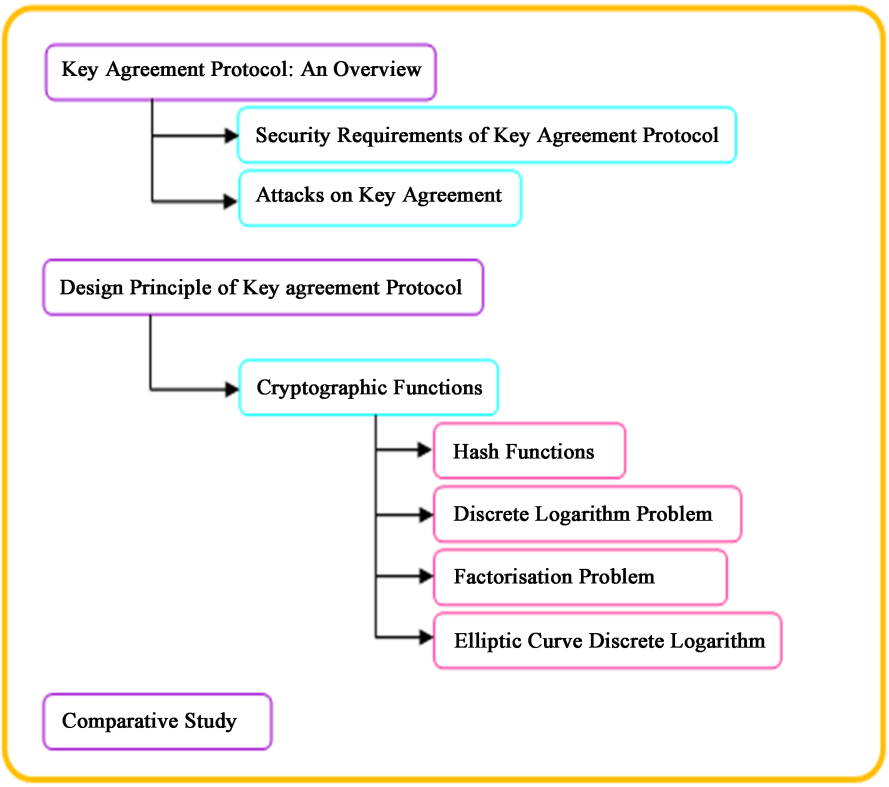

Figure 1. The KAP topics taxonomy.

• **Known key security**: Every protocol must create independent key. It is not being affected if additional secretive sitting keys are revealed.

• **Forward secrecy**: If the long-term private key of one or more of the parties are revealed, the secrecy of earlier created sitting key should not be affected. The system has ideal forward secrecy if every one of the parties long-term key can be damaged without revealing earlier created sitting key, on other hand the system has limited forward secrecy if a few of the parties long-term key can be damaged without revealing earlier created sitting key.

• **Key-compromise impersonation resilience**: The attacker is capable of impersonate *A*, if a long-term private key of a party *A* has been revealed, but this must not allow it to impersonate other parties to *A*.

• Unknown key-share resilience: it should not be potential that *A* is tricked into sharing a key with party *C* if *A* wishes to generate a secret key with *B* [3].

• Key control: *A* and *B* together specified the key. It cannot be forced by either *A* or *B*.

2.2. Attacks on Key Agreement Protocol

KAPs are vulnerable to many attacks. The designers of these protocols must understand the various types of attack to know how to design a protocol that resist them. This section will briefly discuss them. The attacks are divided into two types [3]: active and passive. A passive attack in computing security is when an attacker is eavesdropping to a communication using a network tracking equipment but without attempt to alter or break the communication; this attack is considered the easiest way to attack also to defend. The communication must be encrypted so even though the attacker compromises the exchanged message, it provides no information. The active attack in computing security is when the attacker attempts to alter or modify the data exchanged in the communication, this attack is considered to be complex than passive and require more effort from attacker and the designer sides.

Examples of the most common attacks on the KAP are

• **Eavesdropping**: it is a kind of passive attack [3] [8] that an eavesdropper listening to the information sent in the protocol and the communicating parties are unaware. It is impossible to prevent or stop the eavesdropping, but the message can be protected using encryption. This way the confidentiality is guaranteed. Only the communicating party can clearly read the contents of the message who know the secret key, so the key should be kept secret between communicating parties. Eavesdropping can be used as a part of more complex attack.

• **Modification** [3] [8]: it is a kind of active attacks where the attacker alters or modifies the information which is sent in the protocol. Using cryptographic integrity measures are methods to prevent this attack.

• **Replay**:also known as playback attack which happens when a transmission maliciously or fraudulently repeated or delayed. This can be done either by the sender or by an attacker who catches the data and retransmits, or when the communication is being recorded to be replicated to the same or different parties for criminal intents. This attack can be used as a part of more complex. Using session tokens, one time password or timestamping are ways to prevent this kind of attack [3] [8].

• **Reflection**: By attacking a challenge response authentication system that uses identical protocol in both sides by tricking a target party to offer the answer to his own challenge [8]. By demanding the originating party to first reply to challenge prior to the target party responds to his own challenge to avoid this attack. Another way of protection is to force using a different key or protocol in both sides of a transmission.

• **Denial of Service Attack**: When the attacker is sending a huge number of invalid requests to a network with the aim of overwhelming and exhausting the server's resources and preventing legitimate users from communicating with the server [8]. The attack aims to exhaust the computational resources (CPU and Storage) of the server. There are no means to fully prevent this attack, but the protection can be done by reducing the amount of calculations and number of values the server have to save for each transmission.

• **Certificate Manipulation**: When an attacker modifies the certificates information in order to attack the protocol.

• **Protocol Interaction**: When the attacker selects a new protocol to communicate with a well-known protocol. To defend against this kind of attack is by using different set of keys for each protocol, and including the protocol's information such as: the protocol's identifier and its version in the message authenticated part.

Table 1 summarizes the different common attacks.

Table 1. Common attacks.

Name of Attacks	Description
Heading Eavesdropping	The attacker listens to information sent via the protocol.
Modification	The attacker changes the information sent via the protocol
Replay	The attacker records information sent in the protocol and forwards it to the same or a different party during protocol runs.
Replay	The attacker involves in the run of a protocol earlier to a run by the legitimate parties.
Reflection	The attacker sends protocol messages back to the party who sent them.
Denial of Service	The attacker prevents legitimate parties from finalizing the protocol.
Cryptanalysis	The attacker gets some useful control from the protocol to help in cryptanalysis.
Certificate Manipulation	The attacker picks or alters certificate information to attack one or more protocol runs.
Protocol Interaction	The attacker selects a new protocol to interact with a well-known protocol.

3. Design Principle of Key Agreement Protocol

Any protocol designer must have some mathematics skills that help to invent a good protocol. This section will introduce a brief description about the most important topics that related to protocol design process. Many researches have been done to design new KAPs that satisfy the security requirements, present safe and secured communication. This kind of protocols is hard to develop, because there are many ways to attack the protocol as we stated early in previous section and new attacks are presented [3]. The designer are working hard, making effort and trying to enhance the protocol security but still some of protocols contain problem and defects. The process of designing new protocol is based on try and fail [3], there is no structured way to develop a protocol, because the information is rapidly changing and security requirements are updated contagiously based on it. The process begin by proposing new protocol to achieve an excellent level of security, after that new attack is exposed, or some limitation is found so the protocol fail and are not secure any more, then the process start again. The next subsection presents the core design concepts that all KAPs based on it, which are one-way functions.

3.1. Cryptographic Functions

A one-way function is a computational function that can be easily calculated from a single direction which is the forward direction, but hard to calculate in the inverse direction [3]. A “trapdoor one-way function” [9] is a specific kind of one-way function which is complex to reverse except you have some confidential information named the “trapdoor”. If this extra information is not available, the computation is hard [9]. Cryptosystem with public/private keys is an example of a trapdoor one-way function, where the private key is the trapdoor needed to calculate the function in forward and inverse directions. If the private key is unknown the function can be calculated only in the forward direction. The forward direction is for the encryption and the verification of digital signature, where the inverse direction is for the decryption and generating the digital signature [3]. The next subsection discusses some examples of one way function.

3.2. Discrete Logarithm Problem

Finding an integer n solving the equation $an = z$, where a and z are elements of a Solving the discrete logarithm problems is assumed to be hard. On ordinary computers there is no well-organized method for calculating discrete logarithms. The security of many public-key cryptography algorithms are based on that assumption.

3.3. Integer Factorization Problem

Prime factorization (factorization) in number system means decomposition of an integer into prime numbers which are called factors. When multiplying these factors yields the original integer. Many cryptographic

protocols are based on the complexity of factoring large composite integers such as the RSA problem.

3.4. Discrete Logarithm Problem

This is the logarithms that are defined on multiplicative cyclic groups. Let $\mathbb{G}$ is a multiplicative cycle group and g is a generator of G, then the elements r of the cyclic group are in the form $g^t \bmod n$ for some $t \in \mathbb{Z}_n^*$.

Definition 1. *Discrete logarithm to base* g *of* r *in the group* $\mathbb{G}$ *is defined to be* t.

The discrete logarithm problem is defined as: given a group G, a generator g of the group and an element h of G, to find the discrete logarithm to the base g of h in the group G. Discrete logarithm problem is not always hard. The hardness of finding discrete logarithms depends on the groups.

3.5. Elliptic Curve Discrete Logarithm Problem

In cryptographic context, it is a curve over a finite area, which consists of points satisfying the following equation

$$y^2 = x^3 + ax^2 + b \tag{1}$$

Definition 2 *Given an elliptic curve* E *defined over a finite field* $\mathbb{F}_p$, *a point* $P \in E(\mathbb{F}_p)$ *of order* n, *and a point* $Q \in \langle P \rangle$, *find the integer* $l \in [0, n-1]$ *such that* $Q = lP$. *The integer* l *is called discrete logarithm of* Q *to base* P, *denoted* $l = \log_p Q$ [10].

4. Comparative Study

Authenticated Key Agreement (AKA) Protocol share widely used for any secure communication systems such as electronic commerce, wired lines, wireless and other Internet applications [11]. AKA provide ways to verify the communicating parties authenticity and to establish a common secret session key between the communicating parties for subsequent use. Also, ensure that no attacker can get the information transmitted over the communication channel. An AKA protocol in general is designed using several cryptographic schemes and protocols such as public/private key pairs, Hybrid systems, passwords and other tricks Like shared secret keys.

4.1. W. Hsiang An *et al.*'s Protocol

W. Hsiang An, L. Chun Li and H. Tzonelih [12] propose a protocol that provides secure communications in client—server environment through a low power computing Portable devices such as PDAs,smart cards, and cellular phones and make the client perform as minor computations as possible, and to reach mutual authentication and secure communications The proposed protocol is an Authenticated Key Exchange-for Low Power Computing clients (AKE-LPC) that is based on hybrid-key architecture which means that one party (client) shares a secret with the server whereas the other party (server) stores a pair of matching public/private keys. This protocol involves only one hash operation on the client side during execution stage, considering the cost of LPC client computation. Two protocols are proposed, one is already providing implicit mutual authentication and the other with a minor modification to accomplish explicit mutual authentication which is considered here to be evaluated. The protocol fulfills all requirements of security except the forward secrecy [13].

4.2. C. Popescu's Protocol

Popescu [14] presents secure and efficient AKA that is constructed on DH and works in an elliptic curve group. This protocol is more efficient in the from computational cost perspective, since it involves only one integer multiplication per party. Key compromise impersonation goal doesn't fulfill in the protocol [13] while other security attributes do. The protocol provides efficiency and using simple computations just a hash functions and elliptic curve which does not require many resources.

4.3. L. Harn *et al.*'s Protocol

L. Harn, M. Mehta and W. J. Hsin [11] proposed three AKA protocols based on DH. The proposed protocols

used a single cryptographic assumption. Each protocol is based on one of the cryptographic assumptions which include discrete logarithm, an elliptic curve or an RSA factoring. The first one is an authenticated DH key agreement protocol based on discrete logarithm; it provides both user and shared-key authentication. The second is an authenticated DH key agreement protocol based on the elliptic curve. The third is an authenticated DH key agreement protocol based on RSA factoring. The last one will be evaluated in this comparative study. All the security attributes are achieved with this protocol except the forward secrecy.

4.4. Tseng *et al.*'s Protocol

Two AKAs [15] proposed by Tseng that reduce the impact of denial-of-service attacks. They depend on explicit key confirmation which needs little computational cost. Both proposed protocols are able to concurrently resist both the CPU-exhaustion attack and the storage-exhaustion attack. Storage-exhaustion means that the attacker overwhelms the server's memory with variables connected to the various requests to the server. CPU-exhaustion is when the attacker attempts to consume all server's computational resource. All security attributes of are fulfilled in these protocols. The protocol reduces the impact of denial-of service attacks against the server by minimizing the server's computations and storage needs.

4.5. Y. Eun-Jun *et al.*'s Protocol

An AKA protocol that proposed by Y. Eun-Jun and Y. Kee-Young which is based on ECDLP and usepassword authentication [16]. This protocol is claimed to be simple, efficient and capable to defend against off-line password guessing and modification attacks by isolate the information that may used to confirm the correctness of the guess using an asymmetric structure in the messages exchanged. The computations of the protocol are based on ECC and hash functions, which do not require much computational resources. The benefits from the ECC are in the key block size, speed, and security. This protocol meets all requirements of security if there are no fully private keys in this protocol, only the shared secret password. In this context, the key-compromise impersonation flexibility goal is not fit and decides to leave it out of the evolution. Instead if the password is compromised the parties may not be authenticated. The protocol is efficient, simple and to resist off-line password guessing and modification attacks.

4.6. M. Nabil *et al.*'s Protocol

M. Nabil, Y. Abouelseoud, G. Elkobrosy and A. Abdelrazek [17] have proposed four authenticated KAPs that support explicit authentication. The authentication of the communicating parties is performed in a trusted third party like a firewall. In this way the end user's devices dispose of being overwhelmed with computational burden which is tied up with the authentication. New schemes are proposed where each protocol consists of two phases, the setup phase and key generation phase. The first two protocols are two-party and the other two are three-party scheme. All of them are a certificate based PKI where the communicating parties must be registered. The bilinear maps, the Weil pairing and hard computational problems which are based on the complexity of Bilinear Diffie-Hellman Problem are used to develop these protocols [10] [18]. This paper analyzes the first protocol. The protocol fulfills all the security attributes of KAP. It relieves the communicating parties from the communication burden of the authentication and enhancing the performance.

Table 2 summarizes the security of the above described protocols. We have discussed on the following security attributes:

•: Known Key Secrecy (KkS)
•: Perfect forward secrecy (PfS)
•: Key-compromise impersonation resilience (KiR)
•: Unknown key-share resilience (UkR)
•: Key control (Kc)

Table 3 summarizes the design principle, authentication method, cryptographic function used and the mathematical hard function on which the security of the protocols relies.

5. Conclusion

The need to have a secure system depends on cryptography. KAP is one of the most basic concepts of crypto-

Table 2. Security comparison.

Protocol	KkS	PfS	KiR	UkR	Kc
W. Hsiang An *et al.*'s Protocol	√	√	√	×	×
C. Popescu's Protocol	√	×	√	×	×
L. Harn *et al.*'s Prtocol	√	√	√	×	×
Tseng *et al.*'s Protocol	√	×	√	×	×
Y. Eun-Jun *et al.*'s Protocol	√	√	√	√	√
M. Nabil *et al.*'s Protocol	√	√	√	√	√

Table 3. Summarization of the defined protocols.

Protocol	Security relies on	Method of Authentication	Design Principle
W. Hsiang An *et al.*'s Protocol	Hash Function	Hybrid Key	ECC
C. Popescu's Protocol	ECDLP	Public/Private Key pairs	Diffie-Hellman
L. Harn *et al.*'s Protocol	IFP	Public/Private Key pairs	Diffie-Hellman
Tseng's *et al.*'s Protocol	DLP	Public/Private Key pairs	Diffie-Hellman
Y. Eun-Jun *et al.*'s Protocol	ECDLP	Password Based	ECC
M. Nabil *et al.*'s Protocol	ECDLP	Hybrid Key	ECC

graphy. This paper discusses the KAP, their security requirements and examples of attacks that threat some of them. It presents the concept of one-way function which is considered the core of KAP design. Also, it explains some standardized protocols that are considered as a building block for most of the new protocols. It discusses how the researchers classify KAPs from their perspective and some examples of new protocols are listed. Finally, it presents some AKA protocols and applies simple comparative study on them. The number of new invented protocols is increasing as long as many attacks are appearing, so direction of the future researches about verifying their efficiency.

Acknowledgements

We would like to thank to our supervisor Dr.Jayaprakash Kar for his valuable suggestions and comments that helped improving this works. This support is greatly appreciated.

References

[1] Saha, M. and RoyChowdhury, D. (2009) Provably Secure Key Establishment Protocol Using One-Way Functions. *Journal of Discrete Mathematical Sciences & Cryptography*, **12**, 139-158.

[2] Menezes, A., van Oorschot, P. and Vanstone, S. (2010) Handbook of Applied Cryptography. CRC Press, Boca Raton.

[3] Vesterås, B. (2006) Analysis of Key Agreement Protocols, 1-46.

[4] Dutta, R. and Barua, R. (2005) Overview of Key Agreement Protocols. Cryptology ePrint Archive, 1-46.

[5] Diffie, W. and Hellman, M. (1976) New Directions in Cryptography. *IEEE Transaction on Information Theory*, **22**, 644-654. http://dx.doi.org/10.1109/TIT.1976.1055638

[6] Mohamed, N., Yasmine, A., Galal, E. and Amr, A. (2013) New Authenticated Key Agreement Protocols. *International Multi Conference of Engineering and Computer Scientists*, **1**, 58-63

[7] Elkamchouchi, H.M., Saleh, Y.A. and Sary, A.M. (2011) New Authenticated Key Agreement Protocols. *International Conference on Computer Engineering & Systems* (*ICCES*), Cairo, 29 November 2011-1 December 2011, 58-63.

[8] Boyd, C. and Mathuria, A. (2003) Protocols for Authentication and Key Establishment. Springer, Berlin, Heidelberg.

[9] Lopez, J. and Dahab, R. (2000) An Overview of Elliptic Curve Cryptography. Technical report, Institute of Computing, State University of Campinas, Brazil, 1-35.

[10] Kar, J. (2014) Provably Secure Online/Off-Line Identity-Based Signature Scheme for Wireless Sensor Network. *International Journal of Network Security*, *Taiwan*, **16**, 26-36.

[11] Harn, L., Hsin, W.J. and Mehta, M. (2005) Authenticated Diffie-Hellman Key Agreement Protocol Using a Single Cryptographic Assumption. *IEEE Proceeding of Communication*, **152**, 404-410.

[12] Wen, H.A., Lin, C.L. and Hwang, T. (2006) Provably Secure Authenticated Key Exchange Protocols for Low Power Computing Clients. *Computer & Security*, **25**, 106-113. http://dx.doi.org/10.1016/j.cose.2005.09.010

[13] Kar, J. (2014) A Novel Construction of Certificateless Signcryption Scheme for Smart Card. In: *Case Studies in Secure Computing Achievements and Trends*, CRC Press, Taylor and Francis, New York, Chapter-22, 437-456.

[14] Popescu, C. (2004) A Secure Authenticate Key Agreement Protocol. *IEEE MELECON*, Mediterranean, 12-15 May 2004, 783-786.

[15] Tseng, Y.M. (2005) Efficient Authenticated Key Agreement Protocols Resistant to a Denial-of-Service Attack. *International Journal of Network Management*, **15**, 193-202. http://dx.doi.org/10.1002/nem.561

[16] Yoon, E.J. and Yoo, K.Y. (2005) New Efficient Simple Authenticated Key Agreement Protocol. *Computing and Combinatorics*, **3595**, 945-954. http://dx.doi.org/10.1007/11533719_95

[17] Nabil, M., Abouelseoud, Y., Elkobrosy, G. and Abdelrazek, A. (2013) Certificate-Based Authenticated Key Agreement Protocols. *Proceeding of IEEE ICCAT*, *Computer Applications Technology* (*ICCAT*), 2013 *International Conference on Location City of Sousse*, 20-22 January 2013, 1-7.

[18] Kar, J. (2014) Authenticated Multiple-Key Establishment Protocol for Wireless Sensor Networks. In: *Case Studies in Secure Computing Achievements and Trends*, CRC Press, Taylor and Francis, New York, Chapter-04, 67-88.