COMPARATIVE ANALYSIS OF SOME CRYPTOGRAPHIC SYSTEMS

VELIBOR ŠABAN
School for secondary and vocational education „ Sergije Stanić“ Podgorica, Montenegro, velibor.saban.mbs@gmail.com

IVANA OGNJANOVIĆ
University of Donja Gorica, Montenegro, ivana.ognjanovic@udg.edu.me

RAMO ŠENDELJ
University of Donja Gorica, Montenegro, ramo.sendelj@udg.edu.me

Abstract: *Cryptography is the study of techniques used for preserving data confidentiality. When the personal, financial, military or national security information is transferred from place to place, it becomes subject to eavesdropping tactics. Such problems can be avoided by information encryption thus making them inaccessible to unwanted (third) parties. Protocols are created by people trying to create a system that will prevent insertion of a third party in the communication or impersonation of a person in communication.*

In this paper the following cryptographic protocols, will be presented: Wide-Mouth Frog, Yahalom, Needham-Scroeder, Otway-Rees, Kerberos, Neuman-Stubblebine, Denning-Sacco and Woo-Lam. Firstly, we will present each protocol shortly with its most important properties, followed by their comparative analysis. We will also make analysis of the the attacks they are resistant to, as well as the attacks that make them vulnerable and they are subject to. The main problem these protocols are working on is the safe exchange of secret keys between the two parties, and ensuring them that the communication is with the person they want, rather than with a stranger. Codes and protocols are important tools, but they are a poor substitute for the real, critical thinking about what is really protected and how different methods of defense may fall. Even if the intruder has access only to the ciphertext, such small cracks in some parts of the system could provide sufficient information, thus turning good cryptosystems into useless.

Examples in this research show us how by the application of logic can be caught slight difference between the protocols. For certain protocols we identify errors and suggest corrections. One of key mistakes could be found in the use of the Kerberos protocol with DES, which is however weak protocol, but it is still found in some products that have not implemented the newer and better AES protocol. Furthermore, the Kerberos could be weakened by using the lower protocols. Protocols that use synchronization of clocks, such as the Needham-Schroeder, which can be a source of the attack, must be supplemented with protocols to access the time servers. There is no easy way to make systems safer, there is no substitute for careful planning and continuous critical examination.

Keywords*: cryptography, protocols, error identification, protocols' improvements*

1. INTRODUCTION

Cryptography is the study of techniques used for preserving data confidentiality. Cryptographic protocols are used to establish secure communication over unreliable global networks and distribution systems. They rely on cryptographic protection methods in order to provide basic security services of confidentiality, integrity and undeniability. In the literature there are numerous protocols, but none of them is the perfect one.

Each has its advantages and disadvantages. When the personal, financial, military or the information of national security is transmitted through a computer network, it becomes vulnerable to listening tactics, which makes information become potentially vulnerable. Vulnerability of information is reflected in the illegal access, illegal modifications and integrity violation. Therefore, the aim of this work is to focus on the analysis and comparison of the existing cryptographic protocols while maintaining

message transfer through the network. The basic cryptographic approach is based on a combination of the authentication and key exchange, in order to solve a common computer problem: two entities -the sender (originator) and the recipient, who want to communicate through a computer network safely. The question is: how can these entities exchange secret keys and be sure to talk to each other, but not to the third party at the same time? A common cryptographic technique is to encrypt each individual conversation by using a special key. This key is called the session key, because it is used only for one specific session. Session keys are useful because they only exist during the session. However, an additional problem in a cryptographic protocol is a way of key distribution to the participants of a session. This study is focused on comparative analysis of algorithms that have different ways of solving the problem of key distribution and the results of the analysis are used to create the overall comparative picture about the properties of algorithms mentioned, which is still the basis for making guidelines on their practical usage and possible solutions.

2. CRYPTOGRAPHIC PROTOCOLS AND ATTACKS

2.1 Cryptographic protocols

There are two types of cryptographic protocols, symmetrical and asymmetrical. At *symmetrical protocols* the same key is used for encryption and decryption, and thus, the main problem with this protocol is the possibility of the password interception, which gives the intruder the ability not only to read the messages, but to send them out as well. Therefore, this encryption method is the most commonly used for data protection that isn't shared with other parties. On the other side, *asymmetrical protocols* use two types of keys, a public (which is used to encrypt the data and it is sent to all those we want to exchange encrypted data with) and a secret key (which is used for data decryption). Sending the public key, which is used only for encryption but not for decryption, is the main advantage of these protocols.

When we are talking about cryptography, the key issues are to provide the following: (1) integrity of encrypted data (to prevent unauthorized changing, deleting or information substitution); (2) information confidentiality (only authorized persons have the key); (3) authentication – introducing is the beginning of each communication followed by information exchange; and (4) Impossible to deny responsibility - Non-repudiation ensures that the contract, particularly the one made over the Internet can not be overridden later by any of the parties involved.

Some considerable consequences can be caused by unauthorized access: the business could operate at a financial loss; a competitive business could become very profitable, decreased trust of service users or product consumers. The examples on this information include the following: data collection on wages, on employees, project files, accounting data, confidential contracts etc. The aim of the cryptographic system attack is getting the code that enables text encryption and decryption. There are many types of attacks, starting with the situation when the intruder has only a cipher text or a cipher text and a plaintext used to get the code. Whereas getting the code in this way is very difficult and it requires huge assets and knowledge as well, the intruders have found some easier ways to get it. These attacks are based on finding a way to be into the communication channel between the sender and the intended recipient, so-called man-in-the-middle attacks. Replay attack is carried out by an intruder who tries to use the old keys and establish communication in that way. In the systems where all the keys are kept at one place such as systems with KDC (Key Distribution Center) the risk of an attack is, at the same time, a possibility that the intruder could compromise or break down the KDC, which would compromise the entire system.

2.2 The types of attacks on cryptographic protocols

Probably the most common attacks on cryptographic protocols are freshness attacks. If the exchanged messages do not have appropriate timestamps, an intruder gets authorization by using a recorded copy of the message from a previous run of the protocol. To avoid this kind of attack the following should be taken into account during the designing of the protocol: (i) each cryptographic statement of the protocol should contain a random number generated by the receiver in the previous run of the protocol; (ii) the usage of synchronized clock and timestamps.

Replay attack refers to a possibility when the intruder uses the old password and frauds the participants of the communication by false representation (social engineering). In order to prevent this type of attack the

following measures must be taken: a special session token for each session and time stamping. Parallel session- at this attack several sessions are run simultaneously. The intruder uses message from one session to run a parallel session.

Type attacks are based on the replacement of a part of the message with the other part of a different type, and a random number is used as the key. This attack can be avoided if these guidelines are followed: (i) When establishing contact between the sender and the receiver, in the systems with symmetric keys, at least one message must be sent containing the sender's identity; (ii) If the system with the public key is used, when establishing contact at least one message must be sent with the sender's identity as well; (iii) In the systems with the secret key, in establishing contact, both messages must contain the identity of the recipient

3. PROTOCOLS

3.1 Wide-Mouth Frog

The Wide-Mouth Frog protocol is a computer network authentication protocol published by Burrows, Abadi and Needham (1) in 1989. This is possibly the simplest symmetric key-management protocol that uses a trusted server. The trusted server has keys that it shares with the principals concerned (sender and receiver). These keys are used not for encrypting real messages between the principals concerned, but for the keys distribution. What makes this protocol special is the principal that generates and sets up a session key, not the center for the key distribution. The most important assumption in this protocol is that the sender is competent enough to generate good session keys, which is not easy to be done. To overcome this problem, a server must generate session keys. Timestamps are used so that the authentication center (server) and the receiver could know how much time has passed since the generation of the message itself. The message is ignored if it took more time than agreed on, (which makes difficult to a third party to find out the secret key or to insert in the communication between sender and receiver). This protocol has never been applied broader because it has several major flaws. The biggest flaw is that all principals and the server as well must have access to a single clock, and the same clock must be protected from the influence of a third party. Another problem is that the server knows all the keys so if it happens that the safety of the server is in danger, than all safe channels established through the server are in danger, too. The third problem is that the shared encryption key is fully determined by sender. Repeated attack at the Frog protocol, the adversary can keep the session keys for later reuse. This attack assumes that the server does not keep a record of keys used recently nor the timestamps as well.

3.2 Yahalom

This protocol uses authentication server and random numbers. In this protocol the server determines the session key, and it is symmetrical. It is designed to be applied in unsafe networks such as the Internet. It can be said that this protocol is a corrected version of the Frog protocol. Attack at Yahalom can be performed by an intruder masked as a sender who starts a parallel session, which is a parallel attack. In this way he is likely to mislead the receiver and to get the session key. In his work, Burrows, suggested a correction of this Protocol, by adding a random number of the receiver in the first message exchanged between the server and the receiver.[1] Even the corrected protocol is un resistant to attacks. For it is possible to be under a replay attack. This weakness comes from the recipient's inability to check whether the session key received a message from the sender or server. If the intruder presents himself as the sender, it is possible to use the old session key and start communicating with the receiver so that and the receiver can not see the identity switch. [2]

3.3 Needham- Schroeder

This protocol is available in two versions, the one with symmetrical and the other one with asymmetrical key, which is the public key. The version using the symmetric key was the basis for the development of the Kerberos protocol. It is used for the keys exchange in unsafe networks such as the Internet. The server for the key exchange and session key allocation is used here, too. This protocol could be attacked by a replay attack. The intruder can use an old session key and start communication with the receiver. The recipient is not aware that this is not a new key. This attack can be thwarted if the timestamps are used in the protocol as well. Type attack is also a possibility, when the intruder types his name instead of a random number.[3]This attack can be prevented if in the message, each field is

checked whether it corresponds to the type it should.[4]Another type of attack that is possible on this protocol is freshness attack, the solution is to use timestamps. This solution is applied at the Kerberos protocol. Another type of attack is MIM (man -in -the middle) in which the sender and receiver think they communicate directly unaware that all communication is via the intruder. Correction of the protocol came out in 1995, and it consists of adding the receiver's name in the second message of the protocol. Denning and Sacco showed that there is a possibility of a parallel attack. This attack can be disabled by adding a random number of the receiver in the second message. Denning and Saccocs have suggested another solution, which is the usage of timestamps. Like all server protocols, this one is also subject to be attacked on its own server.

3.4 Otway- Rees

This protocol uses symmetric keys, random numbers, indexes and authentication server. The protocol is subject to man - in - the middle attack.[5]There is a possibility that the intruder gets a new session key from the server, which the intruder can use to present himself as the receiver to the sender. In this case the intruderuses two different keys to communicate with the receiver and sender. There is a possibility of a type attack when the intruder plants the name of the sender, receiver and the index as the session key.[6] Another attack is a replay attack, when the intruder uses old random numbers in order to deceive the receiver and initiate communication.

3.5 Kerberos

Kerberos is simultaneously an authentication protocol and KDC, too. Kerberos can be described as a safe authentication protocol that uses a Single Sign On login type, which ensures high efficiency. Users are allowed to sign on the system only once, and have access to system or network resources, depending on their authority. Communication between entities within the Kerberos protocol is based on the tickets exchange. A ticket represents a type of encrypted data that is transmitted through the network, and delivered to the client who saves them and uses it later as a pass for establishing communication with the appropriate server. While encrypting messages / tickets, Kerberos protocol uses symmetric DES algorithm or its variants such as 3DES, and Kerberos Version 5 uses AES algorithm only. Kerberos environment consists of two servers as follows: authentication server AS and Ticket-Granting Server.

3.5.1 Kerberos thread-safety

There is a possibility of cache and repeating old Authenticators. Although the timestamps should prevent it, the repetition can be made until the expiration time of the ticket. Servers are supposed to store all valid tickets in order to prevent repeating, but it is not always possible to do so. In addition, the lifetime of tickets can be quite long, and it is usually about 8 hours long. Authenticators rely on the fact that all the clocks in the network are more or less synchronized. If it is possible to trick the server in terms of the time, then the old Authenticator can be repeated without any problems at all. Most network time protocols are unsafe, so this could be a serious problem. Kerberos is subject to password guessing attack. The intruder can obtain tickets and then try to decrypt them. It is known that the average user usually does not choose good passwords. If the intruder has collected enough tickets, he has a good chance to find out the password. Probably, the most serious attack is the one involving malicious software. Kerberos protocols rely on the fact that the programs are reliable. Kerberos improvements are being worked on, including the implementation of public key cryptography and application of smart cards for key management. Kerberos version 4 used symmetrical DES encryption system which wasn't reliable and it is replaced with the 3DES system, and in Kerberos version 5,AES system is commonly used because it is more reliable.

3.6 Neuman – Stubblebine

Due to system errors or diversions, clocks can become unsynchronized. If this happens, it is possible to attack the majority of these protocols. If the sender's clock isn't synchronized within configured limits with the receiver's clock, the intruder can intercept the sender's message and repeat it later, when timestamp matches the current time on the computer of the receiver. This attack is called suppress-replay attack and it can have serious consequences. This protocol tries to repel suppress-replay attack but it is subject to type attack [7] by replacing keys with random numbers. There is a possibility of parallel attack, too. [8]

3.7 Denning-Sacco

This protocol uses timestamps and public key signatures. It is a modified version of Needham - Schroeder protocol with symmetric key. In Denning Protocol, timestamps are applied instead of random numbers in order to eliminate the risk of freshness attack, which was a problem in the Needham - Schroeder protocol. Timestamps entail a problem of clock synchronization. There is a possibility of parallel attack on this protocol. In the original protocol, the receiver has no way to verify if he really receives a message from the sender. The intruder is thus enabled to start a parallel session and send to the receiver an intercepted message from the sender-receiver communication. Lowe is in his work provide a solution to this problem. [9]

3.8 Woo-Lam

This protocol uses public keys, random numbers and signatures. It can be attacked by parallel attacks. The attack is carried out in a way that an intruder presents himself to the receiver as being the server, and convinces him to continue communicating. As an answer to this threat it is necessary to take certain measures, such as: each message should contain session number, accept the session only if the last message session has passed. All these measures taken do not mean that we have eliminated the possibility of other attacks. Another type of attack that is possible, on this protocol, is type attack. An intruder, using an incorrect message, can get the session key. The only way to prevent this is to analyze all the messages and reject those that do not match the characteristics of the protocol. [10]

4. COMPARATIVE PROTOCOLS' ANALYSIS

From the Table 1 we can see that most of the steps are performed in Woo-Lam Protocol. All the protocols, with the exceptionof Wide - Mouth Frog, use the services of KDC (Key Distribution Center). An equal number of protocols use random numbers, which are used only once, and timestamps, in order to prevent a replay attack. Only Neuman-Strubbine uses both. Only Otway- Rees uses indexes. Most protocols are with symmetric keys. The protocols with asymmetric keys use signature as additional way of protection.

Table 1. Protocols' properties

	Number of steps	Keys control	Random number	timestamp	Index	Symmetric keys	Asymmetric keys	Signature
Wide – Mounth Frog	2	sender		x		x		
Yahalom	5	server	X			x		
Needham-Schroeder	6	server	X			x	x	
Otway-Rees	5	server	X		x	x		
Kerberos	4	server		x		x		
Neuman–Stubblebine	5	server	X	x		x		
Denning-Sacco	4	server		x			x	x
Woo-Lam	8	server	x				x	x

The Table 2 shows that all the protocols are the most subject to parallel attacks, and the least to freshness attacks. Needham- Schroeder and Otway- Rees protocols are the most subject to a number of different attacks whereas Kerberos is the least subject to any. The table shows that there is no a completely safe protocol. There is always a possibility of an attack.

Table 2. Protocols' attacks addressed in the literature

	Freshness	Man–in-the middle	Type	Replay	Parallel
Wide – Mounth Frog		[13]		[6],[15]	
Yahalom			[17]	[19]	[1]
Needham-Schroeder	[11]	[17]		[9], [17]	[9]
Otway- Rees		[16]	[10],[11]	[23]	[24]
Kerberos				[22]	
Neuman–Stubblebine		[18]	[19]		[20]
Denning-Sacco	[21]				[15]
Woo-Lam			[10]		[14]

5. CONCLUSION

The disadvantage with Wide-Mouthed Frog protocol is that the sender devises a session key. This protocol is subject to replay attack. Another flaw is the absence of authentication during random numbers exchange. The good side of this Protocol is its simplicity. Yahalom protocol's main flaw is the possibility to run parallel sessions. Furthermore, all the systems that use the services of KDC are subject to possible attacks on the system whether the attack aims to get the passwords or to

prevent communication with KDC, which disables the entire system. In Needham-Schroeder protocol we have a problem with the old session keys and the possibility of starting attack through them. This protocol is subject to "man in the middle" attack. There is a version of this protocol with a public key, which has solved this type of problem. In the Otway-Rees protocol an intruder can communicate both, with the sender and receiver, by using two different session keys. The problem with the old keys appears as well. Kerberos could be attacked in the cases of user's mistake or by taking weak passwords. Furthermore, in this protocol there is a problem with clocks synchronization, as with all other protocols that rely on timestamps. Kerberos version 4 used symmetrical DES encryption system that was not reliable and it is replaced by somewhat better 3DES system, but version 5 with AES system is considered to be more reliable. Another protocol that relies on timestamps, which is possibly its main flaw, is Neuman - Stubblebine protocol. This protocol is subject to replay and "man in the middle" attacks. Attack on Denning-Sacco protocol is possible if the attacker presents himself as being the sender and sends his session key to the receiver. The problem with Woo-Lam Protocol is a possibility for an attacker to run parallel sessions. BAN Logic program is used for Cryptographic Protocols Analysis and detecting their flaws. The problem of establishing secure session keys between pairs of computers (and people) on the network is so significant that it prompted a very extensive research towards the development of new and debugging the old protocols.

REFERENCES

[1] M. Burrows, M. Abadi, and R. M. Needham. A logic of authentication. Proceedings of the Royal Society of London, 426:233–271, 1989.

[2] Aditya Bagchi, Vijayalakshmi Atluri, Information Systems Security: Second International Conference, ICISS 2006, st.196.

[3]Pieter Ceelen,Sjouke Mauw,Sasa Radomirovi. Chosen-name Attacks: An Overlooked Classof Type-flaw Attacks.Universit´e du Luxembourg Facult´e des Sciences, de la Technologie et de la Communication

[4]James Heather, Gavin Lowe, and Steve Schneider. How to prevent type flaw attacks on security protocols. J. Comput. Secur., 11(2):217–244, 2003.

[5]Frédéric Massicott,Man-in-the-middle attack against the initiator of Otway-Rees Key Exchange Protocol, SANS Institute, 2000.

[6] J. Clark ,Attacking Authentication Protocols, 1996

[7] Graham J. Steel ,Discovering Attacks on Security Protocols by Refuting Incorrect Inductive Conjectures, University of Edinburgh, 2003., 101 st.

[8] Gavin Lowe, Some New Attacks upon Security Protocols, Oxford University Computing Laboratory, Wolfson Building, October 1, 1996

[9] G. Lowe, "A family of attacks upon authentication protocols," Department of Mathematics and Computer Science, University of Leicester, Leicester, 1997.

[10] James Heather,Gavin Lowe,Steve Schneider, How to Prevent Type Flaw Attacks on Security Protocols

[11] Graham J. Steel, Discovering Attacks on Security Protocolsby Refuting Incorrect Inductive Conjectures

[12] Jeremy BRUN-NOUVION, Hicham HOSSAYNI, Security models , 1st Semester 2010/2011

[13]John Kelsey , Bruce Schneier, David Wagner, Protocol Interactions and the Chosen Protocol
Attack, U.C. Berkeley, 2005

[14] Anca Jurcut, Tom Coffey, Reiner Dojen, Robert Gyorodi, Security Protocol Design: A Case Study Using Key Distribution Protocols, Department of Electronic & Computer Engineering,University of Limerick,Ireland.

[15] Reiner Dojen, Anca Jurcut, Tom Coffey, Cornelia Györödi: On Establishing and Fixing a Parallel Session Attack in a Security Protocol. Intelligent Distributed Computing, Systems and Applications. Springer Berlin / Heidelberg, Vol. 162, pp. 239-244, September 2008.

[16] M. Panti L. Spalazzi S. Taoni, Attacks on Cryptographi Protools: A Survey,Istituto di Informatia, University of Ancona

[17]G. Lowe, A Family of Attacks upon Authentiation Protools, Tehnial Report, Department of Matematis and Computer Siene, University of Leiester, 1997.

[18] Frederic Massicotte, Man in the middle attack against security protocol, SANS Institute Ottawa, 2002

[19]Alexander Marsalek, A review of attacks found and fixed, University of Technology Graz, Institute for Applied Information Processing and Communications, Graz, Austria

[20]Lowe, Gavin , "An attack on the Needham-Schroeder public key authentication protocol.".Information Processing Letters,November 1995

[21] Paul Syverson, A Taxonomy of Replay Attacks, Naval Research Laboratory Washington,

[22] Tzonelih Hwang , Narn-Yih Lee, Chuan-Ming Li, Ming-Yung Ko, Yung-Hsiang Chen , Two attacks on Neuman—Stubblebine authentication protocols, , Institute of Information Engineering, National Chen-Kung University, Tainan, Taiwan, 1993

[23]Gavin Lowe. A family of attacks upon authentication protocols.Technical Report 1997

[24] Gagan Dua, Nitin Gautam, Dharmendar Sharma, Ankit Arora , Replay attack prevention in kerberos authentication protocol using triple password,Department

of Computer Engineering, National Institute of Technology, Kurukshetra, India, 2013

[25] Lambert M. Surhone, Mariam T. Tennoe, Susan F. Henssonow,Otway-Rees Protocol: Computer Network, Authentication, Communications Protocol, Internet, Replay Attack, Eavesdropping, Security Protocol Notation, Cryptographic Nonce, Tapa blanda – 16 sep 2010

[26] Horea Oros, Florian Boian, Spi Calculus Analysis of Otway-Rees Protocol,Int. J. of Computers, Communications & Control, ISSN 1841-9836, E-ISSN 1841-9844Vol. III (2008), Suppl. issue: Proceedings of ICCCC 2008, pp. 427-432