IJSecurity Protocol Verification: A Survey

Anjana Jha¹Priya Patel²

^{1,2}M.E Student Computer Engineering

^{1,2}L.C.I.T, Bhandu, Mehsana

Abstract—Security protocols are prone to various attacks when two principals communicate over network. Hence the verification of protocol is must. Security protocol verification is a very wide area for research. This paper gives the brief overview of the various approaches that have been applied in this area. It also list some of the other problems that are to be taken care for the betterment of security protocol.

*Keywords:*Security protocol, security protocol verification, formal approach, DoS attack.

I. INTRODUCTION

Like any other protocol, security protocol is the set of rules that are to be followed to achieve the basic security goals. It is also known as cryptographic protocol. It was very firstly introduced by Needham-Schroeder [1] in 1978. The main concern of security protocol is to secure the communication over the network as it was frequently used by us in our dayto-day life. The basic goals include: Authentication of participants, Key Exchange, Confidentiality, Integrity, Non-Repudiation, Anonymity, Availability and so on.

Messages to be shared between two parties often require a help of trusted third party to exchange the key. This process typically includes use of symmetric and asymmetric encryption, digital signature, hash function and more. But to analyze and design such security protocol seems to be difficult because the properties that are supposed to be ensured are very subtle. These protocols dwell in the antagonistic and complex environment. The term antagonistic refers to intruder and whose capability of attack is difficult to capture. Other terms such as attacker, spy, and eavesdropper may also be used instead of intruder.

II. BACKGROUND HISTORY

According to researchers, security protocol is one of the précised field in which research can be carried out as it is one of the critical components of any security architecture. Though security protocols are quite simple but it is difficult to get right. The difficulty is being witnessed by Needham-Schroeder public-key protocol [1]. NSPK was secure for almost 17 years till Lowe [5] discovered the flaw in the protocol. This protocol simply uses the symmetric encryption algorithms to enable two participants to create secure session between both via trusted third party as shown in figure.1.



Steps included in NSPK[1] protocol:

- 1) $A \rightarrow S$: A, B (A requests B's public key from S)
- 2) S \rightarrow A: {K_{PB}, B}Kss (S responds. B's identity is send along with K_{PB} for confirmation)
- 3) A \rightarrow B: {Na, A}K_{PB} (A sends a fresh nonce Na to B)
- 4) $B \rightarrow S$: B, A (B requests S for A's public key)
- 5) $S \rightarrow B$: {K_{PA}, A}Kss (S sends the public key of A to B)
- B→A: {Na, Nb}K_{PA} (B generates a fresh nonce Nb and sends it back to A, along with A's nonce Na)
- 7) $A \rightarrow \{Nb\}K_{PB}$ (A confirms Nb to B)

The flaw that has been discovered by Lowe can be found by applying formal methods. The attack discovered is called man-in-middle attack[5].

Steps:

- 1.1) $A \rightarrow I$: {Na, A} K_{PI} (A sends a fresh nonce Na to I)
- 2.1) I(A) →B: {Na, A}K_{PB} (In a parallel run of the protocol, I masquerading as A, relays the message received from A after encrypting it under B's public key.)
- 2.2) $B \rightarrow I(A)$: {Na, Nb}K_{PA} (B responds to I's message)
- 1.2) $I \rightarrow A$: {Na, Nb}KPA (I relays B's message to A)
- 1.3) $A \rightarrow I$: {Nb} K_{PI} (A returns Nb to complete protocol run with I)
- 2.3) I(A) \rightarrow B: {Nb}K_{PB} (I masquerade A and forwards Nb encrypted under B's public key)



Fig. 2 Man In Middle Attack

Besides man in middle attack, there are various other attack [10] that security protocols can fall prey. Below mentioned list are the vulnerabilities that are due to flaw in the protocol design.

- 1. REFLECTION: It means to spring back messages back at an agent.
- 2. ORACLE: The legitimate user is forced to perform some step of a protocol so that the intruder can obtain some data he could not otherwise obtain.
- 3. **REPLAY:** Attacker keeps on monitoring the protocol and replay some of the messages after some time.
- 4. INTERLEAVE: This is one of the most inventive style of attack in which the intruder plans for the overlapping of more than one protocol run.
- 5. ALGEBRAIC ATTACK: Many of the protocol uses exponentiation function. One of the example is Diffie-Hellman key establishment protocol [15]. As the exponentiation function is commutative, it is easy for intruders to take advantage of such identities to weaken the security of protocol.

25

Because of these attacks the necessity of protocol verification aroused. Cryptographic protocols can be verified either by the formal methods or by provable security. Former method was dependent on the modeling techniques while the later one was based on computational proofs.

III. RELATED WORK

According to Meadow [7], the formal method is one which is used to model the security protocols and its properties with the help of an efficient procedure. There are various approaches to the formal verification as shown in fig 3.





Generally the main focus of any security protocol is to achieve goals like secrecy and authenticity which hides the importance of other goal like availability. Only satisfying former goals doesn't prove that the protocol is safe. Other attacks such as Resource Exhaustion attack should also be taken care of which is the common source of DoS.

DoS make the legitimate user unnecessarily waste the system resources, money and time. Many approaches have been designed to avoid such an flaw. The very first framework as suggested by C. Meadow [2] compares the cost of both intruder and defender to evaluate the protocol. It expands the former model [3] by taking into account the cost and different actions of intruder. This protocol also relates the DoS resilience to the fail - stop protocol as suggested by Gong and Syverson [8].

- A. Fail stop protocol:
- 1. Each message sent by the sender contains the identity of sender and receiver along with the protocol identifier, its version and message sequence number.
- 2. Message is then encrypted using the shared key between sender and receiver.
- 3. All the bogus messages gets rejected and valid messages are accepted.
- 4. Protocol stops if any valid message gets delayed after the timeout period.

According to Meadows[2] framework if the cost incurred by defender is greater than the cost by intruder, attack is

possible. But the cost function that were used are not realistic, they are ad-hoc and crude. Same framework has been applied by the Ramachandran [9] to JFK protocol which discovered the DoS attack. Smith et al.[12] did the deep analysis on JFK protocol and discovered some attacks on it. All the above mentioned analysis is done by hand which is of course a time consuming task. So the researchers decided to automate the same. One way is to formalize the attack condition in rules and the another way is to improve the protocol itself so that it can withstand the DoS attack.

The very first step in this direction is taken by Matsuura and Imai[6] who had suggested the *Three Pass Authentication* for DoS resilience. This criteria demands the more resource consumption by the initiator than the responder. This necessity is the basic principal of proof of work protocols.

Another approach in the same field has been suggested[4] which uses the concept of client puzzle to approve whether the user requesting for the resource is legitimate or not. Before getting access to any resource, the user has to solve the puzzle. Until the server gets convinced, user will not be granted any resource. Conclusion is that the server will perform the expensive operations only if it follows the "accepted state" in which client solves the puzzle.

Besides the client puzzle way of preventing the DoS attack, Cookies is the another way to defend DoS attack. Cookies are the authentication tokens that are issued by the server upon the initial connection. The client must return the same token to server to continue the connection. The connection is stateless i.e. it doesn't store the cookies. It is also used in the Meadow framework for authenticity at early stage.Protocols that use cookies can also be vulnerable to other types of attacks.

Groza and Minea [11] has proposed a set of rules that approve the DoS attack and automate their detection. For the case of ease he divided the cause of DoS attack into two broader categories. One is the attack due to excessive use of resources and the another one is due to malicious use of same. This classification separates the legal issues from the illegal one where legal indicates the valid use of protocol while other indicates the manipulation of protocol. Author has used the ASLan of AVANTSSAR[14] tool to express the rules for DoS detection. It works well with some protocols like STS and JFK.

Even another tools are available for the protocol verification. One such is Scyther[13] which only checks the secrecy and authenticity property of security. Still much work has to be done in order to detect the DoS attack. We can do it in two ways. Either model the protocol in such a way so that it can detect the DoS attack or we can change the tool itself.

IV. CONCLUSION

Security protocols are vulnerable to many attacks which are simply unnoticed for several years. Protocol designer must fix the flaw in protocol for smooth flow. Various approaches have been suggested. This survey paper helps us to compare the pros. and cons. of various approaches of security protocol which in turn enables us to select the better approach for verification. Now a day's automated approach is of growing concern on which many researchers are working and still much work is expected from same.

REFERENCES

- R. Needham and M. Schroeder.Using encryption for authentication in large networks of computers.Communications of the ACM, 21(12), 1978.
- [2] Meadows, C.: A cost-based framework for analysis of denial of service networks. Journal of Computer Security 9(1/2), 143{164 (2001)
 [3] C. Meadows. A formal framework and evaluation method for network denial of service. In Proceedings of the 12th IEEE Computer Security Foundations Workshop, pages 4{13. IEEE Computer Society Press, June 1999.
- [4] D. Stebila and B. Ustaoglu. Towards denial-of-serviceresilient key agreement protocols. In 14th Australasian Conference on Information Security and Privacy, LNCS vol. 5594, pages 389{406.Springer, 2009
- [5] Gavin Lowe. An attack on the Needham-Schroeder public-key authentication protocol. Information Processing Letters, 56(3):131 { 133, 1995.
- [6] K. Matsuura and H. Imai.Protection of authenticated key-agreement protocol gainst a denial-of-service attack. In International Symposium on Information Theory and Its Applications (ISITA), pages 466{470,1998.
- [7] Catherine Meadows. Formal Methods for Cryptographic Protocol Analysis: Emerging Issues and Trends. Selected Areas in Communications, 21(1):44{54, 2003.
- [8] Li Gong and Paul Syverson. Fail-stop protocols: An approach to designing secure protocols. In R. K. Iyer, M. Morganti, Fuchs W. K, and V. Gligor, editors, Dependable Computing for Critical Applications 5, pages 79{99.IEEE Computer Society, 1998.
- [9] V. Ramachandran. Analyzing DoS-resistance of protocols using a cost-based framework.Technical Report DCS/TR-1239, Yale University, 2002.
- [10] G. Lowe. Some new attacks upon security protocols.9th IEEE Computer Security Foundations Workshop, 1996.
- [11] Groza, B., Minea, M.: Formal modelling and automatic detection of resource exhaustion attacks. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS) (2011)
- [12] J.Smith, J.M.Gonzalez-Nieto, and C.Boyd, "Modelling denial of service attacks on JFK with Meadows's costbased framework," In Proceedings of the 2006 Australasian workshops on Grid computing and eresearch (ACSW Frontiers). Darlinghurst, Australia, 2006, pp.125-134, 2006.
- [13]T. Paper, "The Scyther Tool : Verification , Falsification , and Analysis of Security Protocols," pp. 1–4.
- [14] The AVANTSSAR project. http://avantssar.eu/
- [15] W. Diffie and M. E. Hellman.New directions in cryptography.IEEE Transactions on Information Theory, 22, 1976.