ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume4, Issue 5, May 2015

A Review and Comparative Analysis of Modal Logics: BAN, GYN and SVO

Tanuja Thakur, Sachin Dogra, Yamini Sood

***Abstract*— Traditionally, security protocols have been designed and verified using various techniques. Formal logics have been used to identify a number of flaws in protocols previously considered to be secure. The selection of proper modal logic is a crucial goal in the protocol analysis and verification process. This paper gives a comparative study of modal logics, which are widely used in modeling of security protocols. We will focus on logics of authentication .However, we will not only be discussing logics, but also be looking at the 'rhyme and reason' of authentication, the attempts to formalize and define notions of authentication and to apply these. Thus, we will also be considering the logic of authentication in a broader sense. This paper discusses three modal logics: BAN, SVO, and GYN. A formal analysis of these three has been presented.**

***Index Terms*—authentication protocol, modal logic, BAN, SVO, GYN**

I. INTRODUCTION

The methods for analysis of authentication protocols mainly focused on detecting the leakage of information in the protocol. The present methods do not focus much on determining whether authentication protocol attaining goals or not. For some critical reasons the security protocols are not able to fulfill all of the intended objectives **[2].** Hence researchers around the world have developed methods to check whether authentication and security protocols are able to fulfill the intended objectives or not. **[5].**Today most of the modal logics have been used frequently because of the simplicity and effectiveness in the analysis of authentication and security protocols. Modal logics are intended to find out the reason of the working and non-working modules of cryptographic protocols and helps in finding out the missing assumptions, hidden flaws and severances. After finding out the deficiencies the modal logics try to reevaluate the protocol by making required changes in the protocol. After reevaluation the inference rules are applied or reapplied whether the protocol is fulfilling its objectives after changes or not. Many of the researchers have developed so many model logics to verify the authentication protocols security. This paper focus on BAN logic, GYN and SVO, which are popular these days.

Manuscript received April 30, 2015.

***Tanuja Thakur**, Electronics and Communication Dept., Sri Sai University, Palampur, India,*

***Sachin Dogra**, Electronics and Communication Dept., Sri Sai University, Palampur, India.*

***Yamini Sood**, Computer Science Dept., Sri Sai University, Palampur, India.*

Mainly BAN logic have given the popularization to the modal logics because its' strong verification method and ease of use. The BAN logic reduces the redundancies in the authentication protocols. Many of the authors have said BAN logic's success **[6, 11, 4]** and it have been used in verifying several protocols. After the development of BAN logic the researchers tries to develop some other new modal logics in verifying he authentication and security protocols. A popular descendant of BAN is GNY. SVO is also a good extension to BAN logic in this scenario.

There are a number of tools have been developed till date for the formal analysis of authentication and security protocols. These tools can be broadly classified in three categories: model checker, theorem provers and formal logics.

Model checkers are state space explorers. This type of methods verify goals at each state of an authentication or security protocol. Using these type of methods user can verify the modeling between each state or he can use a mathematical technique to verify the entire set of states together.

On the other hand, theorem provers, find out the reasoning of verification at the higher level of the protocols to give the chain of logics that will contain a reasonable proof for a particular property of an authentication protocol to be hold. Also these type of methods find out an alternative or a counter example during the process of verification.

Finally, the main concern and a lot of attention have been given in recent years towards the formal logics. Formal logics give the user an easy way to understand the definitions of modules in authentication protocols. Formal logics also helps to perform reasoning more rigorously. Many of the formal tools have been proposed by researchers, but only few are successful. Formal logics provides answers to almost all the answers about an authentication protocol which helps in developing correct solution to the problems. Formal logics optimizes the authentication protocols for best performances in different applications.

The most widely used methods among all above classifications are the logic-based verification tools, because of simplicity and conciseness of the proofs given by these methods for the authentication and security protocols. The very first protocol proposed under this category is the BAN logic. BAN logic apply the modal logic approach based on certain proof to the authentication protocols. BAN is also known as the logic of belief. [16]**.** BAN begins with analyzing a protocols by firstly formalizing the message exchange process in the authentication protocol in its' own logic language. After this all BAN list out all the assumptions and assertions in the protocol. Finally, BAN applies its' rules to the assumptions and assertions to find out some conclusions. Later many researchers have criticized the BAN logic for some of the flaws in it and try to propose the new formal logic

approaches. However, new approaches are also the extensions to the BAN logic. In this paper we have discussed the BAN and the two of its extensions i.e. GNY and SVO.

Weaknesses in security protocols (SP) are hard to identify, as they can be the result of subtle design flaws [15]. The formal verification of security protocols may be done in two ways. One possibility is to use a modal logic of authentication. The other possibility is to use general purpose formal methods. This paper provides discussion and a comparative analysis of the BAN, GNY and the SVO formal logic verification tools.

II. MODAL LOGICS APPROACH

Modal logic approaches are generally based on the deductive reasoning. These type of approaches use logics of beliefs and knowledge of the protocols to be verified. To verify a protocol the set of axioms and inferences have been applied on the protocols assumptions and assertions to derive the goals of the protocols. The message exchange process has been examined carefully to give a proof of authenticity and security of the protocol. Modal logic approaches give simple and small proofs. These approaches involve the following steps:

- Formalization of protocol messages
- Specification of initial assumptions
- Specification of protocol goals
- Application of logical postulates

A successfully verified protocol can be considered secure within the limitations of the logic. On the other hand, the results of a failed verification assist in the identification of missing initial assumptions and design-flaws of the protocol.

A. BAN Logic

BAN was the first formal logic approach model proposed by M. Burrows, M. Abadi and R. Needham. It helps the user to verify what is reasonable to be believed in an authentication and security protocol [11]. BAN works in three steps mainly to analyse any authentication and security protocol [2]. First, explore the initial assumptions from the protocol statements, and translate them to symbolic notations. For this purpose, BAN uses different logical constructs. Second, verify the goals of the protocol. Third, a group of rules are applied to the message exchange and the assertions to acquire the goal.

First of all the messages and the actions of the protocol to be verified has been converted to the formulas. BAN considers the following formulas in addition to P believes X.

$P \ sees \ X$: The principal P receives a message containing X. Here the principal P needs to decrypt the message to extract X. Principal P can now repeat X in order to send messages to other principals. X can be a statement or a simple item of data such as a nonce. The term 'sees' is meant to convey the fact that the receiving principal observes X, but does not necessarily believe it if X is a statement. Messages belonging to a correct protocol should ultimately entitle principals to new beliefs, otherwise they are useless from the point of view of authentication.

$P \ said \ X$: At some point in the past, P is known to have sent a message including X. This implies that, if P is trusted, P believed X when it sent the message.

$P \ controls \ X$ (P has jurisdiction over X): P is trusted as an authority on X. For example, an authentication server is trusted as an authority on statements about the key that is allocated as a shared secret between two principals.

$fresh\,(X)$: X has not been sent in a message belonging to a previous run of the protocol. Thus nonces are values which, by definition, are constructed to be fresh.

$P \overset{K}{\leftrightarrow} Q$: P and Q are entitled to use the secret key K. K is a secret between P and Q and possibly other principals trusted by P or Q (such as an authentication server).

The postulates of BAN logic

First, a point about notation: To express that the statement Z follows from a conjunction of statements X and Y, say, we write:

$$\frac{X, Y}{Z}$$

The main postulates of BAN logic are:

The message meaning rule [9]:

$$\frac{P \ believes \ P \overset{K}{\leftrightarrow} Q, P \ sees \ \{X\}_K}{P \ believes \ (Q \ said \ X)}$$

Interpretation of this rule is: if P believes that it shares a secret key K with Q, and if P receives a message containing X encrypted with K, then P is entitled to believe that Q once said X (that is, that Q believed X and included X in a message).

The nonce-verification rule [9]:

$$\frac{P believes \ fresh(X), P believes \ (Q said X)}{P believes (Q believes X)}$$

The nonce-verification rule says that, if we have the additional assertion that P believes X is fresh, then P must believe that Q currently believes X. Note that X must not be encrypted – otherwise Q could merely have echoed an encrypted statement in which it does not necessarily believe.

The jurisdiction rule:

$$\frac{P believes (Q controls X), P believes (Q believes X)}{P believes \ X}$$

This rule formalizes the notion of what it means for a principal to have jurisdiction over a statement: if P believes that Q has jurisdiction over whether or not X is true, and if P believes that Q believes it to be true, then P must believe in it also, since Q is an authority on the matter as far as P is concerned.

The basic problems that BAN logic tries to address is:

- there is some goal we want to achieve
- we have some idea of what we want, need
- we want to satisfy ourselves that our solution to the above goal works
- we don't want to depend on trial by fire

There are a lot of problems involved when trying to prove security. As we go over BAN logic, we want to scrutinize it, considering how much do we trust its validity? Are the rules of BAN logic sound and reasonable? When are assumptions being made and what are they? Even if we prove something like Kerberos works theoretically, we still can have problems. Using something like BAN logic, we are proving the ideal. Unfortunately, implementations aren't always (ever?) ideal. This is just another concern we need to be aware of.

B. GYN

When BAN emerged, researchers realized the potential of applying logic based techniques for the formal verification of authentication protocols. Though the BAN logic successfully identify flaws in well-known protocols, it has many weaknesses which are identified by the researchers and several corrective measures have been suggested. The immediate successor of BAN was GYN logic [16]. Recognizability is one of the improvements to BAN logic introduced in GNY .It captures the recipient's expectation of the contents of a message before actually it is being received. For example, a principal may recognize a particular structure of a message or any form of redundancy in the message. This is in contrast to BAN which assumed that redundancy is always present in encrypted messages. The second improvement is *not-originated-here* notation to identify if a principal receives his own conveyedmessages.GNY also separated the notion of possession and beliefs, in addition to extending the capabilities of BAN.

GNY Recognisability Rule

A principal P would recognize X if P has certain expectations about the contents of X before he actually receives X. P may recognize a particular value (for example, his own identifier or nonce), a particular structure (for example, the format of a timestamp), or a particular form of redundancy.

The GNY recognisability rule specifies the formula that a principal can believe to be recognizable, when given his beliefs about the recognisability of other formula [16].

$P\ believes\ \emptyset(X_i) \Rightarrow P\ believes\ \emptyset(X_1 \ldots\ldots\ldots\ldots\ldots X_n)\ for\ any\ i \in \{1,\ldots,n\}$

If a principal P believes that a formula X is recognizable, then he is entitled to believe that the whole message is recognizable.

GNY Message Extension

Typical protocol specifications often include verbal description to the effect that a principal should proceed only if certain conditions hold or only if he holds certain beliefs. This can be regarded as a precondition of a message.

The precondition of a formula X, represented by statement C, is described as $X \rightarrow (C)$where C is called a message extension. When a receiver receives a message that contains $X \rightarrow (C)$, it should interpret it as such.

C. The logic of SVO

SVO logic was proposed by Syvers on and van Oorschot [14] as an extension to the BAN logic. SVO has proven to be a best successor of BAN logic based on the improvements made by it. SVO operates in following steps in order to verify the authentication and security protocols:

1. Initial state assumptions has been defined in this step
2. Target security protocol has been annotated
3. Received messages comprehensions has been asserted
4. Asserting interpretation of comprehended messages
5. Applying inference rules repeatedly until getting the intended results. We briefly describe the notations of SVO logic given in [14] as follows.

SVO Notations

$P\ believes\ X$: P acts as if X is true.

$P\ received\ X$: P has received a message including X.

$P\ said\ X$: P sent X at one time.

$P\ controls\ X$: P has jurisdiction on X.

$fresh\,(X)$: X is fresh.

$P \overset{K}{\leftrightarrow} Q$: K is a shared key between P and Q. It can be shared by a trusted third party of P and Q.

$\{X\}_K$: X is encrypted with K.

$PK\,(P,K)$: K is a public key of P. Also, $PK_\sigma\,(P,K)$ and $PK_\psi\,(P,K)$ can be used to denote K as a public signature key and a public ciphering key respectively.

$\lfloor X \rfloor_K$: X is signed with K.

$SV(X,K,Y)$: Given a signed message X, applying K to it verifies that X is the result of signing Y with the corresponding private key of K.

$\langle X \rangle_{*P}$: P does not know or recognize X but P will recognize hXi————————————————P if it will receive the message again.

$X\ from\ P$: X was sent by P.

Inference Rules

SVO logic has the two inference rules: modus ponens and necessitation.

Modus Ponens (MP):

$$\frac{\varphi \quad \varphi \rightarrow \psi}{\psi}$$

Necessitation (NE):

$$\frac{\dashv \varphi}{\dashv P\ believes\ \varphi}$$

φ, ψ and $\dashv$ are metalinguistic symbols. While ψ and $\dashv$ are used to refer to arbitrary formulae,"$\tau \dashv \psi$' means the formula ψ can be derived from the set of formulae τ. Also, $\dashv \psi$means that $\psi$is a theorem.

III. COMPARATIVE ANALYSIS

In computer networks authentication and security is challenging issue and has attracted lots of researchers in recent years. There are protocols to verify the goals and intended objectives of the protocols. In this paper, a summary of three modal logics BAN, GNY and SVO used for the verification of protocols has been presented. The following table (Table 1) summarize the analysis of the modal logics discussed in the previous sections. The table also incorporates the theoretical comparison based on the study of BAN, GNY and SVO.

If you are using *Word*, use either the Microsoft Equation Editor or the *MathType* add-on (http://www.mathtype.com) for equations in your paper (Insert | Object | Create New | Microsoft Equation *or* MathType Equation). "Float over text" should *not* be selected.

Table 1: The comparative analysis of BAN, GYN and SVO

Modal Logic	Complexity	Improvements	Limitations	Uses
BAN	Low	• First formal logic for the verification of protocols	• BAN which assumed that redundancy is always present in encrypted messages • applicability of BAN to a wider range of protocols	• Used to verify a protocol • Usedto derive the beliefs held by protocol principals.
GYN	Moderate	• GNY Recognisability Rule • GNY Message Extension	• Is not capable of detecting the possibility of certain reflection and interleaving attacks on security protocols using a symmetric algorithm.	• Used to capture the recipient's expectation of the contents • Used to derive the beliefs held by protocol principals.
SVO	High	• Assert comprehensions of received messages. • Assert interpretations of comprehended messages.	• Highly complex as it unify its predecessors	• Used to interpret the message exchange in protocols. • Used to derive the beliefs held by protocol principals.

IV. CONCLUSION

There are many other modal logics also used for the verification of the protocols [6] [7]. In this we have presented only the best known and used modal logics. BAN, GNY and SVO has been discussed in this paper briefly. In general we can say that, the basic constructs for logic verification were outlined with foundation of BAN logic. BAN has been extended to produce GNY and SVO. SVO is best in verifying a protocol but is more complex.

The selection of proper modal logic for security protocol verification is the crucial goal in the protocol analysis process. The main contribution of this paper consists in the comparison of various logics, their target area of use and description of specific advantages.

REFERENCES

[1] John T. Kohl, B. Clifford Neuman, and Theodore Y. T'so, The Evolution of the Kerberos Authentication System. In Distributed Open Systems, pages 78-94. IEEE Computer Society Press, 1994.

[2] Tom Yu, Sam Hartman, and Ken Raeburn. The Perils of Unauthenticated Encryption: Kerberos Version 4. In Proceedings of the Network and Distributed System Security Symposium. The Internet Society, February 2004.

[3] B. Clifford Neuman and Theodore Ts'o. Kerberos: An Authentication Service for Computer Networks, IEEE Communications, 32(9):33-38. September 1994.

[4] Abdelmajid, N.T., Hossain M.A., Shepherd, S., Mahmoud, K (2010), "Improved Kerberos Security Protocol Evaluation using Modified BAN Logic", IEEE Computer and Information Technology (CIT).

[5] Bellovin S. M., M. Merritt, "Limitations of the Kerberos Authentication System" Computer Communication Review, 20, pp 119-132, 1991.

[6] Clark John and Jeremy Jacob, "A survey of authentication protocol literature", 1997.

[7] Bhandari R., S. Sharma, and N. Sharma, "Analysis of Windows Authentication Protocols: NTLM and Kerberos," in International Conf. on Computer Networks and Information Technology. Chandigarh, pp. 254-263, 2014.

[8] Neuman C., T. Yu, S. Hartman, K. Raeburn, "The Kerberos Network Authentication System" (RFC4120) July 2005.

[9] Yu Tom, Sam Hartman, and Ken Raeburn, "The Perils of Unauthenticated Encryption: Kerberos Version 4". In Proceedings of the Network and Distributed System Security Symposium. The Internet Society, February 2004.

[10] http://web.mit.edu/kerberos/papers.html

[11] http://kerberos.org/software/tutorial.html.

[12] Abadi, M., Tuttle, N. A Semantic for a Logic of Authentication, In: Proceedings of the ACM Symposium on Principles of Distributed Computing, 2001, pp. 201-216.

[13] Agray, N., van der Hoek, W., de Vink, E.: On BAN Logics for Industrial Security Protocols, In: CCEMAS, p. 8.

[14] Yun-yun Du, Hong-yunNing, Ping Yang, Yan-xia CuiImprovement of Kerberos protocol based on dynamic password and "One-time public key", in 10th International Conference on Natural Computation (ICNC), IEEE,pp. 1020 – 1025, 2014.

[15] Shahabuddin Muhammad. 2007. *Extending Distributed Temporal Protocol Logic to a Proof Based Framework for Authentication Protocols*. Ph.D. Dissertation. University of Central Florida, Orlando, FL, USA. Advisor(s) Ratan K. Guha. AAI3276378.

[16] You, Ilsun, Yoshiaki Hori, and Kouichi Sakurai. "Enhancing svo logic for mobile ipv6 security protocols." *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 2.3 (2011): 26-52.

[17] T. Co_ey, R. Dojen, and T. Flanagan. "Formal verification: an imperative step in thedesign of security protocols." *Computer Networks*, 43:601–618, 2003.

[18] S. Chen, B. Mulgrew, and P. M. Grant, "A clustering technique for digital communications channel equalization using radial basis function networks," *IEEE Trans. on Neural Networks*, vol. 4, pp. 570-578, July 1993.

[19] J. U. Duncombe, "Infrared navigation—Part I: An assessment of feasibility," *IEEE Trans. Electron Devices*, vol. ED-11, pp. 34-39, Jan. 1959.

[20] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and M. Miller, "Rotation, scale, and translation resilient public watermarking for images," *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 767-782, May 2001.

Er. Tanuja Thakur has completed B.Tech in ECE from Himachal Pardesh University in 2012. She is currently pursuing her M.Tech from Sri Sai University, Palampur. Interest of area is authentication protocol and their analysis using modal logics .

Er. Sachin Dogra has completed B.tech and M.tech in Electronics and Communication Engineering from Lovely Professional University, Jallandhar. He is working as Assistant Professor in Sri Sai University, Palampur. His fields of research interest are Wireless Networks and OFDM. He has published papers in the international journals and presented research papers in international and national conferences.

Ms. Yamini Sood has completed B.Tech in Computer Science & Engineering Department from Punjab Technical University, Jalandhar and M.Tech in Computer Science & Engineering Department from Jaypee University, Waknaghat (Solan) She is working as Head Of Department in Sri Sai University, Palampur. Her fields of research interest are Wireless Sensor Network and Multimedia System. She has published papers in the international journals and presented research papers in international and national conferences.