ATTACKS ON SECURITY PROTOCOLS USING AVISPA

Vaishakhi S
M. Tech Computer Engineering
KSV University, Near Kh-5, Sector 15
Gandhinagar, Gujarat
vdsoni586@gmail.com

Prof.Radhika M
Dept of Computer Engineering
KSV University, Near Kh-5, Sector 15
Gandhinagar, Gujarat
radhikamanjusha@gmail.com

Abstract
Now a days, Use of Internet is increased day by day. Both Technical and non technical people use the Internet very frequently but only technical user can understand the aspects working behind Internet. There are different types of protocols working behind various parameters of Internet such as security, accessibility, availability etc. Among all these parameters, Security is the most important for each and every internet user. There are many security protocols are developed in networking and also there are many tools for verifying these types of protocols. All these protocols should be analyzed through the verification tool. AVISPA is a protocol analysis tool for automated validation of Internet security protocol and applications. In this paper, we will discuss about Avispa library which describes the security properties, their classification, the attack found and the actual HLPSL specification of security protocols.

Keywords- HLPSL,OFMC,SATMC,TA4SP,MASQURADE,DOS

I. INTRODUCTION

As the Usage of Internet Increases, its security accessibility and availability must be increased. All users are concerns about their confidentiality and security while sending the data through the Internet. We have many security protocols for improve the security. But Are these protocols are technically verified? Are these protocols are working correctly? For answers of all these questions, there are some verification tools are developed. There are many tools like SPIN, Isabelle, FDR, Scyther, AVISPA for verification and validation of Internet security protocols. Among these, we will use the AVISPA research tool is more easy to use[1].

The AVISPA tool provides the specific language called HLPSL (High Level Protocol Specification Language). Avispa tool has the library which includes different types of security protocols and its specifications. Avispa library contains around 79 security protocols from 33 groups[1]. It constitutes 384 security problems. Various standardization committees like IETF (Internet Engineering Task Force), W3C(World Wide Web Consortium) and IEEE(Institute of Electrical and Electronics Engineers)work on this tool. AVISPA library is the collection of specification of security which is characterized as IETF protocols, NON IETF protocols and E-Business protocols.

Each protocol is describe in Alice-Bob notation. AVISPA library also describes the security properties, their classification and the attack found[2].AVISPA library also provides the short description of the included protocols. AVISPA tool is working using four types of Back Ends:(1)OFMC(On the Fly Model Checker) performs protocol falsification and bounded verification. It implements the symbolic techniques and support the algebraic properties of cryptographic operators.(2)CL-Atse(Constraint logic Based Attack Searcher)applies redundancy elimination techniques. It supports type flaw detection.(3)SATMC(SAT based Attack Searcher)builds proportional formula encoding a bounded unrolling of the transition relation by Intermediate format.(4)TA4SP(Tree Automata Based Protocol Analyser).It approximates the intruder knowledge by regular tree language.TA4SP can show whether a protocol is flawed or whether it is safe for any number of sessions[4]. We found some security attacks while analyzing the security protocols. All security attacks are discussed below:

II. HLPSL Syntax

PROTOCOL Otway_Rees;

Identifiers
A, B, S : User;
Kas,Kbs, Kab: Symmetric_Key;
M,Na,Nb,X : Number;

Knowledge
A : B,S,Kas;
B : S,Kbs;
S : A,B,Kas,Kbs;

Messages
1. A -> B : M,A,B,{Na,M,A,B}Kas
2. B -> S : M,A,B,{Na,M,A,B}Kas,{Nb,M,A,B}Kbs
3. S -> B : M,{Na,Kab}Kas,{Nb,Kab}Kbs
4. B -> A : M,{Na,Kab}Kas
5. A -> B : {X}Kab

Session_instances
[A:a; B:b; S:s; Kas:kas; Kbs:kbs];

Intruder Divert, Impersonate;

Intruder_knowledge a;

Goal secrecy_of X;

A.Basic Roles[2]

It is very easy to translate a protocol into HLPSL if it is written in Alice-Bob notation. A-B notation for particular protocol is as following:

A ->S: {Kab}_Kbs

S ->B:{Kab}_Kbs

In this protocol ,A want to set up a secure session with B by exchanging a new session key with the help of trusted server. Here Kas is the shared key between A and S.A starts by generating a new session key which is intended for B.She encrypts this key with Kas and send it to S.Then S decrypts message ,re encrypts kab with Kbs.After this exchange A and B share the new session key and can use it to communicate with one another.

B.Transitions[2]

The transition part contains set of transitions.Each represents the receipt of message and the sending of a reply message.The example of simple transition is as follows:

Step 1: State = 0 /\ RCV({Kab'}_Kas) =|>
State':=2/\SND({kab'}_Kbs)

Here, Step 1 is the name of the transition. This step 1 specifies that if the value of state is equal to zero and a message is received on channel RCV which contain some value Kab' encrypted with Kas, then a transition files which sets the new value of state to 2 and sends the same value kab' on channel SND, but this time encrypted with Kbs.

C.Composed Roles[2]

Role session(A,B,S : agent,
Kas, Kbs : symmetric key) def=
Local SA, RA, SB,RB,SS,RS :channel (dy)
Composition
Alice (A,B,S, Kas, SA,RA)
/\bob (B, A, S, Kbs, SB, RB)
/\server (S, A, B, Kas, Kbs, SS, RS)
end role

Composed roles contains one or more basic roles and executes together in parallel. It has no transition section. The /\ operator indicates that the roles should execute in parallel[4]. Here the type declaration channel (dy)stands for the Dolev-Yao intruder model[2]. The intruder has full control over the network, such that all messages sent by agents will go to the intruder. All the agents can send and receive on whichever channel they want; the intended connection between certain channel variables is irrelevant because the intruder is the network.

We create the HLPSL code of security protocol using above syntax and verify those through the AVISPA tool [2]. Here we found some protocols with attack and some protocols without attacks. All the verified security protocol list are as below (figure 1):

III. Security Attacks

As we show in the table that Internet security protocols may suffer from several types of attacks like flaw, replay, Man in the middle, masquerade, DOS etc. In Dos attack ,the attacker may target your computer and its network connection and the sites you are trying to use, an attacker may able to prevent you for accessing email, online accounts, websites etc[6].A flaw attack is an attack where a principal accepts a message component of one type as a message of another[7]. A replay attack occurs when an attacker copies a stream of messages between two parties and replays the stream to one or more of the parties.

Masqurade is the type of attack where the attackers pretends to be an authorized user of a system in order to gain access the private information of the system. Man in the middle is the attack where a user gets between the sender and receiver of information and sniffs any information being sent[6]. Man in the middle attack is sometimes known as Brigade attacks. Evasdropping attack is the act of secretly listening to the private conversation of others without their concent. It is a network layer attack. The attack could be done using tools called network sniffers [7]. These types of attacks can be removed by making some changes in the sessions and transactions.

IV.CONCLUSION

Here we have studied about the protocols using the AVISPA verification tool and we found different types of attacks on different Internet security protocols. All different types of goals are specified for different protocols.The attacks are interrupting to achieve their goals.We have to remove those attacks to make the protocols working properly.

PROTOCOL NAME	ATTACK	PROTOCOL NAME	ATTACK	PROTOCOL NAME	ATTACK
AAAMobileIP	Flaw	EAP_Archie		RADIOUS-RFC-2865	
CTP		EAP_IKEV2		8021x-Radious	
SIP		EAP_SIM		HIP	
H.530	Replay	EAP-TLS		PBK-FIX	REPLAY
H.530-FIX		EAP_TTLS_CHAP		PBK-FIX-With Auth	
NSIS QoS Authorization		PEAP		Kerb basic	
Geopriv		SKEY		Kerb-Ticket-Cache	
Geopriv with two self Signatures	DOS	EKE	Man in the middle	Kerb-croos-Realm	
Geopriv-two psudonems		Lipkey SPKM Unknown Initiator		Kerb-Forwardable	
Geopriv-pervasive		IKEv2-DS		Kerb-preauth	
Geopriv password		IKEv2-DSx		Kerb-PKINIT	
Simple		IKEV2-MAC	Man in the middle	TESLA	
Lipkey SPKM known Initiator		IKEV2-MACx		SSH-Transport	
APOP		EKE2		TSP	
CRAM-MD5		SPEKE		EAP	
DHCP-Delayed-Auth		SRP		CHAPV2	
TSIG		IKEV2-CHILD		UMTS-AKA	
TLS		IKEV2-EAP-Archie		ISO1	REPLAY
ISO2		ISO3	Evasdropping and Replaying	ISO4	
2pRSA		LPD-MSR	Masqurade	SHARE	Man in the middle
NSPK	Man in the Middle	NSPK-FIX		NSPK-KS	Man in the Middle
NSPK-KS-FIX		NSPK-XOR		LPD-IMSR	

Figure 1: Attacks on security protocols

V.FUTURE WORK

In this paper we have defined the AVISPA library for Internet security protocols and survey the protocols and categorized the protocol with attacks and protocols without attacks. In the next stage we will apply some modifications in HLPSL language code on the security protocol which have the man in the middle attack using the techniques and we will try our best to remove the particular attack.

VI.REFERENCES

[1] Information Society Technologies, Automated Validation of Internet Security Protocols and Applications (version 1.1) user manual by the AVISPA team,IST-2001-39252
[2] Information Society Technologies, High Level Protocol Specification language Tutorial, A beginners Guide to Modelling and Analyzing Internet Security Protocols,IST-2001-39252
[3] Laura Takkinen,Helsinki University of Technology,TKKT-110.7290 Research Seminar on Network security
[4] Daojing He,Chun Chen,Maode Ma,Sammy chan,International Journal of Communication Systems DOI:10.1002/Dac.1355
[5] Luca Vigano,Information Security Group,Electronic Theoretical Computer Science 155(2006)61-86
[6] U.Oktay and O.K.Sahingoz,6th International Information security and cryptology conference,Turkey
[7] James Heather,Gavin Lowe,Steve Schneider,Programming Research group Oxford University