Analysis of E-commerce Security using AVISPA

Daassa Asma†, Machhout Mohsen††, and Aguili Taoufik†††

† Electronics and Microelectronics Laboratory, Faculty of Sciences Monastir National Engineering School of Tunis, University of Tunis El Manar Tunis, Tunisia
†† Electronics and Microelectronics Laboratory Faculty of Sciences University of Monastir Monastir, Tunisia
††† SYSCOM Laboratory Department of Information and Communications Technology National Engineering School of Tunis, Tunis, Tunisia

Summary
E-commerce security is very necessary especially nowadays, as critical attacks are being detected in a still growing number. Therefore, it is very important to enhance the security of electronic transactions, to encourage customers providing goods and purchasing items. Normal communication protocols require less rigorous and detailed verification than security protocols before their deployment.
There are many protocols originally designed for secure e-commerce transactions, these protocols are now used much more widely. That's why an attack could be catastrophic as it may cause distrust and loss of communication.
There are many formal methods for testing the security of e-business protocols to detect if it is safe or not, such as AVISPA, ProVerif , Casper etc.

This research includes a comparison between protocols used for securing e-commerce transactions that has been made, the verification of security properties of electronic transaction protocol using AVISPA tool has been presented, and finally open research problems has been highlighted, there will also be a description on how SPAN (an animation tool for AVISPA) can be used to interactively find and build attacks.

Key words:
SSL/TLS, SET, security, e-commerce, attacks, AVISPA, mutation

1. Introduction

With the expansion of data transmissions and the development of communication networks, the need to ensure the confidentiality and authenticity of the messages exchanged becomes especially important especially nowadays with the appearance of covid-19. It is also more secure to use electronic transactions to avoid touching money.
Cryptographic protocols are now used to protect banking data or critical information exchanged during electronic transactions.
In such situations, there is a real need for verification of cryptographic protocols, before the protocol is published or completed,
if possible. However, verifying the security protocol model does not guarantee that the actual implementation of the protocol is really secure.
In this paper, there will be focus on current formal specifications and verification tools that can reveal vulnerabilities, which would be difficult to fix at the implementation level, on an early basis. However, the huge gap between the specification method used in the academic world and the industrial world makes this task exceedingly difficult.
Formal methods for verifying cryptographic protocols have been appearing for the past decade, which resulted in the appearance of a number of verification tools, such as AVISPA, ProVerif ..., however, these tools use a formal specification language (HLPSL for example is a particular case of AVISPA).
Many protocols are developed to ensure the security of electronic transactions such as TLS, SET, and 3D secure. The credibility of the proposed protocols is studied to secure against renegotiation attack and replay attack. The proof is performed using AVISPA with HLPSL.
In this work, we adopt the concept of the mutation technique to avoid vulnerabilities in the entire security system of e-commerce transactions and explain how SPAN (an animation tool for AVISPA) can be used to interactively find and build attacks.

Contributions

(i) We try to test the existence of attacks using the verification tool AVISPA after applying mutation techniques. If attacks cannot be obtained by AVISPA, we show how we use SPAN intruder mode to find and also construct them by hand.
(ii) We save attack traces generated by AVISPA, we intend to replay them on corrected versions of protocols to guarantee its robustness.
(iii) We present SSL/TLS protocol and SET protocol as the most used protocol in securing e-commerce transactions, and we apply mutation on these protocols.

Manuscript received December 5, 2020.
Manuscript revised December 20, 2020.
https://doi.org/10.22937/IJCSNS.2020.20.12.2

(iv) We present result of studies verifying 3D secure using automated tools.

Paper organization

The rest of the paper is organized as follows: Section 2 reviews related work, section 3 discusses the validation of security protocols using AVISPA tool, section 4 introduces AVISPA tool, security properties and verification assumptions, and section 5 presents formal analysis of e-commerce security protocol, such as SSL/TLS and SET, for attack detection . Finally, section 7 concludes the paper explaining the future work that could be accomplished based on the contributions of the paper.

2. RELATED WORK

It is necessary to think seriously about the protection of data security in e-commerce transaction. There are three protocols used for securing e-commerce transaction: Secure Socket Layer (SSL), Secure Electronic Transaction (SET), and 3D Secure.

This paper focuses on the comparison and analysis of e-commerce security protocols using AVISPA tool [9]. Many discussions on formal verification of security protocol focus on method to improve e-commerce security properties such as Confidentiality, Integrity and Authentication. Including these properties, e-commerce needs more security properties. These properties are :

- Access Control.
- Privacy/Confidentiality.
- Authentication.
- Non Repudiation.
- Integrity.
- Availability

But tools such as Proverif [2], Scyther [4] and AVISPA [3] [10] [11] are limited to only two security properties (the authentication goal and the secrecy goal). Verifying payment properties such as non-replay, non-repudiation, is still an open issue.

In our previous work [5], we tried to compare the efficiency of the four back-end of AVISPA with modifying SSL/TLS specification, and using these back-ends, we tried to detect this modification. We found that SATMC and TA4SP were useless and OFMC and CLAtSe found attacks and provided traces. That is why, we employ in this work just the two back-ends OFMC and CLAtSe.

Verifying the specification of such security protocol does not guarantee that this protocol is secure in the implementation level.

Some works [3] [6] [12] introduce another approach called the mutation technique, this approach consists in making faults in the model of such protocol that can appear in the implementation level, these mutations simulate errors caused by programmers.

Therefore, mutation testing is very useful to prevent and also detect logical attacks.

3. AVISPA TOOL AND SECURITY PROPERTIES VERIFICATION

3.1 AVISPA tool

In this section, we try to briefly introduce this tool. In July 2005, the partners of the European project AVISPA [9] published

their work on the development of a platform containing four analysis of back-ends allowing the detection of logical attacks on security protocols.

This platform also suggests improvements ensuring the validity of the confidentiality and authentication properties.

Verification techniques used by AVISPA are techniques based on the principle of Model-checking. Therefore, AVISPA provides the specific language called HLPSL [8] (the High-Level Protocol Specification Language) used for protocol specification. It works using four back-ends (On-the-fly Model-Checker OFMC, CL-based Attack Searcher CL-AtSe, SAT-based Model-Checker SATMC, and Tree-Automata-based Protocol Analyzer TA4SP).

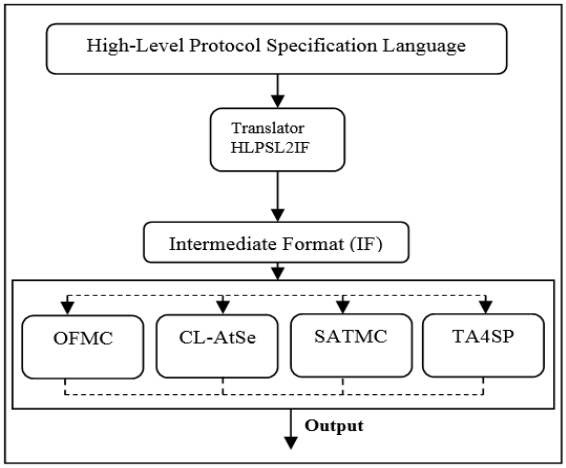
We choose to use AVISPA tool especially for verifying security properties of the most used protocol for securing both e-commerce and m-commerce transactions.

3.2 SPAN: An Animation tool for AVISPA

SPAN is a security protocol animator for HLPSL and CAS+ specifications.

SPAN has many features. First, we can debug HLPSL formal specifications of protocols. Second, we can interactively buid a Message Sequence Chart (MSC) of the protocol execution from HLPSL specifications and automatically build attacks MSC on HLPSL specifications, then we can also interactively build specific attacks on specifications using the intruder mode.

Fig 1: AVISPA Tool: Architecture



3.3 Verification steps

In our work we used the AVISPA tool on ubuntu10, after the protocol specification in HLPSL, (1) access the AVISPA tool and load a file with .hlpsl extension containing the specification in HLPSL, (2) automatically transform this file into a protocol description in IF (Intermediate Format). (3) This file which is in intermediate format will be automatically sent as an input to the four back-ends which will verify the protocol and present their diagnostics. (4) These diagnostics provide, if necessary, an attack trace that can be viewed graphically

3.4 Security properties verification

Analyzing Security Properties

Security properties like authentication and secrecy are provided by the protocol using the keywords ((secret, witness, request, and wrequest) in the state transition.

```
%goal
%
% secrecy_of sec_clientk,sec_serverk
% %Alice authenticates Bob on na_nb1
% authentication_on na_nb1
% %Bob authenticates Alice on na_nb2
% authentication_on na_nb2
%
%end goal
```

In the section goal, we define security properties, the protocol goal is mutual authentication and to establish a secret key between the client and server; the intruder cannot achieve valid authentication since he could not know the secret session key, client and server.

- Authentication
  Authentication gives the possibility to both participants to know each other and guarantee that they are communicating with the required party. Using AVISPA tool, to specify the authentication goal, we exploit, witness and request command.
- Secrecy

This property guarantees that the information is not made available to unauthorized users In addition, to specify the secrecy goal, we make use of the secret command.

Formal model

The formal model of the protocol is described using HLPSL language

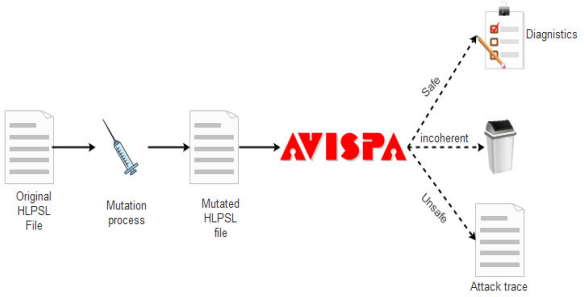
Mutation techniques

In our work, we have used mutation process; it consists of introducing logical faults into the HLPSL model in order to create vulnerabilities. To do this we use an existing mutant generator named jMuHLPSL. [3]

Attack trace

After applying mutation techniques on e-commerce security protocols, we use model-checking tools to verify the protocol. If the mutant is declared unsafe, an abstract attack trace will be generated

Fig 2: Applying the mutation process and AVISPA analysis



4. ANALYSIS OF E-COMMERCE SECURITY PROTOCOLS USING AVISPA

In this work, our purpose is to find attacks on vulnerable versions of protocols. To do this, we apply mutation techniques to generate attack traces, describing an attack scenario against security property.

We also use intruder simulation which gives us the possibility to construct an attack by hand, if the verification tool cannot obtain this particular attack or stick to another one.

Therefore, we save these attack traces. We aim to replay them on corrected versions of protocols, to prove its robustness.

4.1 SSL/TLS Protocol

SSL/TLS protocol Description

SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security) are the most popular deployed protocol; they are now implemented in all web browsers. In fact, they are the security protocol behind HTTP (HTTPS) and they are able to secure any protocol working over TCP. TLS is a cryptographic protocol that ensure confidentiality by encrypting the data between a web server and a browser, and provide authentication. In SSL handshake, the two communicating parties authenticate themselves and negotiate an encryption key.

In literature a large number of papers study security protocols using formal security analysis tools.

These tools become very useful especially for the analysis of TLS 1.3 versions [23] [24] [25].

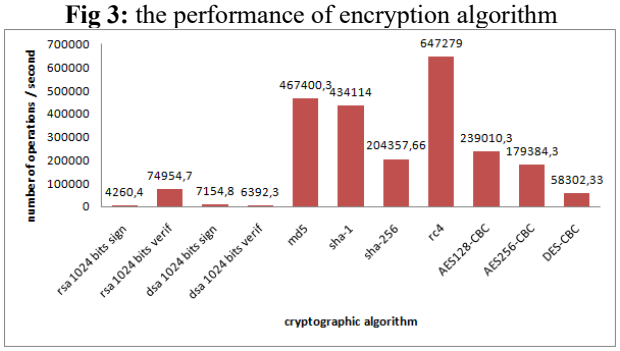
We have found several papers analyze SSL/TLS versions using automated verification tools. [25] [26] [27] [28]
Cremers et al analyse [23] TLS 1.3 draft-10 using the Tamarin prover, a tool for the automated analysis of security protocols.
Although, TLS 1.0 (RFC2246) is coming under pressure from attacks, is still widely supported especially for securing e-commerce transactions.

From SSL Pulse [1], in September 2020, TLS v1.0 is still widely supported. In fact, 52.5% of sites surveyed support the TLS v1.0 protocol. In this paper we analyze TLS1.0 using AVISPA and mutations techniques to generate attack traces. These attack traces represent attacks at a formal level.

Performance test of cryptographic algorithm
In order to expand our knowledge on the subject and suggest improvements and contributions, we conducted our research with the development of an exploratory prototype.
In fact (For instance), in our experiments we used the Linux virtual machine with Intel (R) core (TM) i5-3230M CPU 2.60 GHZ. The operating system used is Fedora 21, and we started our experiments by installing an implementation of SSL / TLS: OpenSSL 1.0.1k.
Our first experiment consists in using the ”speed” command provided by openSSL in order to test the performance of cryptographic algorithms.

Through the first experiment to measure the performance of encryption algorithm, we created this curve.

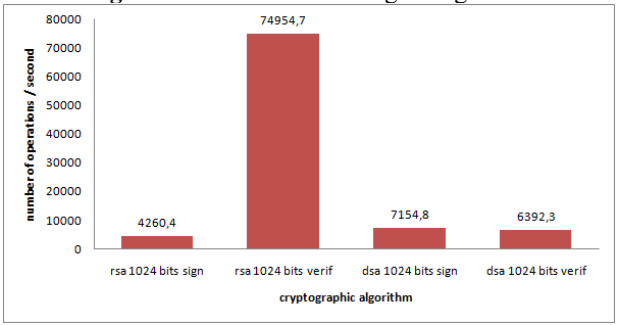
Fig 3: the performance of encryption algorithm



We found that the hash algorithms are the fastest, then we found symmetric encryption (AES, DES, etc.) because of a single small key (128,256 bits), and finally we found asymmetric encryption (RSA, etc.).
That is because of the presence of two keys (public + private + certificate) with larger sizes (1024,2048,4096 bits).

Performance test of digital signature

Fig 4. Performance test of digital signature



We noticed a big difference between generation and verification of digital signature using RSA unlike DSA. Therefore, it is not recommended to use RSA as a key exchange algorithm.

Implementation and Verification Results
The implementation involves modeling of the protocol using HLPSL. The verification results are given below after applying the hash mutation

Fig. 5. Output of TLS protocol specification verified in AVISPA using CL-AtSe back-end after applying Hash Functions Mutation.

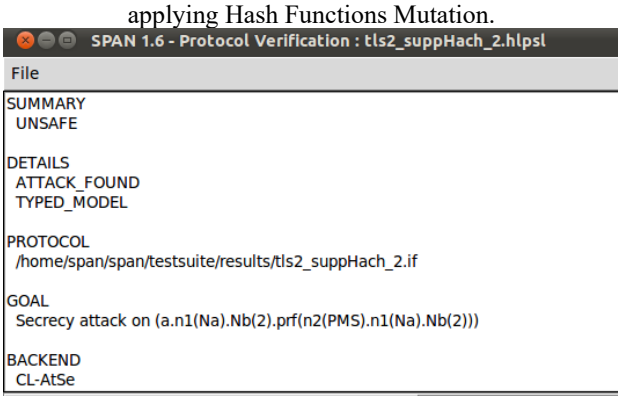


Fig. 6. Attack trace

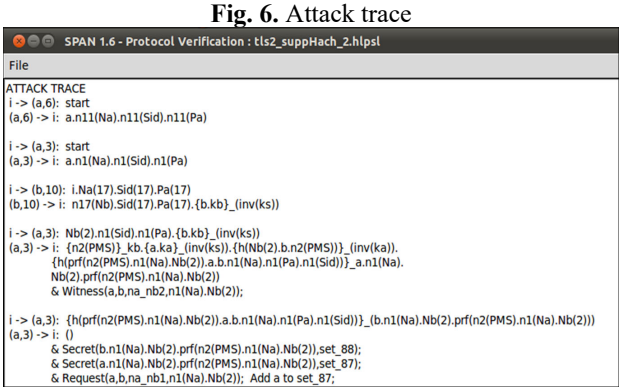
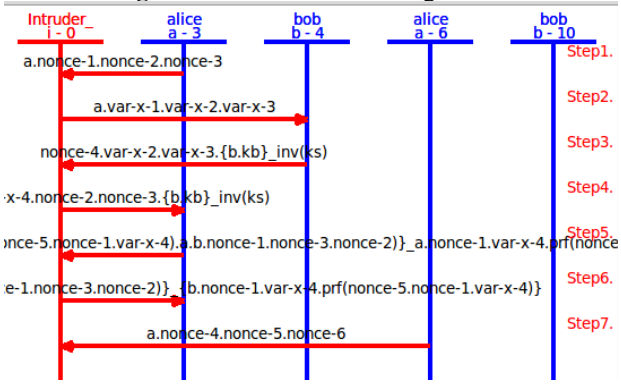


Fig. 7. Attack simulation using SPAN

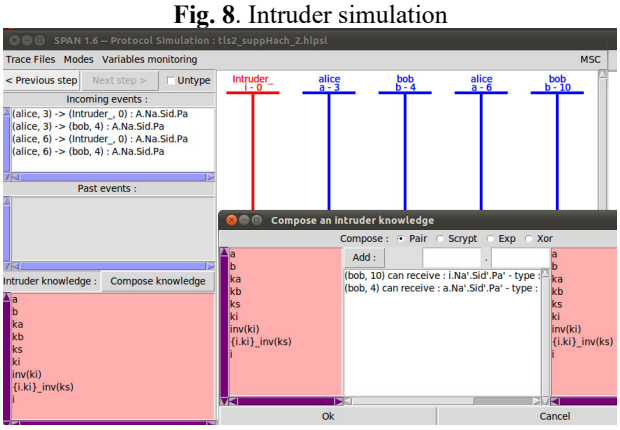


The attack trace describes a man-in-the-middle attack.
In fact, In the attack trace i stands for intruder and a and b stands for Alice and bob agents. The number in notation (a,3) is a session number.
We observe that the intruder captures a secret from Alice but he uses it to forward a message to bob.
As we said previously, there are many advantages using automated verification tools. In our case, we try to find known vulnerabilities.

It seems unnecessary at first: if vulnerabilities are known, why wasting time to find them automatically? However, we see two good reasons for doing this: to increase confidence in the tool, to avoid the reappearance of old vulnerabilities.

We notice that it is possible to save attack traces and try to play them later on corrected versions of the protocols.
AVISPA offers an intruder simulation that allows to add the intruder in possible transitions.
At any time, the attacker can capture a message or forge any message from his initial knowledge and what he has captured.
To do this the tool offers an interface to construct messages.

Fig. 8. Intruder simulation



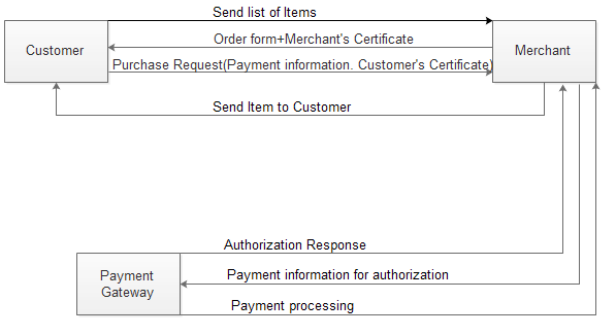
4.2 Secure Electronic Transaction (SET) Protocol

SET protocol Description

There are essential requirements for SET protocol, first it provide confidentiality of order and payment information. Second, it ensures the integrity of payment instructions and all transmitted data. Finally, it authenticates both the cardholder and the merchant. Cardholder and merchants must register with certificate authority before making transactions.

The payment process is simplified in this figure.

Fig. 9. Working of SET Protocol [13]



Implementation and Verification Results

The implementation involves modeling of the protocol using HLPSL. The verification results are given below after applying the Public key mutation.

Fig. 10. CL-AtSe analysis log after applying public key Mutation on SET PROTOCOL

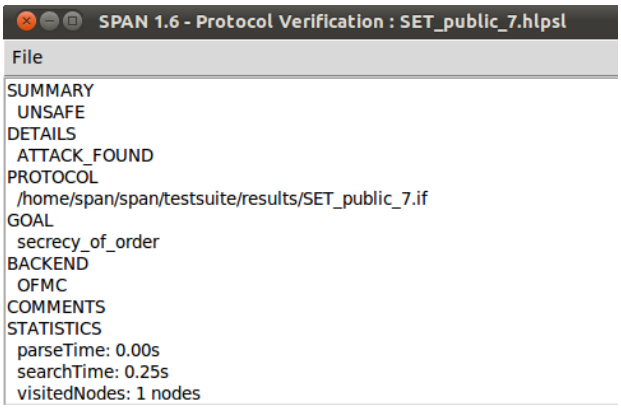
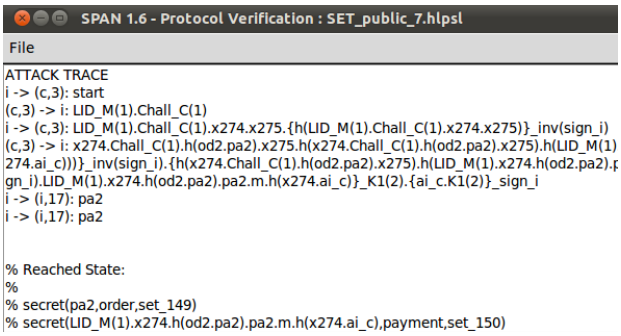


Fig. 11. Attack trace



4.1 3D secure

TLS and SET protocols suffer from many problems. In fact, one problem of TLS protocol is that merchants do not authenticate the cardholder.

Using SET protocol, consumers must store certificates on their PC. In addition, the use of this Protocol requires an advanced certification infrastructure. This is complex and very difficult to be used in practice. The 3D secure comes to reduce the complexity of SET implementation at end-users.

Technically, the term 3D Secure refers to 3 Domain Server. Acquirer Domain, Issuer Domain (such as Visa or MasterCard), Interoperability Domain (such as payment system).

Dalal et al [19] analyze 3D secure using Proverif and Scyther to evaluate the two verification tools. Pasupathinathan et al [20] analyze 3D secure using Casper .

The table below summarize their results.

TABLE I: RESULTS OF ANALYSING 3D SECURE PROTOCOL

	Casper	Scyther	Proverif
Customer side	SAFE	SAFE	SAFE
Merchant side	UNSAFE	SAFE	SAFE
Bank side	SAFE	UNSAFE	SAFE

Using Casper/FDR, we observe an attack from the merchant side.

Using Scyther, we notice that the tool detects an attack from the bank side, and it is safe from customer side and merchant side.

Using proVerif, we observe that the protocol is safe.

5. ANALYSIS OF RESULTS

After applying the mutation on the protocols, AVISPA tool is used to verify secrecy and authentication properties. For our verification, we use OFMC and CL-ATSE back-ends to detect attacks on the protocol under test. As a result, it gives us whether the protocol is safe or not. If the result is safe then it means that the mutation applied did not present any attack. However, if the result is unsafe, it means that the mutation applied presents an attack; therefore, it produces the trace of the attack found.

SET and SSL/TLS are the most used protocols to secure e-commerce transactions. In this section, we apply mutations on these protocols, and we present the experimental results that we have obtained

TABLE II: RESULTS OF APPLYING MUTATIONS ON SSL/TLS PROTOCOL

Mutations	CL-AtSe	OFMC
Homomorphism	SAFE	SAFE
Permutation	SAFE	SAFE
Public Key	SAFE	SAFE
Substitution	SAFE	SAFE
Hash Functions	UNSAFE	UNSAFE

TABLE III: RESULTS OF APPLYING MUTATIONS ON SET PROTOCOL

Mutations	CL-AtSe	OFMC
Homomorphism	UNSAFE	UNSAFE
Permutation	UNSAFE	UNSAFE
Public Key	UNSAFE	UNSAFE
Substitution	UNSAFE	UNSAFE
Hash Functions	-	-

6. DISCUSSION

Considering the security protocols, which are already verified using AVISPA, we conclude that SSL/TLS is safer than SET protocol after applying mutations to introduce leaks in it.

We analyze the mutated models using AVISPA tool. If the mutant is declared safe, therefore, it indicates that authentication and secrecy properties are fulfilled. In addition, if it is declared unsafe AVISPA generates counterexample traces exploiting the security flaws.

OFMC and CL-AtSe are the attack searchers; they indicate that the mutated model of SSL/TLS protocol is SAFE, giving us no information about the attack. However, the mutated model of SET protocol is declared UNSAFE. The integrity property is guaranteed by including the hash function in modeling.

The mutation hash function consists of the removal of hash function in the HLPSL specification of the protocol. The mutated model of SSL/TLS protocol is declared unsafe after applying this mutation, and an attack trace is generated.

7. Conclusion

This paper is an opening out of the conference paper in [29] ,we used the model checking AVISPA to analyze payment protocols such as SSL/TLS, SET, to check for security properties against vulnerabilities, such as renegotiation and replay attacks.

In our paper, we addressed the problem of checking e-commerce protocols using AVISPA tools. This verification is important to ensure the confidentiality and authentication properties for securing e-commerce transactions; but this will not confirm that these protocols are totally secure because of the existence of particular properties which are difficult to verify automatically such as non-Repudiation, Availability...

Our future work is concerned with extending our analysis to other e-commerce protocols like 3D secure using AVISPA tool.

We will replay attack traces on corrected versions of TLS protocol, to prove that a protocol is correct in a formal model.

We notice that we found several documented attacks over SSL/TLS protocol, but these attacks are performed over real implementations of the protocol, not over its specification.

References

[1] https://www.ssllabs.com/ssl-pulse/

[2] Blanchet, B. (2009). Automatic verification of correspondences for security protocols. Journal of Computer Security, 17(4), 363-434.

[3] Dadeau, F., H´eam, P. C., & Kheddam, R. (2011, March). Mutation-based test generation from security protocols in HLPSL. In Software Testing, Verification and Validation (ICST), 2011 IEEE Fourth International Conference on (pp. 240-248). IEEE.

[4] The Scyther Tool : Verification, falsification, and analysis of security protocols

[5] Asma, Daassa, Machhout Mohsen, and Aguili Taoufik. ”TLS PROTOCOL VERIFICATION FOR SECURING E-COMMERCE WEBSITES.” Journal of Internet Banking and Commerce 22.2 (2017).

[6] Maatoug, Ghazi, Frédéric Dadeau, and Michael Rusinowitch. ”Model-based vulnerability testing of payment protocol implementations.” HotSpot’14-2nd Workshop on Hot Issues in Security Principles and Trust, affiliated with ETAPS. 2014.

[7] Dolev, Danny, and Andrew Yao. ”On the security of public key protocols.” IEEE Transactions on information theory 29.2 (1983): 198-208.

[8] [AVISPA Team. ”HLPSL tutorial the Beginner’s guide to modelling and analysing internet security protocols.” 2013-01-20]. http://www. avispa-project. org (2006).

[9] Team, T. A. ”AVISPA v1. 1 User manual.” Information Society Technologies Programme (June 2006), http://avispa-project. org (2006).

[10] Vishesh, Kinchit, and Amandeep Verma. ”Formal verification of authenticated AODV protocol using AVISPA.” International Journal of Computer Applications 50.19 (2012).

[11] Kasraoui, Mohamed, Adnane Cabani, and Houcine Chafouk. ”Formal verification of wireless sensor key exchange protocol using AVISPA.” Computer, consumer

and control (IS3C), 2014 international symposium on. IEEE, 2014.

[12] B¨uchler, Matthias, Johan Oudinet, and Alexander Pretschner. ”Security mutants for property-based testing.” International Conference on Tests and Proofs. Springer, Berlin, Heidelberg, 2011

[13] Parihar, Pankaj Singh, Vikas Kurdia Pankaj Suwalka, and Ratnesh Parasher Deepali Mahatma. ”An Implementation of Set Protocol with DES Algorithm.”

[14] Shinde, Amol H., and A. J. Umbarkar. ”Analysis of Cryptographic Protocols AKI, ARPKI and OPT using ProVerif and AVISPA.” International Journal of Computer Network and Information Security 8.3 (2016): 34.

[15] Yang, Huihui, Vladimir A. Oleshchuk, and Andreas Prinz. ”Verifying Group Authentication Protocols by Scyther.” JoWUA 7.2 (2016): 3-19.

[16] Kurkowski, Mirosław, Adam Kozakiewicz, and Olga Siedlecka-Lamch. ”Some Remarks on Security Protocols Verification Tools.” Information Systems Architecture and Technology: Proceedings of 37th International Conference on Information Systems Architecture and Technology–ISAT 2016–Part II. Springer, Cham, 2017.

[17] Henzl, Martin, and Petr Hanacek. ”A Security Formal Verification Method for Protocols Using Cryptographic Contactless Smart Cards.” Radioengineering 25.1 (2016): 132-139.

[18] Islam, Salekul. ”Security analysis of LMAP using AVISPA.” International journal of security and networks 9.1 (2014): 30-39.

[19] Dalal, Nitish, et al. ”A comparative analysis of tools for verification of security protocols.” International Journal of Communications, Network and System Sciences 3.10 (2010): 779.

[20] Pasupathinathan, Vijayakrishnan, et al. ”Formal analysis of card-based payment systems in mobile devices.” Proceedings of the 2006 Australasian workshops on Grid computing and e-research-Volume 54. Australian Computer Society, Inc., 2006.

[21] Tobarra, M. L., Cazorla, D., Pardo, J. J., & Cuartero, F. (2008). Formal Verification of the Secure Sockets Layer Protocol. In ICEIS (3-2) (pp. 246-252).

[22] Tobarra, M. L., Cazorla, D., Pardo, J. J., & Cuartero, F. (2008). Formal Verification of the Secure Sockets Layer Protocol. In ICEIS (3-2) (pp. 246-252).

[23] Cremers, C., Horvat, M., Scott, S., & van der Merwe, T. (2016, May). Automated analysis and verification of TLS 1.3: 0-RTT, resumption and delayed authentication. In 2016 IEEE Symposium on Security and Privacy (SP) (pp. 470-485). IEEE.

[24] Cremers, Cas, et al. A comprehensive symbolic analysis of TLS 1.3.” Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2017.

[25] Bhargavan, Karthikeyan, Bruno Blanchet, and Nadim Kobeissi. Verified models and reference implementations for the TLS 1.3 standard candidate.2017 IEEE Symposium on Security and Privacy . IEEE, 2017.

[26] Paulson, Lawrence C. ”Inductive analysis of the Internet protocol TLS.” ACM Transactions on Information and System Security (TISSEC) 2.3 (1999): 332-351.

[27] Vigan`o, Luca. ”Automated security protocol analysis with the AVISPA tool.” Electronic Notes in Theoretical Computer Science 155 (2006): 61-86.

[28] Blanchet, Bruno. ”Modeling and verifying security protocols with the applied pi calculus and ProVerif.” Foundations and Trends® in Privacy and Security 1.1-2 (2016): 1-135.

[29] Asma, Daassa, Machhout Mohsen, and Aguili Taoufik. ” E-commerce issues and verifying security protocols using AVISPA.” The 5th International Conference on Automation,Control Engineering and Computer Science (ACECS-2018).