E-commerce issues and verifying security protocols using AVISPA

1st DAASSA Asma
Electronics and Microelectronics Laboratory
Faculty of Sciences Monastir
National Engineering School of Tunis,
University of Tunis El Manar
Tunis, Tunisia
asma.daassa@gmail.com

2nd MACHHOUT Mohsen
Electronics and Microelectronics
Laboratory Faculty of Sciences
University of Monastir
Monastir, Tunisia
machhout@yahoo.fr

3rd AGUILI Taoufik
SYSCOM Laboratory
Department of Information
and Communications Technology
National Engineering School of Tunis
Tunis, Tunisia

***Abstract*—Nowadays, customers are still hesitant to make purchases online, because e-commerce suffer from many security issues. Therefore, hackers can have access to sensitive information by exploiting errors in security protocols.**
Detecting vulnerabilities in e-commerce security protocol remains difficult, because we need to study in depth the protocol and acquire a deep knowledge of it. That is why we will focus on verifying and validating such security protocol especially e-Business Protocols like TLS, SET . . .
This paper presents e-commerce security issues and the verification of security properties of electronic transaction protocol using AVISPA tool, and finally it highlights several open research problems.

***Index Terms*—SSL/TLS, SET, security, e-commerce, attacks, AVISPA, mutation testing**

I. Introduction

The security of e-commerce is necessary due to critical data exchanged during an electronic transaction like bank account management, personal information (credit card number, password...). Therefore, it is very indispensable to protect these assets from unauthorized access, use, alteration, or destruction. In order to ensure the integrity, confidentiality, non-repudiation, authenticity, privacy and availability of these electronic transactions, many security protocols have been developed like SSL/TLS and SET. On the one hand, these protocols need more rigorous and detailed verification than normal communication protocols before their deployment.

On the other hand, ensuring its rigorous analysis and validation is still an open issue. As a result, flaws and attacks are still growing giving the possibilities to hackers to exploit them to access critical data and information.

In order to avoid these attacks, many prevention techniques are being used. Among these techniques, we have the validation and verification of security protocols, which is based upon the abstract formal methods giving analytical rules to indicate if such protocol is secure, or not.

If non-mathematicians use the formal techniques, they will find technical difficulties, that's why they choose to use online validation tools like AVISPA, HERMES which are easy to use and produce outputs assuring if a given cryptographic protocol is secure or not.

This paper investigates the concept of the mutation technique to avoid vulnerabilities in the entire security system of e-commerce transactions.

Contributions

The contributions of this paper can be summarized as follows:

- We present e-commerce and m-commerce security issues.
- As prevention techniques, we focus on the validation and verification of security protocols using automated tools like AVISPA
- In our case, we aim to test the existence of some attacks in SSL/TLS protocol such as the renegotiation vulnerability, replay attack, triple handshake.
- We discuss countermeasures and we highlight open problems.

Paper organization

The remainder of the paper is organized as follows. Section 2 reviews related work, section 3 presents e-commerce and m-commerce security issues, section 4 discusses the validation of security protocols using AVISPA tool, security properties and verification assumptions, and finally, we conclude the paper in section 5.

II. Related Work

Nowadays e-commerce becomes very important for the commercial world. It holds many advantages such as efficiency and convenience. Unfortunately, it has many disadvantages due to the openness of the internet world, especially the security issue of electronic transactions. That is why many articles study in depth the topic of e-commerce security. Thus, it is crucial to improve the security of electronic transactions and to deny the attacker to access highly important information including credit card numbers, personal details etc. Prior work looked at security protocols from the perspective of automated verification using tools such as Proverif [1] [17], Scyther [3] [18], AVISPA [2] [14] [15] [19] [20] [21]. In our previous work [4], we modified the HLPSL model and through AVISPA, we analyzed TLS handshake and we tried to compare results of four back-ends, we noticed from these results that SATMC and TA4SP were useless and OFMC and CLAtSe

ISSN 1737-930X

found attacks and also provided traces. We focused also on the verification of SSL/TLS protocol using the AVISPA tool for automated verification and analyzing security properties. In fact, dedicated modeling and verifying security protocol languages such as HLPSL (High-Level Protocol Specification Language) give researchers the opportunity to verify many security properties such as data secrecy and authentication. However, verifying security protocols is not enough to guarantee the existence of these security properties in the actual implementation of the protocol. That is why few studies [2] [5] [16] introduced a technique that appeared recently called mutation testing.However, the major causes of attacks are the misusing of cryptographic libraries, misunderstanding and misinterpreting of parameters, configurations and options. Therefore, if developers use these libraries incorrectly, they will make many mistakes in their individual applications causing many vulnerabilities and attacks. Mutation testing is very useful. In fact, it consists on injecting faults into models that aim at introducing leaks in the security protocols. These mutations can simulate errors caused by programmers. Then, by using AVISPA tool, we manage to analyze the mutant model to produce an attack trace or a counterexample violating a security property. This technique is useful to detect and prevent logical attacks.

III. E-COMMERCE AND M-COMMERCE ISSUES

It is very important to identify e-commerce security issues, and to analyze different attacks and vulnerabilities within security protocols, to enhance the security of transactions and customers information. Both m-commerce and e-commerce are based on the same fundamental principles, and aim at making transactions on the internet using computers or laptops for the sake of the web world and using mobile devices for the sake of the mobile world. It has been noticed from a statistical survey research that it is necessary to analyze the security of mobile transactions as well as web transactions. The security of m-commerce is very important nowadays due to the big number of Smartphone users and several research studies noted that e-commerce sales via mobile is still increasing. Over time, it can be assumed that sales done through mobile devices are rapidly growing due to its features compared to e-commerce, such as mobility convenience, connectivity (3G, 4G, and WI-FI), and interactivity. [6] [7] However, m-commerce security is a serious problem and it is a challenge because the service durability is limited to features such as memory, battery storage . . . Therefore, to encourage customers making the purchase of goods and items, we have to improve the security of electronic transactions. That is why researchers study in depth different attacks and propose solutions to these problems. The security of m-commerce is very important especially nowadays over untrusted media (internet).To improve the security of electronic transactions, many protocols are developed. SSL/TLS is the most commonly used, though many dangerous attacks are still found. Many studies confirm that SSL implementations in android applications are actually more prone to vulnerabilities than browsers. Therefore, developers have to ameliorate SSL/TLS to eliminate these attacks and improve security. We choose to highlight the example of Heartbleed because it is the most dangerous attack and especially that it has many attack patterns. The main solution proposed is to update Openssl version, but it is not the best if we talk about Smartphone or tablets. To patch vulnerable server on Android device, we have to update the ROM's phone, and the update cycle is too long. Therefore, some old phones cannot be updated that is why they are still vulnerable. SSL vulnerabilities, especially Heartbleed, have impacts on embedded devices especially Smartphone if they contain a version of Openssl with Heartbleed bug and they have problems with software update. In addition, we can also detect the problem if the mobile browser exposes the vulnerability on the client side. Nowadays many attacks are discovered on SSL/TLS protocol: the logjam attack [**?**], the FREAK attack [**?**] etc. Through Heartbleed, hackers could steal many important information (credit card information, password . . .). As we see, in recent years many vulnerabilities in SSL/TLS have been revealed. So, the security of Smartphones became very exhausting due to its limited features. That is why; many studies analyze the security of mobile transactions and its limited features. [7] [8]

Countermeasures

There are several countermeasures to avoid Heartbleed vulnerability and provide security of data, applications and important information of mobile devices. One of the scenarios of attacks on Heartbleed is like MITM but more dangerous, because of a malicious server that exploits revoked certificates.

DNSSEC and OCSP (Online Certificate Status Protocol) are solutions to this problem. On android devices, we recommend the use of SSL certificate pinning, to, securely, exchange important information between server and android banking applications. In fact, users can install unsafe certificates; therefore, the device's trust store can be compromised. SSL pinning ignores these certificates and trusts certificates stored inside the applications. Another important countermeasure is the use of perfect forward secrecy PFS to secure old traffic [9] [10] , but nowadays it is not a good solution due to the discovery of the new attack called the Logjam Attack [**?**].

IV. VERIFICATION AND VALIDATION

In this paper, we show how existing verification and formal specification tools are revealing very early vulnerabilities that will be difficult to correct at the implementation phase. First-of-all, there are many advantages using automated verification tools. Among these advantages, we can cite; first, using automated verification tools, through which we can find known vulnerabilities. It seems useless to waste time looking for these attacks if they are already known. There are two raisons to do this, to increase the confidence in the tool and to avoid the reappearance of old vulnerabilities. Second, attacks found automatically do not appear in their known form, and this leads us to think differently and to better assess the consequences of attacks. Finally, it is more important to find new vulnerabilities; this is the purpose of many researchers, in fact, automated tools can find unknown attacks and this helps to avoid them in an early phase. There are many techniques to prevent such cryptographic vulnerabilities. In this section, we focus on one of these techniques, which is formal verification of cryptographic protocols. Many mistakes arise when using cryptographic protocol for securing e-commerce transactions. Fuzzing techniques can be applied to the protocols and they can detect vulnerabilities in specific implementations. How to ensure that a new protocol is secure even before its implementations? Nowadays, in view of malicious activity, intrusion attempts and various attacks which computer network suffers from, the verification of security protocols became very important. That is why automated verification tools like AVISPA are effective and efficient ways to test the robustness of cryptographic protocols.

A. *Verification assumptions*

In the context of modeling security protocols, it is necessary to model the intruder, also define its behavior and limit it. For this, the assumptions used are collected under the name of ”Delev-Yao” [11]. This model is based on two assumptions, which are; cryptography is secure and the intruder is the network.

The first assumption is that the intruder cannot decrypt a message without the key; he cannot also guess a secret key or a nonce.

The second assumption is that the intruder has a full control over the internet; in fact, he knows all the public data of such protocols. He can read, store, and block every sent message, he can also compose and decompose messages and he can encrypt and decrypt if he has the key.

B. *Security properties verification*

E-commerce has additional challenges, in fact, although the properties of secrecy and authentication are still basic, they are not the essential one that we are trying to prove.

Other properties need to be proved for the security of e-commerce transactions. However, Avispa is limited to only two security properties (the authentication goal and the secrecy goal). E-commerce security requires verifying payment properties such as non-replay, non-repudiation...

These properties require working on protocols abstractions that can be verified automatically using automated tools for building and analyzing security protocols.

We also notice another challenging aspect of e-commerce security protocols; these protocols do not include typically two agents or participants (more a server S) for assurance, but instead they include three agents (the buyer, the seller and the bank).

AVISPA tool is essentially used to prove the security properties. Some of these properties are verified as follows.

Analyzing Attacks on Protocol

Using AVISPA tool, we try to detect some attacks on the protocol such as Renegotiation attack, replay attack, triple handshake attack, etc.

- Renegotiation attack (CVE-2009-3555)
  The renegotiation attack is a serious flaw made by the renegotiation feature of TLS. It give the possibilities to attacker to inject data into a running connection deprived of destroying the session.
- Replay Attack
  Replay attack is to intercept a communication and send a message already sent in this communication. This can be used to send authentication information copied from those of past communication. SSL pare this attack through the MAC that contains the message sequence number and other parameters specific to the connection. So a forwarded message is detected as not in its place. Either bad sequence number, or bad connection number, etc. In addition, the MAC cannot be modified because it is hashed.

V. Conclusion

In our paper, we have discussed the problem of validation and verification of e-commerce security protocols using AVISPA tools.

This verification is important to ensure the secrecy and authentication properties in these protocols; but this verification does not guarantee that the implementation of protocol fulfills these properties, also other security properties are difficult to be verified automatically.

As we have seen in this paper, AVISPA is able to verify only secrecy and authentication properties.

The models derived from the Dolev and Yao seem to be the most advanced in what concerns the expressiveness and automation, but they are still relatively abstract. There are still many improvements to add to Dolev-Yao model(Automation, management of various multi-session mode, extension to problems specific to e-commerce) Automatic generation of implementation of cryptographic protocols tested is still an open issue.

References

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

[2] Dadeau, F., Ham, 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.

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

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

[5] Maatoug, Ghazi, Frdric 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.

[6] Sharma, Archana, Vineet Kansal, and R. P. S. Tomar. ”Location Based Services in M-Commerce: Customer Trust and Transaction Security Issues.” International Journal of Computer Science and Security (IJCSS) 9.2 (2015): 11.

[7] Ngai, Eric WT, and Angappa Gunasekaran. ”A review for mobile commerce research and applications.” Decision support systems 43.1 (2007): 3-15.

[8] Onwuzurike, Lucky, and Emiliano De Cristofaro. ”Danger is my middle name: experimenting with SSL vulnerabilities in Android apps.” Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks. ACM, 2015.

[9] pratik guha sarkar, Perfect Forward Security : An Extra Layer Of Security and Privacy, iSEC Partners, Inc 123 Mission Street, Suite 1020 San Francisco, CA 94105, 2014.

[10] Cremers, Cas, and Michele Feltz. One-round strongly secure key exchange with perfect forward secrecy and deniability. ETH Zurich, 2011.

[11] Dolev, Danny, and Andrew Yao. ”On the security of public key protocols.” IEEE Transactions on information theory 29.2 (83): 198-208.

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

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

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

[15] 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.

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

[17] 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.

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

[19] Kurkowski, Mirosaw, 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 TechnologyISAT 2016Part II. Springer, Cham, 2017.

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

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

ISSN 1737-930X