ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 9, Issue 6, December 2019

THE PROTECTION OF DATA PHONE IN THE WIRELESS NETWORK WITH SSL, SSH AND IPSEC

AMMAR ES-SAID' LABRIJI EL-HOUSSINE, ILHAM IBNOUZAHIR
University Hassan II/ Faculty of Sciences Ben M'sik
Casablanca Morocco

Abstract: Our work revolves around the field of mobility; we are primarily interested in the security of mobile data traffic more precisely the security of mobile data in wireless network. We seek to propose a new approach, which is full, and responds to the requirements in this in this latter. We seek that our approach will be useful for the actors of information technology, and communications, to secure data. Our strategy, and the evaluations carried on it have shown that our approach provides improved outcomes without the son communications rudiment .This paper presents a new methodology and strategy that generalizes the proper use of mobile platforms, indicating the difference between mobility TCP/IP and mobility in networks without son , valuing it . But unfortunately this simplicity coupled with the fact that the data is transmitted in an aerial way, makes it vulnerable to interception and network attacks. Thus, we have elaborated a methodology that supports the study and identification of this security management protocols, which recommends changing the study and identification of the SSL/SSH, this methodology is based on modeling .Knowledge in VPN form, through the exchange protocols, we found that the IPSEC is a multi protocol resources which is lower and constructive. The study of the IPSEC protocol helps us to infer that the latter offers a more substantial and secured to meet the overall requirement to protect the transfer of data in order to be achieved .the implementation of Finally, we opted for IPSEC as the best solution for mobile data security in networks without son.

Keywords: **Mobility, Considerable, Securing, Terminal mobility, SSL/SSH/IPSEC.**

I. INTRODUCTION

This article will be as follows, we will introduce in the first part of the existing mobility approaches and challenges encountered, and the second part will be devoted to the problems of mobility in networks without son and the strategy used. At the third part we will take an interest in the implementation and solutions.

The last part discusses the possibilities found for our strategy most often with SSL, SSH, and IPSEC protocol and choose the best of security of mobile data in the networks without son.

II. MOBILITY IN NETWORKS

Mobility is resulting in the possibility that some entities may be moved between different attachment points, types of mobility:

- ✓ Mobility in networks.
- ✓ Mobility in the TCP /IP stack.
- ✓ Mobility in wireless networks.

But…what is the best kind of mobility? Mobility in networks contains several types, namely:

A. *Terminal Mobility*

This type consists of two Sub-categories:

1. *Portability*

Its main feature that the device is not using the network while it is moved; it is incurring a disconnection-reconnection-displacement sequence.

2. Continued Mobility

When a device is connected to a wireless network, it can be moved without problem, the only consequences appear at transmission errors if the terminal moves away.

B. Mobility of People

The networks connections must be established between people, not between terminals or applications.

III. MOBILITY IN THE TCP / IP STACK

Mobility in the TCP/IP stack: based on datagram routing to mobile machinery and the connection at TPC/UDP, for the name TCP/IP. This name comes from its two main components, the transmission control protocol in internet protocol to transport and network level. Routing data grams to mobile machines is done by routers or machines with multiple network interfaces maintain a routing table that contains mappings between prefixes of IP addresses and the next node to which the router must deliver the message.

Mobility Connections AT TCP/ UDP

Once a TCP connection is established, both ends will send and receive data. It conflicts with the mobility and breakfast: if a machine is moving to a different sub network, it cannot keep the old IP address because the packets are sent there will be routed to the old subnet. We noticed similar problems, related to the change of the IP address and the inability to transfer the network session.

IV. MOBILITY IN WIRLESS NETWORKS

Mobility in wireless networks: wireless networks are networks with no fixed infrastructure. This infrastructure uses infrared waves and radio waves for transmission of mobile data in the network without son.

Manuscript received: 22 November 2019
Manuscript received in revised form: 17 December 2019
Manuscript accepted: 04 January 2020
Manuscript Available online: 10 January 2020

DOI:10.17605/OSF.IO/QMD7R

A. *Transmission Technique in Networks without Son*

There are two types, Transmission:

1. Transmission by infrared waves: requires that the devices are facing each other without any obstacles.
2. The transmission by radio waves: it is used for the creation of networks without son that have several kilos meters, these waves cannot be stopped by barriers; they say that the transmission is unidirectional. we have seen the comparison of mobility in networks, mobility in the TCP/ IP stack and mobility in wireless networks, so mobility in wireless networks is defines as a solution, which meets the limits set by mobility the networks.
3. Mobility in networks without son can improve the performance of the organization with the benefits system, further transmission of data very fast and sale terminals can communicate wirelessly liaison.
4. One of the main benefits of mobility in networks without son is peripherals. Unfortunately connection ease the way data is transmitted unsecured, making the network vulnerable to interception and attacks. The next part will be devoted to detailing the various problems of mobility in networks without son.

V. THE PROBLEMS OF MOBILITY IN NETWORKS WITHOUT SON

The majority of mobile applications are exposed to several problems with security levels due to severe data loss and attacks:

1) The weakening.
2) The noise.
3) Limitation and variation of bandwidth.

Our strategy to integrate an efficient system for security mainly focused on data mobiles .In the next chapter we will propose a strategy and a basic study of the conventional solution to realize these problems.

VI. METHODOLOGY USED

1) Amelioration of mobile process: to reduce the cost and duration or increase efficiency.
2) The access to mobility services: we will use a protocol that will maintain a stable connection that will facilitate the exchange of mobile data.
3) The importance of data, not the peripherals: they have exploited the technique to reduce the risk of intellectual property.
4) Secure the functioning of mobility.

All this realize more often with SSL, SSH and IPSEC consider as a better solution for the security of data. In the next part we will treat all the possibilities found our strategy most often with SSL, SSH, IPSEC and select the best protocol of security of mobile data in the networks without son.

VII. CRYPTOGRAPHIC MECHANISMS

The three protocols are similar in their initialization phase and in their data protection mechanism. As to the initialization phase of IPSEC protocols meaning ISAKMP (Internet Security Association and Key Management Protocol) and SSH, they are based on the negotiation of a group DH (Diffie -Hellman) for generating shared keys. The SSL / TLS protocol, even if it supports an exchange DH, most of its negotiations for security are based on asymmetric encryption with the public key of the server. Regarding data protection, the three protocols use functions of symmetric encryption and hashing to ensure confidentiality in services and in data integrity.

VIII. AUTHENTICATION INTEGRITY AND CONFIDENTIALITY

With IPSEC users' authentication is mainly related to network equipment such as users' machines and routers. ISAKMP (Internet Security Association and Key Management Protocol) offers multiple authentication methods such as shared keys. Both SSH and SSL protocols are exchange protocols. They only authenticate the two ends of the communication (client, server). Concerning SSL / TLS, it offers a single authentication method based on identity certificates, SSH gives customers a choice between several authentication methods negotiated through a secure tunnel. For this, even the authentication methods that appear for the first time non-secure (password) can be safely used with SSH. With SSL and SSH, the integrity and privacy services are explicit. Messages from the initialization phase of the two protocols are protected in integrity and application data is encrypted and protected in integrity.

IX. PROTECTION AGAINST ACTIVE AND PASSIVE ATTACKS

The three protocols provide protection mechanisms for initialization phases and data protection phases.

- If the integrity service is triggered (case of SSH, SSL, IPSEC, AH (authentication header), the traffic is protected against any changes made by malicious third parties.
- If the confidentiality service is triggered (case of SSH, SSL, IPSEC ESP (Encapsulating Security Payload) traffic is protected against information spying attack and traffic analysis. If the non-withheld service is triggered (case of SSH, SSL, IPSEC- ESP, AH, ISAKMP), the sent data cannot be replayed after a while.
- If the protection service against denial service is activated (if IPSEC- AH, ESP, ISAKMP), traffic is protected against the IP, TCP and UDP floorings.

X. PROTECTION OF EXCHANGE OR NETWORK PROTECTION

Amongst the three studied protocols, IPSEC is the only

DOI:10.17605/OSF.IO/QMD7R

protocol that offers IP level traffic safety. It can there by ensure securing all IP based applications. The SSH and SSL / TLS protocols ensure safety of all types of traffic flowing over the TCP transport protocol. SSH and IPSEC protocols ISAKMP provide identity protection service while with SSH, the client's identity (ID / password or public key) is protected. ISAKMP protects the identity of the two communicators. Note that the exchange of identity protection ISAKMP protects certificates and public key of communicators and other types of information such as the actual IP addresses, and emails. Therefore, trust among communicators is obtained with the authentication methods negotiated between the players... Both IPSEC and SSL / TLS protocols use trusted authorities (PKI (Public Key Infrastructure)) to provide a strong authentication service based on identity certificates. Regarding the SSH protocol, several studies are currently underway to integrate its authentication mechanism based on public / private key in a trusted infrastructure.

XI. DELEGATION MANAGEMENT BETWEEN ACTORS

The three studied protocols do not ensure the delegation management services between actors. SSH protocol has the intermediary entity as a trusted entity. An SSH server can act as an intermediary server by double tunnel. The first is located between the client and the SSH server. As for the second, it is located between the SSH server and the recipient server.

With the SSL / TLS protocol, the standard does not allow the delegation of authentication role. It is for this reason that the Proxy is powerless in the case of use of SSL / TLS between the two ends of communications without conducting any activity in this area to include a delegation of roles mechanism between SSL / TLS servers and intermediate proxy.

Since IPSEC is a network layer protocol, users' authorization service is often left to the Firewalls and checklists ACL (Access Control List). The SSL / TLS protocol does not have this feature which is rather left to applications. SSH defines static checklists based on the operating system by categorizing users into groups according to their access privileges. As per IPSEC Protocol (ISAKMP) it does not include this service. Indeed, IPSEC differs in the method of authentication hop-by -hop, which establishes a series of secure tunnels and the end-to -end approach that establishes a single tunnel between the two ends of the communication.

XII. MANAGEMENT AND ACCESS CONTROL

Nowadays, most security protocols use both IPSEC and Firewalls techniques. Indeed, IPSEC and firewalls do not provide the same access control and filtering services. For instance, Firewalls allow the control traffic leaving a site globally.

The SSL / TLS protocol defined in RFC (requests for comments) is an end -to-end security protocol that prohibits access control out of the server machine. In addition, the application requests (as the case of HTTP headers or SMTP) pass through an encrypted tunnel SSL / TLS .It is essentially for these reasons that proxy caches are disabled when the SSL / TLS protocol is used. They are then unable to play their role as access control or filtering

The access control mechanism with SSH is based on the definition of static checklists by classifying users in groups according to their access privileges.. It has as an advantage a unique authentication system or SSO (Single Sign On). Indeed, the SSH server installs an authentication agent in front of a set of applications. The SSH agent intercepts the users access. Once the user is identified, it transmits the identification data to the application via environment variables (in the case of a Web server module) or in HTTP header fields.

XIII. CONCLUSION

The main objective of our research is to find out the right solution for data security in wireless networks. Hence, even though SSH protocol was able to circumvent many threats to network security, it remains related in its specification to software design than to a proper security protocol. This made this protocol inapplicable in new environments and thus unable to meet the new requirements of applications and users.

SSL / TLS is the only large-scale deployed security protocol because it is already available on the most secure platforms of the web, both at the server level and at the level of customers. Indeed, this protocol has been adapted beyond the usual transactional applications. Thus, it is used by the consortium WAP (Wireless Application Protocol) for radio communication of GSM, for the EAP (Extensible Authentication Protocol) for wireless environments and even in approaches for smart cards with a protocol version available to mobile users. The modular architecture of SSL / TLS helps move some parts of the protocol without jeopardizing the entire system.

The IPSEC protocol and its associated sub-protocols provide today a standard and safe solution to achieve secure private networks. IPSEC also provides supplementary security to other protocols in order to meet the overall requirements for a protective and successful data transfer.

REFERENCES

[1] FLORIAN MALEKI, Concerned about security issues related to BYOD and mobility 03 November 2014. Vol-60, No-17 PP No: 1-5.

[2] PIOTR KIJEWSKI, The reference data underlying the entire information system June 2007, PP No: 98-101.

[3] CHADI HANTOUCHE, Mobile security and application are IT priorities, Vol-63, Oct-2000, PP No: 544-547.

DOI:10.17605/OSF.IO/QMD7R

[4] SAMUEL PIERRE, networks and mobile computing Systems– VOL. 10, NO. 22, 5 June 2003.

[5] NICOLAS JAIMES, “mobile penetration rates in the world Vol-3, August 2003. PP (22_27).

[6] Sylvain HUET, “Security and mobile process”Vol-2, November 2005, PP No: 339-345.