Volume XXIII 2020
ISSUE no.1
MBNA Publishing House Constanta 2020

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Man in the middle attack on HTTPS protocol

To cite this article: Dragoș Glăvan, Ciprian Răcuciu, Radu Moinescu and Sergiu Eftimie, Scientific Bulletin of Naval Academy, Vol. XXIII 2020, pg.199-201.

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-20-I1-026

Man in the Middle attack on HTTPS protocol

Dragoș GLĂVAN, Ciprian RĂCUCIU, Radu MOINESCU, Sergiu EFTIMIE

Military Technical Academy "*Ferdinand I*" – Systems Engineering for Defense and Security Doctoral School
dragos.glavan@gmail.com

Abstract. A "man-in-the-middle" (MITM) attack occurs when an external entity intercepts communication between two systems. This can happen for any form of online communication, such as e-mail, websites social networking and web browsing. Not only does it try to listen to your private conversations, but it also steals all the information from your devices. A man-in-the-middle attack is a procedure that allows the attacker to interpose between the user and the computer it communicates with, to read or modify that conversation. This procedure used to be very common before the massive switch to the HTTP-Secure protocol and continues to be encountered even today, although it is harder to do. the higher threat is the low detection rate. Users may not always know if the network they use is legitimate or if someone monitors traffic ul, whether it's an airport, a hotel or a neighborhood cafe. Our dependence on the Internet has caused us to use the same device for both personal and professional life, thus being automatically exposed to risks. Web-based applications are based on HTTPS protocol to ensure confidentiality and security in transactions ranging from home banking, e-commerce and e-procurement to sensitive data, such as career and identity information. Users trust this protocol to prevent unauthorized viewing of personal, financial and confidential information on the Web.

1. Introduction

Web-based applications are based on the HTTPS protocol to guarantee the security and confidentiality of transactions ranging from e-commerce, banking and online shopping to those with sensitive data for identity and career. Secure Socket Layer (SSL) was introduced by Netscape Communications for security sensitive communications in 1994, and in 1999 it was adopted as a standard as Transport Layer Security for HTTP security in HTTPS. An HTTPS URL indicates that the browser will download a web page using HTTP, but with a different default port and a TLS authentication layer between HTTP and TCP. Therefore, the majority of the population believes that HTTPS-based data exchanges are secure and the user tends to trust the Web application as soon as the "lock" symbol appears. This paper presents how attackers can successfully intercept data transfer and corrupt communication security.

2. The concept of the MITM attack

Man-in-the-middle attacks exploit the fact that the HTTPS server sends a certificate with its public key to the web browser (if this certificate is not trusted, the entire communication path is vulnerable). This attack replaces the original certificate that authenticates the HTTPS server with a modified certificate. The attack is considered a success if the user neglects to double-check the certificate when the browser sends a warning notification. This happens all too often - especially among users who frequently encounter self-signed certificates when accessing intranet sites. This article presents the case of the screen shown in the figure below, in which a user from the client host (CH) wishes to perform a secure transaction on the server host (SH) using HTTPS. Since CH and SH need to exchange data on the

network, the attacker's host (ATH) acts as a gateway to the flow of traffic. The attacker intercepts the traffic from the source and sends it to the destination, thus obtaining the possibility to modify messages and to insert new ones without any party noticing.

The attacker carries out an attack in the following steps:

- it acts as a gateway between the CH and the LAN router;
- forwarding CH requests to connect to SH without any interference;
- the SH interception responses are sent from the default LAN gateway;
- the creation of a self-signed fake certificate takes place;
- the fake certificate is sent to the CH;
- an encrypted channel between CH and attacker is built and another between SH and attacker when CH accepts the certificate.

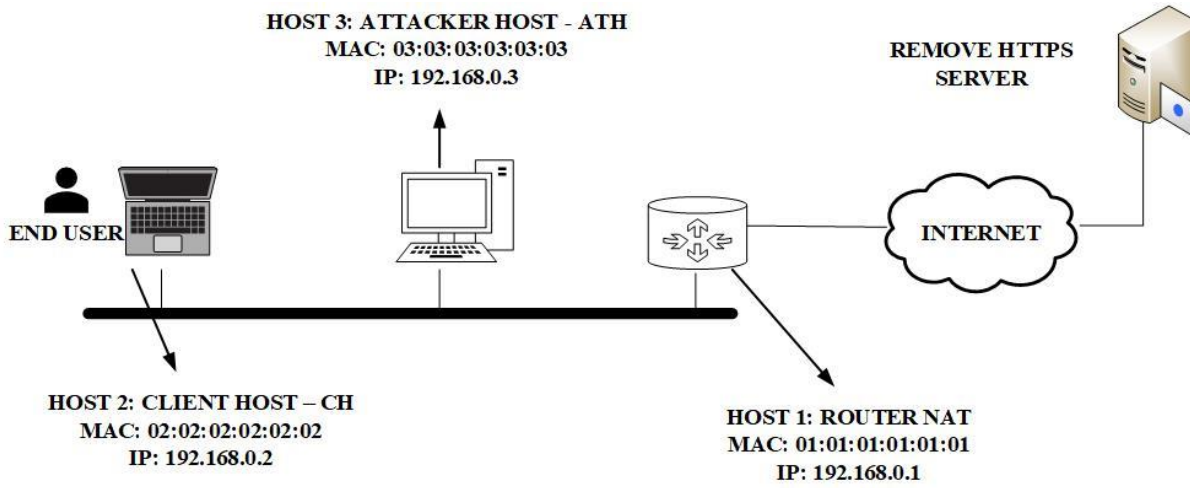

Fig.1. Typical network configuration

Upon completion of these steps, CH and SH see a communication channel that seems seemingly secure. Due to the fact that the attacker holds the necessary keys, he has the ability to decrypt the entire communication. Depending on the network configuration there are several variants of this attack, in this article the CH is connected to a switched Ethernet (the most common LAN technology in companies) that is connected to the Internet using a router, and the attacker is connected to a host (ATH) on the same LAN. This is possible because the LAN is open or because a LAN host has been broken and so unauthorized users can log in.

The MITM attack occurs by modifying the Address Resolution Protocol (ARP) and the Domain Name System (DNS). ARP poisoning is based on retrieving the traffic sent over a switched LAN network using direct IP forwarding. Given that ARP requests are transmitted, the attacker can read / learn the MAC addresses of other hosts. By matching between MAC and IP addresses, the attacker receives traffic from another IP address

3. Practical example

Suppose a student wants to retrieve data from a secure web server by calling htttps: //school.ro. In this scenario, the user must log on to the HTTPS server to see their school situation. Going back to the figure presented above, it is assumed that hosts connected to the LAN use private router ip addresses and implement NAT (Network Address Translation). The attacker starts with ARP poisoning of the LAN, then discovers the HOST1 and 2 IP and ARP addresses during normal LAN operation. It sends periodically during the attack ARP responses to HOST1 and 2 that it replaces. This action involves redirecting all traffic between the CH and the router to ATH. At this point, the attacker must execute a DNS spoof to redirect all DNS requests to his machine, with the aim of passing all the CH traffic to the

web server through ATH. This attacker uses a tool called dnsspoof to issue responses to the DNS requests issued by CH and indicates other addresses. At this time, all traffic between HOST1 and 2, as well as DNS requests from HOST2 can be modified and intercepted by ATH.

In order for CH to believe that everything is okay, ATH must redirect traffic between SH and CH, thus allowing IP redirection to ATH by modifying the IP routing tables. Once the attacker manages to intercept the traffic between CH and SH, ATH can start a fake HTTPS session where it can decrypt its traffic. In order to generate a fake certificate in the name of SH, the webmitm is running, by running it the attacker has to offer some answers related to SH because the browser from CH could display it to the user receiving the certificate. If CH accepts the fake certificate when it connects to htttps: //school.ro, ATH will intercept and decrypt all traffic because it does not have the private key that matches the public key in the certificate. Most browsers alert the user when they receive a certificate that is not signed by a trusted authority. ATH has a good chance of seeing the HTTPS session initiated under its control, ATH captures the traffic flowing through the secure channel. When the attacker decides to complete the capture phase, ATH saves the captured network traffic. Therefore, in the saved file the attacker will most likely find confidential data such as the user and password of a person connecting to HOST2.

4. Conclusions

In this paper it has been shown that it is possible to attack secure web-based connections through HTTPS by exploiting some properties of the common LAN networks as well as the typical behaviors of the inexperienced users. For an experienced user, implementing a MITM type attack is not difficult but not very easy. The ease with which an attacker can spoof a certificate, emphasizes that sites should recognize the potential dangers of signed certificates. In most cases users ignore browser warnings because they are used to them. Although strong encryption is a secure and powerful data protection tool, the security it provides is just as good as the weakest link in the chain. Our dependence on the Internet has caused us to use the same device for both personal and professional life, thus being automatically exposed to risks.

References:

[1] E. Rescorla, "*HTTP over TLS*", IETF RFC 2818, 2000

[2] C. Allen and T. Dierks, "*The TLS Protocol*", IETF RFC 2246, 1999

[3] D.C. Plummer, "*An Ethernet Address Resolution Protocol*", IETF RFC 826, 1982

[4] J.C. Brustoloni and Xia, "*Hardening Web Browsers against Man-in-the-Middle and Eavesdropping Attacks*", 2005