A SIMULATION-BASED PERFORMANCE COMPARISON STUDY OF A MAN-ON-THE-SIDE ATTACK BASED ON ARP SPOOFING, ITS DETECTION, AND PREVENTION

Kashaija Joel

V.V. Popovsky Departanent Infocommunication Engineering,
Kharkiv National University of Radio Electronics, Ukraine

E-mail: kashaija.joel@nure.ua

Abstract

The work describes a simulation-based performance comparison study of a Man-on-the-Side attack based on ARP spoofing, its detection, and prevention. Using Wireshark as the deep packet analyzer, we performed a Man-on-the-Side attack leveraging the ARP spoofing table, showing the real environment created to simulate a Man-on-the-Side attack. The presented sample revealed how a MotS attack could quickly get the password from an unsecured login. The two frames from the victim and the attacker's relay to the website have been displayed.

An active attack in computer security is known as a Man-on-the-Side attack (MotS) [1, 2]. Cyber-attackers can eavesdrop on and insert messages into the two parties' communication. When responding to a victim's request, the attacker uses a timing advantage to ensure his message gets there first and before the proper response [3-8]. One technique for identifying a MotS attack is latency examination. The majority of IoT devices use fog computing to guarantee fast data transport. During network monitoring, man-on-the-side attacks can also be found using deep packet inspection (DPI) and deep flow inspection (DFI). Network monitors may access data such as packet size and length thanks to DPI and DFI. Forensic analysis of the network traffic must be performed to establish whether the collected network traffic is a MotS attack in the first place. 95% of websites on Google use HTTPS, according to Google's transparency report. Organizations should think about setting up stringent HTTP transport security (HSTS). HSTS allows servers to reject untrusted connections when configured. Attacks like SSL stripping are rendered impossible by this. One of the best ways to stop a MotS attack is with the help of an automated certificate management system. For instance, a MotS attacker can take advantage of a single image loading over unencrypted HTTP.

The man-on-the-side attack is comparable to a man-in-the-middle attack [7]. The attacker can only access the communication channel regularly, which allows him to read the traffic and add new messages but not alter or delete those sent by other participants. This condition differs from a man-in-the-middle attack when the attacker controls a network node completely. When responding to a victim's request, the attacker uses a timing advantage to ensure that his message gets there first and before the proper response [6].

Using Wireshark as the deep packet analyzer, we performed a Man-on-the-Side attack leveraging the ARP spoofing table below, showing the real environment created to simulate a Man-on-the-Side attack.

Table 1. Simulation environment parameters

	IP address	MAC address	Modified MAC address on victim's IP table
Gateway	147.174.120.1	PrimaryA 6b:40:99	DellComp 4e:4f:69
Victim	147.174.120.208	AmbitMic cc:1b:6c	–
Attacker	147.174.120.235	DellComp 4e:4f:69	–

This process, also known as ARP poisoning, involves the attacker pretending to be the victim's gateway to exploit the ARP protocol. The victim's site and the gateway's IP forwarding table are modified. The attacker now has access to every message sent or received between the Web server and the victim. The IP tables of the gateway, the victim's correct MAC addresses, and the modified MAC addresses as a result of the ARP spoof are listed in Table 1. Every message sent from the victim to the gateway will be retransmitted to the victim from the attacker since the attacker essentially acts as the relaying station of the messages

exchanged between the victim and the gateway. The source and destination MAC address at the Network Access Layer, Ethernet II, indicated in the detailed area, are the sole thing separating these two packets. This sample demonstrates how a MotS attack can quickly get the password from an unsecured login. Once more, we display the two frames from the victim and the attacker's relay to the website (Fig. 1).

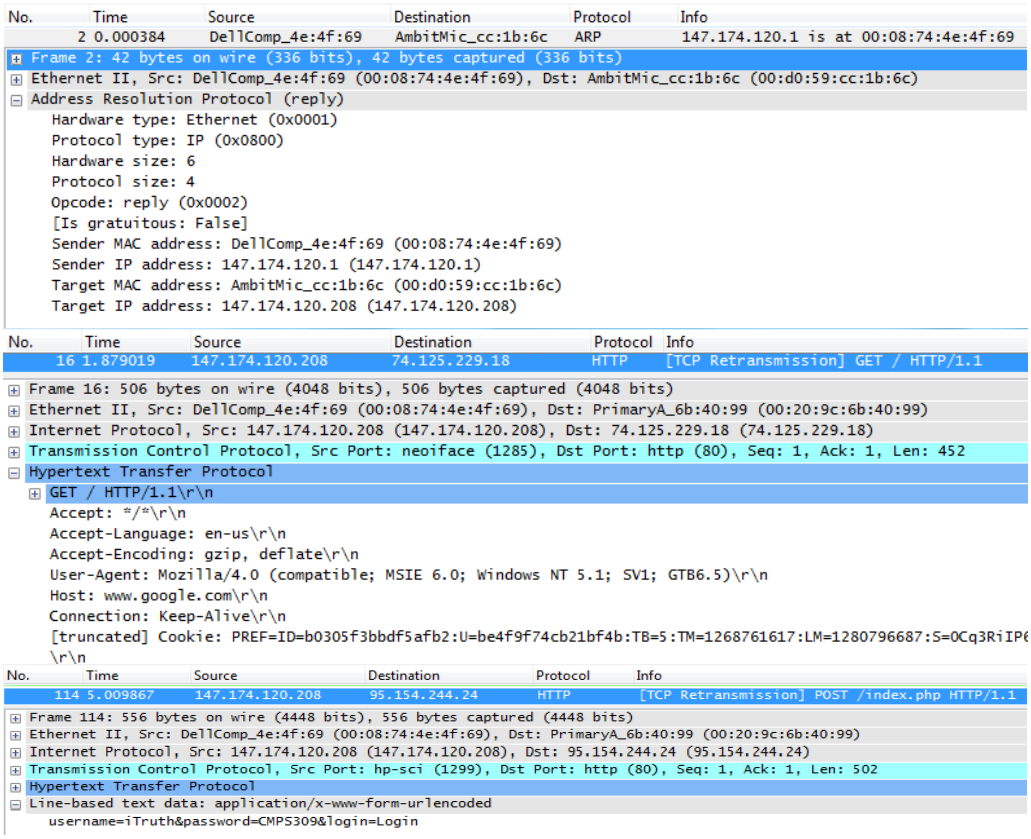

Fig. 1. The two frames from the victim and the attacker's relay to the website

References:

1. Gallagher R., Greenwald G. How the NSA Plans to Infect 'Millions' of Computers with Malware. The Intercept. URL: https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/ (дата звернення: 12.11.2022).

2. China's Man-on-the-Side Attack on GitHub. Netresec. URL: https://www.netresec.com/?page=Blog&month=2015-03&post=China's-Man-on-the-Side-Attack-on-GitHub (дата звернення: 12.11.2022).

3. Schneier B. Attacking Tor: how the NSA targets users' online anonymity. the Guardian. URL: https://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity (дата звернення: 12.11.2022).

4. Mozur P. China Appears to Attack GitHub by Diverting Web Traffic (Published 2015). The New York Times. URL: https://www.nytimes.com/2015/03/31/technology/china-appears-to-attack-github-by-diverting-web-traffic.html (дата звернення: 12.11.2022).

5. Aver H. WinDealer via man-on-the-side. Kaspersky-Cybersicherheitslösungen für Privatanwender und Unternehmen | Kaspersky. URL: https://www.kaspersky.com/blog/windealer-man-on-the-side/44518/amp/ (дата звернення: 12.11.2022).

6. Maynard P., McLaughlin K. Towards Understanding Man-on-the-Side Attacks (MotS) in SCADA Networks. arXiv preprint arXiv:2004.14334. 2020. P. 1-9. DOI: https://doi.org/10.48550/arXiv.2004.14334

7. Man in the Middle (MITM) Attacks | Types, Techniques, and Prevention. Rapid7. URL: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/ (дата звернення: 12.11.2022).

8. LuoYu APT delivers WinDealer malware via man-on-the-side attacks. Security Affairs. URL: https://securityaffairs.co/wordpress/131921/apt/luoyu-apt-windealer.html (дата звернення: 12.11.2022).