Simple Man-in-middle Attack, Investigation, and Defense

Tzu-Chi Huang, Kuo-Chih Chu, Jun-Ming Liang
Department of Electronic Engineering,
Lunghwa University of Science and Technology,
Taoyuan County, Taiwan
tzuchi.phd@gmail.com, kcchu@mail.lhu.edu.tw, aazz77aa@gmail.com

ABSTRACT

An IP address is well known as a part of elements to identify a communication end point in the Internet, so criminal investigators often use it as the evidence to accuse someone of committing criminal activities. However, criminal investigators can easily make a miscarriage of justice by relying on an IP address as the only evidence because IP packets may be forged by an attacker. In this paper, criminal investigators can understand how a Simple Man-in-middle Attack (SMA) can be easily performed in LAN and Wireless LAN (WLAN). Since SMA has the capabilities of passing ingress filters at routers, sharing communication with a victim via the victim IP address, and having certain untraceable features, criminal investigators are given suggestions about how to investigate and defend it for potential victims.

Keywords: Simple Man-in-middle Attack, Criminal Investigation, ARP Spoofing

I. INTRODUCTION

An IP address [1] [2] is well known as a part of elements to identify a communication end point in the Internet. Today, an IP address is usually used in criminal investigation to find the attacker in somewhere because it has locality features. An IP address furthermore is widely used to accuse someone of committing criminal activities such as distributing illegal software, sending spam emails, and posting articles to harm someone's reputation in the Internet. An IP address is almost taken by the judge to determine the suspect's guilt.

However, an IP address should not always be considered the only evidence because it is merely a field in an IP packet (technically speaking, two fields have IP addresses in an IP packet). An IP address in an IP packet can be modified to forge a new packet as if it were sent by a victim in the Internet. Although criminal investigators believe that routers with ingress filters and connection-oriented protocols such as TCP [2] [3] can effectively resist the packet forges in the Internet, an IP address is still vulnerable to attacks, especially man-in-middle attacks in LAN and Wireless LAN (WLAN) [4]. Although certain packet protection mechanisms such as IP Security [5] can be used to shield packets from being forged, an IP address still should not be used as the only proof of identifying a communication end point in the Internet because not all connections are established with the enable of packet protection mechanisms.

In this paper, the author explains a Simple Man-in-middle Attack (SMA) capable of resisting ingress filters at routers, sharing communication with a victim via the victim IP address, and having certain untraceable features. The author details the technology of SMA and its implementation. The author discusses how to roughly identify and avoid such an attack. The author argues that an IP address should not always be considered the only evidence to accuse a person of committing criminal activities, because it is very easy to make a miscarriage of justice.

This paper is organized as follows. This paper introduces Simple Man-in-middle Attack (SMA) in Section 2. This paper explains how to implement and defend SMA in Section 3. Finally, this paper has conclusions in Section 4.

II. SIMPLE MAN-IN-MIDDLE ATTACK (SMA)

Simple Man-in-middle Attack (SMA) can be easily carried out by packet forges. In LAN or Wireless LAN (WLAN), SMA can easily pass ingress filters at routers of Internet Service Provider (ISP) [6], seamlessly share communication with a victim via the victim IP address, and natively have untraceable features. SMA roughly consists of ARP Spoofing, Packet Forging, and Packet Forwarding technologies [7] [8] in its attack procedures as shown in Figure 1.

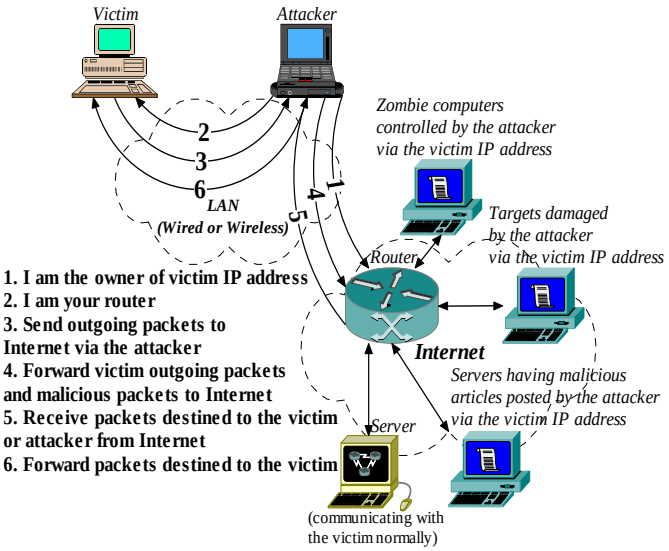

Figure 1, SMA Overview

First, SMA uses the ARP Spoofing technology to tell the router in LAN or WLAN that the victim IP address is bound to the attacker's MAC address [9] instead of the victim's MAC address. Second, SMA uses the ARP Spoofing technology as well to tell the victim that the router address is bound to the attacker' MAC address now. When performing the ARP Spoofing technology, SMA sends unicast and unsolicited ARP packets to the router for avoiding IP address collisions [8] detected by the victim. Accordingly, SMA makes the victim unaware of the fact that its IP address is hijacked by the attacker now.

Next, SMA may receive outgoing packets from the victim and can have several options. 1) SMA can read the contents of the packets and get something that interests the attacker, e.g., user account, password, and privacy. 2) SMA can forge the packets entirely and perform some necessary operations to maintain functions of connection-oriented protocols, e.g., synchronizing sequence and acknowledgement numbers in TCP splice [10]. 3) SMA can forward the packets directly to the router simply by replacing their destination MAC addresses with the MAC address of the router. Usually, SMA at this time may create a table like what a Network Address Port Translator (NAPT) [11] does in order to distinguish packets destined to the victim from packets received by the attacker on demand in the future.

If SMA receives packets destined to the victim from the Internet via the router, it forwards them back to the victim simply by replacing their destination MAC addresses with the MAC address of the victim. If SMA receives packets destined to the attacker from the Internet via the router, it locally forwards them to the applications of the attacker. If SMA is implemented to consider high compatibility, it can do what a NAPT does to applications of the attacker in order to make all local applications running well without any modification. Finally, SMA can perform anything the attacker wants to do via the victim IP address while the victim still communicates with its corresponding server in the Internet normally without perceiving any difference.

Because the victim IP address is approved by ingress filters at routers, SMA can use the victim IP address to send any packet and easily pass the routers. At the premise of maintaining communication functionality of the victim, SMA can use the victim IP address to communicate with other computers in the Internet at the same time. Because of using the ARP spoofing technology based on unicast and unsolicited ARP packets, SMA is hard to be traced while initiating attacks such as controlling zombie computers, damaging targets, and posting malicious articles to harm someone's reputation. In today's Internet composed of high speed LANs and wide range WLANs, SMA can easily aim an attack at a victim and damage targets in the Internet via the victim IP address. When SMA is performing attacks and the victim is communicating as well, the victim can easily be accused of committing criminal activities but hardly proves his or her innocence – because all evidences gotten by criminal investigators from ISP or servers in the Internet strongly point at the victim as the source of attacks.

III. Attack, Investigation, and Defense

A. SMA Implementation

In the section, we discuss how to implement, identify, and defend SMA. According to our experiences in implementing a SMA prototype in Windows XP as shown in Figure 2, we can divide SMA into the user-level part and the kernel-level part. In the user-level part, we need to implement SMA Console as a native process to accept commends and parameters such as starting SMA, stopping SMA, the attacker MAC address, the victim IP address, the victim MAC address, and the router MAC address, although certain MAC address query or monitor mechanisms can be implemented as well. We use SMA Console to configure the kernel-level part of SMA inside Windows.

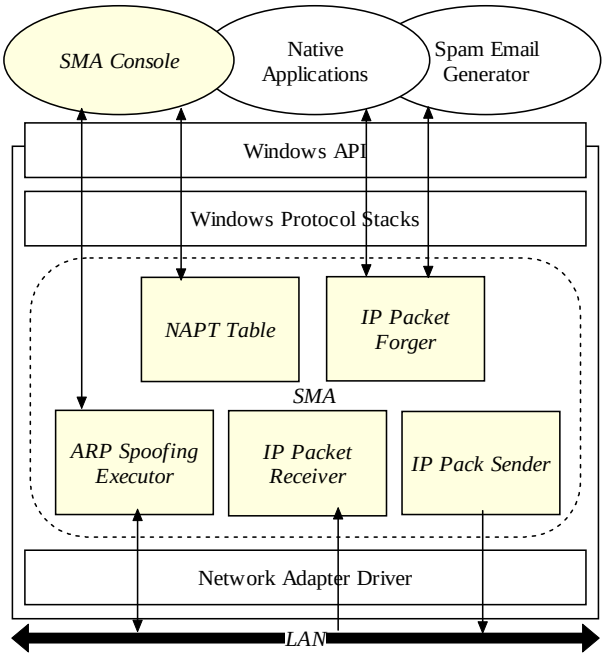

Figure 2, SMA in Windows

In the kernel-level part, we need to implement NAPT Table, IP Packet Forger, IP Packet Receiver, IP Packet Sender, and ARP Spoofing Executor by deploying them at the location between network adapter drivers and Windows protocols stacks. We use NAPT Table to monitor sessions established by a victim. We use IP Packet Forger to not only forge packets but also translate IP addresses and port numbers in local packets on demand. We use IP Packet Receiver to take packets received by the network adapter via Windows network adapter. We use IP Packet Sender to not only send packets to the router but also forward packets to the victim on demand. We use ARP Spoofing Executor to periodically give the router ARP packets for binding the victim IP address to the attacker MAC address in the ARP cache. Meanwhile, we use ARP Spoofing Executor to periodically give the victim ARP packets for binding its router IP address to the attacker MAC address in the ARP cache.

Implementing most SMA components inside the Windows kernel allows local applications or further malicious software in the attacker to work well without any modification, which gets the performance similar to the packet translation done by NAPT boxes in the Internet. Besides, implementing most SMA components inside the Windows kernel can easily handle all local packets passing through Windows and forward victim packets on demand.

B. Defense

According to the working principle of SMA, criminal investigators are suggested to perform investigation procedures as follows, although SMA is difficult to be traced. First, criminal investigators can dump the ARP table and further ARP logs in the router, although most routers only keep an entry in the ARP table for 4 hours at default [12] and periodically clean up the logs. Second, criminal investigators can check camera records operating near the victim and query suspects because IP addresses have locality features, although suspects may not tell the truth. Third, criminal investigators can compare the MAC addresses in the suspects' network devices with the ARP logs in the router in order to see whether the victim IP address is ever bound to one of the MAC addresses, although suspects can change the working MAC addresses of their network devices with software configuration. Fourth, criminal investigators do not always think that an IP address is the effective evidence to prove criminal activities committed by a specific person.

For defending SMA, we have some suggestions. First, we suggest that a router should be upgraded to have the capability against ARP spoofing, e.g. not trusting information from unsolicited ARP packets. Second, we suggest that the potential victims in LAN should configure an ARP record that statically binds the router IP address to the MAC address of the real router, because the network adapter of the router in LAN unlikely will be changed frequently. Third, we suggest that the potential victims in WLAN should always use access points [4] that support high-level authentication mechanisms such as user account, password, and protection guaranteed by the existing wireless security protocols such as WPA and WPA2 [13] before accessing the Internet, because low-level authentication mechanisms such as MAC address filters at access points are useless to MAC addresses forged by attackers. Fourth, we suggest that the potential victims should enable packet protection mechanisms such as IP Security [5] or Transport Layer Security (TLS) [14] before sending privacy or sensitive data to networks.

IV. CONCLUSIONS

In this paper, we explain a Simple Man-in-middle Attack (SMA) capable of resisting ingress filters in a router, sharing communication with a victim via the victim IP address, and having certain untraceable features. We detail the technology and its implementation. We discuss how to roughly identify and avoid such a simple man-in-middle attack. We argue that an IP address should not always be considered the only evidence to accuse a specific person of committing criminal activities, because it is very easy to make a miscarriage of justice.

ACKNOWLEDGEMENTS

We gratefully acknowledge the National Science Council of Taiwan for their support of this project under grant numbers NSC 100-2628-E-262-001-MY2. We further offer our special thanks to the reviewers for their valuable comments and suggestions, which materially improved the quality of this paper.

REFERENCES

[1] J. Postel, "Internet Protocol," RFC 791, 1981

[2] T. Socolofsky and C. Kale, "A TCP/IP Tutorial," RFC 1180, 1991

[3] J. Postel, "Transmission Control Protocol," RFC 793, 1981

[4] P. Calhoun, M. Montemurro, and D. Stanley, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11," RFC 5416, 2009

[5] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, 1998.

[6] T. Killalea, "Recommended Internet Service Provider Security Services and Procedures," RFC 3013, 2000

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

[8] T. C. Huang, K. C. Chu, "Networking without Dynamic Host Configuration Protocol server in Ethernet and Wireless Local Area Network", Journal of Network and Computer Applications (JNCA), Vol. 34, Issue 6, 2011, pp. 2027-2041.

[9] U. Garg, P. Verma, Y. S. Moudgil, S. Sharma, "MAC and Logical addressing (A Review Study)," International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, 2012, pp.474-480.

[10] M. C. Rosu and D. Rosu, "An Evaluation of TCP Splice Benefits in Web Proxy Servers," Proceedings of the 11th international conference on World Wide Web, 2002, pp. 13-24.

[11] G. Tsirtsis and P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)," RFC 2766, 2000.

[12] Cisco Express, "Configuring the Address Resolution Protocol (ARP)," CSS Routing and Bridging Configuration Guide (Software Version 7.30)

[13] A. H. Lashkari, M.M.S. Danesh, and B. Samadi, "A survey on wireless security protocols (WEP, WPA and WPA2/802.11i),"Proceedings of 2nd IEEE International Conference on Computer Science and Information Technology, 2009, pp. 48-52.

[14] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2,", RFC 5246, 2008