Enhancing the performance and security against media-access-control table overflow vulnerability attacks

Yih-Jou Tzang¹, Hong-Yi Chang²,¹ and Chih-Hsuan Tzang³

Article first published online: 14 OCT 2014
DOI: 10.1002/sec.1142
Copyright © 2014 John Wiley & Sons, Ltd.

Additional Information (Show All)
How to Cite | Author Information | Publication History

Abstract
A media-access-control (MAC) table of switches is used to store the MAC addresses of stations in a local area network (LAN) segment to enable frame forwarding. Each incoming frame is broadcast to all switch ports through a switch backplane when an MAC address is not registered in the MAC table. If an address is registered, the switch forwards the frame to the port connected to the destination host. An MAC table overflow (MTO) vulnerability attack causes the MAC table of all switches to overflow in an LAN segment, and all incoming frames are broadcast to every port in the switch. The attack degrades switch-based LANs (each port of a switch comprises an individual operating domain and switch bandwidth) to bus-based LANs (all ports are bounded to one operating domain and share a bandwidth similarly to a hub), causing information leakages and reducing the effective bandwidth; a virtual LAN configuration can reduce but not eliminate the associated damage. This paper presents the security effect of an MTO vulnerability attack, and a novel per-port-based MAC table design is proposed to solve this type of vulnerability. The experimental results indicate that the mechanism of the proposed design eliminates the damage caused by such attacks. Copyright © 2014 John Wiley & Sons, Ltd.

Keywords:
media-access-control (MAC) table overflow vulnerability attack; network security; virtual local area network (VLAN); information leakages; defense; switch

More content like this
Find more content: like this article
Find more content written by: Yih-Jou Tzang | Hong-Yi Chang | Chih-Hsuan Tzang | All Authors
Enhancing the performance and security against media-access-control table overflow vulnerability attacks

Yih-Jou Tzang1, Hong-Yi Chang2 * and Chih-Hsuan Tzang3

1 Department of Computer Science and Information Engineering, De Lin Institute Technology, New Taipei City, Taiwan
2 Department of Management Information Systems, National Chiayi University, Chiayi, Taiwan
3 Department of Computer Science, University of Taipei, Taipei, Taiwan

ABSTRACT

A media-access-control (MAC) table of switches is used to store the MAC addresses of stations in a local area network (LAN) segment to enable frame forwarding. Each incoming frame is broadcast to all switch ports through a switch backplane when an MAC address is not registered in the MAC table. If an address is registered, the switch forwards the frame to the port connected to the destination host. An MAC table overflow (MTO) vulnerability attack causes the MAC table of all switches to overflow in an LAN segment, and all incoming frames are broadcast to every port in the switch. The attack degrades switch-based LANs (each port of a switch comprises an individual operating domain and switch bandwidth) to bus-based LANs (all ports are bounded to one operating domain and share a bandwidth similarly to a hub), causing information leakages and reducing the effective bandwidth; a virtual LAN configuration can reduce but not eliminate the associated damage. This paper presents the security effect of an MTO vulnerability attack, and a novel per-port-based MAC table design is proposed to solve this type of vulnerability. The experimental results indicate that the mechanism of the proposed design eliminates the damage caused by such attacks. Copyright © 2014 John Wiley & Sons, Ltd.

KEYWORDS

media-access-control (MAC) table overflow vulnerability attack; network security; virtual local area network (VLAN); information leakages; defense; switch

*Correspondence
Hong-Yi Chang, Department of Management Information Systems, National Chiayi University, Chiayi, Taiwan.
E-mail: hychang@mail.ncyu.edu.tw

1. INTRODUCTION

Network security has become critical for the Internet businesses because of the growing number of Internet applications. Viruses, worms, malicious code, and spyware are constantly being created and spread rapidly through email, instant messenger, and peer-to-peer applications. Attacks are also being launched internally [1] by affected wired or wireless hosts in Intranets. These hosts or access points typically access an intranet through a layer-2/3 switch. Nevertheless, firewalls, intrusion prevention systems, and unified threat management systems are generally installed near the router of an enterprise and cannot prevent the propagation of attacks and worms within the intranet [2,3]. Consequently, several security switches have been developed [4–7] to provide first-mile (the closest to hosts from intranet to Internet) protection, although they remain expensive and their market is relatively immature. Network admission control has recently been presented to prevent unwanted access from hosts that are not patched adequately [8].

1.1. Background

Layer-2 switches are widely used in Intranets worldwide. Most local area network (LAN) segments are composed of layer-2 switches forming switch-based LANs. The IEEE 802.1d standard [9] defines the spanning tree protocol and enables layer-2 switches to forward incoming frames and learn the media-access-control (MAC) addresses of the stations within the LAN segment. An MAC table with a limited size (typically 8000 to 16 000 entries) is established in each layer-2 switch to store the learned source MAC addresses. The switch that receives incoming frames verifies whether the destination MAC address within the frame
is located in the MAC table. If so, the switch forwards the frame to the destination switch port. Otherwise, the frame is broadcast to all switch ports excluding the frame source port. Although layer-3 switches are increasing in popularity, layer-2 switches remain the most deployed devices in LAN segments. The security issues of layer-2 switches have not been widely addressed because their handling of passing-through frames is straightforward and does not cause vulnerabilities. Nevertheless, severe damage can result if the switch-based infrastructure crashes or is hacked.

In a switch operation process, when any host connects to the switch for the first time and transmits a data frame to other hosts, the MAC address of the host and the receiving port number of the switch (from which the data frame derives) are recorded in an MAC table. If a host linked with switch A connects to switch B through switch A and transmits data frames to hosts linked with switch B for the first time, the receiving port number of switch B and the MAC addresses of the hosts and switch A are similarly recorded in the MAC table of switch B. When the destination address of the transmitting data frame is unknown to the switch because the switch has not yet recorded the address in the MAC table, the switch broadcasts the transmitted data frames. Once the target receiver receives the data frame and acknowledges the switch, the switch also uses this acknowledgment to record the destination address and port number in the MAC table. Consequently, broadcasting is not required when a switch is requested to transmit data to these destination addresses again in the future. Only a receiver with a destination MAC address and one switch port receives the transmitted data frame from a switch.

Switch broadcasting is originally a mechanism to transmit data frames with an unknown MAC address for the first time. However, a switch constantly broadcasting all data frames with a registered but missed MAC address in an MAC table is unfavorable. At this point, the idea of MAC table overflow (MTO) vulnerability attack is gradually emerging. Because MAC table size is limited and a switch records new MAC addresses but cannot identify legal MAC addresses during received frame, switches exhibit MTO vulnerability. An MTO vulnerability attack occurs when an attacker exploits the vulnerability inherent in normal switch operation. When a host from a specific switch port transmits frames rapidly by using many unregistered MAC address, the MAC table within the switch is continually updated. This situation causes the existing MAC address entries in the MAC table to be overwritten. All data frames with registered MAC addresses are still broadcast to every port in a switch because they are not listed in the MAC table. Furthermore, the local cache of communication users still contains MAC address, port information, and a normal data interchange, and users are unaware of the data broadcast and loss (i.e., eavesdropping). Consequently, practical security problems pose severe threats to companies, universities, and individual worldwide.

1.2. Contributions

This paper proposes a novel attack model for MTO vulnerability attacks, as well as an appropriate solution. An MTO vulnerability attack is categorized as a layer-2 problem. This type of attack does not necessitate the learning or spoofing of existing Internet protocol (IP) or MAC addresses using an address resolution protocol (ARP) or reverse address resolution protocol (RARP) request to launch an attack. Furthermore, such an attack cannot redirect frame streams through a specific port to acquire data. Although connections to servers cannot be established, attackers can still receive data at any port of an LAN switch. The goal of such attacks is to fill the MAC table and eavesdrop the information by using layer-2 frames over a nonedge or nonborder switch or core switch. Attacker can use C programming of raw sockets or a packet generator (e.g., Smartbit series; products of Spirent [10] or IXIA series: products of IXIA [11]) for launching this type of attack to attack switches. Also, any PC easily leaks data for connecting to the attacked switches. Furthermore, this type of attack is designed to raid the LAN, not the Internet. Once an LAN connects to another attacked LAN through a switch, all LAN switches are attacked. Consequently, this attack generates a cascading effect among LANs. All incoming frames are broadcast to all switch ports, instead of only to the destination port according to standard operations. Any host can use the Sniffer, Wireshark, or Ethereal tools to capture sensitive data (e.g., unencrypted passwords, emails, file transfer protocol (FTP) files, and instant-messaging conversations) from other computers, which would not be accessible if the switch is operating normally. The strategy of MTO vulnerability attacks is based on the weakness of regular operations in switches. No study thus far has discussed MTO vulnerability attacks. Accordingly, no study has proposed a resolution for MTO vulnerability attacks on switches until now; however, there is a real weakness on the existing switches [12,13].

Furthermore, this paper proposes a per-port-based MAC table design, which can assist in preventing severe attacks. The scheme does not require an additional central server or central switch to control the frames. In addition, switch hardware is not altered, and only the switch firmware is modified. The per-port-based MAC table is designed to limit the number of MAC address of a port, but the number of registered MAC addresses remains the size of the MAC table in the switch. To achieve this, the total memory of an MAC table is equally divided among all switch ports. Per-port-based MAC tables are based on the concept of public search (forwarding flow) and individual record (learning flow) to the switch table. In this scheme, when a switch forwards to a received frame (i.e., the forwarding flow), the switch must also search the entire MAC table for the destination MAC address (i.e., a public search). Conversely, the source MAC addresses of every transmitted frame (i.e., the learning flow) can only be added to a corresponding block of the source port in the per-port-based MAC table (i.e.,...
the individual record). Based on this design, the frames of an MTO vulnerability attack can only write or overwrite the corresponding block in the MAC table, and frames are forwarded among the other ports as usual.

The remainder of this paper is organized as follows: Section 2 includes a review of related studies. Section 3 introduces MTO vulnerability attacks and the cascading effect of an MTO vulnerability attack among LANs. Section 4 presents an analysis of the proposed strategy. Section 5 presents an evaluation of defense efficiency based on experiments and equation models. Finally, Section 6 provides the research conclusion.

2. RELATED STUDIES

Layer-2 switches [12,13] are used to transmit frames in the data link layer (i.e., layer 2) of an open system interconnection (OSI) reference model in networks. Layer-2 switches depend on the MAC addresses of frames to forward, filter, and switch frames in LANs. Layer-3 switches (i.e., IP switches) [14] are used to route, filter, and switch packets in the network layer (i.e., layer 3) of the OSI reference model in networks. Layer-3 switches can not only switch MAC frames (i.e., layer 2) but also route IP packets (i.e., layer 3) by using MAC and IP addresses. The routing of IP packets results in all legal packets being appropriately forwarded from LANs to wide area networks (WANs). WAN hosts can access or connect to Intranets by using IP, MAC addresses, and layer-3 switches (i.e., through routing). By contrast, LAN hosts can only connect to Intranets by using MAC address and layer-2 switches. A firewall [15,16] is a security device designed to protect intranets from Internet-based attacks by processing only layer-3 or upper-level (connection or application layer) network traffic based on rules, connection states, and other network layers (e.g., a packet filter firewall is operated in layer 3, a stateful packet inspection is operated in layer 4, and an application filter firewall is operated in layer 7). In layer-2 switch operations, upon receiving a frame, the switch searches its MAC table for the frames destination address. When the address is determined, the switch compares its port with the source port to ensure that they are distinct; frames are forwarded in a switch when the source and destination hosts are located at distinct switch ports. After completing this task, the switch forwards the frame to the port, which is connected to the destination host. Therefore, only the specified destination port receives the frame. If the frames destination address cannot be determined because the MAC table does not contain this information, the frame is broadcast to every port of the switch except the source port. This operation ensures that the destination host eventually receives the frame.

Multiple MAC addresses being recorded in the MAC table of a single switch port is possible because of switch interconnection in LANs. A switch port can be connected to a host (one MAC address in an MAC table) or a switch (multiple MAC addresses in an MAC table, including that of the switch and all hosts attached to the switch). In reality, a switch port is connected to a switch that cascades numerous switches. In other words, a switch can be registered to multiple MAC addresses via a port in an MAC table [4–7]. For example, four levels or upper topologies of linked switches are typically adopted by companies and schools. If a switch possesses a 16-port and 16K (214)-entry MAC table, the MAC table of a top-level switch registers 216 (16×16×16×16) MAC addresses in four levels with a complete topology, thereby reaching the bounded range of the switch MAC. A switch interconnection with 216 hosts is possible in an LAN, regardless of whether they are distinct legal MAC addresses of numerous hosts or various fake MAC addresses of one host. A switch cannot identify but only records these addresses in the MAC table for the first time. Therefore, establishing a threshold for the number of MAC addresses of a switch is not feasible. The threshold approach not only violates the operation of a switch but also results in an inability to connect networks when a host is attached to a switch port. Once a threshold is set and the quantity of recorded MAC addresses of a switch exceeds the threshold, the communication of data frames between switches (even legal hosts) stops. Fake MAC addresses cannot be recorded again, but MAC addresses of fresh hosts or hosts linked with other switches also cannot be recorded in the MAC table of a switch. Therefore, hosts linked to switches cannot transfer data to or receive data from switches. Approximate thresholds interfere with continually operating switches and destroy the partial topologies of switch LANs. Generally, the MAC table size is the default threshold in a switch.

Media-access-control table overflow vulnerability attacks involve transmitting numerous layer-2 MAC frames to the switch. Regarding the vulnerability of layer-2 switch operations, when the transmitted frames of various MAC addresses are registered and the MAC table is full, an MTO vulnerability attack is launched. The broadcast frames are propagated, and the MAC table of all LAN switches is affected (registered and filled). These broadcast frames cause the MAC table of all LAN switches to overflow, and the transmitted data frames are broadcast and leaked to all switch ports, thereby flooding them. Thus, the attacker can easily eavesdrop on all data broadcast from any port of an LAN switch. MTO vulnerability attacks are not worms and require no specific frames. Instead, MTO vulnerability attacks are layer-2 operating problems involving switches in networks. Because LAN switches only process layer-2 MAC addresses and bypass layer-3 IP addresses, MAC frames are used to attack LAN switches directly and attackers can easily implement MTO vulnerability attacks.

However, 802.1X [17] port authentication can only partially solve the problem. In reality, a link always exists between switches to form an LAN. Additionally, 802.1X port authentication can be deployed on edge or border switches to avoid an unauthenticated connection, but it cannot be applied to nonedge or nonborder switches or
core switches. Because a switch cannot actively display and input passwords, a switch cannot be authenticated by another switch. Furthermore, the MAC address of a switch is its legal address when delivering frames between two switches. Once a nonedge or nonborder switch or core switch deploys 802.1X port authentication, all frames are dropped through the switch. Attackers only attack the port of a nonedge or nonborder switch or core switch during an MTO vulnerability attack, which generates LAN problems. Therefore, switches must not only deploy 802.1X port authentication but also install a per-port-based MAC table to ensure their protection against MTO vulnerability attacks.

A single layer-2 network can be partitioned into multiple distinct operating domains. These domains are known as virtual LANs (VLANs) [18]. Grouping hosts with common requirements into a VLAN, regardless of their physical location, can greatly simplify network designs. A default value of switch configuration is a switch without VLANs. The number of specific ports in a VLAN depends on the users work department (e.g., research and design, marketing, and accounting) or the host delivery content of actual network jobs. The VLAN settings are not a dynamic adjustment. Moreover, the switch operations are based on the administrator VLAN settings for continuing to forward frames in an LAN. When a VLAN is attacked, all the ports of the VLAN are still broadcast frames. In addition, a single port is rarely set for a VLAN because a VLAN with one port cannot be used to communicate with other members. Therefore, if a VLAN is assigned only one port in a switch, this is meaningless. Furthermore, attacks can occur at any port of a switch and at any time, and the attacked port can belong to any VLAN, which port and VLAN of a switch will be attacked cannot be predicted. The affected range of an attack differs according to the number of ports in a VLAN. Employing this VLAN strategy only limits the damage incurred from a VLAN attack without eliminating the problem. VLAN 1 is assumed to be equipped with six ports, and VLAN 2 is equipped with 10 ports at a 16-port switch. When VLAN 1 is attacked, VLAN 2 is unaffected. However, VLAN 1 is still induced to broadcast all frames and leak data to all of its switch ports. Furthermore, the resolution strategy for a problem should not be estimated through trial and error. Therefore, this paper proposes the per-port-based MAC table design to eliminate the problem.

This study is the first to present this type of MTO vulnerability attack. First, experiments of MTO vulnerability attacks are conducted on a real intranet (a detailed explanation is provided in Section 3). Data can be intercepted at switches by using the Wireshark or Ethereal tools. Second, no studies have discussed MTO vulnerability attacks (by using MAC address and ports). Therefore, this paper proposes the per-port-based MAC table design to eliminate the problem. The white paper of switch device in many companies confirms the weakness of switch [12,13]. Therefore, only layer-2 MAC frames are used to attack switches, which has not been previously addressed. MAC frames are used to directly attack LAN switches through the vulnerability of switch operations. Accordingly, MAC tables are overflowed, data frames are leaked to switch ports, and broadcast frames interfere with switch operations. In the past, attack strategies have involved using IP and MAC addresses to attack network devices. For example, an ARP table attack [19–21] uses IP or MAC addresses to trick routers into forwarding packets to incorrect ports where data are intercepted. Such attacks focus on spoofing IP and MAC addresses to bypass switches. This problem has been addressed in numerous studies, and most switch products are supported by defense mechanisms [12,13]. The UNIDES system [22] employs a proxy server (a centralized system) to counter ARP table and MAC and IP address spoofing attacks but did not address MTO vulnerability attacks (by using MAC address and ports). Other attack methods employ numerous random IP addresses to deliver packets and flood a server. For example, an SYN flooding attack [23–28] prohibits servers from providing standard services. Regarding network flooding problems, an MTO vulnerability attack should not be confused with an ARP table attack or a broadcast storm attack. ARP spoofing (i.e., an ARP table attack) and SYN flooding (i.e., a broadcast storm attack) are other attacks that can be categorized as layer-3 problems because they are not focused on the MAC table of layer-2 switches.

3. MODEL AND EFFECT OF A MEDIA-ACCESS-CONTROL TABLE OVERFLOW VULNERABILITY ATTACK

An MTO vulnerability attack is measured using two parameters \(n, \tau\), where \(n\) denotes the number of attack frames generated each time and \(\tau\) represents the time interval between two consecutive attacks. For example, \((10,000,10\ \text{ms})\) signifies that an attack is launched once every 10 ms and that 10,000 attack frames are generated during each attack. These parameters determine the propagation speed of an MTO. Therefore, an attacker can gain vital information without being detected by controlling the parameters.

Attacker can use C programming of raw sockets or packet generators (e.g., Smartbit series: products of Spirent [10] or IXIA series: products of IXIA [11]) to launch this type of MTO vulnerability attack. Packet generators are commonly used to test packet throughput and the quality of service of networks. In this study, packet generators are employed to launch an MTO vulnerability attack. Packet generators are set to input the source MAC parameters, frame transmission rate, and frame length. Numerous frames are generated and delivered after a setting and trigger. In the experiment, clients A and B separately download a file from two FTP servers by using switches 1 and 3 (Figure 1). The attacker connects only to a port of switch 1 to launch the MTO vulnerability attack. The MAC
Table of switch 1 is then overflowed, and all data frames are broadcast to all ports of switch 1. Switches 2 and 3 are equally affected (broadcasting all data frames) when the MTO vulnerability attack cascades among the LAN switches. Therefore, the attacker can readily eavesdrop on all broadcast data transmitted by clients A or B on any port of the LAN switches. Client A can receive downloaded data from client B, and client B can receive downloaded data from client A.

The effects of a one-time MTO vulnerability attack and continuing MTO attacks differ. One-time MTO vulnerability attacks only affect switches for a limited time (the lifetime of an MAC address in the MAC table), whereas switches are constantly affected during continuing MTO vulnerability attacks. A basic scenario is established to assess how switches affect the ability of two (i.e., few) hosts to transmit data frames during three one-time MTO vulnerability attacks involving a varying number of frames on cascading switches. After three one-time MTO vulnerability attacks, another experiment is conducted using a high-utilization scenario to examine the effects that the switches of numerous hosts exert on the ability to transmit data frames during a continuing MTO vulnerability attack on cascading switches.

### 3.1. Basic scenario for a media-access-control table overflow vulnerability attack

To understand the speed at which an MTO vulnerability attack propagates within an LAN segment, an experimental test with three Cisco 2950 (Cisco Systems, Inc., Taipei, Taiwan) switches is designed (Figure 1). The MAC table size of each switch contains 8000 entries. The setup comprises two pairs of FTP servers and clients: one pair (with client B) connecting to switch 3, and the other pair (with client A) connecting to switch 1, to which the MTO vulnerability attacker is also connected.

Figure 2(a) and (b) presents the bandwidth effect on clients A and B exerted by MTO vulnerability attacks, respectively. Initially, both clients A and B receive files at a data rate of 70 Mbps. The first MTO vulnerability attack with 1000 frames (1000, 1000 ms), using short 64-byte packets with randomized source addresses, is launched at approximately 21 s. This attack reduces the download speed of client A and causes oscillation but does not affect client B. The second MTO vulnerability attack with 3000 frames (3000, 1000 ms) is launched at approximately 105 s. This attack reduces the download speed of client A (larger oscillation) dramatically but only reduces the download speed of client B slightly. Finally, an MTO vulnerability attack with 10 000 frames (10 000, 1000 ms) is generated at approximately 273 s, severely affecting both clients A and B. Oscillation lasts for a few minutes after the attack is terminated.

Regarding the first one-time MTO vulnerability attack, the attacker generates 1000 fps of short 64-byte packets by using randomized source MAC addresses (1000 × 64 × 8 = 5000 Kbps) to execute the MTO vulnerability attack. Because the quantity of attack frames does not exceed 8000 (the size of the MAC table), the MAC table of switch 1 does not overflow. In addition, the frames of switch 1 are not transmitted to switch 2; therefore, switch 2 and client B are not even temporarily affected. The download speed of client A is only affected by the broadcast attack frames. In the second one-time MTO vulnerability attack, the number of attack frames generated using randomized source MAC addresses (3000 × 64 × 8 = 15 000 Kbps) exceeds the size of the MAC table. Accordingly, the MAC table of switch 1 overflows, and the effect of the download data for client A gradually increases for all broadcast frames. Nevertheless, data frames are continually transmitted by the FTP server, and the MAC table of switch 1 is reregistered using certain MAC addresses of the transmitted data frames. During the lifetime of one-time attack frames, data frames and attack frames are broadcast, yielding a reciprocal effect of available bandwidth on switches. In the final one-time MTO vulnerability attack, numerous frames that employ randomized source MAC addresses (10 000 × 64 × 8 = 50 000 Kbps) are adopted for the experiment. When the MAC table of switch 1 is completely overwritten by the various source addresses of the MTO vulnerability attack frames, the switch cannot determine a data frame address in the MAC table as normal. Although the data frame addresses are registered in the MAC table, the switch does not transmit the frames to the destination ports but continues to broadcast every frame to all switch ports. Thus, the download bandwidth is affected by the broadcasting of all frames to switch 1. Furthermore, the frames (including attack frames and data frames) broadcast to switch 1 are also transmitted to switch 3 through switch 2. The MAC table of switch 3 is also induced to broadcast the frames. The data frames of switch 3 are similarly broadcast to all switch ports and return to switch 1. All frames (including attack frames and the data frames of switches 1 and 2) are transmitted to all ports of switch 1. The final severity of the situation is higher than at the beginning of the one-time MTO vulnerability attack regarding the download bandwidth. The more attacks and useless frames are broadcast by switches, the less bandwidth is available for downloading data.
3.2. High-utilization scenario for a media-access-control table overflow vulnerability attack

Overwriting the recorded MAC address of a high-utilization switch with transmitted frames is more difficult in an MAC table. The more data frames are transmitted within an LAN, the more messages are leaked during an MTO vulnerability attack. To achieve the goal, the speed of transmitting frames must exceed over the learning-caching rate (LCR) of a switch. The number of MAC addresses that can be registered to a switch determines the size of an MAC table. The LCR of a switch is the maximum speed at which a source address is learned (fps). When $LCR = N$, the switch cannot learn all the source addresses when the rate of incoming frames exceeds $N$. The MTO vulnerability attacker can adopt this feature to execute an attack using a limited bandwidth. Therefore, MTO vulnerability attackers only need to generate $N$ frames per second to overflow the MAC table. For example, for most switches, $N = 8000$ entries (i.e., the MAC table size). An attacker can generate 8000 fps of short 64-byte packets with randomized source addresses (a total bandwidth of $8000 \times 64 \times 8 = 4$ Mbps) to execute an MTO vulnerability attack.

The experiment is conducted on a real intranet. The MAC table size of the switches is 8000 entries. The LCR of the switches is 8000 fps. Smartbit is used to input the source MAC parameters, frame transmission rate (8000 fps), and frame length (a short 64-byte packets with randomized source addresses). The total bandwidth of the attack is 4 Mbps ($8000 \times 64 \times 8$). To keep switches working (high utilization) and transmit the data to each other, all clients are limited speed by using 2-Mbps speed to download a 20-M file in the experiment. The utilization of total bandwidth is lower than 100 Mbps (a bounded LAN bandwidth). Negies [29] and NetBalancer [30] are freeware programs that are used to control the speed of downloading and uploading files and are installed in normal end clients in the experiment.

Generally, switches are widely employed for delivering frames. Four 24-port switches are used to establish a test bed on the intranet. Each switch is connected to 20 clients who download files from an FTP server as normal. When an MTO vulnerability attack is launched on one of the four switches that exhibit high utilization, severe effects (leaked data) are clearly demonstrated. Because each switch exhibits a specific MAC table size and address learning speed, the attacker need only launch enough frames to exceed the table size and at a sufficient LCR by using various sources of MAC addresses, easily yielding leaked data. The forwarding frames become broadcasting frames, because the destination MAC address is not found in the MAC table. The more data frames are transmitted within an LAN, the more messages are leaked during an MTO vulnerability attack. Accordingly, all data can be received from any port of an LAN switch. Thus, data transmissions are neither private nor secure. An experiment is performed to demonstrate the effect of this attack on the number of leaked messages. Four switches, S1, S2, S3, and S4, are connected, and each switch is connected to 20
clients (Figure 3). Each client downloads files from an FTP server at a rate of 2 Mbps. The 20 clients of S1 download files from the FTP server on the left of the figure, and the other 60 clients download files from the other FTP server. The MTO vulnerability attacker connected to S1 generates the attack frames at 4 Mbps and receives frames from the attached port.

The MTO vulnerability attacker launches five continue attacks every second (8000, 1000 ms). The MTO vulnerability attacker cannot receive any FTP downloaded packets before attacking because it is not the destination of these packets. The first attack is launched at the first second, and the 4-Mbps ($N = 8000$) attack frames slightly overflows the MAC table of S1. The attacker then begins to receive the leaked broadcasting frames of S1. Figure 4 presents the effect on security. The attacker launches a second attack, already receiving 30 Mbps. This attack causes the MAC tables of both S1 and S2 to overflow, allowing the frames downloaded by the clients of S2 to be forwarded and received by the attacker. Therefore, an additional 50 Mbps for the previous second is received by the attacker at the third second. The attacker then launches the third attack. As expected, this causes all the MAC tables of S1, S2, and S3 to overflow, resulting in frames downloaded by the clients of S3 being forwarded to S2 and S1, and finally, to the attacker. The attacker launches the fourth and fifth attacks at the fourth and fifth seconds, respectively. The attacker then receives the leaked message at a rate of 100 Mbps, the upper-bound of fast Ethernet connections, at the fifth second. This experiment indicates that by using limited bandwidth (which is difficult to detect), an attacker can rapidly launch an MTO vulnerability attack on an entire network, and most importantly, easily steal numerous messages.

### 3.3. Analysis of the effect of various combinations

A new source address can be handled in one of two ways when an MAC table is full: by removing an existing entry to create space for a new entry (class I) or by ignoring the new source address (class II). To determine the effect of an MTO vulnerability attack on the number of leaked messages, another experiment similar to the previous experiment (with the same experimental environment, as indicated in Figure 3) is conducted with various combinations of classes I and II switches.

Figure 5 presents the experimental results, which indicates that the environment with only class II switches cause the most messages to be leaked quickly. The message leakage rate reaches 100 Mbps when 60 clients join to download files after the attack is launched. The message leakage rate reaches 90 Mbps when 80 clients join to download files, even with only class I switches. These results indicate that the MTO vulnerability attack enables an attacker to steal multiple messages under any combination of classes I and II switches. Such attackers can easily eavesdrop all data frames transmitted within an LAN segment with numerous types of switch.

### 4. STRATEGY DESIGN FOR DEFENDING AGAINST A MEDIA-ACCESS-CONTROL TABLE OVERFLOW VULNERABILITY ATTACK

A VLAN configuration only reduces the attacked area in an LAN and cannot eliminate the damage caused by MTO vulnerability attacks. Accordingly, this paper proposes a per-port-based MAC table design to resolve this type of MTO vulnerability attack. An MAC table is redesigned as a per-port-based MAC table. The switch of the per-port-based table is also required to search for the destination MAC address in the entire MAC table. Conversely, the
Y.-J. Tzang, H.-Y. Chang and C.-H. Tzang

MAC table overflow vulnerability attacks

The source of MAC addresses of the received frame can only be added to the corresponding block of the per-port-based MAC table. To achieve the target, all MAC table sizes are equally partitioned into blocks, with one block for one switch port. This type of design is used to prevent MAC tables from being overwritten or filled with attack frames and prevent data frames with addresses registered in the MAC table from being broadcast. Crucially, data frames with registered addresses should be forwarded to the specified port and not broadcast to all ports during switch operation. Consequently, the frame process is revised in the records of the MAC table. The design of per-port-based MAC tables is unchanged in the forwarding flow and unaffected during normal switch operations; parts of the records in the tables are only adjusted in the learning flow. Accordingly, the MAC table must be allocated before the initial switch operating state. The function of a per-port-based MAC table is to install firmware on switches. Deploying switches does not necessitate any additional settings. The scheme also requires no additional central server or central switch to control the frames. However, switch firmware must be modified and updated to facilitate the functions of per-port-based MAC tables. An additional overhead is required to install and update new firmware for the switches, although the switch hardware remains unaltered.

Figure 6 presents an example of the per-port-based MAC table of a 16-port switch with a table size of 8000. Each port is assigned a 0.5-k (8 k divided by 16 ports) block in the per-port-based MAC table. A frame (source MAC address: 00-02-03-07-23-91; destination MAC address: 00-02-A5-C3-13-AD) is transmitted from ports 1 to 9 of the switch. A flow diagram of the processed frames is adjusted according to the operations of a per-port-based MAC table (Figure 7). Figure 6(a) presents the state of a per-port-based MAC table before receiving frames (source MAC address: 00-02-03-07-23-91). The destination MAC address (00-02-A5-C3-13-AD) of port 9 is registered in the MAC table. In the forwarding flow presented in Figure 7, when the switch receives a frame, an entire per-port-based MAC table must be checked. Searching the MAC table ensures that all registered MAC addresses are checked for the destination MAC address (00-02-A5-C3-13-AD). If the address is found, the switch compares its port (port 9) with the source port (port 1) to ensure that they differ (frames are forwarded when the source and destination hosts are located on different switch ports). After completing this task, the switch forwards the frame to port 9, which is connected to the destination host. Therefore, only the specified port (the port 9 destination) receives the frame. In the learning flow presented in Figure 7, all registered MAC addresses are also checked for the source MAC address. If the address is not found, the switch then records the source MAC address and the source port (port 1) in the MAC table to ensure that the receiver can accurately transmit frames to the sender according to the per-port-based MAC table. However, the

Figure 6. Example of a per-port-based MAC table: (a) the state before receiving frames and (b) the state after receiving frames.

Figure 7. Flow diagram of operations for per-port-based MAC table.
source MAC address is recorded only in the block corresponding to the source port (port 1) in the per-port-based MAC table. Because a source host is connected to the source port of a switch, its MAC address should only be affected in the block of the source port. Therefore, the source MAC address is only recorded in the block corresponding to the source port (port 1). Figure 6(b) presents the state of the per-port-based MAC table after receiving frames. The source MAC address is registered with port 1 in the per-port-based MAC table. Using this design, the address of the MTO vulnerability attack frame only writes or overwrites the corresponding block in the MAC table, and the other frames are forwarded among the other ports as usual.

5. Evaluation of the Design Efficacy

This section compares two methods for reducing the damage caused by MTO vulnerability attacks. In the VLAN method, some switch ports are assigned to VLANs. In the VLAN configuration, the overflowed frames are broadcast only to the switch ports belonging to the same VLAN. The damage from the MTO vulnerability attack is thus controlled in the VLAN. Nevertheless, the problem still exists in the VLAN. These broadcasting frames are sent only to the hosts within the attacked VLAN; however, they can still be easily stolen by the attacker in the VLAN. For the per-port-based method, the MAC table is redesigned as a per-port-based MAC table. The switch of the per-port-based table is also required to search for the destination MAC address in the entire MAC table. Conversely, the source MAC addresses of the received frame can only be added to the corresponding block of the per-port-based MAC table.

5.1. Correlation factor definition

These two methods are subsequently evaluated through experiments and by using an equation model. When a VLAN is assigned additional switch ports, the affected portion of the operational area increases. Furthermore, the more MAC address (host) frames are transmitted through a VLAN, the more MAC addresses are registered on the MAC table of the switch.

Each VLAN is assumed to be assigned a distinct number of switch ports in a switch. Thus, the following parameters are used:

- Number of ports in a switch, \( P_s \)
- Number of VLANs in a switch, \( V_s \)
- Number of ports in \( j \)th VLAN, \( P_{Vj} \), \( 1 \leq j \leq V_s \)
- Minimum number of all \( P_{Vj} \) in a switch, \( \text{Min}(P_{Vj}) \)
- Maximum number of all \( P_{Vj} \) in a switch, \( \text{Max}(P_{Vj}) \)

The capability of a forward frame is identical for any switch port in a switch. When all switch ports of a switch are equally assigned to \( k \) VLAN (\( \#V_s = k \)), these \( P_{Vj} \) values (number of ports in a VLAN) are also the same in the switch; in other words, \( P_{V1} = P_{V2} = \ldots = P_{Vk} \).

Consequently, the formula \( P_3 = \sum_{j=1}^{V_s} P_{Vj} \) is always true. Furthermore, we derive the following results from this assumption. When an attack is launched to generate \( N \) frames per second (\( LCR = N \) in the switch) in one switch port of \( i \)th VLAN, the method of VLAN possesses a \( ((P_s - P_{Vj})/P_s) \) defense-attack rate and the proportion of leaked messages is \( (P_{Vj}/P_s) \). Because \( \text{Max}(P_{Vj}) \leq P_{Vi} \leq \text{Min}(P_{Vj}) \), the VLAN method is a \( ((P_s - \text{Max}(P_{Vj}))/P_s) \) defense-attack rate at most and the proportion of leaked messages is \( (\text{Min}(P_{Vj})/P_s) \) at least. Generally, the value of \( \text{Max}(P_{Vj}) \) is greater than or equal to 2 because all VLANs must assign two or more switch ports for security policy or data sharing. Consequently, the value of \( \text{Max}(P_{Vj}) \) is smaller than or equal to \( P_3 \) minus 2.

For a per-port-based method, the entire memory size of the MAC table is shared and allocated among all switch ports, and the size for each port is constant. All MAC table sizes are equally partitioned into blocks, with one block for one switch port. Therefore, the per-port-based method possesses a \( ((P_3 - 1)/P_3) \) defense-attack rate, and the proportion of leaked messages is \( (1/P_3) \) only, when an attack is launched in any switch port of a switch. Only one port is affected for a switch in the per-port-based method when an MTO vulnerability attack is launched. Evidently, the proportion of leaked messages \( (1/P_3) \) is smaller than the minimum value \( (2/P_s) \) of the VLAN method, and the defense-attack rate \( ((P_3 - 1)/P_3) \) is greater than the maximum value \( ((P_s - 2)/P_s) \) of the VLAN method.

A per-port-based MAC table possesses several advantages because only one port is affected in the switch during an MTO vulnerability attack and no host is isolated from communication between switch ports during normal operation. Accordingly, the per-port-based method is the optimal solution against an MTO vulnerability attack.

5.2. Experiment and evaluation

Any VLAN with a distinct quantity of ports can be attacked from one port by MTO vulnerability attack. The objective of this experiment is to determine the difference in the proportion of affected frames among various VLANs with distinct numbers of ports. Therefore, the number of affected frames (the transmitted frames to all ports and hosts of a switch) and total transmitted frames is evaluated. Furthermore, the number of unaffected frames (according to normal transmission for specific ports and receivers) is also evaluated to determine the difference in the percentage of unaffected frames (defense-attack rate) among various VLANs with distinct numbers of ports. Consequently, the evaluation metric is the number of frames including the correct (unaffected), incorrect (affected), and total transmitted frames. The performance and security capability
Subsequently, the defense-attack rate is also tested based on the same conditions, and the experimental results are plotted. The experimental evaluations focus on the comparison of various VLANs with distinct numbers of ports but the same amount of transmissions and hosts during an MTO vulnerability attack. The defense-attack rate is the quantitated ratio of unaffected frames to total transmitted frames. Figure 9(a) presents the variant proportion of unaffected frames in VLANs with varying numbers of ports (2–10 ports) in a 12-port switch during an MTO vulnerability attack. In Figure 9(a), the upper line is the proportion of unaffected frames in two ports, and the lower line is the percentage of unaffected frames in 10 ports. The results reveal that the percentage of unaffected frames does not increase or decrease over time but bases on the number of ports in the VLAN. When a VLAN is assigned few switch ports, the number of incorrect (affected) transmitted frames decreases in the VLAN based on the number of transmissions of each port in a switch. In other words, if the number of switch ports in a VLAN decreases, the proportion of correct (unaffected) transmitted frames (the defense-attack rate) in the VLAN increases during an MTO vulnerability attack by launching in any port of the VLAN. Furthermore, the variant percentage of unaffected frames in VLANs with varying numbers of ports (2–22 ports) in a 24-port switch during an MTO vulnerability attack is evaluated. Figure 9(b) presents the same situation; the upper line is the proportion of unaffected frames in two ports VLAN, and the lower line is the percentage of unaffected frames in 22 ports VLAN. The percentage of unaffected
frames does not increase or decrease over time but is based on the number of ports in the VLAN. When the number of switch ports in the VLAN decreases, the proportion of correct transmitted frames of the VLAN increases during an MTO vulnerability attack by launching at any port of the VLAN. Consequently, the VLAN with two switch ports exhibits favorable defense and few affected frames, despite experimental tests of 12-port and 24-port switches. The VLAN with two switch ports demonstrates the optimal conditions for MTO vulnerability attacks, but the attack can only occur in a VLAN with two switch ports. Each VLAN is not always equipped with two ports, but the attacker can attack any VLAN randomly. Figure 9(a) and (b) indicates that when the number of switch ports in a VLAN decreases, the defense-attack rate of the VLAN increases during an MTO vulnerability attack by launching at any port of the VLAN. If a VLAN is assigned few switch ports, the number of transmitted packets decreases for the VLAN based on a specific number of transmissions in each port in a switch. Consequently, the VLAN with two switch ports exhibits favorable defense and few affected packets, despite experimental tests of 12-port and 24-port switches.

Finally, the experimental tests individually measure the proportion of leaked messages and the defense-attack rate of a per-port-based scheme, the VLAN configuration method, and the defenselessness case in 12-port and 24-port switches. In the VLAN configuration, the optimal condition (two ports) of a VLAN during an MTO vulnerability attack is adopted as the test base. An attack is assumed to be launched on this VLAN with two ports. The results presented in Figure 10(a) and (b) indicate that all forwarding information is almost leaked for an unprotected switch. Under the optimal two-port VLAN condition, the proportion of leaked messages is below 20%. A per-port-based method is the optimum for the proportion of leaked messages (lower than that of the VLAN method) regardless of 12-port or 24-port switches. Figure 11(a) and (b) reveals that all forwarding information exhibits almost no defense capability (the defense-attack rate is nearly 0%) for an unprotected switch. For a VLAN configuration (with two ports), the defense-attack rate is above 80%; however, the per-port-based method is still excellent regarding the defense-attack rate (higher than the VLAN method) during an MTO vulnerability attack launched at any port for a 12-port or 24-port switch.

These experiments confirm that the per-port-based mechanism leads to a superior defense-attack rate compared with the VLAN configuration and prevents an attacker from accessing transmitted packets among all unaffected switch ports. Accordingly, the per-port-based scheme eliminates all possibilities of damage from an MTO vulnerability attack. To verify and validate the method of the per-port-based mechanism, the following equation is established. Table I lists the notation and descriptions employed in this study.

\[
a_i = \begin{cases} 
0 & \text{if } i \neq F(P_a) \\
1 & \text{if } i = F(P_a)
\end{cases}, \forall i \in [1..#B_k], F(P_i) \in [1..#B_k]
\]
Equation (1) defines $R_a$, which is a function of attack blocks.

$$R_a = \sum_{i=1}^{\#B_s} \frac{a_{i}}{\#B_s}$$  \hspace{1cm} (1)

Equation (2) defines $D_r$, which correlates to the number of leaked messages from the MTO vulnerability attack. The value of $D_r$ when all packets are forwarded to the destination and approaches 0% when the forwarding data are leaked completely in the switches. As indicated in Eq. (2), the floor Gauss of $R_a$ ignores the attacked block of the MAC table. Furthermore, Eq. (2) indicates that the attacked MAC table overflowed when $T_a = LCR$ (the LCR) and the value of the defense-attack rate ($D_r$) decreases to 0 because the entire MAC table overflows.

Figure 10. Comparison of the proportion of leaked data for defenselessness, VLAN with two ports, and per-port-based method under an MTO vulnerability attack: (a) for 12-port switch and (b) for 24-port switch.

Figure 11. Comparison of the defense-attack rate for defenselessness, VLAN with two ports, and per-port-based method under an MTO vulnerability attack: (a) for 12-port switch and (b) for 24-port switch.
MAC table overflow vulnerability attacks

Y.-J. Tzang, H.-Y. Chang and C.-H. Tzang

Table I. Notations.

<table>
<thead>
<tr>
<th>Terms</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_a$</td>
<td>Attack port number</td>
</tr>
<tr>
<td>$#B_a$</td>
<td>Number of block (port) in a switch</td>
</tr>
<tr>
<td>$F(P_i)$</td>
<td>A function value, the switch port $P_i$ belongs to one of blocks</td>
</tr>
<tr>
<td>$a_i$</td>
<td>Attack (true or false)</td>
</tr>
<tr>
<td>$R_a$</td>
<td>Percentage of attack blocks on media-access-control table</td>
</tr>
<tr>
<td>$N$</td>
<td>Media-access-control table size</td>
</tr>
<tr>
<td>$T_a$</td>
<td>Transmission rate of attack</td>
</tr>
<tr>
<td>$D_r$</td>
<td>Defense-attack rate, forwarding rate of normal operation</td>
</tr>
</tbody>
</table>

\[ LCR \leq N \]
\[ a_i = \begin{cases} 
T_a & \text{if } T_a \leq LCR \\
LCR & \text{if } T_a > LCR 
\end{cases} \]
\[ D_r = \frac{[(1-R_a)^*N] + [(R_a)^*N] - (T_a+1)]}{N} \times 100\% \tag{2} \]

For 12-port and 24-port switches, where $N = 8000$ and $T_a = LCR = 8000$, the values of $D_r$ are calculated according to the following three cases. For an unprotected switch (VLAN = 1), $D_r = 0$, and all forwarding information is leaked. The second case is a switch with VLAN = 2 to assign a different number of ports. The defense-attack rate ranges from 9% to 85%, meaning that the information is partially leaked. The third case is a novel switch with a per-port-based MAC table, where $D_r \approx 95\%$. These results indicate that the per-port-based MAC table reduces the proportion of leaked messages, and thus, efficiently defeats the MTO vulnerability attack.

6. CONCLUSION

This paper identified an MTO vulnerability attack for switches in layer 2. This type of attack is only applied to layer-2 frames by a packet generator or PC and can be easily launched against a switch. Such an MTO vulnerability attack can cause the MAC table of switches to overflow, thereby degrading switch-based LANs to bus-based LANs. Moreover, this attack also causes a cascading effect among all switches of LANs. The experimental results indicated that an MTO vulnerability attack reduces the effective bandwidth, causes the leakage of substantial information, and spreads the effects to the LAN infrastructure. This paper further proposed a design of a novel per-port-based MAC table for resolving this attack. The per-port-based strategy can eliminate the loss of information efficiently. Furthermore, the proposed mechanism was defined and verified using a novel formula. Through extensive evaluation, the results indicated that the per-port-based MAC table can reduce the proportion of leaked messages (the defense-attack rate approached 95% at least), and thus, efficiently defeat such attacks. The per-port-based method was concluded to provide an effective, scalable, and practical solution for layer-2 switches during MTO vulnerability attacks.

REFERENCES


