Insecurity of WLAN for M-Learning Implementation in Tertiary Level by DoS

Chandrasekaran Nammalwar and Rajeswari C.

Abstract—**Mobility, mobile technology and mobile computing are few buzz words in all the fields. This makes human beings life easy and goes for anywhere, anytime working conditions. In educational field Networking and mobile computing are playing major role in the shift from the traditional black board teaching to contemporary E-Learning and M-Learning environment. But the major issue with the wireless network is vulnerability, denial of service and in general security compared to the wired network. To secure WLAN in organizations and institutions, the world is moving to ubiquitous and seamless computing environments. On the negative side, unlike wired networks, these networks are more vulnerable making it easy for an intruder to capture transmitted signals and also send massive volume of illegitimate traffic and utilize system resources in a way that renders the system inoperable thus denying access to authorized users. This paper demonstrated different methods of achieving denial of service (DoS) attack as it applies to wireless networks and discusses and proposes different defense mechanisms so as to minimize the attacks.**

Index Terms—**Network security, network vulnerability, DoS, DDoS.**

I. Introduction

Technological innovation in computing such as wireless have indeed opened up new dimensions of threat to system's security. While many of the breaches of wired network will be found in wireless networks, the nature of wireless medium requires a degree of trust and cooperation is not guaranteed, a malicious user can exploit the weakness in order to deny service, collect confidential information, or disseminates unwanted or false information.

Denial of Service is an attack on service availability or denying authorized users access to the service provider. According to CERT/CC [1], it is an explicit attempt to prevent the legitimate user of a service from using that service. This can be categorized into:

- Attempts to "flood" a network, thereby preventing legitimate network traffic.
- Attempts to disrupt connections between two machines, thereby preventing access to a service.
- Attempts to prevent a particular individual from accessing a service.
- Attempts to disrupt service to a specific system or person.

Another term known as Distributed Denial of Services (DDoS) deploys multiple attacking entities (or agents) to attain the same goal. In this attack, the attacker installs DoS software on a number of servers, and these servers in turns attack the target server. The CSI/FBI [2] recent report shows that the most expensive computer crime over the past year was due to denial of service.

Denial of service can result from unintentional action such as error or software bugs. For instance, it reported in Garfinkel and Spaffort [3] that older version of Netscape Navigator HTLM layout engine can be used to allocate gigabytes of memory. More recently, it is reported in US/CERT [4] that several denial-of-service vulnerabilities have been discovered in Cisco's Internet Operating System (IOS). On the other hand, intentional DoS attacks are designed purposely to degrade the performance of the system or bring it to a halt as in Wadlow [5].

II. Vulnerability of Wireless Networks

Vulnerability has been reported in hardware implementations of IEEE802.11 wireless protocol IEEE-SA [8] that allows effective attack against the availability of wireless local area network (WLAN) devices. An attacker using a low powered, portable device such as an electronic PDA and a commonly available wireless networking card may cause significant disruption to all WLAN traffic within range, in a manner that makes identification and localization of the attacker difficult. The vulnerability is related to the medium access control (MAC) function of the IEE 802.11 protocol. WLAN devices perform Carrier Sense Multiple Access with Collision Avoidance (CSMAICA), which minimizes the likelihood of two devices transmitting simultaneously. Fundamental to the functioning of CSMA/CA is the Clear Channel Assessment (CCA) procedure, used in all standard-compliant hardware Spread Spectrum (DSSS) physical (PIE layer. An attack against this vulnerability exploits the CCA function at the physical layer and causes all WLAN nodes within range, both clients and access points (AP), to defer transmission of data for the duration of the attack. When under attack, the device behaves as if the channel is always busy, preventing the transmission of any data over the wireless network. It is reported in Jim [9] that WiFi Protected Access (WPA) is vulnerable to DoS attack. WPA uses mathematical algorithms to authenticate users to the network. If a user is trying to get in and sends two packets of unauthorized data within one second, WPA will assume it is under attack and shut down. A similar report on Wi-Fi's vulnerability can be found in Thomas [10].

Vulnerability was identified in Nortel Networks VPN Router, which may be exploited by remote attackers to cause

Manuscript received April 4, 2012; revised May 18, 2012.

The authors are with the Botho College, Gaborone, Botswana (e-mail: chandarasekaran.namalwar@bothocollege.ac.bw., Tel.: + 267-74703230, fax: + 267-3911252).

a denial of service. Similar vulnerability was identified in Microsoft Internet Explorer, which may be exploited by attackers to cause a denial of service. The flaw resides in the "jscript.dll" file that does not properly handle malformed Javascript "onLoad" events, which may be exploited via a specially crafted HTML page to crash the browser. It is also reported that TCP does not adequately validate segments before updating timestamp value. If an attacker knows (or guesses) the source and destination address and ports of a connection between two peers, he can send spoofed TCP packets to either peer containing bogus timestamp options as reported in French Security Incident Response Team or FrSirt [11]. Examples of DoS attacks on commercial web sites include yahoo, eBay, Amazon, E*Tradet and the like as in CLIPS[12].

III. DoS Attacks

In general, DoS attackers rely on the ability to source spoofed packets to the "amplifiers" in order to generate the traffic which causes the denial of service. Hence, the attacks are commonly launched from systems that are subverted through security related compromises. Regardless of how well secured the victim systems may be, its susceptibility to the attack depends on the state of security in the rest of the global Internet CERT/CC [1]. In generally, DoS exploit weakness in operating system, network interface, and software or Internet protocols. Further, attacker's objectives and interests differ. While some attackers are interested in re-routing messages, others might be interested in disrupting the whole network and degrading its performance or jamming the radio by overloading the system with unwanted messages or packets.

In general, denial-of-service attacks come in a variety of forms and the attackers have variety of objectives. CERT/CC [1] described three basic types of DoS attacks:

- Consumption of scarce, limited, or non renewable resources.
- Destruction or alteration of configuration information
- Physical destruction or alteration of network components.
- Practical implementations of attacks that are DoS in nature or attacks that could lead to subsequently DoS attacks are described below with other variants.

A. ARP Poisoning

In ARP Poisoning, an attacker can exploit ARP Cache Poisoning to intercept network traffic between two, let's say the attacker wants to see all the traffic between hosts A and host B. The attacker begins by sending a malicious ARP "reply" (for which there was no previous request) to host B, associating his computer's MAC address with host A's IP address. Now host B thinks the attacker's computer is host A. Next, the attacker sends a malicious ARP reply to host A, associating his MAC addresses with host B's IP address. Now host A thinks that the hacker's computer is host B. Finally, the hacker turns on an operating system feature called IP forwarding. This feature enables the hacker's machine to forward any network traffic it receives from host A to host B. Instead of enabling IP forwarding the attacker has the choice off drowning host B with any DoS attack, so that the communication actually happens between host A and attacker (whom A thinks to be host B)[26].

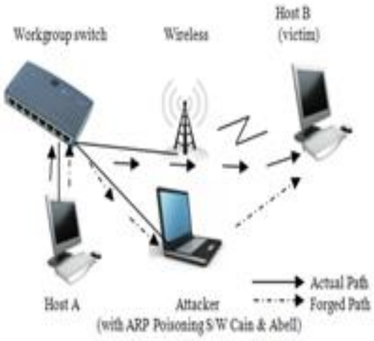

Fig. 1. Implementation of ARP poisoning

In fig.1, the host A has been deceived to send the ICMP help packets to the attacker's computer first instead of communicating with host B. In order to perform ARP poisoning, 2 desktop computers acted as the victims while the laptop acted as the attacker. The attacker laptop was equipped with the Ethereal packet capturing software and an ARP poisoning software known as Cain and Abel. Host A sent continuous ICMP packets to the host B by pinging it. It was observed in the Ethereal software on the attacker's machine that the ICMP packets were sent only between host A and the attacker, even though host A sent it to host B. In Cain and Abel, it was observed that attacker could monitor the ICMP packets sent between those two computers. It showed that the sender has been fooled to send ICMP packets to the attacker, which has a different set of MAC and IP address.

B. MAC Spoofing

In MAC spoofing, the attacker would change the manufacturer-assigned MAC address of a wireless adapter to the MAC address he wants to spoof. Mac makeup was the software we used to perform MAC spoofing. An attacker can learn the MAC address of the valid user by capturing wireless packets using any packet capturing software like Packetyzer, Linkferret or Ethereal by passively or actively observing the traffic. It was observed that upon successful MAC spoofing besides the spoofed MAC address, the IP address assigned to the attacker's computer was identical to the IP address of the victim computer, whose MAC address was being spoofed. In order to access the wireless network, the attacker had to perform DoS attack to disconnect the target computer from its wireless connection. We tested it as follows: The MAC address was spoofed on host A and it sent ICMP packets to host B which is on the same network. Host B used Ethereal to see the packet traffic and saw various packets from host A with spoofed MAC address. Software as previously explained that can be used to obtain user's MAC address is NetStumber. The software can also be used to show the details of different wireless networks.

C. Web Spoofing

In Web spoofing, the attacker convinces the victim that he is visiting a legitimate web site, when the web pages are created by the attacker or even hosted by attacker's web server to eavesdrop the victim. Information such as passwords and credit card numbers can thus be stolen. The attacker can achieve this by compromising the intranet server of company XYZ and redirecting some links to his web server. The other option is to send forged emails (email spoofing) with such links in it.

D. ICMP Flooding

Internet control Protocol or ICMP is used to report the delivery of Internet Protocol (IP) echo packets with an IP network. It can be used for network trouble shooting purposes to show when a particular end station is not responding, when an IP network is not reachable, when a node is overloaded or when an error occurs in the IP header information etc [13]. Typical DoS attack using ICMP is known as ICMP flooding. It involves flooding the buffer of the target computer with unwanted ICMP packets > a. one can enter the target enter the number of ping packets and press the start toggle button, that can be stopped by pressing stop. After ess = k hour, it was found out that the computer browse any websites although it was stir to the wireless network. The excess ICMP packets that flood the target cache buffers have caused this lack of response.

IV. Defense Mechanism

DoS method of attack has been known for some time. Defending against it, however, has been an ongoing concern. Though, there is no known way at present to fully protect systems against DoS attacks, however, measures to reduce or minimize them may include disabling any unused or unneeded network services. This can limit the ability of an intruder to take advantage of those services to execute the attack.

A. Against Spoofing

ARP poisoning or spoofing can easily happen because ARP packets are readily available in wireless networks as they are broadcasted to all without any authentication to all without any authentication mechanism. Use network switches that have MAC binding features that store the first MAC address that appears on a port and do not allow this mapping to be altered without authentication. Another alternative proposal is to make ARP negotiation centralized (say, through a DHCP server and relays with extended facility to answer/forward the ARP packets). Making ARP request unicast can save lot of congestion. Adding authentication to know the identity of the sender or against packet tampering makes it secure. ARP request packets can be sent to a central server which has the IP-MAC address mapping and the server can sent the ARP response with a strong digital signature using a collision free one way has function to the requested host. This can protect against tampering or injection of new forged ARP packets. Lastly the host can send an encrypted acknowledgement with the timestamp of the server response.

V. Conclusion and Results

This paper shows that DoS attacks are much easier to launch on wireless networks than on wired networks. This is typically due to the nature of wireless communication as packets frantically move around in the air. We have comprehensively explained different DoS attacks, some of which we implemented in our lab and also explained a full set of effective defense mechanisms that could help against such attacks.

References

[1] CERT/CC, "Denial of Service Attacks", Available Online.html, 2001.

[2] CSI/FBI, "Computer Crime and Security Survey-Ninth annual Report," 2004.

[3] S. Garfinkel and G. Spafford, "Web Security and Commerce," O'Reilly, USA, 1997.

[4] US/CERT, "Multiple Denial-of-Service Vulnerabilities in Cisco IOS," Available online 2005.

[5] T. A. Wallow, "The Process of Network Security," Allison-Wesley Massachusetts, USA, 2000.

[6] J. Walker, "Unsafe at Any Key Size: An Analyses of WEP encapsulation," Technical Report 03628E.IEEE 802.11 committee

[7] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4," *Proc. Of Selected Areas of Cryptography* (SAC), 2001.

[8] IEEE-SA, Standards Board, IEEE Std IEEE 802.11999 Information Technology- "Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements – part 11: Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specification," Available Online: 802.11-1999.pdf, 1999.

[9] J. Geier, "Denial of Service a Big WLAN Issue," - 2003.

[10] W. Thomas, "Living In Wireless Denial – CIOS must understand Wi-fi's Risks in order to mitigate."

[11] French Security Incident Response Team (FrSirt), "Nortel Networks VPN Router 600 Denial of Service Vulnerability" "Computer Crime and Intellectual Property Section (CLIPS)" *Internet Control Message Protocol* (ICMP).

[12] M. Jelena and R. Peter, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," *ACM SIGCOMM, Computer Communication Review*, 2004, vol. 34, no.2. pp. 39-53.

[13] E. D. Zwicky, S. Cooper, and D. B. Chapman, "Building Internet Firewalls 2e," O'Really, CA, USA, 2000.

[14] McAfee – Personal Firewall and S. Available Axelsson, "Intrusion Detection Systems: A survey and Taxonomy," Tech Report 99-15, Dept. of Comp Eng., Chalmers University, 2000.

[15] Paul Campbell, Ben Calvert, and Steven Boswell, "Security + guide to Network Security fundamentals," *Thomson Course Technology*, 2003, pp. 47-84.

[16] M. Willaimson, "Throttling Viruses: Restricting Propagation to Defeat Malicious Mobile Code."