Analysis of secure routing scheme against vampire attack for Manet

[1]Pratibha Rathore,[2]Ashish Tiwari,[3]Himangni Rathore
[1]Mtech Student,[2]Assistant Proffesor,[3]Employee
[1] *Computer Engineering Department, Vindhya Group of Technology and Science*
Khandwa Road, Indore, India

Abstract **- Defence against Vampire attacks is one of the primary concerns on the Internet today. Vampire attacks are difficult to prevent because of the open, interconnected nature of the Internet and its underlying protocols, which can be used in several ways to deny service. Attackers hide their identity by using third parties such as private chat channels on IRC (Internet Relay Chat). They also insert false return IP address, spoofing, in a packet which makes it difficult for the victim to determine the packet's origin. We propose three novel and realistic traceback mechanisms which offer many advantages over the existing schemes. All the three schemes take advantage of the Autonomous System topology and consider the fact that the attacker's packets may traverse through a number of domains under different administrative control. Most of the traceback mechanisms make wrong assumptions that the network details of a company under an administrative control are disclosed to the public. For security reasons, this is not the case most of the times.**
The proposed schemes overcome this drawback by considering reconstruction at inter and intra AS levels. Hierarchical Internet Traceback (HIT) and Simple Traceback Mechanism (STM) trace back to an attacker in two phases. In the first phase the attack originating Autonomous System is identified while in the second phase the attacker within an AS is identified. Both the schemes, HIT and STM, allow the victim to trace back to the attackers in a few seconds. Their computational overhead is very low and they scale to large distributed attacks with thousands of attackers. Fast Autonomous System Traceback allows complete attack path reconstruction with few packets.

IndexTerms **- MANET, Vampire Attack, Traceback Mechanism, HIT, STM.**

I. INTRODUCTION

Distributed Vampire attacks are one among the most malicious attacks in the Internet today. In a Vampire attack a myriad of compromised systems attack a target, causing it to crash or deny service to legitimate users. Vampire attacks overwhelm the target system with data such that the response time is slowed down or stopped altogether [1]. In order to create the necessary traffic an attacker installs Vampire daemons on a large number of systems (agents). These agents either exploit vulnerabilities present at the victim or overload the victim with inordinate requests. The former attack causes the victim to reboot or crash while the latter causes the victim to utilize some of its critical resources to handle the attack traffic and deny service to legitimate users. There are two broad categories into which the defense against a Vampire attack falls: a) Prevention of the attack from happening b) Detecting the attack traffic and reacting to it. Proactive measures avert host based or network based attacks from compromising systems. Reactive measures constitute of two phases, detection and reaction. In the first phase, the attack is identified using signature detection schemes like Intrusion Detection System and Anomaly Detection. The second phase includes reactive methods such as adhering to the Disaster Recovery Plans of reinstalling OS and applications on compromised systems. Reactive measures like trace back mechanisms play a crucial role when proactive approaches fail to block a malicious attack. Reactive measures may be the only means to identify and shutdown a zombie to prevent any further damage.

II. OVERVIEW

This report, presents three novel and realistic traceback schemes namely Hierarchical IP Traceback (HIT), Fast Autonomous System Traceback (FAST) and Simple Traceback Mechanism (STM). All the approaches employ Autonomous System Border Routers (ASBRs) for marking as they are few in number, more powerful and have higher incentives to implement 3 traceback mechanisms when compared to normal routers. HIT reconstructs to the attacker in two phases, the first phase identifies the attack originating AS and second phase traces the attacker within an Autonomous System. In comparison with Authenticated Marking Scheme (an existing scheme), HIT involves lower overhead, reconstruction time, complexity and requires less number of packets to reconstruct to the attacker. FAST uses a node append mode of marking and requires a very few packets to reconstruct to the attack originating AS. This scheme is very efficient for attackers at large AS path lengths. Simple Traceback Mechanism can identify the attack originating AS in a single packet and the originating attacker in a few tens of packets. This scheme suffers from pollution attacks. As compared to HIT and FAST, STM has lower reconstruction time and computation overhead but suffers from pollution attacks.

III. LITERATURE REVIEW

We do not imply that power draining itself is novel, but rather that these attacks have not been rigorously defined, evaluated, or mitigated at the routing layer. A very early mention of power exhaustion can be found in [68], as “sleep deprivation torture.” As per the name, the proposed attack prevents nodes from entering a low-power sleep cycle, and thus depletes their batteries faster. Newer research on “denial-of-sleep” only considers attacks at the medium access control (MAC) layer [59]. Additional work mentions resource exhaustion at the MAC and transport layers [60, 75], but only offers rate limiting and elimination of

insider adversaries as potential solutions. Malicious cycles (routing loops) have been briefly mentioned [10, 53], but no effective defenses are discussed other than increasing efficiency of the underlying MAC and routing protocols or switching away from source routing. Even in non-power-constrained systems, depletion of resources such as memory, CPU time, and bandwidth may easily cause problems. A popular example is the SYN flood attack, wherein adversaries make multiple connection requests to a server, which will allocate resources for each connection request, eventually running out of resources, while the adversary, who allocates minimal resources, remains operational (since he does not intend to ever complete the connection handshake). Such attacks can be defeated or attenuated by putting greater burden on the connecting entity (e.g. SYN cookies [7], which offload the initial connection state onto the client, or cryptographic puzzles [4, 48, 73]). These solutions place minimal load on legitimate clients who only initiate a small number of connections, but deter malicious entities who will attempt a large number. Note that this is actually a form of rate limiting, and not always desirable as it punishes nodes who produce burst traffic but may not send much total data over the lifetime of the network. Since Vampire attacks rely on amplification, such solutions may not be sufficiently effective to justify the excess load on legitimate nodes .There is also significant past literature on attacks and defenses against quality of service (QoS) degradation, or reduction of quality (RoQ) attacks, that produce long-term degradation in network performance [23, 26, 41, 42, 44, 71, 76]. The focus of this work is on the transport layer rather than routing protocols, so these defenses are not applicable. Moreover, since Vampires do not drop packets, the quality of the malicious path itself may remain high (although with increased latency). Other work on denial of service in ad-hoc wireless networks has primarily dealt with adversaries who prevent route setup, disrupt communication, or preferentially establish routes through themselves to drop, manipulate, or monitor packets [14, 28, 29, 36, 78]. The effect of denial or degradation of service on battery life and other finite node resources has not generally been a security consideration, making our work tangential to the research mentioned above. Protocols that define security in terms of path discovery success, ensuring that only valid network paths are found, cannot protect against Vampire attacks, since Vampires do not use or return illegal routes or prevent communication in the short term.

IV. ACKNOWLEDGMENT

This research paper is made possible through the help and support from everyone, including: parents, teachers, family, friends, and in essence, all sentient beings. I would like to express my deep gratitude to **Mr. Ashish Tiwari**, my research supervisors, for their patient guidance, enthusiastic encourage-ment and useful critiques of this research work.

Finally, I offer my deep gratitude to my parents who have appreciated, encouraged and assisted in our endeavor.

REFERENCES

[1] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing", Proc. 2nd IEEE Wksp. Mobile comp. Sys. And Apps. Feb,1999, pp. 90-100

[2] C.E. Perkins, E. M. Belding-Royer, and S. R. Das, "Ad Hoc On-Demand Distance Vector Routing", IETF RFC 3561, July 2003

[3] D. Remondo , "Tutorial of Wireless Ad Hoc Networks", HET-NETs 2004.

[4] P.Ning, K. Sun, "How to misuse AODV: A Case Study of Insider Attacks Against Mobile Adhoc Routing Protocols", Info Assurance Wksp, IEEE sys, Man and Cybernetics Soc, june 2003, pp. 60-67

[5] Weichao Wang, Yi Lu, Bharat K. Bhargava, "On Vulnerability and Protection of Ad Hoc On-demand Distance Vector Protocol", IEEE Proceedings, 2003, pp. 375-382

[6] Kimaya Sanzgiri, Bridget Dahilly, Brian Neil Leviney, Clay Shieldsz, Elizabeth M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks", Proceedings of the 10th IEEE International Conference on Network Protocols, 2002, pp.1-10

[7] M. Gurrero Zapata and N. Asokan, "Securing Adhoc Routing Protocols", Proceeding 1st ACM Workshop. Wireless Sec., 2002, pp. 1-10.

[8] M. Gurrero Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing, IETF Internet draft, September 2006, pp-1-22

[9] Asad Amir Pirzada, Chris McDonald, "secure Routing with the AODV protocol", Asia-Pacific Conference on Communications, Perth, Western Australia, October 2005. pp. 57-61

[10] K. A. Sivakumar, M. Ramkumar, "Safeguarding Mutable fields in AODV Route Discovery Process", Proceedings of 16th International Conference on ComputerCommunications and Networks, 2007. pp. 645-651

[11] Qing Li, Meiyuan Zhao, Jesse Walker, Yih-Chun Hu, Adrian Perrig, Wade Trappe, "SEAR: A Secure Efficient Ad Hoc On Demand Routing Protocol for Wireless Networks", Proceedings of the 2008 ACM symposium on Information, computer and communications security**,** 2008, pp. 201-204

[12] Davide Cerri, Alessandro Ghioni, "Securing AODV: The A-SAODV Secure Routing Prototype", IEEE Communication Magazine, Volume 46, Issue 2, February 2008 pp.120 – 125

[13] Yuxia Lin, A. Hamed Mohsenian Rad, Vincent W.S. Wong, Joo-Han Song, "Experimental Comparisons between SAODV and AODV Routing Protocols", Proceedings of the 1st ACM workshop on Wireless multimedia networking and performance modeling**,** 2005, pp. 113 – 122

[14] NS Manual, http://www.isi.edu/nsnam/ns/ns documentation.html

[15] Altman, Jimenez, "NS Simulator for Beginners", http://www- sop.inria.fr/maestro/personnel/Eitan.Altman/COURS-NS/n3.pdf.

[16] M. Aziz, M. Al-Akaidi, "Security issues in wireless Ad Hoc Networks and the application to the telecare project", Proceedings of the 15th International Conference on Digital Signal Processing, DSP 2007, pp. 491-494

[17] Lindong Zhou, Zygmunt J. Hass, "Securing Ad Hoc Networks", IEEE Network Magazine, 1999 pp. 1-12

[18] P. Papadimitratos, Z. Haas, "Secure Routing for Mobile Ad Hoc Network", In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), 2002 pp. 1-13

[19] Liu Jinghua, Geng Peng, Qiu Yingqiang, Feng Gui, "A Secure Routing Mechanism in AODV for Ad Hoc Networks", Proceedings of International Symposium on Intelligent Signal Prcessing and Communiction System, 2007 pp. 435-438
[20] Mohammad Ilyas, "The Hand Book of Ad Hoc Wireless Networks", CRC Press LLC.