IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

Detecting and Preventing Traffic Attack through Stepping Stones and Securing the information using watermarking

S. Jayanthi[1] , G. Shamili[2] , R. Sathya[3] , B. Vaidhegi[4]

[1]Department of computer science and engineering /Agni College of Technology/Assistant Professor Chennai, Tamilnadu, India

[2,3,4]Department of Computer Science and Engineering /Agni College of Technology/Final Year Chennai, Tamilnadu, India

Abstract

Network based attackers attack the target directly from their computer, and mostly they perform these kind of attacks through "stepping stones" in order to hide their identity. In order to spot the basis of the attack at the back of stepping stone, it is necessary to compare the incoming and outgoing flows or the connection of a stepping stone.. The earliest work was based on host activity that is log in activities of the host will be traced out. Then it is based on connection content comparison. In this paper we present a method to find the connection of an intruder for tracing back to the origin, and protecting the information from intruders using watermarking.

Keywords*: Network level security and protection, intrusion tracing, stepping stone*.

1. Introduction:

Network based attacks have become a serious risk to the critical information communications to which we depend. Without security measures and controls in place, our information might be subjected to an attack. Some attacks are passive that our information will be monitored by the attacker, and some attacks are active that our information will be altered with intent to corrupt or destroy the data or the network itself. Our network and data are in danger to any of the following types of attacks, if we do not have a security plan, they are 1)eaves dropping; 2)data modification; 3)IP spoofing4)password-based attacks;5)denial-of-service attack, 6)man-in-the-middle attack; 7)compromised-key attack; 8)sniffer attack; 9)application-layer attack; In general, the majority of network communication occur in an unsecured format, which allows an attacker who has gained access to data paths in our network to interpret the traffic. When an attacker is eavesdropping on our communication, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services, our information can be read by others as it traverses the network.

After an attacker has read our data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver. Then about IP spoofing, most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed that the intruder sends messages to a computer that has an IP address that indicates that the messages are coming from a trusted host. After gaining access to the network with a valid IP address, the attacker can modify, delete our data.

Password based attacks is that, when an attacker finds a valid user account, the attacker has the same rights as the real user. After gaining access to our network with a valid account, an attacker can modify server and network configurations, including access controls and routing tables, and modify or delete our data.

Man-in-the-middle attack is that, as the name implies this attack occurs when someone between the sender and receiver is actively monitoring, capturing, and controlling their communication. In our paper we mainly concentrate on overcoming the problem that occurred due to distributed denial-of-service attack (DDoS), DDoS is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted systems.

2 EXISTING SYSTEM

In existing connection correlation are based on three different characteristics,1)host activity; 2)content comparisons; 3)timing characteristics. The host activity approach collects and tracks user login activities at each stepping stones. And the content comparisons is that contents between each stepping stones will be compared. Timing based approach make use the arrival and departure times of packets to correlate connections.

The host activity based approach (DIDS and CIS). DIDS (Distributed Intrusion Detection System) [5] is a system where all TCP connections and logins within the supervised network are monitored and the system keeps track of all the movement and the current states of users. A host monitor resides on each host in the network, gathering audit information about the host, which is transmitted to the central DIDS director, where the network behavior is accounted for. DIDS (Distributed Intrusion Detection System) [5] is a system where all
TCP connections and logins within the supervised network are monitored and the system keeps track of all the movement and the current states of users. A host monitor resides on each host in the network, gathering audit information about the host, which is transmitted to the central DIDS director, where the network behavior is accounted for.

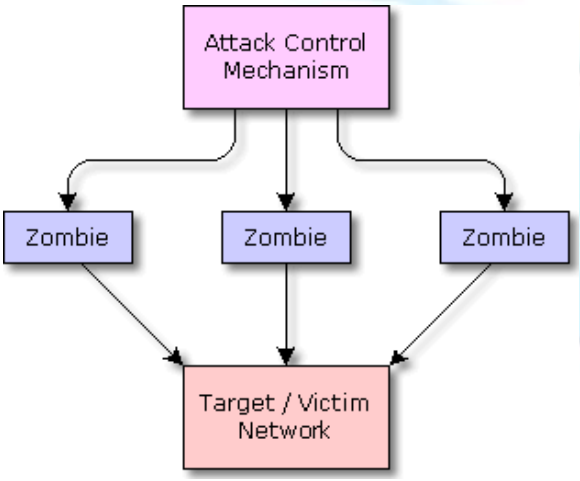

Fig 2.1 Attackers attacking the target

The figure 2.1 shows how that how the attacker attacks the final target, this can be done by that the attacker will be compromising the number of nodes that is a system before attacking the final target. The compromised nodes are known as ZOOBIES.

The fundamental problem with the host-based tracing approach is its trust model. Host-based tracing places its trust upon the monitored hosts themselves. In specific, it depends on the correlation of connections at every host in the connection chain. If one host is compromised and is providing misleading correlation information, the whole tracing system is fooled. Because host-based tracing requires participation and trust of every host involved in the network-based intrusion, it is very difficult to be applied in the context of the public Internet.

One fundamental problem with passive network-based approaches is its computational complexity. Because it passively monitors and compares network traffic, it needs to record all the concurrent incoming and outgoing connections even when there is no intrusion to trace. To correlate at any host in the connection chain, it needs to match every concurrent incoming connection with every concurrent outgoing connection at that host. That is, for a host with m concurrent incoming connections and n concurrent outgoing connections, the passive network-based correlation approach would take $O(m \times n)$ comparisons, in addition to the $O(m+n)$ scanning and recording of concurrent connections.

2.1 Disadvantages of existing system:

The drawbacks of the previous works were that 1) host activity based methods are that the host activity collected from each stepping stone is generally not trustworthy. Since the attacker is assumed to have full control over each stepping stone, he/she can easily modify, delete or forge user login information.2) Since the attacker can easily transform the connection content by encryption at the application layer, these approaches are suitable only for unencrypted connections.3) require a large number of packets in order to correlate timing-perturbed flows.

3. PROPOSED SYSTEM

In proposed system we suggest a watermark-based correlation scheme that is intended purposely to be robust against timing perturbations. Unlike most earlier correlation approaches, our

watermark-based approach is *active*; that is, it embeds a unique watermark into the encrypted flows by somewhat adjusting the timing of chosen packets. The distinctive watermark that is embedded in the encrypted flow gives us a number of advantages over passive timing based correlation in overcoming timing perturbations. First, our active watermark based correlation does not make any limiting assumptions about the distribution of the original inter-packet timing of the packet flow. If the embedded watermark is both unique and robust, the watermarked flows can be effectively identified and thus correlated at each stepping stone.

In compare to nearly all previous passive correlation methods, our watermark-based correlation makes no limiting guess about the distribution or random process of the original inter-packet timing characteristics of the flows to be correlated. We assume the following about the random timing perturbations: 1) While the intruder can insert extra delay to any or all packets of an leaving flow at the stepping stone, the highest delay he or she can introduce is bounded. 2) All packets in the original flow are kept. no packets are dropped from or further added to the flow by the stepping stone. 3) While the watermarking idea is open knowledge, the watermarking embedding and decoding parameters are secrets known only to the watermark embedder and the watermark detector(s). Here we do not need that the packet order of two flows be the similar, as long as the total number of packets is not modified. Our watermark-based approach is able to show a relationship encrypted flows even if chaff and timing perturbation are applied at the same time In difference to all previous passive approaches, our correlation method does not require the random timing perturbation introduced by the attacker to follow any particular distribution or random process to be effective.

3.1 IMPLEMENTATION

In this paper, we propose an attack scheme that compromises timing-based active watermarking trace-back systems by analyzing the packet delays between adjacent stepping stones. We develop a suite of algorithms to infer watermark parameters, recover/duplicate watermarks, and detect the existence of watermarks as early as possible. We also investigate the trade-off between watermark capability and watermark secrecy, and demonstrate that a watermark cannot avoid detection without degradation of its trace-back capability. Our experimental results have confirmed that almost the entire watermark can be recovered or duplicated if the watermark parameters are not selected cautiously. Although our attack focuses on a specific watermarking scheme, it can potentially be extended to compromise other timing-based active watermarking approaches. Our results indicate that the threats of intelligent attackers must be carefully considered for any active trace-back scheme that manipulates packet timing.

The attackers will traced out by using a concept of media access control (MAC). **MAC address is** typically used as a unique identifier for all the nodes on the network. we have found that the distance between the centroids in signal space is a good test statistic for effective attack detection All the Client nodes always login with our Specific IP and MAC address attackers can't easily fake their MAC address so they can avoid IP spoofing attacks In this module ,authentication process will be carried that checking whether he is valid user or not, it is done with the help of MAC address. MAC address is typically used as a identifier for all the nodes on the network.

As already mentioned in this paper we propose a method to avoid DDOS attack, this is done by monitoring all the request from the client When the request is coming, it identifies the IP address with MAC address and stored in cache and starts counting the request from the same IP address and also maintains the timer. More than 50 requests within one second from same IP address are considered as DDOS attack. Then the IP address is blocked for certain time periods (e.g. 5 sec). **Detection:** More than 50 requests within one second from same IP address is considered as DDOS attack. **Prevention:** The suspicious IP address is blocked for certain time periods (e.g. 5 sec)

And then the information will be secured by using watermarking embedding and decoding concept. Generally, watermarking involves the selection of a watermark carrier, and the design of two complementary processes: embedding and decoding. In the registration, we collect the watermark signature... The watermark embedding process inserts the information by a slight modification of some property of the carrier. The

watermark decoding process detects and extracts the watermark (equivalently, determines the existence of a given watermark). To correlate encrypted connections, we propose to use the MAC or IP or User information as the watermark carrier property of interest. The embedded watermark bit is guaranteed to be not corrupted by the timing perturbation. Then by using the correlation analysis the checking process will be carried out whether the information is secured or not, aim to compare and evaluate the correlation effectiveness of our proposed active watermark based correlation and previous passive timing-based correlation under various timing perturbations. By embedding a unique watermark into the inter-packet timing, with sufficient redundancy, we can make the correlation of encrypted flows substantially more robust against random timing perturbations. We can correlate the watermark signatures and identify it's the positive or negative correlation, if positive occurs it detect it is the authenticated user otherwise, if negative occurs it detect it is an Intruder.

3.2 ADVANTAGES

1) Our active watermark-based correlation makes no assumptions about the original distribution of the inter-packet timing of the original packet flow, and it does not require the adversary's timing perturbation to follow any specific distribution or random process to be effective.
2) Our active watermark-based correlation was shown to require substantially fewer packets than a representative passive timing-based correlation method to achieve a given level of robustness.

4.CONCLUSION:

Tracing attackers' traffic through stepping stones is a challenging problem, especially when the attack traffic is encrypted, and its timing is manipulated (perturbed) to interfere with traffic analysis. The random timing perturbation by the adversary can greatly reduce the effectiveness of passive, timing-based correlation techniques. We presented a novel active timing-based correlation approach to deal with random timing perturbations. By embedding a unique watermark into the inter-packet timing, with sufficient redundancy, we can make the correlation of encrypted flows substantially more robust against random timing perturbations. Our analysis and our experimental results confirm these assertions. Our watermark-based correlation is provably effective against correlated random timing perturbation as long as the covariance of the timing perturbations on different packets is fixed.

5.REFERENCES

[1]. Robust Correlation of Encrypted Attack Traffic through Stepping Stones by Flow Watermarking Xinyuan Wang, *Member, IEEE*, Douglas S. Reeves, *Member, IEEE*

[2] X. Wang and D. Reeves. Robust Correlation of Encrypted Attack Traffic through Stepping Stones by Manipulation of Interpacket Delays. In *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS 2003)*, pages 20–29. ACM, October 2003.

[3]. S. Snapp. et al. DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and Early Prototype. In *Proceedings of the 14th National Computer Security Conference*, pages 167–176, 1991.

[4]. P. Peng, P. Ning, D. S. Reeves, On the Secrecy of Timing-Based Active Watermarking Trace-Back Techniques. In *Proceedings of the 2006 IEEE Symposium on Security & Privacy (S&P 2006)*, May 2006.

[5]. Y. Zhang and V. Paxson. Detecting Stepping Stones. In Proceedings of 9th USENIX Security Symposium, 2000

[6]. 8 X. Y. Wang. Survivability through Active Intrusion Response. In Proceedings of 3 rd IEEE Information Survivability Workshop (ISW-2000), October 2000.

[7]. J. Li, M. Sung, J. Xu and L. Li. Large Scale IP Traceback in High-Speed Internet: Practical Techniques and Theoretical Foundation. In *Proceedings of the 2004 IEEE Symposium on Security and Privacy*, IEEE, 2004.

[8].Y. Zhang and V. Paxson. Detecting Stepping Stones. In *Proceedings of the 9th USENIX Security Symposium*, pages 171–184. USENIX, 2000.

[9] L. Zhang, A. G. Persaud, A. Johnson, and Y. Guan. Detection of Stepping Stone Attack under Delay and Chaff Perturbations. In *Proceedings of the 25th IEEE International Performance Computing and Communications Conference (IPCCC 2006)*, April 2006.