Implementation of Network Level Security Process through Stepping Stones by Watermarking Methodology

B. Bazeer Ahamed[1] and S. Hariharan[2]

[1]Department of Information Technology, Pavendar Bharathidasan College of Engineering & Technology, Tiruchirapalli (India)

[2]Department of Computer Science & Enggineering,
TRP Engineering College Tiruchirapalli (India)

bazeerahamed@gmail.com, mailtos.hariharan@gmail.com

Abstract

Network based attacks have become a serious threat to the critical information infrastructure on which we depend .Identifying the source of the attackers behind the stepping stone(s), it is necessary to correlate the incoming and outgoing flows or connections of a stepping stone. To resist attempts at correlation, the attacker may encrypt or otherwise manipulate the connection traffic. Timing based correlation approaches have been shown to be quite effective in correlating encrypted connections. However, timing based correlation approaches are subject to timing perturbations that may be deliberately introduced by the attacker at stepping stones. In this paper we propose a novel watermark-based correlation scheme that is designed specifically to be robust against timing perturbations. Unlike most previous timing based correlation approaches, our watermark-based approach is "active" in that it embeds a unique watermark into the encrypted flows by slightly adjusting the timing of selected packets. The unique watermark that is embedded in the encrypted flow gives us a number of advantages over passive timing based correlation in resisting timing perturbations by the attacker.

***Keywords**: Network Security, Stepping stone, Watermarking methodology, Network based Intrusion*

1. Introduction

Network based attacker's makes a serious threat in a wide computer era, to stop or repel network-based attacks, it is critical to be able to identify the source of the attack [2]. Attackers, however, go to some lengths to conceal their identities and origin, using a variety of countermeasures [5]. As an example, they may spoof the IP source address of the attack traffic. Methods of tracing spoofed traffic, generally known as IP trace back have been developed to address this countermeasure. Another common and effective countermeasure used by network-based intruders to hide their identity is to connect through a sequence of intermediate hosts, or stepping stones, before attacking the final target [7]. For example, an attacker at host A may Telnet or SSH into host B, and from there launch an attack on host C.

In effect, the incoming packets of an attack connection from A to B are forwarded by B, and become outgoing packets of a connection from B to C [9]. The two connections or flows are related in such a case. The victim host C can use IP trace back to determine the second flow originated from host B, but trace back will not be able to correlate that with the attack flow originating from host A. To trace attacks through a stepping stone, it is necessary to correlate the incoming traffic with the outgoing traffic at the stepping stone. This would allow the attack to be traced back to host A in the example [6].

Timing based correlation approaches, however, are sensitive to the use of countermeasures by the attacker, or adversary. In particular, the attacker can perturb the timing characteristics of a connection by selectively or randomly introducing extra delays when forwarding packets at the stepping stones [11]. This kind of timing perturbation will adversely affect the effectiveness of any timing-based correlation. Timing perturbation can either make unrelated flows have similar timing characteristics, or make related flows exhibit different timing characteristics. This will increase the correlation false positive rate, or decrease the correlation true positive rate, respectively [13].

2. Related Works

2.1 Detection of Interactive Stepping Stones

Intruders on the Internet often prefer to launch network intrusions indirectly, i.e., using a chain of hosts on the Internet as relay machines using protocols such as Telnet or SSH. This type of attack is called a stepping-stone attack. The analyze algorithms for stepping-stone detection using ideas from Computational Learning Theory and the analysis of random walks [15]. Our results are the rest to achieve provable (polynomial) upper bounds on the number of packets needed to contently detect and identify encrypted stepping-stone streams with proven guarantees on the probability of falsely accusing non-attacking pairs [13]. Moreover, our methods and analysis rely on mild assumptions, especially in comparison to previous work. We also examine the consequences when the attacker inserts cha into the stepping-stone trac, and give bounds on the amount of cha that an attacker would have to send to evade detection. Our results are based on a new approach which can detect correlation of streams at a one-grained level [17]. Our approach may also apply to more generalized trac analysis domains, such as anonymous communication.

2.2 Encrypted Interactive Stepping Stone Connections

Network intruders often hide their identities by sending attacks through a chain of compromised hosts that are used as “steppingstones”. The difficulty in defending against such attacks lies in detecting stepping-stone connections at the compromised hosts. In this paper, to distinguish normal from attacking connections, [19] we consider strategies that do not depend on the content of the traffic so that they are applicable to encrypted traffic. We propose a low complexity detection algorithm that has no miss detection and an exponentially-decaying false alarm probability. A sequential strategy is then developed to reduce the required number of testing packets.

2.3 A Signal Processing Perspective to Stepping-stone Detection

Malicious use of anonymity techniques makes network attackers difficult to track. The problem is even worse in stepping-stone attacks, where multiple anonymous connections are linked to form an intrusion path. The tracking of a steppingstone attacker requires the detection of all the connection pairs on the intrusion path [2]. The problem of identifying a stepping-stone connection pair at an intermediate host. We formulate the problem as one of nonparametric hypotheses testing. Our attacker model allows the attacker to encrypt the traffic and modify the timing. We propose two algorithms which do not depend on the content of the traffic. Our techniques only make generic assumptions such as delay or memory constraints, and therefore they are applicable in most practical systems [4]. We show that our algorithms can detect all the stepping-stone connections while falsely accusing normal traffic with exponentially-decaying probabilities

3. Problem Definition

Existing connection correlation approaches are based on three Different characteristics:

- ✓ host activity;
- ✓ connection content (i.e. packet payload);
- ✓ Inter-packet timing characteristics. The host activity based approach collects and tracks users' login activity at each stepping stone.

The major drawback of host activity based methods is that the host activity collected from each stepping stone is generally not trustworthy [14]. Since the attacker is assumed to have full control over each stepping stone, he/she can easily modify, delete or forge user login information. This defeat the ability to correlate based on Host activity.

4. Methodology

The objective of watermark-based correlation is to make the correlation of encrypted connections probabilistically robust against random timing perturbations by the adversary. Unlike existing timing-based correlation schemes, our watermark-based correlation is active in that it embeds a unique watermark into the encrypted flows [6], by slightly adjusting the timing of selected packets. If the embedded watermark is both unique and robust, the watermarked flows can be effectively identified and thus correlated at each stepping stone.

- ➢ While the attacker can add the secret key in watermarking, we can easily analysis and identify the intruder.
- ➢ All packets in the original flow are kept. No packets are dropped from or added to the flow by the stepping stone.
- ➢ While the watermarking scheme is public knowledge, the watermarking embedding and decoding parameters are secrets known only to the watermark embedded and the watermark detector(s).

These proposed are used in different application like LAN Security, Illegal Network sharing prevention, Attackers detected accurately.

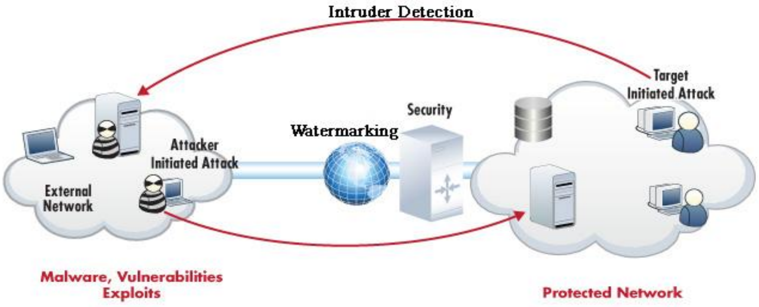

Figure 1. Architecture Diagram of Watermarking Methodology

5. Experimental Results and Analysis

The probability of detecting real edge points should be maximized while the probability of falsely detecting non-edge points should be minimized [8]. This corresponds to maximizing the signal-to-noise ratio.

5.1 Watermark Bit Embedding And Decoding

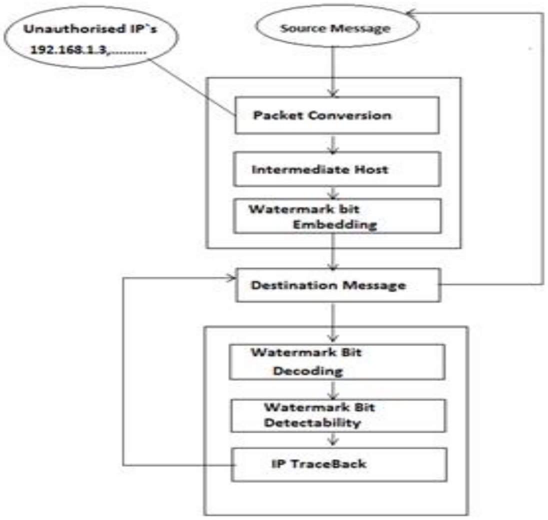

Figure 2. Watermarking Methodology through Stepping Stone Process

5.2. Correlation Analysis

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 [10]. 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 inter-packet timing as the watermark carrier property of interest. The embedded watermark bit is guaranteed to be not corrupted by the timing perturbation [3]. If the perturbation is outside this range, the embedded watermark bit may be altered by the attacker.

5.3. Watermark Tracing Model

In practice, the number of packets available is the fundamental Limiting factor to the achievable effectiveness of our watermark based correlation [12]. This set of experiments 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 [1]. 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.

The watermark tracing approach exploits the observation that interactive connections are bidirectional. The idea is to watermark the backward traffic (from victim back to the attacker) of the bidirectional attack connections by slightly adjusting the timing of selected packets [14, 5]. If the embedded watermark is both robust and unique, the watermarked back traffic can be effectively correlated and traced across stepping stones, from the victim all the way back to the attacker, assuming the attacker has not gained full control on the attack target, the attack Target will initiate the attack tracing after it has detected the attack. Specifically, the attack target will watermark the backward traffic of the attack connection, and inform across the network about the watermark. The stepping stone across the network will scan all traffic for the presence of the indicated watermark, and report [16]. To the target if any occurrences of the watermark are detected.

5.4. Parameter & Mapping Randomization

One simple technique to achieve this is to use a secret key to generate a pseudo-random sequence of numerical values and add them to either or both of and for the pixels in the watermarking area. This technique is hereinafter referred to as parameter randomization [7].

This parameter exchanges does not affect the effectiveness of lossless recoverability, because we can now recover the original pixel values by the compound mappings. We will refer to this technique in the sequel as mapping randomization [20]. We may also combine this technique with the parameter randomization technique to enhance the security. Finally, the Authenticated user takes the file in zip format with proper password.

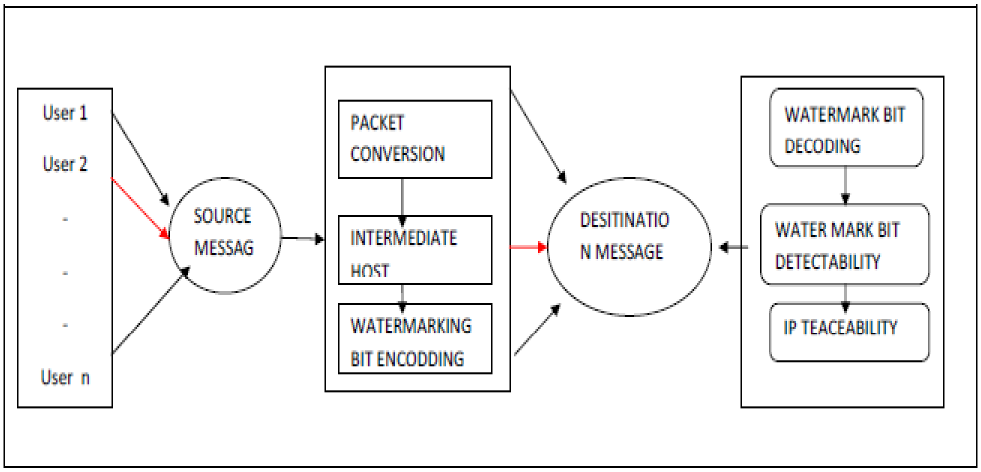

Figure 3. Transmission of Message from Source to Destination

6. Conclusion and Future Enhancement

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. Specifically, the proposed watermark-based correlation can, with arbitrarily small average time adjustment, achieve arbitrarily close to 100% watermark detection (correlation true positive) rate and arbitrarily close to 0% collision (correlation false positive) probability at the same time against arbitrarily large (but bounded) random timing perturbation of arbitrary distribution (or process), as long as there are enough packets in the flow to be watermarked. Compared with previous passive correlation approaches, our active watermark-based correlation has several advantages.

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.

- We presented a novel active timing-based correlation approach to deal with random timing perturbations.
- The effectiveness of our active watermark-based correlation can be modeled more accurately.
- Our experimental results validate the accuracy of these tradeoff models.

References

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

[2] X. Wang, S. Chen and S. Jajodia, "Network Flow Watermarking Attack on Low-Latency Anonymous Communication Systems", In Proceedings of the 2007 IEEE Symposium on Security & Privacy (S&P 2007), **(2007)** May.

[3] B. D. Song and S. Venkataraman, "Detection of Interactive Stepping Stones: Algorithms and Confidence Bounds", In Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID 2004), Springer, **(2004)** October.

[4] P. Danzig and S. Jamin, "Tcplib: A Library of TCP Internetwork Traffic Characteristics", Technical Report USC-CS-91-495, University of Southern California, **(1991)**.

[5] P. Danzig, S. Jamin, R. Cacerest, D. Mitzel and E. Estrin, "An Empirical Workload Model for Driving Wide-Aea TCP/IP Network Simulations", Journal of Internetworking, vol. 3, no. 1, **(1992)** March, pp. 1–26.

[6] D. Donoho, et al., "Multiscale Stepping Stone Detection: Detecting Pairs of Jittered Interactive Streams by Exploiting Maximum Tolerable DeLay", In Proceedings of the 5th International Symposium on Recent Advances in Intrusion Detection (RAID 2002): LNCS vol. 2516, Springer, **(2002)** October, pp. 17–35.

[7] M. T. Goodrich, "Efficient packet marking for large-scale ip traceback", In Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS 2002), ACM, **(2002)** October, pp. 117–126.

[8] T. He and L. Tong, "Detecting Encrypted Stepping-Stone Connections", In IEEE Transactions on Signal Processing, vol. 55, no. 5, **(2006)**, pp. 1612-1623.

[9] G. Kramer, "Generator of Self-Similar Network Traffic", http://wwwcsif.cs.ucdavis.edu/ Kramer/code/ trf gen2.html.

[10] P. Moulin, "Information-Hiding Games", In Proceedings of International Workshop on Digital Watermarking (IWDW 2003), LNCS vol. 2613, **(2003)** May.

[11] P. Moulin and J. A. O'Sullivan, "Information-Theoretic Analysis of Information Hiding", In IEEE Transaction on Information Theory, vol. 49, no. 3, **(2003)** March, pp. 563–593.

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

[13] P. Peng, P. Ning, D. Reeves and X. Wang, "Active Timing-Based Correlation of Perturbed Traffic Flows with Chaff Packets", In Proceedings of the 2nd International Workshop on Security in Distributed Computing Systems (SDCS-2005), **(2005)** June.

[14] Y. J. Pyun, Y. H. Park, X. Wang, D. S. Reeves and P. Ning, "Tracing Traffic through Intermediate Hosts that Repacketize Flows", In Proceedings of the 26th Annual IEEE Conference on Computer Communications (Infocom 2007), **(2007)** May.

[15] S. Savage, D. Wetherall, A. Karlin and T. Anderson, "Practical Network Support for IP Traceback", In Proceedings of ACM SIGCOMM 2000, ACM, **(2000)** September, pp. 295–306.

[16] E. Shannon, "A Mathematical Theory of Communication", In Bell System Technical Journal, vol. 27, **(1948)** July and October, pp. 379–423 and 623-656.

[17] S. Staniford-Chen and L. Heberlein, "Holding Intruders Accountable on the Internet", In Proceedings of the 1995 IEEE Symposium on Security and Privacy, IEEE, **(1995)**, pp. 39-49.

[18] M. S. Taqqu, W. Willinger and R. Sherman, "Proof of a Fundamental Result in Self-Similar Traffic Modeling", ACM Computer Communication Review, vol. 27, (1997), pp. 5-23.

[19] X. Wang, S. Chen and S. Jajodia, "Network Flow Watermarking Attack on Low-Latency Anonymous Communication Systems", In Proceedings of the 2007 IEEE Symposium on Security & Privacy (S&P 2007), **(2007)** May.

[20] 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), ACM, **(2003)** October, pp. 20-29.