INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2873 - 2879
RECEIVED : 25.02.2018 PUBLISHED : 21.03.2018

March 21, 2018

POWERFUL RELATIONSHIP FOR ENCRYPTED BARRAGE TRAFFIC THROUGH STEPPING MOVE BY SEQUENCE WATERMARK

Ms.A.Malini.,M.Sc (computer science) IInd year.
Asst. Prof.S.Lalitha.,M.Phil.,M.Tech.,
Department of Computer Science, Kamban Arts And Science College for Women, Thiruvannamalai.

ABSTRACT:

Network based intruders seldom attack their victims directly from their own computer. Often, they stage their attacks through intermediate “stepping stones” in order to conceal their identity and origin. To identify the source of the attack 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 project, 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. A two-fold monotonically increasing compound mapping is created and proved to yield more distinctive visible watermarks in the watermarked image. Security protection measures by parameter and mapping randomizations have also been proposed to deter attackers from illicit image recoveries.

1. INTRODUCTION

NETWORK based attacks have become a serious threat to the critical information infrastructure on which we depend. To stop or repel network-based attacks, it is critical to be able to identify the source of the attack. Attackers, however, go to some lengths to conceal their identities and origin, using a variety of countermeasures. In this paper, we address the random timing perturbation problem in correlating encrypted connections through stepping stones. Our goal is to develop an efficient correlation scheme that is probabilistically robust against random timing perturbation, and to answer fundamental questions concerning the effectiveness of such techniques and the tradeoffs involved in implementing them. We propose a watermark-based correlation scheme that is designed specifically to be robust against timing perturbations by the adversary. Unlike most previous correlation approaches, our watermark-based approach is *active*; that is, 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 overcoming timing perturbations by the adversary.

First, our active watermark based correlation does not make any limiting assumptions about the distribution or random process of the original inter-packet timing of the packet flow, or the distribution of random delays an adversary can add. This is in contrast to existing passive timing based correlation approaches. Second, our method requires substantially fewer packets in the flow to achieve the same level of correlation effectiveness as existing passive timing based correlation, despite arbitrarily large (but bounded) timing perturbation of arbitrary distribution by the adversary. To the best of our knowledge, our work is the first that identifies 1) the accurate quantitative tradeoffs between the achievable correlation effectiveness and the defining characteristics of the timing perturbation; 2) a provable upper bound on the number of packets needed to achieve desired correlation effectiveness, given a bound on the amount of timing perturbation.

2. STUDY OF EXISTING SYSTEM

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.

Disadvantages: The major drawback of host activity based methods is 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. This defeat the ability to correlate based on Host activity.

3. PROPOSED SYSTEM

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, by slightly adjusting the timing of selected packets.

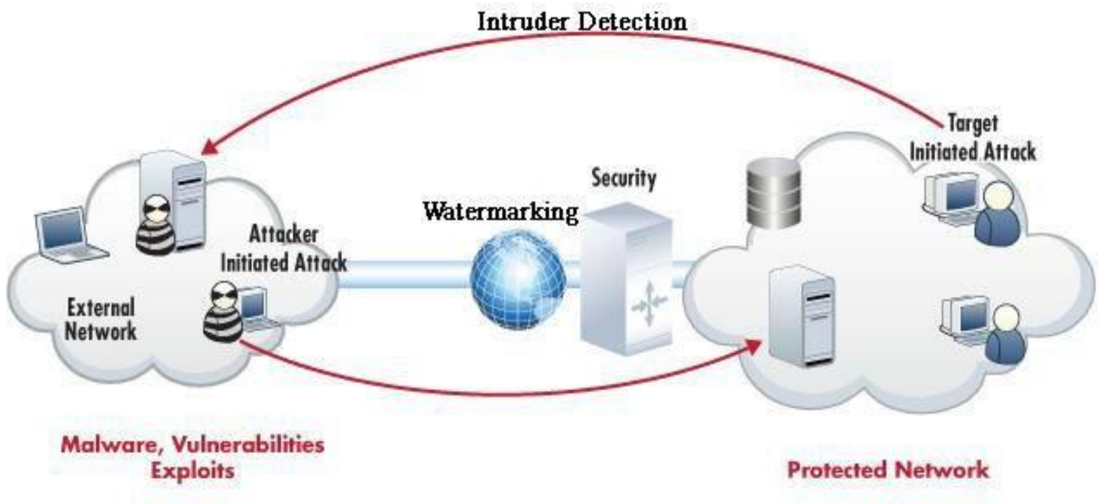
If the embedded watermark is both unique and robust, the watermarked flows can be effectively identified and thus correlated at each stepping stone.

Advantages: 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 parameterrs are secrets known only to the watermark embedder and the watermark detector(s).

4. ARCHITECTURE FOR WATERMARK-BASED CORRELATION



5. IMPLEMENTATION

1) Watermark Bit Embedding and Decoding: 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 inter-packet timing as the watermark carrier property of interest. The embedded watermark bit is guaranteed to be not corrupted by the timing perturbation. If the perturbation is outside this range, the embedded watermark bit may be altered by the attacker.

2) Correlation Analysis: In practice, the number of packets available is the fundamental Limiting factor to the achievable effectiveness of our watermark based correlation. 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. 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) Watermark Tracing Model: 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. 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 To the target if any occurrences of the watermark are detected.

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. This parameter exchange 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. We may also combine this technique with the parameter randomization technique to enhance the security. Finally, the Authenticated user take the file in zip format with proper password.

6. EXPERIMENTS

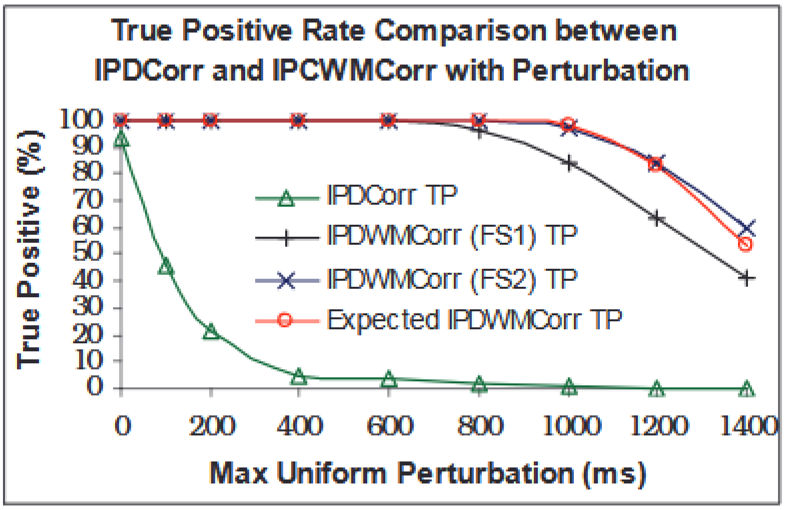
The goal of the experiments is to answer the following questions about watermark-based correlation (as well as existing timing-based correlation) in the face of random timing perturbation by the attacker:

1) How vulnerable are existing (passive) timing-based correlation schemes to random timing perturbations?
2) How robust is watermark-based correlation against random timing perturbations?
3) How effective is watermark-based correlation in correlating the encrypted flows that are perturbed in timing?
4) What is the collision (false positive) rate of watermark-based correlation?
5) How well do the models of watermark bit robustness, watermark detection rate and watermark collision rate predict the measured values?

We have used two flow sets, labeled FS1 and FS2 in our experiments. FS1 is derived from over 49 million packet headers of the Bell Labs-1 Traces of NLANR. It contains121 SSH flows that have at least 600 packets and that are at least 300 seconds long. FS2 contains 1000 telnet flows generated from an empirically-derived distribution of telnet packet inter-arrival times, using the tcplib tool.

Correlation True Positive Experiment:

To answer the first three questions, we have conducted the following experiment. First, we used an existing, passive timing-based correlation method called IPD-Based Correlation to correlate each flow in FS1 with the same flow, after the inter packet delays of the flow have been randomly perturbed. If the flow and the perturbed flow are reported correlated, it is considered a true positive (TP) of the correlation in the presence of timing perturbation. Second, we embedded a random 24-bit watermark into each flow of FS1 and FS2, with redundancy number m=12, and quantization step size s=400ms for each watermark bit.



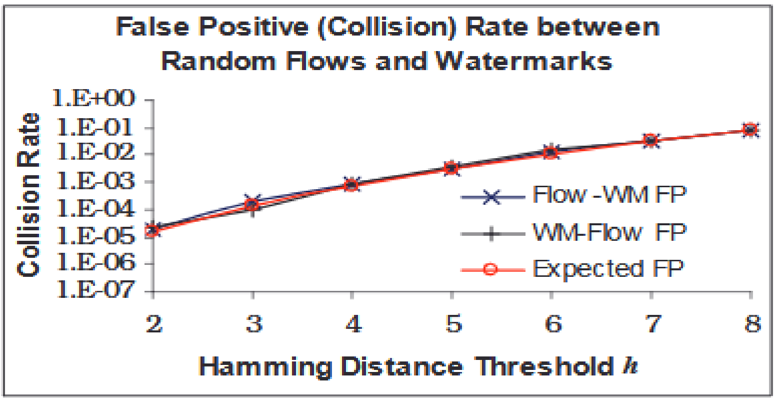
Correlation True Positive Rates under Random Timing Perturbs

Above diagram shows the average of 100 separate experiments measuring the true positive rates of IP D-based Correlation and watermark-based correlation on FS1 and FS2. The results clearly indicate that IPD-based correlation is vulnerable to even moderate random timing perturbation. Without timing perturbation, IPD-based correlation is able to successfully correlate 93.4% of the SSH flows of FS1. However, with a maximum 100ms random timing perturbation, the true positive rate of IPD-based correlation drops to 45.5%, and for a 200ms maximum delay, the rate drops to 21.5%.

Correlation False Positive Experiment:

As explained above, there is a non-zero probability that an un-watermarked flow will happen to exhibit the randomly chosen watermark. This case is considered a correlation collision, or false positive. According to our correlation collision model, the collision rate is determined by the number of watermark bits land the Hamming distance threshold h. We there for experimentally investigated the following, for varying values of the Hamming distance threshold h:

1) Collision rates between a given flow and 10,000~1,000,000 randomly generated 24-bit watermarks.
2) Collision rates between a given 24-bit watermark and 10,000~1,000,000 randomly generated (using tcplib) telnet flows.



Correlation False Positive (Collision) Rate vs Hamming Distance Threshold *h*

The measured collision rates and expected values are very close, validating our model. In addition, the results show that the collision rate can be controlled to a low value by appropriate selection of the Hamming distance threshold.

7. 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 an 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.

8. REFERENCES

1. Amichai-Hamburger, Y., Fine, A., & Goldstein, A. (2004). The impact of Internet interactivity and need for closure on consumer preference. **Computers in Human Behavior, 20,** 103-117.
2. Balabanis, G., Reynolds, N., & Simintiras, A. (2006). Bases of e-store loyalty: Perceived switching barriers and satisfaction. **Journal of Business Research, 59,** 214-224.
3. F. Baboescu, S. Singh, and G. Varghese, "Packet classification for core routers: Is there an alternative to cams," in *Proc. IEEE INFOCOM*, 2003.
4. F. Baboescu and G. Varghese, "Scalable packet classification," in *Proc. ACM SIGCOMM*, 2001, pp. 199–210.
5. N. Bar-Yosef and A. Wool, "Remote algorithmic complexity attacks against randomized hash tables," in *Proc. International Conference on Security and Cryptography (SECRYPT)*, Barcelona, Spain, Jul. 2007, pp. 117–124.
6. M. M. Buddhikot, S. Suri, and M. Waldvogel, "Space decomposition techniques for fast Layer-4 switching," in *Protocols for High Speed Networks IV*, Aug. 1999, pp. 25–41.

7. W. R. Cheswick, S. M. Bellovin, and A. Rubin, *Firewalls and Internet Security: Repelling the Wily Hacker*, 2nd ed. Addison- Wesley, 2003.
8. M. Christiansen and E. Fleury, "Using interval decision diagrams for packet filtering," 2002, http://www.cs.auc.dk/_fleury/publications.html.
9. E. Cohen and C. Lund, "Packet classification in large ISPs: Design and evaluation of decision tree classifiers," in *Proc. ACM SIGMETRICS*. New York, NY, USA: ACM Press, 2005, pp. 73–84.
10. S. Crosby and D. Wallach, "Denial of service via algorithmic complexity attacks," in *Proceedings of the 12th USENIX Security Symposium*, August 2003, pp. 29–44.
11. M. de Berg, M. van Kreveld, and M. Overmars, *Computational Geometry: Algorithms and Applications*, 2nd ed. Springer-Verlag, 2000.
12. P. B. Danzig and S. Jamin. tcplib: A Library of TCP Internetwork Traffic Characteristics. USC Technical Report, USC-CS-91--495.
13. P. B. Danzig, S. Jamin, R. Cacerest, D. J. Mitzel and E. Estrin. An Empirical Workload Model for Driving Wide-Area TCP/IP Network Simulations. In Journal of Internetworking 3:1, pages 1--26 March 1992.
14. M. H. DeGroot. Probability and Statistics. Addison-Wesley Publishing Company, 1989.
15. D. Donoho, A.G. Flesia, U. Shanka, V. Paxson, J. Coit and S. Staniford. 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), October, 2002. Springer Verlag Lecture Notes in Computer Science,