ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Implementation of Active Watermark-Based Correlation Framework Developed Exclusively To Be Robust Against Timing Perturbations

Sharmila.M
M.Tech (CSE)
Department of CSE,
VITAM College of Engineering,
Andhra Pradesh, India.

M.Srinivasa Rao, M.Tech
Associate Professor & HoD,
Department of CSE,
VITAM College of Engineering,
Andhra Pradesh, India.

Abstract:

Network security consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.

Network security is complex and challenging problem in today's world. Despite of many sophisticated techniques, attack on the network continues to increase. At present, in order to hide the identity of the attacker, attackers send their attack through a chain of compromised hosts that are used as "stepping stones". In this paper we present an approach to find the connection chain of an intruder for tracing back to the origin especially if the attack through the traffic is encrypted one. Our approach will based on analyzing correlations of encrypted connection between number of packets sent in outgoing connections and that of the incoming packets in the connection. We proposed a correlation scheme based on watermarking which will be robust against timing perturbation. This approach yields effective better results in terms of number of packets than in existing passive timing based correlation. This paper presents a new method of embedding a watermark in traffic flow. Here for the purpose of embedding the watermark, the packet timing is adjusted for specific intervals. By slightly changing the packet timing, we achieve robust correlation of encrypted network against random timing perturbation.

Keywords - ***Correlation, IPD, Robustness, Stepping stones, Watermark***

INTRODUCTION

Networks are subject to attacks from malicious sources. Attacks can be from two categories: "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation. 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.

Literature Survey

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system.
We have to analysis the secure computing.

Data centre Security?

- Professional Security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means.
- When an employee no longer has a business need to access datacenter his privileges to access datacenter should be immediately revoked.
- All physical and electronic access to data centers by employees should be logged and audited routinely.
- Audit tools so that users can easily determine how their data is stored, protected, used, and verify policy enforcement.

Data Location:

- When user uses the cloud, user probably won't know exactly where your data is hosted, what country it will be stored in?
- Data should be stored and processed only in specific jurisdictions as define by user.
- Provider should also make a contractual commitment to obey local privacy requirements on behalf of their customers.
- Data-centered policies that are generated when a user provides personal or sensitive information, that travels with that information throughout its lifetime to ensure that the information is used only in accordance with the policy

Backups of Data:

- Data store in database of provider should be redundantly store in multiple physical locations.
- Data that is generated during running of program on instances is all customer data and therefore provider should not perform backups.
- Control of Administrator on Databases.

Data Sanitization:

- Sanitization is the process of removing sensitive information from a storage device.
- What happens to data stored in a cloud computing environment once it has passed its user's "use by date"
- What data sanitization practices does the cloud computing service provider propose to implement for redundant and retiring data storage devices as and when these devices are retired or taken out of service.

Network Security:

- Denial of Service: where servers and networks are brought down by a huge amount of network traffic and users are denied the access to a certain Internet based service.
- Like DNS Hacking, Routing Table "Poisoning", XDoS attacks.
- QOS Violation: through congestion, delaying or dropping packets, or through resource hacking.
- Man in the Middle Attack: To overcome it always use SSL.
- IP Spoofing: Spoofing is the creation of TCP/IP packets using somebody else's IP address.
- Solution: Infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.

How secure is encryption Scheme:

- Is it possible for all of my data to be fully encrypted?
- What algorithms are used?
- Who holds, maintains and issues the keys? Problem:
- Encryption accidents can make data totally unusable.
- Encryption can complicate availability Solution.
- The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists.

Information Security:

- Security related to the information exchanged between different hosts or between hosts and users.
- This issues pertaining to secure communication, authentication, and issues concerning single sign on and delegation.
- Secure communication issues include those security concerns that arise during the communication between two entities.
- These include confidentiality and integrity issues. Confidentiality indicates that all data sent by users should be accessible to only "legitimate" receivers, and integrity indicates that all data received should only be sent/modified by "legitimate" senders.
- Solution: public key encryption, X.509 certificates, and the Secure Sockets Layer (SSL) enables secure authentication and communication over computer networks.

Existing System

Existing connection correlation approaches are based on three Different characteristics:
1) Host activity;
2) Connection content (i.e. packet payload);
3) Inter-packet timing characteristics.

Disadvantages of Existing System:

1) The major drawback of host activity based methods is that the host activity collected from each stepping stone is generally not trustworthy.
2) 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.

IJMETMR
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Proposed System:

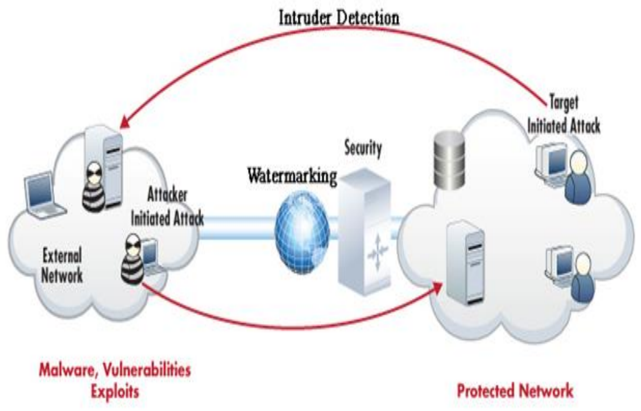
The objective of watermark-based correlation is to make the correlation of encrypted connections probabilistically robust against random timing perturbations by the adversary.

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 of Proposed System:

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

Architecture:



Algorithm:

Detection algorithm:

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

Let ±*i* be the delay added to packet *Pi*, and *t0 i* be the distorted time stamp of packet *Pi*, then *t0 i* = *ti* + ±*i*. The original and distorted inter-packet delays (IPD) between *Pi*+1 and *Pi* are *Ii* =*ti*+1 ¡ *ti* and *I0 i* = *t0 i*+1 ¡ *t0 i* respectively. Therefore, *k* = *t0k* ¡ *tk* = ±1 +*k*X¡1*i* = 1(*I0i* ¡ *Ii*) The original and the perturbed inter-packet timing characteristics of packet flow *P*1*; : : : ; Pn* can be represented by < *t*1*; I*1*; : : : ; In*¡1 > and < *t0*1*; I0*1 *; : : : ; I0n*¡1
According to results from section VI-A, in order to completely remove any hidden information from the original inter packet timing characteristics, the adversary needs to disturb < *t*1*; I*1*; In*¡1 > into an independent one. That means < *I0*1 *; : : : ; I0n*¡1 > needs to be independent from < *I*1*; : : : ; In*¡1 >.

Therefore, the distortion pattern < *I0*1*; : : : ; I0n*¡1 > can be thought to be pre-determined before the original inter-packet timing characteristics > respectively. In, particular, < *I0*1*; I0n*¡1 > represents the distortion pattern over the original inter-packet timing characteristics.

Modules Description:

- Watermark Bit Embedding and Decoding
- Correlation Analysis
- Watermark Tracing Model
- Parameter & Mapping Randomization

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.

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.

Future Enhancements:

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 stones.

REFERENCES

[1] A. Blums, D. Song, and S. Venkataraman, "Detection of Interactive Stepping Stones: Algorithms and Confidence Bounds," Proc. Seventh Int'l Symp. Recent Advances in Intrusion Detection (RAID '04), Oct. 2004.

[2] R.C. Chakinala, A. Kumarasubramanian, R. Manokaran, G. Noubir, C. Pandu Rangan, and R. Sundaram, "Steganographic Communication in Ordered Channels," Proc. Eighth Information Hiding Int'l Conf. (IH '06), 2006.

[3] T.M. Cover and J.A. Thomas, Elements of Information Theory. John Wiley & Sons, Inc., 1991.

[4] I. Cox, M. Miller, and J. Bloom, Digital Watermarking. Morgan-Kaufmann Publishers, 2002.

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

[6] P. Danzig, S. Jamin, R. Cacerest, D. Mitzel, and E. Estrin, "An Empirical Workload Model for Driving Wide-Area TCP/IP Network Simulations," J. Internetworking, vol. 3, no. 1, pp. 1-26, Mar. 1992.

[7] M. DeGroot, Probability and Statistics. Addison-Wesley Publishing Company, 1989.

[8] D. Donoho et al, "Multiscale Stepping Stone Detection: Detecting Pairs of Jittered Interactive Streams by Exploiting Maximum Tolerable Delay," Proc. Fifth Int'l Symp. Recent Advances in Intrusion Detection (RAID '02), pp. 17-35, Oct. 2002.

[9] M.T. Goodrich, "Efficient Packet Marking for Large-Scale IP Traceback," Proc. Ninth ACM Conf. Computer and Comm. Security (CCS '02), pp. 117-126, Oct. 2002.

[10] T. He and L. Tong, "Detecting Encrypted Stepping-Stone Connections" IEEE Trans. Signal Processing, vol. 55, no. 5, pp. 1612-1623, May 2006

Author details

Sharmila.M is pursuing his M.Tech in Computer Science and Engineering from VITAM College of Eng affiliated to JNTU Kakinada. She received his B.Tech degree from VITAM College of Engg, JNTU Kakinada, and Andhra Pradesh, India.

Molli Srinivasa Rao is pursuing his Ph.D from Andhra University. He received his M.Tech in Computer Science and Technology from Andhra University in 2003. He received his B.Tech degree from C.B.I.T., Hyderabad in 2001. He is currently working as Associate Professor, CSE Dept. in VITAM College of Engg., Andhra Pradesh, India. His Research Interests include mobile Ad-hoc Networks, Sensor Networks, Wireless Mesh Networks, computer and network security.