Stepping Stone Technique for Monitoring Traffic Using Flow Watermarking

S.R. Ramya
Department of CSE
PPG Institute of Technology
Coimbatore, Tamilnadu, India

A. Reyana
Department of CSE
PPG Institute of Technology
Coimbatore, Tamilnadu, India

Abstract : The proposed system describes a watermarking technique on ownership authentication providing secured transactions. The unique watermark signature is invisible. The specific request preferred by the user is identified by the watermark extraction procedure, which identifies the signature and returns the user requested data with a proper secret key, indicating authorized user. The watermark extraction algorithm returns an error that tells impostor user. Here it requires a unique signature during both the insertion and the request procedures, thus the user remains unauthorized until it passes the signature validation test. Here the versions of signature and secret key techniques are followed.

Keywords – Perturbation, Embedding, Correlation, Extraction, validation

1. INTRODUCTION

Today, creators and owners of digital video ,audio, document and images fears to put their multimedia data over the Internet, because there is no way to track the illegal distribution and violation of protection. Without mechanisms to support the above requirements, owners cannot generate proof that somebody else violated law. The techniques that have been proposed for solving this problem are collectively called unique digital watermarking. Unique digital watermarking refers to the embedding of unobtrusive marks or labels that can be represented as bits in digital content. The method also provides a unique way for propagating information in the form of an encrypted document. Existing connection correlation approaches are based on three different characteristics: 1) host activity; 2) connection content; and 3) inter-packet timing characteristics. The host activity based approach collects and tracks users login activity at each stepping stone, therefore not trustworthy as the attacker is assumed to have full control over each stepping stone, he/she can easily modify, delete or forget user login information. Content based correlation approaches require that the payload of packets remains invariant across stepping stones. And the attacker can easily transform the connection content by encryption at the application layer; these approaches are suitable only for unencrypted connections. The traffic timing based approaches monitors the arrival or departure times of packets, and uses this information to correlate incoming and outgoing flows of a stepping stone.

2. PROPOSED SYSTEM

The proposed system has a robust technique that is unique watermarking and image authentication schemes. The proposed scheme includes two parts. The first is a unique watermarking which will be embedded into image for ownership authentication. The second is a signature verification process, which can be used to prove the integrity of the image. The unique signature will be extracted from the image. The signature is verified when the image is incidentally damaged such as loss compression thus provides a high degree of robustness against the attacker, the attacker can add the secret key in watermarking, which can be easily analyzed to identify the intruder. Thus all the packets in the original flow are kept and no packets are dropped from or added to the flow by the stepping stone. Attackers commonly relay their traffic through a number of (usually compromised) hosts in order to hide their identity. Detecting such hosts, called stepping stones, is therefore an important problem in computer security. The detection proceeds by finding correlated flows entering and leaving the network. Traditional approaches have used patterns inherent in traffic flows, such as packet timings, sizes, and counts, to link an incoming flow to an outgoing one rather than storing or communicating traffic patterns, all the necessary information is embedded in the flow itself. This, however, comes at a cost: to ensure robustness.

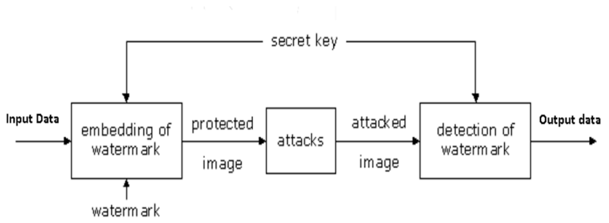

Fig 1. Correlation Analysis

3. SYSTEM DESCRIPTION

3.1 Watermark Bit Embedding And Decoding

Watermarking bit embedding involves the selection of a watermark carrier embeds with unique watermark signature. At the time of user registration, it collects the unique watermarking signature from the user. This process embeds the signature by a slight modification of some property of the carrier. The embedded bit watermark is guaranteed to be not corrupted by the timing perturbation. The watermark is subsequently embedded by delaying the packets by an amount such that the IPD of the watermarked packet.

The IPD is conceptually a continuous value; it first quantizes the IPD before embedding the watermark bit. Given any IPD ipd > 0, we define the quantization of ipd with uniform quantization step size s > 0 as the function q (ipd, s) = round (ipd/s) - - (1) where round(x) is the function that rounds off real number x to its nearest integer. The quantization for scalar x. It is easy to see that q (k s, s) = q (k s + y, s) for any integer k and any y [-s/2, s/2). Let ipd denote the original IPD before watermark bit w is embedded, and ipdw denote the IPD after watermark bit w is embedded. To embed a binary digit or bit w into an IPD, we slightly adjust that IPD such that the quantization of the adjusted IPD will have w as the remainder when the modulus 2 is taken. Given any ipd > 0; s > 0 and binary digit w, the watermark bit embedding is defined as function e (ipd; w; s) = [q(ipd + s=2; s) + ¢] £ s (2) where ¢ = (w ¡ (q(ipd + s=2; s) mod 2) + 2) mod 2. The embedding of one watermark bit w into scalar ipd is done through increasing the quantization of ipd + s=2 by the normalized difference between w and modulo 2 of the quantization of ipd+s=2, so that the quantization of resulting ipdw will have w as the remainder when modulus 2 is taken. The reason to quantize ipd+s=2 rather than ipd here is to make sure that the resulting e(ipd;w; s) is no less than ipd, i.e., packets can be delayed, but cannot be output earlier than they arrive. The embedding of watermark bit w by mapping ranges of unwatermarked ipd to the corresponding watermark ipdw. The watermark bit decoding function is defined as d (ipdw; s) = q (ipdw; s) mod 2.

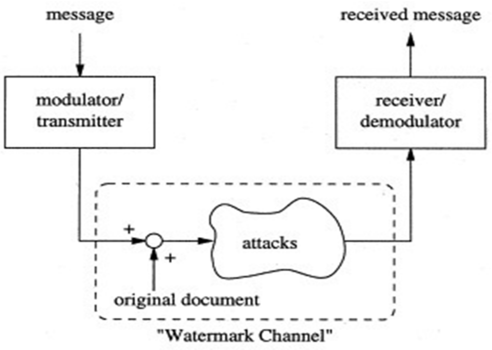

Fig 2. Tracing Model

3.2 Watermark Tracing Model

The watermark tracing approach exploits the observation that interactive connections are bidirectional. The idea is to watermark the backward traffic 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, which 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 sensors across the network about the watermark. The sensors 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. Gateway, firewall and edge router are good places to deploy sensors, deployed based on the administrative privilege. Since the backward traffic is watermarked at its very source - the attack target, which is not controlled by the attacker. The attacker will not have access to an unwatermarked version of the traffic. This makes it difficult for the attacker to determine which packets have been delayed by the watermarking process, running at the target.

3.3 Correlation Analysis And Decoding

The number of packets available is the fundamental limiting factor to the achievable effectiveness of our watermark based correlation. This compares and evaluates 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.

To map parameter with Secret Key, we generate secret key and add them into decrypt response. The parameter mapping does not affect the effectiveness of lossless recoverability. Finally the authenticated user takes the requested file in zip format with proper password. Finally the packet header information is extracted for analysis. Packet contents are decrypted in the analysis process. Watermark, source and time information are extracted from the packets. Address verification is also carried out in the packet analysis. The source information is verified in the user authentication process. User information is maintained in encrypted form. Watermarks are used to represent user identity. Time information is also used in the user authentication process.

3.4 WATERMARKING AND EXTRACTION

Flow watermarking is used in the authentication process. Watermarks are embedded by the source node and the receiver node verifies the watermarking images that are updated in the packets. An invisible watermark must be perceptually unnoticeable. Adding the watermark should not corrupt the original audio, video, or image. An invisible watermark should also be robust to common signal distortions and the removal of the watermark should result in degradation of the quality of the original digitized medium. Moreover, the watermark should serve as an original signature of the owner, so that retrieving the watermark from a digitized medium would readily identify the original owner. In order to extract the watermark, both the original image and the watermarked image are needed. First, DCT of the entire watermarked image is computed to obtain the image spectrum. Then, the DCT of the original image is computed. Next, the difference between the two spectrums is computed to extract the watermark X*. Finally, the originally watermark X is compared with the extracted watermark using the following equation: sim (X, X*) = (X X*) / sqrt (X X*). If the original watermark is similar to the extracted watermark, then the watermarked image belongs to the original owner.

Fig 3. Watermarked image

Fig 4. Original image

4. CONCLUSION AND FUTURE SCOPE

The watermarking of multimedia image prevents unauthorized copies from being distributed without the consent of the original owner. Stepping stones are used to hide identity and origin of the attacker. Flow watermarking technique is used to detect attacks with encrypted packets and time perturbed data. The system is enhanced to perform detection with minimum test packet count that manages the detection of stepping stone attacks. Time information is used in the delay analysis. Time information is perturbed in the header. Transmission delay is verified in the system. Packet modification is identified in the delay analysis. The system improves the detection rate.

5. REFERENCES

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

[2]R. C. Chakinala, A. Kumarasubramanian, R. Manokaran, G. Noubir, C. Pandu Rangan, and R. Sundaram. Steganographic Communication in Ordered Channels, *Proceedings of the 8th Information Hiding International Conference (IH 2006), 2006*

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

[4]P. Danzig, S. Jamin, R. Cacerest, D. Mitzel, and E. Estrin. An Empirical Workload Model for Driving Wide-Area TCP/IP Network Simulations. *Journal of Internetworking, 3(1) pages 1–26, March 1992.*