GLOBAL JOURNAL OF ENGINEERING, DESIGN & TECHNOLOGY
(*Published By:* Global Institute for Research & Education)
www.gifre.org

Analysis for Traffic and Intrusion Detection

A.M.J.Niyaz Hussain & C.Deepa
Assistant Professor in Information Technology,
S.N.R Sons College, SNR College Road, Coimbatore-641006, Tamilndau, India.

Abstract

In recent era of information security system all major network intrusion detection system uses signature based approaches for attack detection. Some attacks exploit the vulnerabilities of a protocol other attacks seek to survey a site by scanning and probing. These attacks can often be detected by analyzing the network packet headers, or monitoring the network traffic connection, attempts and session behaviors of computer Network.This paper focus on a particular class of traffic analysis attacks, Flow correlation attacks, by which an adversary attempts to analyze the network traffic and correlate the traffic of a flow over an input link with that over an output link. Two classes of correlation methods are considered, namely time-domain and frequency-domain methods. Based on our threat model and known strategies in existing mix networks and perform extensive experiments to analyze the performance of mixes. It is found that all but a few batching strategies fail against flow-correlation attacks, allowing the adversary to either identify ingress or egress points of a flow or to reconstruct the path used by the flow.

Keywords: *Content, Payload, Anomaly detection, attacks, Correlation, Time domain.*

Introduction

Network Communication

A Network Communication is sharing of information. This sharing can be either local or remote. Local communication usually occurs face to face between the individuals and Remote communication is used to transfer the information between two or more points that are physically not connected. In Network communications the data's are been exchanged between two devices via some form of transmission medium such as electrical cable, optical fiber, and radio waves (wireless LAN). Data in network communication represent the information that has been translated into a form that is more convenient to move or process. The data‘s are travelled inside the network communication using different network patterns like topologies namely Physical and Logical. Topology is a schematic description of the arrangement of a network, including its nodes and connecting lines.

Patterns in Network Communication

Networks are another aspect of direction and flow of communication. Data travels in the form of packets. Each packet consists of header, payload and trailer. The Header contains information about source, destination, length, port etc., Payload's are the actual information that travels with in the packet and the Trailer specifies whether the packet has a successor or not.

In global data communications, security has become a basic requirement for global computing as it is inherently insecure. As the data moves from point to point on the network, it may pass through several other points along the way giving other users the opportunity to intercept and even alter it. It is possible for any users to transfer data's from any system maliciously which the specific user of the respective system is not intended to do it. Unauthorized access to the system may be obtained by intruders who uses the advanced knowledge to impersonate, steal information from the user, or even deny the access to users their own resources.

Computer Security In Network Communication

The objective of computer security includes protection of information and property from theft, corruption or natural disaster while allowing the information and property to remain accessible and productive to its intended users. The term computer system security means the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively. The strategies and methodologies of computer security often differ from most other computer technologies because of its elusive objective of preventing unwanted computer behavior instead of enabling wanted computer behavior

A network traffic monitor allows to quickly and easily examine the network usage of the local computer. In Network Traffic Monitor a network analysis tool examines local area network usage and provides a display of upload and downloads statistics. The Main purpose of the application is monitoring (and counting) the IP traffic between your local area network (LAN) and Internet.

Network Traffic Monitor provides real-time traffic accounting and monitoring. It is very dynamic, every new (dial-up) connection is registered and monitored, user can use it to count useful download and upload traffic of a computer or extend it to build the traffic accounting system for all computers in [1] or date to date life.

Traffic Analysis

It is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. Traffic analysis can be performed in the context of military intelligence or counter-intelligence, and is a concern in computer security. The size of packets being exchanged between two hosts can also be valuable information for an attacker, even if they aren't able to view the contents of the traffic (being encrypted or otherwise unavailable). Seeing a short flurry of single-byte payload packets with consistent pauses between each packet might indicate an interactive session between two hosts, where each packet indicates a single keystroke. Large packets sustained over time tend to indicate file transfers between hosts, also indicating which host is sending and which host is receiving the file, by itself, this information might not be terribly damaging the security of the network, but a creative attacker will be able to combine this information with other information to bypass intended security mechanisms.

Security Focus ran an article on a "Method based on traffic behavior that helps identify P2P users, and even helps to distinguish what type of P2P applications are being used".[2] In this case focus was on the default port numbers the tools use,though there are more sophisticated methods using flows.[3].

Traffic analysis can also be used as a defensive technique by identifying anomalies in traffic patterns. Using traffic analysis, administrators can baseline the traffic to and from hosts on the network over time, in a graphical format (line charts or other graphs).

Traffic Flow Security

Traffic-flow security is the use of measures that conceal the presence and properties of valid messages on a network to prevent traffic analysis. This can be done by operational procedures or by the protection resulting from features inherent in some cryptographic equipment.

Techniques used include:

- changing radio call signs frequently
- encryption of a message's sending and receiving addresses (codress messages)
- causing the circuit to appear busy at all times or much of the time by sending dummy traffic
- Sending a continuous encrypted signal, whether or not traffic is being transmitted. This is also called masking or link encryption.

Traffic-flow security is one aspect of communications security [5].

If a certain emitter is known as the radio transmitter of a certain unit then using DF (direction finding) tools, the position of the emitter is locatable, hence the changes of locations can be monitored. So that is possible to understand that this certain unit is moving from one point to another, without listening to any orders or reports. If is unit reports back to a command on a certain pattern and if another unit reports on the same pattern to the same command then the two units are probably related and that conclusion is based on the metadata of the two units' transmissions and not on the content of their transmissions [4].

Using all, or as much of the metadata available is commonly used to build up an Electronic Order of Battle (EOB) – mapping different entities in the battlefield and their connections. Of course the EOB could be built by tapping all the conversations and trying to understand which unit is where, but using the metadata with an automatic analysis tool enables a much faster and accurate EOB build-up that alongside tapping builds a much better and complete picture.

Network Traffic Monitor

In NTM network analysis tools examines local area network usage and provides a display of upload and download statistics. The Main purpose of the application is monitoring (and counting) the IP traffic between your local area network (LAN) and Internet. It is very dynamic, every new (dial-up) connection is registered and monitored, user can use it to count useful download and upload traffic of a computer or extend it to build the traffic accounting system for all computers in. [6] or date to date life in real time traffic.

HTTP Anomaly Detection

An anomaly based method to detect web-based attacks was developed in [7][8][9]. Different from other IDS techniques, which identify attacks based on different packet fields such as source IP, destination IP, destination port, etc., this method is based on only the packet payload. Since this approach only focuses on HTTP traffic, it could take advantages of the known protocol format to extract useful fields from the HTTP request, then construct associated statistical models. In the earlier approach, which was described in [7], three properties were used: the request type, the request length, and the payload characters distribution. More properties were incorporated in the later implementation in [8][9]. Although this method claims to have 0.06% or less false positives when testing on Google and campus networks, it only focus on HTTP traffic and cannot be adopted for other applications. So it is almost impossible to compare it with other methods.

Network Packet Analysis for Intrusion Detection

Intrusion detection systems are evolving component of computer security. Three main issues define success of IDS: false negatives, false positives and throughout put. Integrated IDS that includes misuse and anomaly detection should be able to have all three of them at needed levels. Anomaly detection network IDS need most improvement. Historical data used to create model of normal behavior should be periodically filtered of intrusions as new attack signatures become available. New services that might recognized as anomalies should be modeled in advance. Network packet analysis would contribute the most to current intrusion detection needs. HTTP protocol data provide an avenue for attack and therefore their analysis could improve application level security significantly. Modeling of normal and anomalous HTTP payload might be achieved using artificial neural networks. Size of packets needed for successful intrusion detection might be small enough to allow real time processing.

Conclusion

The empirical result provided in this paper give an indication to designers of Mix networks about appropriate configurations and mechanisms to be used to counter flow-correlation attacks.

References

[1] Original idea by Dirk Claessens; GUI, TTraffic class and text by Zarko Gajic.

[2] http://www.securityfocus.com/infocus/1843

[3] Identifying P2P Heavy-Hitters from Network-Flow Data, Arno Wagner¤ Thomas D¨ubendorfer¤ Lukas H¨ammerle† Bernhard Plattner, Communication Systems Laboratory, Swiss Federal Institute of Technology Zurich, Gloriastr. 35, CH-8092 Zurich, {wagner, duebendorfer, plattner}@tik.ee.ethz.ch SWITCH, PO Box, CH-8021 Zurich, Switzerland, haemmerle@switch.ch Contact Author: Arno Wagner, phone: +41 44 632 7004, fax: +41 44 632 10 35

[4] Payload Content based Network Anomaly Detection, Sandeep A. Thorat Amit K. Khandelwal Bezawada Bruhadeshwar K. Kishore Centre for Security, Theory, and Algorithmic Research (CSTAR) International Institute of Information Technology-Hyderabad, India.

[5] On Traffic Analysis in Anonymous Communication Networks - YE ZHU

[6] Original idea by Dirk Claessens; GUI, TTraffic class and text by Zarko Gajic.

[7] C. Kruegl, T. Toth, and E. Kirda, “Service Specific Anomaly Detection for Network Intrusion Detection”, Proceedings of the 2002 ACM symposium on Applied computing (SAC 2002), pp. 201-208, Madrid, Spain, 2002

[8] C. Kruegl, G. Vigna, “Anomaly Detection of Web-based Attacks”, Proceedings of the 10th ACM Conference on Computer and Communication Security (CCS’03), pp. 251-261, Washington, DC, October, 2003

[9] Christopher Kruegel, Giovanni Vigna, and W. Robertson, “A multi-model approach to the detection of web-based attacks”, Computer Networks, vol. 48, no. 5, pp. 717-738, August, 2005