Statistical Analysis of False Positives and False Negatives from Real Traffic with Intrusion Detection/Prevention Systems

Cheng-Yuan Ho, National Chiao Tung University

Yuan-Cheng Lai, National Taiwan University of Science and Technology

I-Wei Chen, Fu-Yu Wang, and Wei-Hsuan Tai, National Chiao Tung University

ABSTRACT

False positives and false negatives happen to every intrusion detection and intrusion prevention system. This work proposes a mechanism for false positive/negative assessment with *multiple* IDSs/IPSs to collect FP and FN cases from real-world traffic and statistically analyze these cases. Over a period of 16 months, more than 2000 FPs and FNs have been collected and analyzed. From the statistical analysis results, we obtain three interesting findings. First, more than 92.85 percent of false cases are FPs even if the numbers of attack types for FP and FN are similar. That is mainly because the behavior of applications or the format of the application content is self-defined; that is, there is not complete conformance to the specifications of RFCs. Accordingly, when this application meets an IDS/IPS with strict detection rules, its traffic will be regarded as malicious traffic, resulting in a lot of FPs. Second, about 91 percent of FP alerts, equal to about 85 percent of false cases, are not related to security issues, but to *management policy*. For example, some companies and campuses limit or forbid their employees and students from using peer-to-peer applications; therefore, in order to easily detect P2P traffic, an IDS/IPS is configured to be sensitive to it. Hence, this causes alerts to be triggered easily regardless of whether the P2P application has malicious traffic or not. The last finding shows that buffer overflow, SQL server attacks, and worm slammer attacks account for 93 percent of FNs, even though they are aged attacks. This indicates that these attacks always have new variations to evade IDS/IPS detection.

INTRODUCTION

During the last several years, malicious traffic detection has been an active area of network security because the Internet has witnessed a surge in malicious traffic generated by network attacks, such as denial of service (DoS), and propagation of botnets, viruses, worms, trojan horses, spyware, and so on. Moreover, malicious traffic makes network performance inefficient and troubles users. For example, distributed DoS (DDoS) attacks increase Domain Name Service (DNS) latencies by 230 percent and web latencies by 30 percent [1]. During July–August 2001, 395,000 computers were infected worldwide with the CodeRed worm, which resulted in approximately $2.6 billion in damages [1].

There are a multitude of malicious traffic detection techniques, and thus, vulnerabilities in common security components, such as firewalls, are unavoidable. Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) are commonly used today. They are used to detect different types of malicious traffic, network communications, and computer system usage with the mission of preserving systems from widespread damage; that is because other detection and prevention techniques, such as firewalls, access control, skepticism, and encryption have failed to fully protect networks and computer systems from increasingly sophisticated attacks and malware [2, 3].

An IDS/IPS monitors the activities of a given environment and decides whether these activities are malicious or normal based on system integrity, confidentiality and the availability of information resources. As soon as a malicious or an intrusive event is detected, the IDS produces a relative alert and passes it to the network administrator promptly while the IPS not only executes what the IDS does but also blocks network traffic from the suspected malicious source. However, there is no "perfect" detection approach, which can always correctly distinguish between malicious and normal activities. In other words, IDSs/IPSs can identify a normal activity as a malicious one, causing a false positive (FP), or malicious traffic as normal, causing a false negative (FN). FPs and FNs cause several problems. For example, FNs generate unauthorized or abnormal activities on the Internet or in computer systems. On the other hand, a lot of FPs may easily conceal real attacks[1] and thus overwhelm the security operator. When real attacks occur,

[1] *This kind of attack is called a snowblind attack.*

true positives (real alerts) are deeply buried within FPs, so it is easy for the security operator to miss them [4].

Accordingly, a variety of commercial products, open source, and research into IDSs were proposed. Wu and Banzhaf [2] provided an overview of different IDS algorithms, such as artificial neural networks, swarm intelligence, evolutionary computation, artificial immune systems, fuzzy sets and soft computing, and their problems. A collaborative intelligent IDS and a fuzzy inference system were proposed to reduce FPs through fuzzy alert correlation in [3] and [5], respectively, while Sourour et al. in [4] reduced both FPs and FNs with their environmental awareness intrusion detection and prevention system. A system of Attack Session Extraction (ASE) was proposed in [6] to create a pool of traffic traces causing possible FPs and FNs to IDSs. One to two years later, the ASE was expanded into a bigger system, called the *PCAPLib system* [7]. The PCAPLib system not only extracted and classified the real-world traffic captured from *Campus BetaSite* [8] into proper categories by leveraging multiple IDSs, but also anonymized users' privacy in these FP and FN traffic traces out of security considerations. However, previous work only focused on studying how to reduce FPs and/or FNs in IDSs or how to collect and extract the FP and FN traffic traces from real-world traffic.

This work collects more than two thousand cases of FPs and FNs from the real-world traffic of Campus BetaSite by the PCAPLib system, in order to observe what kinds of FPs or FNs happen easily in which protocols and in what kind of attacks, and investigate their frequencies across all FPs and FNs. Also, the reasons behind these FP and FN cases for network forensics and trends in malicious traffic attacks are conjectured in this work. From statistical analysis results, we find that

- There are *13 times* more FPs than there are FNs although the number of attack types in FP and FN are similar
- About 91 percent of FP alerts are not related to security issues
- Buffer overflow, SQL server attacks and worm slammer attacks account for 93 percent of FNs

With this work, application users and developers can understand why the traffic of an application is sometimes blocked by the IPS while the developers of IDS/IPS can pay attention to the mentioned FN cases, protocols and so on.

The remainder of this article is organized as follows. The effects of FPs and FNs are detailed. The methodology of how to collect and assess FPs and FNs from real-world traffic is described. The experimental environment in this work and statistical analysis are shown. Finally, the last section concludes this work and outlines future work.

FPs and FNs

FPs and FNs of the IDS/IPS are mystery terms that describe a situation where the IDS/IPS makes a mistake. The former means that the IDS/IPS triggers an alert when there is no malicious activity in the traffic while the latter means that there is no alert raised by the IDS/IPS when malicious traffic passes through it. FP and FN rates are two metrics important in measuring the accuracy of the IDS/IPS [9].

An FP of the IDS/IPS will not result in an intrusion and it may be caused by two reasons: the detection mechanism of the IDS/IPS may be faulty or the IDS/IPS detects an anomaly that turns out to be benign. Therefore, an FP may cause security analysts to expend unnecessary effort. Moreover, if a hacker launches a *snowblind* attack, the challenge for security analysts is to somehow identify the real attack amidst the chaff caused by the hacker. This may create a potential vulnerability for the IDS. On the other hand, when an IPS has an FP, the primary concern is that legitimate traffic might be blocked. Most organizations consider blocking legitimate traffic as a much more serious problem than generating a false alert. Consequently, an FP of the IPS is a much more serious matter than that of the IDS. If the IPS blocks legitimate traffic a few times, it will be yanked out of the network.

An FN is simply a missed attack, which may put networks or computer systems in danger. Clearly an FN is undesirable, and every vendor strives to provide the most complete coverage possible. However, there is no silver bullet: no product detects all attacks. Hence, the goal becomes providing coverage against high priority attacks. Aside from lack of coverage, several other reasons may also cause an FN. For example, in order to evade the IDS or IPS, the attack may incorporate obfuscation techniques. Another possibility is overwhelming the IDS with traffic beyond its processing capacity, so the IDS will drop the packets needed to detect the attack. For an IPS, overwhelming it has a different effect: it causes traffic to be dropped. The attack doesn't succeed because attack packets are dropped, but it is also not detected. Accordingly, the attack can be tried again.

In practice, for a vendor of IDSs/IPSs, an FN is much more serious than an FP because of negative effects of an FN including reduced trust in the IDS/IPS, and because of damage caused by the intrusion. However, from a user's point of view, an FP may be more serious than an FN because an FP may cause the IPS to block the user's benign traffic. In addition, the user may allow some FNs as long as they're not too frequent. Therefore, it is necessary to investigate and analyze FPs and FNs with IDSs/IPSs in detail.

from a user's point of view, an FP may be more serious than an FN because an FP may cause the IPS to block the user's benign traffic. In addition, the user may allow some FNs as long as they're not too frequent. Therefore, it is necessary to investigate and analyze FPs and FNs with IDSs/IPSs in detail.

Methodology

This section first takes a look at the Campus BetaSite and the PCAPLib system (which is the traffic source), and then details how to identify and assess 2000 cases of FPs and FNs for network forensics on a set of IDSs/IPSs. Herein, the method of assessing FPs/FNs is called false positive/negative assessment (FPNA).

The Campus BetaSite and the PCAPLib System

As shown in Fig. 1, the traffic source for the PCAPLib system comes from the Campus BetaSite deployed at National Chiao Tung Universi-

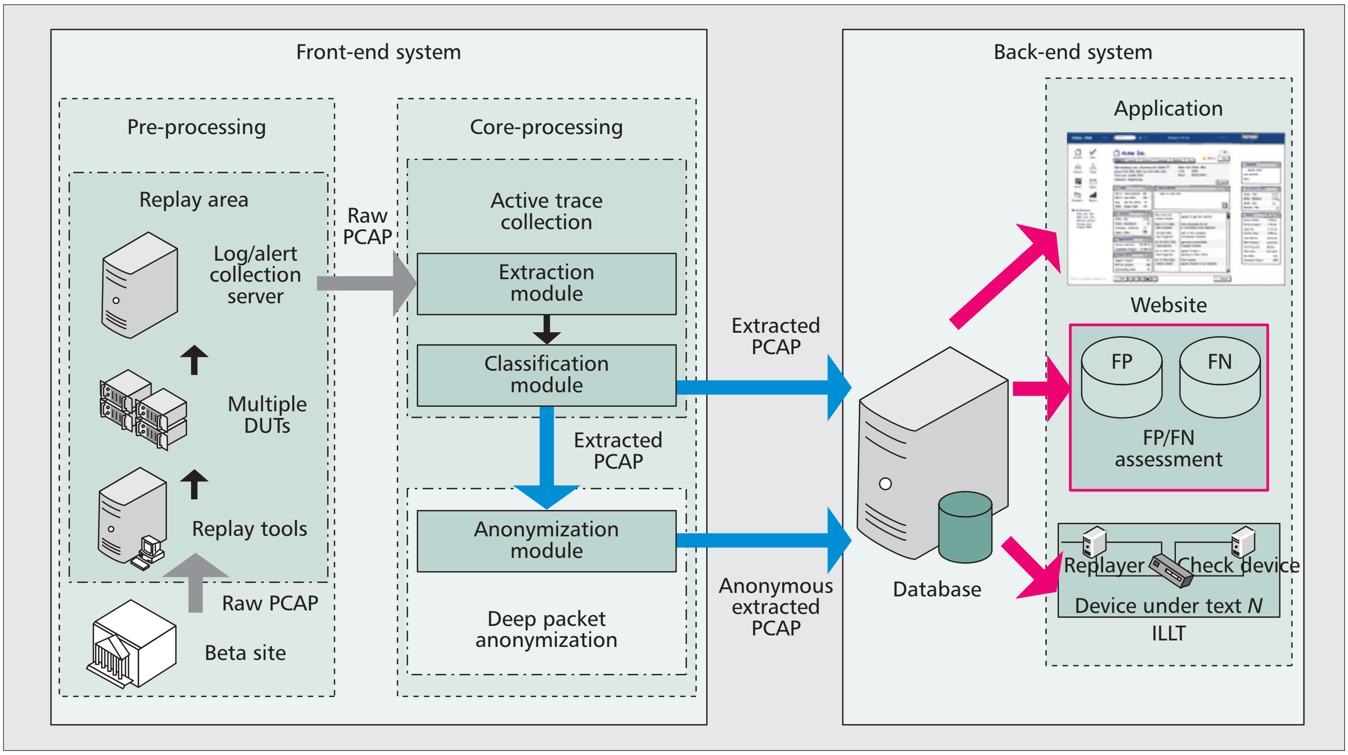


Figure 1. *Architecture and block diagram of the PCAPLib system.*

ty, Hsinchu, Taiwan. The Campus BetaSite is used by developers to test and debug products while maintaining network quality for network users. Moreover, it is an operational network on campus and records network traffic from network users into packet capture (PCAP) files. The volume of network traffic on/through the BetaSite is roughly 100 Gbytes/h.

The goal of trace sharing is to preserve real-world traffic behavior in packet traces so that it can be replicated and picked up easily by researchers for network forensics.[2] To achieve this goal, the PCAPLib system consists of front-end and back-end systems. The front-end system not only extracts and classifies valuable packet traces from real-world traffic but also precisely and deeply protects the sensitive information in the packets. This is because recording the entire real-world traffic consumes storage space and searching for specific events within the huge traces is time-consuming. Therefore, recording only traffic associated with specific/special events would be better. Besides, packet anonymization protects privacy from leakage in trace sharing. On the other hand, the back-end system is responsible for storing the extracted PCAP files, whether anonymous or otherwise, and for demonstrating the usefulness of the PCAPLib system in network forensics when used in conjunction with other applications, such as FPNA.

The preprocessing component of the front-end system uses a traffic replay tool (e.g., tcpreplay) to replay captured raw traffic to multiple devices under test (DUTs) to leverage their domain knowledge. If a DUT detects abnormal behavior in the traffic, it will trigger an alert. For the core processing component of the front-end system, there are two mechanisms, Active Trace Collection (ATC) and Deep Packet Anonymization (DPA). Based on DUT logs, the ATC finds out the anchor packets that trigger the logs, processes packets and connection associations to extract each specific/special session into packet traces, and uses supervised classification to categorize the extracted packet traces. On the other hand, the DPA parses application-level protocol identities and anonymizes sensitive fields for privacy protection of packet traces, while still maintaining their usefulness for research.

False Positive/Negative Assessment

FP and FN rates are two important metrics in measuring the accuracy of a network security system, such as an IDS or IPS. It has been demonstrated that even a small rate (1 in 10,000) of FPs could generate an unacceptable number of FPs in practical detections [7]. The assessment is important to IDS/IPS developers trying to optimize the accuracy of detection by reducing both FPs and FNs, because the FP/FN rate limits the performance of network security systems due to the base-rate fallacy phenomenon. The statistical analyses in this work can elucidate the causes and rankings of FPs and FNs, thus allowing developers to avoid similar pitfalls during their product development.

As in previous work [6, 7], the ATC leverages the domain knowledge of the DUTs of intrusion detection/prevention, antivirus, anti-spam and application classifier to collect real-world packets. The detection of DUTs may be incorrect, resulting in FPs or FNs. As a demonstration of network forensics using real-world traffic, this work assesses FP/FN cases using the FPNA mechanism as shown in Fig. 2a. FPNA has the following three procedures, *majority voting*, *trace*

[2] *It captures, records, and analyzes network events in order to discover the source of security attacks or other problem incidents.*

verification and *manual analysis*. First, majority voting is a decision which has a majority, that is, more than half of the votes. It is a binary decision voting used most often in influential decision-making bodies, including the legislatures of democratic nations. In this work, the voters are all DUTs and *potential FPs/FNs* are detected under the definition of majority voting. In other words, if only one or a few DUTs generate a detection log for some specific packet trace, this trace appears as an FN or a true negative (TN) case. On the other hand, when more than half of the DUTs have alerts for this trace, the trace is likely to be an FP or a true positive (TP). Majority voting's flow chart is described in Fig. 2b.

Second, after detecting the potential FPs/FNs/TPs/TNs, this work replays the extracted packet trace according to the log to the DUTs again. This step is called trace verification because it verifies whether this case is reproducible to the original DUTs. This case is a reproducible FP/FN/TP/TN when it meets the following two conditions.

- For any DUT, it must produce an alert if it did last time
- The two alerts must be the same when one came from some DUT last time and the other is produced by the same DUT this time

Otherwise, this case is un-reproducible. For example, there are one traffic flow and three DUTs, A, B and C. After this traffic flow passes through the PCAPLib system, we get an extracted packet trace from this traffic and two alerts from A and C. Two alerts are named A1 and C1, respectively. Then, we replay this extracted packet to A, B and C again. If A and C produce alerts, called A2 and C2, and the content of A2 and C2 are same as that of A1 and C1, respectively, this extracted packet trace is reproducible. In order to show these two conditions in Fig. 2c, we use "are all alerts same as before?" to represent them. Late, in order to know whether the reproducible traffic trace is a publicly malicious case, the step of manual analysis manually investigates the causes of the reproducible traffic trace and compares these causes with Common Vulnerabilities and Exposures (CVE), a dictionary of publicly known information security vulnerabilities and exposures. After this step, an FP/FN or a TP/TN is identified and the occurrences of frequent cases are also counted. Figures 2c and 2d respectively describe the flow charts of the second and third steps.

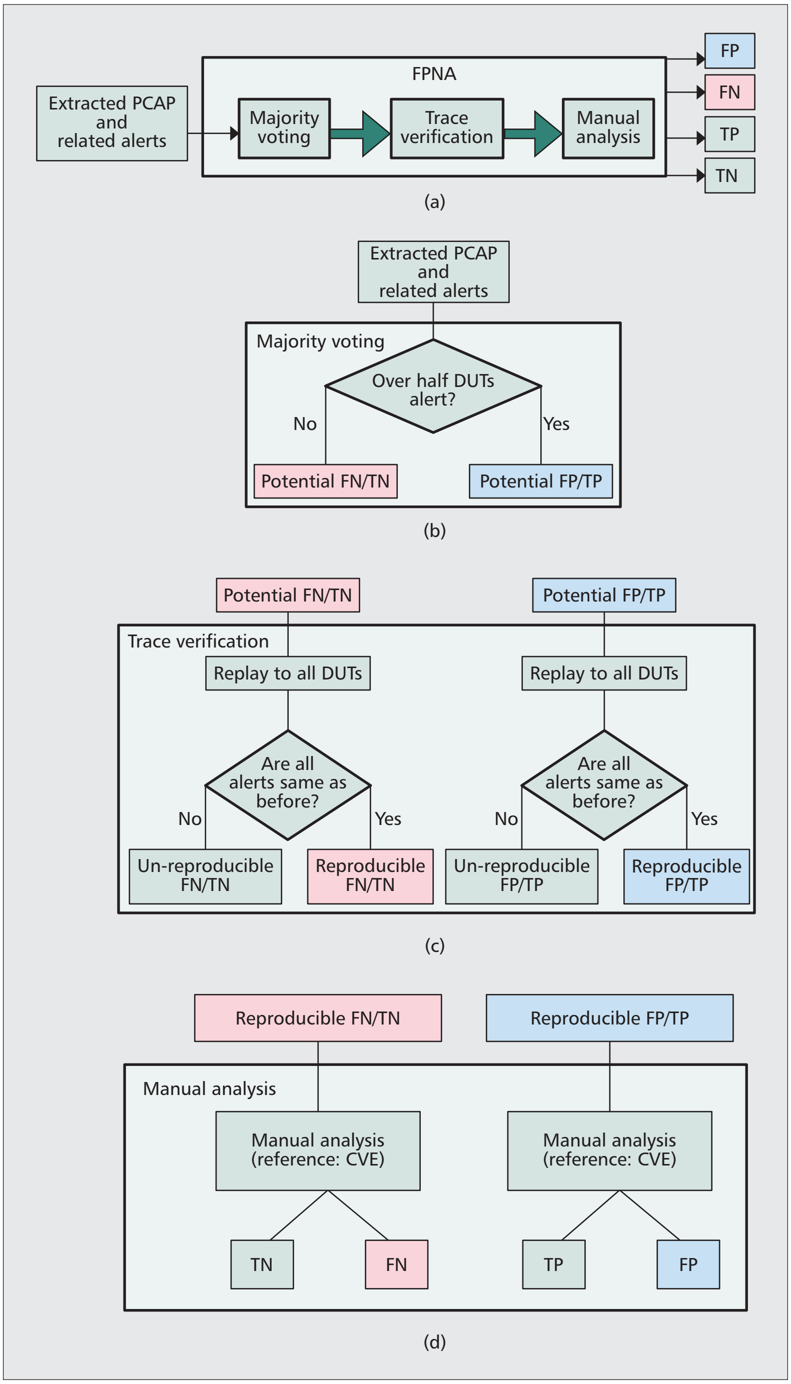


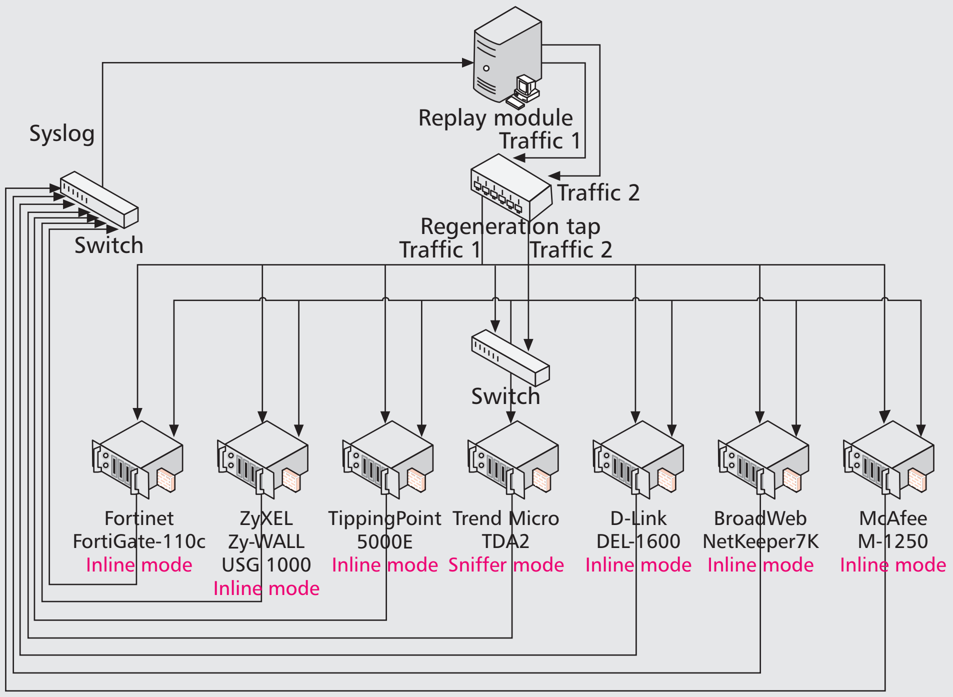
Figure 2. *Details of the false positive/negative assessment mechanism: a) whole flow chart of FPNA mechanism; b) flow chart of majority voting; c) flow chart of trace verification; and d) flow chart of manual analysis*

Statistical Analysis

This section reviews the experimental environment and DUTs' information of the FPNA is first overviewed. Then, statistical analysis of FPs and FNs, and some interesting observations and summarization are detailed.

Experimental Environment

The PCAP files were captured real-world traffic at the BetaSite, as shown in Fig. 1, during the period Oct. 1, 2009 to Feb. 1, 2011. As mentioned in Section 3, the FPNA has majority voting, trace verification and manual analysis mechanisms. Majority voting can be executed in a computer because it only counts the number of logs/alerts for a PCAP file and marks "potential FP, FN, TP or TN" on this PCAP file. An experimental environment for trace verification for replaying PCAP files is shown in Fig. 3a. Here, seven DUTs are used and their detailed information, such as vendor, device, name, etc., is described in Fig. 3b. Depending on where the IDS/IPS locates, an IDS/IPS can be either *network-based* or *host-based*. A network-based IDS/IPS is an independent platform, while a host-based one consists of an agent on a host. According to the detection method, an IDS/IPS



(a)

Vendor	Fortinet	ZyXEL	TippingPoint	Trend Micro	D-Link	BroadWeb	McAfee
Device name	FortiGate-110c	ZyWALL USG1000	5000E	TDA2	DFL-1600	NetKeeper7K	M-1250
IDS/IPS	IPS	IPS	IPS	IDS	IPS	IPS	IPS
Location	Network	Network	Network	Network	Network	Network	Network
Method	Signature	Signature	Signature	Signature	Signature	Signature	Signature
AntiVirus	Yes	Yes	No	Yes	No	No	No
AntiSpam	Yes	No	No	No	No	No	No
P2P	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IM	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Streaming	No	No	No	Yes	No	No	No

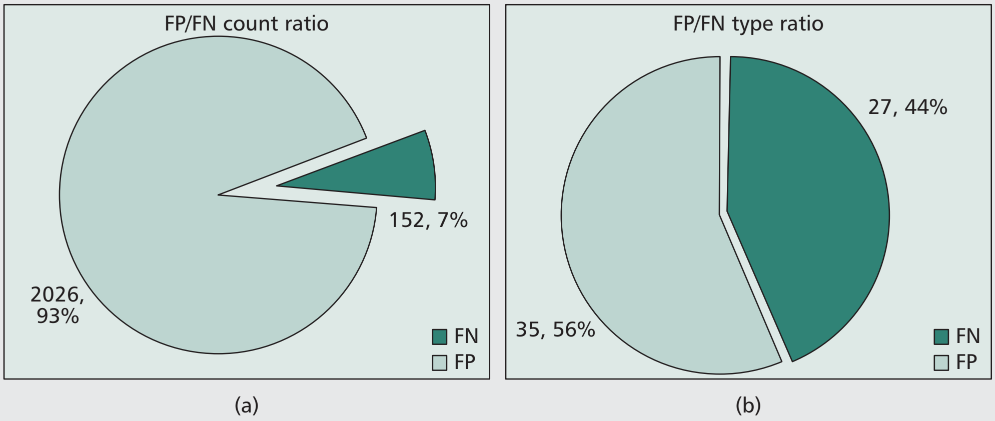
(b)

Figure 3. *a) Experimental environment; b) detailed information of seven DUTs.*

can be placed into one of two categories, namely *signature-based* and *anomaly-based*. A signature-based IDS/IPS compares packets with preconfigured and predetermined attack patterns or predefined descriptions of intrusive behavior known as signatures. On the other hand, an anomaly-based one tries to build models for normal behaviors and detects anomalies in observed data by noticing deviations from these models. From Fig. 3b, we observe that only Trend Micro TDA2 is an IDS while the other six DUTs are IPSs. In this work, all DUTs are network-based security detection systems due to the PCAPLib system's architecture whereas they are all signature-based because a signature-based IDS/IPS is more easily implemented than an anomaly-based one. During replay, all functions, like antivirus, anti-spam, P2P, instant messenger (IM), streaming scan, and system logs of DUTs are enabled if possible. After trace verification, reproducible FPs/FNs/TPs/TNs will be passed to the manual analysis step, where all alerts are compared to the CVE in order to check whether they are FPs, FNs, TPs, or TNs.

Statistical Results

This subsection analyzes what kinds of FPs or FNs happen easily to IDS/IPS with real-world traffic and investigates their frequencies across all FPs and FNs. There are two hierarchies of classification in this work. One is by protocols, such as HTTP, FTP, NetBIOS and IRC and the other is by IDS policy types (also called "attack types"), like DDoS, buffer overflow, Web attack, scan, and so on.



(a)

(b)

Protocol	Attack message	No.
HTTP	HTTP-Inspection (8119001) ASCII-ENCODING ATTACK	460
HTTP	HTTP-Inspection (8119012) APACHE-WHITESPACE ATTACK	399
HTTP	HTTP-Inspection (8119013) NON-RFC-HTTP-DELIMITER ATTACK	276
HTTP	Sig (8009136) SQL injection SQL command attempt-2	191
HTTP	Sig (8009000) SQL injection comment attempt	176
HTTP	Sig (8009004) SQL injection SQL command attempt	116
TCP (scan)	Scan-detection (8122001) TCP port scan	106
FTP	Sig (8000392) FTP wu-ftp bad file completion attempt	76

(c)

Figure 4. *Statistics and comparisons between FPs and FNs: a) FP/FN count ratio; b) FP/FN type ratio; and c) examples of FP types (protocol, attack message and number).*

Some companies and campuses limit or forbid their employees and students from using peer to peer (P2P) applications, and therefore, thresholds of P2P traffic in an IDS/IPS will be configured very low. Hence, this causes alerts to be easily triggered regardless of whether the P2P application has malicious traffic or not.

FP Cases Taking the Most Percentage of False Cases — Figure 4a depicts the numbers and ratios of FP and FN cases, while Fig. 4b shows those of FP and FN types. From Fig. 4a, we can observe that the number of FPs is 13 times that of FNs. In other words, more than 92.85 percent of false cases are FPs. However, when we calculate how many kinds of attack there are in FPs and FNs, as shown in Fig. 4b, we find that the number of kinds of attack in FN cases, 27, is close to that in FP cases, 35. According to Figs. 4a and 4b, we guess that FP cases have many cases with traffic similarity, meaning that network traffic of a certain protocol happens to exhibit some characteristics belonging to other protocols [7]. To prove this guess, the number of each type of attack is calculated. For instance, the information of protocol, attack message and the number of each attack type in FP cases is depicted in Fig. 4c. There are dozens or hundreds of FP cases as compared to only a few FN cases.

From the information in Fig. 4c, we can see that about 91 percent of FP alerts, equal to about 85 percent of false cases, are not related to security issues, but to management policy. Policy here means some configuration arguments are artificially constructed for some reason. For instance, some companies and campuses limit or forbid their employees and students from using peer to peer (P2P) applications, and therefore, thresholds of P2P traffic in an IDS/IPS will be configured very low. Hence, this causes alerts to be easily triggered regardless of whether the P2P application has malicious traffic or not.

Policy and Self-Defined Formats Causing FPs — Figure 5a shows the most frequent attack types of FPs from the sample traces in our investigation.

- The "HTTP-Inspection" alert results from application clients using their self-defined formats, not defined by RFCs, and the traffic happens to be similar to an ASCII-encoding attack, apache-whitespace attack, and so on.
- The "SQL Injection comment attempt" alert results from BitTorrent clients who happen to bind port 80, and the traffic happens to be similar to an injection attempt.
- Then "TCP port scan" alert results from applications which test how many free ports there are in order to establish many connections at the same time.
- The "FTP wu-ftp bad file completion attempt" alert results from the "[" character which appears often in FTP transfer data.
- The "Veritas Backup Agent DoS attempt" alert results from BitTorrent clients who bind port 10000 (the port monitored by the rule), and the traffic happens to be similar to a DoS attempt.

Figures 5b, 5c, and 5d present the proportions of four protocols of FPs, those of five attack types under HTTP and those of two attack types under unknown applications using TCP (UAT), respectively. From Fig. 5b, HTTP accounts for 90 percent of FPs, and from Fig. 5c, 67 percent of HTTP is web attacks.

Although buffer overflow, SQL server attacks and worm slammer attacks are aged attacks, they still account for 93 percent of FNs. This may indicate that these attacks always have new variations to avoid IDS/IPS detection.

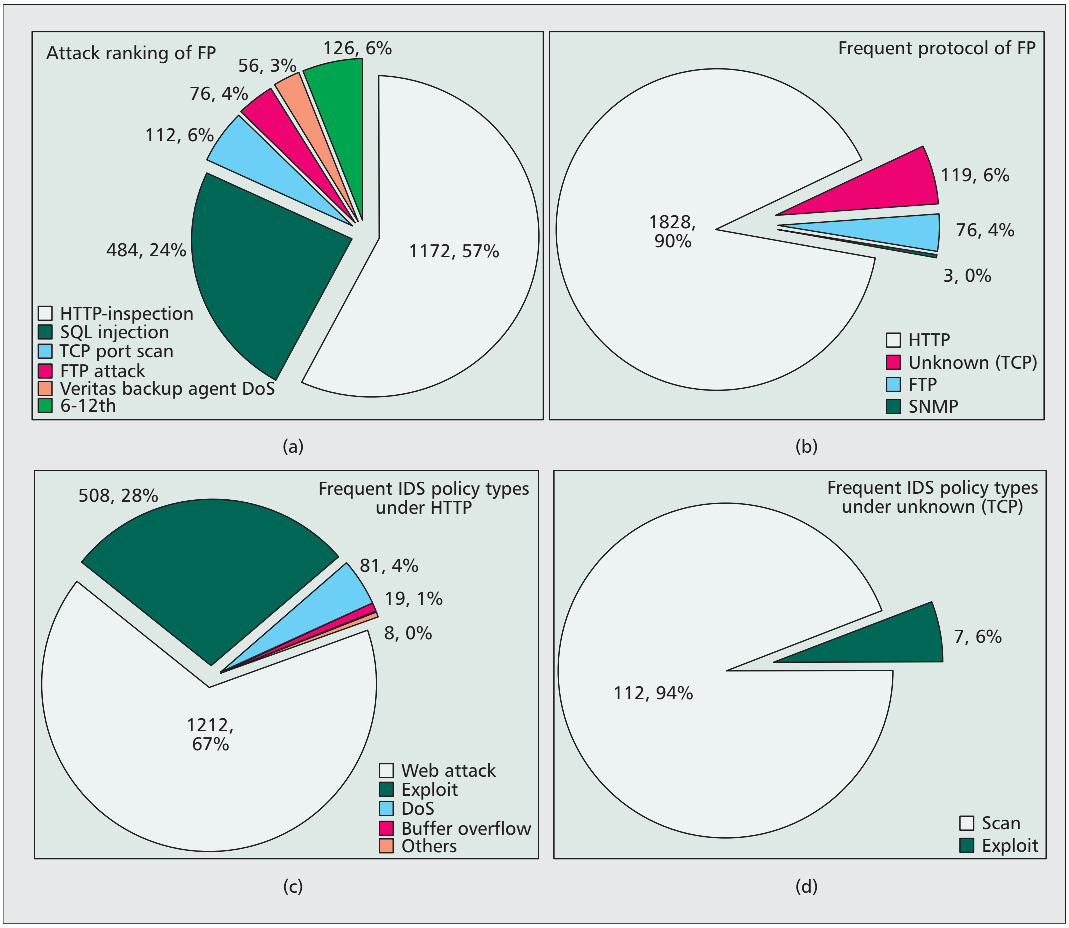


Figure 5. *FP attack ranking and detailed analysis: a) top five frequent attack types; b) proportion of four protocols of FP; c) five attack types under HTTP; d) only two attack types under UAT.*

Many Aged Attacks Having New Variations — Figure 6a shows the most frequent attack types of FNs.

- The "Buffer Overflow" alert results from Windows being vulnerable to buffer overflow when handling certain types of Remote Procedure Call (RPC) traffic, and this flaw occurs within the 'netapi32.dll' component of the Server service with NetPathCanonicalize requests.
- The "SQL Server Attack" alert results from a login that fails for user 'sa'.
- The "MS-SQL Worm Slammer" alert is caused by DoS on some Internet hosts.

In sum, the buffer overflow and the MS-SQL worm slammer, totaling 103 FN cases, are aimed at Microsoft products because Microsoft is estimated to make up nearly 90 percent of the OS marketshare [10]. Moreover, although buffer overflow, SQL server attacks and worm slammer attacks are aged attacks, they still account for 93 percent of FNs. This may indicate that these attacks always have new variations to avoid IDS/IPS detection.

Figures 6b–d, and 6e present the proportions of four protocols of FNs, those of two attack types under NetBIOS, that of one attack type under UAT and that of one attack type under an unknown application using UDP (UAU), respectively. From Fig. 6b, NetBIOS accounts for 68 percent of FNs, and from Fig. 6c, 90 percent of NetBIOS is buffer overflow attacks.

Conclusion

This work proposes the FPNA mechanism in the PCAPLib system to provide statistical analysis of FP and FN cases. The FPNA collected more than two thousand FPs and FNs during sixteen months. 92.85 percent of false cases were FPs and 7.15 percent were FNs. Out of numerous FPs, about 91 percent of FP alerts occur because of IDS's or IPS's policy, not due to security issues. The distribution of the collected FPs shows that 90 percent are using HTTP and 57 percent of FPs are thought to be HTTP inspection attacks. NetBIOS accounts for 68 percent of FNs and about 67 percent of FN cases are aimed at Microsoft products. From the statistical analysis, we also observe that traffic similarity is the main cause of FP cases, and missing attack signatures in the signature design is the cause of FN cases.

Although there are thousands of FP and FN cases in this work, these FPs/FNs are detected by the signature-based IDSs/IPSs. Maybe some FPs or FNs occur in the anomaly-based IDSs/IPSs, and accordingly, new DUTs, including anomaly-based or online/cloud IDSs/IPSs, will join the experimental environment in the future. Furthermore, the FPNA will continue to trace whether statistical results change when the DUTs update their engines and virus patterns. In summary, FPs/FNs are still the key issues for

The FPNA will continue to trace whether statistical results change when the DUTs update their engines and virus patterns. In summary, FPs/FNs are still the key issues for IDSs/IPSs which are less reliable today because of the limitations of the signature-based methodology.

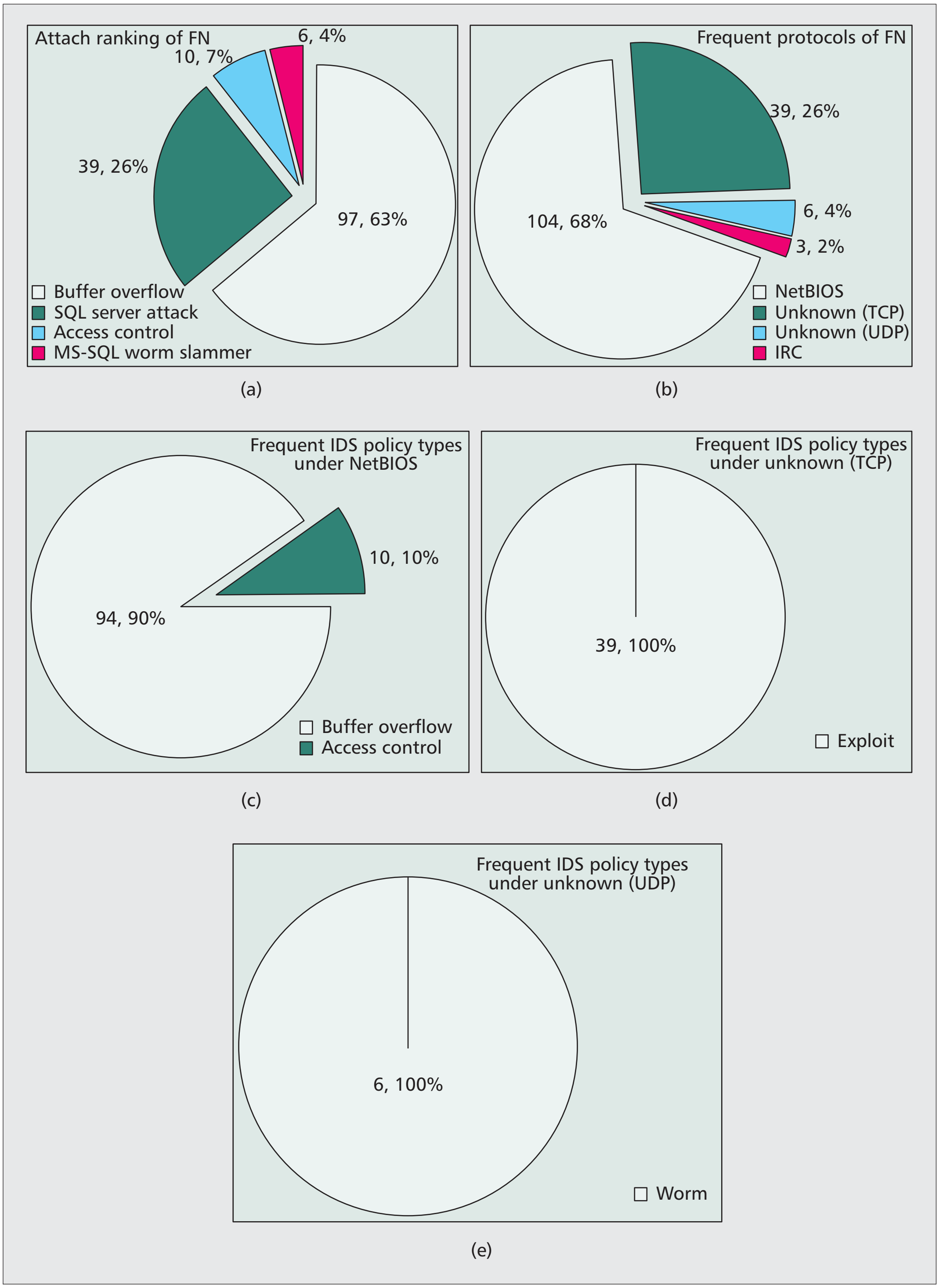


Figure 6. *FN attack ranking and detailed analysis: a) top four frequent attack types; b) proportion of four protocols of FN; c) only two attack types under NetBIOS; d) only one attack type under UAT; e) only one attack type under UAU.*

IDSs/IPSs which are less reliable today because of the limitations of the signature-based methodology.

References

[1] K.-C. Lan, A. Hussain, and D. Dutta, "Effect of Malicious Traffic on The Network," *Proc. Passive and Active Measurement Wksp. (PAM)*, San Diego, CA, Apr. 2003.

[2] S.-X. Wu and W. Banzhaf, "The Use of Computational Intelligence in Intrusion Detection Systems: A Review," *Elsevier Applied Soft Computing*, vol. 10, issue 1, Jan. 2010, pp. 1–35.

[3] H. T. Elshoush and I. M. Osman, "Reducing False Positives through Fuzzy Alert Correlation in Collaborative Intelligent Intrusion Detection Systems — A Review," *Prof. IEEE Int'l. Conf. Fuzzy Systems*, July 2000, pp. 1–8.

[4] M. Sourour, B. Adel, and A. Tarek, "Environmental Awareness Intrusion Detection and Prevention System toward Reducing False Positives and False Negatives," *Proc. IEEE Symp. Computational Intelligence in Cyber Security*, Apr. 2009.

[5] G. P. Spathoulas and S. K. Katsikas, "Using a Fuzzy Inference System to Reduce False Positives in Intrusion

Detection," *Proc. 16th Int'l. Conf. Systems, Signals and Image Processing*, June 2009.

[6] I.-W. Chen *et al.*, "Extracting Attack Sessions from Real Traffic with Intrusion Prevention Systems," *Proc. IEEE ICC*, June 2009.

[7] S.-H. Wang, "Extracting, Classifying and Anonymizing Packet Traces with Case Studies on False Positives/Negatives Assessment," M.S. thesis, Dept. Comp. Sci., Nat'l. Chiao Tung Univ., Taiwan, 2010.

[8] Y.-D. Lin *et al.*, "On Campus Beta Site: Architecture Designs, Operational Experience, and Top Product Defects," *IEEE Commun. Mag.*, vol. 48, no. 12, Dec. 2010, pp. 83–91.

[9] TippingPoint Technologies, "IPS vs. IDS: Similar on the Surface, Polar Opposites Underneath," Whitepaper, http://rovingplanet.net/resources_whitepapers.html.

[10] "Global Market Share Statistics and News," http://marketshare.hitslink.com/os-market-share.aspx?qprid=9.

BIOGRAPHIES

CHENG-YUAN HO (cyho@csie.nctu.edu.tw) is an assistant research fellow in the Information and Communications Technology Laboratory of Microelectronics and Information Systems Research Center, Network Benchmarking Lab, and D-Link NCTU Joint Research Center at National Chiao Tung University, Hsinchu, Taiwan. His research interests include the design, analysis, and modeling of the congestion control algorithms, real-flow test, network security, cloud computing, high-speed networking, embedded hardware-software co-design, quality of service, and mobile and wireless networks. Ho received a Ph.D. in computer science from National Chiao Tung University, Taiwan, in 2008.

YUAN-CHENG LAI (laiyc@cs.ntust.edu.tw) received a Ph.D. degree in computer science from National Chiao Tung University in 1997. He joined the faculty of the Department of Information Management at National Taiwan University of Science and Technology in 2001 and has been a professor since 2008. His research interests include wireless networks, network performance evaluation, network security, and content networking.

I-WEI CHEN (iwchen@nbl.org.tw) received an M.S. degree in computer science and information engineering from National Chiao Tung University in 2003. He is the Director of the Network Benchmarking Laboratory at National Chiao Tung University. His research interests include network benchmark, network security, high-speed networking, real-flow test, and wire-speed switching and routing.

FU-YU WANG (sagual@nbl.org.tw) received an M.S. degree in computer science and information engineering from Chung Hua University, Taiwan, in 2007. He joined the Network Benchmarking Laboratory at National Chiao Tung University in 2008. His research interests include network security, botnet, real-flow certification, and quality of service.

WEI-HSUAN TAI (weihsuantai@gmail.com) received an M.S. degree in computer science from National Chiao Tung University in 2011. His research interests include network security, intrusion detection, and false positive and false negative analysis. His mentor is Dr. Cheng-Yuan Ho.