TRACKING ANALYSIS FOR NETWORK SECURITY

Nge

Information Technology Engineering Department, Technological University (Monywa), Myanmar

Abstract

The field of system security research has long been dominated by individual analysis results – either illustration of individual system vulnerabilities or expositions on the protection provided by individual security measures (e.g., firewalls, virus detectors, IDS systems, etc). These contributions, though clearly valuable, are difficult to evaluate without a complementary analysis context describing the prevalence and impact of various attacks, vulnerabilities, and responses. The need for empirical data of this type is critical, both for guiding future security research and to provide a well-reasoned basis for developing operational best practices. At the same time, there are tremendous challenges in collecting and analyzing network information at sufficient scale that these findings are globally meaningful. The system demonstrated for attacking these problems in the context of internet connected systems – particularly focusing on large-scale attacks such as denial-of-service and self-propagating network worms. Using a new technique, called "backscatter analysis". In this journal monitors to redirect a subset of packets to simulated hosts to automatically identify and characterize new worms as they emerge.

Keyword: Dos, Dos Attack, Attack Rate, Attack Duration, Backscatter Analysis

1.INTRODUCTION

Securing millions of interconnected hosts under autonomous administrative control is far more daunting, and yet that is the scope of the problem facing the internet today. In hindsight, it is obvious that the combination of unsecured resources, unrestricted communications, and virtual anonymity makes the internet an ideal environment for developing and targeting large scale distributed attacks. When a single attacker must the resources of several hundred hosts to overwhelm and effectively shut down several bellwether e-commerce sites. This was the first large-scale internet denial-of-Service (DoS) attack.

In this paper analyse network tracking measurements of network security analysis such as these are essential for understanding the scope of today's problems and the direction of tomorrow's, and for evaluating security technologies within an objective engineering context. Without this information, it is difficult to focus research efforts, operational practices, and policy decisions to best address these problems given the limited time and resources available[1].

There are multiple network tracking the widespread collection of such data. Generally, most individual corporations and service network providers do not have a monitoring infrastructure that allows network security threats to be detected and tracked. Moreover, those providers that do monitor security events usually treat the data as sensitive and private. Finally, even if all organizations provided open access to their networks, monitoring and analysing traffic from enough locations to obtain representative measures of internet-wide behaviour's a significant logistical challenge [2].

2. RELATED WORK

Denial-of-service attacks consume the resources of a remote host or network that would otherwise be used for serving legitimate users. The most damaging class of DoS attacks are flooding attacks that overwhelm a victim's CPU, memory, or network resources by sending large numbers of various requests. Because there is typically no simple way to distinguish the "good" requests from the "bad", it can be extremely difficult to defend against flooding attacks .Given the importance of these kinds of attacks, the system focus on monitoring flooding DoS attacks [3].

There are two related consequences to a flooding attack, the network load induced and the impact on the victim's CPU. To load the network, an attacker generally sends small packets as rapidly as possible since most network devices (both routers and network interface cards) are limited not by bandwidth but by packet processing rate. Therefore, packets-per-second are usually the best measure of network load during an attack[4].

Here the attacker sends a series of SYN (Synchronous) packets towards the victim using a series of random spoofed source addresses named B, C, and D. Upon receiving these packets the victim responds by sending SYN/ACKs (Acknowledgement) to each whose address was spoofed by the attacker[5].

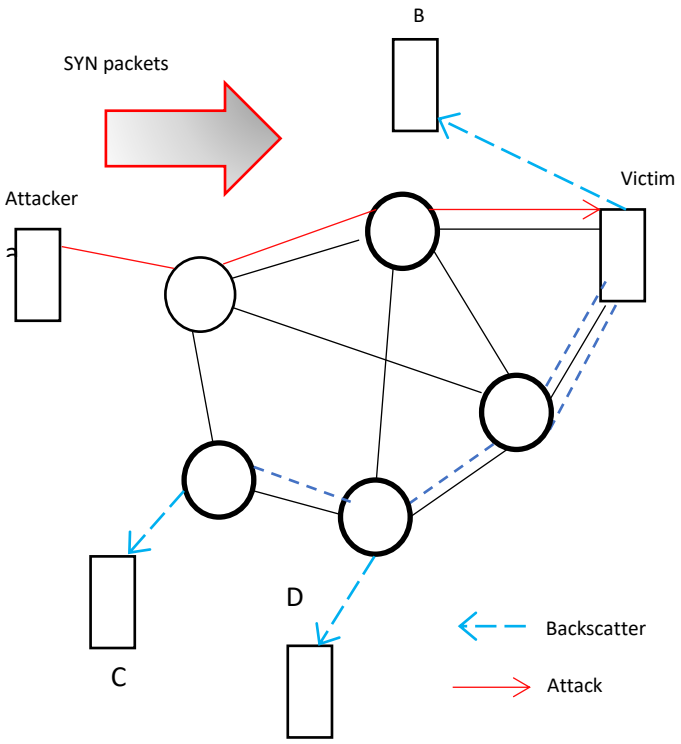

Figure 1: An illustration of backscatter in action.

An attacker often simultaneously attempts to load the victim's CPU by requiring additional processing above and beyond that required to receive a packet. For example, the best known denial-of-service attack is the "SYN flood" [12] which consists of a stream of TCP SYN packets directed to a listening TCP port at the victim. Without additional protection, even a small SYN flood can overwhelm a remote host. There are many similar attacks that exploit other code vulnerabilities including TCP ACK, data floods, IP fragment floods, ICMP (Internet Control Message Protocol) Echo Request floods, DNS Request floods, and so forth. Furthermore, attackers can mount more powerful attacks by combining the resources of multiple hosts in a distributed denial-of-service attack (DDoS). The backscatter technique is able to monitor flooding DoS attacks for all such code vulnerabilities and distributed attacks [6].

2.1. Backscatter Analysis

Attackers commonly spoof the source IP address field to conceal the location of the attacking host. The key observation behind our technique is that, for direct denial-of-service attacks, most programs select source addresses at random for each packet sent .When a spoofed packet arrives at the victim, the victim sends

what it believes to be an appropriate response to the faked IP address [7].

Because the attacker's source address is randomly selected, the victim's responses are equip-probably distributed across the entire internet address space, an inadvertent effect the traffic call "backscatter". Figure 1 illustrates this behaviour using an example of three hosts (B, C, and D) receiving backscatter packets due to one host attacking a victim.

Assuming per-packet random source addresses, reliable delivery, and one response generated for every packet in an attack, the probability of a given host on the internet receiving at least one unsolicited response from the victim is $\frac{m}{2^{32}}$ during an attack of m packets [8]. Similarly, if one monitors n distinct IP addresses, then the expectation of observing an attack is:

$$E(X) = \frac{nm}{2^{32}}$$

By observing a large enough address range, what the system refer to as a backscatter analysis[10], the system can effectively "sample" all such denial-of-service activity everywhere on the internet. Contained in these samples are the identity of the victim, information about the kind of attack, and a timestamp from which the system can estimate attack duration. Moreover, given these assumptions, the system can also use the average arrival rate of unsolicited responses directed at the monitored address range to estimate the actual rate of the attack being directed at the victim, as follows:

$$R \geq R^{i}\frac{2^{32}}{n}$$

Where R^{i} is the measured average inter-arrival rate of backscatter from the victim and R is the extrapolated attack rate in packets-per-second.

TABLE I
Summary of Dos attacks in the internet during three weeks

	Trace-1	Trace-2	Trace-3
Duration	01-08(days)	08-15(days)	15-22(days)
Unique victim IPs	1942	1821	2385
Unique victim DNS domain	750	693	876
Unique victim Network	1132	1085	1281
Unique victim system attacks	585	575	677

Table I, summarizes this data, collected three traces, each roughly spanning showing more than 5000 distinct victim IP address in more than 2000 distinct DNS domains[14].Across the entire period the system observed almost 200 million backscatter packets representing less than $\frac{1}{256}$ of the actual attack traffic during this period.

2.1.1. System Design

The system was described a traffic monitoring technique called backscatter analysis. The aim is focus on monitoring flooding Dos at tracks in different conditions

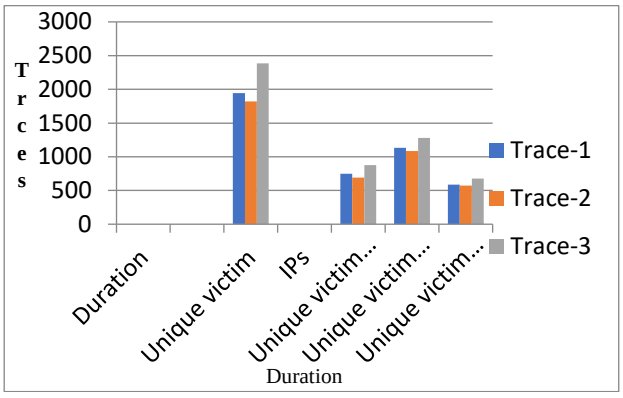

Fig 2: Estimate number of attacks per hours as a function

2.1.1.1. DoS Attack Activity over Time

Figure 2, shows a time series graph of the estimated number of actively attacked victims throughout the three traces, as sampled in one hour periods. There are two gaps in this graph corresponding to the gaps between traces [13]. The outliers on the three traces, with more than 150 victim IP addresses per hour, represent broad attacks against many machines in a common network. While most of the backscatter data averages one victim IP address per network prefix per hour, the ratio climbs to above five during many of the outliers.

3. SIMULATION RESULT

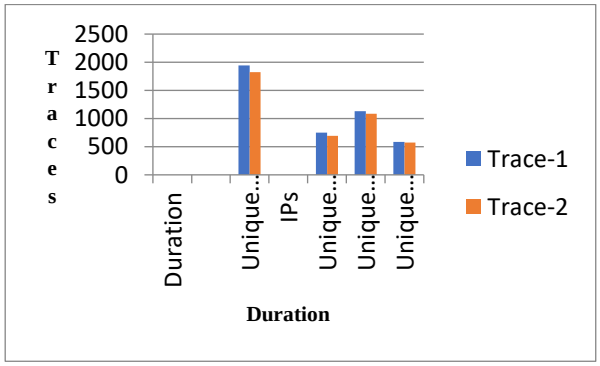

Fig 3: Performance comparison in various number of DoS attack over Trace-1 and Trace-2.

3.1. Attack Rate

Figure 3, estimate the attack rate by multiplying the average arrival rate of backscatter packets by 256 (assuming that an attack represents a random sampling across the entire address space, of which the system monitor$\frac{1}{256}$). Analyzing the distributions of attack rates across all attacks in three traces, the system found that 50% of all attacks have a packet rate greater than 350 packets/sec [9].

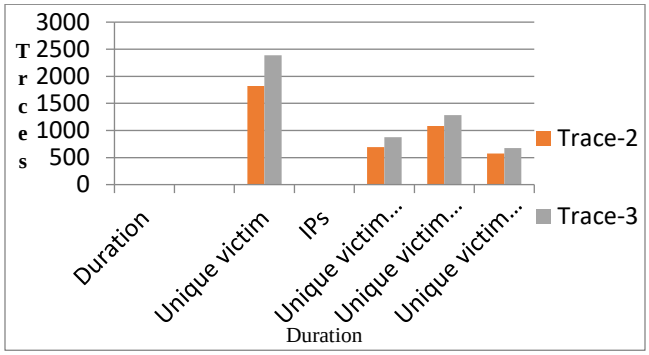

Fig 4: Performance comparison in various number of DoS attack over Trace-2 and Trace-3.

3.1.1. Attack Duration

Figure 4, estimate attack event rates characterize the intensity of attacks, the system do not give insight on how long attacks are sustained. Analyzing the distribution of attack durations, the system find that most attacks are relatively short: 50% of attacks are less than 10 minutes in duration, 80% are less than 30 minutes, and 90% last less than an hour [11]. However, the tail of the distribution is long: 2% of attacks are greater than 5 hours, 1% are greater than 10 hours.

4. CONCLUSIONS

Using backscatter analysis technique, the systems are able to observe global DoS activity in the Internet. Based upon the initial study, the system find that DoS activity is widespread across the Internet, some are intense and long-lasting, and a surprising number of attacks target machines and Internet services. This initial work forms the basis for the work that the system are proposing, including analyzing DoS attacks over long time scales to detect long-term trends, online analysis to infer the extent of damage on the victim and whether victims in

situated defenses and the efficacy of those defenses, and the impact of attacks on critical infrastructure.

REFERENCES

[1] B. Huffaker, D. Plummer, D. Moore, and k. claffy, "Topology discovery by active probing," inSymposiumonApplionInternet(SAINT),(Nara,Japan),SAINT,Jan2002.http://www.caida.org/outreach/papers/2002/SkitterOvererview/.

[2] [2] B. Huffaker, M. Fomenkov, D. Moore, E. Nemeth, and k. claffy, "Measurements of the Internet topology in the Asia-Pacific Region," in INET '00, (Yokohama, Japan), The Internet Society,18,21July2000.http://www.caida.org/outreach/papers/2000/asia_paper/.

[3] [3] B. Huffaker, M. Fomenkov, D. Moore, and k. claffy, "Macroscopic analyses of the infrastructure: measurement and visualization of Internet connectivity and performance," in PAM2001,(Amsterdam,Netherlands),RIPENCC,Apr2001,http://www.caida.org/outreach/papers/2001/SkitViz/.

[4] [4] B. Huffaker, M. Fomenkov, D. Plummer, D. Moore, and k. claffy, "Distance Metrics in the Internet," in IEEE International Telecommunications Symposium(ITS),(Brazil),IEEE,Sept2002.http://www.caida.org/outreach/papers/2002/Distance/.

[5] [5] M. Fomenkov, k. claffy, B. Huffaker, and D. Moore, "Macroscopic Internet Topology and Performance Measurements From the DNS Root Name Servers," in Usenix LISA, (San IEEE, Sept2002.Diego, CA), Use nix, 4-7Dec 2001http://www.caida.org/outreach/papers/2001.

[6] [6] C. Dovrolis, P. Ramana than, and D. Moore, "What do packet dispersion techniques measure?,"

[7] [7] C. Shannon, D. Moore, and k. claffy, "Beyond Folklore: Observation on Fragmented Traffic," ToappearinIEEE/ACMTransactionsonNetworking,Dec2002.http://www.caida.org/outreach/papers/20Frag/Rssac20001/.

[8] [8] D. Moore, K. Keys, R. Koga, E. Lagache, and k. claffy, "CoralReef software suite as a tool for system anetwork administrators," in Usenix LISA, (San Diego, CA), Usenix, 4-7 Dec 2001. http://www.caida.org/outreach/papers/2001/CoralApps/. INFOCOM2001,(Alaska),Apr2001.

[9] [9] D. Moore, R. Periakaruppan, J. Donohoe, and k. claffy, "Where in the world is netgeo.caida.org?," in INET'00, (Yokohama, Japan), The Internet Society,18-21Jul2000. http://www.caida.org/outreach/papers/2000/inet_netgeo/.

[10] [10] D. Moore and C. Shannon, "The spread of the code-red worm (crv2)."http://www.caida.org/analysis/security/codered/coderedv2_analysis.xml.

[11] [11] D. Moore, G. M. Voelker, and S. Savage, "Inferring Internet Denial-of-Service Activity," Usenix Security Symposium,2001.

[12] [12] Computer Emergency Response Team, "CERT Advisory CA-1996-21 TCP SYN Flooding Attacks." http://www.cert.org/advisories/CA-1996-21.html, Sept. 1996.

[13] [13] D. Moore, "Network telescopes: Observing small or distant security events,"Aug.2002.

[14] [14] K. Keys, D. Moore, R. Koga, E. Lagache, M. Tesch, and k. claffy, "The architecture of CoralReef: an Internet traffic monitoring software suite,"in PAM 2001, (Amsterdam, Netherlands), RIPE NCC,Apr2001.http://www.caida.org/outreach/papers/2001/CoralArch/.