Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI '05)

July 7, 2005, Cambridge, MA

Summarized by Jayanthkumar Kannan and Lakshminarayanan Subramanian, and edited by Balachander Krishnamurthy

SRUTI, a first-time USENIX workshop, sponsored by AT&T Labs, Cisco Systems, and the Department of Homeland Security, was attended by 55 people, and 13 peer-reviewed papers were presented.

DDOS AND WORMS

- *Using Routing and Tunneling to Combat DoS Attacks*

Adam Greenhalgh, Mark Handley, and Felipe Huici, University College London

The first session of the SRUTI workshop focused on different forms of network-level filtering mechanisms to defend against DDoS and worm attacks. The first paper argues that while many existing DoS defense mechanisms are hard to deploy, one can use a combination of routing and tunneling techniques to obtain a deployable DoS defense. The basic idea is to tunnel the traffic bound to a server across a fixed set of control points (edge routers in ISPs), which act as IP-level filtering gateways and use underlying routing protocols (e.g., I-BGP, E-BGP, OSPF) to signal information across different control points. The concept of using naming and path information as separate entities to force inspection at different control points is potentially applicable in other network security mechanisms.

- ***Reducing Unwanted Traffic in a Backbone Network***

Kuai Xu and Zhi-Li Zhang, University of Minnesota; Supratik Bhattacharyya, Sprint ATL

This paper shows how one can observe the communication patterns of end-hosts and use this information to determine unwanted traffic within the backbone of an ISP. The goal is to use the behavioral profile of each end-host based on IP header information and the Zipf-like nature of traffic characteristics to identify and filter the large sources of unwanted traffic. One open question remains: Under what constraints can good traffic be separated from bad traffic based only on observing the IP header information?

- ***Analyzing Cooperative Containment of Fast Scanning Worms***

Jayanthkumar Kannan, Lakshminarayanan Subramanian, Ion Stoica, and Randy H. Katz, University of California, Berkeley

The final paper in this session focused on analyzing the effectiveness of different cooperative strategies for worm containment, specifically, on the relationship between the type of signaling between firewalls and the level of containment. This paper illustrates that the signaling strategy essential for good containment depends on various factors, including the reproduction rate of the worm (i.e., the number of new hosts one vulnerable host affects), the level of malice, and the extent of deployment. How to generate robust and succinct worm filters with a low false-positive probability remains a goal for future work.

SPAM-1

- ***Push vs. Pull: Implications of Protocol Design on Controlling Unwanted Traffic***

Zhenhai Duan and Kartik Gopalan, Florida State University; Yingfei Dong, University of Hawaii

The second session was the first of two that focused on spam evasion and detection. This paper proposes a simple design principle for communication protocols that help participants avoid unwanted traffic. The main observation is that a receiver-pull approach is superior to a sender-push approach in the degree of control offered to a recipient. However, in some applications, such as email, a pure receiver-pull approach is not possible, since communication is initiated by the sender. For such applications, a sender-intent receiver-pull approach is proposed, where the sender first sends a short intent-to-send message, on the basis of which the receiver makes the decision to accept or reject the message. The principal advantage of this approach is the potential bandwidth savings, since the receiver does not need to download the entire message. As pointed out by one workshop participant, this basic idea has been proposed before, but this paper suggests a way of implementing it using simple extensions to SMTP.

- ***Detecting Spam in VoIP Networks***

Ram Dantu and Prakash Kolan, University of North Texas, Denton

This paper deals with the problem of spam detection in VoIP networks. VoIP spam is likely to be more irritating to users than email spam, since VoIP is synchronous. In VoIP spam detection, the decision about spam potential has to be made using only the initial context of the message and cannot be dependent on the content of the entire message. The paper proposes a multi-stage VoIP spam identification mechanism that involves several building blocks such as Bayesian detection, rate limiting, and blacklisting. This mechanism also leverages the social network of caller-callee relationships in deducing the reputation of a caller.

BOTS AND SPOOFED SOURCES

- ***The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets***

Evan Cooke and Farnam Jahanian, University of Michigan; Danny McPherson, Arbor Networks

A common message from this session was the need for security developers to share information in order to keep pace with the growing sophistication of Internet attacks.

The first paper illustrates the prevalence of bots on the Internet, where thousands of new bots show up on a daily basis, and it describes different techniques for detecting and disrupting botnets. Among the different detection strategies, this paper stresses the need for a behavioral methodology for analyzing IRC traffic from end-hosts to detect bot communication. One challenge in measuring the prevalence of bots is that one needs to be part of several botnets to perform such measurements, raising legal issues.

- ***An Architecture for Developing Behavioral History***

Mark Allman and Vern Paxson, International Computer Science Institute; Ethan Blanton, Purdue University

This paper examines how architecture can aid in determining the sources of unwanted traffic where the identity of a source can be in different granularities (e.g., email, end-host). The grand vision is to build a repository that consists of the sources of different forms of malicious traffic, with the challenges that the architecture be scalable, open system, distributed, robust, abe to handle various types of traffic, and policy neutral. To detect bogus information in this repository, one would need audit trails for evidence and the ability to assess the reputation of reporters and corroborate different entries for correctness in the system.

- *The Spoofer Project: Inferring the Extent of Internet Source Address Filtering on the Internet*

  Robert Beverly and Steve Bauer, MIT

  The final paper in this session describes a measurement study to quantify the extent and nature of source address filtering. Among the important findings are that a significant number of netblocks allow some form of spoofing, filtering is applied inconsistently, filtering policies correspond to netblocks in BGP, and no specific geographic patterns abound in spoofing.

ADAPTIVE DEFENSE SYSTEMS

- *Stress Testing Traffic to Infer Its Legitimacy*

  Nick Duffield and Balachander Krishnamurthy, AT&T Labs—Research

  This paper proposes stress testing as a general approach to distinguish between legitimate and malicious traffic. By inducing artificial impediments to traffic and examining the reaction of the sender, one can deduce whether the traffic is malicious. This idea is predicated on two points: (1) differentiation: response to impairment differs between malicious traffic and legitimate traffic; and (2) recovery: legitimate traffic can deal with impairments. They examine the applicability of these principles in different domains, such as TCP, HTTP, UDP, SMTP, and BGP. The extent to which a TCP sender backs off in response to an induced loss can be used as a metric of the malice of the sender. The frequency of HTTP connection establishment in response to a "Service unavailable" message can be used similarly. The authors are also working on evaluation of these techniques over normal traffic. One comment by an audience member was that stress testing may lead to an increase in the total traffic under certain conditions.

- *Adaptive Defense Against Various Network Attacks*

  Cliff C. Zou, University of Massachusetts; Nick Duffield, AT&T Labs—Research; Don Towsley and Weibo Gong, University of Massachusetts

  This paper proposes a general way to adaptively tune an attack detection mechanism in response to the volume of attack traffic. The basic idea is to periodically vary parameters in a detection mechanism so as to optimize an objective function that includes penalties for missed attacks (false negatives) and incorrect alarms (false positives). This is based on the intuitive observation that a higher false positive probability is tolerable during periods of high attack. This technique is applied to two detection mechanisms known in literature: the hop-count filtering method for detecting spoofed SYN flood attacks, and the threshold random walk for defending against worms. This paper provoked considerable discussion among attendees regarding the pros and cons of such adaptive defense techniques. While it is clear that smart attacks (such as pulsed DoS attacks) are still viable against adaptive defense mechanisms, it was generally agreed that adaptive defense would reduce the impact of the attack.

SPAM-2 AND ENCRYPTION

- *HoneySpam: Honeypots Fighting Spam at the Source*

  Mauro Andreolini, Alessandro Bulgarelli, Michele Colajanni, Francesca Mazzoni, and Luca Messori, Università di Modena e Reggio Emilia

  The final session dealt with email spam detection and encryption mechanisms. The first paper described the architecture of HoneySpam, a honeypot implementation to reduce spam. The goal is counter-cultural in that it encourages spammers to use the system to send spam so that HoneySpam can then identify the spammers, traffic-shape them, and provide them with incorrect information to hinder their progress. The challenge is to hide the identity and location of the HoneySpam system.

- *Improving Spam Detection Based on Structural Similarity*

  Luiz H. Gomes, Fernando D.O. Castro, Virgilio A.F. Almeida, Jussara M. Almeida, and Rodrigo B. Almeida, Universidade Federal de Minas Gerais; Luis M.A. Bettencourt, Los Alamos National Laboratory

  This paper deals with improving traditional spam detection algorithms using information regarding the social networks of the sender and the recipient. All senders are grouped into clusters based on the similarity of the recipients they send mail to. Similarly, receivers are grouped into clusters based on the senders who have contacted them in the past. The probability that a particular email is spam is computed based on the extent to which the sender's (recipient's) cluster have sent (received) spam in the past. This decision is used to augment a Bayesian classifier, and the results demonstrate that false positives are reduced, but not by a significant amount. A question on the scalability of the system to several thousands of senders/receivers was raised, and the author suggested schemes like LRU aging to deal with this issue.

- *Lightweight Encryption for Email*

  Ben Adida, Susan Hohenberger, and Ronald L. Rivest, MIT

  The final paper leverages identity-based encryption (IBE) techniques for easing the use of encrypted email. The basic idea is to leverage DNS as a distribution mechanism for public keys at the domain level. In IBE, a sender can use the recipient's email address along with a master public key (MPK) to derive the recipient's public key. The paper suggests that each email domain should designate a set of key servers that would generate an MPK jointly and distribute it via DNS. These key servers would communicate the secret key for an email address in their domain by simply sending it via email. For additional security, a recipient could also publish a second public key on a broadcast channel. The security of this scheme is dependent on that of DNS and the channel between the key server and the recipient.

One comment raised was that the ease of deriving the public key for a particular recipient might also allow a spammer to encrypt messages and render them unreadable by spam filters.

writing for ;login:

Writing is not easy for most of us. Having your writing rejected, for any reason, is no fun at all. The way to get your articles published in *;login:*, with the least effort on your part and on the part of the staff of *;login:*, is to submit a proposal first.

PROPOSALS

In the world of publishing, writing a proposal is nothing new. If you plan on writing a book, you need to write one chapter, a proposed table of contents, and the proposal itself and send the package to a book publisher. Writing the entire book first is asking for rejection, unless you are a well-known, popular writer.

;login: proposals are not like paper submission abstracts. We are not asking you to write a draft of the article as the proposal, but instead to describe the article you wish to write. There are some elements that you will want to include in any proposal:

- What's the topic of the article?
- What type of article is it (case study, tutorial, editorial, mini-paper, etc.)?
- Who is the intended audience (syadmins, programmers, security wonks, network admins, etc.)?
- Why does this article need to be read?
- What, if any, non-text elements (illustrations, code, diagrams, etc.) will be included?
- What is the approximate length of the article?

Start out by answering each of those six questions. In answering the question about length, bear in mind that a page in *;login:* is about 600 words. It is unusual for us to publish a one-page article or one over eight pages in length, but it can happen, and it will, if your article deserves it. We suggest, however, that you try to keep your article between two and five pages, as this matches the attention span of many people.

The answer to the question about why the article needs to be read is the place to wax enthusiastic. We do not want marketing, but your most eloquent explanation of why this article is important to the readership of *;login:*, which is also the membership of USENIX.

UNACCEPTABLE ARTICLES

;login: will not publish certain articles. These include, but are not limited to:

- Previously published articles. A piece that has appeared on your own Web server but not been posted to USENET or slashdot is not considered to have been published.
- Marketing pieces of any type. We don't accept articles about products. "Marketing" does not include being enthusiastic about a new tool or software that you can download for free, and you are encouraged to write case studies of hardware or software that you helped install and configure, as long as you are not affiliated with or paid by the company you are writing about.
- Personal attacks

FORMAT

The initial reading of your article will be done by people using UNIX systems. Later phases involve Macs, but please send us text/plain formatted documents for the proposal. Send proposals to login@usenix.org.

DEADLINES

For our publishing deadlines, including the time you can expect to be asked to read proofs of your article, see the online schedule.

COPYRIGHT

You own the copyright to your work and grant USENIX permission to publish it in ;login: and on the Web. USENIX owns the copyright on the collection that is each issue of *;login:*. You must grant permission for any third party to reprint your text; financial negotiations are a private matter between you and any reprinter.

FOCUS ISSUES

In the past, there has been only one focus issue per year, the December Security edition. In the future, each issue will have one or more suggested focuses, tied either to events that will happen soon after *;login:* has been delivered or events that are summarized in that edition.

PROFESSORS, CAMPUS STAFF, AND STUDENTS— DO YOU HAVE A USENIX REPRESENTATIVE ON YOUR CAMPUS? IF NOT, USENIX IS INTERESTED IN HAVING ONE AT YOUR UNIVERSITY!

The USENIX University Outreach Program is a network of representatives at campuses around the world who provide Association information to students, and encourage student involvement in USENIX. This is a volunteer program, for which USENIX is always looking for academics to participate. The program is designed for faculty who directly interact with students. We fund one representative from a campus at a time. In return for service as a campus representative, we offer a complimentary membership and other benefits.

A liaison's responsibilities include:

- Maintaining a library (online and in print) of USENIX publications at your university for student use
- Distributing calls for papers and upcoming event brochures, and re-distributing informational emails from USENIX
- Encouraging students to apply for travel stipends to conferences
- Providing students who wish to join USENIX with information and applications
- Helping students to submit research papers to relevant USENIX conferences
- Providing USENIX with feedback and suggestions on how the organization can better serve students

In return for being our "eyes and ears" on campus, liaisons receive a complimentary membership in USENIX with all membership benefits (except voting rights), and a free conference registration once a year (after one full year of service as a campus liaison).

To qualify as a campus representative, you must:

- Be full-time faculty or staff at a four year accredited university
- Have been a dues- paying member of USENIX for at least one full year in the past

For more information about our Student Programs, see
http://www.usenix.org/students

USENIX contact: Tara Mulligan, Scholastic Programs Manager, tara@usenix.org