Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 2, Issue 13; July-September, 2015 pp. 58-61

http://www.krishisanskriti.org/Publication.html

Tools and Techniques for Network Forensics

Swati Srivastava[1] and Gaurav Srivastava[2]

[1]Department of Computer Science and Engineering Naraina Vidya Peeth Engineering And Management Institute
[2]Department of Electrical Engineering Poornima college of Engineering
E-mail: [1]srivastavaswati2011@gmail.com, [2]gaurav.aryan.srivastava4@gmail.com

Abstract—*Network forensics deals with the capture, recording and analysis of network events in order to discover evidential information about the source of security attacks in a court of law. This paper discusses the different tools and techniques available to conduct network forensics. Some of the tools discussed include: eMailTrackerPro–to identify the physical location of an email sender; Web Historian–to find the duration of each visit and the files uploaded and downloaded from the visited website; packet sniffers like Ethereal–to capture and analyze the data exchanged among the different computers in the network.*

Keywords: *Network Forensics, IP Traceback, Packet Sniffers, Legal Aspects*

1. INTRODUCTION

Internet usage has increased drastically in the past ten years. Recent studies revealthat today in the United States for every three people, one would be using the Internet for their personal activity, or for their business needs. As the number of people using the Internet increases, the number of illegal activities such as data theft, identity theft, etc also increases exponentially.

Computer Forensics deals with the collection and analysis of data from computer systems,networks, communication streams (wired and wireless) and storage media in a manneradmissible in a court of law. Network forensics deals with the capture, recording or analysis of network events in order to discover evidential information about the source of security attacks in a court of law. With the rapid growth and use of Internet, network forensics has become an integral part of computer forensics. This paper surveys the tools and techniques (efficient, easy to use and cost effective) available to conduct network forensics. Section 2 explains how to conduct "Email Forensics" using certain freely available tools such as *EmailTrackerPro* and *SmartWhoIs*. Spam emails are a major source of concern within the Internet community. The tools described in this Section could be used to trace the sender of an email. Section 3 describes how to conduct "Web Forensics" using freely available tools like *Web Historian* and *Index.dat analyzer*. These tools help to reveal the browsing history of a person including the number of times a website has been visited in the past and the duration of each visit, the files that have been uploaded and downloaded from the visited website, the cookies setup as part of the visits and other critical information. Section 4 describes the use of packet sniffers like *Ethereal* to explore the hidden information in the different headers of the TCP/IP protocol stack. These sniffers capture the packets exchanged in the Ethernet and allow the investigator to collect critical information from the packets.

2. EMAIL FORENSICS

Email is one of the most common ways people communicate, ranging from internal meeting requests, to distribution of documents and general conversation. Emails are now being used for all sorts of communication including providing confidentiality, authentication, non-repudiation and data integrity. As email usage increases, attackers and hackers began to use emails for malicious activities. Spam emails are a major source of concern within the Internet community. Emails are more vulnerable to be intercepted and might be used by hackers to learn of secret communication. Email forensics refers to studying the source and content of electronic mail as evidence, identifying the actual sender and recipient of a message, date/time it was sent and etc.

Emails frequently contain malicious viruses, threats and scams that can result in the loss of data, confidential information and even identity theft. The tools described in this section provide an easy-to-use browser format, automated reporting and easy tool bar access features. The tools help to identify the point of origin of the message, trace the path traversed by the message (used to identify the spammers) and also to identify the phishing emails that try to obtain confidential information from the receiver. *eMailTrackerPro*[4] analyzes the header of an email to detect the IP address of the machine that sent the message so that the sender can be tracked down. All email messages contain a header, located at the top of the email. The header contains the source of an email in the "From" line, while in the "Received" lines, the header lists every point the email passed through on its journey, along with the date and time. The message header provides an audit trail of every machine the email has passed through. The built-in location database in *eMailTrackerPro*helps to track emails to a country or region of the world, showing information on a global map. To trace an email message, one has to just copy and paste the header of the email in *eMailTrackerPro*and start the tool. A basic trace will be shown on the main Graphical User Interface and a summary report can be obtained. The summary report provides an option to report the abuse of the particular email address to the administrators of the sender and/or victim networks and also contains some critical information that can be useful for forensic analysis and investigation. The report includes the geographic location of the IP address from which the email was sent, and if this cannot be found, the report at least includes the location of the target's ISP. The report also includes the domain contact information of the network owner or the ISP, depending on the sender email address.

3. WEB FORENSICS

The predominant web browsers in use today are Microsoft's Internet Explorer (IE) and the Firefox/ Mozilla/ Netscape family. Each of these browsers saves, in their own unique formats, the web browsing activity (also known as web browsing history) of the different users who have accounts on a machine. IE stores the browsing history of a user in the index.dat file and the Firefox/ Mozilla/ Netscape family browsers save the web activity in a file named history.dat.

These two files are hidden files. So, in order to view them, the browser should be setup to show both hidden files and system files. One cannot easily delete these two files in any regular way. There is also no proof that deleting these files has sped up the browsing experience of the users.

4. IP TRACEBACK TECHNIQUES

Masquerade attacks [9] can be produced by spoofing at the link-layer (e.g., using a differentMAC address than the original), at the Internet layer (e.g., using a different source IP addressthan the original), at the transport layer (e.g., using a different TCP/IP port than the originalone), at the application layer (e.g., using a different email address than the original). Let $C = h1\text{->}h2\text{ -> } \ldots \text{ ->}hi \text{ ->}hi{+}1\text{-> } \ldots \text{ ->}hn$be the connection path between hosts $h1$ to hn. Then, the IPtraceback problem is defined as: Given the IP address hn, identify the actual IP addresses ofhosts $h\ n$-1, …,h1. If h1 is the source and $hn$is the victim machine of a security attack, then C iscalled the attack path.

Reconstruction of the attack path back to the originating attacker h1 may not be aStraightforward process because of possible spoofing at different layers of the TCP/IP protocolstack and also the intermediate hosts becoming compromised hosts, called stepping-stone, andacting as a conduit for the attacker's communication. The security functions practiced inexisting networks may also preclude the capability to follow the reverse path. For example, ifthe attacker lies behind a firewall, then most of the traceback packets are filtered at the firewalland one may not be able to exactly reach the attacker.

5.1 Input Debugging

After recognizing that it is being attacked, the victim develops an attack signature that describes common feature contained in all the attack packets. The victim communicates this attack signature to the upstream router that sends it the attack packets. Based on this signature, the upstream router employs filters that prevent the attack packets from being forwarded through an egress port and determines which ingress port they arrived on. The process is then repeated recursively on the upstream routers, until the originating site is reached or the trace leaves theboundary of the network provider or the Internet Service Provider (ISP). From now on, theupstream ISP has to be contacted to repeat the procedure.

5.2 Controlled Flooding

The victim uses a pre-generated map of the Internet topology to iteratively select hosts that could be coerced to flood each of the incoming links of the upstream router. Since the router buffer is shared by packets coming across all incoming links, it is possible that the attack packets have a higher probability of being dropped due to this flooding. By observing changes in the rate of packets received from the attacker, the victim infers the link through which the attack packet would have come to the upstream router. This basic testing procedure is then recursively applied on all the upstream routers until the source is reached. Though this method is both ingenious and pragmatic, using unsuspecting hosts to flood is itself a denial-of-service attack

5.4 Packet Marking Techniques

The idea behind the packet marking techniques is to sample the path one node at a time ratherthan recording the entire path. A "node" field, large enough to hold a single router address, inthe packet header is reserved. For IPv4, this would be a 32-bit field in the Options portion of theIP header. Upon receiving a packet, a router chooses to write its own address in the node fieldwith a probability p. Given that enough packets could be sent and the route remains stable, thevictim would receive at least one sample for every router in the attack path.

Assuming the probability of marking p is the same for every router, the probability ofreceiving a packet marked from a router d hops away and not marked by any other router sincethen is $p(1-p)d$-1. Fig. 2 illustrates the probability of receiving a packet marked from a router1, 2, 3, 4, 5 and 6 hops away and not marked by any other router on a 6-hop path for differentvalues of the individual probability of marking p.

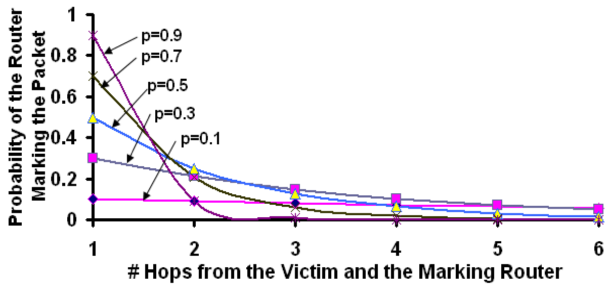

Fig. 2: Probability of Marking by a Vs Hop Count of Attack Path

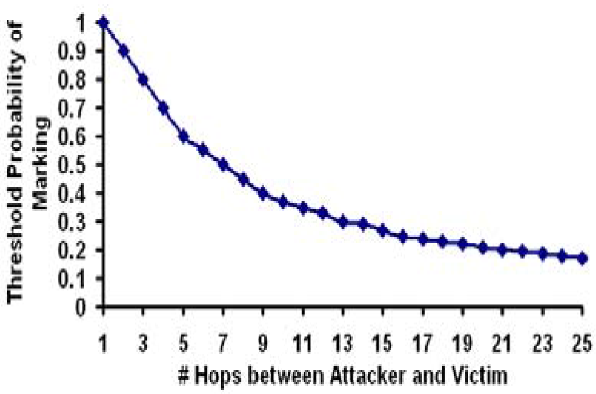

Fig. 3: Threshold Probability of Marking RouterVs Hop Count of Attack Path

The threshold probability of marking is defined as the minimum probability value to beassigned to every router on a path in order to guarantee with 99% probability that at least onerouter on the path will mark a packet. The threshold probability of marking decreases with theincrease in the number of hops. The larger the number of intermediate routers, the greater is thechance of at least one router in the path deciding to mark the packet. Fig. 3 shows thethreshold probability of marking as the number of hops is varied from 1 to 25.

The convergence time is defined as the minimum threshold number of packets required todetermine the sequence of routers that form the attack path. To determine the order of therouters in the attack path, each router on the path should have marked different number of timeson the packets. The router that is closest to the victim will have the highest number of marksand the router that is closest to the attacker will have the minimum number of marks.

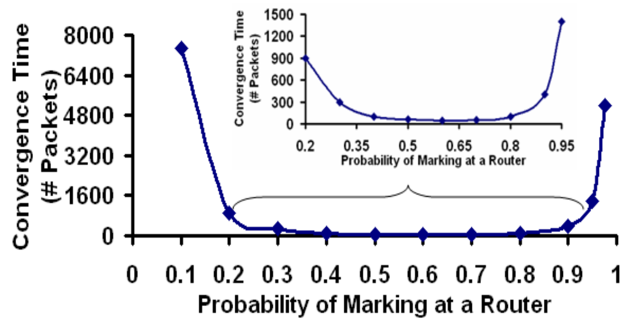

Fig. 4: Convergence Timefor a 3-hop Attack Path

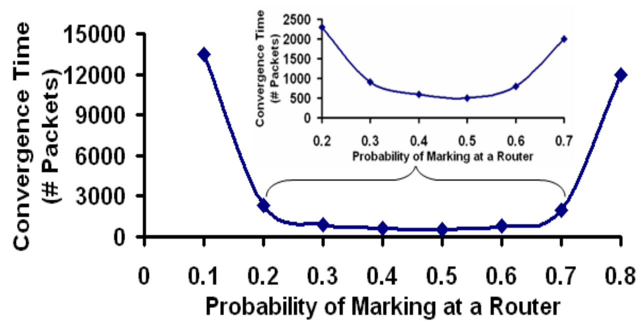

Fig. 5: Convergence Timefor a 6-hop Attack Path

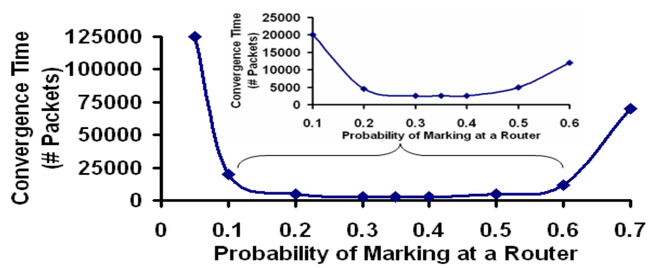

Fig. 6: Convergence Timefor a 9-hop Attack Path

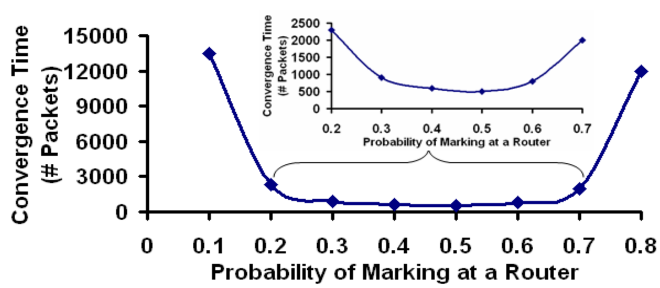

Fig. 7: Convergence Time for a 12-hop Attack Path

The value of the convergence time depends on the probability of marking by a router and thehop count of the attack path. Figures 4 through 9 show the convergence time measured fordifferent probability of marking values on attacks paths with different hop counts, measuredwith 95% to 97% confidence intervals. For a given hop count of the attack path, theconvergence time is minimum for a certain range of values for the probability of marking. Thevalue of the threshold marking probability decreases as the hop count of the attack path isincreased because the probability of any router on the attack path marking the packet increasesas the hop count increases. Thus, it is possible to reduce the threshold probability of marking apacket as the hop count increases. The minimum convergence time also increases as the hopcount of the attack path increases. This is because as the hop count increases, it takes more timefor a router closer to the attacker to have a packet marked such that the packet is not marked byany downstream router on the attack path. In order to lower the convergence time in larger hopcount attack paths, it is essential to assign a lower probability of marking for the routers.

5. CONCLUSIONS AND FUTURE WORK

The overall contribution of this paper is an exhaustive survey of the several tools and techniques available to conduct network forensics. All the tools surveyed in this paper are free to use, atleast available for trials. The paper explored in detail the different IP traceback mechanisms.

Simulations were run to find out the convergence time for attack paths with different lengthsand attack routers with different probabilities of marking.

In general, the security and forensic personnel need to keep up pace with the latest attack toolsand techniques adopted by the attackers. With freely available tools, one can enforce thesecurity mechanisms and analyze attack traffic only to a certain extent. To detect all kinds ofattacks and conduct a comprehensive forensic analysis, one would have to deploy and analyzethe effectiveness of commercial tools. This is the plan for future research. Future work wouldalso involve exploring the tools and techniques available for wireless network forensics.

REFERENCES

[1] http://www.time.com

[2] G. Kessler, “Online Education in Computer and Digital Forensics,” *Proceedings of the 40th Hawaii International Conference on System Sciences*, 2007.

[3] K. Sisaat and D. Miyamoto, “Source Address Validation Support for Network Forensics,”*Proceedings of the 1st Joint Workshop on Information Security*, Sep 2006.

[4] http://www.emailtrackerpro.com

[5] http://www.tamos.com

[6] http://www.mandian.com

[7] http://www.majorgeeks.com/index.dat_analyzer_d5259.html, last accessed: 04/03/2009

[8] http://www.ethereal.com

[9] S. Mitropoulos, D. Pastos and C. Douligers, “Network Forensics: Towards a Classification of Traceback Mechanisms,” *Proceedings of the Workshop on Security and Privacy for Emerging Areasin Communication Networks*, pp. 9–16, Sep 2005.

[10] Honeynet Project, http://www.honeynets.org

[11] V. Maheswari and P. Sankaranarayan, “Honeypots: Deployment and Data Forensic Analysis,” *International Conference on Computational Intelligence and Multi-media Applications*, May 2007.

[12] http://www.janusware.comInternational Journal of Network Security & Its Applications (IJNSA), Vol.1, No.1,April 200925