Adding digital forensic readiness to electronic communication using a security monitoring tool

F.R. Van Staden
Department of Computer Science
University of Pretoria
Pretoria, South Africa
ruan.vanstaden@up.ac.za

H.S. Venter
Department of Computer Science
University of Pretoria
Pretoria, South Africa
hventer@cs.up.ac.za

Abstract— **Electronic communication is used in our daily lives. One can receive email on a PC, Laptop or mobile phone. SMTP was designed to be an easy and cost-effective implementation. This fact, however, makes SMTP a target to be abused. Unsolicited electronic communication, also known as spam, is just one such example of abuse of email. Tracing the origin of spam by using the information contained in SMTP headers is not possible because SMTP is a clear text protocol and can easily be intercepted and modified.**

Digital forensic specialists are plagued with sifting through large data sets to find incident information. During the process of introducing digital forensic readiness the amount of information that is gathered is inadvertently increased, to ensure that the information is valid and usable. Drawing from the experience of digital forensic experts to find specific data subsets that prove or disprove that an incident occurred can be used to automate the analysis process. Data analysis tools are created for the purpose of sifting through data, looking for known data patterns, and storing these patterns as a subset of the original data.

Monitoring tools have been used successfully to gather information pertaining to the performance of IT systems. Security monitoring tools have been designed to collect security information in order to detect security breaches within the IT system. An extension to the security monitoring tool is proposed to gather security and usage information with regard to electronic communication. The collected information is saved in a database for future analysis.

Keywords- Digital Forensics, Digital forensic readiness, Digital forensic data analysis, gap-detection algorithm

I. INTRODUCTION

Spam is an inconvenience to electronic communication, but where is the harm? Since most anti-spam strategies are implemented either on the user's mail box or on the company's mail servers, the spam needs to be downloaded from an Internet Service Provider (ISP) before it can be scanned. This downloading has a direct impact on the bandwidth use of a company. The harmfulness of spam can thus be calculated in monetary value. The implementation of anti-spam strategies also has its own cost implications.

Spam can clog up the electronic communication lines of a company to such an extent that there is a loss of service and therefore a loss of revenue. According to Microsoft (1) 95.4 % of all email delivered in the first half of 2010 to Microsoft Exchange® servers was blocked as spam. However, the problem is that blocking spam does not lead to any consequences for spammers.

Employing digital forensic techniques to gather and analyze messaging information provides a new dimension to the fight against spam, which will lead to consequences for spammers. The authors investigated the possibilities of adding digital forensic readiness to electronic communications by augmenting SMTP and IP. Adding digital forensic readiness to SMTP and IP did not solve the problem of spoofing.

The paper introduces the design for a security monitoring system that adds digital forensic readiness to electronic communication. Probes are used to collect data from different areas of the electronic communication system. The data collected from the probes is stored for later digital forensic analysis.

The remainder of the paper is constructed as follows; Section two gives backround information on SMTP, IP, IPSec, Spoofing and Digital Forensic Readiness. Section three looks at the addition of digital forensic information to SMTP and IP. Section four looks at the security monitering system section five is the conclusion of the paper, where future work that will be needed, is discussed.

II. BACKGROUND

SMTP, IP, IPSec, Spoofing and Digital Forensic Readiness are discussed in the background section. SMTP and IP are discussed to show the development of the different protocols. The discussion on spoofing shows the developments that were proposed to combat spoofing. The digital forensic readiness sections show what is needed to make electronic communication digital forensically ready.

A. Simple Message Transfer Protocol

The Simple Mail Transfer Protocol, known as SMTP, was first proposed in the Request for Comments (RFC) 821 (2) in

August of 1982. RFC 1425 , (3) accepted in February 1993, described a way to extend the services SMTP offers, so that calling clients can ask what services are available on the server. SMTP Service Extensions are added to the core specification as the service extension becomes more popular. RFC 821 was made obsolete in April 2001 by RFC 2821 (4).The new specification included some service extensions and updates that were in use at the time. The latest RFC that describes SMTP is RFC 5321, released October 2008 (5).

Information in the SMTP headers is stored in clear text. Therefore the information can easily be edited. The possibility that the mail headers could have been edited makes the information in the headers suspect. Editing of the mail headers is done to hide information, like the origin of the email, from the receiving email box. The action of editing the mail headers to hide information is called spoofing and is discussed later in the paper. SMTP describes a header called the trace header. The next section gives a short description of the SMTP trace header.

B. SMTP trace header

The trace header consists of two sub headers, return-path and received headers. The return path header is used to store the address where error reports should be sent. The received header stores the delivery path with a data stamp for each delivery entry. The format of the trace header is defined in RFC 5322 (6) as the trace rule. The trace rules are defined in Augmented Backus-Naur Form (ABNF) which is defined in STD0068 (7).

The usage of the trace header is defined in RFC 5321 (5) for delivering error reports to the sender, as well as to create delivery reports that can be used as input information when doing trouble shooting. Klensin (5) proposes that the trace header should be made compulsory for all SMTP servers that implement the RFC 5321 standard.

The augmentation that will be discussed later is defined for the received header, therefore only the received rule for the received header is discussed. The received rule indicates that the received header must start with the word “Received” followed by a possible empty list of received-tokens. The list of received-tokens is followed by a date-time stamp and a Carriage Return Line Feed (CRLF) character that indicates the end of the received header entry.

The received-token rule indicates that the received-token must start with the word “from” followed by the address of the sending host. The received-token ends with the word “by”, followed by the receiving host’s address. Section C gives a short overview of the Internet Protocol (IP) and the Security Architecture for the Internet Protocol (IPSec).

C. Internet Protocol

Internet Protocol (IP) version 4 (IPv4) was first published in RFC 791 (8). RFC 2460 (9), published in December 1998, described the next generation Internet Protocol, IP version 6. IPv4 is still widely in use, although some network devices now support IPv4 and IPv6 and the ability to convert between the two protocol versions.

The specification for IPv4 and IPv6 describes an optional header called the Routing header. Inside the routing header there is an option called the record route. The record route option is updated for each datagram, by every router that the datagram passes through. The length of the Routing Header is set by the origin. When the maximum length is reached, no more addresses are added but an ICMP parameter problem message is sent to the origin of the message.

The Security Architecture for the Internet Protocol (IPSec) provides security functions for IPv4 and IPv6. IPSec was published in August 1995 in RFC 1825 (10) and describes the security services offered and how these services can be employed in the IP environment. The specification discusses the use of the IP Authentication header (AH), as defined in RFC 1826 (11) and the IP Encapsulating Security Payload (ESP), as described in RFC 1827 (12). IPSec was upgraded in November 1998, with the publication of RFC 2401 (9). Section D discusses email spoofing.

D. Spoofing

Email spoofing is the act of editing or falsifying the SMTP header information to hide the true origin or root of an email (13). Spoofing is also used to add fake validity to the content of an email by using a well known and trusted domain as the originating domain in order to perpetrate a phishing attack. RFC 4406 (14) is an experimental RFC that describes two tests for SMTP servers to perform, to verify that a mail header has not been spoofed.

The first test is the Purported Responsible Address (PRA) test (15). Lyon (15) describes a way to try and find the PRA inside the SMTP headers. If no PRA can be found, the email has a high probability of being spoofed. If the PRA can be established, it is still not proof that the SMTP header has not been spoofed, since the address used for the PRA, is the first well formed address the PRA algorithm found. The PRA needs to be tested further, to establish its validity.

The second test uses a Sender Policy Framework (SPF) (16) to authenticate if a SMTP client is allowed to act on behalf of the originating domain. Wong (16) proposes the SPF as a method to detect a spoofed email that uses valid domain information to appear legitimate. The supposed sender domain and the routing information in the header is authenticated by the DNS of the domain owner, to determine if the SMTP client’s domain has the authority to act on behalf of the supposed sending domain. If the DNS returns a failed authentication, the email is marked as possibly spoofed.

RFC 4871 (17) proposes Domain Key Identified Mail (DKIM) Signatures. DKIM defines a domain-level process that domain owners can use to verify that a message that was supposedly sent by the domain owner was actually sent by the domain owner. The verification process uses public-key cryptography and key sever technology to authenticate the message sender. Section E discusses digital forensic readiness.

E. Digital Forensic Readiness

Digital forensic science is a relatively new field of study that evolved from forensic science. According to the Oxford Dictionary (18), digital forensic science is the systematic

gathering of information about electronic devices, that can be used in a court of law. Digital forensic science is more popularly called digital forensics and sometimes also called computer forensics.

Palmer (19) defines digital forensics as "the use of scientifically derived proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events". Palmer's definition describes the digital forensic process whereas Oxford describes digital forensic science. The Digital Forensic Process Model (DFPM) by Kohn, et al. (20) states that "any digital forensic process must have an outcome that is acceptable by law".

Rowlingson (21) defines digital forensic readiness as consisting of two objectives. The first objective is to maximise the environment's capability of collecting digital forensic information and the second objective is to minimize the cost of a forensic investigation. Preparing any enviroment to be digital forensically ready, a mechanism will need to be added to preserve, collect and validate the information contained in the enviroment. The information gathered from the enviroment can then be used as part of a digital forensic investigation.

The remainder of the paper elaborates on the research conducted by the authors. Section three discusses the addition of digital forensic information to the Simple Message Transfer Protocol (SMTP) and the Internet Protocol (IP). Section four discusses the design of the security monitoring system.

III. Adding digital forensic readiness to SMTP and IP

This section discusses two approaches to adding digital forensic readiness to electronic communications, to show the previous work done. Although the addition of the validated token and the messaging header did not produce the desired results as originally anticipated by the authors, we feel that it is still an important discussion to include in the paper because it leads to our reasoning for introducing the security monitoring system as discussed in section four. Section A and B discuss the augmentation of the SMTP trace header with a validated token and the issues that were identified. Section C and D discuss the addition of the messaging header to IP and the issues that were encountered.

A. Augmenting the SMTP trace header

Adding digital forensic information to SMTP requires the addition of a hash value to verify the trace information. According to the background discussion of section II.E, digital forensic information must be verifiable. Looking at the trace header, the best place to store the hash value would be the received header. Two hash values are added to the original received rule. The first hash value appears after the "from" line that contains the value of the sending domain hashed together with the DNS lookup IP of the sending domain. The second hash value appears after the "by" line that contains the value of the host's domain hashed together with the DNS lookup IP address of the host's domain. Creation of the hash value is done using MD5 hashing to preserve the integrity of the received-token.

The received header was changed to contain at least one and only one received-token entry per line. The received header must contain at least one received token so that the digital forensic information is always present. Only one received-token entry is allowed per line to simplify the information extraction process. Section B discusses the issues encountered with the addition of the hash value to the received header.

B. Issues with augmenting the SMTP trace header

SMTP is an open protocol, which means that the information contained in the headers are human readable and easy to edit. The authors wanted to keep the token creation process as simple as possible, so that it fits with SMTP. The simple hash value creation process is easy to be copied and therefore does not give protection against spoofing.

The authors could not find a simple way of safeguarding the token information in the header but decided that safeguarding the information would have added too much complexity to SMTP. There was, therefore, no way to ensure that the tokens were not removed during message transportation. Thus the authors proved that it is possible to add digital forensic information to the received header although the information could not be safeguarded and therefore not truly trusted. Section C discusses the addition of digital forensic readiness by adding a hash token to the Internet Protocol.

C. Adding the Messaging header to IP

The digital forensic information is captured in a new optional header called the messaging header. Hash data is added to the routing header to create the messaging header. Information in the messaging header is updated by each router before the message is sent to the next router. At the origin, the messaging header is loaded with the origins address and a hash value. Generating the hash value is done by using the MD5 hashing function. Initially the hash value is generated using the origin and destination address. After the initial entry, every hash value is generated using the sending router address and the receiving router address.

The output is reconfigured according to the IP version of the datagram. If the datagram is IPv4 the hash value is reduced from 128 bits to 32 bits. If the datagram is IPv6, the hash value is kept at 128 bits. Before a router forwards the message, the message header is loaded with the current router's address and the hash value.

When a message is delivered to the final host, the IP header and messaging header information is saved for further processing. If a message is received without the messaging header, the message is marked with a high spam probability. Section D discusses the issues that were encountered by adding the messaging header to IP.

D. Issues encountered when adding the messaging header

The size of the messaging header could become a problem. The hash value is 32 bits for IPv4 and 128 bits for IPv6. If a

message is routed through 15 hops, the number of added bits is 960 bits for IPv4 and 3840 bits for IPv6. Depending on the frame size for a given network, the size of the messaging header might mean that it becomes detrimental to the efficiency of the transportation layer.

The presence of the messaging header is the only indication, to the routers, that the packets being sent belong to a message. The messaging header cannot be restarted during routing if the messaging header is removed. Unless the messaging header is created at the origin, the messaging header will not exist when the message is delivered. All the routers in the route must be set up to maintain the message header.

The need for all the routers to maintain the messaging header implies a change to all routers. According to (22) the rate of user adoption is directly proportional to the perceived value that is gained from the adoption. Since the addition of the messaging header cannot guarantee that the message is not spam, the cost might still be perceived as too high.

IV. Adding digital forensic readiness using a Security monitoring system

The security monitoring system makes use of different types of probes that collect data and send it to the security monitoring system to be stored. Each probe communicates with the monitoring system using private key encryption so that the probe data is secure and verifiable. The rest of the section discusses the DNS probe, network probe, SMTP probe and the anti-spam probe.

A. The DNS probe

The DNS probe collects data with regard to DNS requests for the SMTP server address. A record is made containing the address of the requesting server and the date-time that the request was received. It is assumed that the requesting server will use the correct address as the origin of a DNS request because the requested information must be returned to the requesters address. The next section discusses the network probe.

B. The network probe

The network probe collects data on all the SMTP traffic that passes through the network core. Data generated by the network probe contains the sender and receiver address of each SMTP interaction. A date-time stamp is added to the data set to enable data sets to be matched to data sets collected by the SMTP probe. The next section discusses the SMTP probe.

C. The SMTP probe

Data surrounding the activity of the SMTP servers are collected by the SMTP probe. The data set that is recorded contains the sender and receiver address as well as a date-timestamp. Data sets from the SMTP probe and the network probe have the same data structure. The next section discusses the anti-spam probe.

D. The anti-spam probe

The anti-spam probe collects data about spam that have been filtered by anti-spam software. Anti-spam data is generated by stripping the SMTP information, like the sender and receiver address, and storing it with a timestamp of when the spam was received. Information like the anti-spam rating of the email is also stored but in a different data set.

E. Using the data

The data collected will be used in digital forensic investigations of the electronic communication system. The data can also be analyzed to find known or new patterns that indicate some sort of event. An example would be detecting SMTP traffic on the network probe that cannot be detected on the SMTP probe might indicate a secondary SMTP server on the network. It could also indicate that there might be a botnet operating on the network. Matching the data from the different probes will at least give us a better understanding of how the electronic communication systems are used.

V. Conclusion

The paper discussed previous work of the authors to add digital forensic readiness to electronic communication. The previous work was not as successful because the proposed solutions could not combat spoofing. Trying to change the way SMTP and IP worked was not a cost effective idea.

The authors decided to look into a way to still add digital forensic readiness to electronic communication that would not rely on changing SMTP or IP. The paper proposes a probe based security monitoring system that collects digital data about the electronic communication system.

Future work will include implementing the monitoring system and analyzing the data to see what can truly be learnt from the data.

Acknowledgment

I would like to take this opportunity to express my respectful thanks to my supervisor Prof Venter for his continued input and guidance during this project. I would also like to thank my wife Isobel van Huyssteen for her help, support and patience. Lastly I offer my gratitude to the National Research Foundation and the University of Pretoria for the opportunity that was afforded me.

This work is based on research supported by the National Research Foundation of South Africa (NRF) as part of a SA/Germany Research cooperation programme. Any opinion, findings and conclusions or recommendations expressed in this material are those of the author(s) and therefore the NRF does not accept any liability in regard thereto.

References

[1] **Pecelj, Daryl and Arroyo, Jossie T.** Microsoft Security Intelligence Report Key Findings. *Microsoft Security Intelligence Report 2010.* s.l. : Microsoft, 2010. Vol. 9.

[2] **Postel, J.** Simple Mail Transfer Protocol. *RFC821.* s.l. : IETF, 1982. 821. Obsoleted by RFC 2821.
[3] **Klensin, J., et al.** SMTP Service Extensions. *RFC1425.* s.l. : IETF, 1993. 1425. Obsoleted by RFC 1651.
[4] **Klensin, J.** Simple Mail Transfer Protocol. *RFC2821.* s.l. : IETF, 2001. 2821. Obsoleted by RFC 5321, updated by RFC 5336.
[5] **Klensin, J.** Simple Mail Transfer Protocol. *RFC5321.* s.l. : IETF, 2008. 5321.
[6] **Resnick, P.** Internet Message Format. *RFC5322.* s.l. : IETF, 2008. 5322.
[7] **Crocker, D. Ed. and Overell, P.** Augmented BNF for Syntax Specifications: ABNF. *Augmented BNF for Syntax Specifications: ABNF.* 2008. 0068.
[8] **Postel, J.** Internet Protocol. *RFC791.* s.l. : IETF, 1981. 791. Updated by RFC 1349.
[9] **Deering, S. and Hinden, R.** Internet Protocol, Version 6 (IPv6) Specification. *RFC2460.* s.l. : IETF, 1998. 2460. Updated by RFCs 5095, 5722, 5871.
[10] **Atkinson, R.** Security Architecture for the Internet Protocol. *RFC1825.* s.l. : IETF, 1995. 1825. Obsoleted by RFC 2401.
[11] **Atkinson, R.** IP Authentication Header. *RFC1826.* s.l. : IETF, 1995. 1826. Obsoleted by RFC 2402.
[12] **Atkinson, R.** IP Encapsulating Security Payload (ESP). *RFC1827.* s.l. : IETF, 1995. 1827. Obsoleted by RFC 2406.
[13] **Allman, E and Katz, H.** SMTP Service Extension for Indicating the Responsible Submitter of an E-Mail Message. *RFC 4405.* [Electronic]. s.l. : The Internet Society, April 2006.
[14] **Lyon, J. and Wong, M.** Sender ID: Authenticating E-Mail. *RFC4406.* s.l. : IETF, 2006. 4406.
[15] **Lyon, J.** Purported Responsible Address in E-Mail Messages. *RFC4407.* s.l. : IETF, 2006. 4407.
[16] **Wong, M. and Schlitt, W.** Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1. *RFC4408.* s.l. : IETF, 2006. 4408.
[17] **Allman, E., et al.** DomainKeys Identified Mail (DKIM) Signatures. *RFC4871.* s.l. : IETF, 2007. 4871. Updated by RFC 5672.
[18] **Oxford.** AskOxford.com. *AskOxford.com.* s.l. : Oxford University Press, 2010.
[19] **Palmer, G.L.** Road Map for Digital Forensic Research. *Road Map for Digital Forensic Research.* [Electronic Publication]. s.l. : Digital Forensic Research Workshop (DFRWS), 2002.
[20] **Kohn, Michael, Eloff, J.H.P. and Olivier, M.S.** *UML Modelling of Digital Forensic Process Models (DFPMs).* [Document] Pretoria : Information and Computer Security Architectures (ICSA) Research Group University of Pretoria, 2009.
[21] **Rowlingson, R.** A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence.* 2004. Vol. II, 3.
[22] **Ozment, Andy and Schechter, Stuart E.** Bootstrapping the Adoption of Internet Security Protocols. *http://weis2006.econinfosec.org/.* [Online] June 26, 2006. [Cited: March 21, 2011.] http://weis2006.econinfosec.org/docs/46.pdf.