SECURING THE WEB DOMAIN BASED ON HASHING

Jyoti P. Asabe
Information Technology, Pune University

R. W. Deshpande
Information Technology, Pune University

Abstract - Now a day's risk of becoming a victim of spam and phishing attacks increases while accessing Internet. Many Web sites exhibit violent and illegal content. Most of users are now unable to protect their networks and themselves also. However, some countries have deployed systems for filtering the Web content. Since, the existing systems show high latency and over-blocking. Thus, an efficient method for Web filtering concept to protect users at the Internet service provider level is presented. The proposed solution can detect and block illegal and threatening Web sites. The suggested scalable software-based approach can examine Internet domains in wire speed without over-blocking. The Web filter serves as security measure for all connected users, especially for users with limited IT expert knowledge. This solution is totally transparent to all Network devices in the network. Setup, installation and maintenance can be created only by the Internet Service provider administrator. So, the suggested security system is safe from attacks from users and from the network side.

KEYWORDS: over-blocking, phishing, service provider administrator, web filtering.

I. INTRODUCTION

Providing security to the network is one of the most important tasks in today's Internet. There are various threats such as [1] viruses, malware, and phishing that are able to harm Internet users. Moreover, violent and illegal contents such as child pornography are found on the Internet. Users may use antivirus software and firewalls to protect their computers and networks against this malicious software. However, these kinds of programs do not give protection against [1] malicious Web content. As a preventive measure against this type of content, Web filters can be used. Users of computer have installed security Measures on computer. But installing security measures at the users' side has two serious drawbacks [1].

Firstly, threat detection is done on the target machine, which [1] is often already infected with malicious software. Second thing is that, the users must have install, maintain, and upgrade these security measures without any professional support. Especially, a Web filter is often not installed at all and requires additional maintenance [4]. Moreover, the majority of Internet users are missing the necessary expertise to configure their security Software so that it provides optimal protection. Therefore, it is mandatory to support users in issues of Internet security by means of a Web [1] filter.

A trustworthy place for the placement of a Web [1] filter is the ingress of the network – in the access network. Users, are referred to as subscribers by Internet Service Providers (ISPs), are connected to the Internet through the internet access network. The access nodes (ANs) [2] already present in the access network. As ANs are transparent for subscribers and the core network, these components are secure and safe from, e.g., Denial of Service attacks (DoS) which affect on ISP. In order to provide protection for subscribers, an AN is the optimal place to develop extra security Service for the dataset such as Web filter. With the help of this extra security feature, the user does not need to care about security measures himself [5]. However, although an ISP can take up new security [1] measures in its portfolio, various challenges have to be addressed:

- On an AN, high traffic rates (e.g., 1Gbit/s or More than that) have to be processed.
- The Web surfing experience of users must not be disturbed.
- Web sites, which are not malicious, must not be falsely [1] blocked by the Web filter.

The suggested approach was developed as part of the Secure Access Node (SecAN) project presented in [2] as "work in progress". Purpose of devoting SecAN is to protect the ordinary users of access networks. It deals with firewalls, intrusion detection systems and Web filters. Thereby, Web filtering functionality moves from the subscriber to the ISP [3]. This paper elaborates on the Web filter approach highlighting its benefits concerning speed, resource consumption, scalability, and distinct pattern matching. Briefly summarized, the main contributions of this paper are the following:

- A novel scalable software approach of a Web filter placed onto an AN is presented.
- The suggested architecture does not create false positives. Thus, only blacklisted domains will be blocked.

The system is able to control traffic with more than 1Gbit/s in wire speed on the target platform without packet loss.

In next section II we are presenting the literature survey over the various security methods at data sharing systems. In section III, the proposed approach and its system block diagram are depicted. In IV, we are presenting the current Status of the solution. Finally conclusion and future work is predicted in section V.

II. LITERATURE SURVEY

Several researchers have done the qualitative and quantitative analysis for Securing the Web Domain based on hardware and software using different techniques for this purpose, as well as many new techniques has introduced:

- Below we are discussing some of the J. Rohrbeck, V. Altmann, S. Pfeiffer and D. Timmermann, “Secure Access Node: an FPGA-based Security Architecture for Access Networks,” ICIW, 2011. Providing network security is one of the most important tasks in today’s Internet. Since, users do not have capability to protect themselves and also their networks.

- Therefore, we present a security concept to protect users at the Internet Service Provider (ISP) level. Now, ISP is already using various security measures, e.g. Virtual Local Area Network tags and limitation of MAC, or address translation of MAC. Our approach extends these security measures by a packet filter firewall and a deep packet Inspection engine. A firewall and a deep packet inspection system, at the ingress of the network, offers security measures to all the connected users, especially to those who have limited IT expert knowledge. The ISP Administrator can have an ability of adjustments. Consequently, our security system is safe against attacks from users and from the network side.

- R. Clayton, “Anonymity and traceability in cyberspace,” the risk of becoming a victim of spam and phishing attacks increases in today’s Internet. Most of the Web sites on World Wide Web show violent or not legal content. Since, Most of users are not able to protect themselves and their networks. Most of the countries have deployed the systems for filtering the Web content. However, solutions which are already present shows high latency and *over-blocking*. Thus, a Web filtering concept to protect users at the Internet Service provider level is presented. Ability of proposed system is that it can detect and block illegal and threatening Web sites are on the Web. The suggested scalable software-based approach examines Internet domains in wire speed without over blocking. The proposed system is totally transparent and flexible over network devices. Administrator is responsible for the setup and maintenance for Internet service provider (IPS). Consequently, the suggested security system itself is safe from attacks from users and from the network side.

- US District Court for the Eastern District of Pennsylvania, “CDT, ACLU, Plantagenet Inc. v Pappert, [1]” A firewall engine controls the header of Ethernet frames, Internet Packets, and the next following protocols. Furthermore, a Web filter method disables access to violent and child pornography Web content. The third subsystem is a Bloom filter-based deep packet inspection engine to observe the payload after the Protocol header. Possibilities of detecting network intruder are depending on deep Packet inspection. A firewall, a Web filter as well as a network intrusion detection system, at the ingress of the network, offer security measures [3] to all connected users, especially to users with limited IT expert knowledge. Each of the mentioned systems has a powerful packet classification engine and a high speed rule set engine used by the Firewall to find specific rules for each frame [3]. Consequently, the security system itself is secured against attacks from users and from the network side [10].

OVERVIEW OF PHISHING EMAILS

In this section, we discuss various types of phishing attacks, the life cycle of phishing email, email-analyzing methods, phishing email evaluation methods, features to detect phishing email, and feature selection and extraction methods. We discuss zero-day phishing email attacks in detail, and then compare this survey with existing work.

A. Various types of phishing attacks

Phishing is a particular type of spam. There are two techniques, deceptive phishing and malware-based phishing.

First technique was totally same as engineering dataset schemes, that are depend on forged email claims that are available to generate it from a legitimate organization and bank. Subsequently, through an embedded link within the email, the phisher attempts to redirect users to fake Websites. On the Web available fake Web sites are designed to fraudulently obtain financial data and private authenticated data (usernames, passwords, credit card numbers, and Personal information) from victims.

The second technique contain technical subterfuge schemes that rely on malicious code or malware after Phishing attach link embedded in the email, or by detecting and using privacy authentication security holes at the client machine (computer) to obtain the victim’s online account information directly [9]. Sometimes, phisher attempts to give wrong advice to the user from a fake Web site monitored by proxies. In the proposed design, our focus is on deceptive phishing

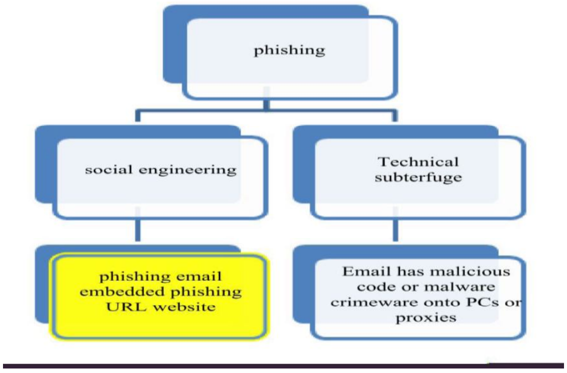
phishing
social engineering
Technical subterfuge
phishing email embedded phishing URL website
Email has malicious code or malware crimeware onto PCs or proxies

Fig. 1: Types of phishing attacks

using social engineering schemes, as it is one of the popular ways to steal victim's information by phishing. Figure 1 explains the various types of phishing attacks.

III. PROPOSED APPROACH FRAMEWORK AND DESIGN

3.1 PROPOSED SYSTEM:

Every subscriber is connected to the Internet by the access network. Access networks contain access nodes like Digital Subscriber Line (DSL) Access Multiplexers. Because the Web filter is located on an AN, a bandwidth of at Least 1 Gbit per second must be achieved. Therefore, the Web filter was designed and developed.

- **Web Filtering:** The purpose of protecting ordinary Internet users on internet, e.g., against malicious Web content, there are three general possibilities: Either IP addresses, URLs, or domain names can be controlled. The filtering of IP addresses can lead to crucial *over-blocking* since different Web sites can share the same Web server. Moreover, a Web site can move to a new Web server while [1] it remains accessible over the old domain names [11].

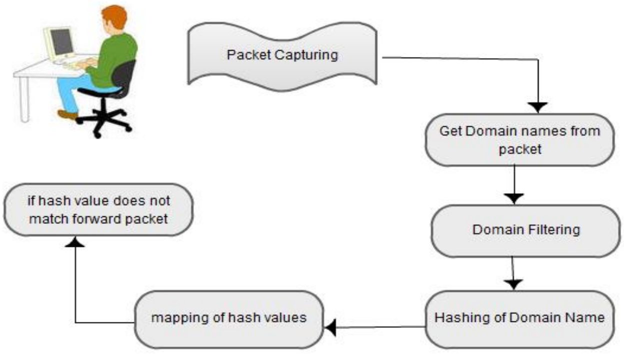

Fig 2: Proposed System Architecture

- Moreover, HTTP requests to proxies are checked, as well. HTTP redirections as used by URL shorteners are captured too, since the final request is still sent to the target domain. As the goal is to monitor the Web traffic, other protocols should not be blocked. Using HTTP monitoring, the Web filter cannot be simply bypassed by adding the IP address of the Web server into [8] the Local hosts file [8]. Based on the results, which highlight the benefits of HTTP filtering, it is advantageous to check domain names in HTTP requests.
- **1st level search architecture:** For the 1st level searching, hashing method is used. While the Web filter processes and caches the domain name, the hash value is calculated in parallel. The hash table is stored in a cache memory (BRAM) and thus access to it is very fast (one cycle) [1][7]. As hash function, parallel CRC64 was chosen as it provides optimal resource consumption in term of speed/collision ratio. The size of the hash table corresponds to the blacklist length.

- **2nd level search architecture:** The 2nd level search architecture contains plain text domain names and extra Meta information. The architecture shows a Buckets structure. Each bucket contains a domain name list with information on domains producing the same hash value.[9]

IV. WORK DONE

4.1 CURRENT STATUS

- **Packet Capturing:** It is the Process of intercepting and logging web traffic.
- **Domain name filtration:** In this we filter out domain which is not valid. If URL does not contain http:// then it is not valid URL, so we first filter this type of domain name.
- **Hashing of domain name:** In this process we apply hashing on domain names with its hash key means with unique hash key.
- **Block list:** Then at last makes list of blocked URLs which are not allowed to access in web browser.

V. CONCLUSION AND FUTURE WORK

In this paper, the working prototype of the [1] Web filter is presented. As hardware solution, it offers more advantages in terms of security and robustness than a software solution. The solution can control HTTP Traffic in wire speed without packet loss. On the test platform, 1 Gbit/s throughput is achieved. As a high speed Web filter, it can be deployed in the access Networks of ISPs.

Hereby, the suggested solution can protect users without IT expert knowledge from illegal, aggressive, violent or threatening Web-contents like child Pornography or phishing. It is unable to produce false positives. Thus, only blacklisted domains will get blocked. The configuration of the blacklist can be done only by the ISP administrator. Since it is fully transparent for all network participants, it is safe from attacks. Prospectively, the functionality of the Web [1] filter can be extended to URL filtering allowing blocking specific resource.

REFERENCES

[1] Vlado Altmann, Jens Rohrbeck, Jan Skodzik, Maik Roennau, Matthias Ninnemann, 2013 "*SWIFT: A Secure Web Domain Filter in Hardware*", ICAINAW

[2] S. Ooghe, N. Voigt, M. Platnic, et al., May 2010. [Online]., "*Framework and Requirements for an Access Node Control Mechanism in Broadband Multi-Service Networks,*" Internet Requests for Comments, RFC Editor, RFC 5851, Available: http://www.rfc-editor.org/rfc/rfc5851.txt

[3] J. Rohrbeck, V. Altmann, S. Pfeiffer, and D. Timmermann, 2011 "Secure *Access Node: an FPGA-based Security Architecture for Access Networks,*" ICIW.

[4] R. Clayton, Nov. 2005 "*Anonymity and traceability in cyberspace,*" ACM SIGACT News, vol. 36, no. 653, pp. 115–148.

[5] US District Court for the Eastern District of Pennsylvania, September 2004, "*CDT, ACLU, Plantagenet Inc. v Pappert,*" 337 F.Supp. 2d 606.

[6] R. Clayton, S. J. Murdoch, and R. N. M. Watson, June 2006, "*Ignoring the great firewall of china,*" 6th Workshop on Privacy Enhancing Technologies, no. 16.

[7] Telenor Norge, "*Telenor and krips introduce internet child pornography filter,*" Telenor Press Release, September 2004. [Online]. Available: http://presse.telenor.no/PR/200409/961319 5.html

[8] King Abdulaziz City for Science and Technology, 2004, "Local *content filtering Procedure,*" Internet Services Unit. [Online]. Available: http://www.isu.net.sa/saudi-internet/contenet-filtring/filtringmechanism. htm

[9] The Open Net Initiative, 2005 "*Internet filtering In Burma, in 2005: A country study,*" [Online]. Available: http://opennet.net/sites/opennet.net/files/ ONI Burma Country Study.pdf

[10] Barracuda Networks, "*Barracuda web filter,*" 2012. [Online]. Available: http://www.barracudanetworks.com/ns/downloads/Datasheets/ Barracuda Web Filter DS US.pdf

[11] Lue Coat ProxySG, 2012. [Online]. Available: http://www.bluecoat.com/products/proxysg