International Conference on Advancements in Engineering, Technology and Sciences
Dhaanish Ahmed College of Engineering, Chennai (ICAETS-2018)
(Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai)
16th-17th March 2018 www.conferenceworld.in ISBN : 978-93-87793-11-8

SERVING THE NET BY APPLYING E-MESSAGE TUNNELS(SNAET)

Muthazagan.R[1],Nishar Ali.A[2], B.Manikandan[3]

[1,2,3]Final Year Computer Science and Engineering[1,2], Associate professor[3]

Dhaanish Ahmed college of engineering, Padappai, Tamilnadu.

ABSTRACT

Internet censorship is control or suppression of the publishing or accessing of information on the Internet. Internet filtering is on the rise in the world today.Communication over the internet is a tread to the user, because the censorship can easily identified and blocked. With so many websites existing, it will be impossible to categorize each one as 'harmful' or 'safe, or such. This means that there could be sites that are actually helpful that can be banned too. It can also promote ignorance about important events and developments in the world. The network traffic of the internet is also high so the availability also reduced due to censorship.To overcome these issues we proposed SNAET (SERVING THE NET BY APPLYING E-MESSAGE TUNNELS). SNETworks based on encapsulating a censored user's traffic inside email messages that are carried over public email services. It also provide better performance in web browsing and network traffic.

Keywords:Censorship, Communications, Network traffic,Encapsulation.

I .INTRODUCTION

Today's Internet provides users with an environment to freely communicate and to exchange ideas and information with others from around the world. However, free communication continues to threaten repressive regimes, as the open circulation of information and speech among their citizens can pose serious threats to their existence. Recent unrest in the Middle Eastdemonstrates that the Internet can be widely used by citizens under these regimes as a very powerful tool to spread censored news and information, inspire dissent, and organize events and protests.A desire to capture the economic benefits of networked computing while maintaining control over the public's Internet exposure has led to a variety of strategies to split the difference between allowing unfettered access to the global Net and refusing to countenance any deployment beyond trusted elites.As with most technical filtering regimes, whether implemented at the client, Internet service provider, or backbone level, no list of the sites blocked or the methodologies used to block them has been made available by those doing the filtering. Further, while the government-connected Internet Society (not a chapter of the international Internet Society) has asked ISPs and content creators to sign a pledge that includes self-filtering, few official statements document that government-maintained Web filtering exists, much less the criteria employed and thresholds necessary to elicit a block.

Censorship is the main focus here. Specifically, the objective of this research is to increase awareness of the ramifications and negative consequences of Internet censorship and to advance the state 2 of the art of circumvention technologies [3].

The task of maintaining the status-quo through effective censorship policies is undergoing rapid change due to the growth and diversity of different devices and networks including:

- Web traffic
- Email (e.g., Gmail)
- P2P file-sharing
- Video (e.g., YouTube)
- Texting and messaging (e.g., Twitter)
- VoIP (e.g., Skype)
- Social Networks (e.g., Facebook)

The Internet poses a new challenge to such censorship because of the breadth of online content, the rapidity with which sources of content can be moved or mirrored, and because content sources are often remote from jurisdiction.

SNAET provides several key advantages as compared to the existing circumvention systems. First, since email is an essential service in today's Internet it is very unlikely that a censorship authority will block all email communications to the outside world, due to different financial and political reasons. This, along the fact that SNAET can be reached through any email service, provides a high degree of availability for SNAET since a censor will need to block all email traffic to the Internet in order to block SNAET. Second, by using encrypted email messages SNAET is highly unobservable from the censors. Third, the real-world deployment of SNAET does not require cooperation of any third-party entity, e.g., an ISP, a web destination, or even an specific email provider. Finally, unlike several recent proposals a SNAET user does not have to obtain any secret information in order to use SNAET, providing high user convenience and ensuring the security and privacy of the user.

II. RELATED WORK

In 2003 J. Zittrain and B. Edelmanproposed"Internet filtering in China". In This Paper We collected data on the methods, scope, and depth of selective barriers to Internet usage through networks in China. Tests conducted from May through November 2002 indicated at least four distinct and independently operable Internet filtering methods - Web server IP address, DNS server IP address, keyword, and DNS redirection with a quantifiable leap in filtering sophistication beginning in September 2002 [1].

In 2002 I. Clarke, S. G. Miller, T. W. Hong, O. Sandberg, and B. Wiley proposed "Protecting free expression online with freenet". They proposed Freenet is a distributed information storage system designed to address information privacy and survivability concerns. Freenet operates as a self-organizing P2P network that pools unused disk space across potentially hundreds of thousands of desktop computers to create a collaborative virtual file system. Freenet employs a completely decentralized architecture. Given that the P2P environment is

inherently untrustworthy and unreliable, we must assume that participants could operate maliciously or fail without warning at any time. Therefore, Freenet implements strategies to protect data integrity and prevent privacy leaks in the former instance, and provide for graceful degradation and redundant data availability in the latter. The system is also designed to adapt to usage patterns, automatically replicating and deleting files to make the most effective use of available storage in response to demand [2].

In 2010 C.S. Leberknight, M. Chiang, H. V. Poor, and F. Wong proposed "A Taxonomy of Internet Censorship and Anti-Censorship". They proposed Internet is supposed to be born free, yet it is censored almost everywhere, and severely censored in a few countries. The tug-of-war on the Internet between censors and anti-censors is intensifying. This survey presents a taxonomy on the principles, techniques, and technologies of Internet censorship and anti-censorship. It highlights the challenges and opportunities in anti-censorship research, and outlines a historical account via the lenses of news coverage in the past decade [3].

In 2004R. Dingledine, N. Mathewson, and P. Syverson proposed "Tor: The Second-Generation Onion Router".In this paper we present Tor, a circuit-based low-latency anonymous communication service. This second-generation Onion Routing system addresses limitations in the original design by adding perfect forward secrecy, congestion control, directory servers, integrity checking, configurable exit policies, and a practical design for location-hidden services via rendezvous points. Tor works on the real-world Internet, requires no special privileges or kernel modifications, requires little synchronization or coordination between nodes, and provides a reasonable tradeoff between anonymity, usability, and efficiency. We briefly describe our experiences with an international network of more than 30 nodes. We close with a list of open problems in anonymous communication [4].

In 2006 R. Clayton, S. J. Murdoch, and R. N. M. Watson proposed "ignoring the Great Firewall of China" .In this paper operates, in part, by inspecting TCP packets for keywords that are to be blocked. If the keyword is present, TCP reset packets (viz: with the RST flag set) are sent to both endpoints of the connection, which then close. However, because the original packets are passed through the firewall unscathed, if the endpoints completely ignore the firewall's resets, then the connection will proceed unhindered. Once one connection has been blocked, the firewall makes further easy-to-evade attempts to block further connections from the same machine. This latter behavior can be leveraged into a denial-of-service attack on third-party machines [5].

III. THREAT MODEL

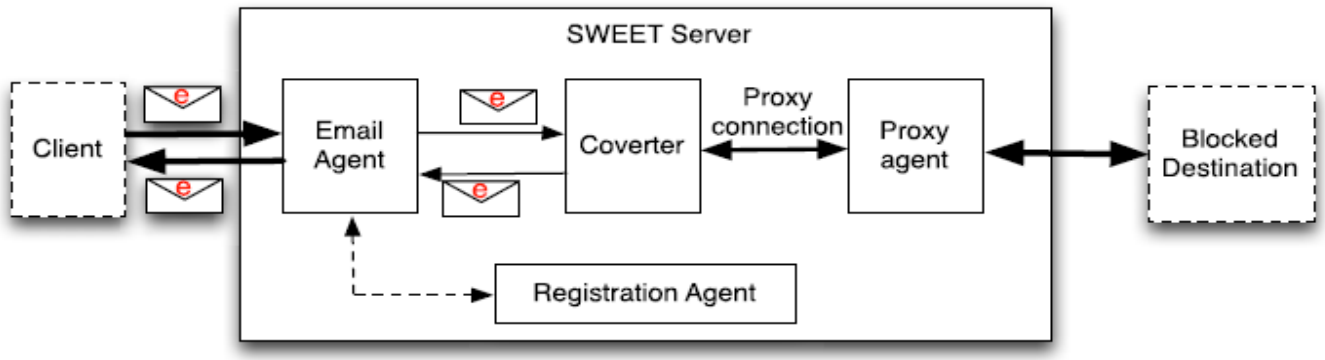
We assume that a user is confined inside a censoring ISP. The ISP blocks the user's access to certain Internet destinations, namely blocked destinations. The censor is assumed to use today's advanced filtering technologies, including IP address blocking, DNS hijacking, Snooping and deep packet inspection techniques. The ISP also monitors all the traffic to detect any use of circumvention techniques. We assume that the censorship is constrained not to degrade the usability of the Internet.In particular, the operation of SNAET system relies on the fact that a censoring ISP does not block all email communications, even though she can selectively block emails/email providers. We also assume that the ISP has as much information about SNAET as any SNAET

client. We also consider active behaviors of the ISP. In addition to traffic monitoring, the censor manipulates its Internet traffic, e.g., by selectively dropping packets, and adding latency to some packets, to disrupt the use of circumvention systems and/or to detect the users of such systems.

IV.DESIGN OF SNAET

SNAET tunnels network connections between a client and a server, called SNAET server, inside email communications. Upon receiving the tunneled network packets, the SNAET server acts as a transparent proxy between the client and the network destinations requested by the client.

1.Email agent: The email agent is an IMAP and SMTPserver that receives emails that contain the tunneled Internet traffic, sent by SNAET clients to SNAET's email address. The email agent passes the received emails to another components of the SNAET server, the converter and the registration agent. The email agent also sends emails to SNAET clients, which are generated by other components of SNAET server and contain



tunneled network packets or client registration information.

2 Converter: The converter processes the emails passed by the email agent, and extracts the tunneled network packets. It then forwards the extracted data to another component, the proxy agent. Also, the converter receives network packets from the proxy agent and converts them into emails that are targeted to the email address of corresponding clients. The converter then passes these emails to the email agent for delivery to their intended recipients. As described later, the converter encrypts/decrypts the email attachments of a user using a secret key shared with that user.

3. Proxy agent: The proxy agent proxies the network packets of clients that are extracted by the converter, and sends them to the Internet destination requested by the clients. It also sends packets from the destination back to the converter.

4. Registration agent: This component is in charge of registering the email addresses of the SNAET clients, prior to their use of SNAET. The information about the registered clients can be used to ensure quality of service and to prevent denial-of-service attacks on the server. Additionally, the registration agent shares a secret key with the client, which is used to encrypt the tunneled information between the client and the server.

Client registration: Before the very first use of the SNAET service, a client needs to register her email address withthe system. This is automatically performed by the client's SNAET software. The objective of client registration istwofold: to prevent denial-of-service (DoS) attacks andto share a secret key between a client and the server.A DoS attack might be launched on the server to disrupt itsavailability, e.g., through sending many malformed emails onbehalf of non-existing email addresses . In order to register the email addressof a client.

Algorithm:

1. Censorship Algorithm.
2. E-Mail Algorithm.

1. Censorship Algorithm:

Internet censorship is the control or suppression of what can be accessed, published, or viewed on the Internet enacted by regulators, or on their own initiative. Individuals and organizations may engage in self-censorship for moral, religious, or business reasons, to conform to societal norms, due to intimidation, or out of fear of legal or other consequences.

The extent of Internet censorship varies on a country-to-country basis. While most democratic countries have moderate Internet censorship, other countries go as far as to limit the access of information such as news and suppress discussion among citizens.[1]Internet censorship also occurs in response to or in anticipation of events such as elections, protests, and riots. An example is the increased censorship due to the events of the Arab Spring. Other areas of censorship include copyrights, defamation, harassment, and obscene material.

Example:

Twitter, Facebook, YouTube, CNN's iReport and many other websites and blogs have played in the recent events in Iran is a great example of this.

E-Mail Algorithm:

Electronic Mail (email or e-mail) is a method of exchanging messages between people using electronic devices. Email first entered limited use in the 1960s and by the mid-1970s had taken the form now recognized as email. Email operates across computer networks, which today is primarily the Internet. Some early email systems required the author and the recipient to both be online at the same time, in common with instant messaging. Today's email systems are based on a store-and-forward model. Email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need to connect only briefly, typically to a mail server or a webmail interface, for as long as it takes to send or receive messages.

Originally an ASCII text-only communications medium, Internet email was extended by Multipurpose Internet Mail Extensions (MIME) to carry text in other character sets and multimedia content attachments. International email, with internationalized email addresses using UTF-8, has been standardized, but as of 2017 it has not been widely adopted.

Example:

- Alice or Bob may use a client connected to a corporate email system, such as IBM Lotus Notes or Microsoft Exchange. These systems often have their own internal email format and their clients typically communicate with the email server using a vendor-specific, proprietary protocol. The server sends or receives email via the Internet through the product's Internet mail gateway which also does any necessary reformatting. If Alice and Bob work for the same company, the entire transaction may happen completely within a single corporate email system.
- Alice may not have a MUA on her computer but instead may connect to a webmail service.
- Alice's computer may run its own MTA, so avoiding the transfer at step 1.
- Bob may pick up his email in many ways, for example logging into mx.b.org and reading it directly, or by using a webmail service.
- Domains usually have several mail exchange servers so that they can continue to accept mail even if the primary is not available.

V. DISCUSSIONS ANDCOMPARISONS:

Unobservability :

Ensures that a user may make multiple uses of resources orservices without others being able to link these uses together. [...] Unlinkability requires that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system." In contrast to this definition, the meaning ofunlinkability in this text is less focused on the user, but deals with unlinkability of "items" and therefore is a general approach. Normally, the attacker's knowledge cannot decrease (analogously to Shannon's definition of "perfect secrecy", see above). In the special case where it is known before that some items are related, of course the probability of these items being related stays the same. Even in this "degenerated" case it makes sense to use the term unlinkabilitybecause there is no additionalinformation.

Availability:

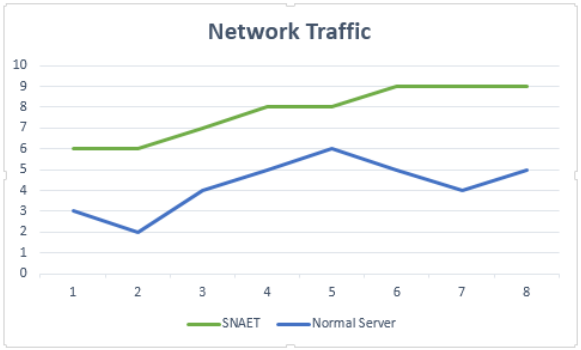
Availability provides more user can access the server simultaneously. It can easily prevent the Dos(Denial of Service) attack and other attack that occurs during the process.

V. PROTOTYPEIMPLEMENTATION:

SNAET can implemented in windows machine, 2 GHz CPU and 4GB of memory. Each email that stored in the email have unique id and email address. The Converter agent has some set of code that runs in background simultaneously. Converter convert all the emails and send it to proxy server. A Google chrome used to connection through SNAET, configured and use as a proxy. we install a Firefox extension, Greasemonkey, to allow a user to run her own JavaScript, i.e., Userscript,while browsing certain destinations. We write a

UserScript thatruns in Gmail's webmail interface and listens for the receiptof new emails. Our UserScript saves new emails in a localdirectory, which is watched by the converter. Note that theFirefox browser is directly connected to the Internet and doesnot use anyproxies.

Traffic Analysis:



Comparison of normal server with SNAET server.

It shows the network traffic of the normal server with the SNAET server. The normal server does not provide high availability and transfer rate of emails, but SNAET server provides high availability and transfer rate of emails per second.A powerful censor can perform traffic analysis to detect the use of SWEET, e.g., by comparing a user's email communications with that of a typical email user. As a result, a SWEET user who is concerned about Unobservability needs to ensure that her SWEET email communications mimic that of a normal user.

VI.CONCLUSION

In this paper, we presented SWEET, a deployable systemfor unobservable communication with Internet destinations.SWEET works by tunneling network traffic through widelyused public email services such as Gmail, Yahoo Mail, andHotmail. Unlike recentlyproposed schemes that require a collection of ISPs to instrument router-level modifications in support of covert communications, our approach can be deployedthrough a small applet running at the user's end host, and aremote email-based proxy, simplifying deployment. Throughan implementation and evaluation in a wide-area deployment,we find that while SWEET incurs some additional latency incommunications, these overheads are low enough to be usedfor interactive accesses to web services. We feel our work mayserve to accelerate deployment ofcensorship-resistant servicesin the wide area, guaranteeing high availability.

REFERENCE

[1] J. Zittrain and B. Edelman, "Internet filtering in China," IEEE Internet
Compute. vol. 7, no. 2, pp. 70–77, Mar. 2003.

[2] I. Clarke, S. G. Miller, T. W. Hong, O. Sandberg, and B. Wiley, "Protecting free expression online with freenet ,"IEEE Internet Compute, vol. 6, no. 1, pp. 40–49, Jan. 2002.

[3] C. S. Leberknight, M. Chiang, H. V. Poor, and F. Wong. (2010).”A Taxonomy of Internet Censorship and Anti-Censorship [Online]Available:
http://www.princeton.edu/chiangm/anticensorship.pdf.

[4] R. Dingledine, N. Mathewson, and P. Syverson, “Tor: The secondgeneration onion router,” in Proc. USENIX Secure. 2004, pp. 21–37.

[5] R. Clayton, S. J. Murdoch, and R. N. M. Watson, “Ignoring the great firewall of China,” inProc. Int. Workshop Privacy Enhancing Technol.,2006, pp. 20–35.

[6] J. Holowczak and A. Houmansadr, “CacheBrowser: Bypassing Chinesecensorship without proxies using cached content,” inProc. 22nd ACM Conf. Comput. Commun. Secur. (CCS), 2015, pp. 70–83.

[7] P. Syverson, G. Tsudik, M. Reed, and C. Landwehr, “Towards an analysis of onion routing security,” in Proc. Designing Privacy Enhancing
Technol., Workshop Design Issues Anonymity Unobserva., Jul. 2000, pp. 96–114.

[8] N. Feamster, M. Balazinska, W. Wang, H. Balakrishnan, and D. Karger, “Thwarting Web censorship with untrusted messenger discovery,” inInt. Workshop Privacy Enhancing Technol., 2003, pp. 125–140.

[9] M. Nasr and A. Houmansadr, “GAME OF DECOYS: Optimal decoy routing through game theory,” in Proc. 23rd ACM Conf. Comput.
Commun. Secur. (CCS), 2016, pp. 1–12.

[10] A. Juels and J. G. Brainard, “Client Puzzles: A cryptographic countermeasure against connection depletion attacks,” inProc. Netw. Distrib. Syst. Secur. Symp., 1999, pp. 151–165. [Online]. Available: http://www.isoc.org/isoc/conferences/ndss/99/proceedings/papers/juels.pdf.

[11] D. McCoy, J. A. Morales, and K. Levchenko, “Proximax: A measurement based system for proxies dissemination,”Financial Cryptogr. Data
Secur., vol. 5, no. 9, pp. 1–10, 2011.

[12] A. Houmansadr, T. Riedl, N. Borisov, and A. Singer, “I want my voice to be heard: IP over voice-over-IP for unobservable censorship circumvention,” inProc. Netw. Distrib. Syst. Secur. Symp. (NDSS), 2013, pp. 1–17.