IJDCST @ Jan,-2018, Issue- V-6, I-1, SW-18
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

# SWEET: Serving the Web by Exploiting Email Tunnels

MD.Yasmin[1], Y.Karuna Manjusha[2], MD.Imran[3]

[1]Student, M.Tech (CSE), Nimra Institute of Science & Technology, A.P., India.

[2]Assistant Professor, Dept. of Computer Science and Engineering, Nimra Institute of Science & Technology, A.P., India.

[3]Assistant Professor & HOD, Dept. of Computer Science and Engineering, Nimra Institute of Science & Technology, A.P., India.

**Abstract**— The Internet provides users from around the world with an environment to freely communicate, exchange ideas and information. Censorship circumvention systems such as Tor are highly vulnerable to network-level filtering. Because the traffic generated by these systems is disjoint from normal network traffic, it is easy to recognize and block, and once the censors identify network servers (e.g., Tor bridges) assisting in circumvention, Open communications over the Internet pose serious threats to countries with repressive regimes, leading them to develop and deploy censorship mechanisms within their networks. Unfortunately, existing censorship circumvention systems do not provide high availability guarantees to their users, as censors can easily identify, hence disrupt, the traffic belonging to these systems using today's advanced censorship technologies. In this paper, we propose Serving the Web by Exploiting Email Tunnels (SWEET), a highly available censorship-resistant infrastructure. SWEET works by encapsulating a censored user's traffic inside email messages that are carried over public email services like Gmail and Yahoo Mail. As the operation of SWEET is not bound to any specific email provider, we argue that a censor will need to block email communications all together in order to disrupt SWEET, which is unlikely as email constitutes an important part of today's Internet. Through experiments with a prototype of our system, we find that SWEET's performance is sufficient for Web browsing. In particular, regular Websites are downloaded within couple of seconds.

***Keywords:* *Email Communications, Traffic Encapsulation, Censorship Circumvention.***

## I. INTRODUCTION

Internet censorship is typically practiced by governments to, first, block citizens' access to certain Internet destinations and services; second, to disrupt tools such as Tor that help users circumvent censorship; and, third, to identify users engaging in circumvention. There is a wide variety of censorship technologies. Most of them exploit the fact that circumvention traffic is easy to recognize and block at the network level. Traffic filtering is cheap, effective, and has little impact on other network services and thus on the vast majority of users in the censorship region who are not engaging in circumvention. Another problem with the existing censorship circumvention systems is that they cannot survive partial compromise. The earliest circumvention tools are HTTP proxies that simply intercept and manipulate a client's HTTP requests, defeating IP address blocking and DNS hijacking techniques. The use of more advanced censorship technologies such as DPI, rendered the use of HTTP proxies ineffective for circumvention. This led to the advent of more advanced tools such as Ultrasurf and Psiphon, designed to evade content filtering. While these circumvention tools have helped, they face several challenges. We believe that the biggest one is their lack of availability, meaning that a censor can disrupt their service frequently or even disable them completely. The common reason is that the network traffic made by these systems can be distinguished from regular Internet traffic by censors, i.e., such systems are not unobservable. For example, the popular Tor network works by having users connect to an ensemble of nodes with public IP addresses, which proxy users' traffic to the requested, censored destinations. This public knowledge about Tor's IP addresses, which is required to make Tor usable by users globally, can be and is being used by censors to block their citizens from accessing Tor. To improve availability, recent proposals for circumvention aim to make their traffic unobservable to the censors by pre-sharing secrets with their clients. Others suggest to conceal circumvention by making infrastructure modifications to the Internet. Nevertheless, deploying and scaling these systems is a challenging problem, as discussed in Section II. A more recent approach in designing unobservalbe circumvention systems is to imitate popular applications like Skype and HTTP, as suggested by Skype-Morph , CensorSpoofer, and StegoTorus. However, it has recently been shown that these systems' unobservability is breakable; this is because a comprehensive imitation of today's complex protocols is sophisticated and infeasible in many cases. A promising alternative suggested , is to not mimic protocols, but run the actual protocols and find clever ways to tunnel the hidden content into their genuine traffic; In this paper, design and implement SWEET, a censorship circumvention system that provides high availability by leveraging the openness of email communications. A SWEET client, confined by a censoring ISP, tunnels its network traffic inside a series of email messages that are exchanged between herself and an email server operated by SWEET's server. The SWEET server acts as an Internet proxy by proxying the encapsulated traffic to the requested blocked destinations. The SWEET client uses an oblivious, public mail provider (e.g., Gmail, Hotmail, etc.) to exchange the encapsulating emails, rendering standard email filtering mechanisms ineffective in identifying/ blocking SWEET-related emails. More specifically, to use SWEET for circumvention a client needs to create an email account with some public email provider; she also needs to obtain SWEET's client software from an out-of-bound channel (similar to other circumvention systems). The user configures the installed SWEET software to use her public email account, which sends/receives encapsulating emails on behalf of the user to/from the email address of SWEET.

## II. LITERATURE REVIEW

**AUTHORS: R. Clayton, S. J. Murdoch**

The so-called "Great Firewall of China" 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 behaviour can be leveraged into a denial-of-service attack on third-party machines.

**AUTHORS: D. McCoy, J. A. Morales**

Many people currently use proxies to circumvent government censorship that blocks access to content on the Internet. Unfortunately, the dissemination channels used to distribute proxy server locations are increasingly being monitored to discover and quickly block these proxies. This has given rise to a large number of ad hoc dissemination channels that leverage trust networks to reach legitimate users and at the same time prevent proxy server addresses from falling into the hands of censors. To address this problem in a more principled manner, we present Proximax, a robust system that continuously distributes pools of proxies to a large number of channels. The key research challenge in Proximax is to distribute the proxies among the different channels in a way that maximizes the usage of these proxies while minimizing the risk of having them blocked. This is challenging because of two conflicting goals: widely disseminating the location of the proxies to fully utilize their capacity and preventing (or at least delaying) their discovery by censors.

**AUTHORS: M. Mahdian**

In countries such as China or Iran where Internet censorship is prevalent, users usually rely on proxies or anonymizers to freely access the web. The obvious difficulty with this approach is that once the address of a proxy or an anonymizer is announced for use to the public, the authorities can easily filter all traffic to that address. This poses a challenge as to how proxy addresses can be announced to users without leaking too much information to the censorship authorities. In this paper, we formulate this question as an interesting algorithmic problem. We study this problem in a static and a dynamic model, and give almost tight bounds on the number of proxy servers required to give access to n people k of whom are adversaries. We will also discuss how trust networks can be used in this context.

**AUTHORS: J. McLachlan and N. Hopper**

In Tor, a bridge is a client node that volunteers to help censored users access Tor by serving as an unlisted, first-hop relay. Since bridging is voluntary, the success of this circumvention mechanism depends critically on the willingness of clients to act as bridges. We identify three key architectural shortcomings of the bridge design: (1) bridges are easy to find; (2) a bridge always accepts connections when its operator is using Tor; and (3) traffic to and from clients connected to a bridge interferes with traffic to and from the bridge operator. These shortcomings lead to an attack that can expose the IP address of bridge operators visiting certain web sites over Tor. We also discuss mitigation mechanisms.

## III. EXISTING SYSTEM:

- Tor network works by having users connect to an ensemble of nodes with public IP addresses, which proxy users' traffic to the requested, censored destinations. This public knowledge about Tor's IP addresses, which is required to make Tor usable by users globally, can be and is being used by censors to block their citizens from accessing Tor. To improve availability, recent proposals for circumvention aim to make their traffic unobservable to the censors by pre-sharing secrets with their clients.
- Telex and Cirripede provide this unobservable communication without the need for some pre-shared secret information with the client, as the secret keys are also covertly communicated inside the network traffic.
- Cirripede uses an additional client registration stage that provides some advantages and limitations as compared to Telex and Decoy routing systems.

### DISADVANTAGES OF EXISTING SYSTEM:

- Lack of availability, meaning that a censor can disrupt their service frequently or even disable them completely.
- It has recently been shown that these systems' unobservability is breakable; this is because a comprehensive imitation of today's complex protocols is sophisticated and infeasible in many cases

### PROPOSED SYSTEM:

- In this paper, we design and implement SWEET, a censorship circumvention system that provides high availability by leveraging the openness of email communications.
- This paper makes the following main contributions: i) we propose a novel infrastructure for censorship circumvention, SWEET, which provides high availability, a feature missing in existing circumvention systems; ii) we develop two prototype implementations for SWEET (one using webmail and the other using email exchange protocols) that allow the use of nearly all email providers by SWEET clients; and, iii) we show the feasibility of SWEET for practical censorship circumvention by measuring the communication latency of SWEET for web browsing using our prototype implementation.

### ADVANTAGES OF PROPOSED SYSTEM:

- The SWEET server acts as an Internet proxy by proxying the encapsulated traffic to the requested blocked destinations.
- Our approach can be deployed through a small applet running at the user's end host, and a remote email-based proxy, simplifying deployment

## IV. RELATED WORK

In this section, we describe the detailed design of SWEET. SWEET tunnels network connections between a client and a server, called SWEET server, inside email communications. Upon receiving the tunneled network packets, the SWEET server acts as a transparent proxy between the client and the network destinations requested by the client. A client's choices of email services: A SWEET client has two options for his email provider: AlienMail, and DomesticMail.

**1) AlienMail** :An AlienMail is a mail provider whose mail servers reside outside the censoring ISP, e.g., Gmail for the Chinese clients. We only consider AlienMails that provide email encryption, e.g., Gmail and Hushmail. A SWEET client who uses an AlienMail does not need to apply any additional encryption/steganography to her encapsulated contents. Also, she simply sends her emails to the publicly advertised email address of SWEET server, e.g., tunnel@sweet.org, since the censors will not be able to observe (and block) the tunnel@sweet.org address inside SWEET messages, which are exchanged ibetween the client and the AlienMail server in an encrypted format.

**2) DomesticMail**: A DomesticMail is an email provider hosted inside the censoring ISP and possibly collaborating with the censors, e.g., 163.com for the Chinese clients. Since the censors are able to observe the email contents, the SWEET client using a DomesticMail should hide the encapsulated contents through steganography (e., by doing image/text steganography inside email messages). Also, the client can not send her SWEET emails to the public email address of SWEET server (tunnel@sweet.org) since the mail recipient field is observable to the DomesticMail provider and/or the censor. Instead, the client generates a secondary email address, myotheremail@somedomain.com (which could be either DomesticMail or AlienMail), and then provides the email credentials for this secondary account only to SWEET server through an out-of-band channel (e.g., through an online social network). The SWEET server uses this email address to exchange SWEET emails only with this particular client. In the following, we describe the details of SWEET's server and client architectures. To avoid confusion and without loss of generality, we only consider the case of AlienMail being used by the client. If DomesticMail is used, the client and server should also perform some steganography operations to hide the encapsulated traffic, as well as they should exchange a secondary email address, as described above. A. SWEET Server The SWEET server is the part of SWEET running outside the censoring region. It helps SWEET clients to evade censorship by proxying their traffic to blocked destinations. More specifically, a SWEET server communicates with censored users by exchanging emails that carry tunneled network packets. Fig. 3 shows the main design of SWEET server, which is composed of the following elements:

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

## CONCLUSION

This project has proposed an SWEET works by tunneling network traffic through widelyusedpublic email services such as Gmail, Yahoo Mail, andHotmail. Unlike recently-proposed schemes that require a collectionof ISPs to instrument router-level modifications in supportof 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 of censorship-resistant servicesin the wide area, guaranteeing high availability.

## REFERENCES

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

[2] (Nov. 2007). Defeat Internet Censorship: Overview ofAdvanced Technologies and Products. [Online]. Available:http://www.internetfreedom.org/archive/DefeatInternet Censorship WhitePaper.pd

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

[5] Ultrasurf, accessed on Jan. 7, 2017. [Online]. Available:https://ultrasurf.us/

[6] J. Jia and P. Smith. (2004). Psiphon: Analysis and Estimation.[Online]. Available: http://www.cdf.toronto.edu/ csc494h/reports/2004-fall/psiphon_ae.html

[7] I. Cooper and J. Dilley, “Known HTTP proxy/caching problems,” IETF,Fremont, CA, USA, Tech. Rep. Internet RFC 3143, Jun. 2001.

[8] R. Dingledine, N. Mathewson, and P. Syverson, “Tor: The secondgenerationonion router,” in Proc. USENIX Secur. Symp., 2004,pp. 21–37.

[9] J. Boyan, “The anonymizer: Protecting user privacy on the Web,”Comput.-Mediated Commun. Mag., vol. 4, no. 9, pp. 1–6, Sep. 1997.

[10] DynaWeb, accessed on Jan. 7, 2017. [Online]. Available:http://www.dongtaiwang.com/home_en.php

[11] R. Clayton, S. J. Murdoch, and R. N. M. Watson, “Ignoring the greatfirewall of China,” in Proc. Int. Workshop Privacy Enhancing Technol.,2006, pp. 20–35.

[12] Y. Sovran, A. Libonati, and J. Li, “Pass it on: Social networks stymiecensors,” in Proc. 7th Int. Conf. Peer-to-Peer Syst., Feb. 2008, p. 3.[Online]. Available: http://www.iptps.org/papers-2008/73.pdf

[13] D. McCoy, J. A. Morales, and K. Levchenko, “Proximax: A measurementbased system for proxies dissemination,” Financial Cryptogr. DataSecur., vol. 5, no. 9, pp. 1–10, 2011.