ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

# Serving the Web by Exploiting Email Tunnel (Sweet)

M.Sumithra, K.Pavithra, E.Priyadharshini, V.Revathi, B.Sowmya

Assistant Professor, Department of Information Technology, Panimalar Engineering College, Varadharajapuram, Poonamalle, Chennai, TamilNadu, India.

B.Tech., Department of Information Technology, Panimalar Engineering College, Varadharajapuram, Poonamalle, Chennai, TamilNadu, India

B.Tech., Department of Information Technology, Panimalar Engineering College, Varadharajapuram, Poonamalle, Chennai, TamilNadu, India.

B.Tech., Department of Information Technology, Panimalar Engineering College, Varadharajapuram, Poonamalle, Chennai, TamilNadu, India

B.Tech., Department of Information Technology, Panimalar Engineering College, Varadharajapuram, Poonamalle, Chennai, TamilNadu, India.

.

**ABSTRACT**: 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**: Censorship circumvention, email communications, traffic encapsulation.

## I. INTRODUCTION

The internet allows the users to freely communicate, exchange ideas and information. 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. As a result, repressive regimes extensively Monitor their citizens access to the internet and restrict open access to public networks by using different technologies, Ranging from simple IP address blocking and DNS hijacking to the more complicated and resource-intensive Deep Packet Inspection. With the use of censorship technologies, a number of Different systems were developed to retain the openness of the internet for the users living under repressive Regimes. 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

DOI: 10.15680/IJIRCCE.2018.0603038

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. A more recent approach in designing unobservable 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; this is the main motivation of the approach taken in this paper. In this paper, we 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. Sweet's unobservability: we claim that a censor is not easily able to distinguish between sweet's email messages and email messages. Sweet client has two options in choosing her email account: 1) alien mail a non-domestic email that encrypts emails (e.g., Gmail for users in china), and 2) domestic mail a domestic Email account with no need for encryption (e.g., 163.com for Users in china). As described in section iv, when alien mail Is used by a client all of its sweet emails are sent to a Publicly known email address, e.g., tunnel@sweet.org, Encrypted; however, a censor will not be able to identify These emails since they are proxied by the alien mail server Running outside the censoring area. In simpler words, the Censor only observes that the client is exchanging encrypted Messages with the alien mail server (e.g., Gmail's mail server in u.s.), but he will not be able to observe neither the Recipient's email address (tunnel@sweet.org), nor the Ip address of the sweet.org mail server.

As a result, **existing Approaches for spam filtering such as shooting the Spamming smtp servers and dropping spam emails are entirely infeasible**. In the case of domestic mail, the Sweet server uses a secondary secret email account, which Is only shared with that particular client, for exchanging Sweet emails (i.e., myotheremail@163.com instead of Tunnel@sweet.org address). As a result, the censor will not be able to identify sweet messages from their recipient Fields (since the censor does not know the association of Myotheremail@163.com with sweet). Also, the use of Steganography/encryption to embed tunneled data renders dpi Infeasible. Sweet's availability: given sweet's unobservability discussed above, a censor cannot efficiently distinguish between Sweet emails and benign email messages. Hence, in order to block sweet a censor needs to block all email messages to the outside world. However, email is an essential service In today's internet and 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 sweet can be reached through a wide Range of domestic/non-domestic email providers provides a High degree of availability for sweet. Prototype implementation: we have built a prototype Implementation for sweet and evaluated its performance. We have also proposed and prototyped two different designs for sweet client. The first client design uses email protocols, e.g., pop3 and smtp, to communicate with the sweet System, and our second design is based on using the webmail Interface. Our measurements show that a sweet client is able to browse regular-sized web destinations with download times In the order of couple of seconds. In fact, the high availability of sweet comes for the Price of higher, but bearable, communication latencies. Compares sweet with several popular circumvention systems regarding their availability and communication latency. Sweet provides communication Latencies that are convenient for latency-sensitive Activities like web browsing (i.e., few seconds).

## II. RELATED WORK

The government of the people's republic of China has a longstanding set of policies[1] restricting their citizens exposure to information. 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 , and because content sources are often remote from Chinese jurisdiction. As with most technical filtering regimes, whether implemented at the client, internet service provider, list of the sites blocked or the methodologies used to block them has been made available by doing the filtering. More than 18,931 sites were inaccessible from atleast two distinct proxy servers within china. Tor[2], 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. It briefly describe the experiences with an international network of more than 30 nodes.There are numerous problems in anonymous communication.

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[3] 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. Internet censorship policies, are primarily concerned with two main principles based on usability and censorship- Limit the performance degradation, Enforce censors. anti-censorship technologies are concerned with censorship resistant systems. There are two main dimensions: free access to information and free publication of information. Freenet[4] 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. The so-called "Great Firewall of China"[5] 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.

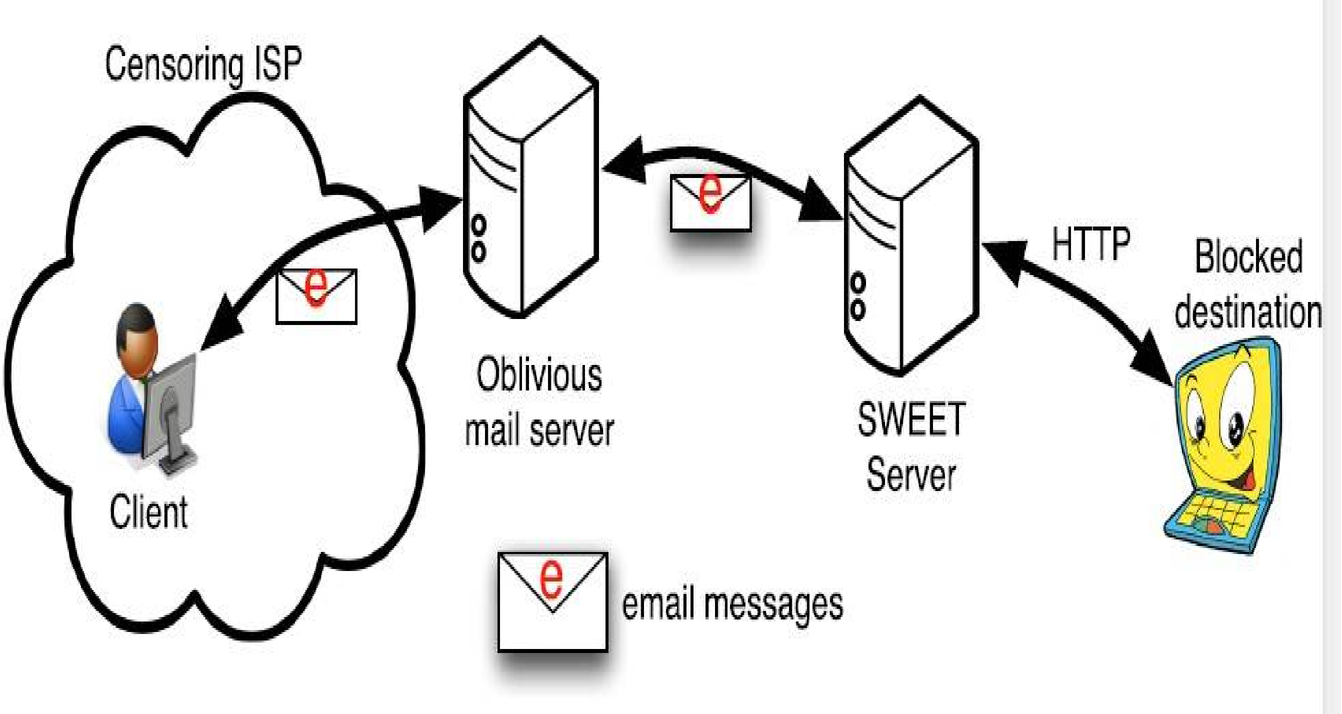
## III. PAST SYSTEM ANALYSIS

The Internet provides users from around the world with an environment to freely communicate, exchange ideas and information. 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 east demonstrates 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. As a result, repressive regimes extensively monitor their citizens' access to the Internet and restrict open access to public networks by using different technologies, ranging from simple IP address blocking and DNS hijacking to the more complicated and resource-intensive Deep Packet Inspection (DPI).The 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.

## IV. PROPOSED SYSTEM

With the use of censorship technologies, a number of different systems were developed to retain the openness of the Internet for the users living under repressive regimes. 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.

## V. PROPOSED SYSTEM ARCHITECTURE DESIGN



\

DOI: 10.15680/IJIRCCE.2018.0603038

## VI. CONCLUSION

In this paper, we presented SWEET, a deployable system for unobservable communication with Internet destinations. SWEET works by tunneling network traffic through widely used public email services such as Gmail, Yahoo Mail, and Hotmail. Unlike recently-proposed schemes that require a collection of ISPs to instrument router-level modifications in support of covert communications, our approach can be deployed through a small applet running at the user's end host, and a remote email-based proxy, simplifying deployment. Through an implementation and evaluation in a wide-area deployment, we find that while SWEET incurs some additional latency in communications, these overheads are low enough to be used for interactive accesses to web services. We feel our work may serve to accelerate deployment of censorship-resistant services in the wide area, guaranteeing high availability.

## REFERENCES

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

[2] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second generation onion router," in Proc. USENIX Secur. Symp., pp. 21–37,2004.

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

[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] R. Clayton, S. J. Murdoch, and R. N. M. Watson, "Ignoring the Great Firewall of China" in Proc.Int.Workshop Privacy Enhancing Technol.,pp.20-35,2006

[6] N.Feamster,M.Balazinska,W.Wang,H.Balakrishnan,and D.Karger, "Thwarting Web censorship with untrusted messenger discovery,"in Int.Workshop Privacy Enchancing Technol.,pp.125-140,2003

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

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

[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] D.McCoy,J.A.Morales,and K.Levchenko,Proximax: "A measurement based system for proxies dissemination,"Financial Cryptofgr.Data Secur.,vol.5,no.9,pp.1-10,2011

[11] M.Schuchard, J.Geddes, C.Thompson,and N.Hopper , "Routing around decoys," in Proc.ACM Conf.Comput.Commun.Secur.,pp.85-96,2012

[12] P.Winter and S.Lindskog,"How China is blocking Tor.",[Online].Available:http://arxiv.org/abs/1204.0447, Apr.2012