SWEET: Serving the Web by Exploiting Email Tunnels

[1] J C.SIRISHA

M.Sc (Computer Science)

Besant theosophical college,madanapalli.

[2] . D.Venkata Siva Reddy
Head dept. of CS
Besant theosophical college,madanapalli

ABSTRACT Open communication over the Internet poses serious threats to countries with repressive regimes, leading to the development and dissemination of control mechanisms within their networks. Unfortunately, control-based circumvention systems do not provide high-availability safeguards for their users, as control can easily identify and thus disrupt the traffic of these systems using advanced control techniques today. In this research, we suggest a web service by exploiting email tunnels (SWEET), a high-resistance controlled infrastructure. SWEET works by including controlled user traffic within emails that are transmitted through public email services such as Gmail and Yahoo Mail. Because the SWEET process is not associated with any specific email provider, we say that censorship will need to block email connections together to disable SWEET, which is unlikely because email is an important part of the Internet today. Through experiments on a prototype of our system, we found SWEET performance sufficient for web browsing. In particular, regular websites are downloaded in a few seconds. Terms of index - circumvention of censorship, e-mail communications, traffic packaging.

INTRODUCTION v The Internet provides users from around the world with an environment to communicate freely and exchange ideas and information. However, free communication continues to threaten repressive regimes, where open circulation of information and talk among its citizens can pose serious threats to their existence. Recent unrest in the Middle East illustrates that the Internet can be widely used by citizens under these regimes as a powerful tool for disseminating censored news and information, inspiring the opposition, organizing events and protests. As a result, repressive regimes widely monitor the access of their citizens to the Internet and restrict open access to public networks [1] using various technologies, ranging from simple IP addresses and DNS intrusion to more complex, (DPI) [2], [3]. With the use of censorship techniques, a number of different systems have been developed to maintain the openness of the Internet to users living under oppressive regimes [4] - [9]. The older phishing tools are HTTP proxies [4], [9], [10] which simply intercept and process client HTTP requests, and defeat IP blocking and DNS hijacking methods. Making use of more advanced control techniques such as DPI [2], [11], the use of HTTP proxies is ineffective to circumvent. This has led to the emergence of more advanced tools such as Ultra Surf [5] and Psiphon [6], designed to evade content filtering. While these fraudulent tools have helped, they face many challenges. We believe that the biggest is not being available, which means that censorship can disrupt their service frequently or even completely disable it [12] - [16]. The common reason is that network traffic generated by these systems can be distinguished from ordinary Internet traffic by censors, ie, these systems are not observable. For example, the popular Tor network [8] works by making users connect to a set of nodes with public IP addresses, which means that the users of the proxy go to the controlled destination destinations. This general knowledge about Tor's IP addresses, which are required to make Tor usable by users worldwide, can be used by censorship to prevent their compatriots from accessing Tor [17], [18]. To improve availability, recent fraudulent proposals aim to make their own traffic unmanageable by censorship by sharing secrets with their clients [19] - [21]. Others [22] - [25] suggest concealing circumvention through infrastructure modifications on the Internet.

RELATED WORK

There has been a lot of work on circumvention systems for unchecked control [23], [24], [26] - [28], [30], [32] - [35]. Like SWEET, FreeWave [30], CloudTransport [32], and CovertCast [35] also work through tunneling to circumvent actual network protocols. For example, FreeWave [30] tunnels the Internet within VoIP connections. This approach, through tunnels, provides a stronger ability to control against censorship than traditional imitation systems [26] - [28], as Houmansadr et al.

[29]. Many designs [19] - [21] seek to be seen by sharing confidential information with their clients, which observers do not know. For example, the Tor network recently adopted the use of Tor Bridges, a set of voluntary nodes that connect customers to the Tor network, whose IP addresses are selectively distributed among Tor users from Tor. Infranet [19], for example, shares a secret key and some confidential URLs with a client, which are then used to establish an invisible connection between the client and the system. Collage [20] works by secretly owning a client and system on some user-generated content sharing sites, for example, flickr.com, and communicating by hiding information. Unfortunately, exchanging secrets with a wide range of customers poses a serious challenge, as the sergeant can obtain the same confidential information by pretending to be a client

EXISTING SYSTEM:

Tor works by making users connect to a set of nodes with public IP addresses, which move proxy users to controlled destination destinations. This general knowledge about Tor's IP addresses, which are necessary to make Tor usable by users worldwide, can be used and used by censorship to prevent its citizens from accessing Tor. To improve availability, recent fraudulent proposals aim to make their own traffic unmanageable by censorship by sharing secrets with their customers.

Telex and Cirripede provide this invisible connection without the need for some confidential information shared with the client, as secret keys are also connected within network traffic.

Cirripede uses an additional client registration stage that offers some advantages and limitations when compared to Telex and Decoy routing systems.

Disadvantages of existing system:

Lack of availability, which means that censorship can disrupt their service frequently or even disable it altogether.

It has recently been shown that these systems can not be monitored because they can be broken, because the complex tradition of complex protocols today is evolving and is not applicable in many cases

Proposed System:

In this paper, we design and implement the SWEET system, a control system that offers high potential to take advantage of the openness of e-mail communications.

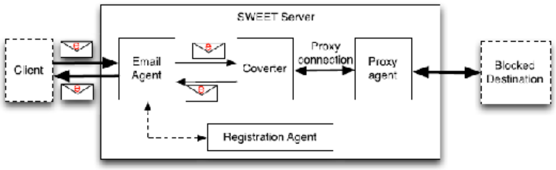
This paper presents the following key contributions: 1) we propose a new SWEET, which provides significant savings, a missing feature in existing fraud regimes; ii) we develop two initial applications for SWEET (one using webmail and the other using protocols) E-mail exchanges) that allow almost all e-mail providers to be used by SWEET customers; and iii) demonstrate the utility of SWEET to circumvent the process control by measuring the connection latency of SWEET to browse the Web using our prototype implementation.

Advantages of the proposed system:

The SWEET server acts as an Internet proxy server by creating a proxy for closed traffic to the required prohibited destinations.

Our policies can be deployed through a small application running on the end user's host, and a remote email-based proxy, making deployment easier

SYSTEM ARCHITECTURE:



CONCLUSIONS

In this paper, we introduced SWEET, a scalable system for communicating with unwanted Internet destinations. SWEET works by transferring network traffic over widely used public email services such as Gmail, Yahoo Mail, and Hotmail. Unlike recent schemes that require a set of ISPs to make router-level modifications to support confidential communications, our approach can be deployed through a small application running on the end user's host and a remote email-based agent, facilitating deployment. Through extensive implementation and evaluation, we find that while SWEET carries some additional latency in communications, these overhead are low enough to be used for interactive access to web services. We feel that our work could serve to accelerate the deployment of control-control services in the wider region, which will ensure great savings.

Author Details

C.SIRISHA

D.Venkata Siva Reddy