SEAS: Secure Email with Asymmetric Cryptography and Steganography

Kawsalya. S[1] Arun Joseph. A[2] Dr. A. Kalaivani[3] M. Vijayakumar[4] P. Boopathi[5]
[1,2,3,4,5]Assistant Professor
[1,2,4,5]Department of Computer Science Engineering [3]Department of Computer Applications
[1,2,3,4,5]Nehru Arts and Science College, Coimbatore, India

Abstract— Countries with authoritarian regimes face major challenges from open Internet communications, prompting them to establish and deploy surveillance systems inside their networks. Unfortunately, modern censorship circumvention schemes do not offer high-efficiency assurances to their consumers because censors can quickly detect. They, therefore, interrupt communication belonging to these systems using today's sophisticated censorship technology. Instead, we recommend servicing the Email Tunnels, a highly accessible censorship-resistant infrastructure. It functions by encapsulating a censored user's traffic inside email messages sent through public email services such as Gmail and Yahoo Mail. We deploy a tunneled server to reduce connectivity overhead between webmail servers. We suggest a strategy for implementing safe data sharing through two mail accounts for a single person, each of which can be used for different purposes, namely, alien mail and domestic mail. Both are connected in various forms of communication. This was designed primarily to minimize contact delays. Email traffic would be minimized by routing email via our tunneled portal. We can also send emails to blocked addresses. Also, through censorship circumvention, computer transfers cannot be leaked with the assistance of an alien mail server since the data would be encrypted using an effective RSA algorithm. Similarly, in domestic mail, the sensor would not recognize tunneled messages from their receiver areas. Furthermore, using steganography/encryption to embed tunneled data makes DPI (deep packet inspection) impossible.

Keywords: Cryptography, steganography, HTTP, Email Server, RSA

I. INTRODUCTION

The Internet allows clients worldwide to communicate, share ideas, and exchange data freely. However, free correspondence continues to undermine authoritarian administrations, as accessible distribution of data and dialogue among their citizens may pose genuine dangers to their reality. Recent unrest in the Middle East demonstrates that residents under these administrations may use the Internet as a powerful tool to disperse blue-penciled news and results, travel to refute, and write events and dissents. As a result, harsh administrations broadly screen their citizens' Internet connections and restrict free access to open networks using various innovations, ranging from simplistic IP address blocking and DNS seizing to the more complicated and asset concentrated Deep Packet Inspection (DPI). Multiple mechanisms were developed using constraint creativity to keep the receptivity of the Internet for clients working under abusive administrations.

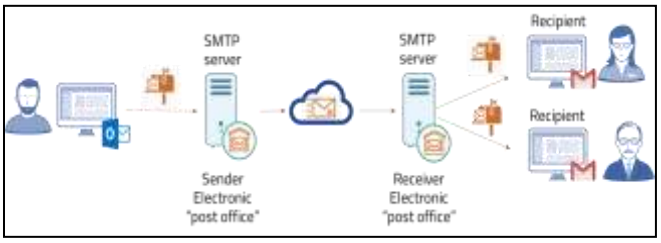

Fig. 1: SMTP Server Architecture

The most effective circumvention tools are HTTP intermediaries that intercept and monitor a customer's HTTP queries, IP address blocking, and DNS hijacking procedures. The use of advanced constraint technologies, such as DPI, made HTTP intermediaries inadequate for circumvention. This sparked the appearance of more advanced technologies, such as Ultrasurf and Psiphon, designed to circumvent content filtering. Although these instruments have become useful, they still have certain drawbacks. We believe that the most significant one is their lack of functionality, which means that an edit will frequently disrupt or even obstruct their administration. The most common explanation is that the device traffic produced by these frameworks can be distinguished from regular Internet traffic using blue pencils, indicating that such frameworks are not inconspicuous. For example, the well-known Tor scheme operates by making clients communicate with a community of hubs with accessible IP addresses, which then route clients' traffic to the desired, managed destinations. This accessible knowledge regarding Tor's IP addresses which is needed to render Tor available by clients worldwide, may and is being used by authorities to prevent their subjects from accessing Tor. The late proposal for circumvention aims to render their traffic imperceptible to blue pencils while providing exclusive insights to their clients to improve usability. Others suggest masking circumvention through modifying the Internet's structure. As indicated by Skype-Morph, Censor Spoofer, and StegoTorus, a later technique in outlining unobservable circumvention mechanisms is to emulate well-known programs such as Skype and HTTP. However, it has recently been shown that the inconspicuousness of these systems is delicate; this is because a comprehensive impersonation of the current complex conventions is advanced and infeasible much of the time.

A promising alternative is running the actual conventions and finding thoughtful ways to burrow the shrouded material into their genuine traffic, rather than copying convention'1 ns; this is the primary motivation for the process. This article prepares and implements SEAS, an oversight circumvention system that provides high usability by leveraging email receptivity. A SEAS client, bound by a governing ISP, burrows the device traffic within a series of emails exchanged between herself and an email server managed by SEAS's server. The SEAS server acts as an

intermediary between the Internet and the blocked targets by proxying the typed traffic. The SEAS user exchanges messages with a careless, free mail provider (e.g., Gmail, Hotmail, etc.), leaving normal email filtering elements incapable of distinguishing/blocking SEAS-related messages. To use SEAS for circumvention, a consumer must first create an email address with an available email provider; she must also obtain SEAS's customer programming from an out-of-bound channel (like other circumvention frameworks). The client configures the implemented SEAS programming to use her accessible email account, which sends/receives exemplary messages for the client's advantage to/from the SEAS email address.

II. BACKGROUND WORK

Ayodele, T. et al. [1] presented an analysis of the proposed methods for extracting key terms from email communications to have a clearer summary than merely running the unprocessed news this is also another improved method of producing useful summaries. Our framework will also be able to categories email messages based on the user's behavior and include a process for emails that need consideration. The authors review email message form, users' preferred dictionary, and vocabulary model, which the authors contend have not been adequately investigated in previous studies on email classification and summarization. The email classification and summarization systems depend on a basic algorithm, but it is extremely difficult to enforce.

Dacosta, I. et al. [2] crafted Email Cloak, an email alias program with OpenPGP encryption capability that allows users to encrypt their emails instantly and selectively until their providers store them. Users may secure their emails independently of other contact partners by depending on a privacy-friendly third-party, the EmailCloak provider, without thinking about complicated key management.

Jayakody, D., & Dias, G. [3] presented a novel approach for determining the relevance of participants of social media networks. The method is focused on the examination of contact habits. The authors are particularly interested in calculating the time it takes to respond to each letter. The authors conclude that users have an implied ranking of the relevance of other users, which can be discovered by calculating procrastination in responding to messages (people tend to quickly respond to messages received from other people perceived as important). Experiments on a vast body of evidence covering a one-year email exchange demonstrate the feasibility of the suggested approach.

Khan, W. Z. et al. [7] Botnet-created Email spam is now a constant threat to Internet protection. It is transmitted by infected compromised computers that create botnet armies and are managed by one or more botmasters. Typically, spamming botnets are used to carry out various spam schemes. It is difficult to detect and classify spambots because spammers are increasingly flexible and agile, and they expect to utilize encrypted C&C communication and functionality more efficiently.

Laclavik, M. et al. [9] discussed a modern approach to email quest focused on disseminating activation and knowledge retrieval using Email Social Networks Our prototype was reviewed and partly validated on the Enron email repository by the authors. The authors agree that the developed search interface, which enables user engagement with social network graphs, provides novel approaches to accessing email archives as an information repository.

A. Problem Description

The first circumvention methods were HTTP proxies, which intercept and exploit HTTP requests from a client, beating IP address blocking and DNS hijacking techniques. Although these techniques have become useful, they pose several obstacles. In our current method, all modes of mail correspondence use a common direction, which causes delays and insecure transmission. We assume that the most significant one is their lack of functionality, which means that a censor will regularly interrupt or even entirely disable their operation. The common explanation is that censors may differentiate network traffic produced by these devices from normal Internet traffic, implying that such methods are not unobservable. There is no encryption on the server. As many emails are sent in the same direction, it may cause traffic. Current circumvention plans seek to render their traffic unobservable to censors by pre-sharing secrets with their clients to boost availability. Another current scheme proposes concealing circumvention by modifying the Internet's architecture.

III. SYSTEM MODEL

Design and deploy SEAS, a censorship circumvention scheme that offers high availability by exploiting the freedom of email messages, in this paper. A SEAS client restricted by a censoring ISP tunnel the network traffic within a collection of email messages shared between herself and an email service run by SEAS's server, which contains both alien and domestic mail. The SEAS server serves as an Internet proxy by proxying the encapsulated traffic to the demanded blocked destinations. However, a hostile third party would not detect these emails since they are proxied by the AlienMail server, which is located outside of the censorship zone. To put it another way, they can see that the client is exchanging encrypted messages with the Alien Mail server, but they can't know the material. The SEAS server requires a secondary private email address only traded with the same client for exchanging SEAS emails in Domestic Mail. Steganography is used for defense purposes in this case.

IV. MAIL SERVER CREATION

The first module of this paper is the construction of a mail server. Initially, the mail server is created to allow users to connect through email. The mail server environment involves submitting emails to recipients through the composer option and obtaining mail from different recipients. Viewing received mails, spam emails, and lost emails is also an alternative on the mail server.

A. Users

Users are the end persons who are making or initialize the communication with the server. Normally in this work, users can split as

– Legitimate users and
– Attackers

The attackers are mainly from the remote system logins, and they use the compromised systems.

– Known machine
– Unknown or remote login system.

B. Web Access Security

Web servers have long been victims of attacks due to their widespread usage for personal and corporate info. These threats have recently been more diverse, as the focus has changed from targeting the front end to leveraging web framework vulnerabilities.

1) Accessibility and Verification

This module will get the cookie storage for the checking purpose while the user login from remote systems. If the user is the first time, the cookie will store the data and can't verify access information.

2) Remote Login Limitation

Once the protocol finds the numerous wrong guess for single and multiple logins, the process will limit the remote login identity.

3) Cookie Verification

This module keeps the copy of every single user login in the remote login and the known machine. Further, it will help to verify the data when the wrong entry implies.

Fig. 2: Email sending to other clients

C. Alienmail:

AlienMail is a mail service whose mail servers are located outside of the censoring ISP, such as Gmail for Chinese users. We take into account Alien Mails that provide email encryption, such as Gmail and Hushmail. A SEAS customer who uses AlienMail does not need to encrypt or steganography her encapsulated contents anymore. She also sends her emails to the SEAS server's publicly advertised email address, e.g., tunnel@SEAS.org, so censors would not observe (and block) the tunnel@SEAS.org address within SEAS messages are shared in encrypted format between the client and the AlienMail server.

D. RSA Algorithm Using an Alien Mail:

RSA algorithm is an asymmetric cryptography algorithm. Asymmetric means that it works on two different keys, i.e., Public Key and Private Key. The name describes that the Public Key is given to everyone, and the Private Key is kept private.

An example of asymmetric cryptography:

1) A client (for example, browser) sends its public key to the server and requests some data.
2) The server encrypts the data using the client's public key and sends the encrypted data.
3) The client receives this data and decrypts it.

Since this is asymmetric, nobody else except the browser can decrypt the data even if a third party has the browser's public key.

Fig. 3: Alien Mail Sending using RSA

E. Domestic Mail

Domestic mail is an email service hosted inside the censoring ISP and may collaborate with the censors, such as 163.com for Chinese clients. Since the censors will see the email contents, the SEAS client utilizing a Domestic Mail should conceal the encapsulated contents using steganography (e.g., image/text steganography inside email messages). Furthermore, unless the mail receiver area is visible to the Domestic Mail provider and the sensor, the client cannot submit her SEAS emails to the public email address of the SEAS registry (tunnel@SEAS.org). Instead, the client creates a secondary email address and sends the email credentials for this secondary account to the SEAS server using an out-of-band channel (e.g., through an online social network). The SEAS server only uses this email address to share SEAS communications with this same client.

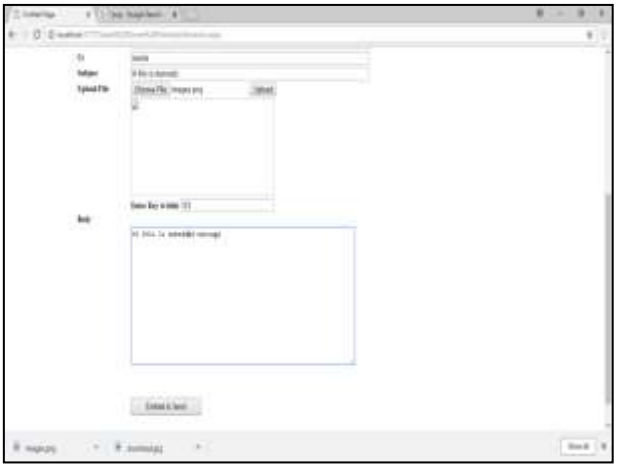

Fig. 4: Domestic Mail Sending

F. Steganography

Steganography is the process of concealing a hidden message inside an ordinary message and extracting it at its destination. Steganography extends encryption by hiding an encrypted code such that no one knows it occurs. Anyone scanning the data should be unaware that it includes secure data.

In modern digital steganography, data is first encrypted and then inserted into redundant (that is, given but unnecessary) data that is part of a certain file format, such as a JPEG document, using a special algorithm. Consider all the bits that reflect the same color pixels in a sequence. By adding the encrypted data to the redundant data randomly or inconspicuously, the effect would be data with the "noise" patterns of normal, no encrypted data.

Fig. 5: Steganography Process

G. Reports

It is the outcome of admin checking and the cookie detail for the whole process; here, the admin can refer to the Alien and domestic mail details for using the sender activity list.

V. Discussions

1) Email agent: The email agent is an IMAP and SMTP server that collects emails containing tunneled Internet traffic sent to SEAS's email address by SEAS clients. The email agent forwarded emails to another SEAS server part, the converter, and the registered agent. The email agent often sends emails to SEAS clients that include tunneled network packets or client registration details provided by other SEAS server features.
2) Converter: The converter removes the tunneled network packets from the emails passed by the email agent. The extracted data is then forwarded to another portion, the proxy agent. Furthermore, the converter accepts network packets from the proxy agent and transforms them into emails sent to the respective clients' email addresses. The converter then forwards these emails to the email agent, who delivers them to their expected recipients. The converter encrypts/decrypts the email attachments using a hidden key shared with that person, as mentioned later.
3) Proxy agent: The proxy agent forwards the network packets extracted by the converter to the Internet destination specified by the clients. It also sends packets back to the converter from the destination.
4) Registration agent: Until utilizing SEAS, this component records the email addresses of the SEAS clients. The details regarding the authorized clients will be used to maintain service consistency and deter server denial-of-service attacks. Furthermore, the registration agent exchanges a private key with the recipient, encrypting the details tunneled between the client and the server.

VI. Conclusions

This paper proposed SEAS through tunneling network traffic via popular public email services like Gmail, Yahoo Mail, and Hotmail. Unlike recently proposed schemes, which include a series of ISPs to instrument router-level modifications in support of covert communications, our solution can be deployed through a small applet running on the user's end-host and is mote email-based proxy, simplifying deployment. Through implementation and assessment in a wide-area application, we discovered that although SEAS adds some latency to communications, these overheads are low enough to be used for immersive web service access. We believe that our work would hasten the widespread rollout of censorship-resistant services while ensuring high availability.

References

[1] Ayodele, T., Zhou, S., & Khusainov, R. (2009). Email Grouping and Summarization: An Unsupervised Learning Technique. 2009 WRI World Congress on Computer Science and Information Engineering. doi:10.1109/csie.2009.298
[2] Dacosta, I., Put, A., & Decker, B. D. (2014). EmailCloak: A Practical and Flexible Approach to Improve Email Privacy. 2014 Ninth International Conference on Availability, Reliability and Security. doi:10.1109/ares.2014.39
[3] Jayakody, D., & Dias, G. (2014). ReputationBox: A system to analyse importance of emails and reputation of email senders. 2014 14th International Conference on Advances in ICT for Emerging Regions (ICTer). doi:10.1109/icter.2014.7083913
[4] Lubarski, P., & Morzy, M. (2012). Measuring the Importance of Users in a Social Network Based on Email Communication Patterns. 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. doi:10.1109/asonam.2012.24
[5] Nampoothiri, A. P., & Madhavu, M. L. (2015). Email forensic analysis based on k- means clustering. 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI). doi:10.1109/icacci.2015.7275710
[6] Kambourakis, G., Gil, G. D., & Sanchez, I. (2020). What Email Servers Can Tell to Johnny: An Empirical Study of Provider-to-Provider Email Security. IEEE Access, 8, 130066–130081. doi:10.1109/access.2020.3009122
[7] Khan, W. Z., Khan, M. K., Bin Muhaya, F. T., Aalsalem, M. Y., & Chao, H.-C. (2015). A Comprehensive Study of Email Spam Botnet Detection. IEEE Communications Surveys & Tutorials, 17(4), 2271–2295. doi:10.1109/comst.2015.2459015

[8] Rompas, P. S., & Perdana, R. S. (2018). Securing Confidential Documents in Local Network Using an Email Filtering Technique. 2018 International Workshop on Big Data and Information Security (IWBIS). doi:10.1109/iwbis.2018.8471696
[9] Laclavik, M., Dlugolinsky, Kvassay, M., & Hluchy, L. (2011). Email Social Network Extraction and Search. 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology. doi:10.1109/wi-iat.2011.30
[10] Julian Jang, Nepal, S., & Zic, J. (2008). Trusted Email protocol: Dealing with privacy concerns from malicious email intermediaries. 2008 8th IEEE International Conference on Computer and Information Technology. doi:10.1109/cit.2008.4594709.

