Cargomail — A Privacy-Aware Email System

Igor Zboran
izboran@gmail.com

***Abstract*—Electronic mail (email) is the most pervasive form of business information exchange. Email is used not only as an interpersonal communication tool but also as a "default choice" for sending files.**

This paper introduces Cargomail: a privacy-aware email system designed with the precept that the storage of email messages should be the responsibility of users and not of email providers.

We explain the importance of separating the identifier (email address) and the locator (mailbox) in the design of the Cargomail architecture. Our paper concludes by highlighting the significant advantages of this design.

I. Introduction

The main components of the email system were designed between the early 1970s and mid-1990s by many inventors. Over time, email has become the most commonly used Internet application. Nowadays, email is the only ubiquitous communication system on the Internet that was built in a decentralized fashion. Moreover, the email infrastructure forms the backbone of the global digital identity.

II. Current Situation

Today, outgoing email is typically transferred from the source system to the destination system as a single text-encoded file using the Simple Mail Transfer Protocol (SMTP). SMTP is an over-40-year-old push-based protocol, and even though SMTP has been updated, modified, and extended multiple times to increase security and efficiency, it still lags behind modern web-based protocols.

III. Problems and Issues

Despite the importance of email infrastructure, the whole ecosystem still relies on more than 40-year-old architecture and protocol design. There have been spam and attachment issues from the very beginning. While conceptually sound as a communication means, the email system is structurally obsolete and functionally deficient.

A. Functional and Security Flaws

Even though the major email service providers claim their email services to be safe, the fact remains that fundamental security and functional flaws are not fixed. There is still a dichotomy of attachment delivery; bulky files are not transferred as an attachment but are shared via links. A "file sharing" is unnatural for the email system, where each message with attachments is expected to be time-consistent. Shared links pose a consent phishing attack threat, where an attacker tricks users into granting malicious application access to sensitive resources.

B. Confidentiality and Privacy

Now, if we (as users) want to use a single email address, we have no choice but to use a single email service provider for all categories of communication. Information about every email we send or receive—"buying a car or a home, applying for a loan, taking out insurance, purchasing potato chips, requesting a government grant, getting turned down for credit, going to work, seeing a doctor" [1]—is funneled through the same service providers. This raises privacy concerns, leading to what we may call a One-Address-Fits-All privacy issue.

C. Hyperlinks to External Files

Documents, images, videos, and audio should be an integral part of the email. The concept of keeping a time-consistent, recipient-owned copy of the sender's files is critical in some industries. Here is the list of issues with hyperlinks to external files in email messages:

- expired, unknown, blocked, phishing, or malicious hyperlink
- masked hyperlink target using a URL shortener
- target updated – not the version it is expected
- target changed – forgery
- target encrypted – need a password
- access control – requires signup or sign in
- consent phishing attack

Given these points—You are buying a "pig in a poke" with each hyperlink to the external file in the email message.

D. Content Repository

The current email system is missing a content repository—a "file system on steroids" with the capability to create, store, locate, and exchange any content.

IV. Proposed Solution

Given that the current email system is lagging behind modern communication and collaboration tools, we propose implementing the Global Reference Identity Protocol (GRIP) [2]—zero-trust authentication mechanism into the email ecosystem to enhance the usability and security of the email system.

A. Goals and Objectives

Email, still the most popular communication tool, lacks an essential part of today's modern communications systems—a zero-trust authentication mechanism. Understanding this led us to employ the GRIP authentication mechanism to enhance the trustworthiness and data sovereignty of the email ecosystem. At the core of the proposed solution is an attempt to improve email usability—not only as an interpersonal communication tool but also as the default choice to send and store files.

B. Concept

Cargomail does not use email attachments or links to external files. Instead, it uses an editor that allows users to reference documents, images, and videos in the message body by their content via a cryptographic hash value while keeping the respective resources in a content-addressed resource mailbox. Cargomail exchanges referenced resources between resource mailboxes using the GRIP authentication mechanism. The final download link is constructed in the email client using the resource mailbox Uniform Resource Locator (URL) and the cryptographic hash value of the referenced resource. The email application renders the content of the email resource directly into the message body. Cargomail uses a two-way push-pull data transfer mode using SMTP/IMAP/POP3 and HTTP protocols, as illustrated in Figure 1.

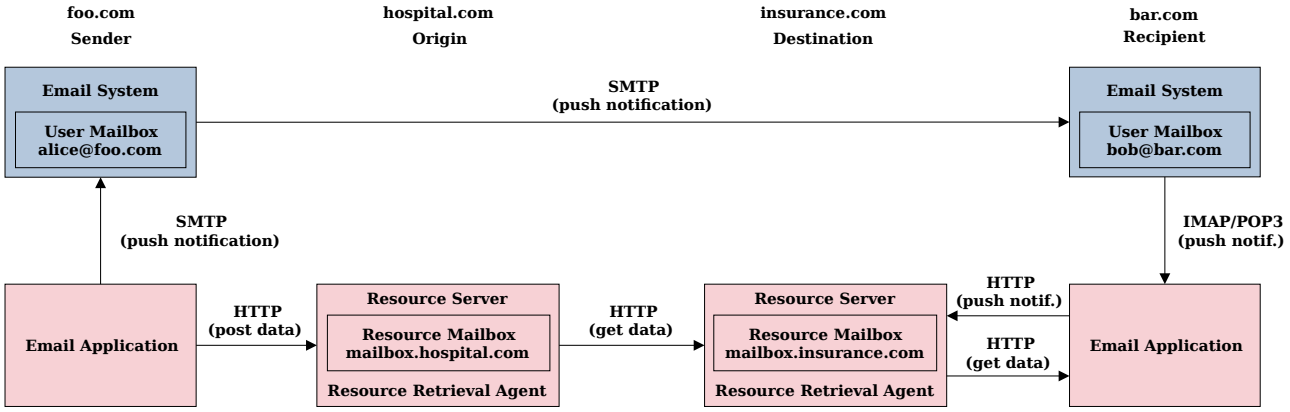

Fig. 1. Cargomail architecture

C. Key Points

• Each email consists of resources (message and referenced files) stored in the resource mailbox—on the email-specific resource server.

• The email resources owned by the sender, stored in an origin resource mailbox, are temporarily shared with recipients. Following a successful sharing process, a notification email is sent to each recipient through the standard email system. The notification email contains the origin resource mailbox URL, the cryptographic hash values of the referenced resources, and the category of correspondence, e.g., personal, business, or healthcare.

• After receiving the notification email, the recipient's email application determines (according to the user's preferences and the category of correspondence) which destination resource mailbox will be used for communication.

• The resource retrieval agent at the destination resource server gets the origin resource mailbox URL and the cryptographic hash values of the referenced resources in the notification email. Using the GRIP authentication mechanism, the agent tries to retrieve the email resources from the origin resource mailbox. After successful authentication, the data is retrieved and stored in the destination resource mailbox. Finally, the email application can access the retrieved data stored in the destination resource mailbox.

V. Advantages compared to the Current Email System

Cargomail has several decisive advantages over the current email system.

A. Security and Privacy

The actual correspondence takes place between resource mailboxes. The user mailbox of the standard email system is only used for notification emails. This architecture guarantees more control over potential security and privacy issues such as leakage of intellectual property or loss of confidential content. In addition, the user decides from whom he receives email resources, thus protecting his mailbox from spam.

B. Usability and Privacy

The resource mailbox is decoupled from the user's email address. This separation allows a user with a single email address to use multiple resource mailboxes side by side. With a single email address and numerous mailboxes, Cargomail can keep official, business, and personal correspondence separately on designated resource servers.

C. Content Repository

With the capability to create, store, locate, and exchange any content, including documents, images, videos, and audio, the proposed solution is a promising foundation for the personal content repository.

VI. Implementation Concerns

This section deals with the issues of implementing the proposed data exchange mechanism into the existing email infrastructure.

A. MIME External-Body Subtype

Cargomail uses the MIME 'message/external-body' subtype in the push notification to indicate that the actual body data are not included but merely referenced. Although this is a standardized method of referencing external data, not every email provider handles it correctly.

B. Decentralized Notification System from Scratch

As an alternative to email-based notifications, a new decentralized notification system built around the GRIP authentication mechanism can be considered.

VII. Models and Scenarios

Although Cargomail can be integrated into the email system of any email service provider, we slightly digress to introduce two visionary models of what a global email ecosystem might look like in the future.

A. Estonian Model

In this model, the government provides email services with user mailboxes. To avoid the risk of governmental surveillance, Cargomail allows citizens to use non-governmental resource mailboxes, e.g., from financial institutions or healthcare providers. Using non-governmental, sector-specific resource mailboxes increases the privacy of individual citizens, as the government cannot obtain detailed information about their activities.

B. Postal Model

According to UPU research [3], more than 93% of postal operators provide some form of digital postal service either directly or in partnership with other companies. Cargomail allows postal operators to expand and become public email service providers or innovate their existing email services and provide the user mailbox services with the ability to attach the resource mailboxes from the government as well as other institutions and organizations.

VIII. Conclusion

Cargomail can play an essential role in communication across various industries in the public and private sectors.

A. Overall Summary

Combining Cargomail with the current email system creates a hybrid architecture that meets the needs of a modern communication tool.

B. Future Work

Cargomail brings content-addressed storage and a new data exchange mechanism into the email ecosystem, predestining the proposed system to become more than a bare messaging tool. It would be fascinating to build a prototype of the proposed solution to serve as a proof of concept.

IX. Discussion

While this proposal seems closely related to the Internet Mail 2000 [4] concept proposed by Daniel J. Bernstein, we differ in the new idea that the storage of email messages and their resources should be the responsibility of users and not of email providers.

References

[1] Jeffrey Rothfeder. 1992. Privacy for Sale: How Computerization Has Made Everyone's Private Life an Open Secret (pp. 22-23). Simon & Schuster Trade.
[2] I. Zboran, "Global Reference Identity Protocol (GRIP)," GitHub repository, March 2023, https://github.com/cargomail-org/grip.
[3] Universal Postal Union/Activities/Digital Services, accessed 27 March 2023, https://www.upu.int/en/Universal-Postal-Union/Activities/Digital-Services.
[4] Internet Mail 2000, accessed 23 April 2023, https://en.wikipedia.org/wiki/Internet_Mail_2000.