Authorization-Enhanced Mail System—Draft

Igor Zboran
izboran@gmail.com

***Abstract*—This paper intends to explain how the zero-trust framework, Correlated Authorization [1], can improve the current mail system.**

Electronic mail (email) is the most pervasive form of business information exchange. Email is being used not only as an interpersonal communication tool but also as a "default choice" for sending files. In this paper, the Correlated Authorization [1] zero-trust framework—built on top of User-Managed Access (UMA) [2, 3] and OAuth 2.0 [4, 5] protocols—is proposed to overcome the data storage, access control, and data transfer limitations of the current mail system.

I. Introduction

The main components of the mail 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 truly decentralized communication system on the Internet, and the email infrastructure forms the backbone of the worldwide digital identity.

II. Current Situation

Today, outgoing mail 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 that emerged long before the World Wide Web became popular. 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 are spam and attachment issues from the very beginning. While conceptually sound as a communication means, the mail 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 attachments delivery; bulky files are not transferred as an attachment but are shared via links. An "attachment sharing" is not natural for the mail 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. This attack exploits an OAuth 2.0 consent mechanism to steal an access token.

B. Confidentiality and Privacy

Now, if we (as users) want to use a single email address, we have no choice but to use one mail 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" [6]—is routed through a single mail service provider. We can call it a One-Address-Fits-All privacy issue.

C. Hyperlinks to Files

Documents, images, video, and audio should be an integral part of the email. The concept of keeping a recipient-owned copy of the sender's files is critical in some industries. List of issues with hyperlinks to 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 file in the email message.

D. Content Repository

The current mail system is missing a private content repository—a private "file system on steroids" with the capability to create, store, locate, send, receive, and share any content.

IV. Proposed Solution

Given that the current mail system is lagging behind modern communication and collaboration tools, we propose implementing the Correlated Authorization [1] zero-trust framework into the email ecosystem to enhance the usability and security of the mail system.

A. Motivation

Email, still the most popular communication tool, lacks an essential part of today's modern communications systems—a trust framework. Understanding this led us to incorporate a trust framework into the email ecosystem. At the core of the proposed solution is an attempt to improve the usability of email—not only as an interpersonal communication tool but also as the default choice to send and store files.

B. Concept

Authorization-Enhanced Mail System (AEMS) follows the concept of Correlated Authorization [1] while keeping compatibility with the standard mail system. We propose to integrate the Correlated Authorization [1] zero-trust framework with the mail system using a standardized SMTP/POP3/IMAP interface and, at the same time, mirror the existing email infrastructure by creating a parallel system of resource mailboxes. A web-based email application will access the resource mailbox, as illustrated in Figure 1. AEMS uses a two-way push-pull data transfer mechanism—SMTP protocol for push data and HTTP protocol for pull data. Mailboxes running on the resource servers will

use the content repository as a storage engine.

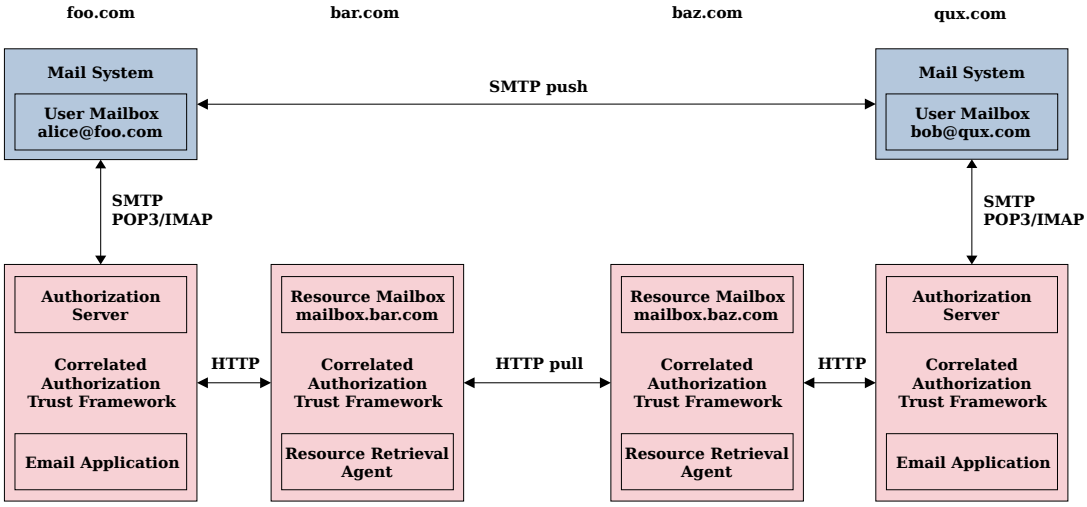

Fig. 1. Concept

C. Key Points

• An email is comprised of resources (message and attachments) stored in a resource mailbox—on an email-specific resource server.

• The email resources owned by the sender, stored in a sender's resource mailbox, are temporarily shared with the recipient. Following a successful sharing process, a notification email is sent to the recipient through the standard email system. The notification email contains the identifier of shared email resources—URI, the digital signature of shared email resources, and the category of correspondence, e.g., personal, business, healthcare.

• After receiving the notification email, the recipient's email application determines which of its resource mailboxes, designated by the recipient, will be used for communication according to the category of correspondence.

• The recipient's resource retrieval agent, which acts on behalf of the recipient, gets the resources URI and digital signature from the email application, gets delegated access from the sender authorization server using an authorization grant, and retrieves the email resources from the sender resource mailbox. The retrieved data is stored in the recipient resource mailbox and verified against the digital signature.

V. Advantages compared to Standard Mail System

AEMS has several decisive advantages over the current mail system.

A. Security and Privacy

User correspondence takes place between resource mailboxes. The user mailbox of the standard mail system is only used for the system (registration, notification) emails. This architecture guarantees more control over potential security and privacy issues such as leakage of intellectual property or loss of confidential content. Moreover, the user decides from whom or not to accept the email and thus protects his email address 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. Therefore, AEMS can keep official, business, personal, and healthcare correspondence separately on designated resource servers; the practical effect is that some critical data stored in this way never leave its resource server.

C. Private Content Repository

With the capability to create, store, locate, send, receive, and share any content, including documents, images, video, and audio, the proposed solution can be considered a promising foundation for the private content repository.

VI. Models and Scenarios

Although AEMS 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, AEMS allows citizens to use the non-governmental resource mailboxes from financial institutions, healthcare providers, etc. 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, more than 93% of postal operators provide some form of digital postal service either directly or in partnership with other companies [7]. AEMS 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.

VII. Conclusion

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

A. Overall Summary

Combining the Correlated Authorization [1] zero-trust framework

with the mail system creates a hybrid architecture that meets the needs of a modern communication tool.

B. Future Work

The Correlated Authorization [1] zero-trust framework brings a web-based data storage and a new data exchange mechanism into the email ecosystem that predestines the proposed system to become more than a bare messaging tool. The following are potential future R&D areas:

- Explore and describe the forwarding mechanism.
- Consider a consent mechanism design.
- Design an attachment version management system.

A prototype implementation of the proposed solution would be interesting to build, which would serve as a proof of concept.

Acknowledgment

This work has benefited from the valuable discussions with Eve Maler, founder of WG-UMA [8], and Alec Laws, chair of WG-UMA [8]. Both gave feedback that improved this paper's content. Last but not least, the UMA Work Group archives [9, 10] serve as a source of comprehensive information on authorization-related topics—many thanks to all involved.

References

[1] I. Zboran, "Correlated Authorization," GitHub repository, March 2022, https://github.com/umalabs/correlated-authorization/releases/download/v0.1/Correlated_Authorization.pdf.
[2] E. Maler, M. Machulak, J. Richer, and T. Hardjono, "User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization," Internet Engineering Task Force (2019), https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html.
[3] E. Maler, M. Machulak, J. Richer, and T. Hardjono, "Federated Authorization for User-Managed Access (UMA) 2.0," Internet Engineering Task Force (2019), https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-federated-authz-2.0.html.
[4] E. D. Hardt, "The OAuth 2.0 Authorization Framework," IETF RFC 6749 (Informational), 2012, http://tools.ietf.org/html/rfc6749.
[5] M. Jones, A. Nadalin, B. Campbell, J. Bradley, C. Mortimore, "OAuth 2.0 Token Exchange," RFC 8693 (2020), https://rfc-editor.org/rfc/rfc8693.txt.
[6] Jeffrey Rothfeder. 1992. Privacy for Sale: How Computerization Has Made Everyone's Private Life an Open Secret (pp. 22-23). Simon & Schuster Trade.
[7] Universal Postal Union/Activities/Digital Services, accessed 4 April 2022, https://www.upu.int/en/Universal-Postal-Union/Activities/Digital-Services.
[8] "User-Managed Access" Work Group at "Kantara Initiative," https://kantarainitiative.org/confluence/display/uma/Home.
[9] "The WG-UMA Archives," https://kantarainitiative.org/pipermail/wg-uma.
[10] "Kantara Initiative User-Managed Access WG," https://groups.google.com/g/kantara-initiative-uma-wg.