Authorization-Enhanced Mail System—Draft

Igor Zboran
izboran@gmail.com

***Abstract*—This paper intends to explain how the 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] mail trust framework—built on top of User-Managed Access (UMA) [2, 3] and OAuth 2.0 [4] 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 1971 and 1992 by many inventors. Over time, email has become the most commonly used Internet application. Nowadays, email is the only truly decentralized communication system of the Internet, and the email infrastructure forms the backbone of the worldwide digital identity.

II. 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. Current Situation

Today, outgoing mail is typically transferred from the source system to the destination system as a single text-encoded file using 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.

B. Functional and Security Flaws

Even though the major email service providers claim email accounts 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 mail systems 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 is known as an OAuth 2.0 authorization exploit.

C. Confidentiality and Privacy

Today, 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" [5]—is routed through a single mail service provider. We can call it a One-Address-Fits-All privacy issue.

III. Proposed Solution

Given that the current mail system is lagging behind modern communication and collaboration tools, we propose implementing the Correlated Authorization [1] mail 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 implement 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] framework with the mail system using a standardized SMTP/POP3/IMAP interface and at the same time mirror the existing email infrastructure by creating the parallel system of resource mailboxes. A web-based email application can 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.

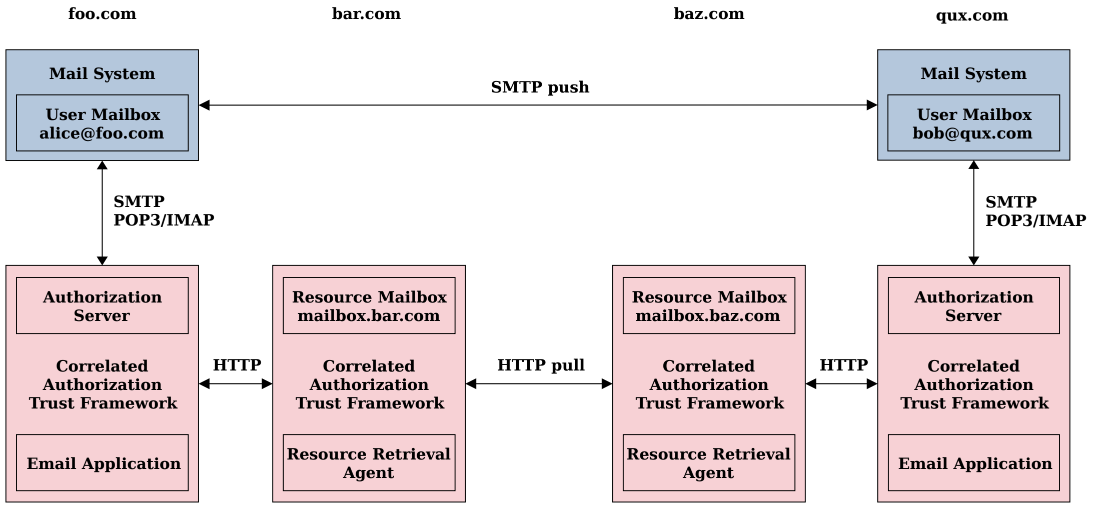

Fig. 1. Concept

Key points

- An email is comprised of resources (message and attachments) stored in a resource mailbox—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 with the email resources identifier (resources URI) is sent to the recipient through the standard email system.
- The recipient's resource retrieval agent, which acts on behalf of the recipient, gets the resources URI 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 are stored in the recipient resource mailbox.

Advantages over Standard Mail System

- 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.
- Usability: 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 simultaneously. To separate official, business, personal, and healthcare correspondence, AEMS provides the flexibility to exchange email correspondence according to various criteria between appropriate resource mailbox service providers.
- Platform: With the capability to store, locate, send and receive any content, including documents, images, audios, and videos, the proposed solution can be considered a promising platform for Content Services.

References

[1] I. Zboran, "Correlated Authorization," GitHub repository https://github.com/umalabs/correlated-authorization/raw/main/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] Jeffrey Rothfeder. 1992. Privacy for Sale: How Computerization Has Made Everyone's Private Life an Open Secret (pp. 22-23). Simon & Schuster Trade.