Authorization-Enhanced Mail System (AEMS) in less than 500 words

Igor Zboran
izboran@gmail.com

Introduction

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

Concept

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.

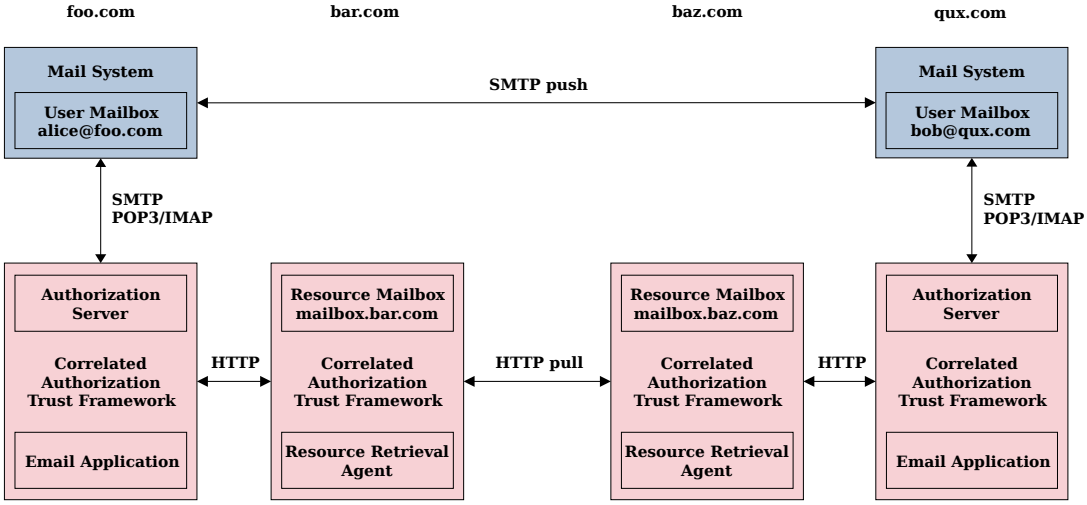

Fig. 1. Concept

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.

Advantages compared to 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 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.
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.

---

[1] I. Zboran, "Correlated Authorization," GitHub repository, March 2022, https://github.com/umalabs/correlated-authorization/releases/download/v0.1/Correlated_Authorization.pdf.