

Authorization-Enhanced Mail System—Draft

Igor Zboran
izboran@gmail.com

Abstract—Electronic mail (email) is the most pervasive form of business information exchange. Email is often used not only as an interpersonal communication tool but also as the default choice to send 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.

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. Despite the fact that SMTP has been updated, modified, and extended multiple times to increase security and efficiency, it still lags behind modern web-based protocols. The Correlated Authorization framework introduces a resource server and an authorization server into the mail system. The resource server is generally accessed by HTTP pull-based protocol. The two-way push-pull data transfer combined with a data storage system controlled by the standardized authorization protocol significantly leverages email security and enhances mail system utilization.

I. INTRODUCTION

The main components of the mail system were designed between 1971 and 1992 by many inventors. In the course of time, email has become the most commonly used application of the Internet. Nowadays, email is the only truly decentralized communication system of the Internet, and the email infrastructure forms the backbone of the world-wide digital identity.

II. PROBLEMS AND ISSUES

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

A. Current Situation

With the rising popularity of free email service providers, such as Gmail or Outlook.com, web browsers are increasingly being used to access the mail server. From a user standpoint, it is easy to read and send emails via web browser on any device, from anywhere in the world.

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. Main Concept

Authorization-Enhanced Mail System (AEMS) follows the concept of Correlated Authorization while keeping compatibility with the current mail system. We propose to integrate the Correlated Authorization 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 the email resource servers. A proprietary email application will be used to access the email resources, as illustrated in Figure 1.

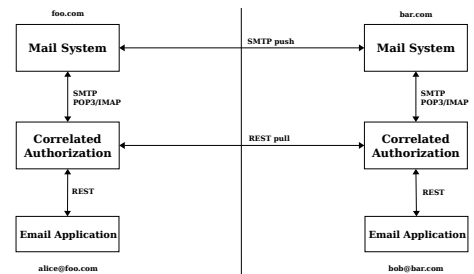


Fig. 1. Main concept

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.kantarinitiative.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.