Authorization-Enhanced Mail System

Igor Zboran
izboran@gmail.com
May 24, 2021

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 User-Managed Access (UMA) authorization framework is proposed to address data storage, access control and data transfer limitations of the current mail system. 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 a push protocol only. The UMA framework introduces a resource server and an authorization server into the mail system. The resource server is accessed generally by HTTP pull protocol. The two-way push-pull data transfer in combination with a data storage system controlled by the standardized authorization framework significantly leverages email security, enhances mail system utilization and elevates the email ecosystem to the ubiquitous Content Services platform.

Introduction

The main components of the mail system have been 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 worldwide digital identity.

Problem

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.

Current Situation

With the rising popularity of free email 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. Centralized access to the mailboxes, increases the security of web-based mail systems.

Current Flaws

Even though the main email service providers claim email accounts to be safe, the fact remains that major security and functional flaws are not fixed. There is still an attachments delivery dichotomy; bulky files are not transferred as an attachment but are shared via links. An “attachment sharing” is not natural for current mail systems where each message with attachments is expected to be time-consistent. Shared links pose a consent phishing attack threat where attacker tricks users into granting a malicious application access to sensitive resources. This is known as an OAuth 2.0 authorization exploit. The Authorization-Enhanced Mail System is resistant to this security exploit as there are no direct user involvement in access granting.

Proposed Solution

Given that the mail system is lagging behind modern communication and collaboration tools, we propose an OAuth-based access control management and consequently a new data exchange channel for the email ecosystem.

Motivation

Email still the most popular communication tool is lacking an important part of today's modern systems – an authorization framework. Understanding this lead us to implement the UMA authorization framework into the mail system. 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.

Main Concept

The Authorization-Enhanced Mail System is designed to follow the Identity and Access Management (IAM) best practices while keeping compatibility with the current mail system. ~~We propose to incorporate the UMA framework between the mail system with standardized SMTP/POP3/IMAP interface and the proprietary RESTful web-based email application as it is illustrated in Figure 1.~~

Features and Comparison with Current Mail System

The novelty of the proposed solution approach can be assessed by comparison with the current mail system.

New Features

The proposed AEMS solution provides several new features that are lacking in the current mail system:

- Intrinsic privacy-preserving properties. Each user can have their own separate UMA/MBX as an email repository. The user can run his own UMA/MBX, even his own AS.
- Single UMA/MBX for both incoming and outgoing emails.
- Multiple UMA/MBXs per one email address.
- Built-in cross-domain autonomic (without conscious user intervention) access control using the standardized UMA framework.
- Autonomous (without interfering with the mail system) data exchange channel.
- No attachments size limit. Attachments are transferred as separate files without size limit.
- Linked content using a clickable hyperlinks.
- Instant messages. Messages and attachments are transferred separately, there is no need to wait for incoming bulky message-with-attachments file. Attachments-stripped bare messages are transferred with a higher priority.

Comparison with Current Mail System

The use of AEMS has many advantages over the current mail system. The AEMS architecture increases the robustness and performance of the existing mail system. In the following we highlight the advantages of the proposed solution compared to the current mail system.

1. Security and Privacy

User correspondence takes place between UMA Mailboxes. The mailbox of the standard email system becomes redundant and is only used for system (registration, authorization) emails. This architecture guarantees more control over potential security and privacy issues such as leakage of intellectual property or loss of confidential content and makes the system compatible with enterprise security policies.

2. Usability

The UMA Mailbox is decoupled from the email address. This allows a user with a single email address to use simultaneously multiple UMA Mailboxes. To separate official, business, personal and healthcare correspondence, AEMS provides the flexibility for storing emails according to various criteria within an appropriate UMA Mailbox provider.

3. 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.

4. Integrations

AEMS provides a standardized Restful/GraphQL application interface to ease the integrations with external marketing, sales, Enterprise Content Management (ECM) or Customer Relationship Management (CRM) systems.

Conclusion

AEMS can play an important role in communication across various industries in the public and private sectors. Consolidation of repository, communication and identity represents a central source of information within any organization.

Overall Summary

The email system technology in combination with the UMA framework creates a composite architecture that meets the needs of the modern communication tool. The proposed solution can be used as a Content Services platform to provide the e-records storage, exchange and retrieval system protected by the standardized authorization framework utilized by users through the email application.

A consolidated access control and a new data exchange mechanism leverages email security and enhances the mail system utilization. The question arises as to whether the standard implementation of UMA 2.0 will fit into the current mail system and how difficult it will be to build the UMA email extension.

Future Work

The UMA framework brings into the email ecosystem a new data storage and exchange technology that predestine the mail system to become more than a bare messaging tool.

The following are potential future R&D areas:

- Use an autoforwarding feature of existing mail system to loose bundling between AEMS and the standard mail system to drive the AEMS adoption.
- Explore the possibility of delivering the authorization code via SMS; use phone numbers instead of email addresses.
- Consider a Consent mechanism extension design.
- Explore linked content using a clickable hyperlinks – linking content across the business.
- Design an extension for exchanging tagged messages and attachments – grouping content across the business.
- Design an attachment versioning extension – managing the attachment content changes.
- Explore health information exchange between healthcare professionals and inspect use of email communication between patients and healthcare professionals.
- Employ regular email clients and applications using JMAP protocol to support a standardized email API.
- Design and use a proprietary GraphQL API to replace the poorly adopted JMAP protocol.
- Incorporate an electronic mailing/discussion list system into the proposed solution to extend the basic email functionality.
- Explore other ways of data origin authenticity (WebFinger, WebFist), replace SMTP with a web-based protocol.

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

About the Author

Igor Zboran is a mechanical engineer by education with professional experience as a software engineer and solutions architect. He'd like to transform his knowledge into a useful system or service that people would love to use.

Igor received Ing. degree in Mechanical Engineering from the University of Žilina, Slovakia in 1988. After graduating, he worked in several small private companies as a software developer. From 2008 to 2009, he provided expert advice to Prague City Hall IT department, Czech Republic as an external consultant. He invented a new decentralized Identity-Based Privacy (IBP) trusted model built around OAuth2 and OpenID Connect standards. Igor is a strong proponent of open source software and open standards.