Authorization-Enhanced Email System

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 access and data transfer limitations of current email systems. 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 Resource Server (RS) and Authorization Server (AS) into the email system. The RS is accessed generally by HTTP protocol that was designed as a pull protocol. The two-way push-pull data transfer in combination with data access control significantly leverages email security and enhances email system utilization.

Introduction

The main components of the email 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 the 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 email 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 email server. From a user standpoint, it is easy to read and send email via web-browser on any device, from anywhere in the world. Centralized access to the mailboxes, increases the security of web-based e-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 problem. The bulky files are not transferred as an attachment but are shared via links. An “attachment sharing” is not natural for postal systems where each message with attachments is expected to be consistent. Shared links pose a content phishing attack threat where attacker tricks users into granting a malicious application access to sensitive resources. It is an OAuth 2.0 authorization exploit. Authorization-Enhanced Email System is resistant to this security exploit as there are no direct user involvement in access granting.

Proposed Solution

Given that email system is lagging behind modern communication and collaboration cloud services, we propose an OAuth-based access control management and consequently a new data transfer channel for 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 User-Managed Access authorization framework into email ecosystem.

Main Concept

We propose to incorporate the UMA framework between email system with standardized SMTP/IMAP interface and proprietary RESTful web-based email application.

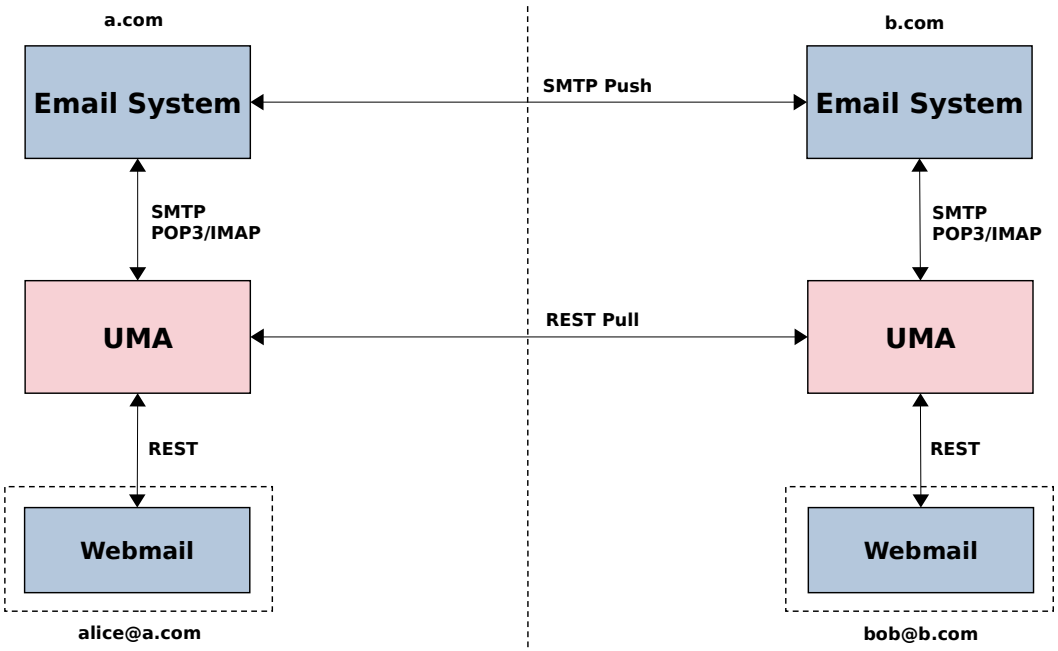

Figure 1. Main concept

Claims:

- No user content is stored in messages, just links to the UMA RS (message body link, attachment links).
- The actual content of the messages and attachments are stored on UMA RS.
- The user communicates to UMA RS via Webmail (REST protocol)
- The user as a sender in RS owner role shares temporary links to the actual message content with recipients and sends dummy email message with links to RS via email system (SMTP protocol) to recipients.
- On the recipent side the incoming email with temporary shared links is processed in Mail Fetch Agent (MFA) that acts in Requesting Party role on behalf recipent and actual message content is downloaded from sender's RS and are copied to recipient RS. Recipient becomes an owner of copied content. The temporary shared links on the sender side are deleted.

Notes:

- This is not a file sharing by email system.
- Both senders and recipients have always RS owner role. They don't share any data with each other - they hold copies.
- UMA Requesting party role belongs recipient's agent – Mail Fetch Agent (MFA) - that acts on behalf recipients and creates data copy using temporary shared links from a dummy email messages.

Trust Model

Decentralized three-way trust relationship model:

- Mail Trust – SMTP to SMTP trust (the most vulnerable).
- Mail to UMA Trust – a trust delegation from email system to UMA framework.
- UMA Trust – a trust between UMA components.

There is no trust relationship between authorization servers and UMA roles remains co-located.

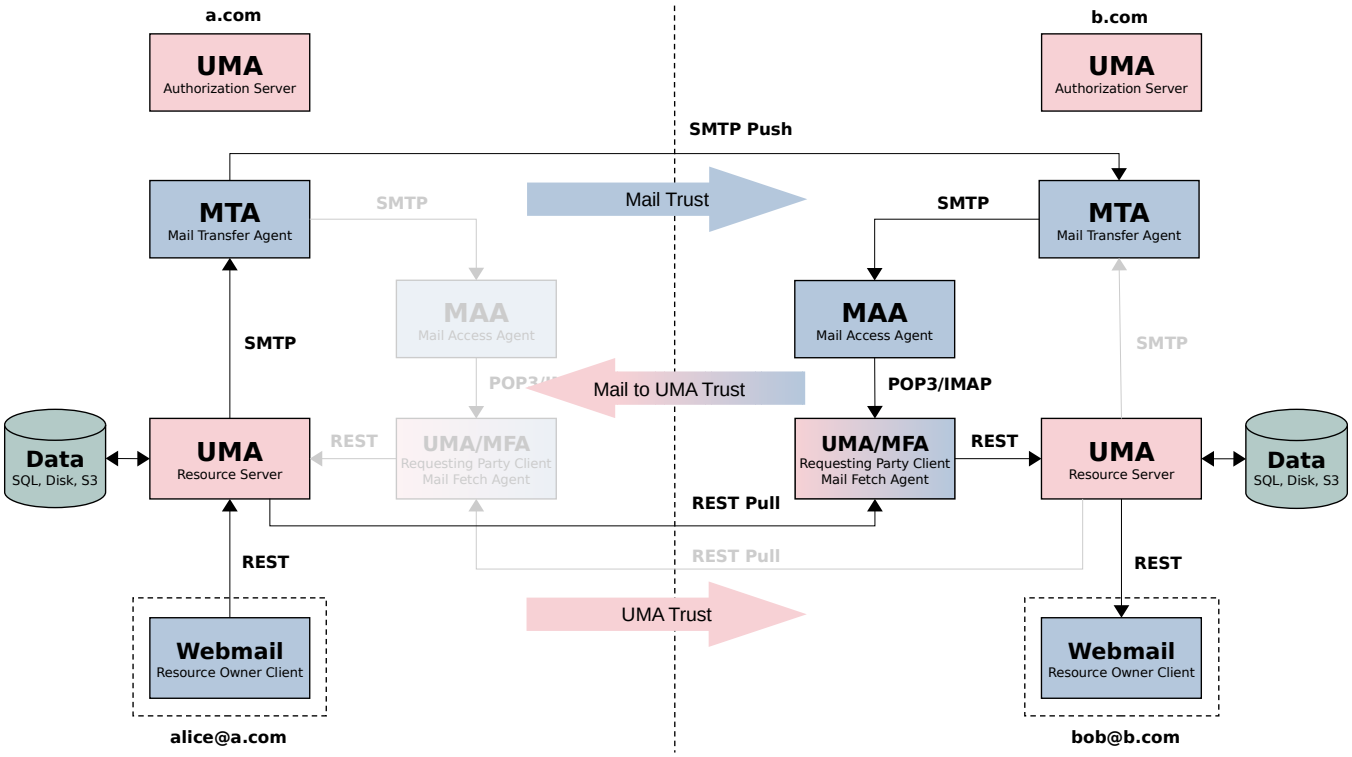

Figure 2. alice@a.com to bob@b.com trust model

Scenarios and Flows

Data-flow …

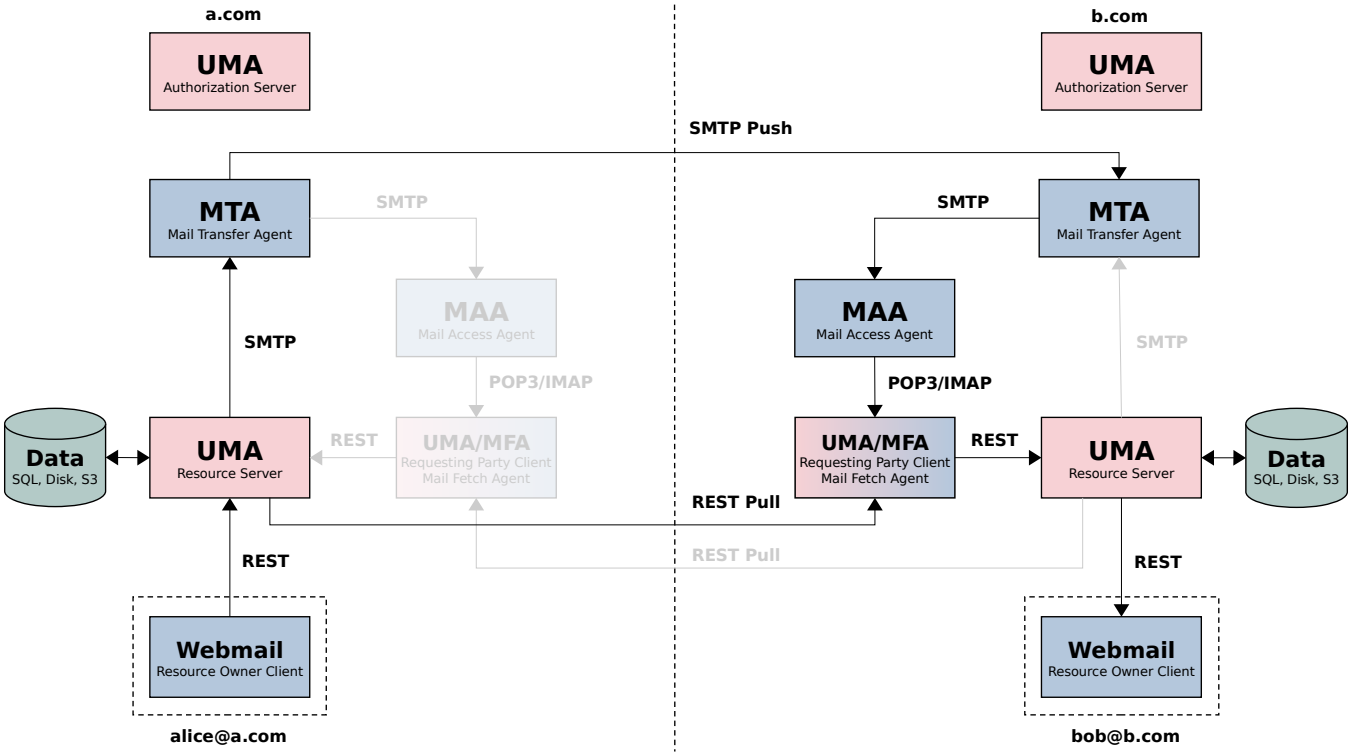

Figure 3. alice@a.com to bob@b.com data-flow

Features and Comparison with Current Email System

Features

Comparison with Current Email System

Conclusion

Authorization-Enhanced Email System has been designed to follow standardized User-Managed Access framework best practices while keeping compatibility with current email systems.

Overall Summary

A consolidated access control and data transfer leverages email security and enhances email system utilization.
The question arrives whether a standard implementation of UMA can be integrated into the current email ecosystem.

Future Work

The combination of User-Managed Access framework with email system outcomes in a new data exchange technology that predestine email system to become more than a bare messaging tool.

The following are potential future use case areas:

- Consent.
- Tagged message and attachment (metadata) exchange.
- Use email system as a Content Management System alternative.
- Explore Health information exchange.

A prototype implementation of Authorization-Enhanced Email System could be interesting.