User-Managed Access and Web-Based Email System

Beyond “Alice to Bob sharing”

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 attachment transfer limitations of current email systems. The proposal goes beyond the UMA primary use case “Alice to Bob sharing”.

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 emails 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. A related security issue is that shared links pose a consent phishing attack threat that exploits OAuth 2.0 authorization technology.

Proposed Solution

Solution Components

Solution Scenarios and Flows

Conclusion

Transparency and unambiguous data ownership - data are transferred not shared.

Overall Summary

Although enterprise file sharing and synchronization systems are seeing strong adoption, centralized systems are not very acceptable solutions for B2B and B2C communication. Missing Identity and Access Management integration on both communication sides can lead to potential privacy issues such as leakage of intellectual property or loss of confidential content and makes these systems incompatible with enterprise security policies.

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 suggested future work objectives:

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