Privacy Enhanced Mail (PEM)

Team Members:

Dr. Sonali Kothari - Guide

Arghadeep Das - PRN. 21070122023

Kashish Mehta - PRN. 21070122073

Sangeet Agrawal - PRN. 21070122140

Vaishnavi Bhoir - PRN. 21070122199

Introduction

Overview In the modern computer era, secure communication is very important, especially in light of the widespread presence of e-mail security holes and cyber-threats. In this respect, a system known as Privacy Enhanced Mail, or PEM, was developed to enhance the security of e-mail and to protect sensitive information from illicit access, modification, and interception. Among the key issues of confidentiality, integrity, and authenticity, the system employs a wide variety of cryptographic techniques.

Significance of PEM

PEM is utilized to preserve the professional and interpersonal communications.The safety of the emails during communication enhances the trust of the parties communicating with each other. In such industries as the health, banking, and legal industries, leakage of confidential information without any permission may result in severe issues. Emails are protected with the help of PEM against cyber attacks like phishing, data leakage, or interception.

Key Features of PEM

I. **Confidentiality:** PEM uses safe techniques like DES (Data Encryption Standard) to encrypt emails, ensuring that only authorized recipients can view them.

II. **Integrity:** This is achieved by employing message digests (hash functions-like MD2, MD5) and digital signatures. Only authorized recipients will be able to open the encrypted email because of secure encryption methods like DES (Data Encryption Standard).

III. **Authentication:** The identity of the sender and the provenance of the communication are authenticated with the use of digital signatures in PEM.

Mechanisms of PEM

PEM operates in four essential steps to achieve secure communication:

I. **Canonical Conversion:** This stage standardizes the email format to guarantee that it is read reliably on all platforms and operating systems. This ensures uniformity in the reading and processing of the message, removing any chance for an error to creep in.

II. **Digital Signature:** This digital signature involves hashing the message and encrypting this result with the sender's private key. This signal guarantees that the message has not been tampered with and informs the receiver of the authenticity of the sender.

III. **Encryption:** This uses a symmetric key to encrypt the actual message as well as the digital signature. This, then, ensures that only the receiver of the decryption key can read what's inside the email.

IV. **Base-64 Encoding:** Base-64 encoding converts the encrypted message into a text-based format so that it may be transmitted over common email systems without incurring damage to the data.

Case Study: Rmail

Email Rmail is a cutting-edge email provider that uses the PEM protocols to safely deliver email. Rmail is used to encrypt content with emails to ensure only authorized access is present to view contents. Its feature list includes reporting capabilities, where the actual sender of an email can track whether the email has arrived in the receivers' inboxes and whether it has been opened. Such transparency becomes very important for sectors like the legal and finance sectors. Furthermore, Rmail ensures that privacies such as GDPR remain confidential, thus making it a safe solution for private communication.

Conclusion

In summary, it can be stated that in the ever-increasing threat world, PEM is an essential protocol that provides a secure mechanism for the protection of private information, thereby building trust, especially while seeking compliance with data protection regulations. Solutions such as Rmail show just how well one can employ PEM in scenarios that have everyday practice, safeguarding the communication that matters most-security and privacy, in the industries.