LAB Assignment

March 7th 2024

Team Members

1. Shreekar Kolanu : 017406493
2. Satwik Upadhyayula : 017423796
3. Vineet Samudrala : 017426253
4. Bala Supriya Vanaparthi : 017464135

Security of Person-to-Person Email Services:

1. **Encryption in Transit:**
    a. Most major email providers use Transport Layer Security (TLS) to encrypt data in transit between the sender and the recipient. This helps protect the email content from interception during transmission.
2. **End-to-End Encryption:**
    a. Some services, like ProtonMail, offer end-to-end encryption, ensuring that only the intended recipient can decrypt and read the message. However, this is often an opt-in feature and requires both the sender and the recipient to use the same service with end-to-end encryption.
3. **Two-Factor Authentication (2FA):**
    a. Many email services provide 2FA, adding an extra layer of security by requiring a second form of verification in addition to the password.
4. **Security Features:**
    a. Email providers employ various security features, such as spam filters, malware detection, and phishing protection, to enhance overall security.
5. **Security Updates:**
    a. Regular software updates and security patches are crucial to fixing vulnerabilities. Reputable email providers typically prioritize and implement these updates regularly.
6. **User Responsibility:**
    a. Users play a significant role in email security. Strong, unique passwords, careful handling of login credentials, and awareness of phishing tactics contribute to overall email security.

Internal Email Leak Prevention:

1. **Data Loss Prevention (DLP) Solutions:**
    a. Companies can implement DLP solutions to monitor and control sensitive data movement within the organization. These systems can identify and prevent the unauthorized transfer of sensitive information.
2. **Access Controls:**
    a. Companies can implement access controls to restrict who can access certain types of information. This includes limiting access to confidential emails to only those employees who need it for their job responsibilities.
3. **Employee Training:**
    a. Education and training programs can raise awareness among employees about the importance of keeping sensitive information confidential. This includes recognizing phishing attempts and understanding the risks associated with sharing sensitive information via email.
4. **Monitoring and Auditing:**
    a. Companies can employ monitoring and auditing tools to keep track of internal email communications. This helps identify any unusual patterns or potential security breaches.
5. **Encryption for Sensitive Data:**
    a. Encrypting sensitive data within emails adds an extra layer of protection. This ensures that even if an email is intercepted, the contents remain secure and inaccessible without the proper decryption key.