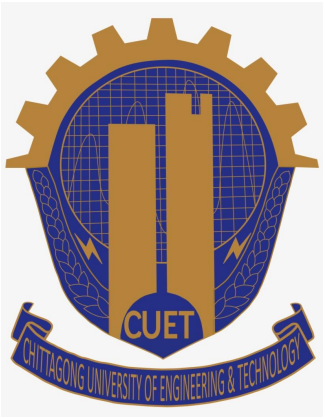
Chittagong University of Engineering & Technology



Department of Computer Science & Engineering

Course Code : CSE-435

Course Title : Information Security

Assignment No : 02

Assignment Title : Techniques for preventing email attacks

Submitted To:

Md. Sabir Hossain

Assistant Professor,

Dept of CSE, CUET

Submitted By:

Name: Md Ashraful Alam

ID: 1804061

Section: A

Level-4 **Term-**I

Remarks

Table of Contents

Objectives

- To identify the various types of preventing email attacks
- To know about their advantages, disadvantages

Introduction

Any unwanted activity or exploitation that impacts email systems, users, or information sent by email is referred to as an email attack. Email assaults continue to be a significant worry in the modern world. They define malevolent actions carried out over email with the intention of deceiving or harming individuals or groups. Over time, these attacks have developed in sophistication, posing a greater threat to cybersecurity.

Preventing email assaults is crucial in today's digital environment when cyber threats continue to grow and pose serious hazards to people and companies. Email assaults including phishing attempts, virus distribution, and email spoofing can cause monetary losses, data breaches, reputational harm, and the release of private and confidential information. These attacks use technological weaknesses, security flaws, and human weaknesses to compromise email integrity, gain unauthorized access, and mislead recipients. Effective preventative measures must be put into place in order to safeguard email systems and guarantee the security of sensitive information communicated over email.

Techniques for Email Attacks

1. **Sender Policy Framework(SPF):** SPF is a technique for email authentication that lets domain owners choose the servers permitted to send emails on their behalf. Organizations may stop email spoofing and shield users from receiving fake emails by publishing SPF entries in the Domain Name System (DNS).

   Pros:

   - checks the IP address of the transmitting server against a list of permitted servers to help prevent email spoofing.
   - reduces the possibility that valid emails may be marked as spam, improving email delivery.
   - quite simple to configure and implement.

Cons:

- End-to-end email security is not provided; only domain-level authorization is addressed.
- depends on the receiving server's ability to handle SPF validation, and not all servers are capable of doing so.
- Limited defense against malware or other email-based threats like phishing.

2. **DomainKeys Identified Mail (DKIM):** Email message integrity and authenticity are checked using cryptographic signatures by DKIM, an email authentication method. It includes including a digital signature in outgoing emails that the recipient's mail server may check to make sure the message was not altered while en route.

   Pros:

   - enables the use of cryptographic signatures to validate the authenticity and integrity of email communications.
   - enables email security at a higher degree than SPF alone.
   - helps email senders establish confidence with their recipients by letting them be accountable for their communications.

   Cons:

   - requires the email sender to set up and manage cryptographic keys.
   - Especially in big enterprises with several domains or email systems, an implementation might be challenging.
   - It could be difficult to identify the problem and take appropriate action if DKIM keys are compromised.

3. **Domain-based Message Authentication, Reporting, and Conformance (DMARC):** SPF and DKIM are built upon by DMARC to offer a robust framework for email authentication. It allows domain owners to specify guidelines for what should happen to emails that don't pass authentication tests. Additionally, DMARC gives enterprises access to email authentication errors so they can keep an eye on fraudulent email traffic and take appropriate action.

   Pros:

   - a framework for email authentication that is comprehensive and builds on SPF and DKIM.
   - allows domain owners to specify handling guidelines for emails that fail authentication tests.

   Cons:

- needs adequate setup and oversight to prevent false positives or negatives.
- Implementation can be challenging, particularly in businesses with intricate email networks.
- If DMARC is not extensively embraced throughout the email industry, it will have limited effectiveness.

4. **Multi-Factor Authentication (MFA):** By requiring users to give additional authentication factors, such as a fingerprint, one-time passwords, or hardware tokens, in addition to their passwords, MFA offers an extra layer of protection to email accounts. Even if passwords are stolen, this prohibits illegal access to email accounts.

   Pros:

   - uses cutting-edge methods to identify and stop complex email threats, such as machine learning and behavioral analysis.
   - offers proactive defense against phishing, malware, and other email-based assaults such as zero-day vulnerabilities.
   - aids firms in adapting to changing attack vectors and staying ahead of emerging dangers.

   Cons:

   - Additional authentication processes may cause problems with user acceptance and usability.
   - Additional infrastructure or third-party authentication services could be needed for implementation.
   - To guarantee correct MFA usage and steer clear of possible hazards, user education and assistance are crucial.

5. **Advanced Threat Protection (ATP):** For the purpose of identifying and thwarting sophisticated email threats including spear-phishing, zero-day assaults, and malware-filled attachments, ATP solutions use a variety of approaches, such as machine learning, behavioral analysis, and sandboxing. To detect and filter fraudulent emails, these technologies examine email content, attachments, and sender activity.

   Pros:

   - uses cutting-edge methods to identify and stop complex email threats, such as machine learning and behavioral analysis.
   - offers proactive defense against phishing, malware, and other email-based assaults such as zero-day vulnerabilities.

- aids firms in adapting to changing attack vectors and staying ahead of emerging dangers.

Cons:

- It is possible for false positives or negatives to happen, which might cause genuine emails to be mistakenly classified as malicious or vice versa.
- Dedicated hardware, software, or cloud-based services can be needed for implementation, raising operating expenses.
- To guarantee that ATP solutions continue to be useful and current, ongoing monitoring and maintenance are required.

Conclusion

A multi-layered strategy is needed to defend email communication against many forms of assault. Email security can be greatly improved and defended against a variety of email attacks by combining secure email protocols, spam and phishing filters, email authentication techniques, encryption, user education, multi-factor authentication, advanced threat protection, incident response, and routine updates.