

Email Safeness Scorer

Email Safeness Scorer Tool

- Malicious users use emails for sending unsolicited messages for either advertising their product and services or for enticing gullible users for sharing their important information.
 - This kind of message is generally referred to as spams.
 - Spams are undesired emails, which are unsolicited bulk messages sent through email for advertising, phishing or inflicting malware on the recipient system.
- The email safeness scorer is a application which would provide the safeness score of the emails based on its content,
 - low safeness score signifies the dubious, scam, phishing, malicious or spam emails
 - high score tells that the email is safe i.e. the email is free from malicious intentions.

Solving Spam Problem

- Various algorithms have been devised for detecting spams.
- Some are successful and effective on the other hand others are highly biased and need regular training.
- We have created a multi layer neural network and trained it with a set of email data, and provided the scope for regular training with new examples.

Types of Email Phishing

Deceptive Phishing

- This is the most common type of phishing attack wherein a cybercriminal impersonates a known popular entity, domain or organization in the email and attempt to steal sensitive private information from the victim such as login, password, bank account detail, credit card detail, etc.
- This type of attack lacks sophistication as it does not have personalization and customization for the individuals.
- For an example, emails containing Phishing URL is disseminated in bulk to large users as a volume of mail is very high the cybercriminal would expect that many users will open the emails and visit the malicious URLs or open the infected attachments
- The email subject will be such that it might create urgency such as "Your account has been hacked, change your password immediately!", "Your bill is overdue-pay immediately of pay fine!" or other similar messages, once a user open such messages or visit the URLs the damage is done

Spear Phishing

- In this type of phishing emails contain an abundance of personalization information about the prospective victim.
 - The email might contain the name, company name, designation or his friends, colleagues and other social information of the recipient.
 - The proliferation of the company website, personal website and social media enables cybercriminals to get such details and assist them in forging a very convincing email.

Whale Phishing

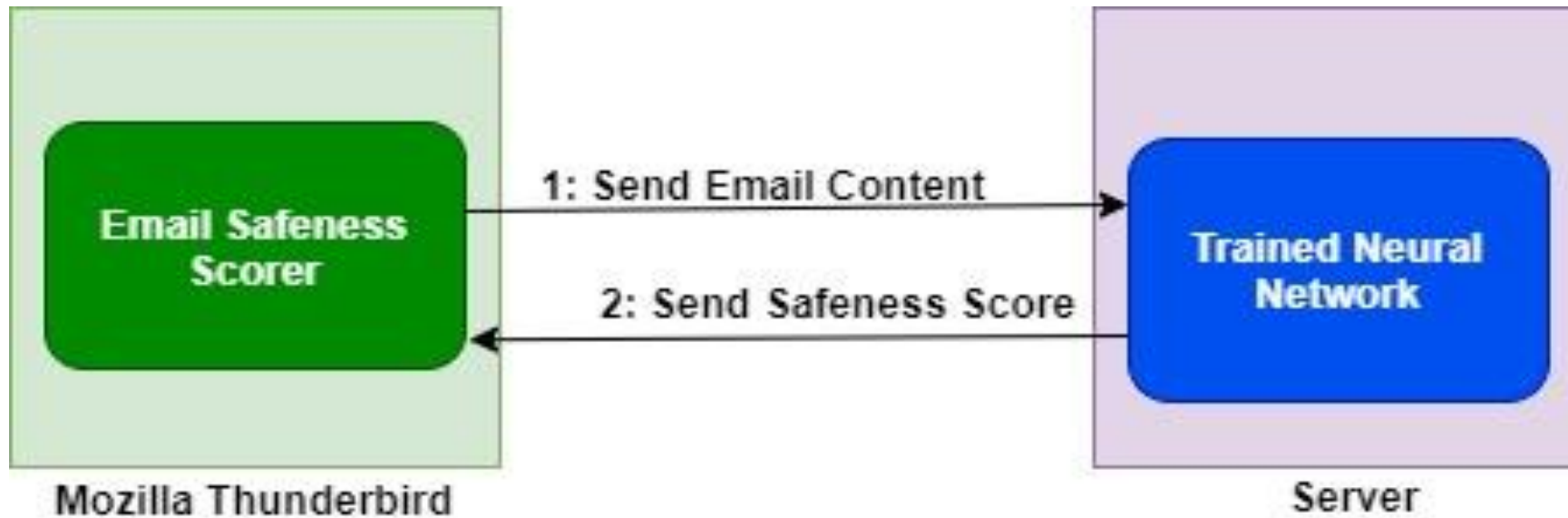
- This type of phishing targets business leaders such as CEO of top-level management employees to spear phish a "whale", here top-level executive such as CEO.
- The main aim of this type of phishing is to gather confidential information from the CEO and impersonate as CEO.
- This attack can render maximum damage to company financial prospects, market value, and reputation.

Email Safeness Scorer

- Brief Description

- ✦ A plug-in for Mozilla Thunderbird(a popular email client) that would display the safeness score for the email received based on its content.
- ✦ The email safeness scorer has two parts.
 - ✦ Server part, with the email content analysing ability component using machine learning techniques.
 - ✦ Client part, a plug-in for Mozilla Thunderbird that would send the email content to the safeness scorer server asynchronously for analysis and would display the safety score returned from the server.

Block Diagram of Email Safeness Scorer



Deployment Methodologies

- Server can be made publicly available that can be accessed by different Mozilla Thunderbird Email Client.
- Its installer for Mozilla Thunderbird plug-in would also be available.
- The plug-in can be made available for download at Mozilla Thunderbird extension store.

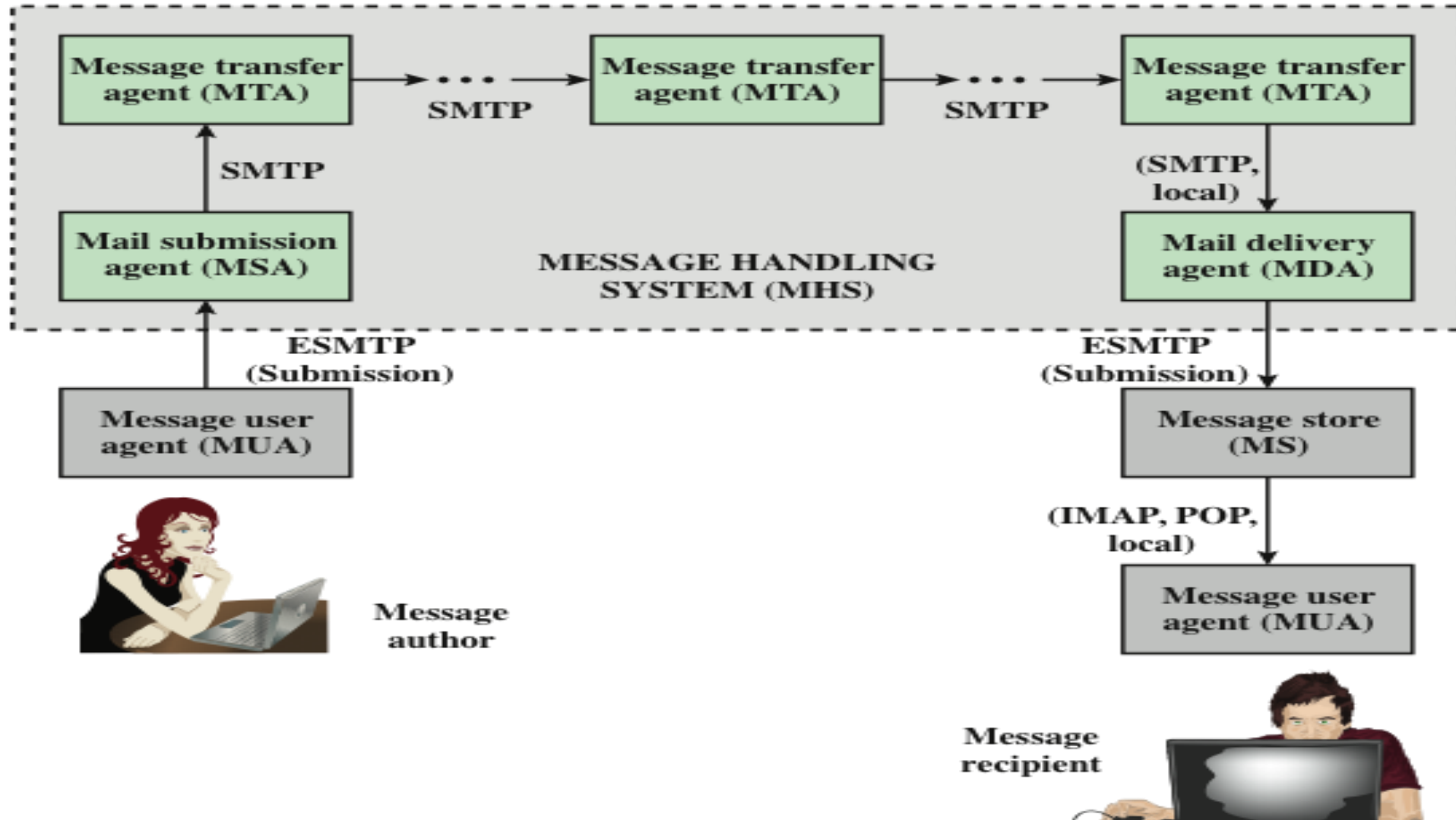
Thank You

Email Security

Quick E-mail History

- SMTP and RFC 822 (later RFC 5322)
 - SMTP is the email transfer protocol running over TCP
 - RFC 822/5322 defines the message format and headers
 - only ASCII messages
- MIME (Multipurpose Internet Mail Extensions)
 - an extension of the original internet e-mail protocol
 - content type
 - Almost any type of information can appear in an email message
 - transfer encoding
 - specifies how the message body is encoded into textual form (radix64 is common)
- S/MIME: Secure MIME
 - new content types, like signature, encrypted data

More on Internet Email Architecture



Email Terminologies

- Mail User Agent (MUA): a program which provides a human user interface for reading and sending mail.
 - Examples: elm, pine, mutt, Outlook, Netscape, Thunderbird.
- Mail Transport Agent (MTA): a program which acts as a "mail server". Specifically, it's responsible for managing a queue of outgoing mail, and for accepting (or rejecting) incoming mail.
 - Examples: sendmail, qmail, postfix, exim.
- Mail Submission Agent (MSA): a relatively new term in the e-mail field.
 - This is the component of an MTA which accepts new mail messages from an MUA, using SMTP.

Continued..

- Mail Delivery Agent (MDA): the component of an MTA which is responsible for the final delivery of a message to a local mailbox on disk.
 - Sometimes this is a separate program, and sometimes it's built into the MTA
- Post Office Protocol (POP): a protocol used by some MUAs to retrieve mail from a user's mailbox on a remote server.
 - Often written "POP3".
 - The official TCP port number for POP3 is 110.
- Internet Message Access Protocol (IMAP): a protocol used by some MUAs to retrieve mail from a user's mailbox on a remote server.
 - This is a newer and more complicated protocol than POP, with a lot more functionality.
 - The official TCP port number for IMAP is 143.
 - IMAP is more flexible and complex than POP3.
- The **main difference** is that **IMAP**(Internet Messaged Access Protocol) always syncs with mail server so that any changes you make in your mail client (Microsoft Outlook, Thunderbird) will instantly appear on your webmail inbox.

Post Office Protocol (POP3)

POP is a simple protocol that only allows downloading messages from your Inbox to your local computer.

The POP server listens on port 110, and the POP with SSL secure(POP3DS) server listens on port 995

In POP3 the mail can only be accessed from a single device at a time.

To read the mail it has to be downloaded on the local system.

The user can not organize mails in the mailbox of the mail server.

The user can not create, delete or rename email on the mail server.

A user can not search the content of mail before downloading to the local system.

After download, the message exists in the local system if the local system crashes message is lost.

Changes in the mail can be done using local email software.

All the message are downloaded at once.

Internet Message Access Protocol (IMAP)

IMAP is much more advanced and allows you the user to see all the folders on the mail server.

The IMAP server listens on port 143, and the IMAP with SSL secure(IMAPDS) server listens on port 993.

Messages can be accessed across multiple devices

The mail content can be read partially before downloading.

The user can organize the emails directly on the mail server.

The user can create, delete or rename email on the mail server.

A user can search the content of mail for specific string before downloading.

Multiple redundant copies of the message are kept at the mail server, in case of loss of message of a local server, the mail can still be retrieved

Changes made web interface or email software stay in sync with the server.

Message header can be viewed prior to downloading.

Email Security

- E-mail is one of the most widely used network services
 - One of the old killer applications of the Internet
- Normally message contents not secured
 - Can be read/modified either in transit or at destination by the attacker
- E-mail service is like postcard service
 - just pick it and read it

Email Security Enhancements

- confidentiality
 - protection from disclosure
- authentication
 - of sender of message
- message integrity
 - protection from modification
- non-repudiation of origin
 - protection from denial by sender

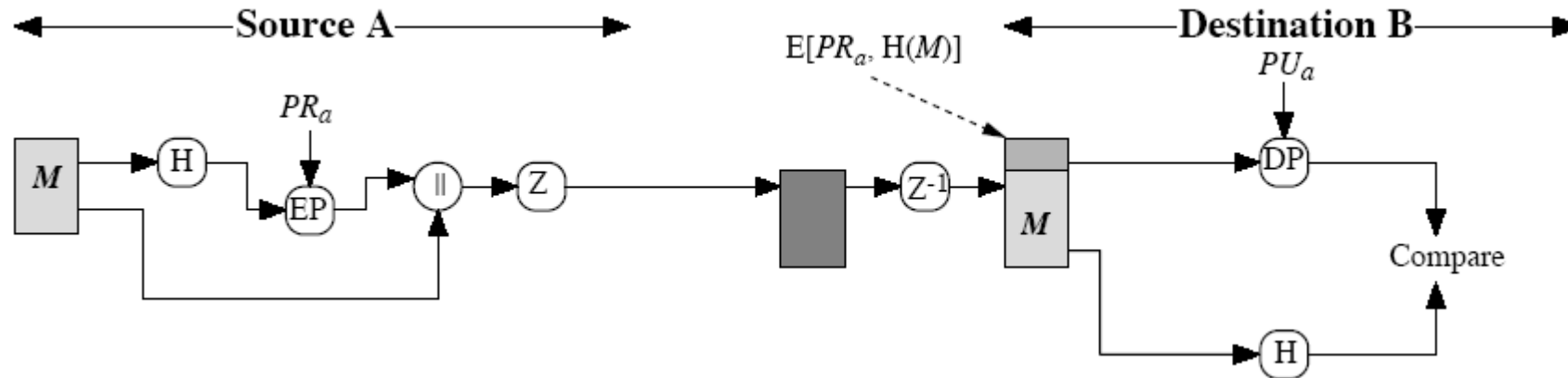
Pretty Good Privacy (PGP)

- Widely used secure e-mail software
 - originally a file encryption/decryption facility
- Developed by Phil Zimmermann
- Best available crypto algorithms are employed
- Available on several platforms with source code
- Originally free, now commercial versions exist
- Not controlled by a standardization body
 - although there are RFCs

PGP Mechanisms

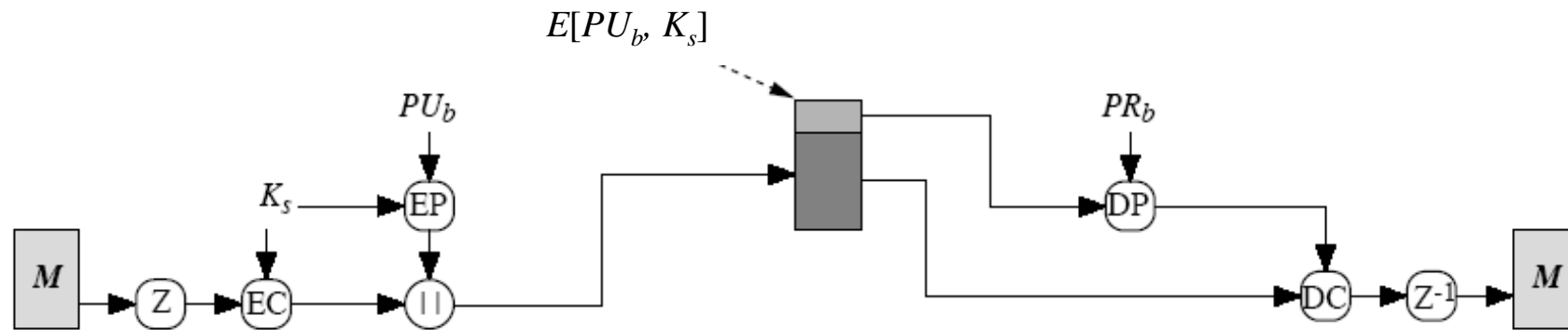
- Digital Signatures (and consequently message authentication and integrity)
 - RSA, DSS, and others
- Message Encryption
 - CAST, IDEA, 3DES, AES, etc.
 - symmetric keys are used once and encrypted using RSA or ElGamal
- Compression using ZIP
- Radix-64 conversion (to ASCII)
 - for e-mail compatibility

PGP Operation – Digital Signatures



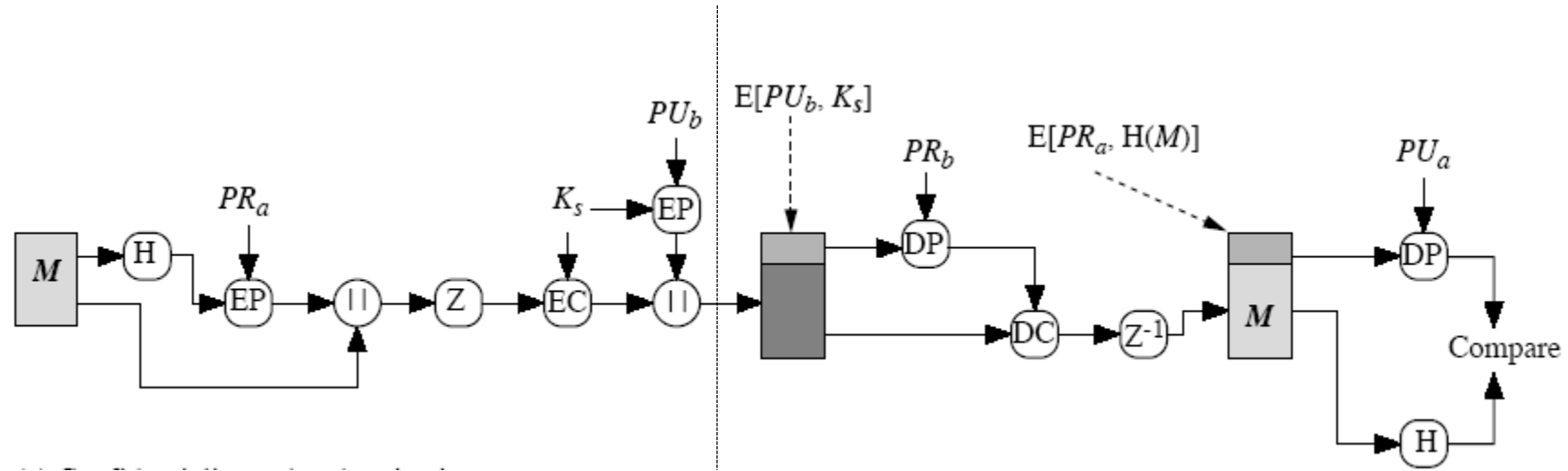
- Classical application of public key crypto
 - This figure is actually for RSA
 - for DSA refer to previous lectures
- Z is zip function
- radix-64 conversion is done after zip at sender, before Z^{-1} at receiver
 - may be done only for signature or for the whole message

PGP Operation – Confidentiality



- One-time session key, K_s
 - generated at random
 - encrypted using a public key cryptosystem, EP
 - RSA or ElGamal
- Message is compressed before encryption
 - This is the default case

PGP Operation – Confidentiality and Authentication



- uses both services on same message
 - create signature and attach to message
 - compress and encrypt both message & signature
 - attach encrypted session key
 - radix-64 conversion is for everything at the end

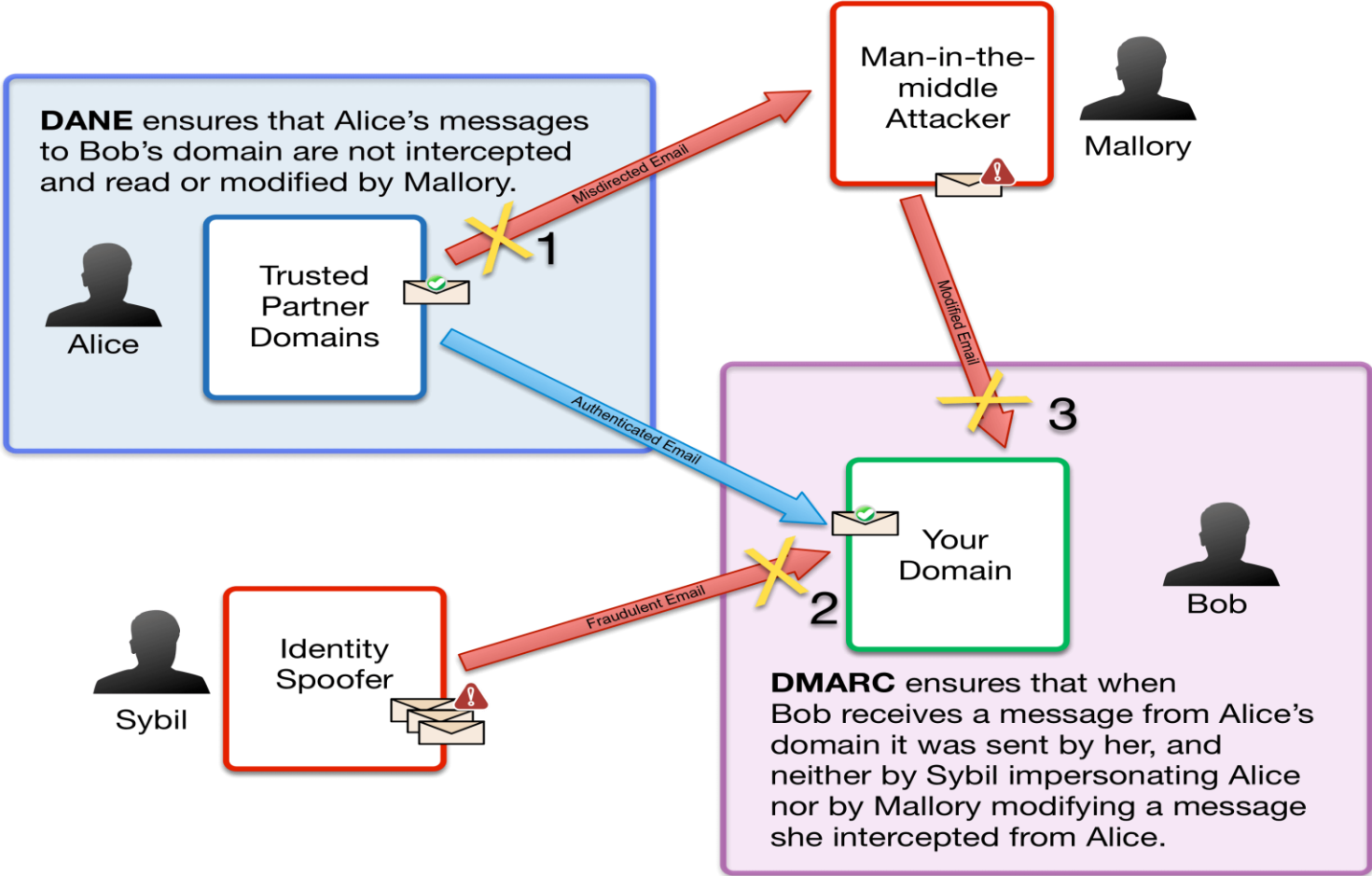
PGP Operation – radix-64 conversion

- Encrypted text and signatures create binary output
- however email was designed only for text
 - hence PGP must encode raw binary data into printable ASCII characters
- uses radix-64 algorithm
 - maps 3 bytes to 4 printable chars

DANE and DMARC

- DNS-based Authentication of Named Entities (DANE)
 - DANE, or [RFC6698](#), is intended to mitigate the threat of a man-in-the-middle intercepting encrypted communications by posing as one of the end points.
 - DANE is built on DNSSEC
- DMARC, or [RFC7489](#), is intended to mitigate the threat of an arbitrary sender
- DMARC, which stands for “Domain-based Message Authentication, Reporting & Conformance”
 - an [email authentication](#), policy, and reporting protocol.
 - It builds on the widely deployed [SPF](#) and [DKIM](#) protocols
 - adding linkage to the author (“From:”) domain name
 - published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email.

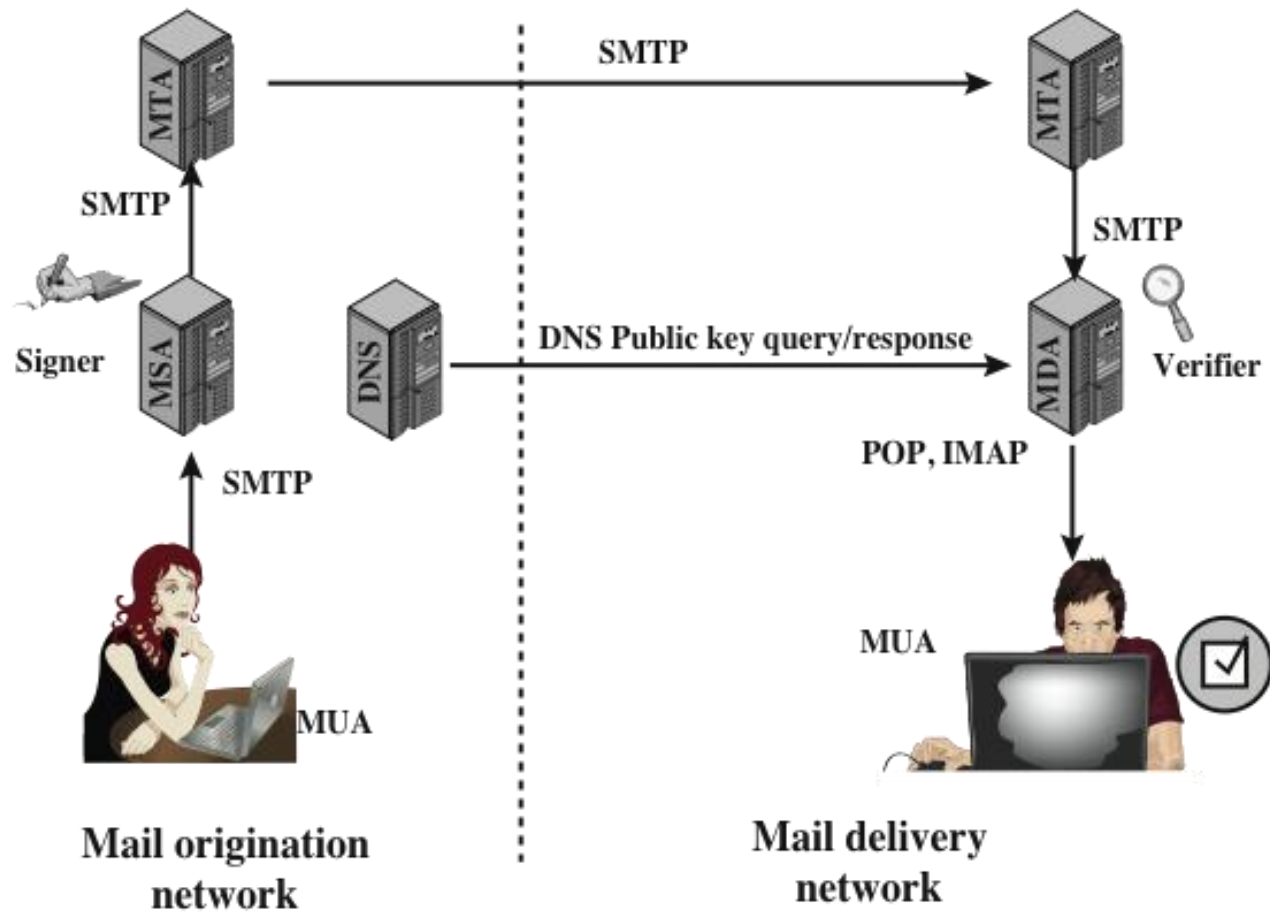
DANE and DMARC



Courtesy: <https://www.agari.com/email-security-blog/dane-vs-dmarc-the-email-authentication-landscape/>

DomainKeys Identified Mail (DKIM)

- Started as an industrial effort but later defined in RFC 6376
 - Adopted widely by a range of e-mail providers and Internet Service Providers (ISPs)
- Basically, signing the emails.
 - But not by the sender; but by the sending mail server
 - Similarly, the verifier is not the recipient user, but the receiving mail server.
 - So not end-to-end, but between sending MTA and receiving MTA (or agents on behalf of the MTAs)
- By signing an email,
 - The sending domain (via its MTA or its agent) claim responsibility for the email – it says “my server is sending it”
 - Thwarts server-spoofing attacks cryptographically
 - But it does not provide any proof about the individual who wrote the email
- Public-private key pairs belong to the domains
 - Public keys are stored as DNS records
- Receiving domain (via its MTA or its agent) verifies the signature before passing the email to the ultimate recipient.
 - Public key of the sender is obtained via a DNS query



DNS = domain name system
 MDA = mail delivery agent
 MSA = mail submission agent
 MTA = message transfer agent
 MUA = message user agent

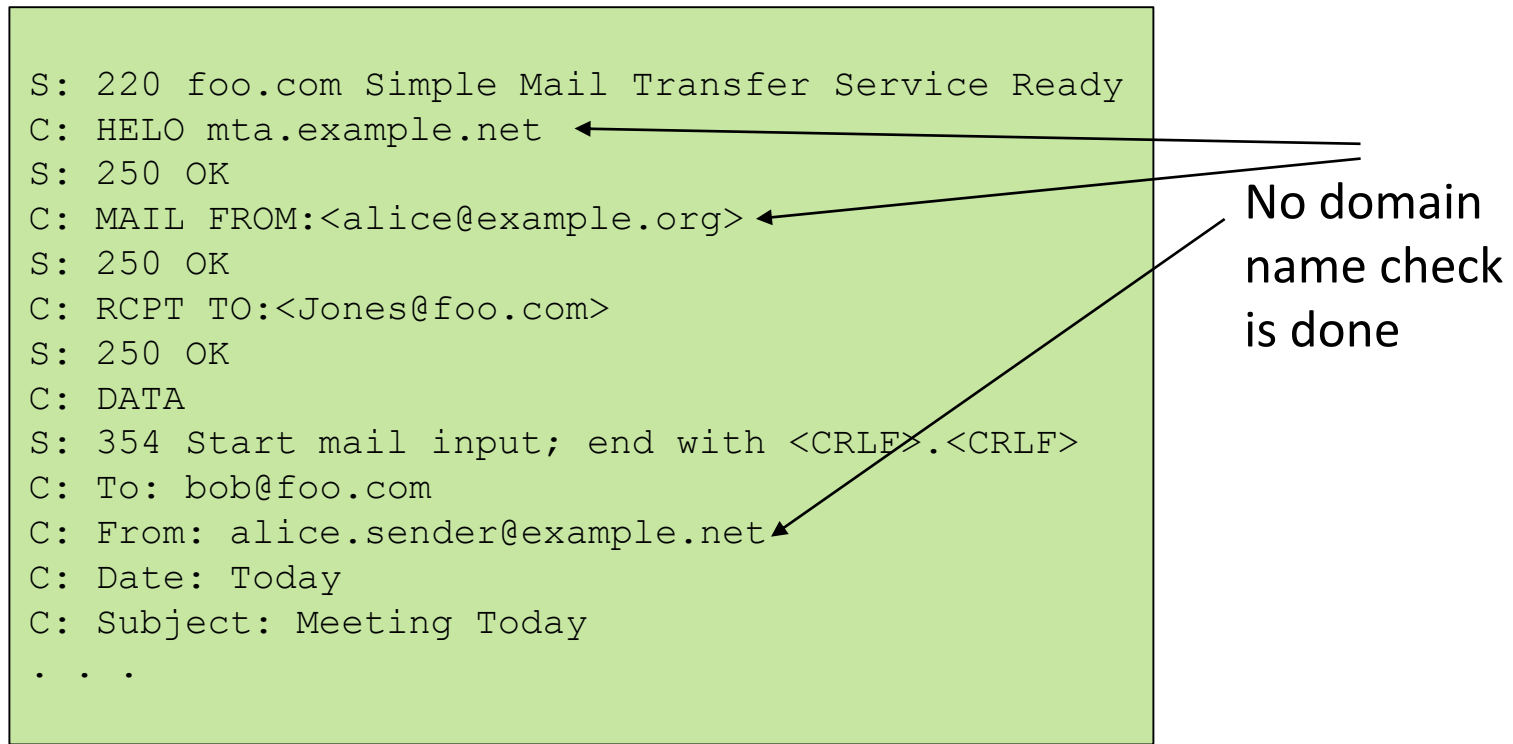
Figure 19.10 Simple Example of DKIM Deployment

Sender Policy Framework (SPF)

- Current email infrastructure allows to use any domain name while sending during SMTP messaging and in the email header.
 - This is the problem that SPF addresses

```
S: 220 foo.com Simple Mail Transfer Service Ready
C: HELO mta.example.net
S: 250 OK
C: MAIL FROM:<alice@example.org>
S: 250 OK
C: RCPT TO:<Jones@foo.com>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLE>.<CRLF>
C: To: bob@foo.com
C: From: alice.sender@example.net
C: Date: Today
C: Subject: Meeting Today
. . .
```

No domain name check is done



Sender Policy Framework (SPF)

- SPF is the standardized way for a sending domain to identify and assert the mail senders for that domain
- SPF works by checking a sender's IP address against the policy encoded in any SPF record found at the sending domain DNS records
 - This means that SPF checks can be applied before the message content is received from the
- SPF policies are stored in TXT type DNS resource records (SPF TXT RR)

Sender Policy Framework (SPF)

- SPF on the Sender Side
 - Basically formation of the policy and adding it to DNS of the sender's domain
 - Sending domain identifies all the allowed senders
 - Creates a policy using SPF syntax and adds to DNS
- SPF on the Receiver Side
 - Receiver first gets the IP address of the sender (TCP connection)
 - Locates SPF policies for the domains
 - If the IP address is allowed for the domains as senders than SMTP continues with mail content transfer
 - Otherwise, stops

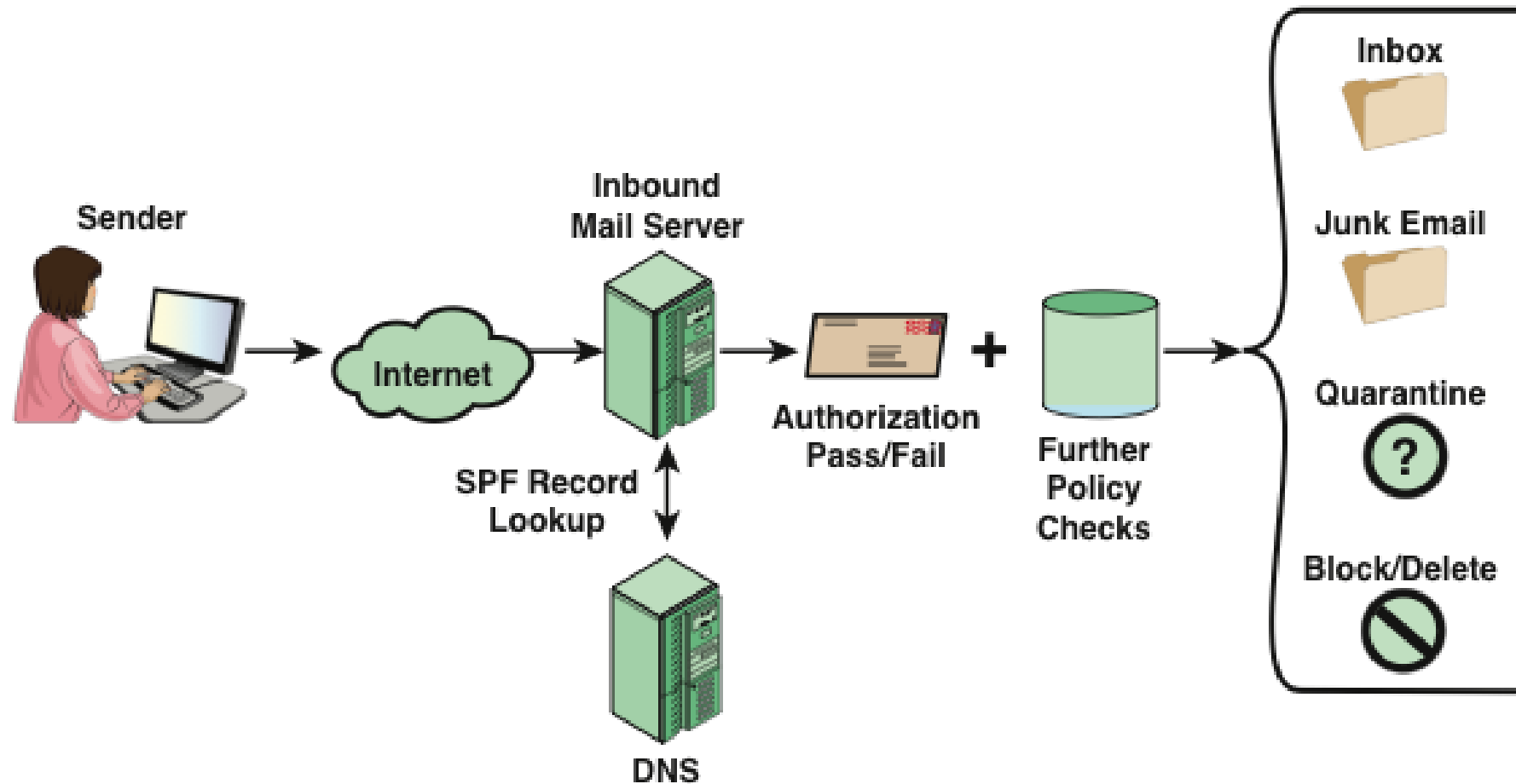


Figure 19.9 Sender Policy Framework Operation

Thank You!