Network & Cyber Security
Topic : Email Security

Dr. Leela GH

Dept.of E & CE,
BIET,
Davangere

May 10, 2020

- S/MIME Messages
- S/MIME Certificate Processing
- DomainKeys Identified Mail
- References

Note

Refer to this book for more information and for the articles which are not included in slides

S/MIME Messages

S/MIME makes use of a number of new MIME content types,

- Enveloped Data
- Signed Data
- Clear Signing
- Registration Request
- Certificates Only Message

Registration Request

- Typically, an application or user will apply to a certification authority for a public-key certificate.
- The application/pkcs10 S/MIME entity is used to transfer a certification request.
- The certification request includes:
  - certification **RequestInfo** block
  - an identifier of the public-key encryption algorithm
  - signature of the certification **RequestInfo** block made using the senders private key
  - The **certification RequestInfo** block includes:
    - a name of the certificate subject (the entity whose public key is to be certified)
    - includes and a bit-string representation of the users public key.

Certificates-only message

1. A message containing only certificates or a certificate revocation list (CRL) can be sent in response to a registration request.
2. The message is an application/pkcs7-mime type/subtype with an smime-type parameter of degenerate.
3. The steps involved are the same as those for creating a signedData message, except that there is no message content and the signerInfo field is empty.

S/MIME Certificate Processing

S/MIME uses public-key certificates that conform to version 3 of X.509. The key-management scheme used by S/MIME is in some ways a hybrid between a strict X.509 certification hierarchy and PGPs web of trust. As with the PGP model, S/MIME managers and/or users must configure each client with a list of trusted keys and with certificate revocation lists. That is, the responsibility is local for maintaining the certificates needed to verify incoming signatures and to encrypt outgoing messages. On the other hand, the certificates are signed by certification authorities.

User Agent Role

An S/MIME user has several key-management functions to perform.

- Key Generation
- Registration
- Certificate Storage & Retrieval

VERISIGN Certificates

There are several companies that provide certification authority (CA) services. For example, Nortel has designed an enterprise CA solution and can provide S/MIME support within an organization.
Some of the Internet Based CAs include:

- VeriSign
- GTE
- U.S. Postal Service

VERISIGN Certificates

The information contained in a Digital ID depends on the type of Digital ID and its use. At a minimum, each Digital ID contains :

- Owners public key
- Owners name or alias
- Expiration date of the Digital ID
- Serial number of the Digital ID
- Name of the certification authority that issued the Digital ID
- Digital signature of the certification authority that issued the Digital ID

Digital IDs can also contain other user-supplied information, including

- Address
- E-mail address
- Basic registration information (country, zip code, age, and gender)

VeriSign provides three levels, or classes, of security for public-key certificates :

- For Class 1 Digital IDs, VeriSign confirms the users e-mail address by send- ing a PIN and Digital ID pick-up information to the e-mail address provided in the application.
- For Class 2 Digital IDs, VeriSign verifies the information in the application through an automated comparison with a consumer database in addition to performing all of the checking associated with a Class 1 Digital ID. Finally, confirmation is sent to the specified postal address alerting the user that a Digital ID has been issued in his or her name.
- For Class 3 Digital IDs, VeriSign requires a higher level of identity assurance. An individual must prove his or her identity by providing notarized credentials or applying in person.

Enhanced Security Services

Three enhanced security services have been proposed in an Internet draft. The details of these may change, and additional services may be added. The three services are:

- Signed Receipts
- Security Labels
- Secure Mailing Lists

Signed receipts:A signed receipt may be requested in a SignedData object. Returning a signed receipt provides proof of delivery to the originator of a message and allows the originator to demonstrate to a third party that the recipient received the message. In essence, the recipient signs the entire original message plus the original (senders) signature and appends the new signature to form a new S/MIME message.

Enhanced Security Services

Security labels: A security label may be included in the authenticated attributes of a SignedData object. A security label is a set of security information regarding the sensitivity of the content that is protected by S/MIME encapsulation. The labels may be used for access control, by indicating which users are permitted access to an object. Other uses include priority (secret, confidential, restricted, and so on) or role based, describing which kind of people can see the information (e.g., patients health-care team, medical billing agents, etc.).

Enhanced Security Services

Secure mailing lists : When a user sends a message to multiple recipients, a certain amount of per-recipient processing is required, including the use of each recipients public key. The user can be relieved of this work by employing the services of an S/MIME Mail List Agent (MLA). An MLA can take a single incoming message, perform the recipient-specific encryption for each recipient, and forward the message. The originator of a message need only send the message to the MLA with encryption performed using the MLAs public key.

DomainKeys Identified Mail

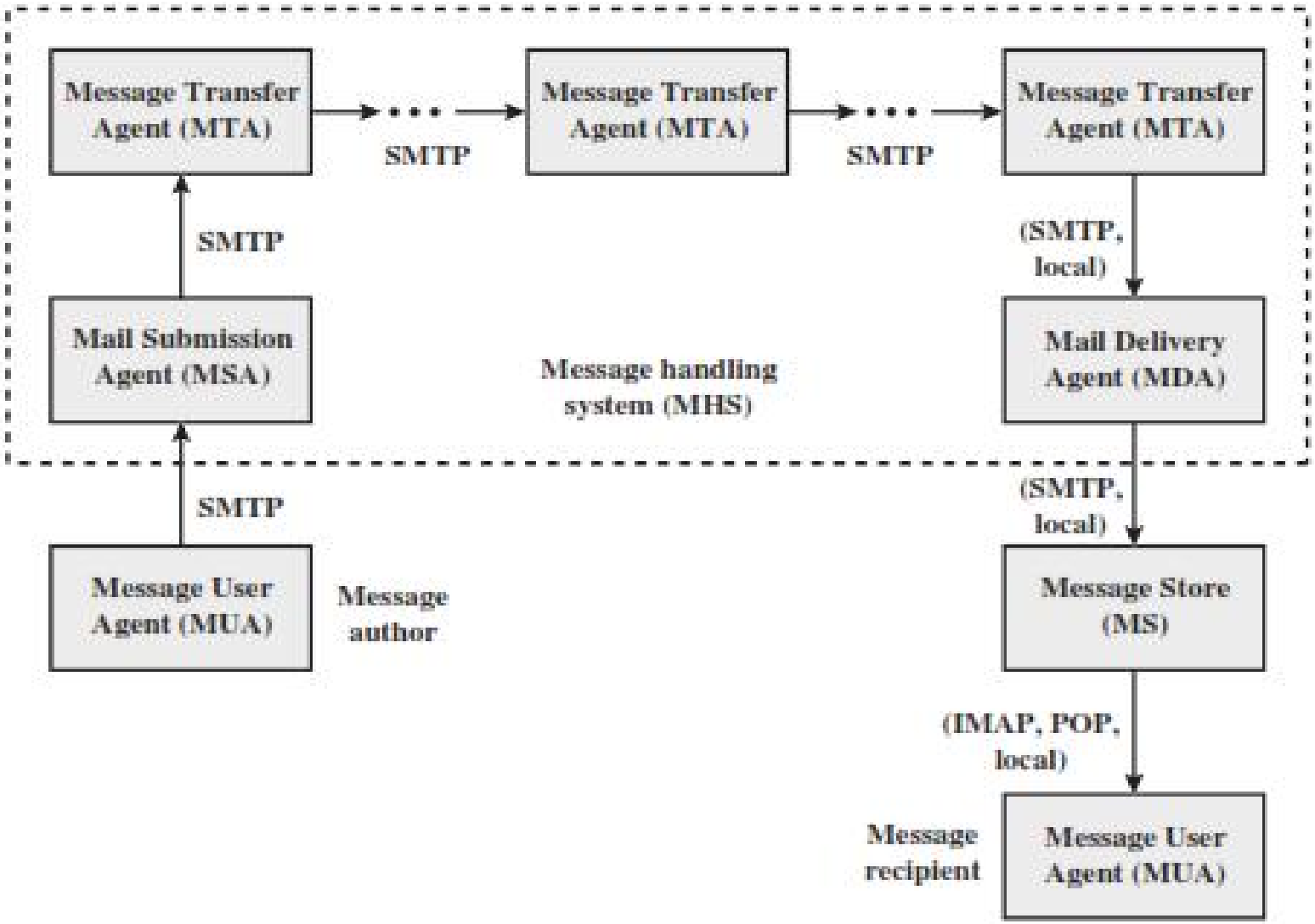
DomainKeys Identified Mail (DKIM) is a specification for cryptographically signing e-mail messages, permitting a signing domain to claim responsibility for a message in the mail stream. Message recipients (or agents acting in their behalf) can verify the signature by querying the signers domain directly to retrieve the appropriate public key and thereby can confirm that the message was attested to by a party in possession of the private key for the signing domain. DKIM is a proposed Internet Standard (RFC 4871: DomainKeys Identified Mail (DKIM) Signatures). DKIM has been widely adopted by a range of e-mail providers, including corporations, government agencies, gmail, yahoo, and many Internet Service Providers (ISPs).

Internet Mail Architecture

At its most fundamental level, the Internet mail architecture consists of :

- a user world in the form of Message User Agents (MUA)
- the transfer world, in the form of the Message Handling Service (MHS), which is composed of Message Transfer Agents (MTA).

key components of the Internet mail architecture



key components of the Internet mail architecture

- **Message User Agent (MUA):** Operates on behalf of user actors and user applications. It is their representative within the e-mail service. Typically, this function is housed in the users computer and is referred to as a client e-mail program or a local network e-mail server. The author MUA formats a message and performs initial submission into the MHS via a MSA. The recipient MUA processes received mail for storage and/or display to the recipient user.
- **Mail Submission Agent (MSA):** Accepts the message submitted by an MUA and enforces the policies of the hosting domain and the requirements of Internet standards. This function may be located together with the MUA or as a separate functional model. In the latter case, the Simple Mail Transfer Protocol (SMTP) is used between the MUA and the MSA.

key components of the Internet mail architecture

- **Message Transfer Agent (MTA):** Relays mail for one application-level hop. It is like a packet switch or IP router in that its job is to make routing assessments and to move the message closer to the recipients. Relaying is performed by a sequence of MTAs until the message reaches a destination MDA. An MTA also adds trace information to the message header. SMTP is used between MTAs and between an MTA and an MSA or MDA.
- **Mail Delivery Agent (MDA):** Responsible for transferring the message from the MHS to the MS.
- **Message Store (MS):** An MUA can employ a long-term MS. An MS can be located on a remote server or on the same machine as the MUA. Typically, an MUA retrieves messages from a remote server using POP (Post Office Protocol) or IMAP (Internet Message Access Protocol).

E-mail Threats

RFC 4686 (Analysis of Threats Motivating DomainKeys Identified Mail) describes the threats being addressed by DKIM in terms of

- characteristics
- capabilities
- location of potential attackers.

RFC 4686 characterizes the range of attackers on a spectrum of three levels of threat.

- At the low end are attackers who simply want to send e-mail that a recipient does not want to receive. The attacker can use one of a number of commercially available tools that allow the sender to falsify the origin address of messages. This makes it difficult for the receiver to filter spam on the basis of originating address or domain.

E-mail Threats-Characteristics

- At the next level are professional senders of bulk spam mail. These attackers often operate as commercial enterprises and send messages on behalf of third parties. They employ more comprehensive tools for attack, including Mail Transfer Agents (MTAs) and registered domains and networks of compromised computers (zombies) to send messages and (in some cases) to harvest addresses to which to send.
- The most sophisticated and financially motivated senders of messages are those who stand to receive substantial financial benefit, such as from an e-mail-based fraud scheme. These attackers can be expected to employ all of the above mechanisms and additionally may attack the Internet infrastructure itself, including DNS cache-poisoning attacks and IP routing attacks.

E-mail Threats-Capabilities

RFC 4686 lists the following as capabilities that an attacker might have

- Submit messages to MTAs and Message Submission Agents (MSAs) at mul- tiple locations in the Internet
- Construct arbitrary Message Header fields, including those claiming to be mailing lists, resenders, and other mail agents.
- Sign messages on behalf of domains under their control.
- Generate substantial numbers of either unsigned or apparently signed mes- sages that might be used to attempt a denial-of-service attack.
- Resend messages that may have been previously signed by the domain.
- Transmit messages using any envelope information desired.
- Act as an authorized submitter for messages from a compromised computer.

E-mail Threats-Capabilities

- Manipulation of IP routing. This could be used to submit messages from spe- cific IP addresses or difficult-to-trace addresses, or to cause diversion of messages to a specific domain.
- Limited influence over portions of DNS using mechanisms such as cache poisoning. This might be used to influence message routing or to falsify advertisements of DNS-based keys or signing practices.
- Access to significant computing resources, for example, through the conscription of worm-infected zombie computers. This could allow the bad actor to perform various types of brute-force attacks.
- Ability to eavesdrop on existing traffic, perhaps from a wireless network.

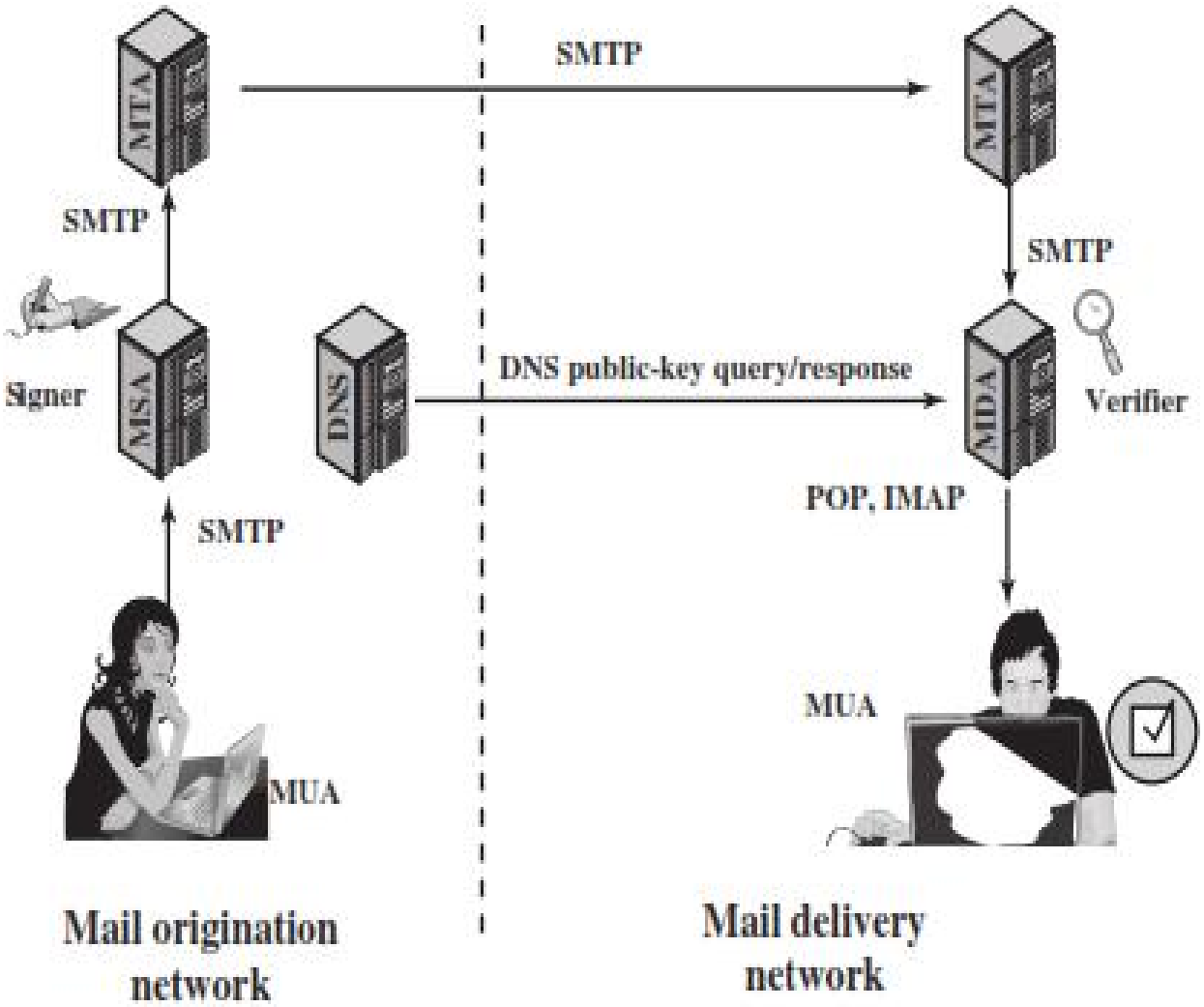
E-mail Threats-Location

DKIM focuses primarily on attackers located outside of the administrative units of the claimed originator and the recipient. These administrative units frequently correspond to the protected portions of the network adjacent to the originator and recipient. It is in this area that the trust relationships required for authenticated message submission do not exist and do not scale adequately to be practical. Conversely, within these administrative units, there are other mechanisms (such as authenticated message submission) that are easier to deploy and more likely to be used than DKIM. External bad actors are usually attempting to exploit the any-to-any nature of e-mail that motivates most recipient MTAs to accept messages from anywhere for delivery to their local domain. They may generate messages without signatures, with incorrect signatures, or with correct signatures from domains with little traceability. They may also pose as mailing lists, greeting cards, or other agents that legitimately send or resend messages on behalf of others.

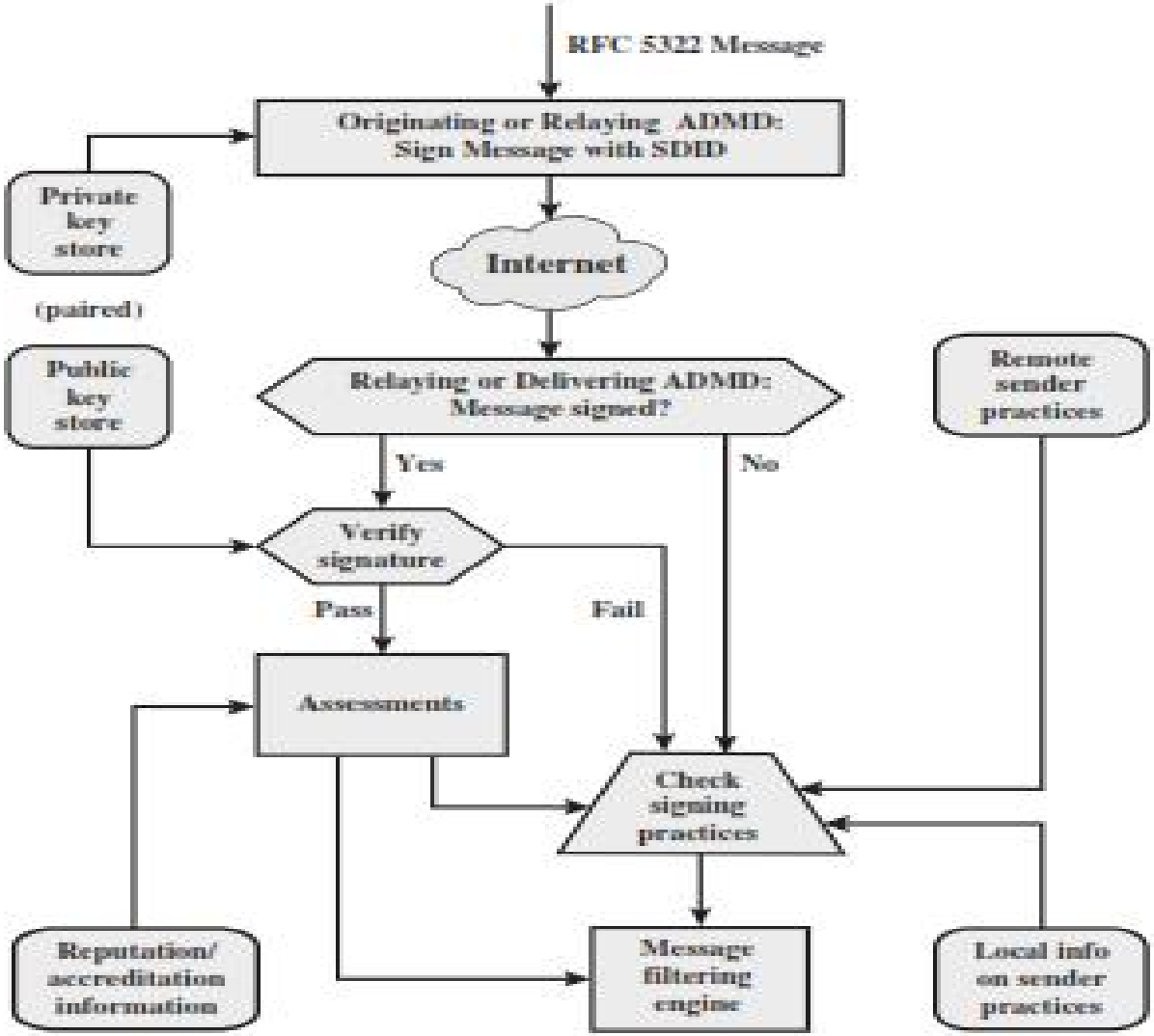
DKIM Strategy

DKIM is designed to provide an e-mail authentication technique that is transparent to the end user. In essence, a users e-mail message is signed by a private key of the administrative domain from which the e-mail originates. The signature covers all of the content of the message and some of the RFC 5322 message headers. At the re- ceiving end, the MDA can access the corresponding public key via a DNS and verify the signature, thus authenticating that the message comes from the claimed administrative domain. Thus, mail that originates from somewhere else but claims to come from a given domain will not pass the authentication test and can be rejected. This approach differs from that of S/MIME and PGP, which use the originators private key to sign the content of the message.

Simple Example of DKIM Deployment



DKIM Functional Flow



References

Refer to this book for more information and for the articles which are not included in slides


William Stallings, *Cryptography and Network Security Principles and Practice*, Pearson Education Inc., 6 Edition, 2014, ISBN: 978-93-3251877-3.