Lecture 20: Email Security

COSC362 Data and Network Security

Book 1: Chapter 19 – Book 2: Chapters 9 and 22

Spring Semester, 2021

Motivation

- Although TLS is the most widely used security protocol on the Internet, there are other important examples.
- Emails remain one of the most widely used forms of electronic communication, but are often sent without any security.

Outline

Email Security Requirements

Link Security
- DomainKeys Identified Mail (DKIM)
- STARTTLS

End-to-End Security
- PGP
- Secure/Multipurpose Internet Mail Extension (S/MIME)

Outline

Email Security Requirements

Link Security
- DomainKeys Identified Mail (DKIM)
- STARTTLS

End-to-End Security
- PGP
- Secure/Multipurpose Internet Mail Extension (S/MIME)

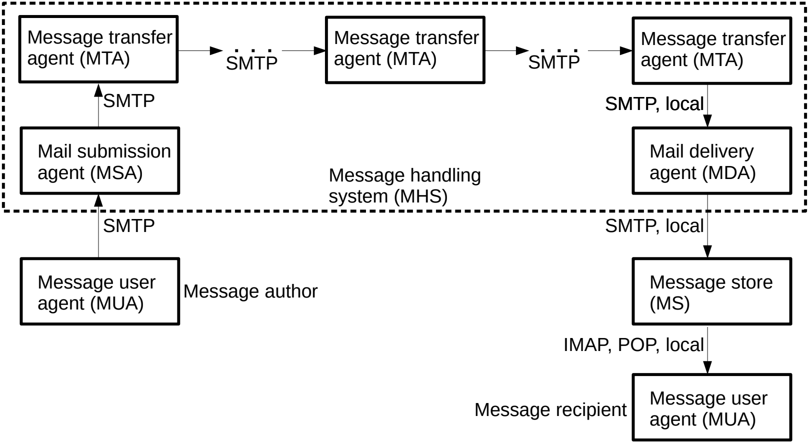
Protocols

- Single message transfer protocol (SMTP) is a mail transmission protocol to send an email from a source to a destination:
  - Standard: RFC 5321
- POP and IMAP are mail access protocols to allow a *message user agent* (MUA) to download an email from a *message transfer agent* (MTA).

Entities

- The *message user agent* (MUA) connects a client to a mail system:
  - Using SMTP to send a mail to a *message submission agent* (MSA).
  - Using POP or IMAP to retrieve the mail from the *message store* (MS).
- The *message handling system* (MHS) transfers a message from MSA to MS via one or more *message transfer agents* (MTAs).

Architecture


Message transfer agent (MTA)
. . .
SMTP
Message transfer agent (MTA)
. . .
SMTP
Message transfer agent (MTA)
SMTP
SMTP, local
Mail submission agent (MSA)
Message handling system (MHS)
Mail delivery agent (MDA)
SMTP
SMTP, local
Message user agent (MUA)
Message author
Message store (MS)
IMAP, POP, local
Message recipient
Message user agent (MUA)

Security Threats

- Considering threats in the usual CIA categories:
  - Email content may require confidentiality and/or authentication.
  - Email service availability may be threatened.
- Metadata in the header is a significant source of information for an attacker.

Spam

- Unsolicited bulk email (UBE).
- A cheap form of advertising?
- Common vector for phishing attacks.
- Countermeasures typically use email filtering.
- Proposals to implement *proof of work*:
    - The email sender must solve a moderately hard puzzle in order to have the mail accepted into MHS.
    - Example: Hashcash.

Link Security and End-to-End Security

- Security may be provided between different agents in the mail system on a *link-by-link* basis, using protocols such as STARTTLS and DKIM.
- Alternatively, security may be provided from client to client (*end-to-end*), using protocols such as PGP and S/MIME.
- Both have their pros and cons.
- Ideally, both are used.

Outline

Email Security Requirements

Link Security
- DomainKeys Identified Mail (DKIM)
- STARTTLS

End-to-End Security
- PGP
- Secure/Multipurpose Internet Mail Extension (S/MIME)

Overview

- Standard: RFC 6376 (2011).
- Allowing the *sending mail domain* to sign an outgoing mail using RSA signatures.
- The *receiving domain* can verify the origin of mail.
- Widely used by prominent email providers, including Gmail.
- Helping to prevent email spoofing, and so to reduce spams and phishing.
- Public key of the sending domain retrieved using a domain name system (DNS).

Example

2048-bit RSA signature on a message, coded in base 64:

```
v=1;  // Version
a=rsa-sha256;  // Algorithm
c=relaxed/relaxed; // Header/body canonicalization (format)
d=gmail.com;  // Domain claiming origin
s=20120113;      // Selector subdividing namespace
h=mime-version:date:message-id:subject:from:to;
// Signed header fields
bh=NJjTF6QE7tvCE3fjCqEDurIGtvA2alydEz7wt4mn4EA=;
// Hash of the body part
b=h7aimB9ROItSF8RWWmd5MmJBQBR3gUo+w5L41UsMBSoDCjdqxmZQKyAhv
F7CxE5+PzFLwQceVCYk3CzYuexyXkRNwuVw7A8lNeJdDxA4blSbFy8MuY5v
c+b2MPYQcP9v2iTli0m5N2AejzwSLyGvGUCtNSC7xQWHm0fTDC2LRY9b/xT
QzO6/608LSE59HW1gIf+AkWQae/ew41fyamu1QBoGFkgWy6ZMeOF+tzKtSy
RSc4FIcU1kcDuHkvQPjmw3hQN0gz+x4zfkb2wD9kyliWjw1tH3MM5FTwKzm
tAT/gDCtpCI7/HW6jeyx6HcevCjeFK+bkMy0nVa6oQc69o0MA==
// Signature
```

Overview

- Extending mail protocols SMTP, POP and IMAP to run over TLS connections.
- Providing link-by-link security, *but not* end-to-end security.
- *Opportunistic* use of TLS encryption security:
  - Using it if possible.
- Standards:
  - RFC 2595 for IMAP and POP3.
  - RFC 3207 for SMTP.
- Widely used by prominent email providers, including Gmail and Microsoft Outlook.
- Vulnerable to STRIPTLS attacks:
  - An attacker interrupts TLS negotiation, and connection falls back to plaintext transmission.

DKIM and STARTTLS Uptake

- Recent survey: Noticeable increase in uptake of DKIM and STARTTLS:
  - Biblio: Z. Durumeric et al., *Neither Snow nor Rain nor MITM... An Empirical Analysis of Email Delivery Security*, 2015.
- Gmail able to use STARTTLS for around 90% of both outgoing and incoming mails (Oct. 2021):
  - `https://transparencyreport.google.com/safer-email/overview`
- Gmail authentication using DKIM covered around 80% of incoming mails (2015).

Outline

Email Security Requirements

Link Security
- DomainKeys Identified Mail (DKIM)
- STARTTLS

End-to-End Security
- PGP
- Secure/Multipurpose Internet Mail Extension (S/MIME)

History

- Originally the product of one person, Phil Zimmermann.
- Subject to widely reported export restriction controversy.
- OpenPGP standard (RFC 4880) allows for interoperable implementations.
- GnuPG (GPG) is an open implementation.
- PGP corporation acquired by Symantec (2010).

Email Processing

- Protecting the mail message contents.
- Hybrid encryption:
  - A new random “session key” is generated for each message.
  - The session key is encrypted with the long-term public key of the recipient.
- Signing with either RSA or DSA.
- Compressing with Zip.
- Coding using radix-64 to ensure that binary strings can be sent in the mail body.

Encryption

- Session keys encrypted using asymmetric encryption:
  - OpenPGP requires the support of Elgamal encryption and recommends the support of RSA encryption.
- Message content encrypted using symmetric encryption:
  - OpenPGP requires the support of 3DES with 3 keys (168 bits in total) and recommends the support of AES-128 and CAST5 (other algorithms are also defined).
- Compression applied before encryption.
- Encryption can be applied independently of signing:
  - No requirement for authenticated encryption.

Signature

- Plaintext message is *optionally* signed with the sender's private key:
  - OpenPGP standard requires the support of RSA signatures and recommends the support of DSA signatures.
- RSA-signed messages are hashed with SHA1 (in the standard) or with SHA2 hash functions.

Web of Trust

- Users generate their own public/private key pairs.
- Public keys available on distributed key servers.
- Any PGP user can sign another user's public key, indicating their level of trust.
- Users can revoke their own key by signing a revocation certificate with the revoked key:
  - Users can also decide on the key expiration date when generating it.

Usability and Security

- Can we expect the average user to understand public key cryptography?
- Is it possible to design an interface that helps users to operate PGP correctly and safely?
  - `https://www.whitehatsec.com/blog/pgp-still-hard-to-use-after-16-years/`
  - A. Witten and J. D. Tygar, *Why Johnny can't encrypt: A Usability Evaluation of PGP 5.0*, Usenix Security Symposium, 1999
- Follow-up studies show that newer PGP versions are still hard to use.
- Vulnerability: EFail (2018).
  - Using a piece of HTML code to trick email users to reveal encrypted messages.

PGP Uptake

- Plugins available for many popular mail clients and for webmail interfaces:
  - Example: Mailvelope, a browser extension that enables the exchange of encrypted emails following the OpenPGP encryption standard.
- Around 100 keys added per day on SKS keyserver pool:
  - `https://sks-keyservers.net/status/key_development.php`
  - DNS records no longer maintained (due to GDPR).
- Growth rate remains linear over past several years.
- Around 60 000 keys in the *strong set* of keys with a trust path between any pair of keys.

OpenPGP Criticisms

- Outdated cryptographic algorithms still used:
    - SHA1, CAST5, etc.
- No support of SHA3 and authenticated encryption (e.g. GCM).
- Lots of metadata available to an eavesdropper:
    - File length
    - Used encryption algorithms
    - Recipient key identity

Overview

- Similar features to PGP:
    - Authentication, integrity, non-repudiation (signature) and confidentiality (encryption) of the message body carried in SMTP messages.
- Different, not interoperable message format.
- Sender's public key included with each message:
    - Used to verify the message.
- X.509 certificates issued by CAs instead of Web of Trust:
    - NIST recommends S/MIME rather than PGP because of greater confidence in CA system.
- Supported by most popular mail clients.

Authentication

1. The sender S creates a message m.
2. S generates a message digest $h(m)$ using SHA-256.
3. S signs $h(m)$ with her RSA private key, resulting into a signature s.
4. S appends s and m together and forwards them to the receiver R.
5. R verifies s (and gets $h(m)$) with the RSA public key of S.
6. R calculates a new digest for m and checks if it matches $h(m)$:
   - If there is a match then m accepted as authentic.

Guarantees

- RSA guarantee:
  - *R* assured that only the owner of the private key can generate *s*.
- SHA-256 guarantee:
  - *R* assured that no one else could generate a new digest that matches that $h(m)$, and a signature of *m*.

Confidentiality

1. The sender *S* creates a message *m* and a random 128-bit *content-encryption key k* for *m* only.
2. *S* encrypts *m* using *k* and AES-128 with CBC mode.
3. *S* encrypts *k* using RSA public key of the receiver *R*.
4. *S* sends both encrypted *m* and *k* to *R*.
5. *R* decrypts the encrypted *k* using her RSA private key.
6. *R* decrypts the encrypted *m* using *k*.

Guarantees

- Combining symmetric cryptography and public key cryptography allows to reduce encryption time.
- Public key encryption:
  - No session (content-encryption) key distribution needed.
  - Only *R* can recover *k*.
- One-time mechanism:
  - Symmetric encryption approach is strengthened.