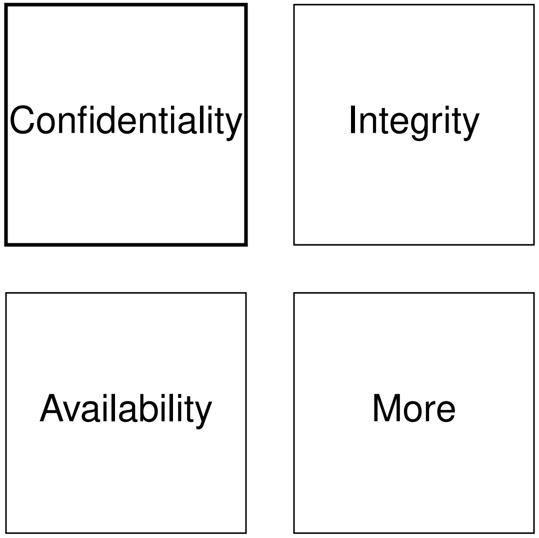
Email Security

DJ Chase

It doesn’t exist.

- Created in early 1960s
- Networked version of system service
  - Designed throughout 1970s & early 1980s
- All attempts to fix it are tacked on
- CIA Triad & more

Confidentiality problem



Confidentiality

Integrity

Availability

More

Encryption

- Plain-text from end to end
  - No client–server TLS by default
  - No server–server TLS by default
  - Messages themselves stored unencrypted
- Store and forward

Server-side solutions

- Require client–server TLS
- Require server—server TLS
  - Prevents users from sending to some domains
- Communicate directly with receiving server
- Require encrypted messages
  - Only works with handful of servers
- Password-based asymmetric encryption at rest
- In corporate environment, require employees to use webmail or IMAP

Client-side solutions

- Use TLS if available
- Encrypt messages with PGP/GPG (Pretty Good Privacy / GNU Privacy Guard)
  - Must have each others public keys
  - Can’t use webmail
- Encrypt messages with S/MIME (Secure MIME)
  - TLS-based — hard/expensive to get certificate
  - Nobody does this
- In personal environment, use POP3 instead of webmail IMAP

Integrity problems

Confidentiality	Integrity
Availability	More

Sender integrity

- No verification by default
- From:
- Return-To:
- Sender: (anti-spam)

Server-side solutions

- SPF (Sender Policy Framework)
  - DNS-based
  - Restricts sender IP addresses
- DKIM (DomainKeys Identified Mail)
  - Header-based
  - Server certifies from address
- DMARC (Domain-based Message Authentication, Reporting, and Conformance)
  - DNS-based
  - Tells other servers how to handle SPF/DKIM errors

Not part of basic standard — negligent servers will happily deliver bad mail

Client-side solutions

- PGP/GPG (Pretty Good Privacy / GNU Privacy Guard)
  - Client-side
  - Key distribution
- S/MIME (Secure MIME)
  - Client-side
  - TLS certificates

Clients might be negligent, outdated, or may not care.

Message integrity

- Servers need to be able to modify headers
  - Includes From:, Subject:, and other user-facing headers
  - Headers are stored in-band (same file), so servers can also modify message body
- Store and forward
  - Trust in third parties
- No end-to-end content verification

Server-side solutions

- Communicate directly with receiving server
- DKIM (DomainKeys Identified Mail)
  - Can provide message-body checksum
  - Breaks mailing lists

Client-side solutions

None — clients inherently trust servers

Availability problems

Confidentiality	Integrity
Availability	More

Availability problems

- Sending server may send to an impostor if not using TLS
- E2EE emails become unavailable if recipient looses their private key
- Emails encrypted at rest become unavailable if recipient forgets their password
- If using POP3, the only copy of your emails are on your computer

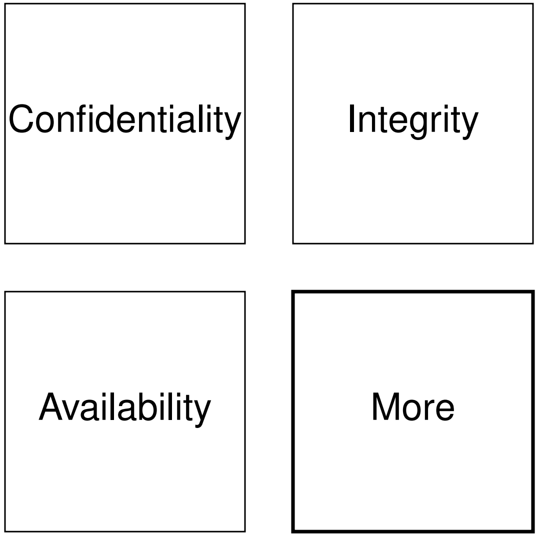
Server-side solutions

- Use TLS

Client-side solutions

- Backup your private key
- Backup your password
- Backup your emails

Other problems



Confidentiality

Integrity

Availability

More

Attachments

- Malware
- Double file extensions
- File icons
- Poorly-designed document formats
- …
- mailto: ?attach

Server-side solutions

- Prevent attachments
- Virus scanner

Client-side solutions

- Virus scanner
- Warn on suspicious files
- Restrict mailto: links to To:, Subject:, and body
- Common sense

HTML mail

- Hyperlinks
- Tracking pixels
- Web browser

Server-side solutions

- Reject HTML email

Client-side solutions

- Pop-up with actual link address
- Disable images
- Show plain-text alternative

Content

- Phishing
- Scams
- Images instead of text

Solutions

- Spam filtering
- Common sense

Email Security

All security enhancements are add-ons, and you can’t make all parties use them.

Sources

“History Of Email” In: *Wikipedia*; Wikipedia, The Free Encyclopedia; 2022-06-30;
https://en.wikipedia.org/wiki/History_of_email?oldid=1101352677