Mail Security

Jishun Zhang, Weiwen Ying, Xiaoyao Guan

Content

Found around the house!

- WHY EMAIL
- THREATS
- SOLUTION
- IMPLEMENTATION

WHY EMAIL ?

Widely used in communication in and among organizations

Sensitive information leak will cause property loss, especially for companies

Also a way to spread malware, spam and phishing attacks

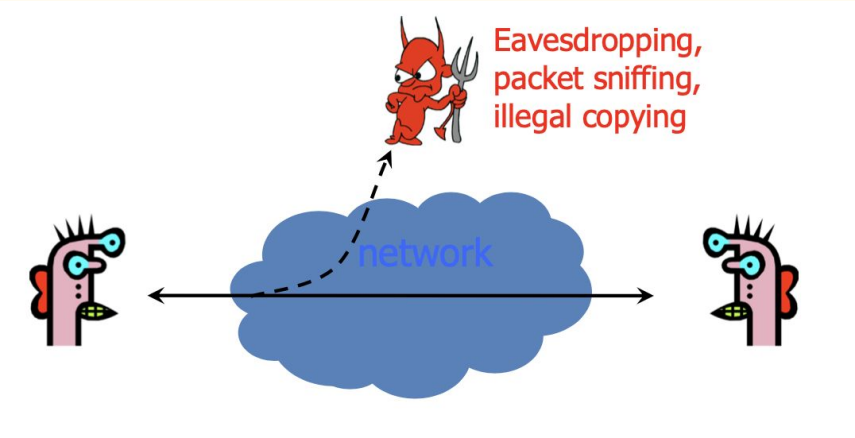
Email-based attacks affect the entire organization

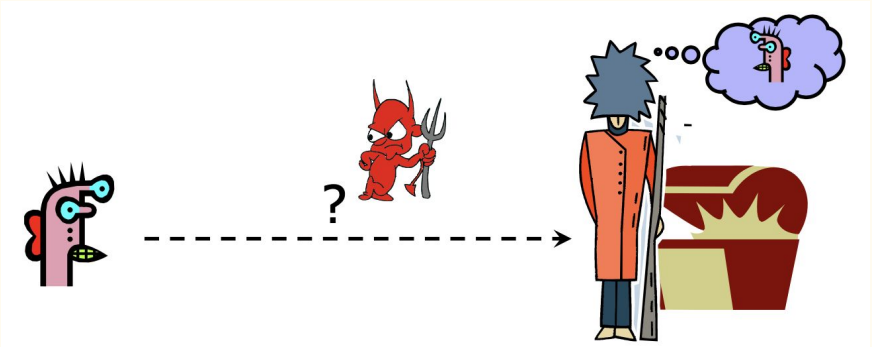
Basic anti-spam email filters are not enough

THREATS

Threats:

1. Phishing: Aiming at tricking the recipient into installing malware or into sharing personal or financial information.
2. Data modification: Modify content of email on its way
3. Spoofing: Pretending some valid person to receive or send email
4. Eavesdropping: Getting context of email





SOLUTION

Solution

Add HMAC for Integrity (SHA-512)

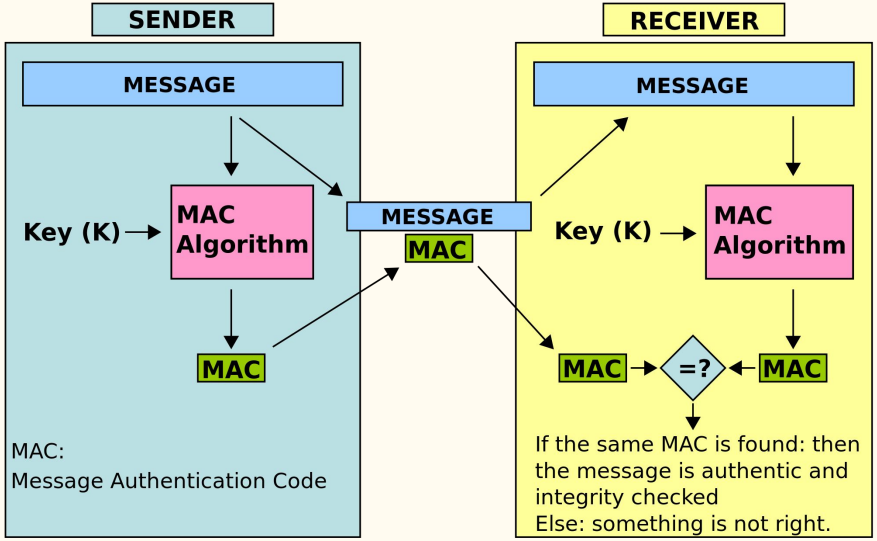
- against data modification

Use RSA for Confidentiality

- against eavesdropping

Add PKI for Authentication

- against spoofing



Solution

Add HMAC for Integrity (SHA-512)

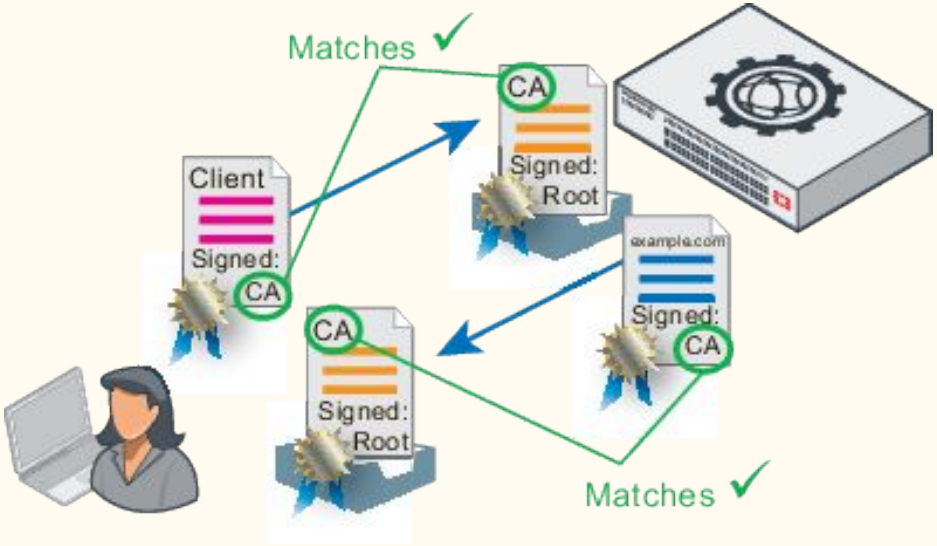
- against data modification

Use RSA for Confidentiality

- against eavesdropping

Add PKI for Authentication

- against cheating(?)



Solution

Intuition

HMAC for Integrity + RSA for Confidentiality + PKI for Authentication

In Reality

Use SSL encrypted tunnel to send and receive messages

Replace SMTP + IMAP with SMTP + IMAPS + SSL

IMPLEMENTATION

IMPLEMENTATION

SMTP to send email messages

IMAPS to receive email messages

All the messages are encrypted and decrypted by SSL, with RSA + SHA512

Thank you!