Protecting Data In Transit

Justin Boyer
PRINCIPAL CONSULTANT

@justinboyer4 www.justinboyerwriter.com

Threats to Data in Transit

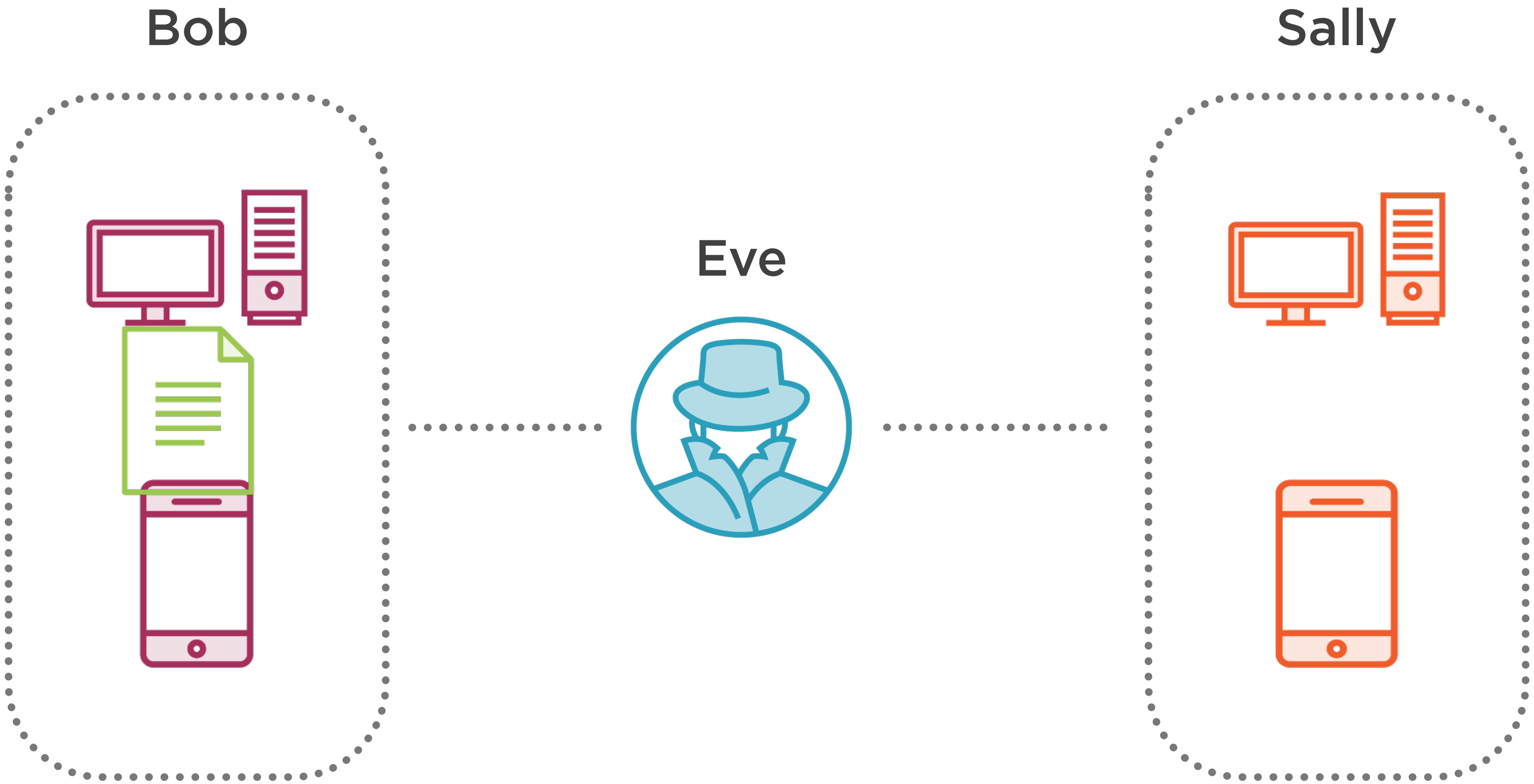
Someone Sees/Changes It

Attacker sees the data between two parties or changes it

Impersonation

Attacker impersonates you or another party

Man-in-the-middle Attack



Combating Threats to Data in Transit

Asymmetric Encryption

Encrypt with one key, decrypt with another

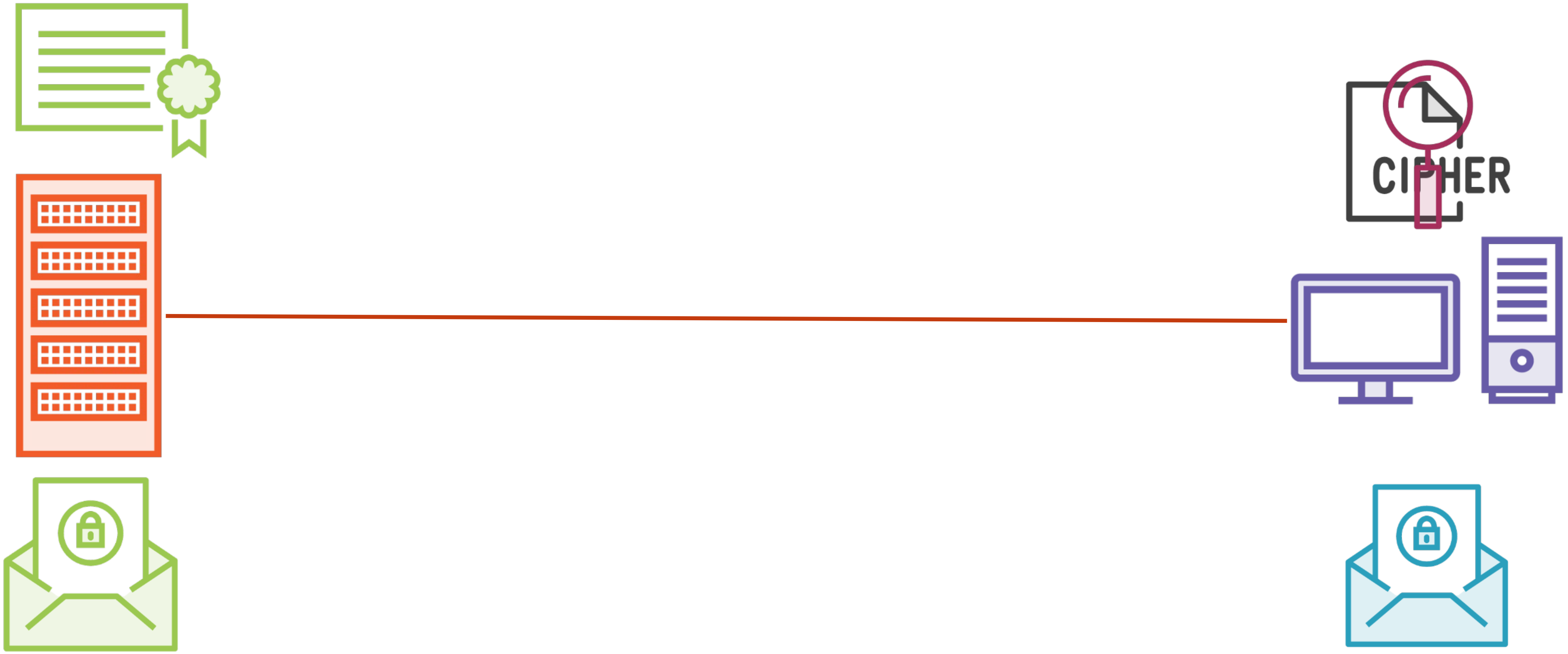
HMAC

Know if something's been changed

Digital Signatures

Verify authenticity and integrity

HTTPS in Action



Summary

Data in transit can be stolen or changed

Attackers may try to impersonate someone

Use asymmetric encryption, HMACs, and digital signatures

HTTPS is built on these technologies and is used to make the web safer