Secure Sockets

Part 1 – TLS Intro

Barak Gonen

Contents Part 1 – Intro

- History
- TLS protocol goals
  - Confidentiality
  - Integrity
  - Authentication
  - Anti-replay
  - Non-repudiation

Contents Part 2 – Cipher Suites

- Encryption
  - Symmetric
  - Asymmetric
- Hashing
- Authentication

Contents Part 3 – Certificates

- Certificates
  - Certification Authority – CA
  - Certificate Chain
  - Certificate Types
  - Certificate Revocation
    - Certificate Revocation List
    - OCSP
    - OCSP Stapling

Contents Part 4 – TLS Handshake

- Records
- RSA Handshake
- Diffie-Hellman Handshake
- Session Resumption
- Extensions
  - Server Name Indication
  - Session Tickets
  - OCSP Stapling
- TLS Decryption

Contents Part 5 – SSH

- Secure Shell goals
- SSH handshake
  - Explore using WSL + Wireshark

Part 1 – TLS Intro

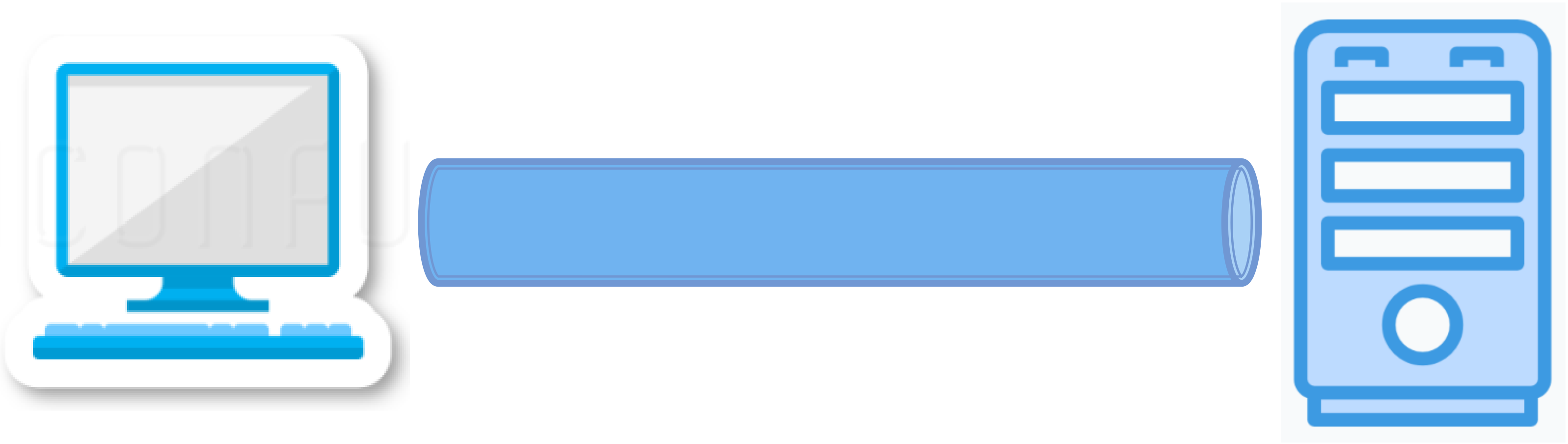
TLS History

Version	Year	Safety
SSL 1.0	1994	🟥
SSL 2.0	1995	🟥
SSL 3.0	1996	🟥
TLS 1.0	1999	🟨
TLS 1.1	2006	🟨
TLS 1.2	2008	🟩
TLS 1.3	2018	🟩

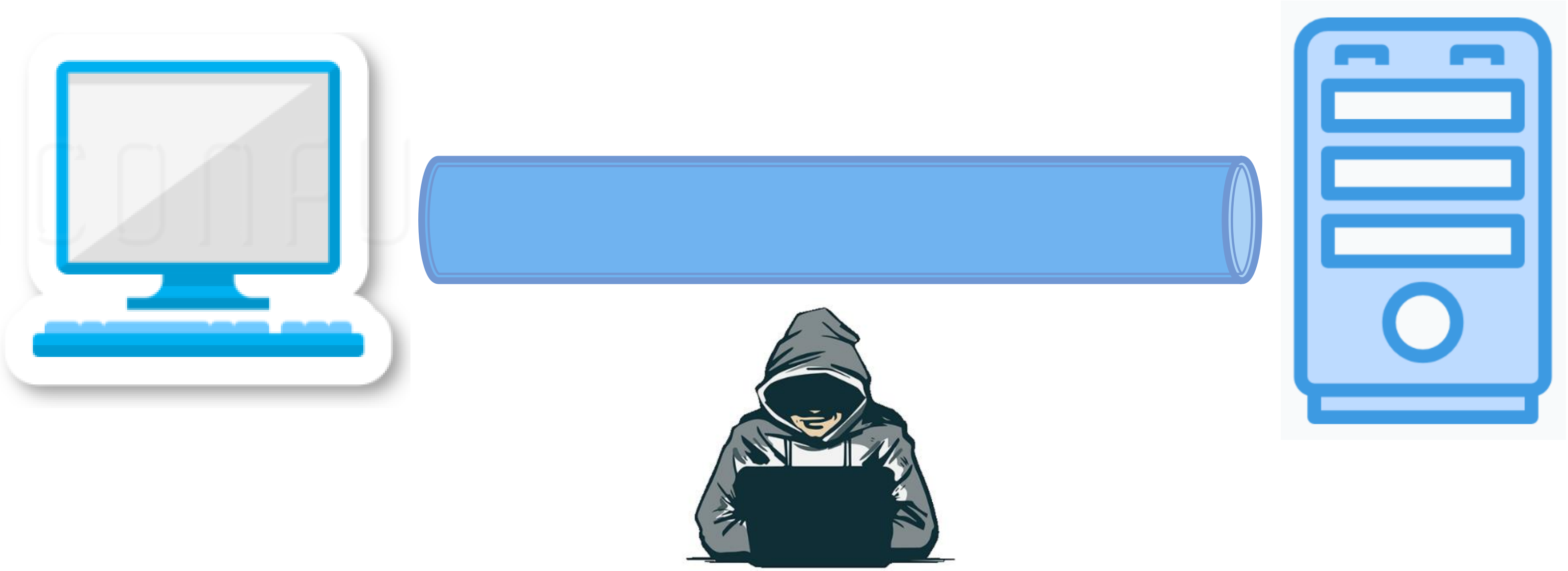
- SSL- Secure Socket Layer
- TLS – Transport Layer Security

TLS – Transport Layer Security

- Given an existing socket, makes it secure
- Not a layer
  - Think about is as a “4.5” layer

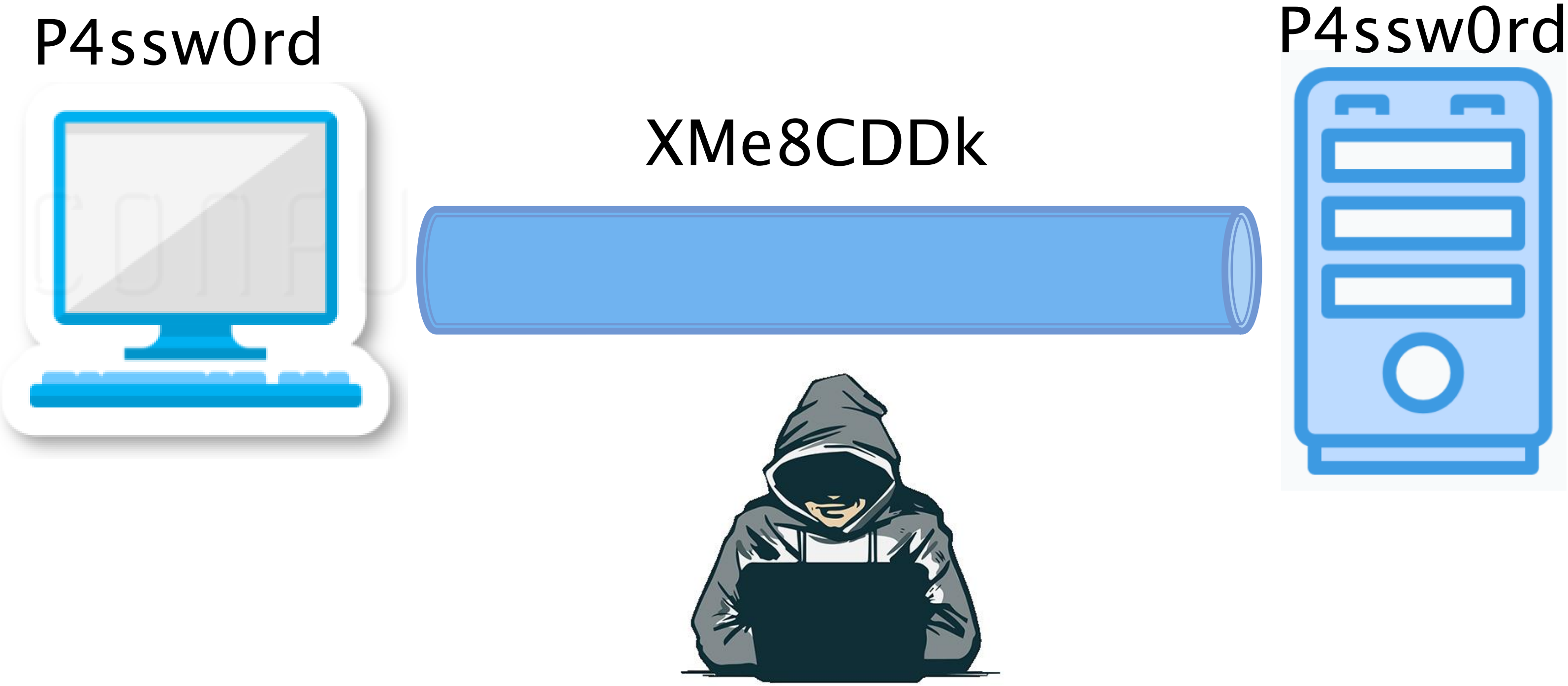


TLS Protocol Goals



- Base assumption – our packets might be eavesdropped and even changed
  - Confidentiality
  - Integrity
  - Authentication

TLS Protocol Goals



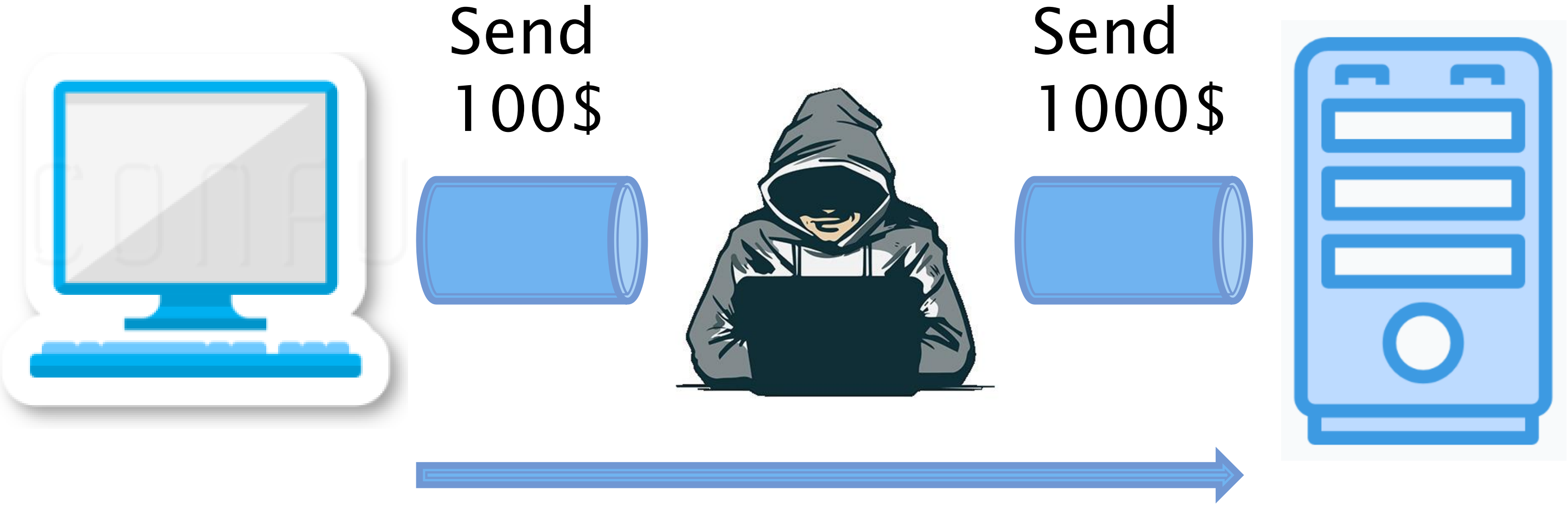
P4ssw0rd

XMe8CDDk

P4ssw0rd

- Confidentiality

TLS Protocol Goals

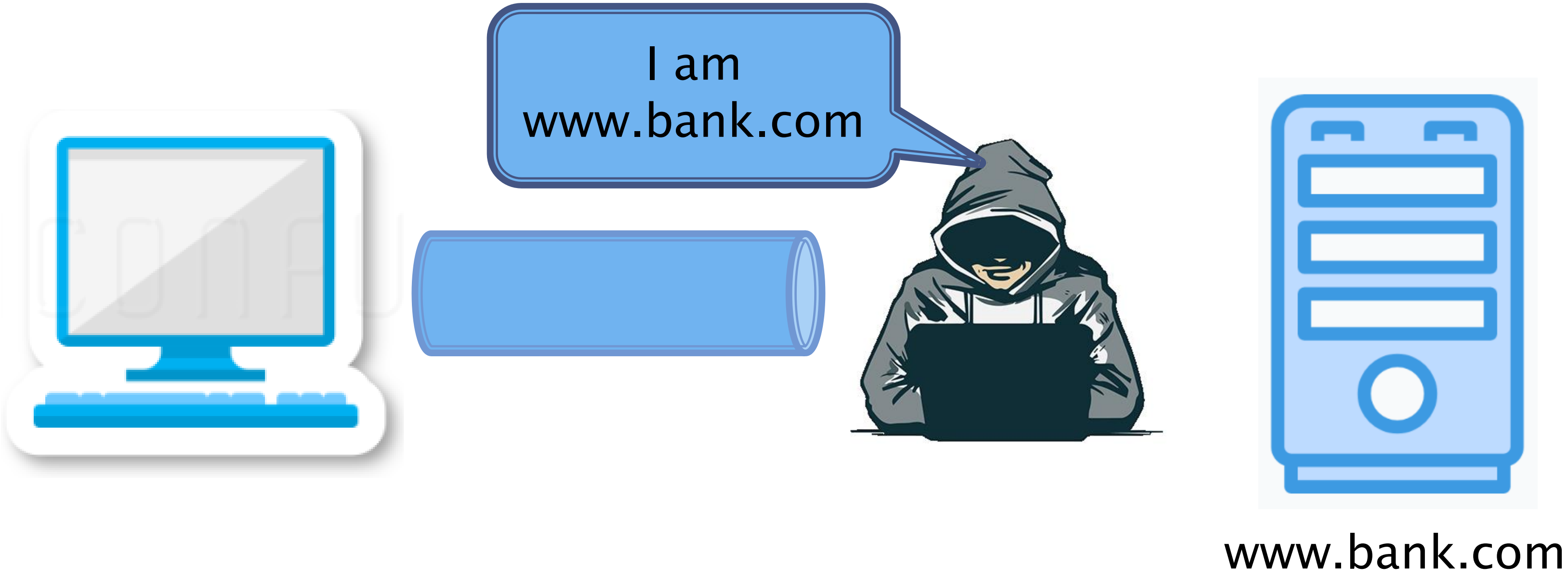


Send 100$

Send 1000$

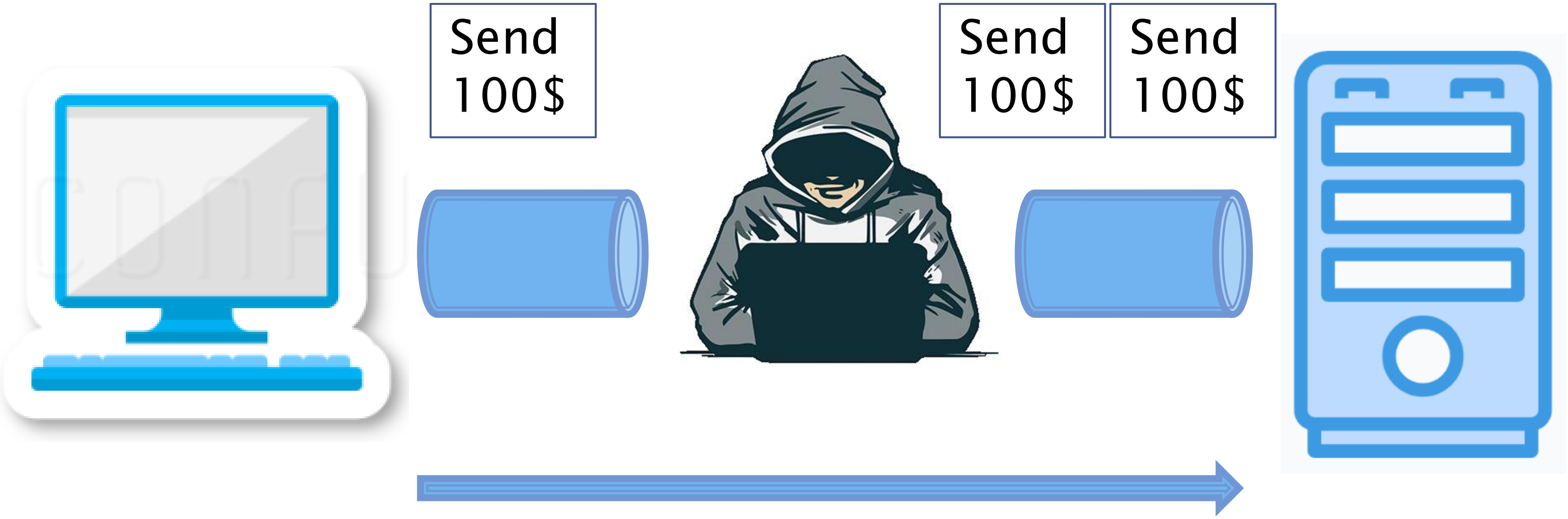
- Integrity

TLS Protocol Goals



- Authentication

Anti-replay



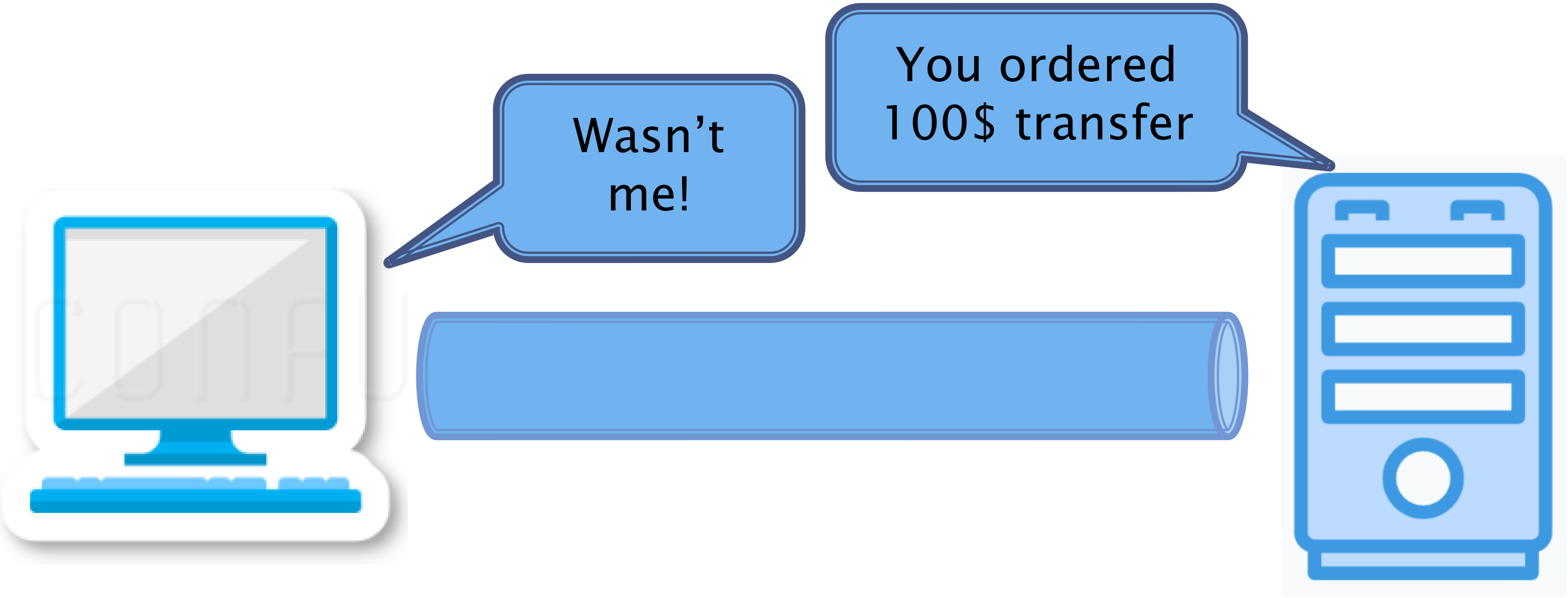
Send 100$

Send 100$

Send 100$

- Part of the encryption process

Non-repudiation



- We can not deny a message we sent
- Ensured by:
  - Authentication – no one can pretend to be us
  - Integrity – no one can change a message we sent

Summary

- Confidentiality
- Integrity
- Authentication
- Anti-replay
- Non-repudiation