SSL - Secure Socket Layer

Arnamoy Bhattacharyya

Tom (client)

Credit Card Details

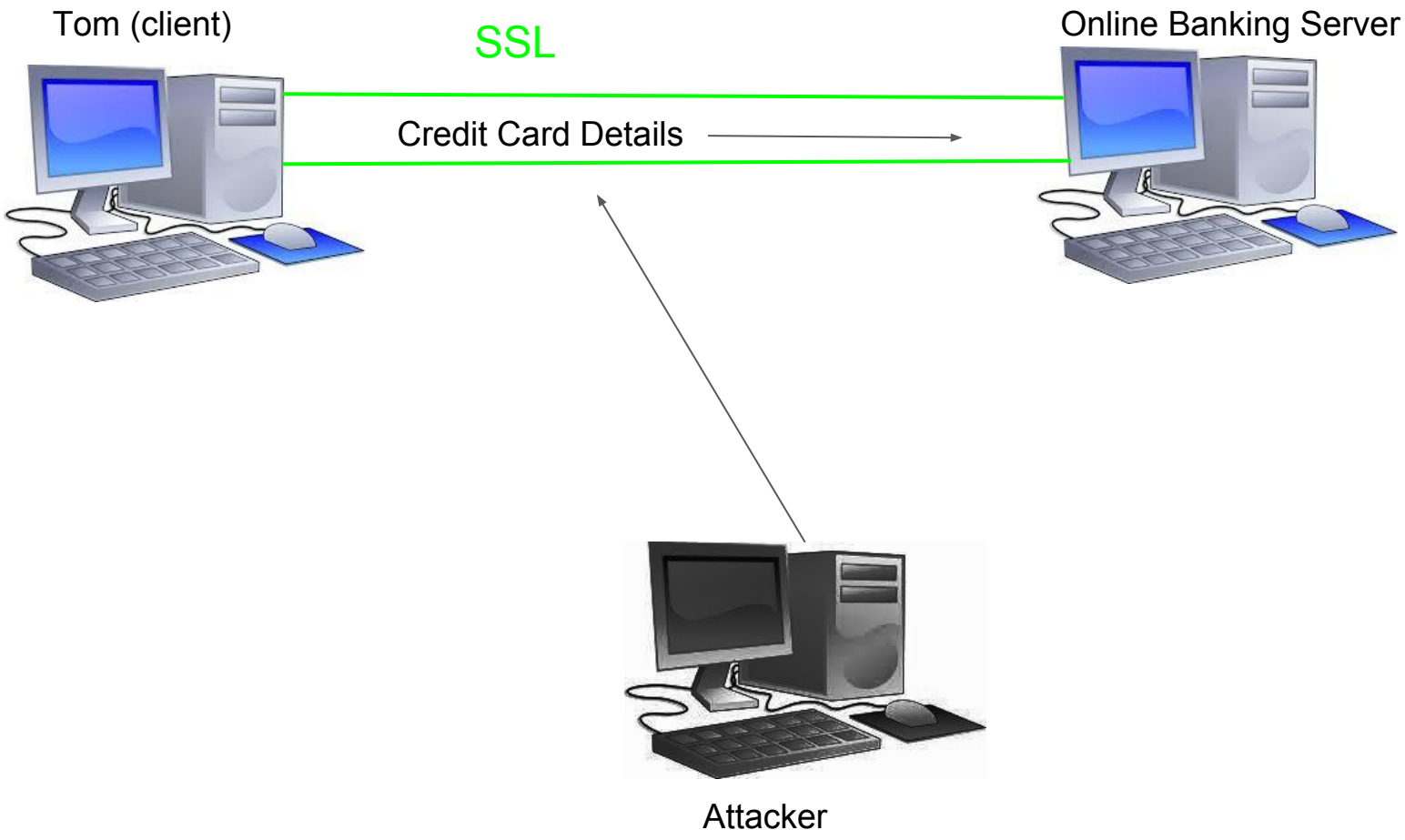
Online Banking Server

Tom (client)

Credit Card Details

Online Banking Server

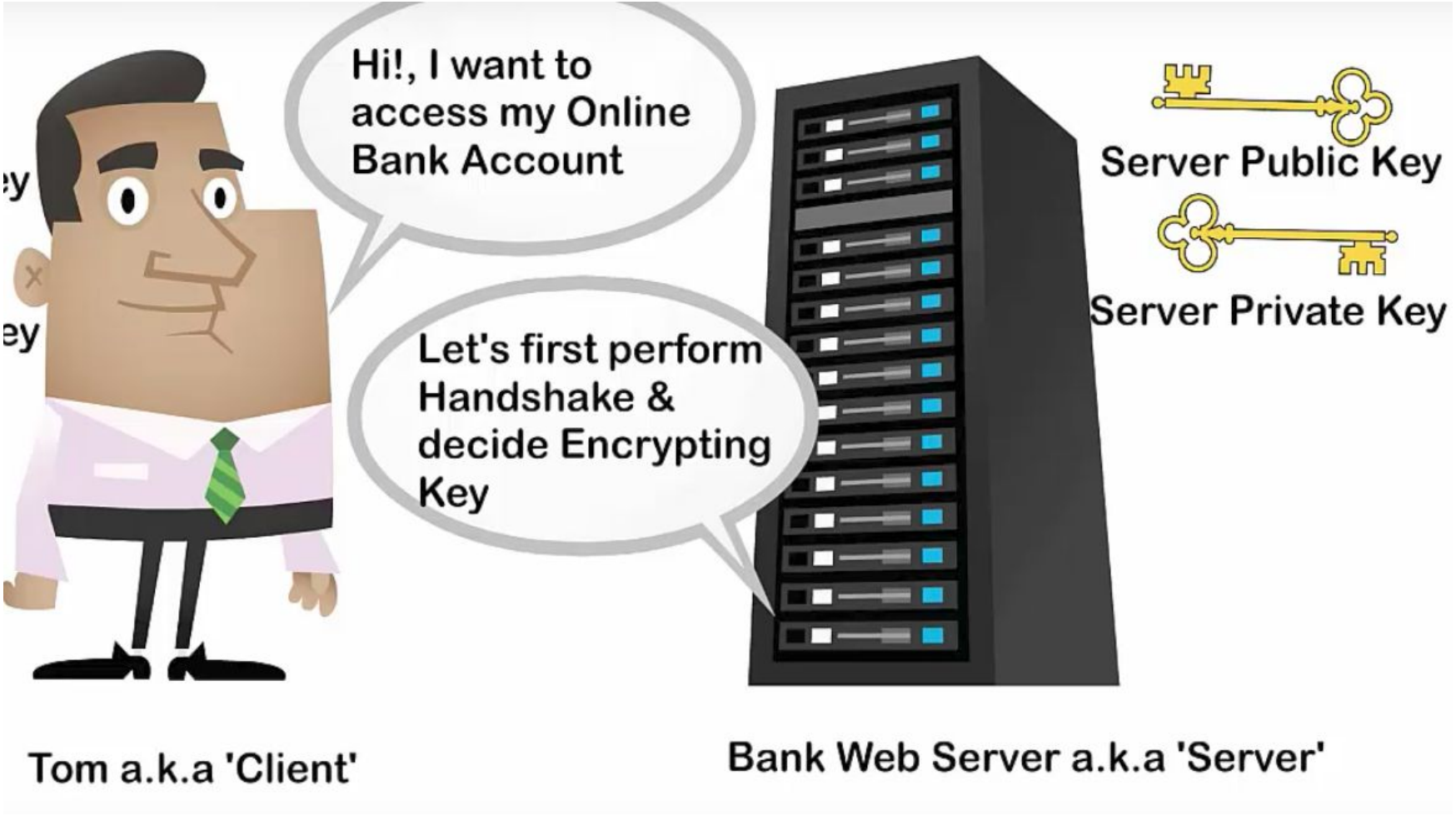
Attacker


Tom (client)
SSL
Online Banking Server
Credit Card Details
Attacker

SSL == Secure Sockets Layer

- Used for secure communications
- Typically seen in web services (https://)
- Uses both public key and private key cryptography

Communication begins with a **handshake protocol** between client and server to establish identity and set up session keys used to encrypt remainder of the transmissions


Hi!, I want to access my Online Bank Account
Let's first perform Handshake & decide Encrypting Key
Server Public Key
Server Private Key
Tom a.k.a 'Client'
Bank Web Server a.k.a 'Server'

TLS/SSL Handshake

Phase 1 : Establishing Security Capabilities (Client-Server Hello)

TLS/SSL Handshake

RNc

Generate Random Number, RNc

Public Key

Private Key

Phase 1 : Establishing Security Capabilities (Client-Server Hello)

TLS/SSL Handshake

RNc

Generate Random Number, RNc

RNc

Client Hello

Crypto Information, RNc

RNc

Public Key

Private Key

RNc

Phase 1 : Establishing Security Capabilities (Client-Server Hello)

TLS/SSL Handshake

RNc

Generate Random Number, RNc

Client Hello Crypto Information, RNc

RNc

RNc

Generate Random Number, RNs

RNs

Public Key

Private Key

RNc

RNs

Phase 1 : Establishing Security Capabilities (Client-Server Hello)

TLS/SSL Handshake

Public Key

Private Key

RNc

RNc

Generate Random Number, RNc

Client Hello Crypto Information, RNc

RNc

RNc

RNs

Generate Random Number, RNs

RNs

Server Hello Crypto Information, RNs

RNs RNs

Phase 1 : Establishing Security Capabilities (Client-Server Hello)

TLS/SSL Handshake

Public Key

Private Key

RNc

RNs

RNc

RNs

Phase 2 : Server Authentication & Key Exchange

TLS/SSL Handshake

Public Key

Private Key

RNc

RNs

Server Certificate (Public Key)

RNc

RNs

Phase 2 : Server Authentication & Key Exchange

TLS/SSL Handshake

verify

Certificate Authority (CA)

Public Key

Private Key

RNc

RNs

Server Certificate (Public Key)

RNc

RNs

Phase 2 : Server Authentication & Key Exchange

TLS/SSL Handshake

RNc

RNs

Server Certificate (Public Key)

Public Key

Private Key

RNc

RNs

Phase 2 : Server Authentication & Key Exchange

TLS/SSL Handshake

Generate Random Number, Pre-Master Secret, PMSc

PMSc

RNc

RNs

PMSc

Public Key

Private Key

RNc

RNs

Phase 4 : Key Generation

TLS/SSL Handshake

Public Key

Private Key

RNc

RNs

PMSc

Generate Random Number, Pre-Master Secret, PMSc

PMSc

Send PMSc encrypted with Server Public Key

RNc

RNs

Phase 4 : Key Generation

TLS/SSL Handshake

Generate Random Number, Pre-Master Secret, PMSc

PMSc

Send PMSc encrypted with Server Public Key

RNc

RNs

Decrypt PMSc using Server Private Key

PMSc

PMSc

Public Key

Private Key

RNc

RNs

PMSc

Phase 4 : Key Generation

TLS/SSL Handshake

Public Key

Private Key

RNc

RNs

PMSc

Generate Random Number, Pre-Master Secret, PMSc

PMSc

Send PMSc encrypted with Server Public Key

Decrypt PMSc using Server Private Key

PMSc

RNc

RNs

PMSc

MS

Calculate Master Secret at both ends, MS

MS

Phase 4 : Key Generation

TLS/SSL Handshake

MS

Send Data Encrypted with MS

End SSL Handshake

MS

Phase 5 : Finish

TLS/SSL Handshake

MS

MS

Send Data Encrypted with MS

End SSL Handshake

Send Data Encrypted with MS

End SSL Handshake

Phase 5 : Finish

TLS/SSL Handshake

MS

MS

Send Data Encrypted with MS

End SSL Handshake

Send Data Encrypted with MS

End SSL Handshake

Encrypted Communication Channel

Phase 5 : Finish