1

The Internet

- Fundamental Concepts (Network layer , server, client)
- Network Programming (Socket, Threading)
- Security Concerns
- Session Handling
- Network Programming II

2

The Hypertext Transfer Protocol

- A Typical HTTP-Session
- Requests and Responses
- Content Negotiation
- Access Control/Password-Protected Pages
- Caching (Proxies)
- State Management
- Authorization

1.1

Security Concerns

Transport Layer Vulnerabilities

- attacking network infrastructure
  - eavesdropping
  - packet injection
- compromise host-address mapping provided by DNS
- attacking host-to-host datagram protocols
  - packet sniffing
  - TCP connection spoofing

1.1

Security Concerns

TLS - Transport Layer Security

- protocol used for authentication and encryption of Internet connections, inserted as a separate layer between transport and application
- it is about guaranteeing the authenticity of the contacted server by a certificate and encrypting the connection between client and server
  - authentication
    mechanism to verify the validity of provided identification material
  - encryption
    mechanism to obfuscate what is sent from one host to another
  - data integrity
    mechanism to detect message tampering and forgery

1.1

Security Concerns

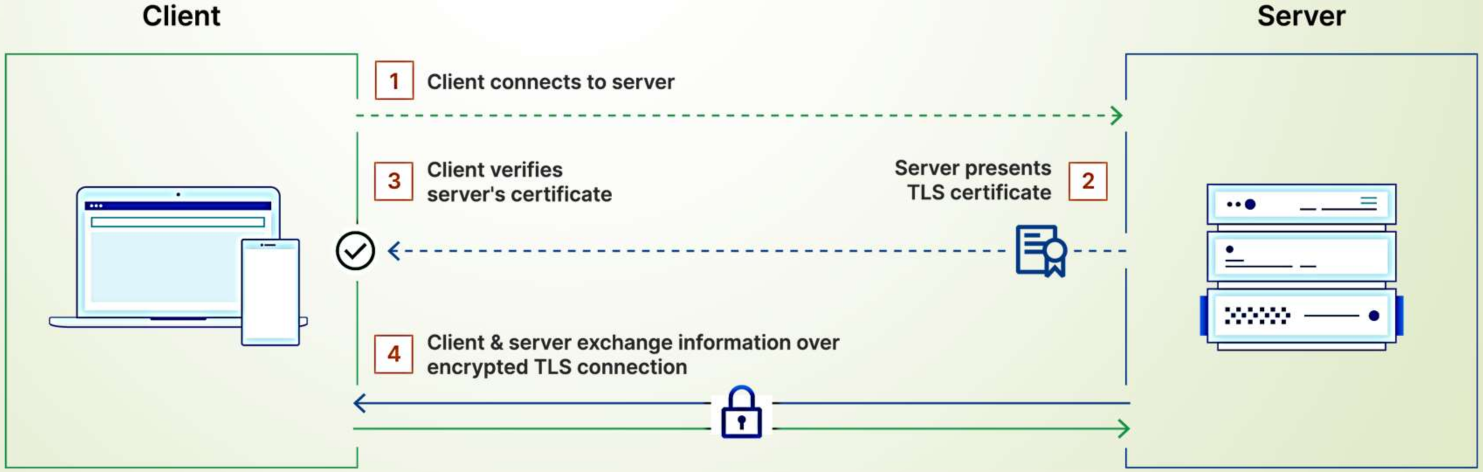
TLS - Transport Layer Security

- stateful cyber security protocol that is used to establish sessions between communication partners
- uses a session to store and use state information over a longer period of time
- a session is a "security association" between a client and a server, established using the handshake protocol
- a session defines a set of cryptographic security parameters that can be shared across multiple connections
- uses two different session keys for the bidirectional connection between client and server

Security Concerns

TLS - Transport Layer Security

- exchange of the certification of a public key and the authentication of the server
- validation of the exchanged certificates
- subsequent encrypted transmission of data between sender and receiver (asymmetric encryption method or public-key method)


Client
Server
1 Client connects to server
2 Server presents TLS certificate
3 Client verifies server's certificate
4 Client & server exchange information over encrypted TLS connection

I.1

Security Concerns

TLS - Transport Layer Security

- handshake
  - negotiating cipher suite: client and server to share their cryptographic capabilities
    - key exchange procedure
      establishes a shared secret between two parties that can be used for secret communication for exchanging data over a public network
    - encryption algorithm including length of encryption key and mode of operation (error propagation, block chaining, parallel processing, data authenticity, ...)
    - one-way-hash function for the keyed-hashing for message authentication code (HMAC)
  - server authentication and exchange of keys
    - normally an X.509v3 certificate that has been issued for a domain
      certificate contains a key pair consisting of a public and private key; the public key is used to encrypt data and the private key is used to decrypt

I.1

Security Concerns

TLS - Transport Layer Security

Advantages

- offers confidential session and server authentication
- built into every browser
- easy to configure on the server
- protocol has been heavily analyzed
- seems like you are getting security "for free"

Disadvantages

- users don't check certificates
- too easy to obtain certificates
- some settings are terrible
- totally insecure cipher suites included
- very little use of client-side certificates
- performance

I.1

Security Concerns

TLS – Domain Certificate

- characteristics
  - unique assignment of a public key to an organization
  - certification authority signs the domain certificate, making it impossible for third parties without the knowledge of the certification authority's secret key to modify the domain certificate
  - content
    - name of the organization whose authenticity is confirmed by this domain certificate
    - public key of the organization (domain)
    - name of the issuing certification authority
    - validity of the domain certificate

I.1

Security Concerns

TLS – Methods of Authentication

1. server and client without authentication

   neither the server nor the client authenticate the communication partner with a certificate

2. server authenticated, client anonymous (most common type)

   server shares its public key to the client by transmitting its certificate; if the client can verify the certificate, it can be can be sure that after a successful establishment of a connection a TLS-connection to exactly that server has been established whose certificate was received:

   - ➢ client generates pre-master-secret; encrypts it using the server's public key
   - ➢ pre-master secret and the exchanged random numbers are used by client and server to calculate the master secret, from which required keys (session keys, ...) are derived

3. server and client authenticated

I.1

Security Concerns

ssl – Python's TLS/SSL wrapper for socket objects

- provides access to TLS encryption and peer authentication facilities for network sockets, both client-side and server-side
  - class `ssl.SSLSocket`, derived from the `socket.socket` type, provides a socket-like wrapper that encrypts and decrypts the data going over the socket with SSL
  - supports additional methods for retrieval of the certificate of the Connection's other side, and the cipher being used for the secure connection

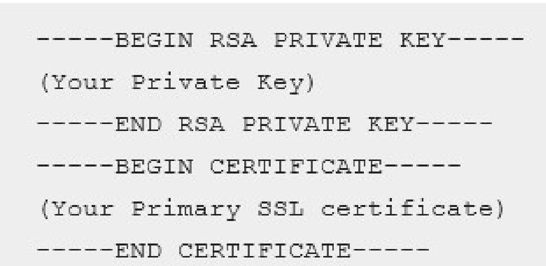
```
context = ssl.SSLContext(ssl.PROTOCOL_TLS_SERVER)
context.load_cert_chain('/path/to/certchain.pem', '/path/to/private.key')

with socket.socket(socket.AF_INET, socket.SOCK_STREAM, 0) as sock:
    sock.bind((HOST, SSLPORT))
    sock.listen()
    with context.wrap_socket(sock, server_side=True) as ssock:
        conn, addr = ssock.accept()
        ...
```

Security Concerns

ssl – PEM privacy enhanced mail

- a container format for digital certificates and keys
- a text file that consists of Base64 encoding of the certificate text, a plain-text header, and footer marking the beginning and end of the certificate
- creation
  1. download intermediate certificate, root certificate, primary certificate, and private key files sent by certificate authority
  2. in a text editor paste the entire body of all certificates and private key in specific order:

     Private Key,
     Primary Certificate, Intermediate Certificate, Root Certificate
  3. Add corresponding tags



```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate)
-----END CERTIFICATE-----
```

I.1

Session

Connections versus Session

- connection
  - negotiated, reliable connections between communicating systems
- session
  - time-delimited two-way link, a practical (relatively high) layer in the TCP/IP protocol enabling interactive expression and information exchange between two or more communication partners
  - responsible for establishing, maintaining, synchronizing, terminating sessions between end-user applications
  - may involve more than one message in each direction
  - is typically stateful