SSL Protocol

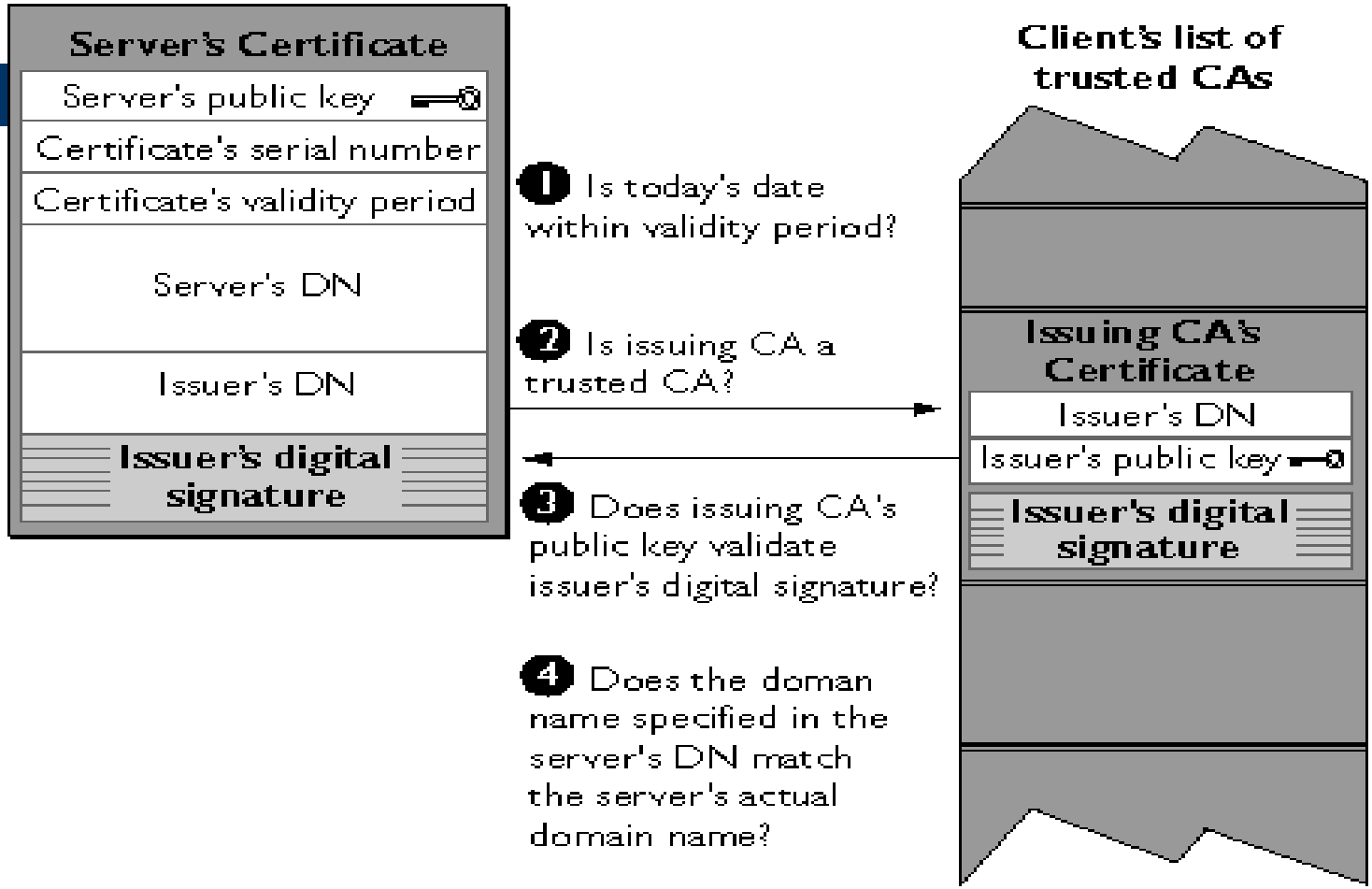
Overview

- Introduction to SSL
- SSL Architecture
- SSL Limitations

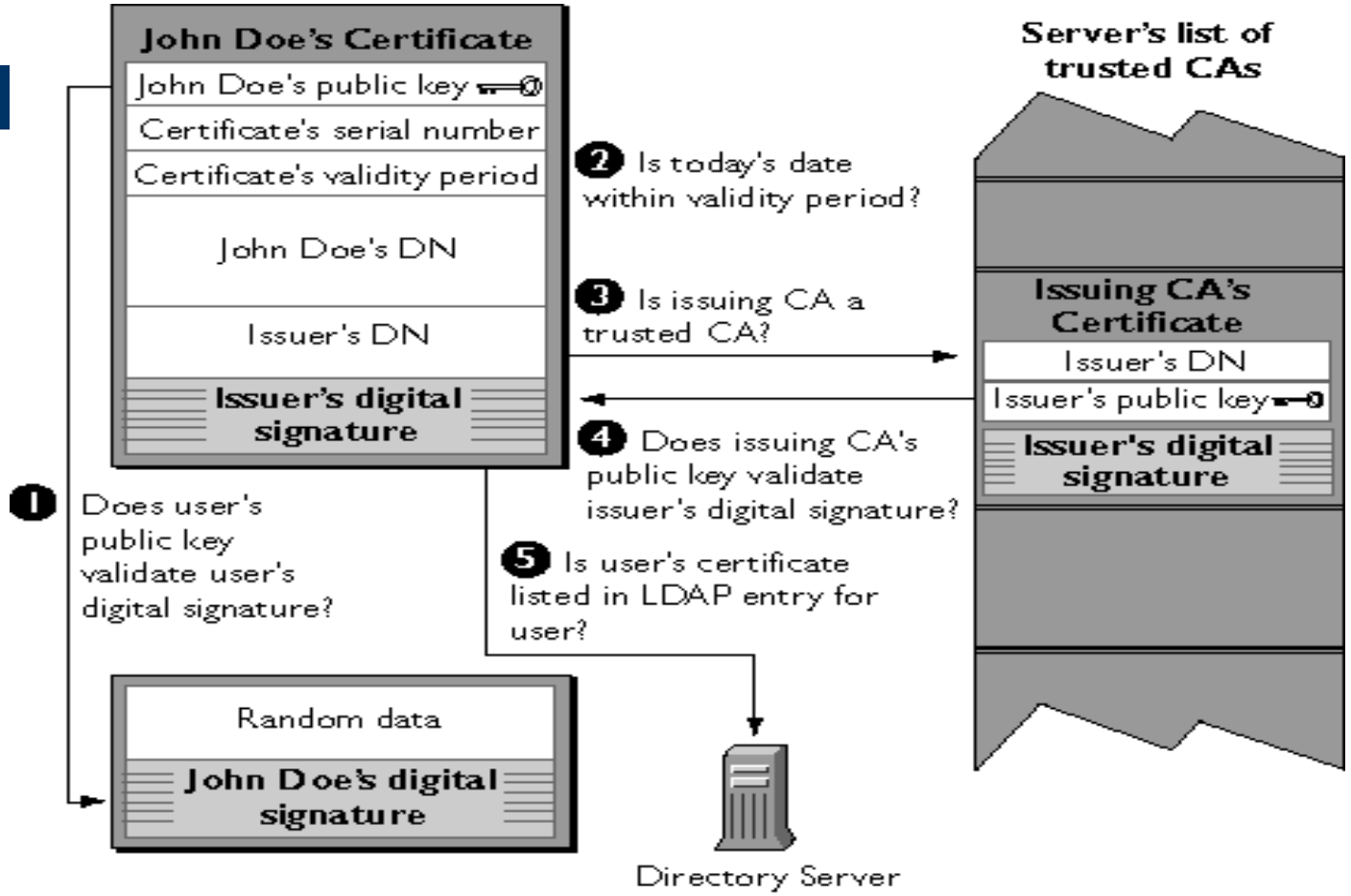
SSL fundamental

- SSL server authentication
- SSL Client authentication
- An encrypted SSL connection
- Sub protocols : SSL record protocol and the SSL handshake protocol

SSL Server authentication



SSL client authentication



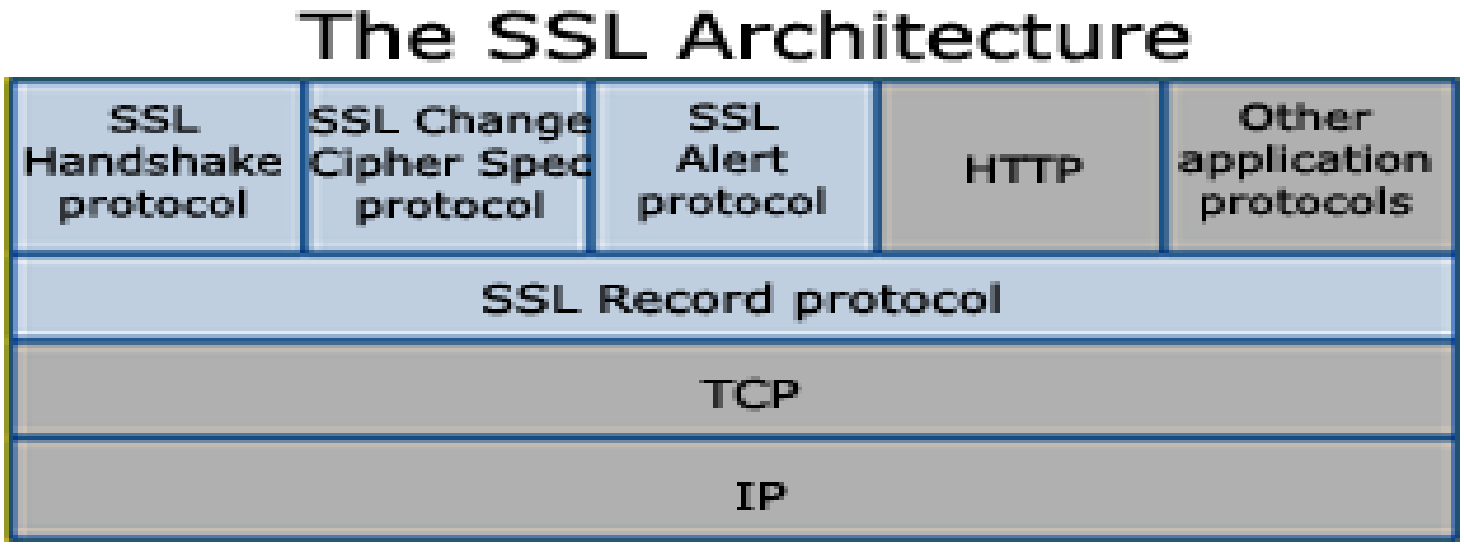
Overview of SSL

- Netscape
- Secure connection between clients and servers essential for Internet's success
- Solution: Encryption and Decryption at a connection's endpoints
- Latest Version is 3.0
- SSL sits directly on top of TCP: provides TCP-like interface to upper-layer applications
- Supports any application Layer Protocol

SSL Protocol (SSL V3.0)

- Two layer Protocol
- SSL Record Protocol-encapsulation of higher layer protocols
- SSL Handshake Protocol-allows server and client to authenticate,negotiate encryption algorithm and cryptographic keys

SSL Architecture



SSL consists of four protocols above the TCP layer, with three sitting alongside higher-layer applications.

SSL Record Layer

- Provide two services for SSL connections:
  - Confidentiality: by encrypting application data.
  - Message Integrity: by computing MAC over the compressed data.
- Can be utilized by some upper-layer protocols of SSL.(hand shake protocol)

Higher- layer Protocol

- SSL- specific protocols
  - Change Cipher Protocol
  - Alert Protocol
  - Handshake Protocol
- Application data layer

Change cipher spec protocol

- Signals transitions in ciphering strategies
- It updates the CipherSuite that will be used on the current connection

Alert Protocol

- Alert messages communicate the severity of the message and a description of the alert
- Fatal messages result in connection termination.

SSL-Handshake Protocol

- Establishment of the secure channel between the client and the server
- Provides the keys and the algorithm information to SSL Record Protocol, above it
- Enables clients and servers
  - Negotiate cryptographic algorithms
  - Optionally authenticate each other
  - Generate shared secrets using public-key encryption techniques

SSL-Handshake Protocol (contd…)

- **Handshake Protocol divided into 4 phases:**
  1. Establish Security Capabilities
  2. Server Authentication and key Exchange
  3. Client Authentication and key Exchange
  4. Change *CipherSpec* and Finish

“SSL is Not a Magic Bullet”

- It provides encrypted connections between two machines
- It verifies that information transmitted during the session is not being monitored or diverted to a malicious third party.
- Unfortunately, SSL is not the answer to every security concern.

Guarantees of SSL

- The server you want to contact is the one you got.
- No attacker can read or modify the data being transmitted between you and the Web server.

Non-Guarantees of SSL

- Host Insecurities
- Authentication issues
- Backend clear-text storage and transmissions
- SSL Implementation Flaws

Host Insecurities

- Having an SSL- enabled Web server, often just called a 'secure Web server,' does not secure the machine itself.
- Examples: If a machine running an SSL enabled Web server also runs an IMAP (Internet Mail Access Protocol) server, then that machine becomes vulnerable. IMAP servers are known to be prone to attacks.

Authentication Issues

- The SSL certificate is based on the host name, nothing else.
- Example: www.my_banks.com instead of www.my_bank.com

Backend clear-text storage and transmission

- Many Web servers get and store data using outside sources, such as databases or flat files
- These files may be sent somewhere else without using a secure channel.
- Example: credit card information

SSL Implementation Flaws

- Different vendors have their own implementation of SSL,which can have different flaws.
- OpenSSL has been discovered to have multiple buffer overflow capabilities
- Microsoft Internet Explorer does not properly check the digital "certificates" which guarantee the security of an SSL connection.

Affected Browsers

- Netscape 4.x and Mozilla are NOT vulnerable.
- IE 5 and 5.5 are vulnerable straight-up, and IE 6 is mostly vulnerable