

# Internet infrastructure

Prof. dr. ir. André Mariën

# HTTP and SSL

- Two systems:
  - Port 80/port 443: RFC 2818
  - UPGRADE within session: RFC 2817
- Most systems use different ports

# Security requirements

- Transmission of **confidential** information
  - Information that can be abused:
    - Credit card numbers
    - Login information
  - Privacy related data
    - Health care data
    - Financial profile

# Security requirements

- Know who you are talking with
- Identification
- Authentication
  - Client-server: which server
  - True confidentiality: both sides must be authenticated

# Security requirements

- Integrity of data
  - Correct information received
  - Correct information sent

# SSL and proxies

- CONNECT
  - Abuses: restricted to port 443
- Breaks caching

# SSL and security measures

- SSL IS security measure
- Confidentiality and other security measures:  
do not mix well
- IDS: blind
- Anti-virus: blind
- Sniffers: blind

# SSL-HTTP Interference

- Supposed to be orthogonal
- Sometimes not possible
  - Connection: keep-alive
  - SSL session life time

# SSL accelerators

- Key reason:
  - address the SSL performance problem
  - Asymmetric key operations during handshake
- Three issues
  - Acceleration
  - Off-loading
  - Termination

# SSL acceleration

- Hardware accelerator
  - Coprocessor
  - PCI/SCSI pluggable card
- Stays on system
  - Communication overhead still on processor
  - May not help (a lot) for symmetric operations

# SSL off-loading

- Move complexity and timing to a different system altogether
- Appliance style solution
- Separate hardware boxes

# SSL termination

- Before the actual server
- Allows for inspection via security tools
- Moves the secret key very close to the border
- From that point on: clear-text traffic (or loose advantage again)
- Client authentication: must follow, as it is integrated

# CA servers

- Certification request
- Certificate storage and retrieval
- Revocation management
  - CRL: certificate revocation list
  - OCSP: online certificate status
- Certificates: X.509v3

# Certificates

- Server certificates
  - Needed for SSL, server authentication and session set-up
- Client certificates
  - Used for email: S/MIME
  - Used for authentication in SSL
- Object signing certificates
  - Java JAR file signing
  - CAB file signing

# Authentication servers

- Servers that offer authentication
  - Authentication protocols
    - RADIUS
    - TACACS+
    - Kerberos
  - Data format
    - SAML (XML variant)

# LDAP servers

- Contain authentication credentials
- Can contain authorization information
- Contain certificate information