

Security in communications and networks

PV018

Vašek Matyáš

Typical Security Requirements

- **Authentication:** originator's identity assured.
- **Integrity:** information received as originated.
- **Confidentiality:** information available only to authorized parties.
- **Availability:** data & resources available when needed.
- **Non-repudiation:** party cannot deny communication (origin, receipt, delivery, etc.).
- **Access Control:** resources controlled by authorized parties.

Major security enablers – critical (infrastructure) applications

- Kerberos
- Public-key crypto based – certificates, typically X.509 – SSH, SSL/TLS
- Shared-key crypto based – symmetric key ciphers, hash functions

Kerberos

- Greek mythology – guardian to the entrance of Hades (master of the Underground)
- MIT project Athena – MIT's UNIX-based campus-wide academic computing facility



M12.1 Kerberos & Herakles



Kerberos – threat model

- Users reading messages of other users
- Users replaying messages of other users
- Users altering a workstation network address
- Users impersonating themselves

Kerberos – approach

- Centralised authentication server authenticating both users and machines
- Using symmetric-key techniques, no public-key techniques

Kerberos

- Trusted third-party authentication service
- Key Distribution Center (KDC) grants authentication tokens (“tickets”) to users
 - Trusted, dedicated machine
- Applications can use Kerberos for:
 - Data authentication
 - Data integrity
 - Data confidentiality

Kerberos – simple authentication

- $C \rightarrow AS:$ $ID_C \parallel P_C \parallel ID_V$
- $AS \rightarrow C:$ Ticket
- $C \rightarrow V:$ $ID_C \parallel \text{Ticket}$

$$\text{Ticket} = E_{K_V}(\text{ID}_C \parallel P_C \parallel \text{ID}_V)$$

Kerberos Tickets

- Ticket-Granting-Ticket
 - Used to obtain further tickets
 - Requires password or additional authentication from user
 - Lifetime in hours
- Service Tickets
 - Issued to user from KDC
 - User can not decrypt ticket
 - User passes ticket to authenticate to server

Kerberos used for applications

- telnet, rlogin, rcp, FTP, etc.
- Use Kerberos Protocol to exchange authentication information
- Client application uses Ticket-Granting-Ticket to obtain service tickets from KDC
- May use session key to encrypt data checksums (data integrity) or encrypt data (data confidentiality)

Kerberos Tickets (Credentials)

- Partly encrypted data structures
 - client ID
 - server ID
 - timestamp
 - session key
 - encrypted part (session key, client info, timestamp)
- Passed the way KDC → client → server
- Encrypted with the key of intended recipient

Kerberos – important terms

- C = Client
- AS = authentication server
- V = server
- ID_C = identifier of user on C
- ID_V = identifier of V
- P_C = password of user on C
- AD_C = network address of C
- K_V = secret encryption key shared by AS and V
- TS = timestamp
- \parallel = concatenation

Kerberos – time vs. replay issue

- The threat: an opponent steals a ticket and uses it before its expiry time
- Lifetime of the ticket-granting ticket
 - Too short \Rightarrow frequent ticket requests
 - Too long \Rightarrow greater risk of replay attack

Tickets

- Ticket-Granting Ticket – *get once per logon*
- Service-Granting Ticket – *get then once before first use of a service (usually in a given logon session)*
- Authenticated Service Request – *once per (service) session*

Kerberos(v4) Authentication Process

Authentication Service Exchange – To obtain the Ticket-Granting Ticket

- 1) $C \rightarrow AS:$ $ID_C \parallel ID_{TGS} \parallel TS_1$
- 2) $AS \rightarrow C:$ $E_{K_c}(K_{C,TGS} \parallel ID_{TGS} \parallel TS_2 \parallel Lifetime_2 \parallel Ticket_{TGS})$

Ticket-Granting Service Exchange – To obtain the Service-Granting Ticket

- 3) $C \rightarrow TGS:$ $ID_V \parallel Ticket_{TGS} \parallel Authenticator_C$
- 4) $TGS \rightarrow C:$ $E_{K_c}(K_{C,V} \parallel ID_V \parallel TS_4 \parallel Ticket_V)$

Client/Server Authentication Exchange: To Obtain Service

- 5) $C \rightarrow V:$ $Ticket_V \parallel Authenticator_C$
- 6) $V \rightarrow C:$ $E_{K_{c,v}}(TS_5 + 1)$

Kerberos today

- **Currently two broadly used versions:**
- 4 - restricted to a single realm (domain)
- 5 - allows inter-realm authentication
- Kerberos v5 is an Internet standard (RFC1510)
- MSFT implementation (since Windows 2000)

Key distribution (with indirect authentication)

- Direct distribution $\underline{\mathbf{A}} \xrightarrow{E_{K_{AB}}(K_S, \dots)} \mathbf{B}$
- Key distribution center (also generates the key – following slide)

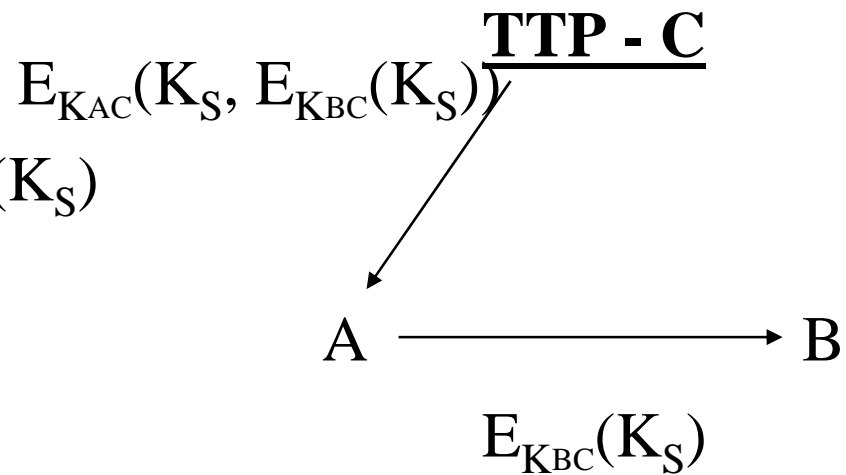
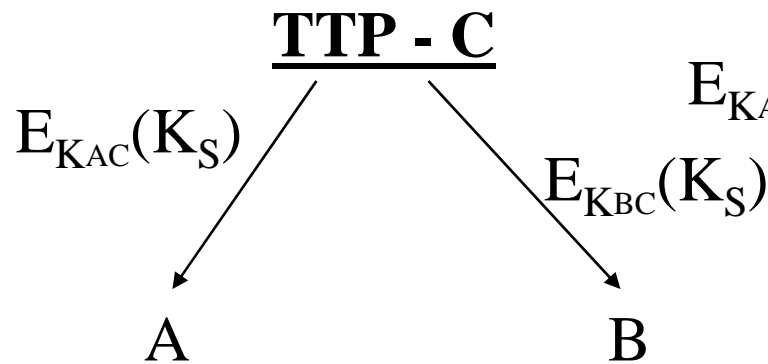
- Key transport center

```
graph TD; A["A"] -- "E_{K_{AC}}(K_S)" --> TTP["TTP - C"]; TTP -- "E_{K_{BC}}(K_S)" --> B["B"]
```

Indirect authentication – key distribution topologies.

TTP-managed

Direct (pull/push)



X.509 based authentication

- X.509 specifies the format for public-key certificates.
- The certificate contains the public key of a user and is signed with the private key of a Certification Authority (CA).
- Distributed environment using a database with certificate (user) information.
- Used in S/MIME, IP Security, SSL/TLS, SET.

What is SSL/TLS?

Secure Sockets Layer / Transport Layer Security

- Protocols providing security and reliability
- Protecting communication of two applications
- Running over standard protocols like TCP
- SSL – developed by Netscape, supported also by Microsoft...
- TLS – IETF standard (sometimes called SSL v3.1)
- Transparent for higher-level protocols like HTTP
- Using PKI and X.509 certificates

What security SSL/TLS provide?

Three basic security services:

- **Entity authentication** – the entities are authenticated using server and client certificates.
- **Integrity** – message authentication code (MAC) which ensures the data received is same as the data sent.
- **Confidentiality** – after the initial "handshake", a symmetric key is defined and used to encrypt all subsequent communication (even checked passwords, etc.).

Concepts of SSL/TLS

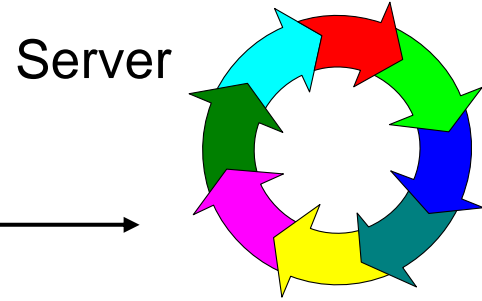
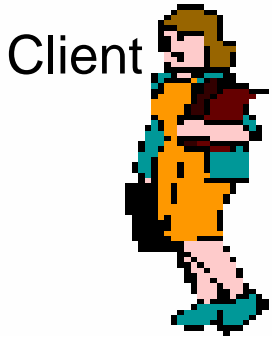
- Record Protocol

- The basic layer of the protocol.
- Works over TCP/IP (or other transport protocol).
- Allows for encapsulation of different higher level protocols (HTTP, FTP, telnet, etc.) which run unmodified.

- Handshake Protocol

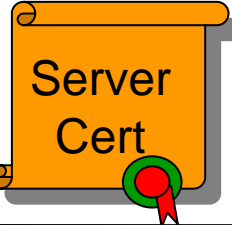
- Allows the server and client to authenticate each other.
- By default, server authentication is mandatory, client authentication optional.
- Authentication through presentation of digital certificates.
 - And verification of the ability to use the related private key!

Handshake Protocol



Client Hello



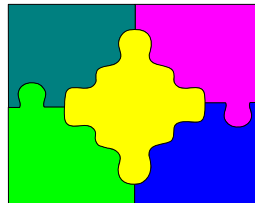
Server Hello, ( , Client Cert Request, ...)



Client Key Exchange, Cipher Spec, ( , ...)



Application

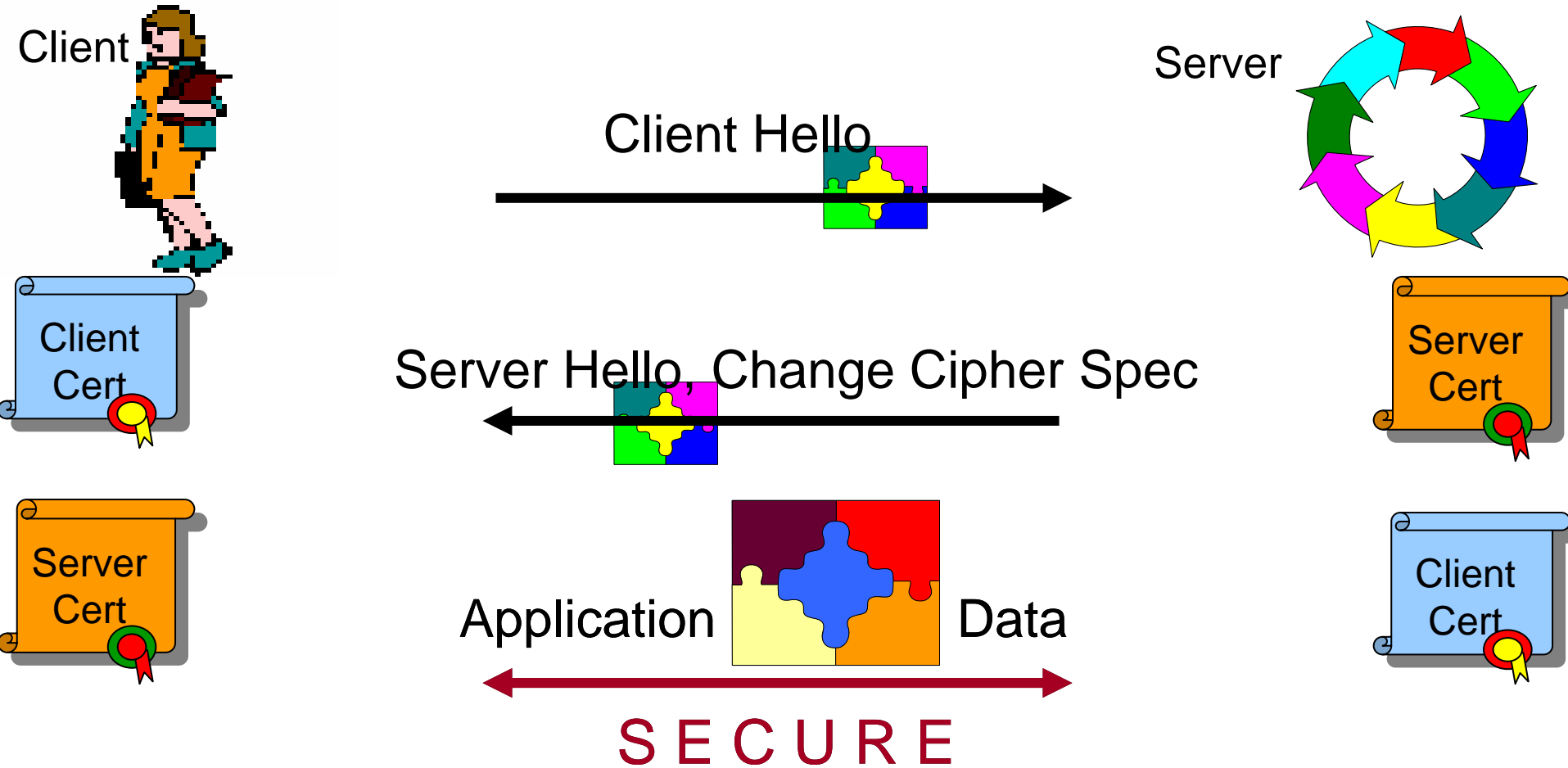


Data



SECURE

SSL/TLS Change Cipher Protocol



... more detail

- Establish Session
 - Send random challenge value, accept public key.
 - Verify signed challenge.
 - Deliver session key protected by recipient's public key.
- Communicate Protected Data
 - Encrypt data using agreed cipher and the session key.
 - Produce hash regularly to protect integrity.
 - Data packed into sequenced records.
- (Change Cipher - optional)
- Finish Session
- *<http://www.ietf.org/rfc/rfc2246.txt>*

Typical network attacks

- Holes in software (sendmail, RPC, NFS, or the firewall itself 😊)
- Network snooping – search for gold
- IP/DNS spoofing – masquerade
- Holes in new (higher-level) protocols

Intrusion Detection Systems

- Intrusion – activity aimed at disrupting or circumventing a service within an organization's system
- Also penetration, breach (, attack)
- Social engineering ☺
- Technical methods

IDS Principles

- Anomaly detection
 - Unusual pattern (as compared to typical user/system behavior).
 - False positives!
- Misuse detection
 - Pattern of intrusion(-like) behavior
 - False negatives!

Combine these two approaches!

IDS Topologies

Network-based

- Checking network traffic
- Use raw network packets.
- Typically a network adapter running in promiscuous - monitoring and analyzing all traffic.
- Responses like admin notification, connection termination, session recording (for forensic analysis), other detailed evidence collection.

Host-based

- Checking machines (log files, etc.).
- Started in 80s – log file review.
- Typically monitor system, event, and security logs on WinNT and syslog on Unix.
- Also critical file checksum control, response time, port activities.
- Responses analogous...

Combine these two approaches!

Email Security

- Postcard-like service
- PGP (Pretty Good Privacy)
- S/MIME (Secure Multipurpose Internet Mail Extension)
- (X.400)

IPSEC

- Authentication Header (AH), RFC-1826
 - Authenticity & integrity
- Encapsulating Security Payload (ESP), RFC-1827
 - Confidentiality (non-repudiation of origin)
 - Tunneling mode (encapsulation incl. headers)
 - Transport mode (data encapsulation)
- Security Associations (SA)

IPSEC – Security Associations

- Set of security features for a given session between two or more systems.
- Identifiable by Security Parameter Index (SPI) and the IP address.
- SPI depends on its Domain of Interpretation (DOI), this defines format, type of key-exchange, naming conventions, etc. One system can support more DOIs.

Parameters of Security Associations

- For AH – key authentication alg.
- For ESP – encryption alg., crypto synchronization, initiation vector.
- Both for AH and ESP – level of security, key lifetime, support of certificates, etc.

Firewalls

- Protect against attacks from the outside (across the firewall)
- Attacks against internal data
- Denial-of-service attacks
- Communication options:
 1. Allow
 2. Deny
 3. Translate (Proxy)

Basic options – firewalls

TCP/UDP	Allow/Deny	Packet filtering <i>(routers)</i>
TCP	A/D/Translate	Circuit-gateway <i>(trust inside)</i>
HTTP, FTP...	A/D/T	Applic.-gateway

Secure SHell

- SSH
- <http://www.ssh.com/>
- Non-commercial downloads
- WinSCP
- <http://winscp.sourceforge.net/eng/>
- WinSCP

Closely related topics – to be discussed later.

- Firewalls and network security
 - Guest lecture next week – Josef Pojsl, Technical Director, Trusted Network Solutions

Recommended reading (assignment #1)

- Paper “*The Evolution of the Kerberos Authentication System*”

ftp://athena-dist.mit.edu/pub/kerberos/doc/krb_evolution.PS

- Limitations of Kerberos 4, and changes made in Kerberos 5.

Questions?

Reminder:

Term project presentations May 3 & 10!
6 slots each date – mail to follow soon...