7.5 hp, Spring term 2008

Network Security

Lecture 4

IPSec

WebSecurity

SNMP

Kristina.Kunert@hh.se

IP Security

- Implementation of security at IP level
- 3 functions: Authentication, Confidentiality, Key management
- Benefits
  - Implemented in firewall: strong security for crossing comm.
  - IPSec in firewall is resistant to bypass
  - Below transport layer: transparent to application & end user
- Routing applications
- Implemented as extension headers
  - Authentication Header (AH) for authentication
  - Encapsulating Security Payload header (ESP) for encryption

IP Security

- Services
  - Access control, Connectionless integrity, Data origin authentication, Rejection of replayed packets, Confidentiality, Traffic flow confidentiality
- Security associations
  - 1-way relationship between sender & receiver
  - Security Parameter Index, IP Dest. Addr., Security Protocol Identifier
- IPSec modes of use
  - Transport: protection of payload
  - Tunnel (encapsulation): protection of packet

Web Security

- 3 approaches
  - network/transport/application level
- SSL
  - Record protocol, HTTP, Handshake protocol, Change Cipher Spec protocol, Alert protocol
  - Connection: transport of service
  - Session: association between client & server
- TLS slightly different
- SET: protects credit card transactions over the Internet

Network Management

- SNMP
  - Simple Network Management Protocol
- Network management system
  - collection of tools for network monitoring & control
- Model with 4 key elements
  - Management station, Management agent, Management information base, Network management protocol
- Application-level protocol
- Connectionless over UDP