7.5 hp, Spring term 2008

Network Security

Lecture 3

E-mail security

Kristina.Kunert@hh.se

Kerberos

- Authentication service
- Centralized authentication server
  - Employs K. server(s) to provide authentication service
  - Trusted 3rd party authentication service
- Assumes a distributed client/server architecture
- Only symmetric encryption, no public-key encryption
- Requirements: secure, reliable, transparent, scalable
- Realm = Full service K. Environment = K. server, nr of clients, nr of application servers
- Version 5 improvements
  - Supports any encryption
  - Supports any network addressing format
  - No double encryptions
  - Added functionality through flags in the tickets

X.509

- Public-key cryptography, digital signatures, hash functions
- Each user has a public-key certificate by a trusted certification authority (CA)
  - Certificates are placed in a directory
- If B has A's cert., B knows that:
  - Messages it encrypts with A's public key are secure from eavesdropping
  - Messages signed with A's private key are unforgeable
- 3 authentication procedures
  - One-/Two-/Three-Way Authentication

PGP

- Operations:
  - Authentication, Confidentiality, Compression, E-mail compatibility, Segmentation

S/MIME

- Security enhancement to the MIME Internet e-mail format standard
- Functionality similar to PGP