Network Security

Henric Johnson
henric.johnson@bth.se

Outline

- Attacks, services and mechanisms
- Security attacks
- Security services
- Methods of Defense
- A model for Internetwork Security
- Internet standards and RFCs

Attacks, Services and Mechanisms

- **Security Attack:** Any action that compromises the security of information.
- **Security Mechanism:** A mechanism that is designed to detect, prevent, or recover from a security attack.
- **Security Service:** A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

Security Attacks

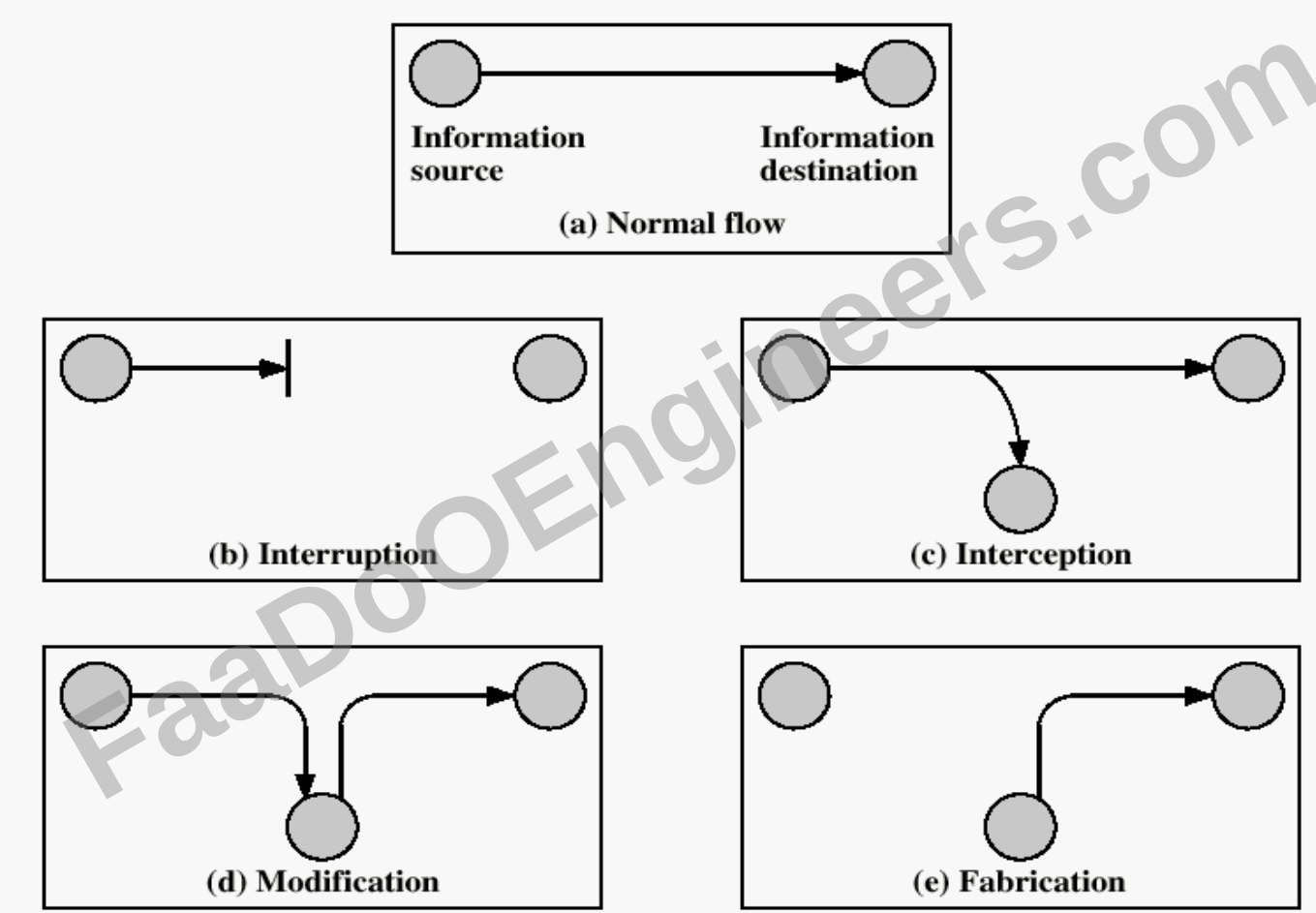
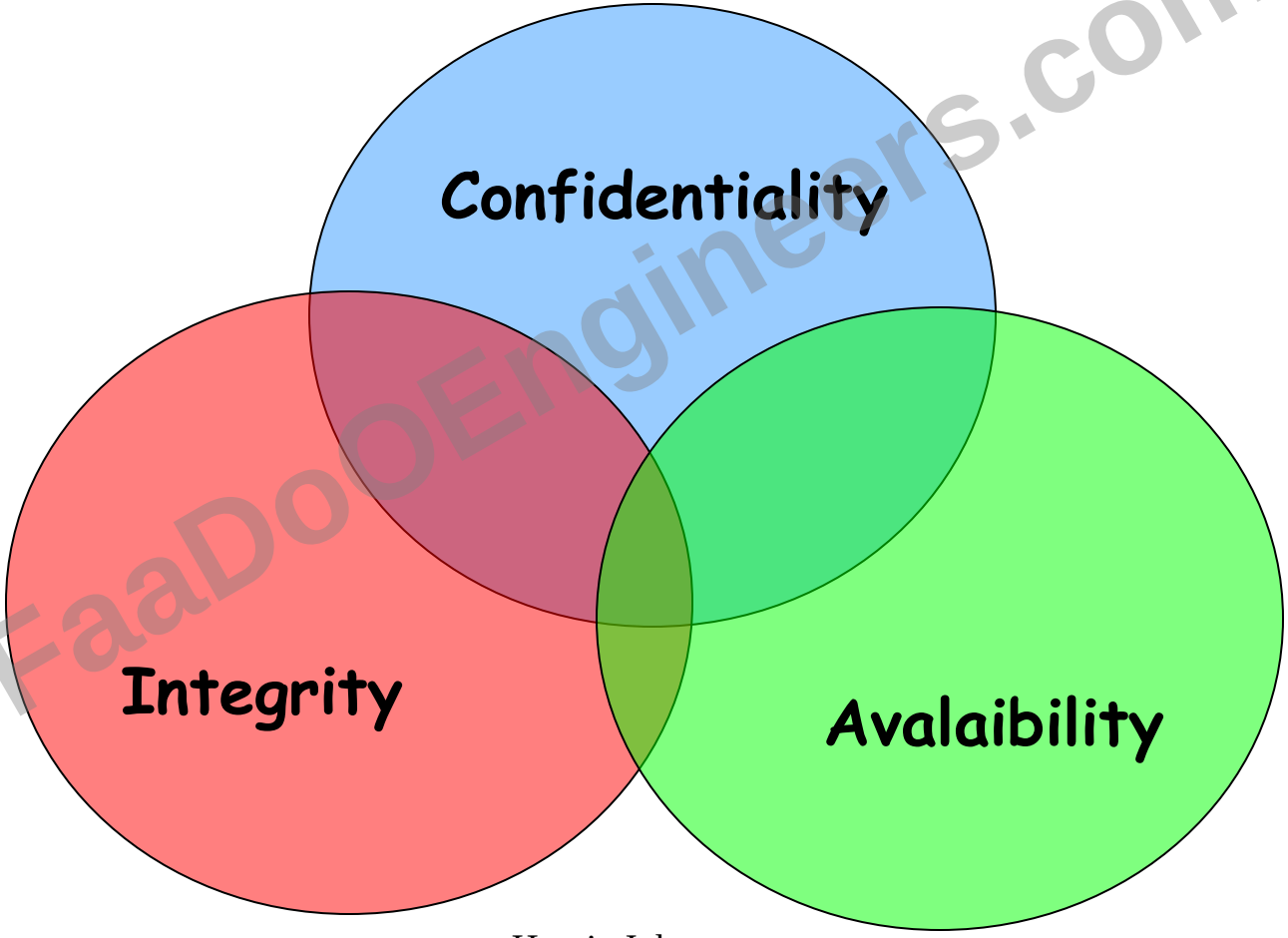


Figure 1.1 Security Threats

Security Attacks

- **Interruption:** This is an attack on availability
- **Interception:** This is an attack on confidentiality
- **Modification:** This is an attack on integrity
- **Fabrication:** This is an attack on authenticity

Security Goals



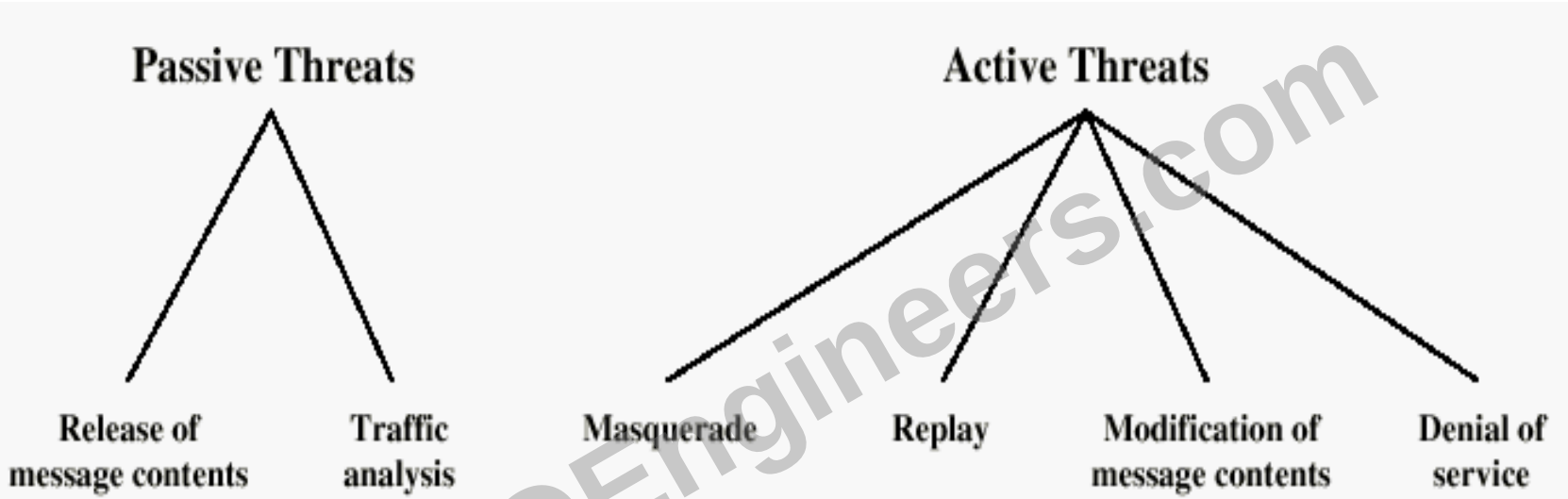


Figure 1.2 Active and Passive Security Threats

Security Services

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files

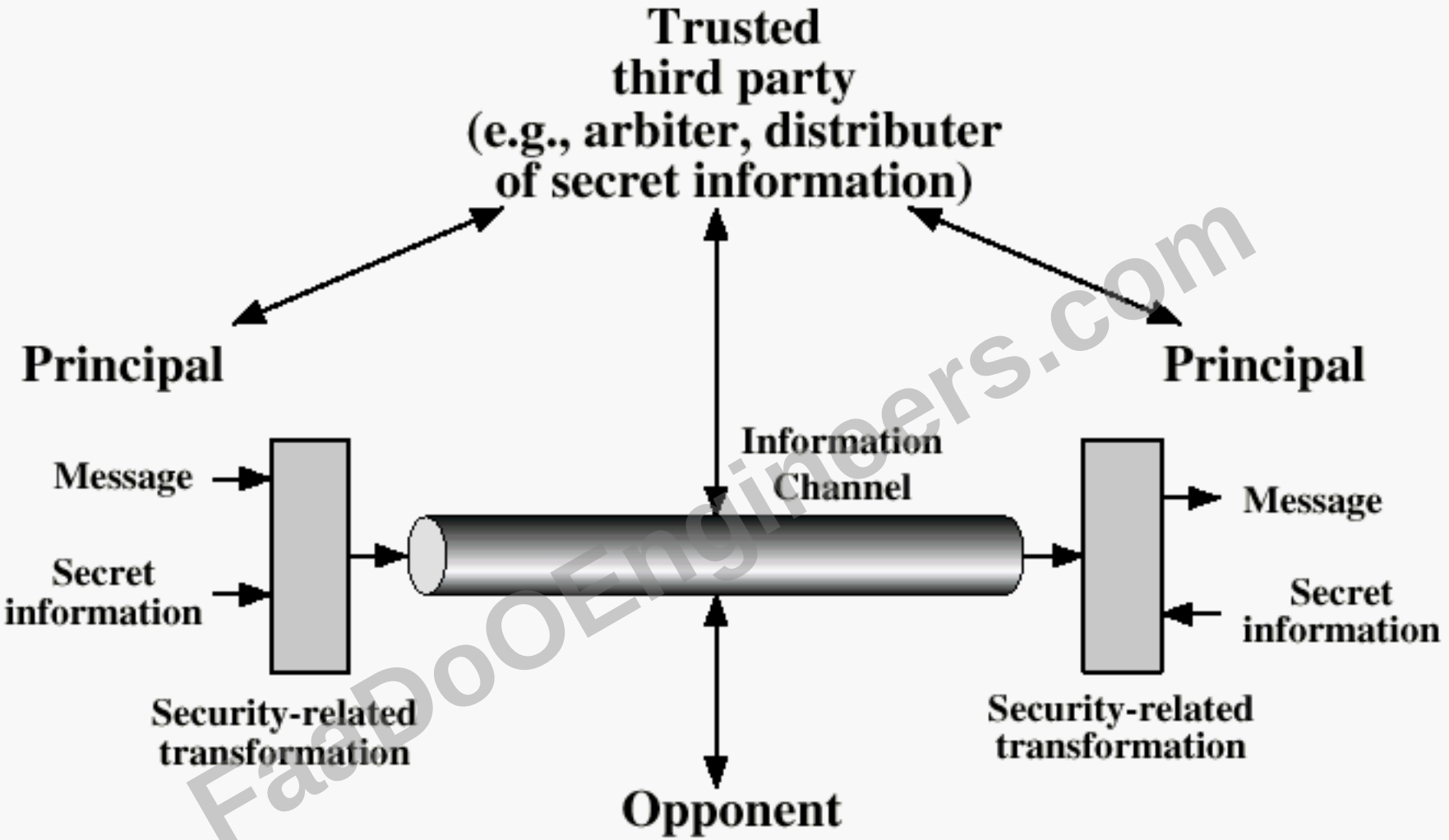


Figure 1.3 Model for Network Security

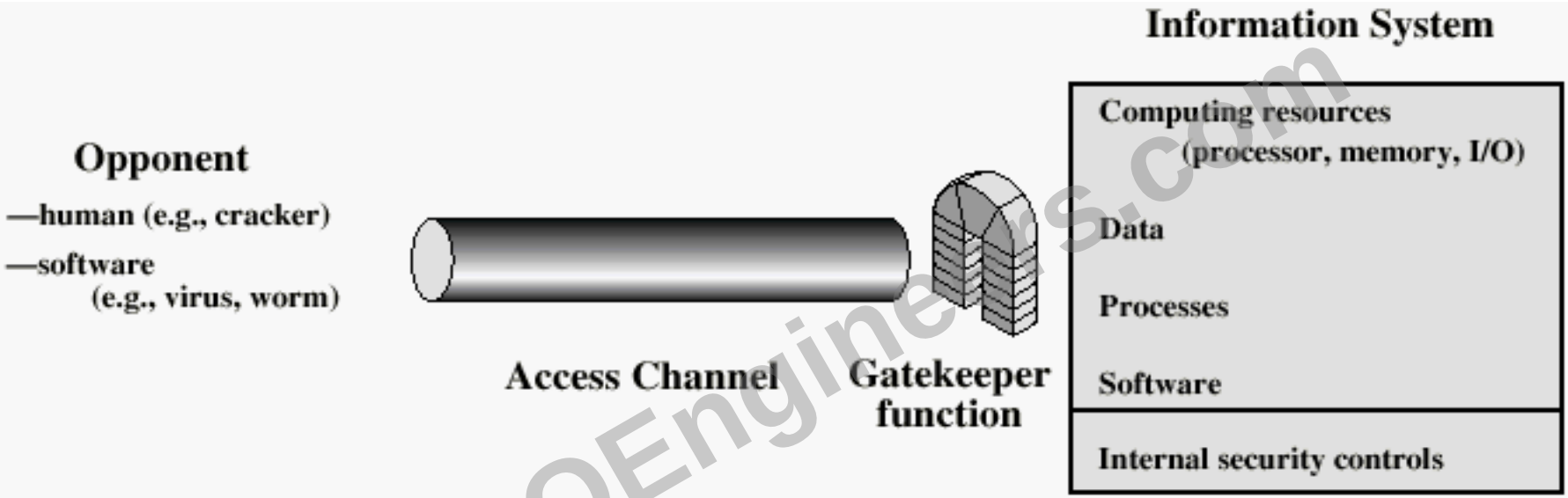


Figure 1.4 Network Access Security Model

Methods of Defence

- Encryption
- Software Controls (access limitations in a data base, in operating system protect each user from other users)
- Hardware Controls (smartcard)
- Policies (frequent changes of passwords)
- Physical Controls

Internet standards and RFCs

- The Internet society
  - Internet Architecture Board (IAB)
  - Internet Engineering Task Force (IETF)
  - Internet Engineering Steering Group (IESG)

Internet RFC Publication Process

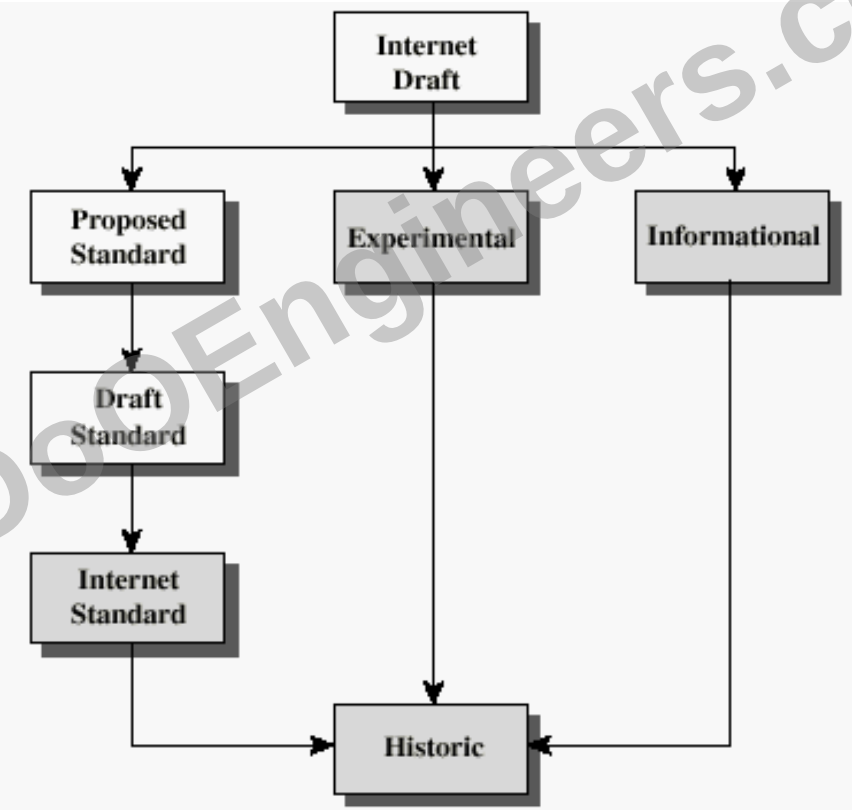


Figure 1.5 Internet RFC Publication Process

Recommended Reading

- Pfleeger, C. *Security in Computing.* Prentice Hall, 1997.
- Mel, H.X. Baker, D. *Cryptography Decrypted.* Addison Wesley, 2001.