Network Security

Generic Aspects and Special Issues for High Speed Networks

Carsten Benecke, DFN-FWL, University of Hamburg
Network Security

- DFN security projects in Hamburg
- What is network security?
- How do we achieve network security?
- How can we migrate security mechanisms to high speed networks (HSN) ?
- Some results of our „Firewall Lab“ activity
DFN Security Projects in Hamburg

• **DFN-CERT (since 1993)**
  – Computer Emergency Response Team

• **Contact for Incidents and Vulnerabilities**
  – Track/chase crackers
  – Provide countermeasures
  – Fix/close holes in operating systems and tools
  – WWW-database for SEC-tools and SEC-bulletins
  – Arrange network security tutorials

• **International Cooperation**
  – Active member of FIRST (Forum of Incident RST)
  – Review advisories
  – Track global incidents/attacks
DFN Security Projects in Hamburg

- **DFN-PCA (since 1996)**
  - (Policy) Certification Authority (CA)
  - also known as „Trustcenter“ / „Trusted 3rd Party“

- **Infrastructure Approach**
  - Hierarchy of CAs: „Public Key Infrastructure“
  - PKI allows for scaling
  - Support and cooperation through „Cross Certificates“

- **Technology offers...**
  - authenticity (through digital signatures)
  - confidentiality (through encryption)
DFN Security Projects in Hamburg

- **DFN-FWL (since 1997)**
  - Firewall Lab for High Speed Networks

- **Firewall Topics:**
  - Describe bottlenecks of firewalls in HSN
  - Find solutions to increase the performance
  - Migrate IP-Firewalls to ATM-Networks
  - Describe problems & solutions for VPN integration

- **ATM Topics:**
  - Identify new vulnerabilities in ATM protocols
  - Provide counter measures for ATM vulnerabilities
  - Utilize ATM features to increase network security
What is „Network Security“?

• Network security is the aim of security management

• Best described by security goals:
  – Integrity (of data, messages)
  – Authenticity (of sender, receiver)
  – Confidentiality (of data and communication)
  – Availability (of network equipment and services)
  – Non-repudiation (receipt, transmit of messages)
  – ...
Enabling Technology

Network Security enables:

- **E-Commerce**
  - Web-based shopping
  - Web-based banking
  - ...

- **Data Protection**
  - Privacy, integrity, availability

- **Distributed Systems**
  - Credentials, ACLs, remote system management
How do we achieve Network Security?

• Organisational Efforts:
  – CERT-Teams
    • Incident response
    • Provide information (about incidents, countermeasures, other contacts)
    • Teach administrators in network security
  – (P)CAs and Trust Centers
    • Establish public key infrastructures
    • Define and enforce certification policies
    • Check identity of key holder (RA)
    • Create/regenerate certificates
    • Offer revocation services
How do we achieve Network Security?

• Technical Efforts:
  – Build better trusted systems
  – Increase host security
    • Install patches
    • Drop unnecessary services
    • Drop unnecessary accounts
    • Check the systems periodically
  – Make use of „security mechanisms“
    • Use cryptography
    • Use access control
    • Use audit/logging/monitoring
Security Mechanisms (Techniques)

- **Firewalls**
  - Access control and audit

- **Virtual Private Networks (VPN)**
  - Confidentiality and authenticity of communication over public networks

- **Intrusion Detection Systems (IDS)**
  - Detect unauthorized access to computers and networks
Migrate Security Mechanism to HSN?

- No Problem in Ethernets (10 Mbit/s)

- Big Problem in HSN
  - Bandwidth increases dramatically
  - Combination of expensive methods
  - New protocols (e.g., ATM) are not well understood (new features, new security risks)

- Major Problems:
  - Cryptography is expensive (slow)
  - Access Control needs choke point (bottleneck)
  - Network based IDS need access to all messages
Some Results of the „DFN-Firewall Lab“

- Parallel Processing (for any HSNs):
  - Parallel packet screen
  - Parallel bastions
  - Parallel VPN encryption / decryption
  - Parallel monitoring / auditing

- Migrate IP-Firewalls to IP over ATM networks (ATM specific aspects)
  - Use ATM-switch to separate networks
  - Use IP-Firewalls for inter-network access control
  - Describe typical ATM-based firewall architectures
Example: Parallel Packet Screen
Example: Parallel Packet Screen

UDP Datagrams (DG) filtered by Parallel Packet Screen
64 Kbyte Socket Size, Fast Ethernet, 0 Rules

- theoretical Throughput
- rcu (2WS)
- rcu (1WS)
- rcu (4WS)

Size of Message [byte]

© 1999 DFN-FWL / Network Security 14
Conclusions

- **Network Security is an enabling technology**
  - E-Commerce
  - Privacy

- **Generic security goals are still valid**
  - Integrity, authenticity, confidentiality, non-repudiation,…

- **HSNs impose new problems**
  - Speed up the security mechanisms
  - Find and fix security flaws in new protocols
  - Concentrate on proactive work