ITU-T Recommendation
X.805 and its application to NGN

ITU/IETF Workshop on NGN

Zachary Zeltsan,
Lucent Technologies
Rapporteur of Question 5 SG 17
Outline

- Introduction to ITU-T Recommendation X.805 -
  Security Architecture for Systems Providing End-to-End Communications
  - Threat model
  - Security Layers
  - Security Planes
  - Security Dimensions
  - Overall model
  - Modular approach
- Security work in FGNGN Security Capability WG and ITU-T Recommendation X.805
## ITU-T X.800 Threat Model

<table>
<thead>
<tr>
<th>Threat Level</th>
<th>Type of Attack</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1 - Destruction</strong></td>
<td>(an attack on availability):</td>
<td>Destruction of information and/or network resources</td>
</tr>
<tr>
<td><strong>2 - Corruption</strong></td>
<td>(an attack on integrity):</td>
<td>Unauthorized tampering with an asset</td>
</tr>
<tr>
<td><strong>3 - Removal</strong></td>
<td>(an attack on availability):</td>
<td>Theft, removal or loss of information and/or other resources</td>
</tr>
<tr>
<td><strong>4 - Disclosure</strong></td>
<td>(an attack on confidentiality):</td>
<td>Unauthorized access to an asset</td>
</tr>
<tr>
<td><strong>5 - Interruption</strong></td>
<td>(an attack on availability):</td>
<td>Network becomes unavailable or unusable</td>
</tr>
</tbody>
</table>
Three Security Layers

1 - Infrastructure Security Layer:
- Fundamental building blocks of networks, services, and applications
- Examples:
  - Individual routers, switches, servers
  - Point-to-point WAN links
  - Ethernet links

2 - Services Security Layer:
- Services provided to end-users
- Examples:
  - Frame Relay, ATM, IP
  - Cellular, WiFi
  - VoIP, QoS, IM, Location services
  - Toll free call services

3 - Applications Security Layer:
- Network-based applications accessed by end-users
- Examples:
  - Web browsing
  - Directory assistance
  - Email
  - E-commerce

• Security Layers are a hierarchy of equipment and facilities groupings
• Each Security Layer has unique vulnerabilities, threats, and mitigations
• Infrastructure security enables services security enables applications security
Three Security Planes

1 - End-User Security Plane:
- Access and use of the network by the customers for various purposes:
  - Basic connectivity/transport
  - Value-added services (VPN, VoIP, etc.)
  - Access to network-based applications (e.g., email)

2 - Control/Signaling Security Plane:
- Activities that enable efficient functioning of the network
- Machine-to-machine communications
- Implementation may be in-band or out-of-band

3 - Management Security Plane:
- The management and provisioning of network elements, services and applications
- Support of the FCAPS functions
- Implementation may be in-band or out-of-band

- Security Planes represent the types of activities that occur on a network.
- Each Security Plane is applied to every Security Layer to yield nine security Perspectives (3 x 3)
- Each security perspective has unique vulnerabilities and threats
8 Security Dimensions Address the Breadth of Network Vulnerabilities

1-Access Control
- Limit & control access to network elements, services & applications
- Examples: password, ACL, firewall

2-Authentication
- Provide Proof of Identity
- Examples: shared secret, PKI, digital signature, digital certificate

3-Non-repudiation
- Prevent ability to deny that an activity on the network occurred
- Examples: system logs, digital signatures

4-Data Confidentiality
- Ensure confidentiality of data
- Example: encryption

5-Communication Security
- Ensure data is received as sent or retrieved as stored
- Examples: MD5, digital signature, anti-virus software

6-Data Integrity
- Ensure data is received as sent or retrieved as stored
- Examples: MD5, digital signature, anti-virus software

7-Availability
- Ensure network elements, services and application available to legitimate users
- Examples: IDS/IPS, network redundancy, BC/DR

8-Privacy
- Ensure identification and network use is kept private
- Examples: NAT, encryption

8 Security Dimensions applied to each Security Perspective (layer and plane)
ITU-T X.805: Security Architecture for Systems Providing End-to-End Communications

Security Layers
- Applications Security
- Services Security
- Infrastructure Security
- Control/Signaling Security
- Management Security
- End User Security

8 Security Dimensions
- Data Confidentiality
- Communication Security
- Integrity
- Availability
- Privacy
- Authentication
- Non-repudiation

Vulnerabilities Can Exist In Each Layer, Plane

THREATS
- Destruction
- Corruption
- Removal
- Disclosure
- Interruption

ATTACKS
Modular Form of X.805

<table>
<thead>
<tr>
<th></th>
<th>Infrastructure Layer</th>
<th>Services Layer</th>
<th>Applications Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Plane</td>
<td>Module One</td>
<td>Module Four</td>
<td>Module Seven</td>
</tr>
<tr>
<td>Control/Signaling</td>
<td>Module Two</td>
<td>Module Five</td>
<td>Module Eight</td>
</tr>
<tr>
<td>User Plane</td>
<td>Module Three</td>
<td>Module Six</td>
<td>Module Nine</td>
</tr>
</tbody>
</table>

- Execute
  - Management Network: Top Row
  - Network Services: Middle Column
  - Security Module: Layer & Plane Intersection

The 8 Security Dimensions Are Applied to Each Security Module

Access Control
Authentication
Non-repudiation
Data Confidentiality
Communication Security
Data Integrity
Availability
Privacy

Provides a systematic, organized way of performing network security assessments and planning
Conclusion: X.805 Provides A Holistic Approach to Network Security

- Comprehensive, end-to-end network view of security

- Applies to any network technology
  - Wireless, wireline, optical networks
  - Voice, data, video, converged networks

- Applies to any scope of network function
  - Service provider networks
  - Enterprise (service provider’s customer) networks
  - Government networks
  - Management/operations, administrative networks
  - Data center networks

- Can map to existing standards addressing
  - Enterprise & service provider, government needs
Security work in FGNGN Security Capability WG and ITU-T Recommendation X.805

- Guidelines for NGN security and X.805
  - Security in NGN
    - NGN threat model (based on ITU-T X.800 and X.805 Recommendations)
  - Security Dimensions and Mechanisms (based on ITU-T X.805)
    - Access Control
    - Authentication
    - Non-repudiation
    - Data confidentiality
    - Communication security
    - Data integrity
    - Availability
    - Privacy

- NGN security requirements for Release 1 and X.805
  - Security requirements
    - General considerations based on the concepts of X.805
Thank you!
Backup Materials
Example: Applying Security Layers to ATM & IP Networks

Applying Security Layers to ATM Networks

Infrastructure Security Layer
- Individual ATM Switches
- Point-to-Point Communication Links Between Switches (e.g., DS-3 links, E-3 links, OC-48 links, and STM-12 links)

Services Security Layer
- ATM Services Classes: CBR, VBR-RT, VBR-nRT, ABR, UBR

Applications Security Layer
- ATM-Based Video Conferencing Application

Applying Security Layers to IP Networks

Infrastructure Security Layer
- Individual Routers, Servers
- Communication Links Between Routers (Could be ATM PVCs)

Services Security Layer
- Basic IP Transport
- IP Support Services (e.g., AAA, DNS, DHCP)
- Value-Added Services: (e.g., VPN, VoIP, QoS)

Applications Security Layer
- Basic Applications (e.g., ftp, Web Access)
- Fundamental Applications (e.g., Email)
- High-End Applications (e.g., E-Commerce, Training)
Example: Applying Security Planes to Network Protocols

**End User Security Plane**
- **Activities**
  - End-User Data Transfer
  - End-User – Application Interactions
- **Protocols**
  - HTTP, RTP, POP, IMAP
  - TCP, UDP, FTP
  - IPSec, TLS

**Control/Signaling Security Plane**
- **Activities**
  - Update of Routing/Switching Tables
  - Service Initiation, Control, and Teardown
  - Application Control
- **Protocols**
  - BGP, OSPF, IS-IS, RIP, PIM
  - SIP, RSVP, H.323, SS7
  - IKE, ICMP
  - PKI, DNS, DHCP, SMTP

**Management Security Plane**
- **Activities**
  - Operations
  - Administration
  - Management
  - Provisioning
- **Protocols**
  - SNMP
  - Telnet
  - FTP
  - HTTP
How the Security Dimensions Map into the Security Threats

<table>
<thead>
<tr>
<th>Security Dimension</th>
<th>Access Control</th>
<th>Authentication</th>
<th>Non-Repudiation</th>
<th>Data Confidentiality</th>
<th>Communication Security</th>
<th>Data Integrity</th>
<th>Availability</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>X.800 Security Threats</td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Destruction</th>
<th>Corruption</th>
<th>Removal</th>
<th>Disclosure</th>
<th>Interruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
</tr>
<tr>
<td>Authentication</td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
</tr>
<tr>
<td>Non-Repudiation</td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
</tr>
<tr>
<td>Data Confidentiality</td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
</tr>
<tr>
<td>Communication Security</td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
</tr>
<tr>
<td>Data Integrity</td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
</tr>
<tr>
<td>Availability</td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
</tr>
<tr>
<td>Privacy</td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
<td><img src="%E2%9C%93" alt="Check Mark" /></td>
</tr>
</tbody>
</table>

Provides just-in-time network security services
NGN Subsystem Architecture Overview

- Based on 3GPP IMS R6
- IP Connectivity Access Network And related subsystems
- Other Multimedia Subsystems...
  - (RTSP-based) Streaming services
  - (SIP-based) IP Multimedia Subsystem (Core IMS)
  - (SIP-I based) PSTN/ISDN Emulation Subsystem

Applications

Network Attachment Subsystem

Resource and Admission Control Subsystem

Access Transport Network

Core Transport Network

PSTN

4/28/2005