

# 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



## 1 - **Destruction** (an attack on availability):

- Destruction of information and/or network resources

## 2 - **Corruption** (an attack on integrity):

- Unauthorized tampering with an asset

## 3 - **Removal** (an attack on availability):

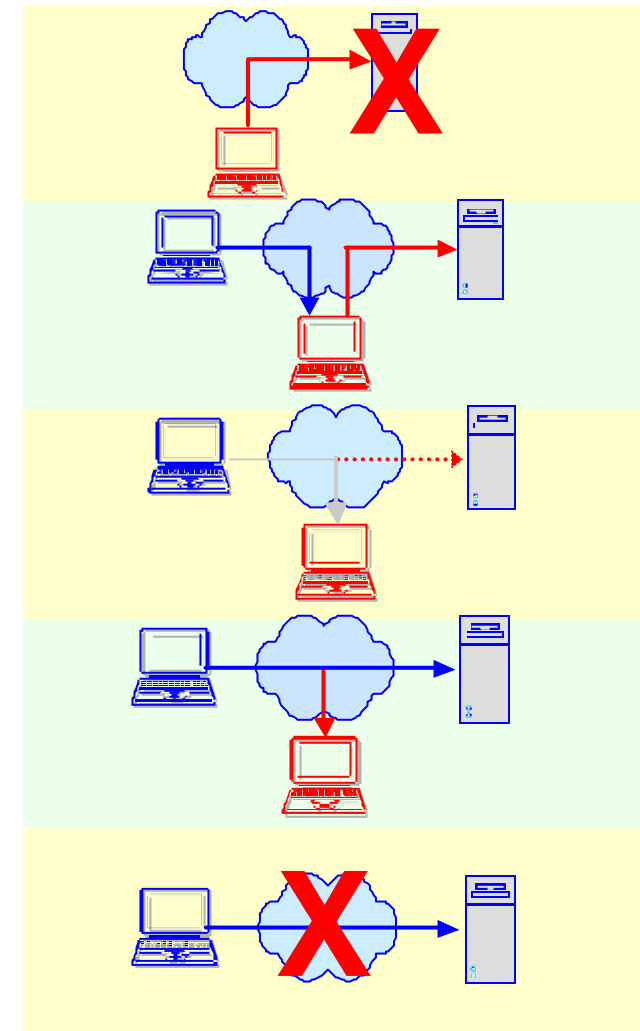
- Theft, removal or loss of information and/or other resources

## 4 - **Disclosure** (an attack on confidentiality):

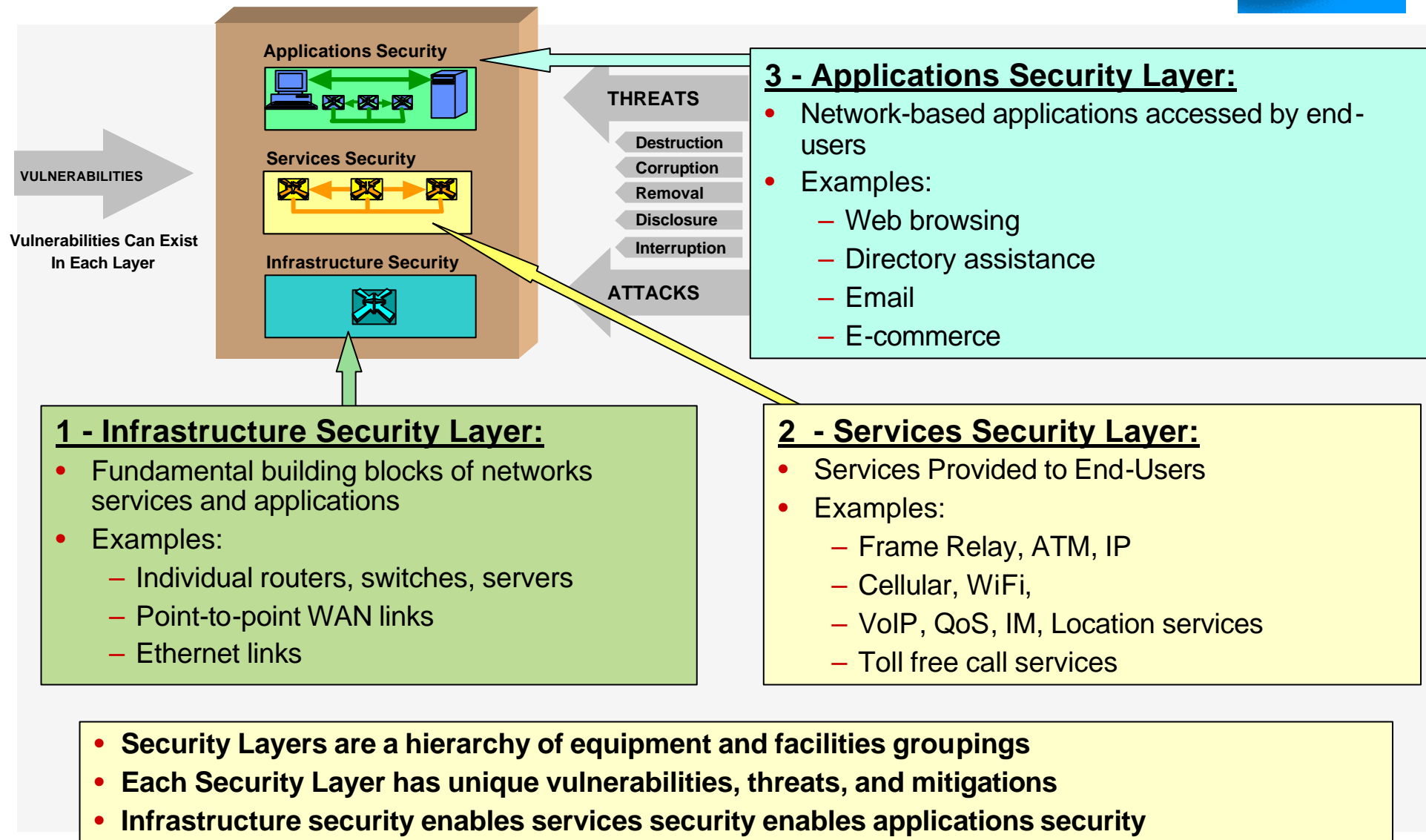
- Unauthorized access to an asset

## 5 - **Interruption** (an attack on availability):

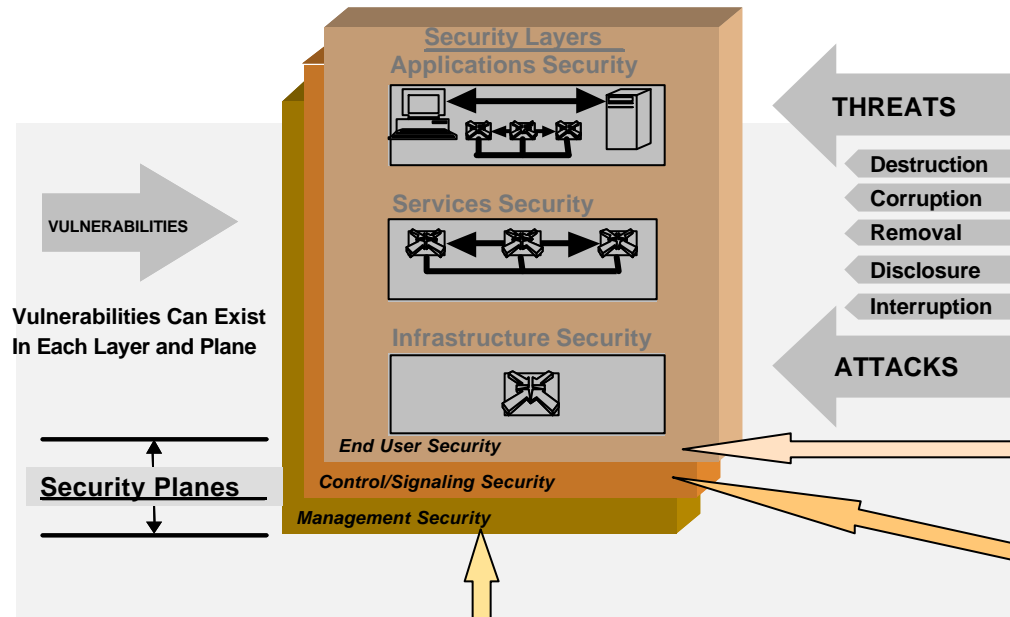
- Network becomes unavailable or unusable



# Three Security Layers



# 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)

## 3 - Management Security Plane:

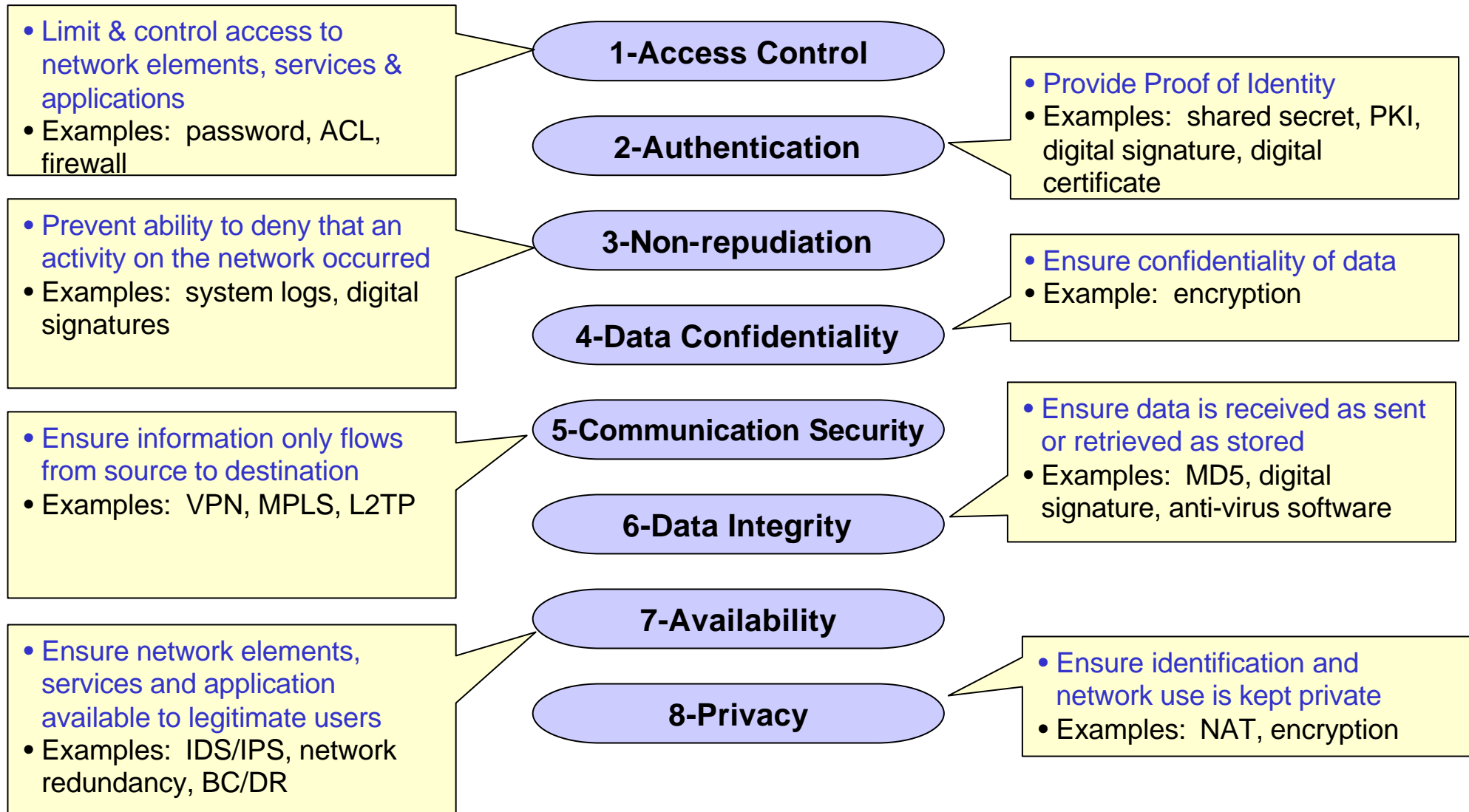
- The management and provisioning of network elements, services and applications
- Support of the FCAPS functions
- Implementation may be in-band or out-of-band

## 2 - Control/Signaling Security Plane:

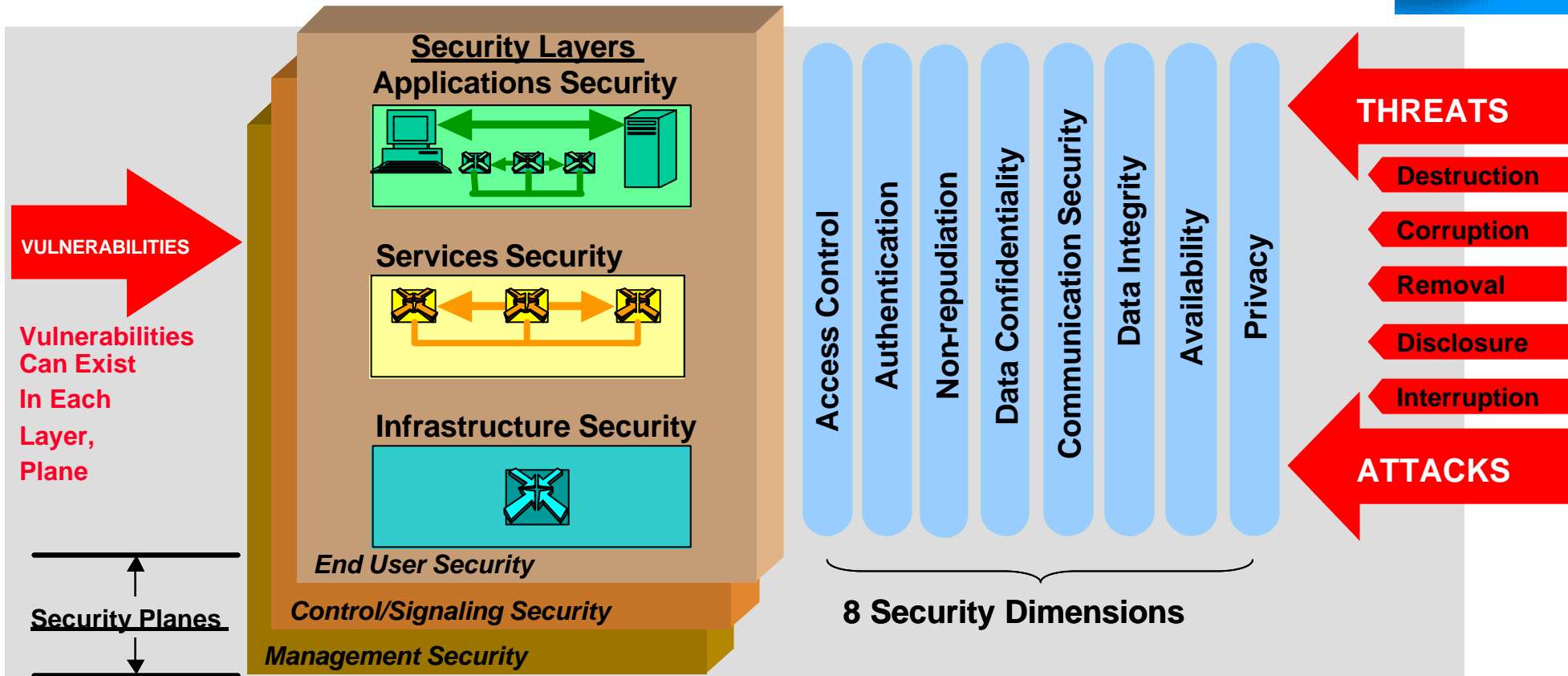
- Activities that enable efficient functioning of the network
- Machine-to-machine communications
- Implementation may be in-band or out-of-band

- **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



# ITU-T X.805: Security Architecture for Systems Providing End-to-End Communications





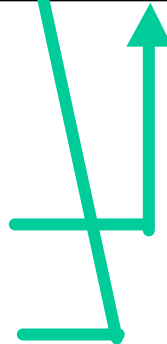
# Modular Form of X.805

	Infrastructure Layer	Services Layer	Applications Layer
Management Plane	Module One	Module Four	Module Seven
Control/Signaling Plane	Module Two	Module Five	Module Eight
User Plane	Module Three	Module Six	Module Nine



## Execute

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



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

The 8 Security Dimensions Are Applied to Each Security Module

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



Security Dimension	X.800 Security Threats				
	Destruction	Corruption	Removal	Disclosure	Interruption
Access Control	✓	✓	✓	✓	
Authentication			✓	✓	
Non-Repudiation	✓	✓	✓	✓	✓
Data Confidentiality			✓	✓	
Communication Security			✓	✓	
Data Integrity	✓	✓			
Availability	✓				✓
Privacy				✓	

**Provides just-in-time network security services**

# NGN Subsystem Architecture Overview

