ITU-T X.805 Training
March 6, 2007

Suhasini Sabnis, Andrew McGee

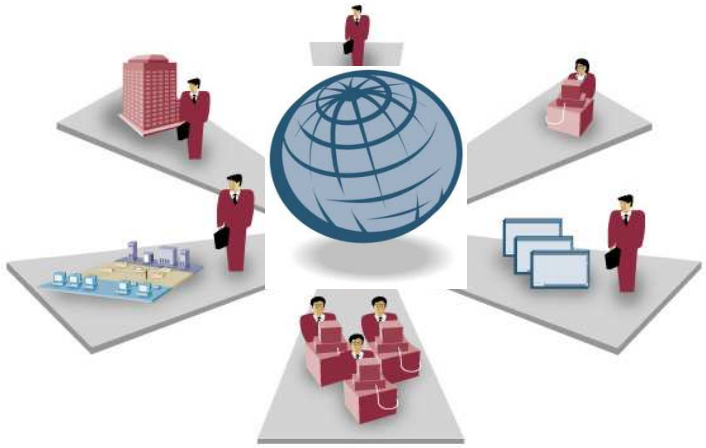
Outline

1. Need for a Security Framework
2. ITU-T X.805 Basics
3. ITU-T X.805 in Action – A Real World Action
4. Other Standards and Compliance
5. Conclusion

Critical Market Concerns – Security Drivers

Ensuring customer privacy

Improving reliability & service availability



Identifying specific risks & quantifying vulnerabilities

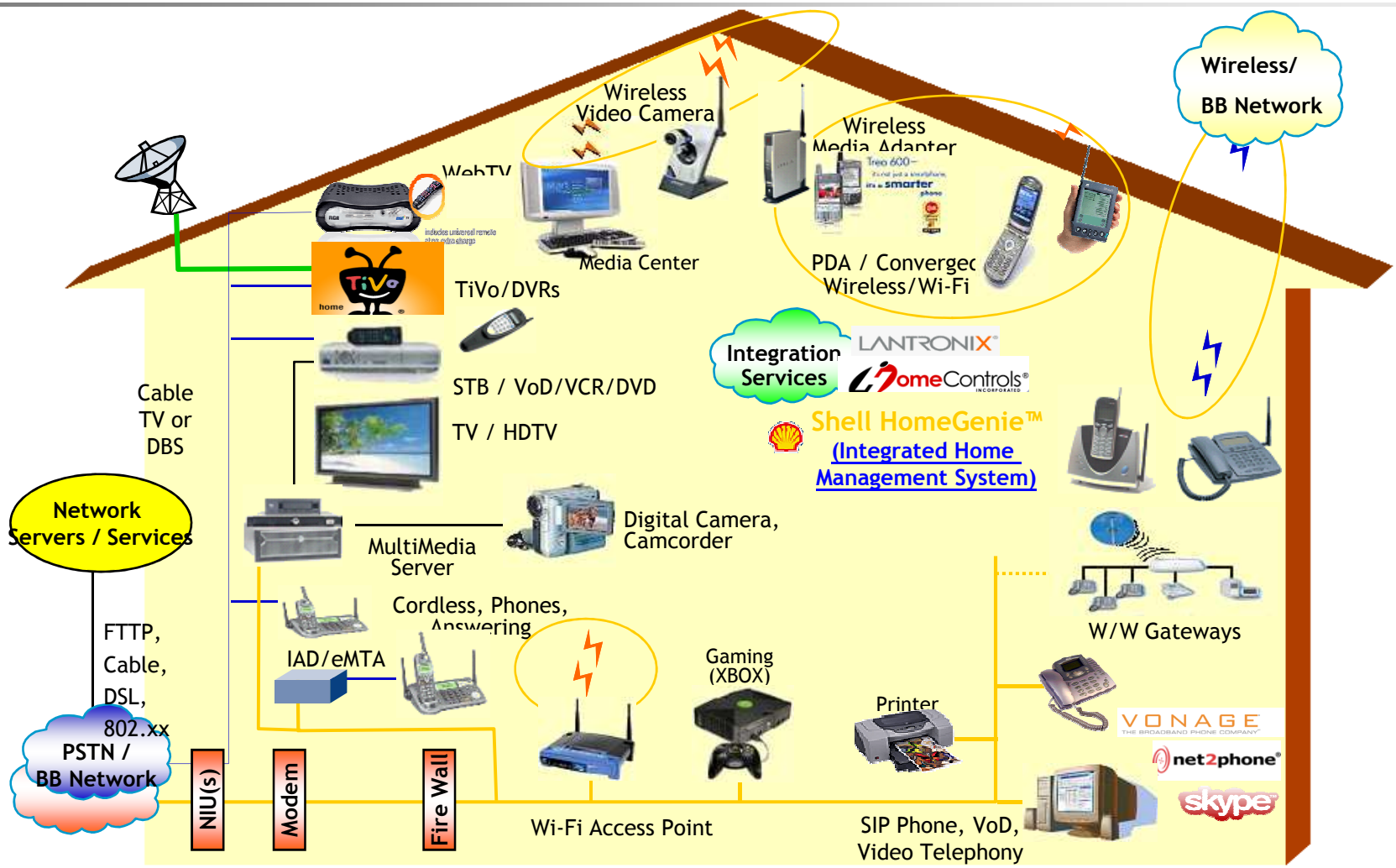
Securing new technologies & applications

Defending against increasingly sophisticated attacks

Managing limited resources for ongoing security administration

A best-in-class company must cover people, process & tools

Network Security Challenges – Example of Consumer's Multimedia Home

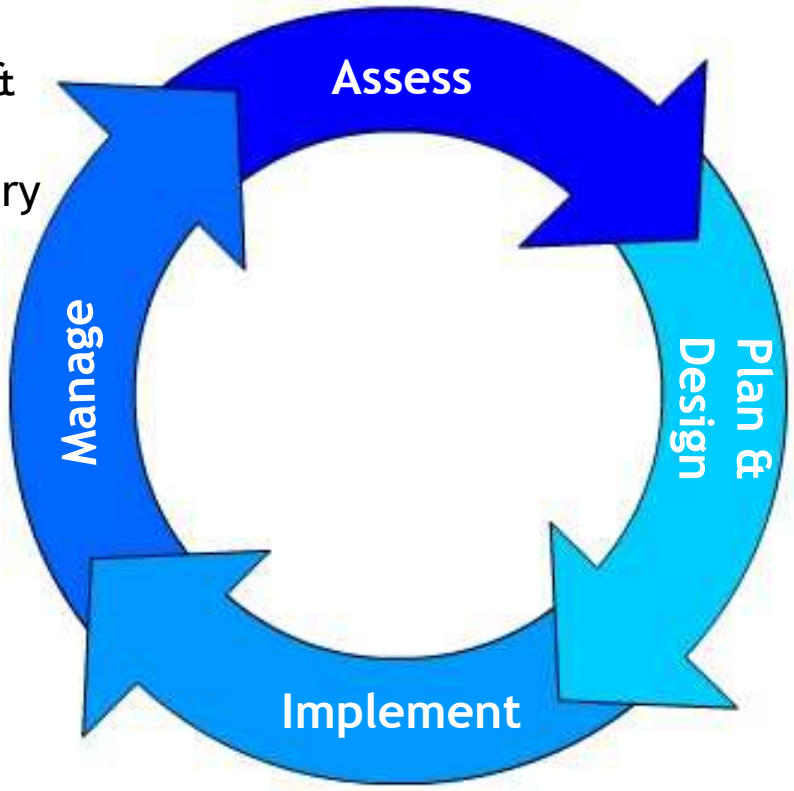


- NGN networks are complex
- Security threats propagate quickly & are increasing in number & severity

Alcatel·Lucent

Becoming a Security Best-in-Class Company

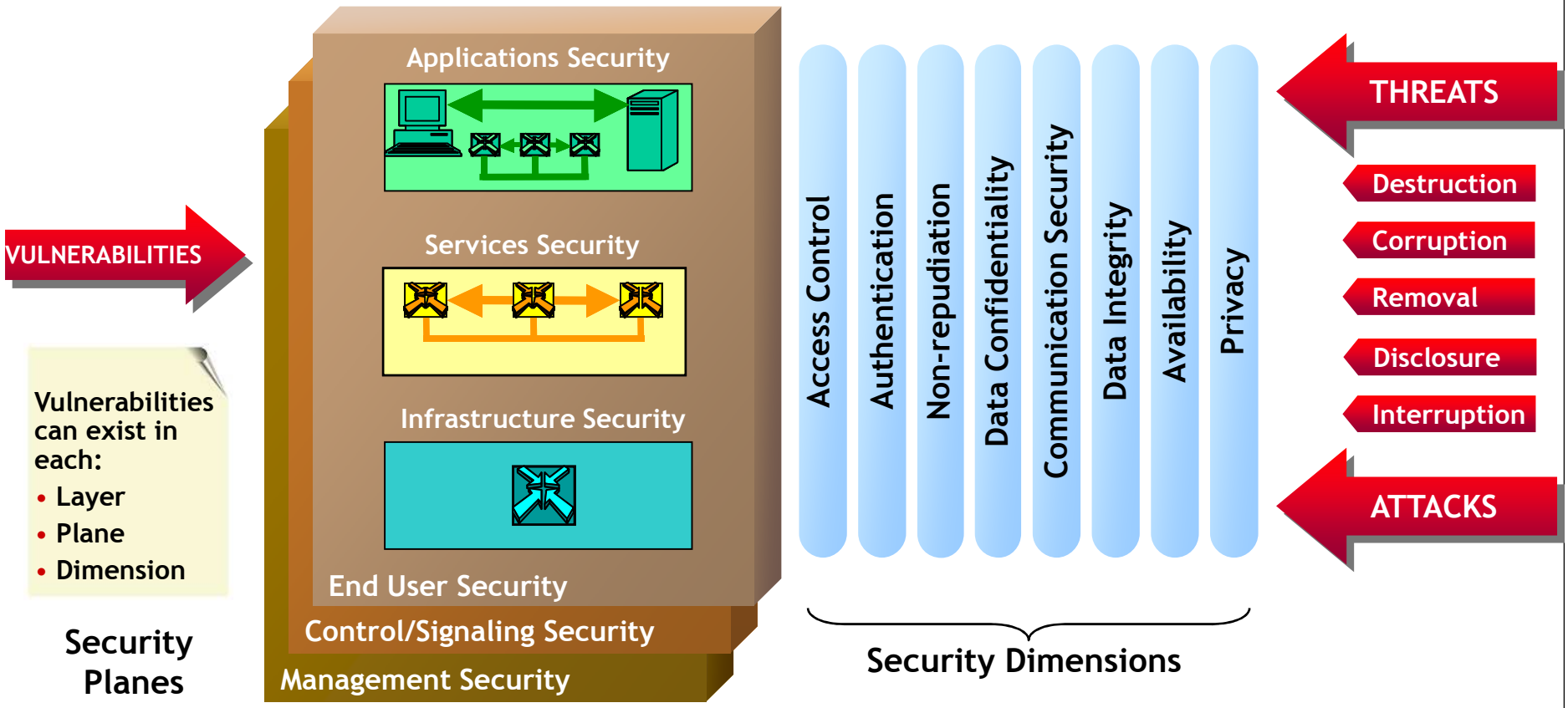
- Strong Information Security Organization
- Unambiguous & up-to-date security policies & awareness
- Identification of critical assets & risk inventory
- Adaptable information security architecture
- Testable business continuity program
- Considers security in the design and planning stage



Security is a continuous *living* process to ensure people, network, & information have the necessary protection the *businesses* require for secure, reliable day-to-day operations

Global Standard ITU-T X.805, ISO/IEC 18028-2:
A Comprehensive Network Security Framework*

*A Bell Labs Breakthrough
ITU-T X.805/ ISO, IEC 18028-2 Standard



What is ITU-T X.805?

Three Essential Questions Answered

1. What kind of protection is needed & against what threats?
2. What are the distinct types of network equipment & facility groupings that need to be protected?
3. What are the distinct types of network activities that need to be protected?

The 72 point framework provides the system-level thinking essential for the next-generation approach to security

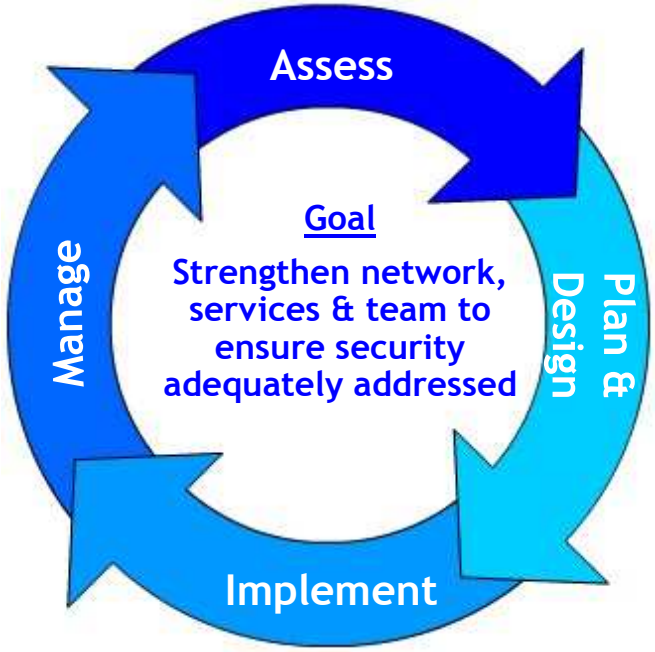
- Organizes amazing complexity into bite-sized requirements
- Comprehensiveness assures all aspects considered
- Common approach leads to shared understanding
- Standardization essential to interoperability in multi-supplier networks

End-to-End; Top Down; Comprehensive

Applies to Complete Security Life Cycle

- Systems architecture review board
- Vulnerability audits: Interviews, tests, protocol analyses
- Software robustness
- Security tools setup

- Security Awareness – checklists
- Formalize internal & 3rd party patch management
- Training
- Process for customer communication
- Incident response



- Security policy
- Prioritizing security roadmap (customer requirements , architecture gaps etc)
- 3rd-party security gaps
- Interoperability of 3rd party
- Reliability & security test strategy
- Software coding practices

- Product hardening
- Security engineering guidelines for the customer
- Technology deployment

Security Threats*

- Destruction of information and/or other resources
- Corruption or modification of information
- Theft, removal or loss of information and/or other resources
- Disclosure of information
- Interruption of services

* Defined by ITU-T X.800 (1991)
"Security Architecture for Open Systems Interconnection for CCITT Applications"

X.800 Threat Model

1. Destruction:

Destruction of information &/or other network resources

Example: (1) Malicious destruction of network equipment

2. Corruption:

An unauthorized tampering with an asset

Examples: (1) Changing network configuration information

(2) Changing data as it is being transmitted across the network

3. Removal:

Theft, removal or loss of information &/or other resources

Examples: (1) Theft of a laptop or a confidential information

4. Disclosure:

An unauthorized access to an asset

Examples: (1) Unauthorized data capture (data sniffing)

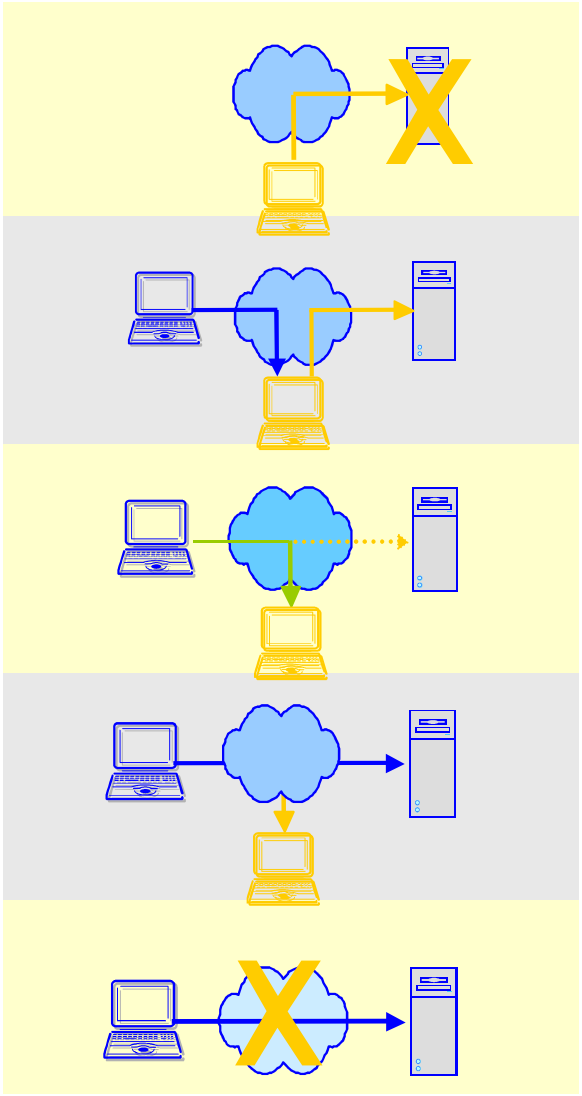
(2) Discovery of unprotected WLAN access points

5. Interruption:

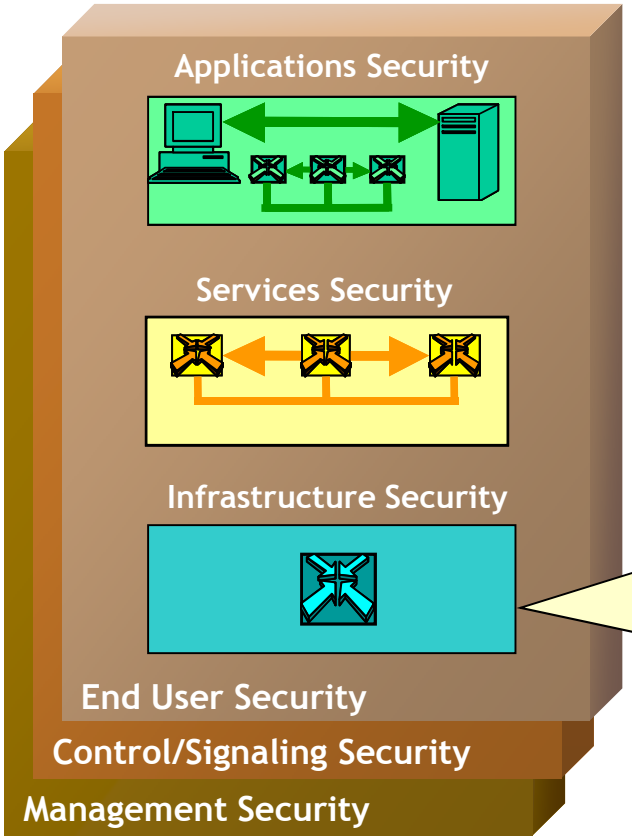
Network becomes unavailable or unusable

Examples: (1) Cutting of a communication facility

(2) Network denial of service attack



X.805: Three Security Layers



1 - Infrastructure Security Layer:

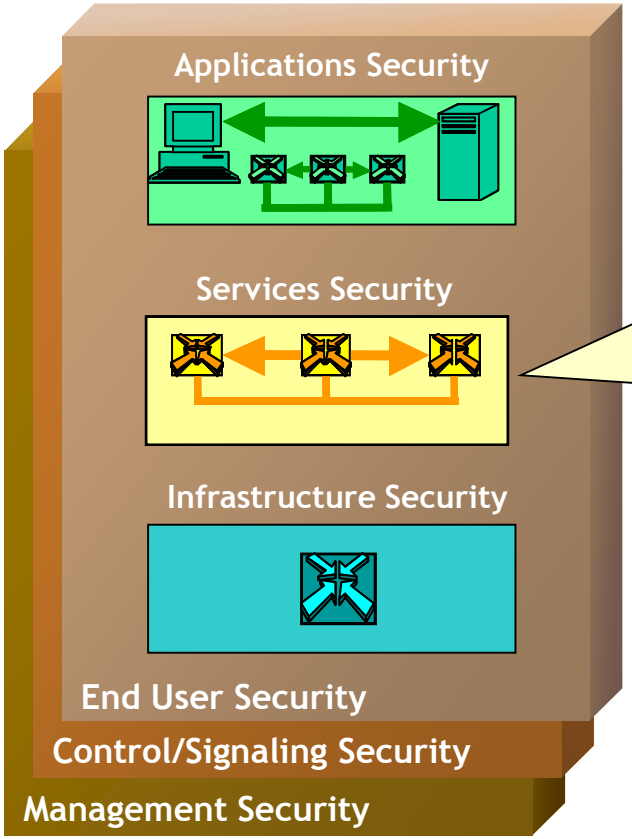
Fundamental building blocks of networks services & applications

Examples:

- Individual routers, switches, servers
- Point-to-point WAN links
- Ethernet links

- **Each Security Layer has unique vulnerabilities, threats**
- **Infrastructure security enables services security enables applications security**

X.805: Three Security Layers



2 - Services Security Layer:

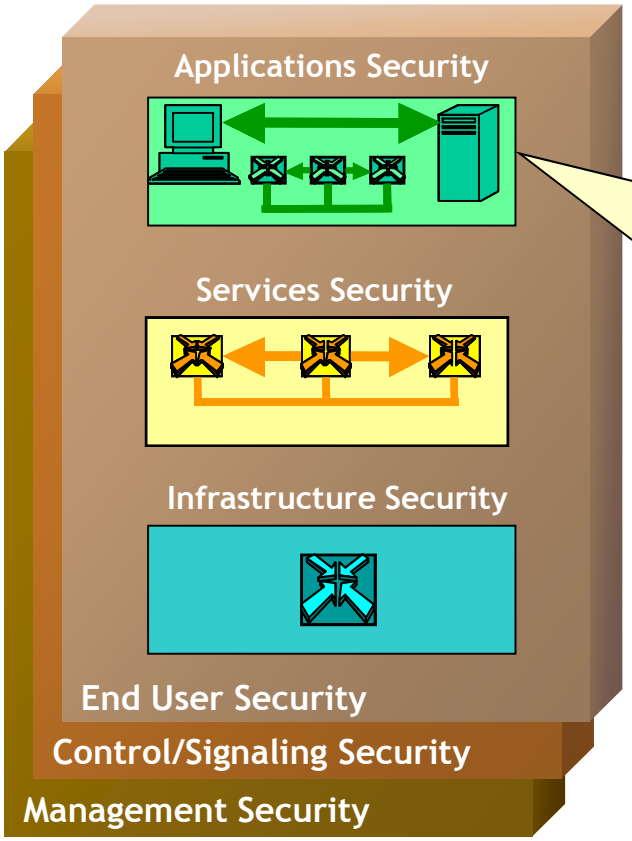
Services provided to end-users

Examples:

- Frame Relay, ATM, IP
- Cellular, Wi-Fi,
- VoIP, QoS, IM, Location services
- Toll free call services

- **Each Security Layer has unique vulnerabilities, threats**
- **Infrastructure security enables services security enables applications security**

X.805: Three Security Layers



3 - Applications Security Layer:

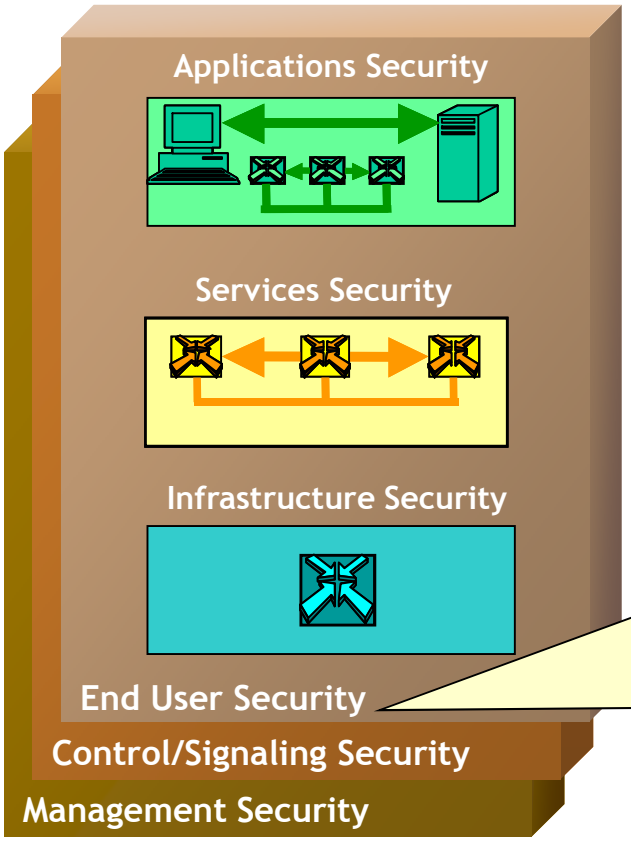
Network-based applications accessed by end-users

Examples:

- Web browsing
- Directory assistance
- Email
- E-commerce

- **Each Security Layer has unique vulnerabilities, threats**
- **Infrastructure security enables services security enables applications security**

X.805: Three Security Planes



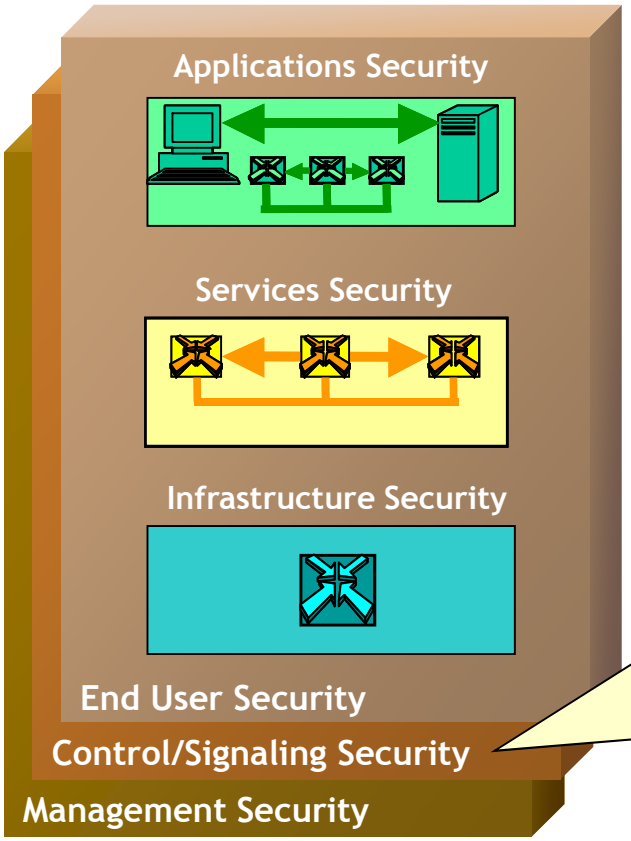
1 - End-User Security Plane:

Access & 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)

- **Security Planes represent the types of activities that occur on a network**
- **Each Security Plane is applied to every Security Layer to yield 9 security Perspectives (3 x 3)**
- **Each security perspective has unique vulnerabilities & threats**

X.805: Three Security Planes



2 - Control/Signaling Security Plane:

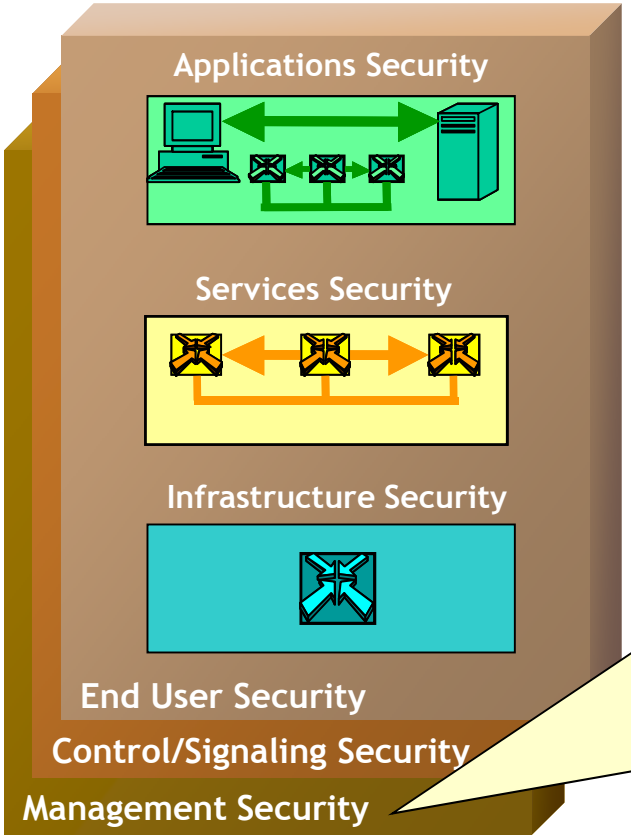
- Activities that enable efficient functioning of the network
- Machine-to-machine communications

Examples:

- Call or session set up (e.g., Session Initiation Protocol-SIP)
- QoS signalling
- Real Time Protocol (RTP), Border Gateway Protocol (BGP)

- **Security Planes represent the types of activities that occur on a network**
- **Each Security Plane is applied to every Security Layer to yield 9 security Perspectives (3 x 3)**
- **Each security perspective has unique vulnerabilities & threats**

X.805: Three Security Planes



3 - Management Security Plane:

- The management & provisioning of network elements, services & applications
- Support of the FCAPS functions

Examples:

- Network operations or management
- Network elements
- Transmission facilities
- Back-office systems
- Data centers

Management plane supports the FCAPS model (Fault, Capacity, Administration, Provisioning, Security)

- **Security Planes represent the types of activities that occur on a network**
- **Each Security Plane is applied to every Security Layer to yield 9 security Perspectives (3 x 3)**
- **Each security perspective has unique vulnerabilities & threats**

Security Dimensions

8 Security Dimensions Address the Breadth of Network Vulnerabilities

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

Access Control:

- Ensures access by authorized personnel & devices only
- Protects against unauthorized use of network resources

Mechanisms:

- Simple log-in/password
- Access Control Lists (ACL)
- Intrusion Detection Systems (IDS)

In addition, Role Based Access Control (RBAC) provides different levels of access control to guarantee that only authorized individuals & devices can only access information

Security Dimensions

8 Security Dimensions Address the Breadth of Network Vulnerabilities

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

Authentication:

- Confirms the identity of communicating entities (e.g., end-users, OA&M activity, network elements)
- Ensures validity of claimed entities
- Provide assurance that an entity is not masquerading

Mechanisms:

- Digital certificates
- Digital Signatures
- SSL
- SSO
- CHAP

Security Dimensions

8 Security Dimensions Address the Breadth of Network Vulnerabilities

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

Non-repudiation:

- Prevents an individual or entity denying having performed an action
- Ensures availability of evidence that can be presented to a third party, an event/incident has taken place

Mechanisms:

- Logs
- Role based access control
- Digital signatures

Security Dimensions

8 Security Dimensions Address the Breadth of Network Vulnerabilities

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

Data Confidentiality:

- Protects data from unauthorized disclosure
- Ensures data content cannot be understood by unauthenticated entities

Mechanisms:

- Encryption (3DES, AES)
- Access control lists
- File permissions

Security Dimensions

8 Security Dimensions Address the Breadth of Network Vulnerabilities

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

Communication Security:

- Ensures information only flows between the authorized end points
- Ensures information is not diverted or intercepted as it flows between these end points

Mechanisms:

- VPNs (IPSec, L2TP)
- MPLS tunnels
- Private Lines
- Separate networks

Security Dimensions

8 Security Dimensions Address the Breadth of Network Vulnerabilities

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

Data Integrity:

- Ensures the correctness or accuracy of information
- Ensures data is protected from unauthorized modification, deletion, creation & replication
- Provides an indication that this has occurred

Mechanisms:

- IPSec HMACs (e.g. MD5, SHA-1)
- Cyclic redundancy checks
- Anti-Virus Software

Security Dimensions

8 Security Dimensions Address the Breadth of Network Vulnerabilities

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

Availability:

- Ensures no denial of authorized access to network elements, stored information, information flows, services, application
- Disaster recovery solutions are included in this category

Mechanisms:

- Redundancy & back-up
- Firewalls, IDS/IPS (for blocking DoS)
- Business continuity
- Managed network & services with SLAs

Security Dimensions

8 Security Dimensions Address the Breadth of Network Vulnerabilities

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

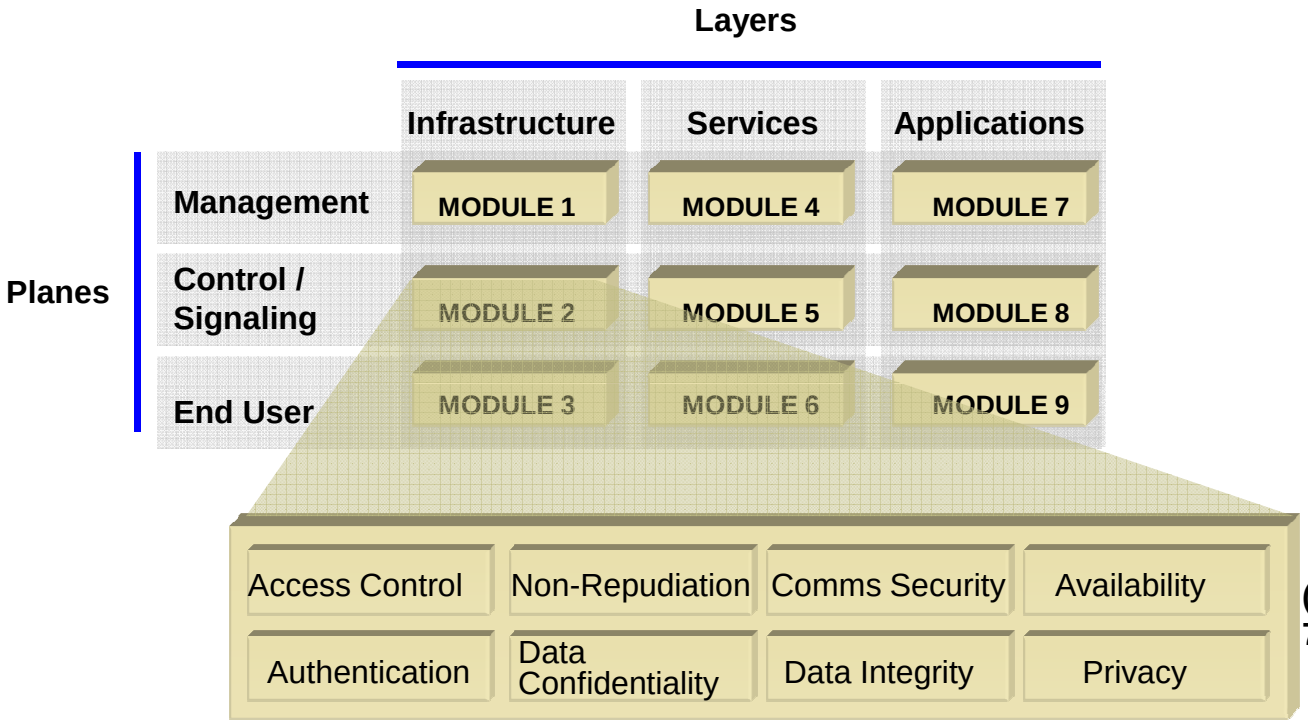
Privacy:

- Provides protection of information that might be derived from network activities

Mechanisms:

- Proxies
- Encryption of IP headers (for example: IPSec VPNs)
- NAT

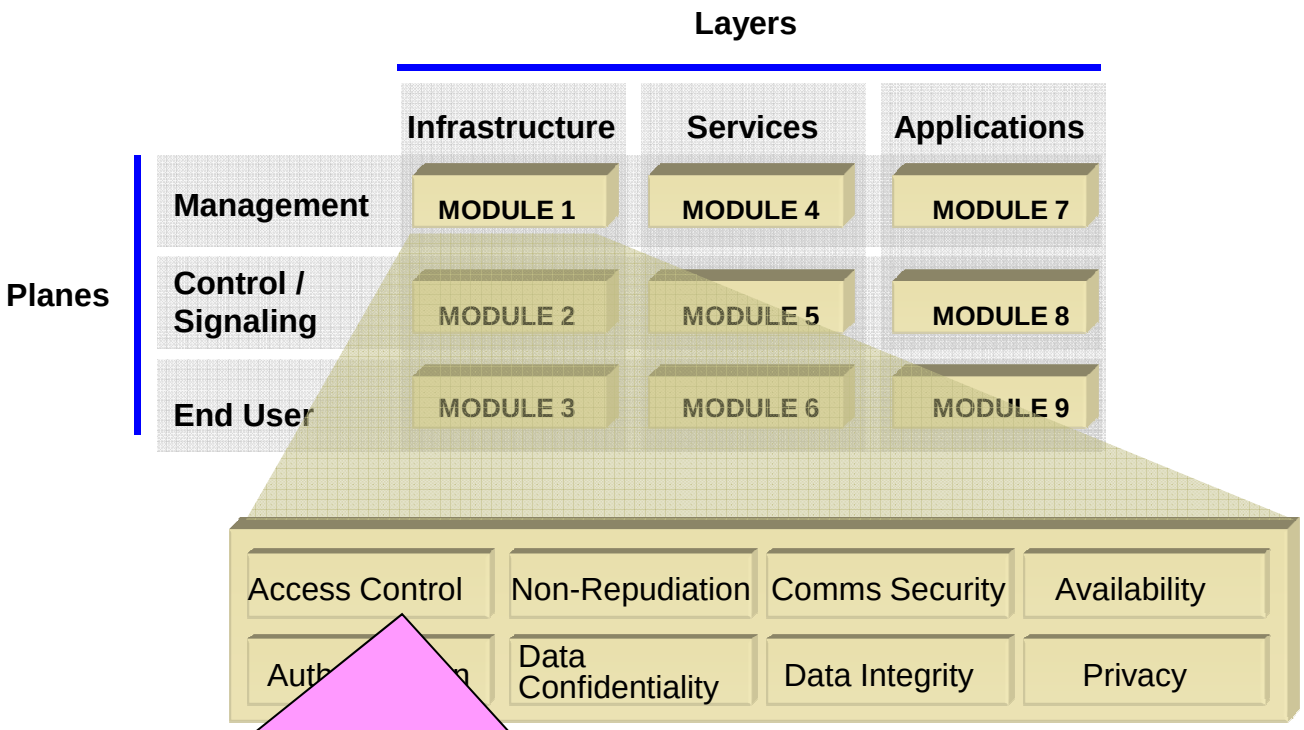
A Comprehensive Security Framework



(9 Modules X 8 Cells = 72 Security Cells)

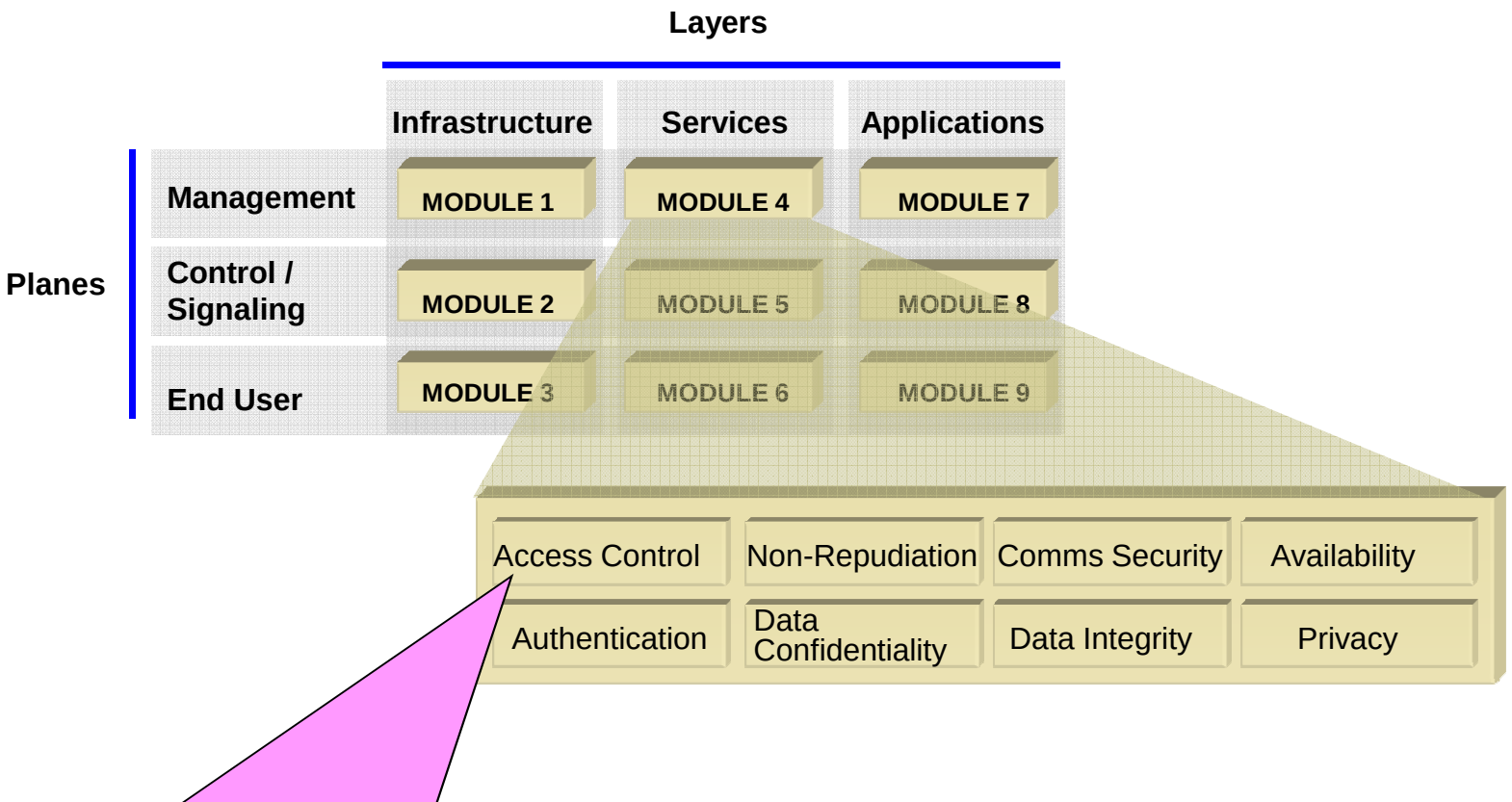
Provides a systematic, organized way for addressing network security

Applying Security Dimensions – An Example



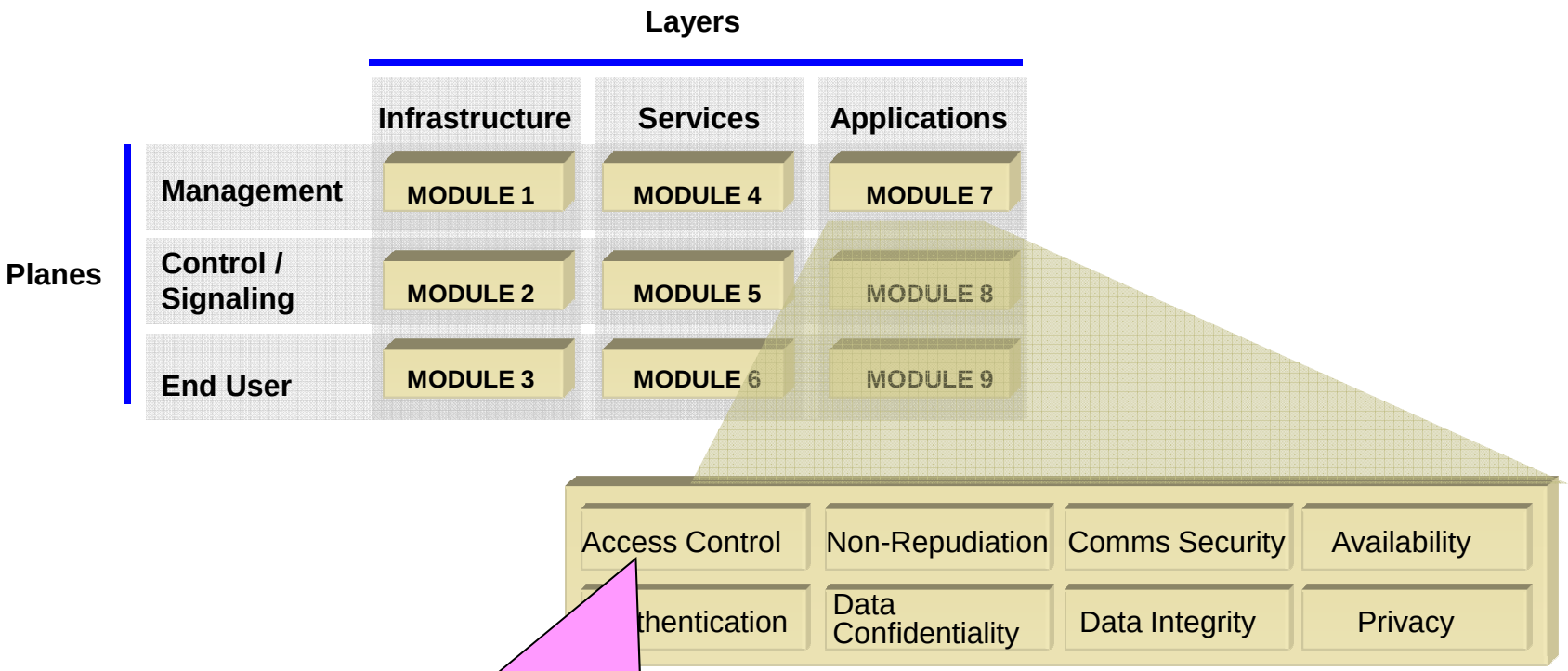
- Ensure that only authorized personnel can perform administrative/management activities on the network device or communications link
- Ensure that only authorized devices (e.g. in the case of SNMP managed devices) are allowed access
- Address both direct & remote management of device

Applying Security Dimensions – An Example



Ensure that only authorized personnel & devices are allowed to perform, or attempt to perform administrative or management activities of the network service (e.g. provision users of the service)

Applying Security Dimensions – An Example



- Ensure that only authorized personnel & devices are allowed to perform, or attempt to perform administrative or management activities of the network-based application (e.g. administer user mailboxes for an email application)

Five-Step Methodology for ITU-T X.805 Security Analysis

IPTV Example

Step 1: Define Threat Scenarios

Priority	Threat Scenario
1.	Request Flooding
2.	Malformed Requests & Messages
3.	Theft of Service
4.	Unauthorized Network Scans & Probes
5.	Eavesdropping

ISMA Internet Streaming Media Alliance

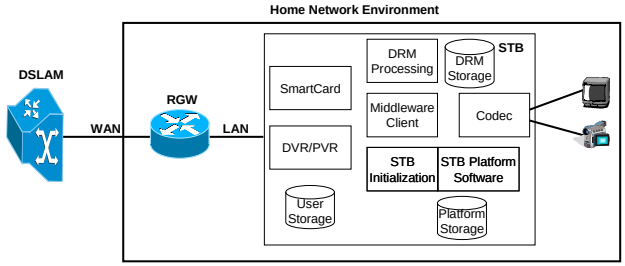
DSL FORUM

atis

Industry Fora

Step 2: Perform X.805 Asset Identification

Asset	Control Plane
Services Layer	
"A" Interface	✓
"B" Interface	✓



Network Architecture

Step 3: Perform X.805 Threat Analysis

Services Layer Threat Exposures (1)	Threat Scenarios
S-1. "A" Interface	
• Corruption:	
– Forged or altered messages	1,2,4,8
– Malformed packets	7
– Replayed packets	2,3

Threat Scenarios (from Step 1)

X.805 Layers, Planes

X.805 Threats

Step 4: Perform X.805 Vulnerability Analysis

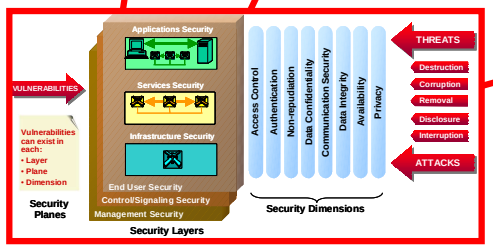
S-1. A Interface	Mitigations	Analysis
• Corruption		
• Forged or altered messages	1	TLS or IPSec provide cryptographic means to detect forged and altered messages.
• Malformed packets	2	The implementation should be robust against parser torture tests.
• Replayed packets	1	TLS or IPSec provide protection against replayed packets.

Vulnerability DBs

CarnegieMellon Software Engineering Institute CERT®Coordination Center

Sponsored by DHS National Cyber Security Division/US-CERT
National Vulnerability Database
a comprehensive cyber vulnerability resource

X.805 Dimensions



X.805

Step 5: Develop Countermeasures

Recommendations
1. Secure the transport layer (Layer 4) or network layer (Layer 3) using technologies such as TLS or IPSec.
2. Develop parser torture test
3. ACLs and DoS firewalls/routers

Standards Orgs.

IETF

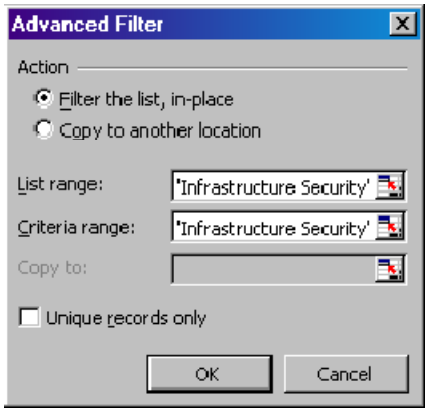
ITU

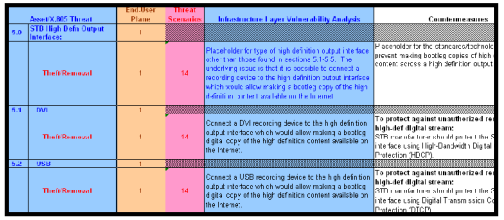
Alcatel·Lucent

X.805 Analysis Spreadsheet is Easily Extensible and Customizable

Contains the Five-Step Methodology

- Step One – Threat Scenario Tab.
- Steps Two through Five Performed in Each Layer's Tab – Infrastructure Security, Services Security, and Applications Security:
  - Step 2: Asset Identification – Columns A – C.
  - Step 3: Threat Analysis – Columns D – Z.
  - Step 4: Vulnerability Analysis – Column AA.
  - Step 5: Countermeasures – Columns AB – AL.
- Key Statistics and Graphs Provided in Spreadsheet.
- Advanced Filtering Capability Allows Users to Customize Each Layer Based on any Combination of Planes, Threat Scenarios, Security Dimensions:





IPTV Security Analysis

Management Plane	Control Plane	End-User Plane
1		
	1	

Filter Criteria – Selects Management Plane and Control Plane

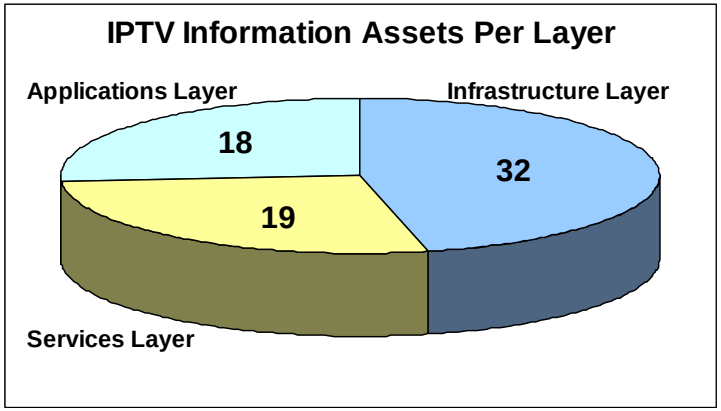
Step One: Threat Scenarios

IPTV Example

	Threat	Priority
1.	Theft of Service	High
2.	Packet Flood/Traffic Flood	High
3.	Malformed Packets and Messages	High
4.	Compromise of Installed Software, Service-Related Data, System Configuration	High
5.	Unauthorized Network Scans and Probes	High
6.	Theft of Content	High
7.	Invasion of Subscriber Privacy/Eavesdropping	Medium
8.	Spoofed Messages	Medium
9.	Underlying Platform DoS	Medium
10.	Resource Exhaustion	Medium
11.	Compromise of Subscriber Information	Medium
12.	Unauthorized Management	Medium
13.	Misrepresenting Authority and Rights	Low
14.	Interception and Modification	Low
15.	Compromise of Subscriber Application Data	Low
16.	Access to Inappropriate Content	Low
17.	IPTV Hijacking and Service Masquerading	Low

Step Two: Asset Identification

IPTV Example

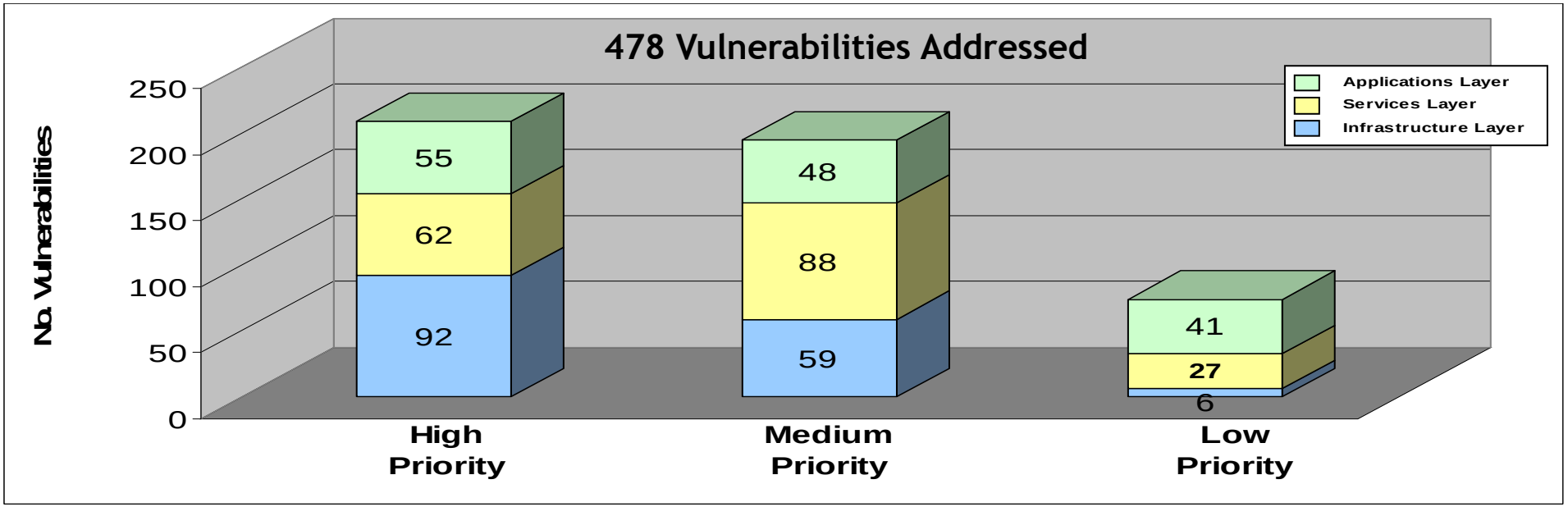


69 Information Assets Identified

- STB, Residential Gateway Platforms and Operating Environments
- DRM and Application Storage - EPG
- Credentials and Digital Certificates
- Content Rights and Decryption Keys
- High Definition Interfaces
- IPTV Usage, Billing and Purchasing Information
- Audience Metering Information
- Multicast Control Protocols (IGMP, PIM, MSDP)
- Multicast Transport Protocols (RTP, SRTP, RSVP)
- Management Protocols (CWMP, NTP)
- MPEG Content
- VOD, PVR/DVR Control Protocols (DSM-CC, RTSP)

Steps Three and Four: Threat and Vulnerability Analysis

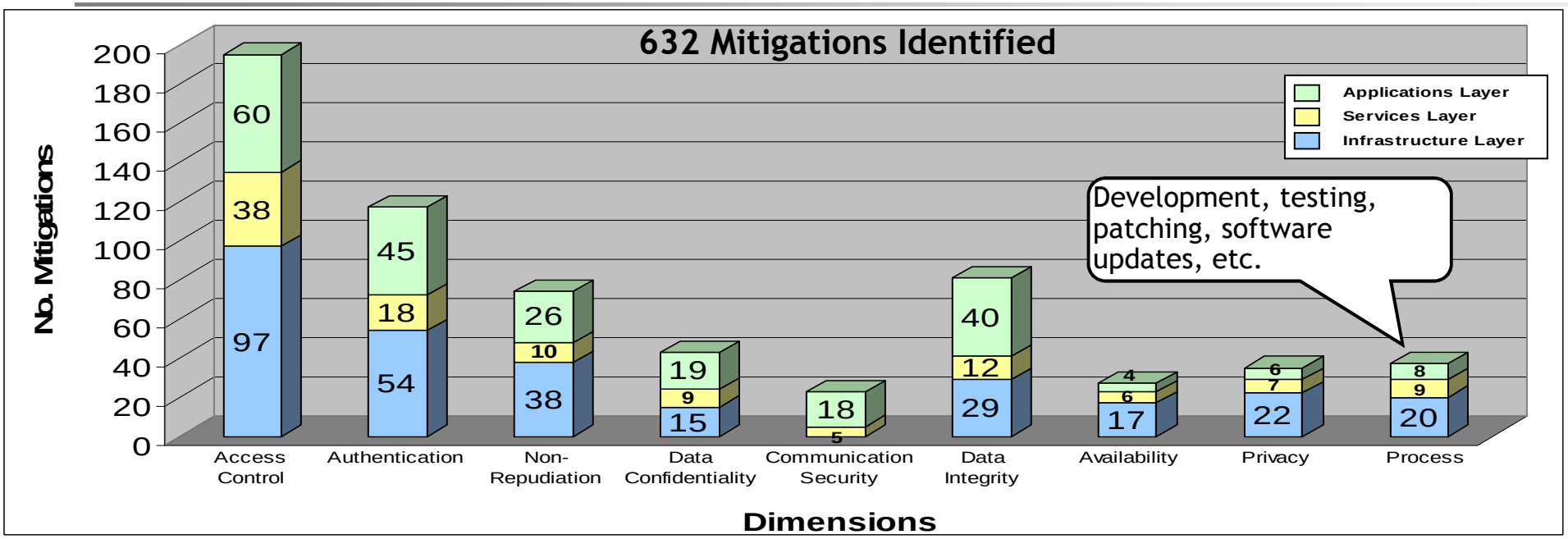
IPTV Example



- Content Stored/Transmitted in Plaintext
- Credentials, Content Rights, Decryption Keys Accessible
- Forged/Malformed Multicast Control Packets (IGMP, PIM, MSDP) –
  - Traffic Deflection
  - Multicast Group Membership Suppression
  - MSDP Storms
- Forged Management Packets (CWMP)
- Forged RSVP Packets, DiffServ QoS Attack
- Billing, Purchasing Information Accessible
- High Definition Interfaces Unprotected
- Unprotected Admin IDs
- Rootkits, Malware, Spyware
- Illegitimate Protocol Port Allocation
- Forged/Malformed VOD/PVR Control Packets (DSM-CC, RTSP)

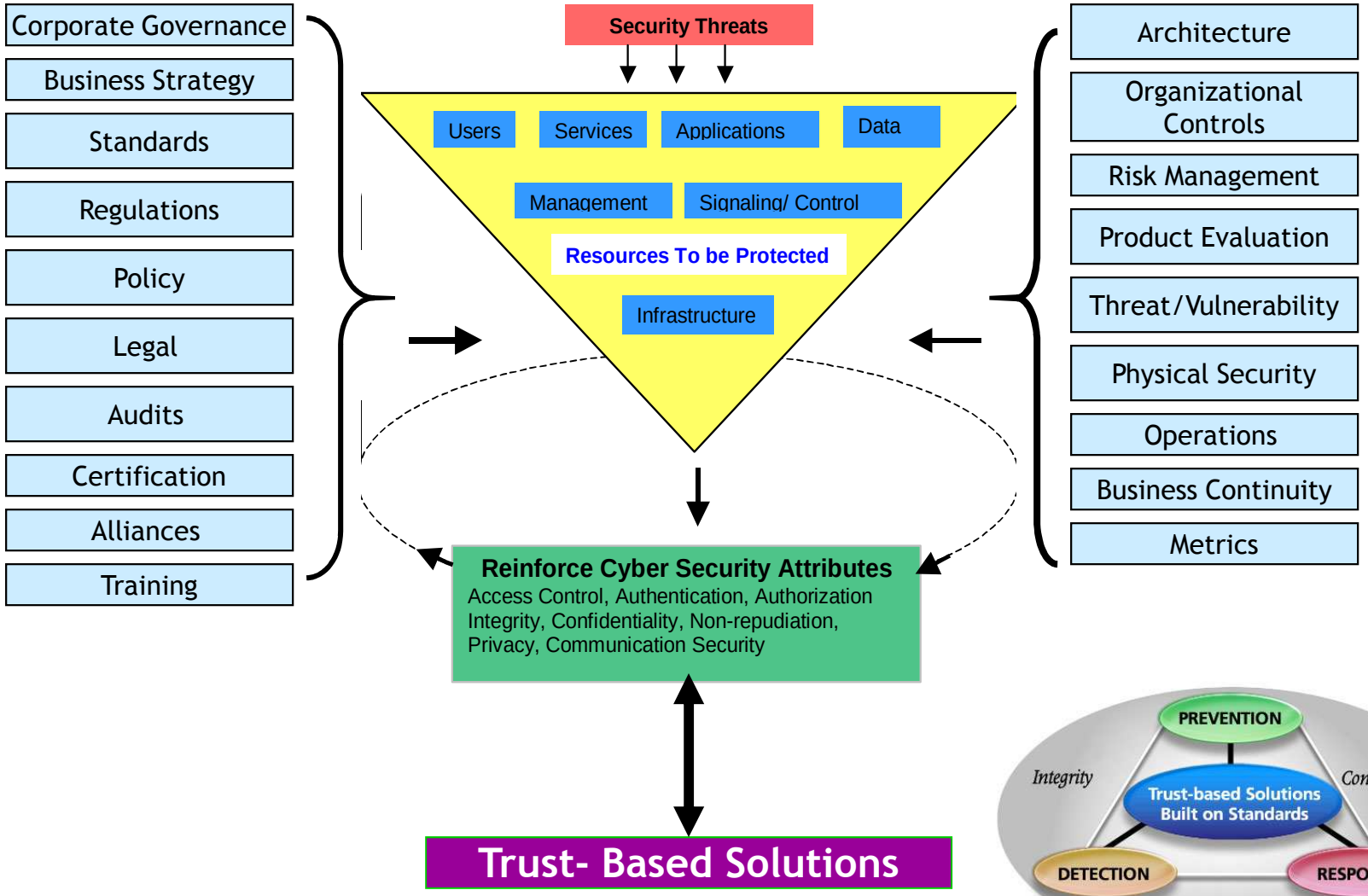
Step Five: Countermeasures

IPTV Example



- Protect MPEG-2 Content w/ Vendor-Specific Encryption
- Protect MPEG-4 Content w/ ISMACryp
- Implement File System Access Controls in STB and DSLAM
- Utilize IGMPv3 instead of IGMPv2
- Use Transport Layer Security to Protect IGMP, PIM, DRM Traffic
- Implement Source Specific Multicast
- Deploy Application-Aware, Rate-Limiting Firewalls
- Transport CWMP via SSL/TLS (i.e., HTTPS)
- Enable RSVP Cryptographic Authentication (i.e., HMAC-MD5)
- Encrypt Usage and Billing Information; Utilize Digital Certificates and Digital Signatures
- Protect High Def Interfaces with DTCP or HDCP
- Deploy HIDS, NIDS
- DHCP Snooping, Port Authentication
- Enable DSM-CC/RTSP Authentication or Protect via Transport Layer Security

Using X.805 for Trust-Based Solutions

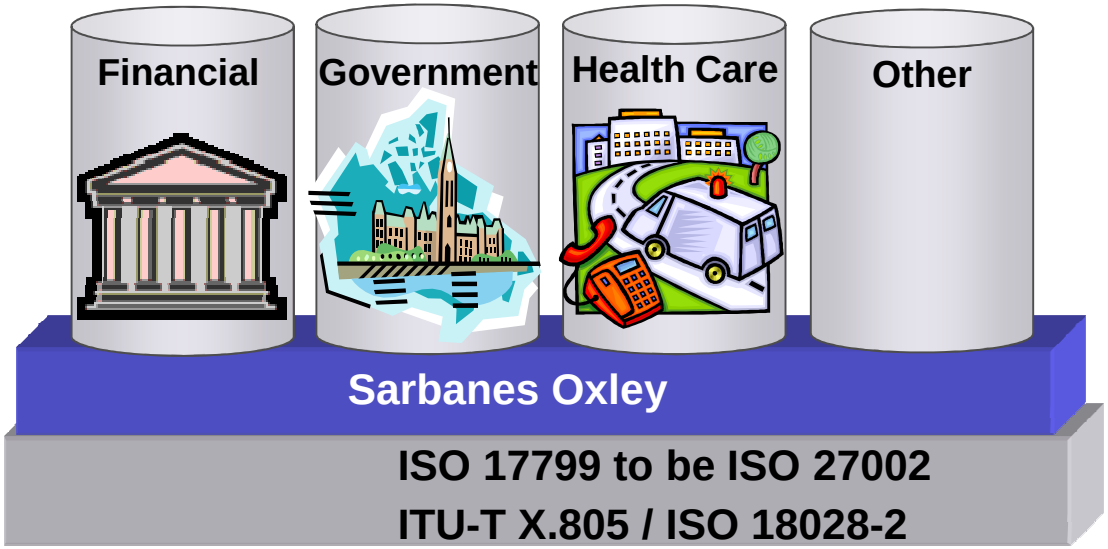


Alcatel·Lucent

Regulatory Compliance

The ISO 17799/ISO 27002 standard prepares organizations for industry specific regulations and standards:

- **Financial:** BASEL II; GLBA
- **Health Care:** eHealth; HIPAA
- **Government:** CSE;



A common framework to adapt to emerging industry requirements

HIPAA – Health Insurance Portability and Accountability Act
GLBA – Gramm-Leach Bliley Act
CSE - Communications Security Establishment

Standards approach provides foundation

Regulatory Compliance & Network Security

Example: Sarbanes-Oxley Section 404
Management Assessment of Internal Controls

- Management must establish effective internal controls for accurate & complete reporting
- Annual assessment by management of the effectiveness of internal controls supported by documented evidence
- Validation of management's assessment by a registered public accounting firm

Systems, data & infrastructure components are critical to the financial reporting process.

Enablers for Reliable Financial Reporting

- Information management & data classification
- Information security (access control, authentication, identity management, cryptography, etc.)
- Real-time reporting & audit logs
- Data processing integrity & validation

Network Security Requirements

Need comprehensive end-to-end network security analysis

Synergy Between ISO/IEC 27001:27005 & ITU-T X.805 / ISO,IEC 18028-2

The combination of ITU-T X.805 / ISO/IEC 18028-2 and ISO 27000 address business, and technical risks associated with information and network security

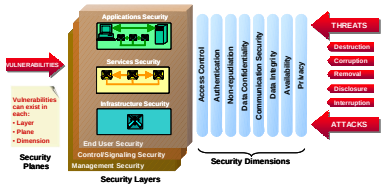
ISO/IEC 27001:27005

- Provides standards for implementing, maintaining and improving an Information Security Management System to manage risk within the context of an organization's overall business environment.

	PLAN	DO	CHECK	ACT
27001	✓	✓	✓	✓
27002 (controls)	✓	✓		
27003 (Implementation)		✓		✓
27004 (Measurements)		✓	✓	
27005 (Risks)	✓		✓	
27006 (Accreditation + certification)	✓	✓	✓	✓
Sector Specific Requirements & Guides (Telecom, healthcare ...)	✓	✓	✓	✓

ITU-T X.805/ ISO,IEC 18028-2

- Provides standards for detailed technical design, architecture, requirements, and test plans for the end-to-end network security solutions or individual products



ISMS = Information Security Management Systems

Conclusion

Business Imperatives		Security Drivers	End-User Needs
Minimize Downtime & Enhance Productivity		**Maintain peak efficiency and effectiveness by** … protecting your staff and data from threats … quickly recognizing and mitigating security incidents … more efficiently managing your network and security	"Conduct business anytime"
Provide trustworthy service		**Provide highly-available, quality services by** … controlling the impact of attacks on customer data … maintaining regulatory compliance to enable operation … alleviating privacy concerns	"Protected personal information"
Operate cost-effectively		**Control risks while managing costs by** … relying on proven, best-in-class solutions … leveraging external capabilities and staff … avoiding losses, liability, and fines	"Secure services now at a competitive price"
Build for the future		**Create a business that can evolve securely by** … encouraging customer loyalty via a secure reputation … ensuring on-going reliability and availability … allowing for smooth migration to new technologies	"Seamless, fast evolution to hot new features"