ITU-T X.805 Workshop
IMF 2007
Stuttgart, Germany
September 13, 2007

Suhasini Sabnis

Bell Labs – Security Technology Application Research

Agenda

Security Drivers and Challenges

ITU-T X.805 Security Framework Overview

Using ITU-T X.805 for Security Assessment

Applying ITU-T X.805 – A Case Study

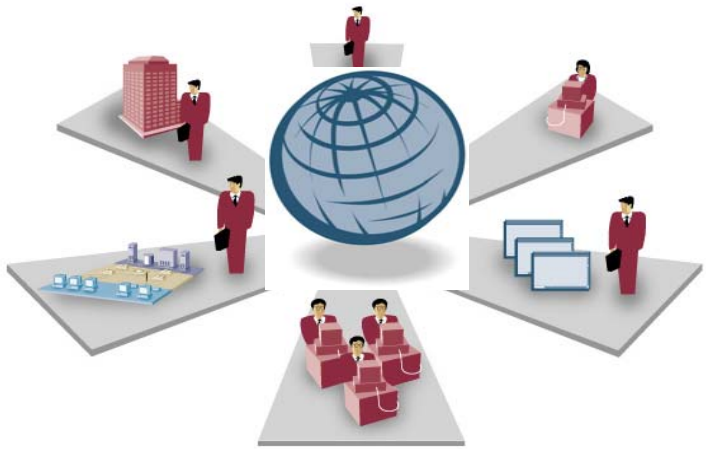
Security Standards and Security Compliance

Questions

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

All Rights Reserved © Alcatel-Lucent 2006, 2007

The Security Challenge

Security as an Opportunity

Cost Reduction

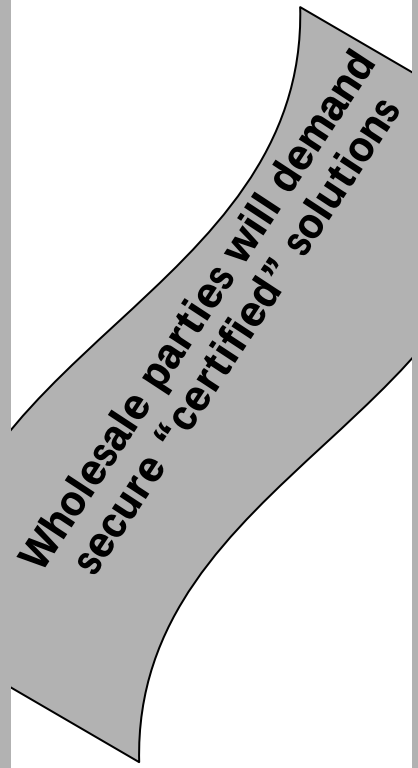
- Optimize operations and productivity
- Compliancy costs
- Lessons learned

Revenue Increase

- More competitive offering through ISO certification

Customer Satisfaction

- More reliable and protected service delivery
- Increased brand image



Security as a Risk

Business Risk

- Loss of Revenue
- Customer Churn

Regulatory

- SOX Compliancy
- EU privacy regulation
- Protection of Critical Infrastructures
- Financial segment: BASEL II

Customer Satisfaction

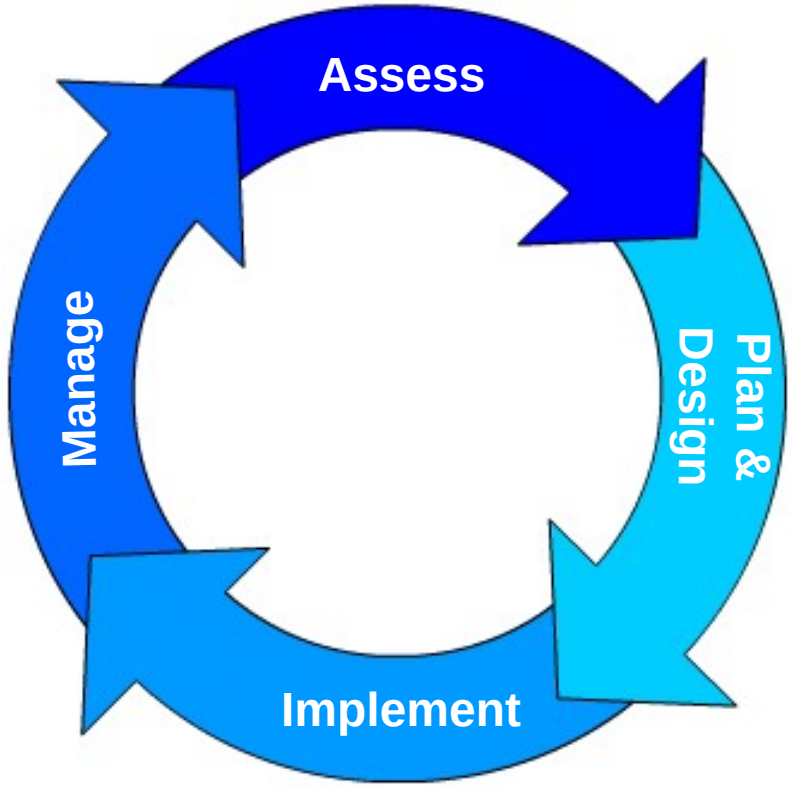
- Intrusion incidents → Higher perceived vulnerability
- Reduced brand image

Security is a Process not a Product

All Rights Reserved © Alcatel-Lucent 2006, 2007

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

All Rights Reserved © Alcatel-Lucent 2006, 2007

Primary Security Planning Considerations

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?

All Rights Reserved © Alcatel-Lucent 2006, 2007

Introducing the ITU-T X.805 Framework

The 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

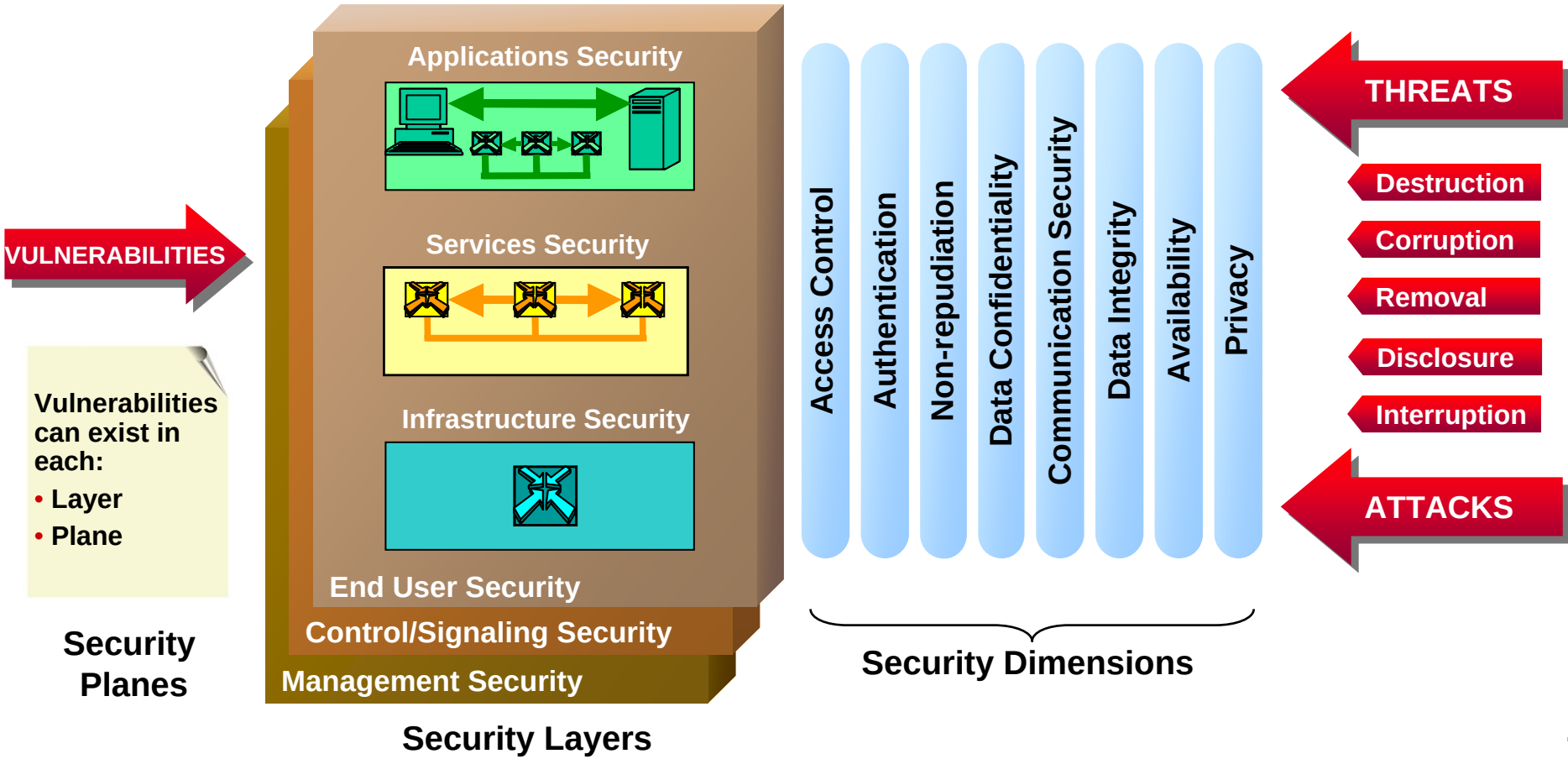
X.805 provides a framework for how complex networks can be examined in a systematic manner for security considerations

All Rights Reserved © Alcatel-Lucent 2006, 2007

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

A Comprehensive Network Security Framework*

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



All Rights Reserved © Alcatel-Lucent 2006, 2007

Alcatel·Lucent

Security Threats*

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

- 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

All Rights Reserved © Alcatel-Lucent 2006, 2007

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)

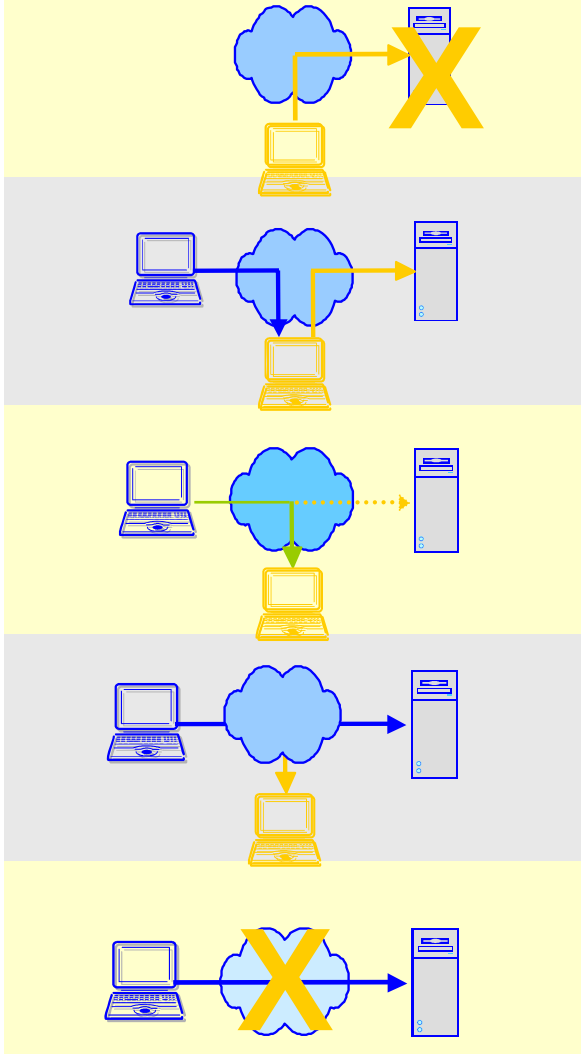
(2) Discovery of unprotected WLAN access points

5. Interruption:

Network becomes unavailable or unusable

Examples: (1) Cutting of a communication facility

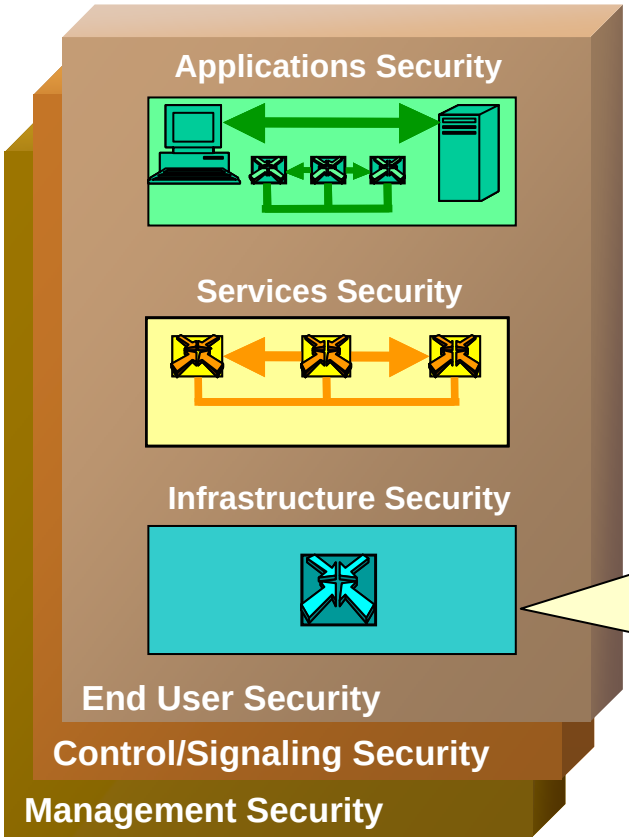
(2) Network denial of service attack



All Rights Reserved © Alcatel-Lucent 2006, 2007

Alcatel·Lucent

X.805: Three Security Layers



1 - Infrastructure Security Layer:

Fundamental building blocks of networks services & applications

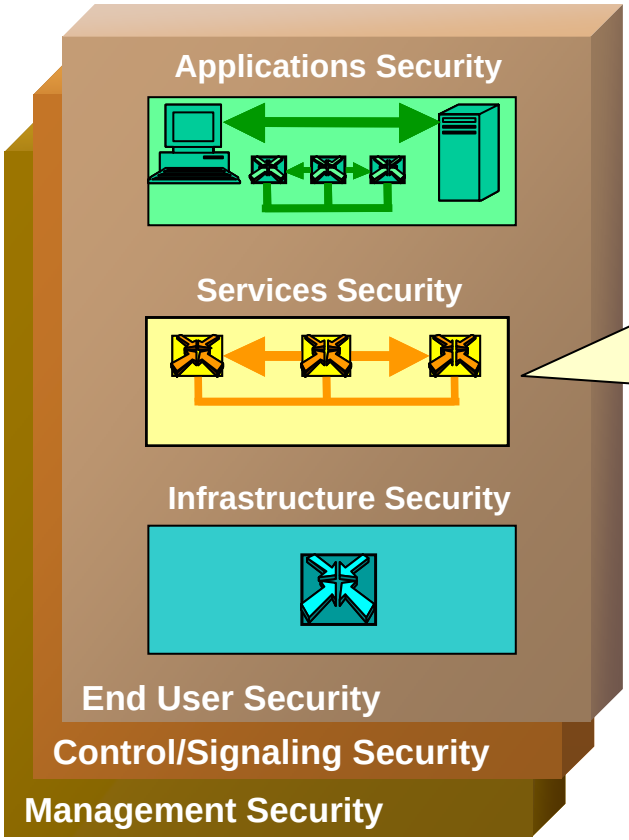
Examples:

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

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

All Rights Reserved © Alcatel-Lucent 2006, 2007

X.805: Three Security Layers



2 - Services Security Layer:

Services provided to end-users

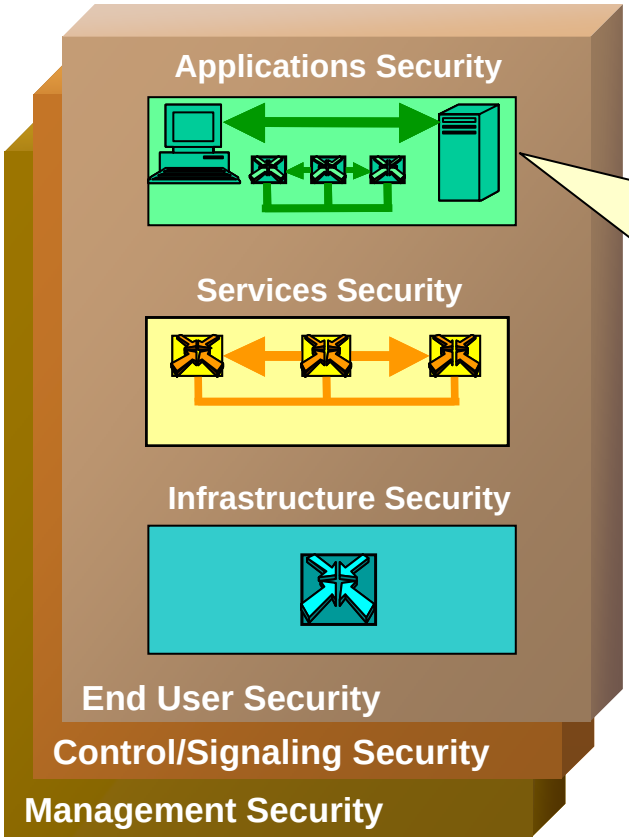
Examples:

- 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

All Rights Reserved © Alcatel-Lucent 2006, 2007

X.805: Three Security Layers



3 - Applications Security Layer:

Network-based applications accessed by end-users

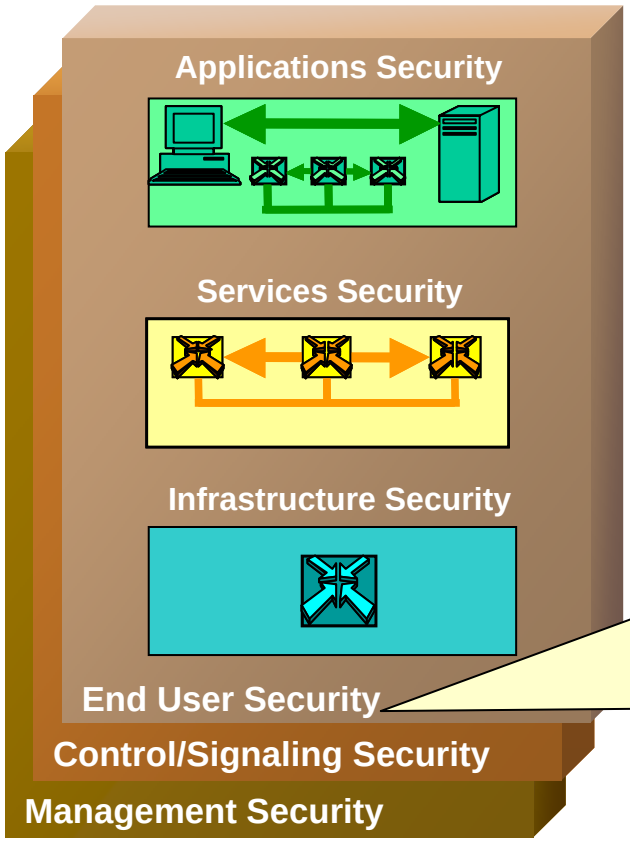
Examples:

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

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

All Rights Reserved © Alcatel-Lucent 2006, 2007

X.805: Three Security Planes



1 - End-User Security Plane:

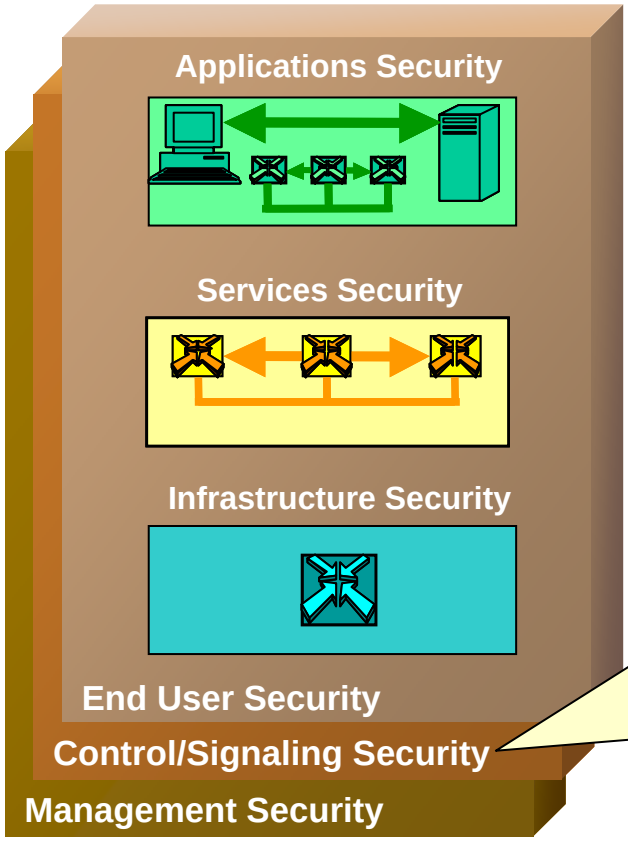
Access & use of the network by the customers for various purposes:

- 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

All Rights Reserved © Alcatel-Lucent 2006, 2007

X.805: Three Security Planes



2 - Control/Signaling Security Plane:

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

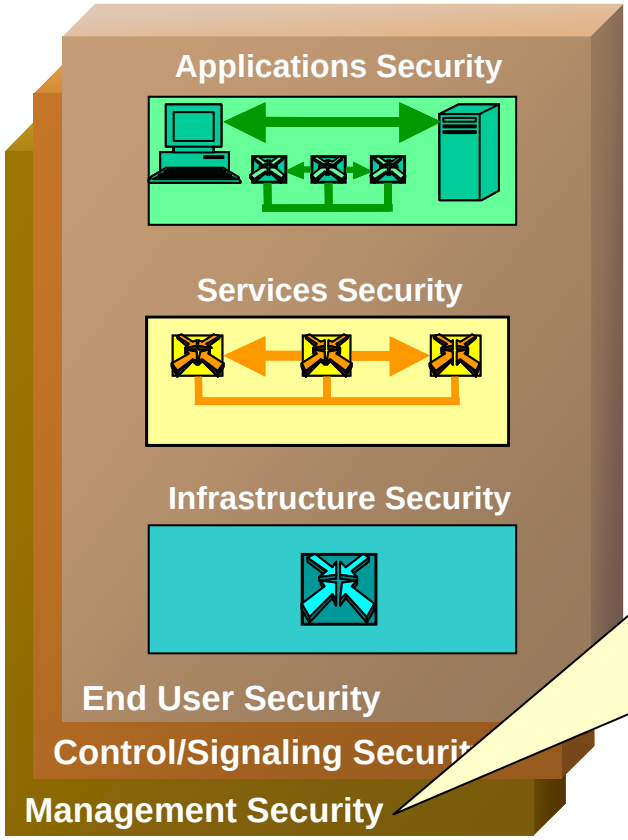
Examples:

- 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

All Rights Reserved © Alcatel-Lucent 2006, 2007

X.805: Three Security Planes



3 - Management Security Plane:

- Access and use of management & provisioning activities of network elements, services & applications by operators

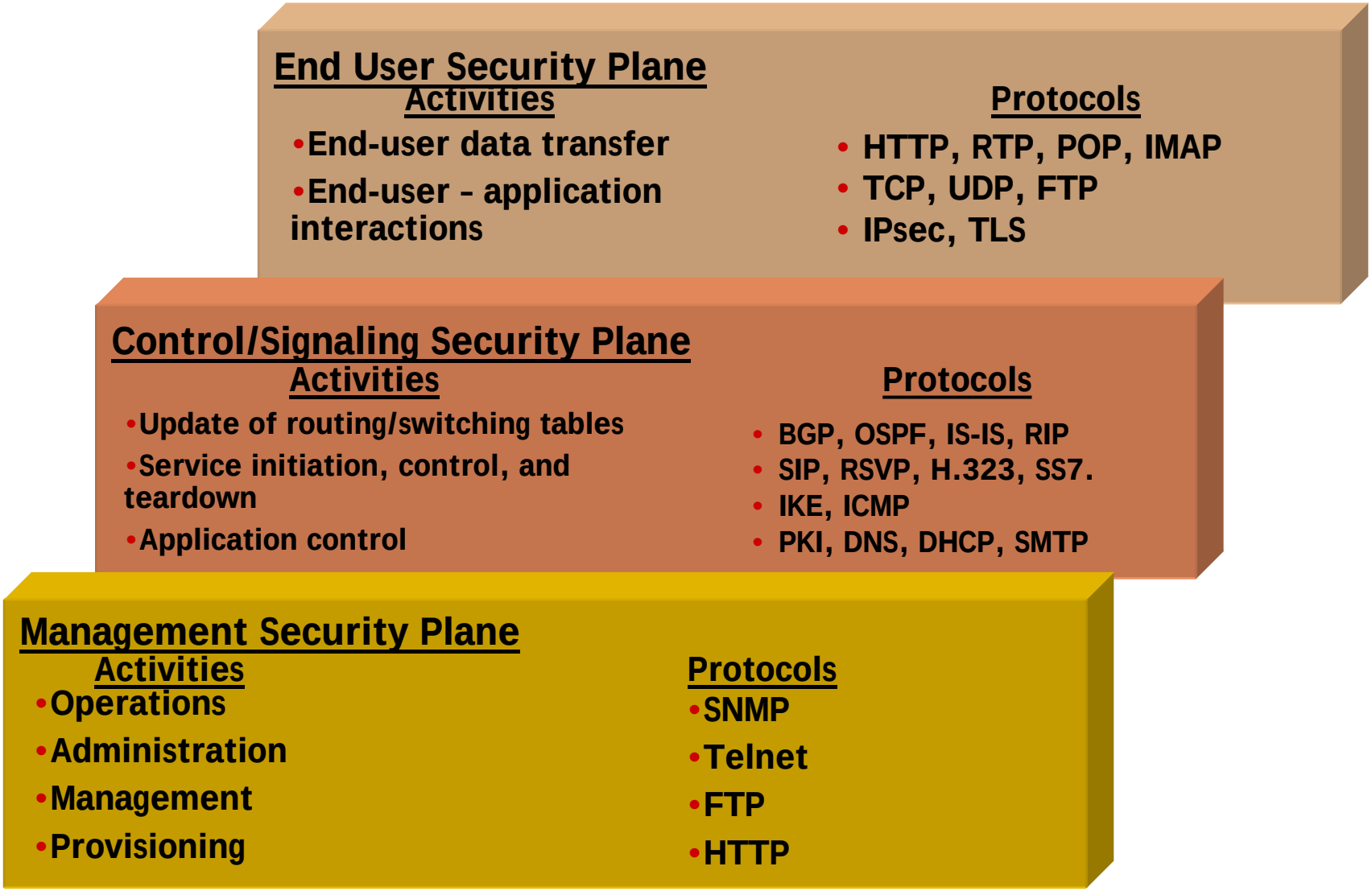
Examples:

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

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

All Rights Reserved © Alcatel-Lucent 2006, 2007

Example: Applying Security Planes to Network Protocols



All Rights Reserved © Alcatel-Lucent 2006, 2007

Using X.805 Layers/Planes – Asset Identification

Assets are identified based on the network architecture or design and the scope of work that needs to be secured; e.g., what services, applications, etc. need to be secured. **It is an iterative process.**

First step is to examine the X.805 Layers:

Infrastructure Layer: The underlying hardware, software platforms, data, transmission facilities, etc. used by the service or application. Assets include operating systems that are running as well as stored on disk, DBMS, etc.

Services Layer: The logical groupings of equipment, facilities, information that comprise services required by the application. For example, in IPTV, IP multicast is a service used by the Video-on-Demand application. Assets include multicast sources, rendezvous points, group members, etc.

Applications Layer: Systems comprising the in-scope applications, the information they generate and use, and information flows. Typically, the end-user directly interacts with these systems. In IPTV, example application is Video-on-Demand. Assets include video servers, MPEG content, video streams, etc.

All Rights Reserved © Alcatel-Lucent 2006, 2007

X.805 for Asset Identification continued

Second step is to use the X.805 Planes to uncover additional assets by examining the activities that must be protected at the management, control and end-user plane for each asset listed in the First step :

For example in an IPTV study, as part of examining IP multicast service control plane, PIM and MSDP protocols are assets that need protecting. Likewise, IGMP protocol is another asset as part of examining the IP multicast service management plane. Examining the video stream control plane, identified DSM-CC and RTSP protocols as assets that need protecting.

All Rights Reserved © Alcatel-Lucent 2006, 2007

Applying X.805 – Asset Identification

Example 1: Internet Service Provider

Plane	Infrastructure	Services	Applications
	Layer		
	Router RAS Web Servers	VPN QoS VoIP	Email Web Hosting
Management	Management GUI Command Line Interface Remote Management	User Provisioning SLA Configuration Billing/Mediation	Provisioning user mailboxes
Control	Routing Tables DNS Database	IPSec/PKI RSVP SIP	SMTP POP3 HTTP
End-User	Access Space Data Email Data	VoIP Traffic	HTTP Traffic User Credentials

All Rights Reserved © Alcatel-Lucent 2006, 2007

Example 2: Large Enterprise

Plane \ Layer	Infrastructure	Services	Applications
	Router PBX Enterprise Servers	VPN VoIP Directory Services	Order Processing NetMeeting SIP Client
Management	Management GUI Command Line Interface Remote Management	Provisioning Users Managing LDAP	Managing Upgrades (Central Distribution) Configuration of SIP clients
Control	Routing Tables DNS Database	IPSec/PKI SIP LDAP	LDAP SIP
End-User	Enterprise Hosted Data Backup of End-user PCs Voice Messages	VoIP Traffic End-User information	NetMeeting Session User Credentials

All Rights Reserved © Alcatel-Lucent 2006, 2007

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

All Rights Reserved © Alcatel-Lucent 2006, 2007

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

All Rights Reserved © Alcatel-Lucent 2006, 2007

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 unauthorized 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

All Rights Reserved © Alcatel-Lucent 2006, 2007

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

All Rights Reserved © Alcatel-Lucent 2006, 2007

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

All Rights Reserved © Alcatel-Lucent 2006, 2007

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

All Rights Reserved © Alcatel-Lucent 2006, 2007

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

All Rights Reserved © Alcatel-Lucent 2006, 2007

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

All Rights Reserved © Alcatel-Lucent 2006, 2007

Rationale for ITU-T X.805 Dimensions Relative to C-I-A

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

Authentication: Proving a person's identity (e.g., userID, password) does not fit into confidentiality, integrity, availability.

Non-repudiation: Being able to unequivocally associate an entity with an action. Identifying the authorized person that performed an unauthorized action on protected data has nothing to do with the data's confidentiality, integrity, availability.

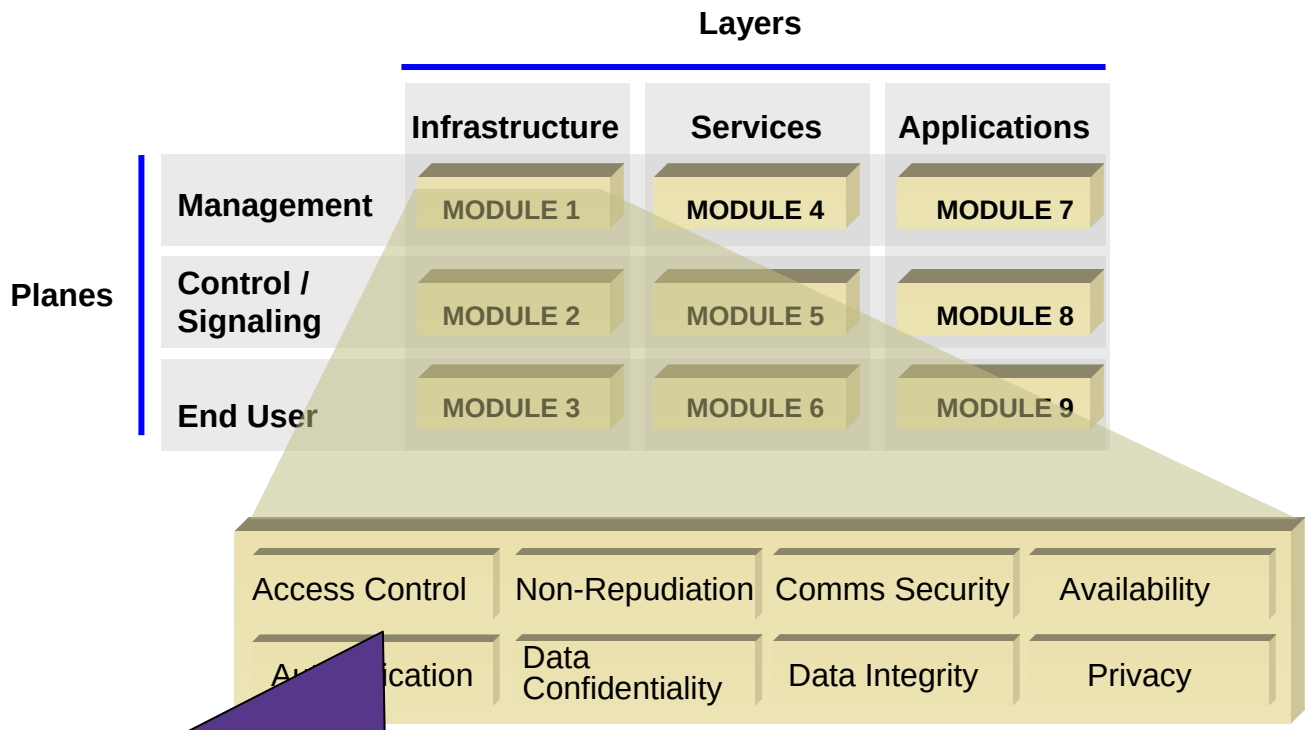
Access control: Placing a lock on a door to prevent someone from entering a hazardous location has nothing to do with confidentiality, integrity or availability.

Privacy: Privacy recognizes the need to protect actions in addition to information. Protecting information is addressed by confidentiality. Protecting the conversation in a phone call between Pat Russo and John Chambers protects their confidentiality. Protecting the fact that Pat Russo and John Chambers had a phone call protects their privacy.

Communications Security: Protecting against call black-holing has nothing to do with confidentiality, integrity, availability.

All Rights Reserved © Alcatel-Lucent 2006, 2007

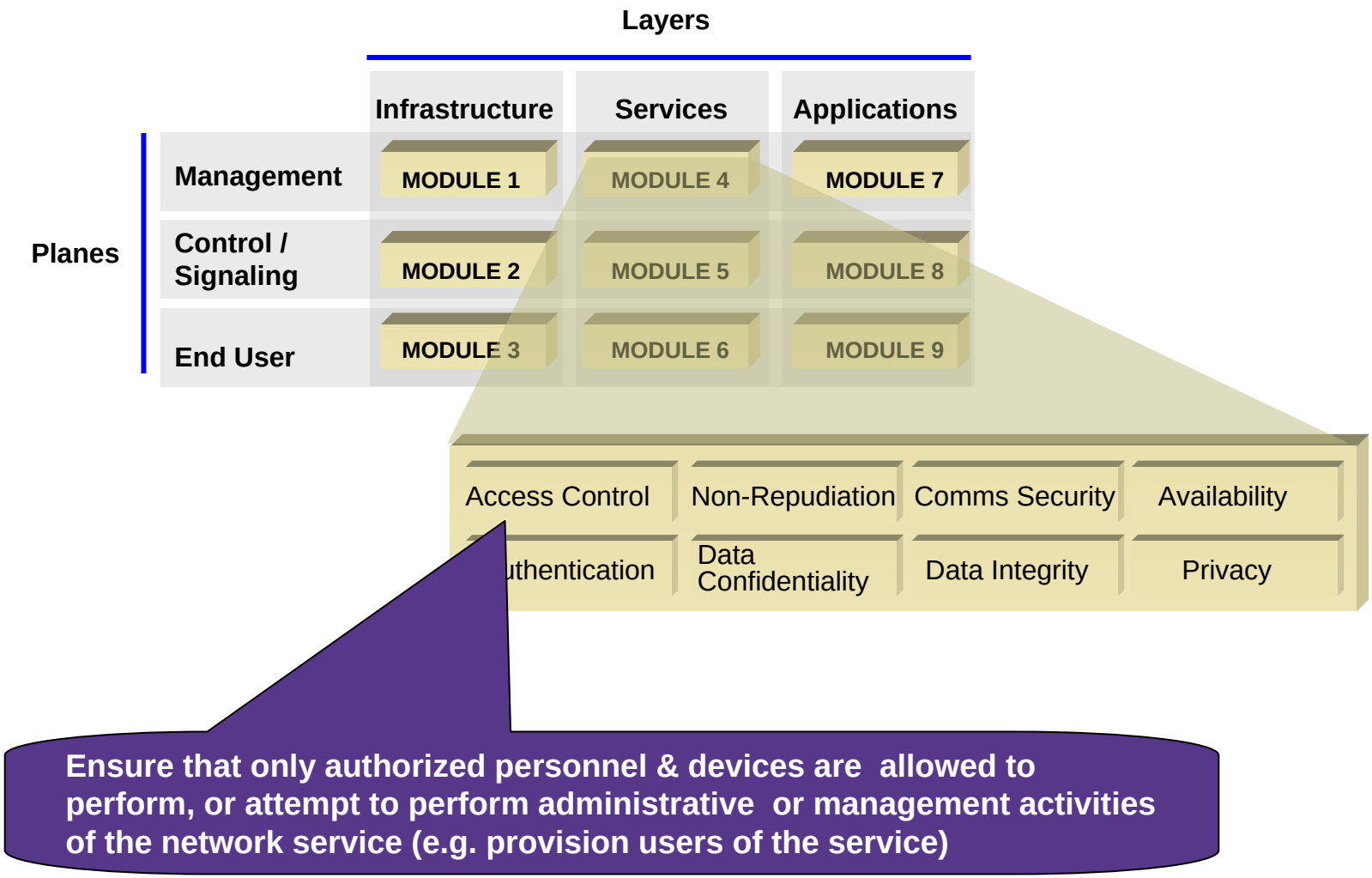
Applying Security Dimensions – An Example



- 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

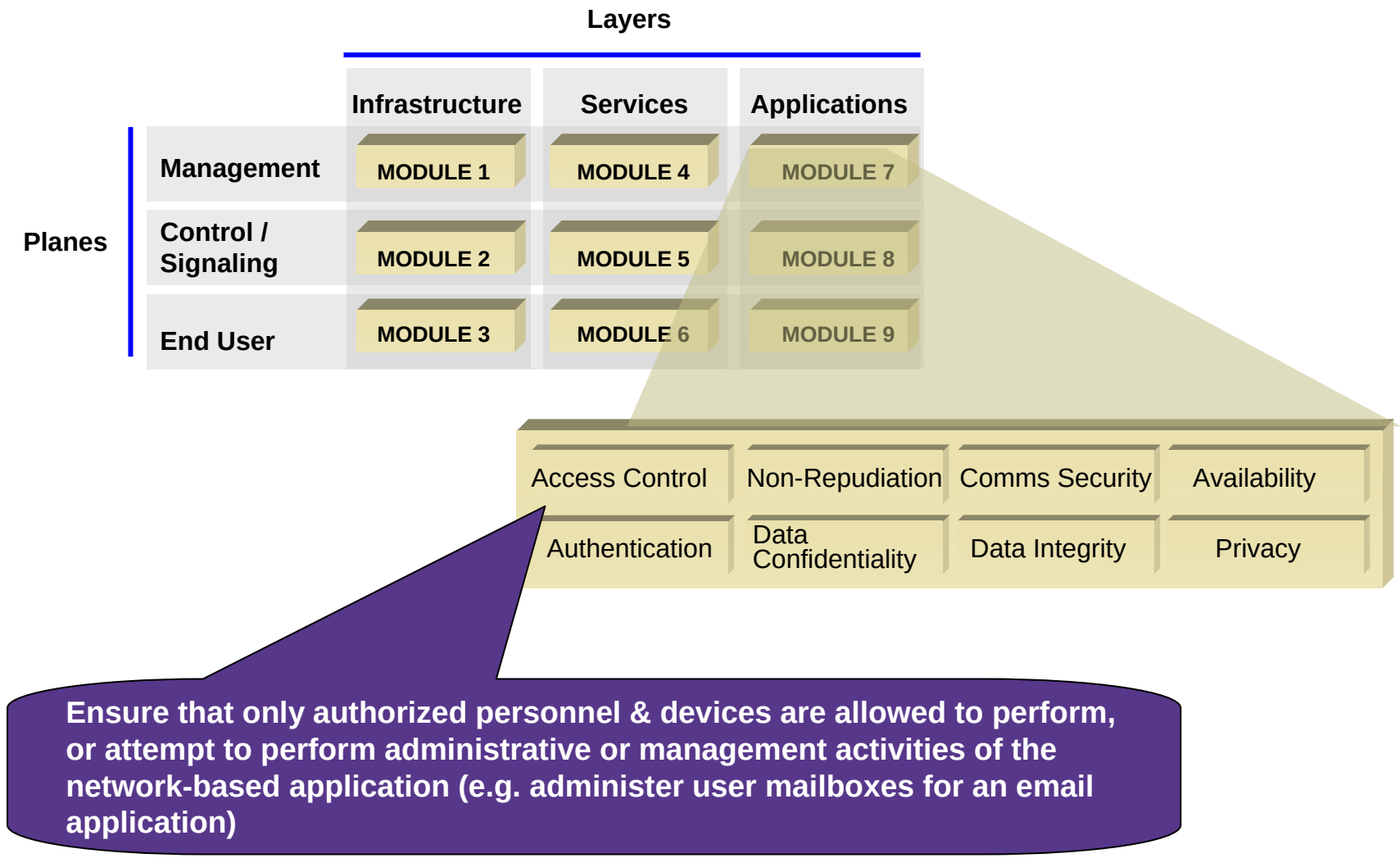
All Rights Reserved © Alcatel-Lucent 2006, 2007

Applying Security Dimensions – An Example



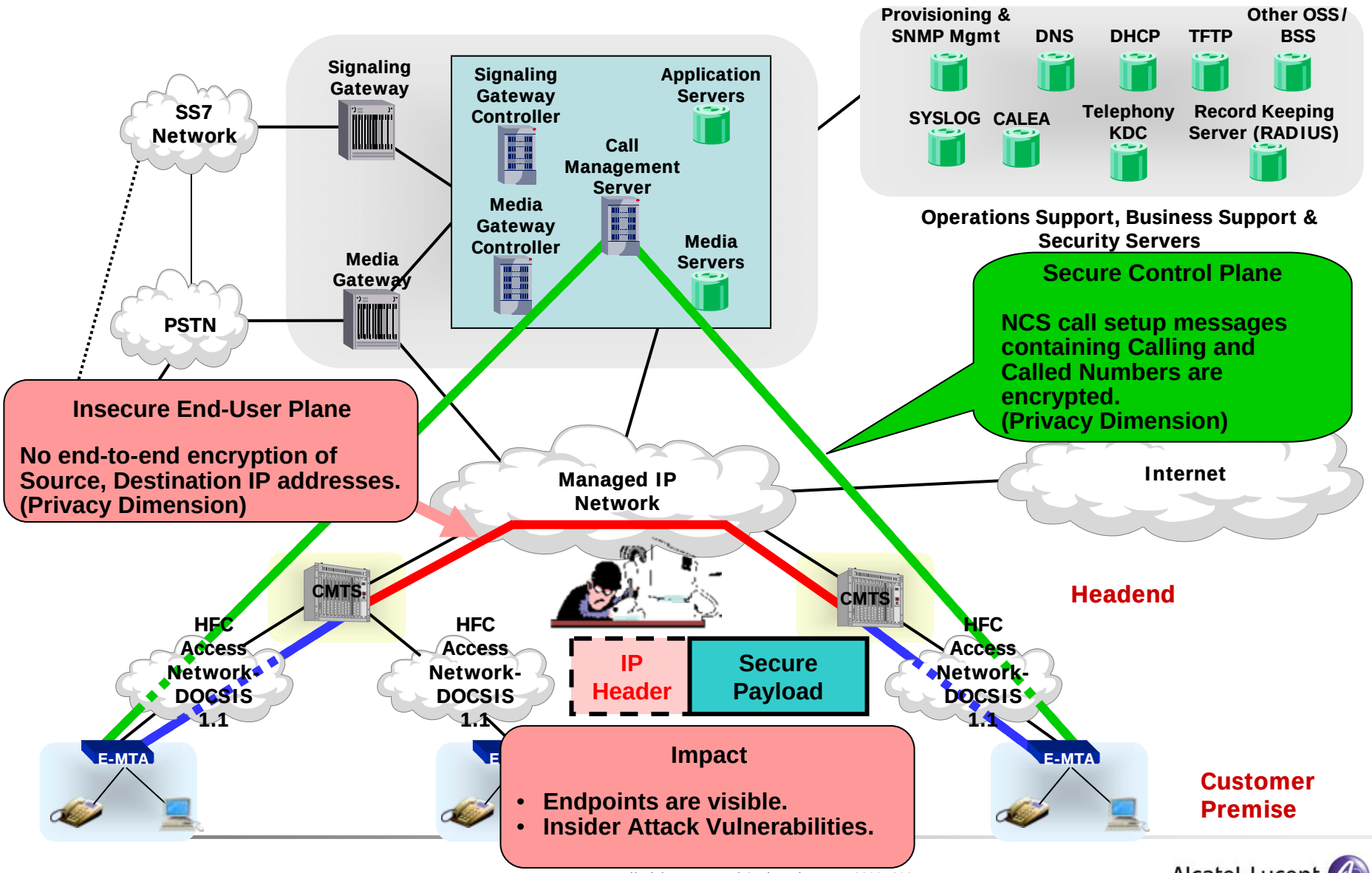
All Rights Reserved © Alcatel-Lucent 2006, 2007

Applying Security Dimensions – An Example



All Rights Reserved © Alcatel-Lucent 2006, 2007

VoCable Network Security – Example Application of ITU-T X.805



All Rights Reserved © Alcatel-Lucent 2006, 2007

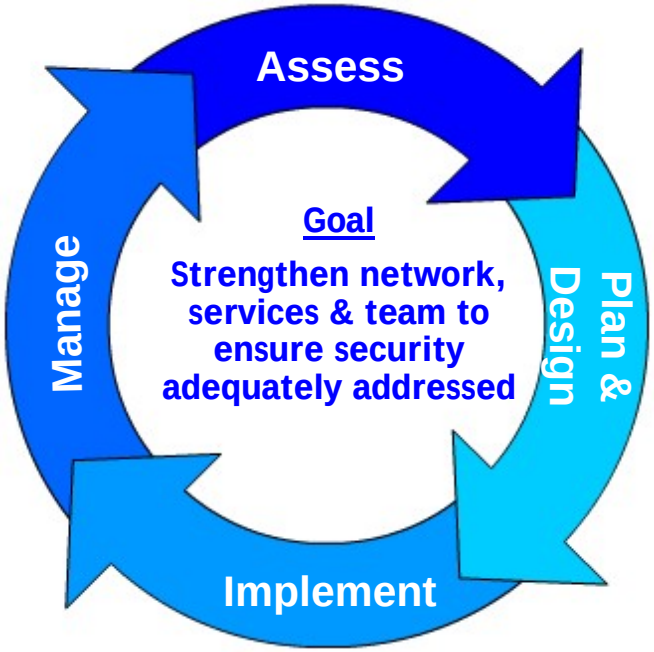
Alcatel·Lucent

Security Life Cycle Objectives –

How ITU-T X.805 assets be leveraged

- 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

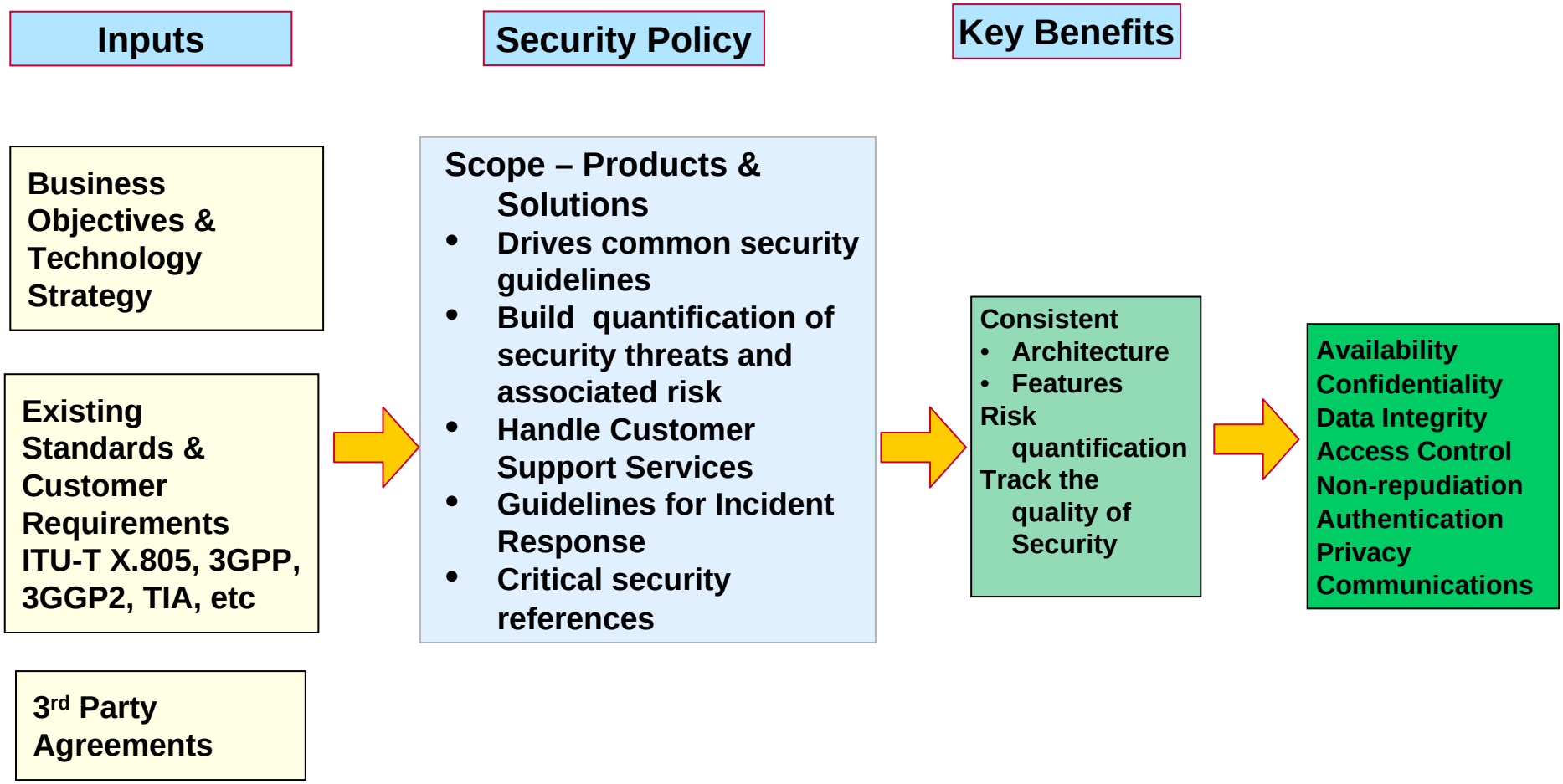


- Security policy
- Prioritizing security roadmap (customer requirements , architecture gaps etc)
- 3rd-party security gaps
- Interoperability of 3rd party
- Reliability & security test strategy
- Secure coding

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

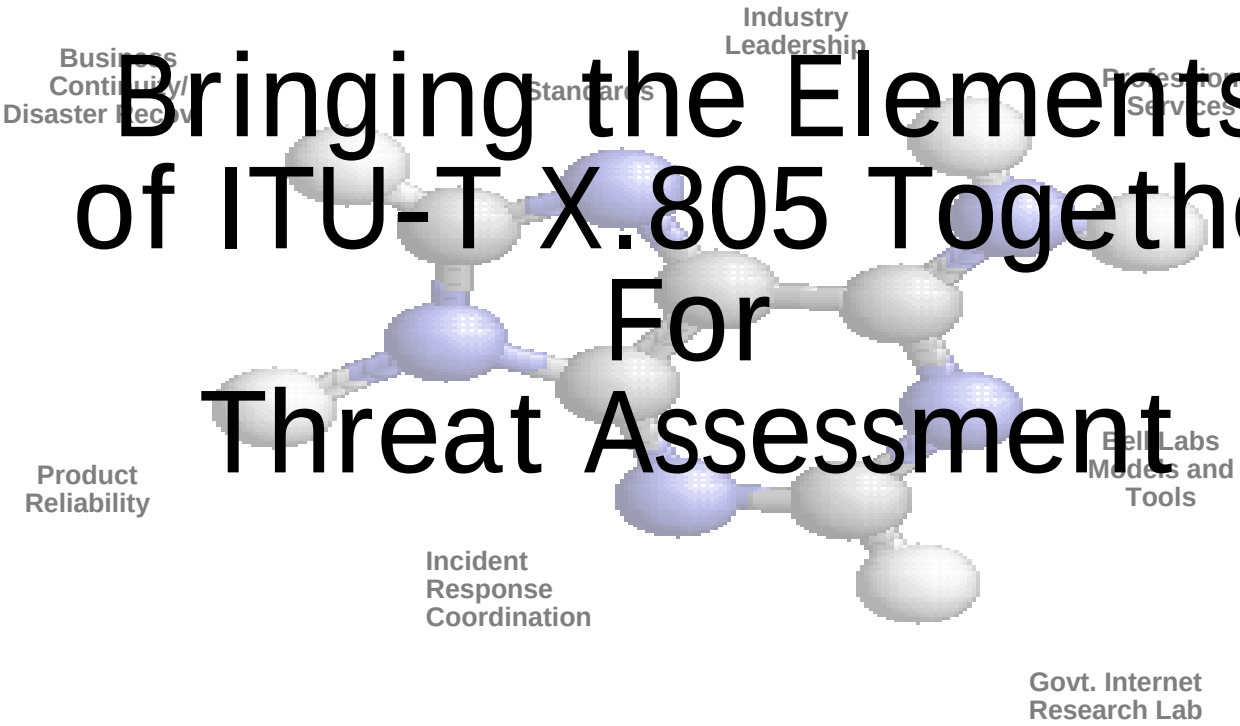
All Rights Reserved © Alcatel-Lucent 2006, 2007

Role of Security Policy



All Rights Reserved © Alcatel-Lucent 2006, 2007

Bringing the Elements of ITU-T X.805 Together For Threat Assessment



All Rights Reserved © Alcatel-Lucent 2006, 2007

High Level Key Definitions

Threats (Threat Scenarios)

- An unwanted (deliberate or accidental) event that may result in harm to a business, institution or individual.
- Any circumstance or event with the potential to adversely impact a business, institution or individual.
- An indication or source of impending danger, declaration of intent to harm a business, institution or individual.
- Adversarial attack or inadvertent error that causes damage to a business, institution or individual.

X.800 Threat Classes (Corruption, Destruction, Theft/Removal, Disclosure, Interruption)

Threat classes are applicable to individual assets. For example, a customer billing record is subject to corruption, destruction, theft/removal, disclosure, interruption

All Rights Reserved © Alcatel-Lucent 2006, 2007

Relationship of Threat Classes and Threat Scenarios

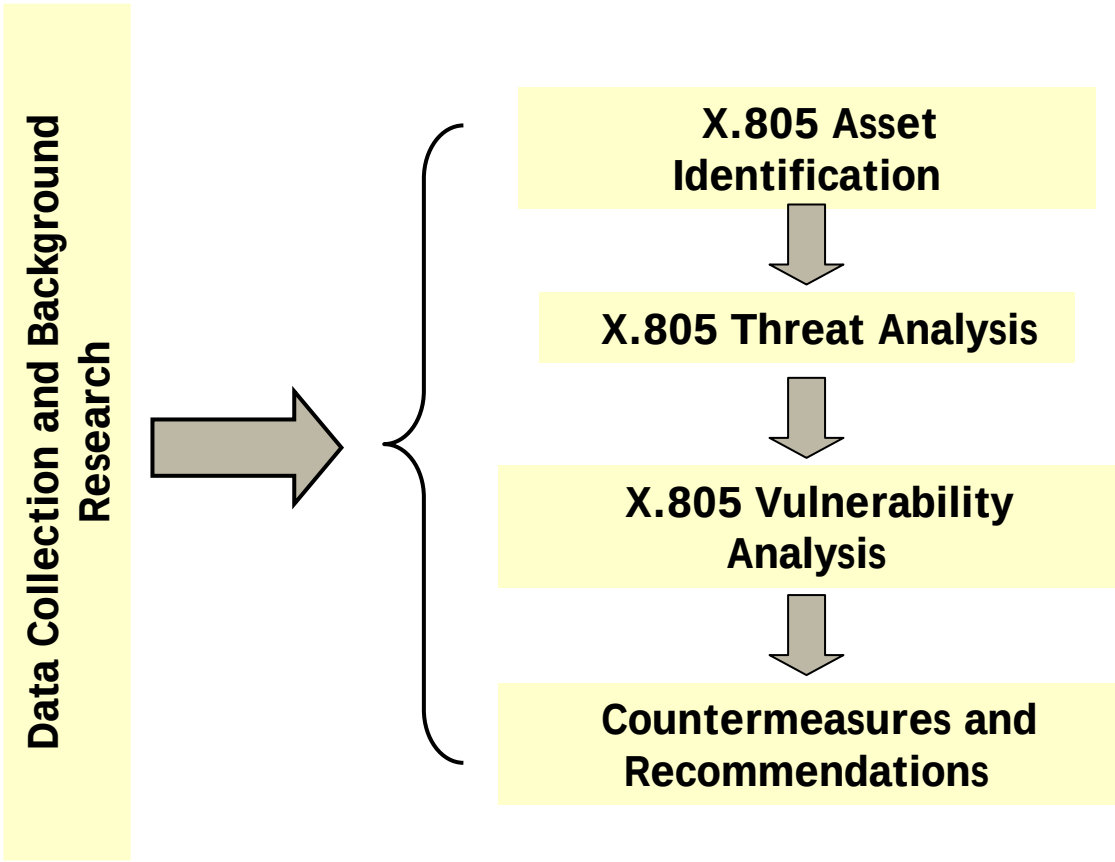
- The threat classes contained in the threat model are fixed regardless of what technology and industry vertical the threat model is applied to.
- A Threat Scenario is realized by a combination of threat classes (threats) on a set of assets. For example, Invasion of Subscriber Privacy can be realized by:
  - Disclosure on the air interface asset,
  - Disclosure of the call detail record asset,
  - Disclosure of the customer billing record asset,

Example of the application of a threat class (threat) to an asset:

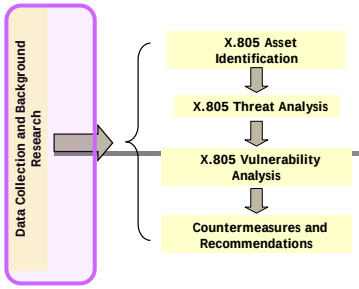
- **Threat Scenario:** Invasion of Subscriber Privacy
- **Asset:** Radio Air Interface
- **Disclosure** Threat Class**:** Sniffing devices can be used to eavesdrop on subscriber conversations.
- **Vulnerability:** EV-DO air interface is not encrypted.
- **Countermeasure:** Employ encryption at a higher protocol layer (e.g., TLS/SSL, IPsec).

All Rights Reserved © Alcatel-Lucent 2006, 2007

High Level X.805-based Methodology for Threat Assessment

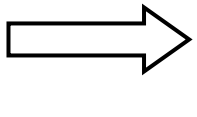


All Rights Reserved © Alcatel-Lucent 2006, 2007

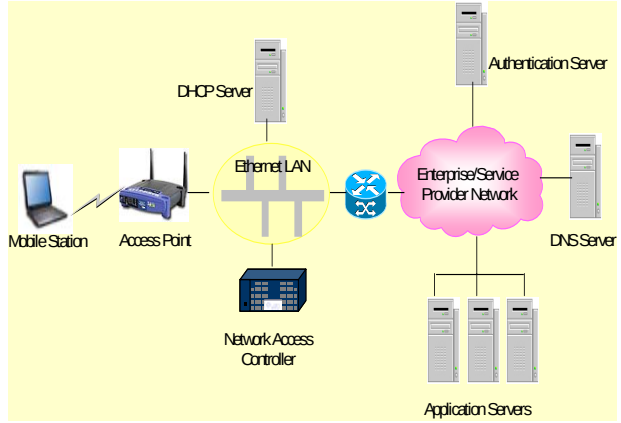


Data Collection & Background Research

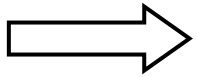
Internal Documents



Network Architecture



Industry Fora



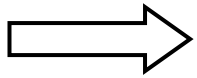
Threats

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

Vulnerability DBs

Carnegie Mellon Software Engineering Institute CERT® Coordination Center

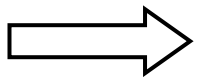
Sponsored by DHS National Cyber Security Division/US-CERT
National Vulnerability Database
a comprehensive cyber vulnerability resource



Known Vulnerabilities

Standards Orgs.

IETF ITU



Known Countermeasures

All Rights Reserved © Alcatel-Lucent 2006, 2007

Alcatel·Lucent

X.805 Asset Identification
X.805 Threat Analysis
X.805 Vulnerability Analysis
Countermeasures and Recommendations

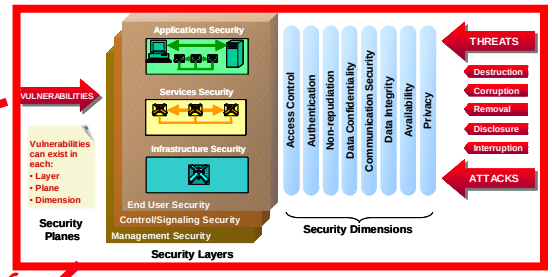
X.805 Security Analysis Process

Network Architecture

Perform X.805 Asset Identification

	Asset	Management Plane	Control Plane	End-User Plane
1.1	IGMPv2/v3 (Snooping)		✓	
1.2	PIM (SM, SSM, Snooping)		✓	
1.3	MBGP		✓	

X.805 Layers, Planes



Threats+

Perform X.805 Threat Analysis

X.805 Threats

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

X.805 Dimensions

+ indicates that there is additional analysis

Known Vulnerabilities+

Perform X.805 Vulnerability Analysis

	Asset	Services Layer Threat Details	Services Layer Vulnerability Analysis
1.1	IGMPv2/v3		
	Corruption	Malformed IGMP packets	Malformed IGMP packets could be created by an attacker and sent to the DSLAM or STB. Malformed packets could cause buffer overflow or the system to hang/crash.

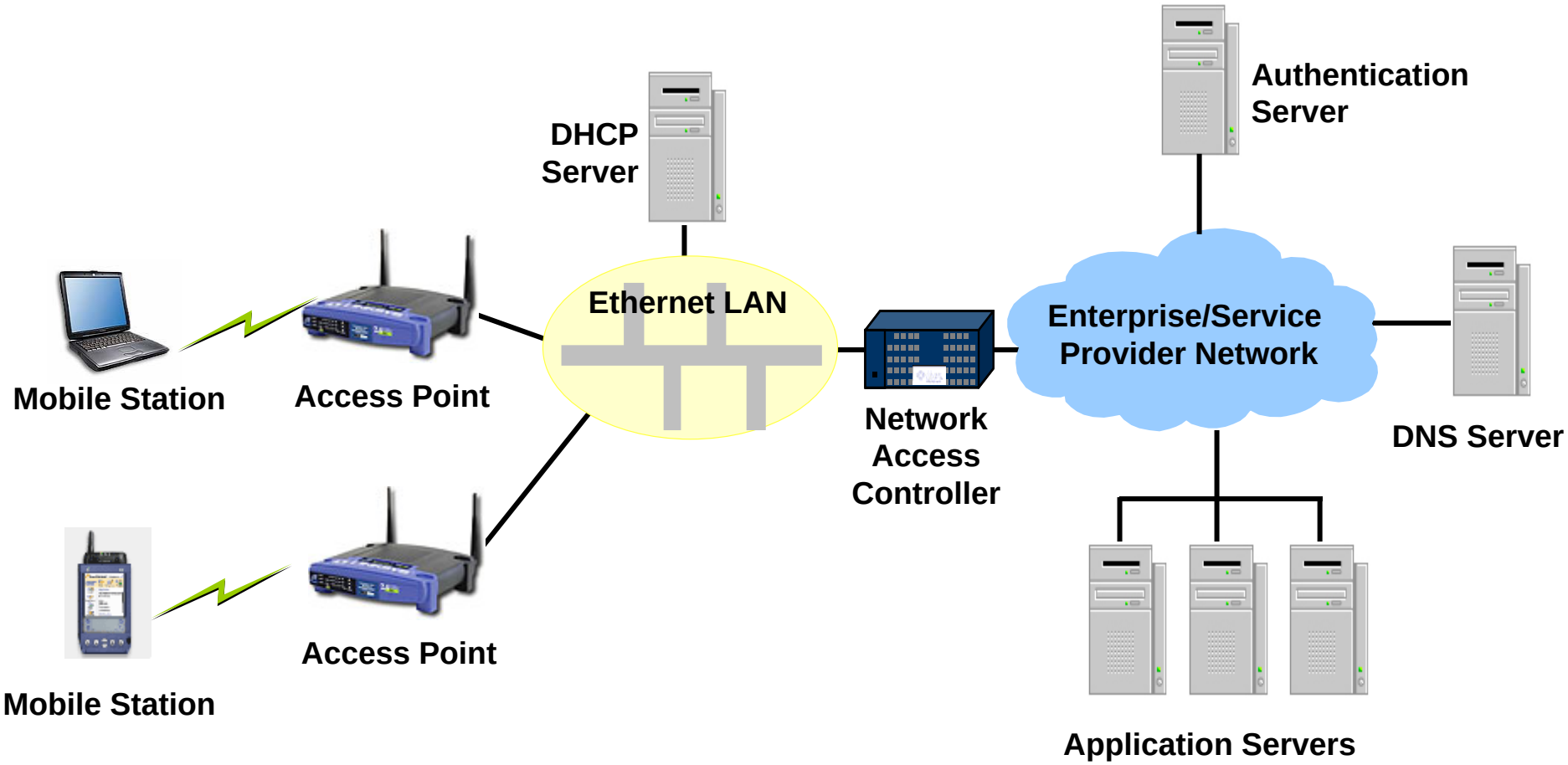
Known Countermeasures+

Countermeasures and Recommendations

	Asset	Services Layer Threat Details	Countermeasures
1.1	IGMPv2/v3		
	Corruption	Malformed IGMP packets	To protect against malformed IGMP packets: 1. Verify DSLAM or STB device manufacturer follows best practices for secure software development. 2. Include security testing during DSLAM or STB acceptance testing.

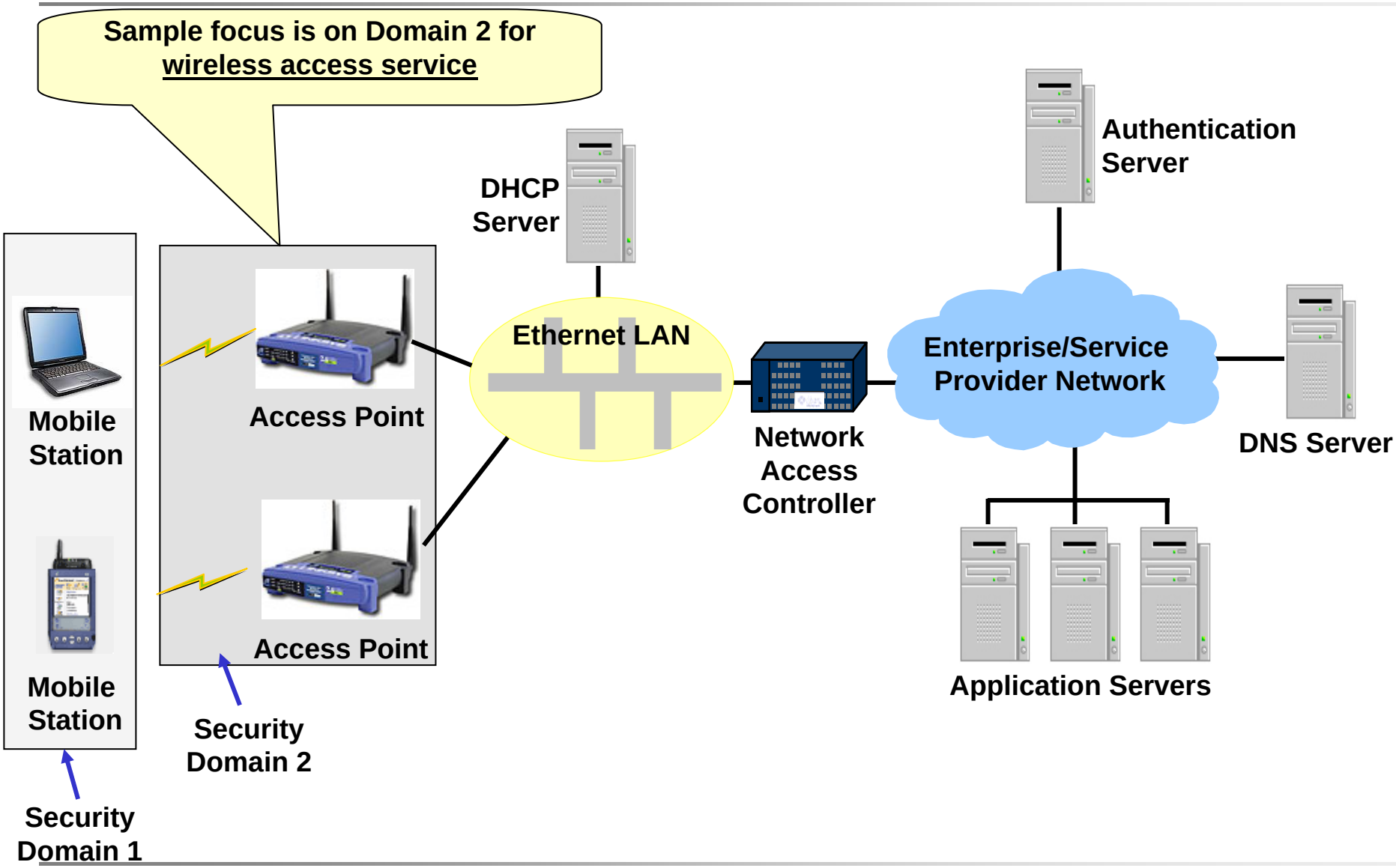
All Rights Reserved © Alcatel-Lucent 2006, 2007

WLAN Reference Architecture



All Rights Reserved © Alcatel-Lucent 2006, 2007

WLAN Network Security Domains



All Rights Reserved © Alcatel-Lucent 2006, 2007

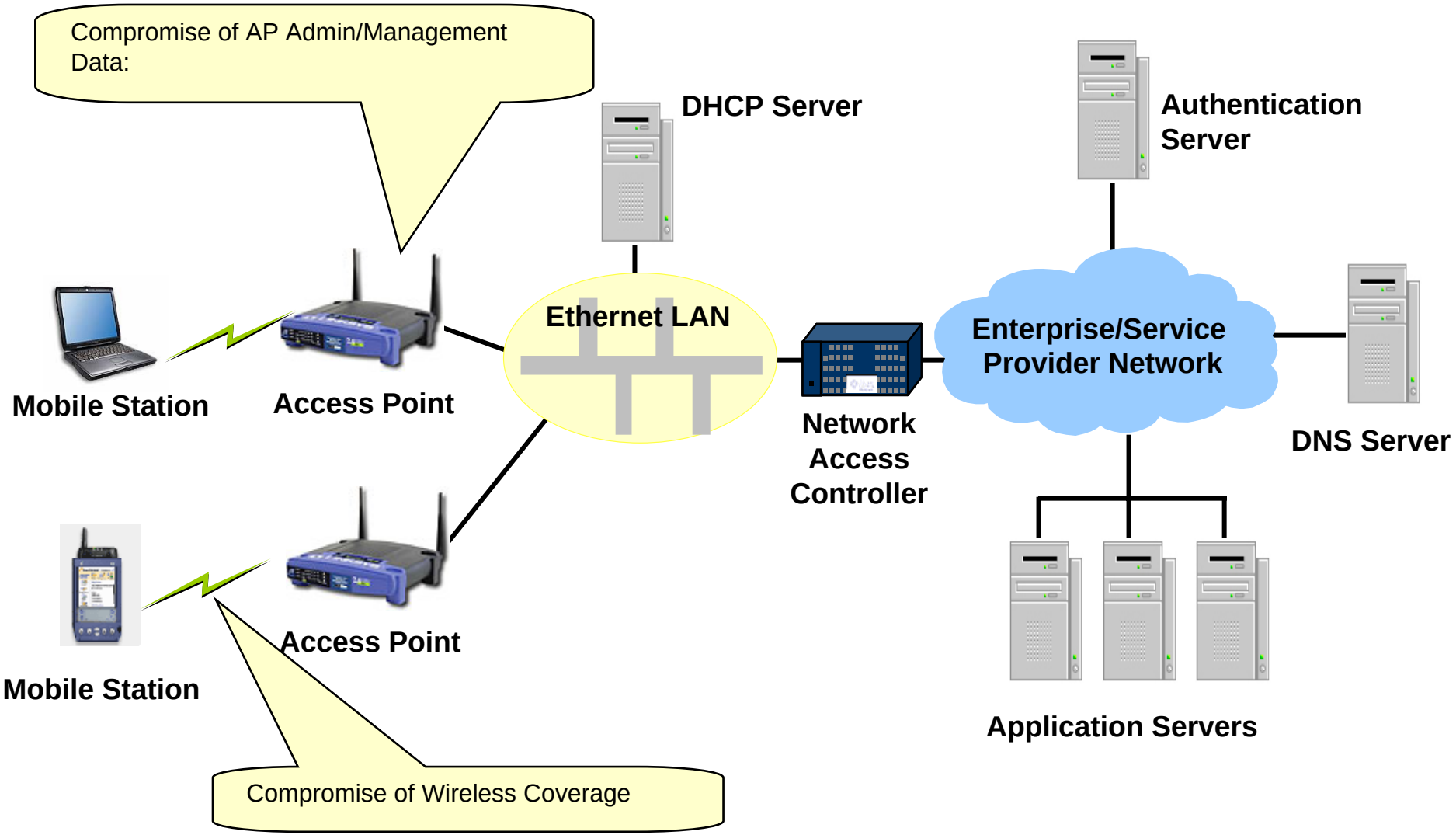
X.805 Asset Identification - Sample Asset Inventory

	Infrastructure Layer Access Point (AP)	Services Layer Wireless Access	Applications Layer
Management Plane	AP GUI AP management traffic	Provisioning a user (e.g., MAC address in AP)	
Control/Signaling Plane	Association table in AP	Authentication traffic 802.11a/b/g DHCP traffic	
User Plane		User traffic between MS and AP	

All Rights Reserved © Alcatel-Lucent 2006, 2007

WLAN Reference Architecture

Sample Threats



All Rights Reserved © Alcatel-Lucent 2006, 2007

Alcatel·Lucent

X.805 Threat Analysis

Asset	Destruction	Corruption	Removal	Disclosure	Interruption	Threat
GUI of all NEs	N/A	N/A	N/A	Unauthorized access	Consuming processing resources (DoS)	1
AP Management Traffic	N/A	Forged management commands	Redirecting messages to another address	Eavesdropping (SNMP v1 and v2)	Consuming processing resources (DoS)	1
Association table in AP	Unauthorized access to AP, software backdoors, buffer overruns	N/A	N/A	Gathering information about clients (depending on what is stored)	N/A	1
User traffic between MS and AP	N/A	Session hijacking Man in the middle attack	Evil twin	No encryption Key cracking	RF jamming Data flooding	2
Authentication handshake	N/A	N/A	N/A	Shared, static key common across all clients key stored in clear text	Data flooding	2
802.11a/b/g	N/A	Session hijacking Man in the middle attack	Evil twin	No encryption	RF jamming Data flooding	2

Threats:
1. Compromise of administrative and management data
2. Compromise of wireless coverage

All Rights Reserved © Alcatel-Lucent 2006, 2007

Threat Analysis Summary

Asset	ISO 18028-2 Threat Exposure					Covered in Threat
	Destruction	Corruption	Removal or Theft	Disclosure	Interruption	
1. AP GUI				X	X	1
2. AP Management Traffic		X	X	X	X	1
3. Association Table in AP	X			X		1
4. User traffic between MS and AP		X	X	X	X	2
5. Authentication Traffic				X	X	2
6. 802.11a/b/g		X	X	X	X	2

Threats:
1. Compromise of administrative and management data
2. Compromise of wireless coverage

All Rights Reserved © Alcatel-Lucent 2006, 2007

X.805 Vulnerability Analysis
-Sample illustration

Asset/Threat	Analysis
1. **AP GUI**	
Disclosure	Use of HTTP for web-based access
Interruption	Physical access of AP or password compromise
2. **AP Management Traffic**	
Corruption	Forged management commands (protocol weakness)
Removal	Spoofed ARP Response (low probability vulnerability)
Disclosure	Eavesdropping (SNMP v1, v2)
Interruption	DoS attack on the management port of the AP
3. **Association Table in AP**	Weak access control, lack of software integrity
Destruction	
Disclosure	

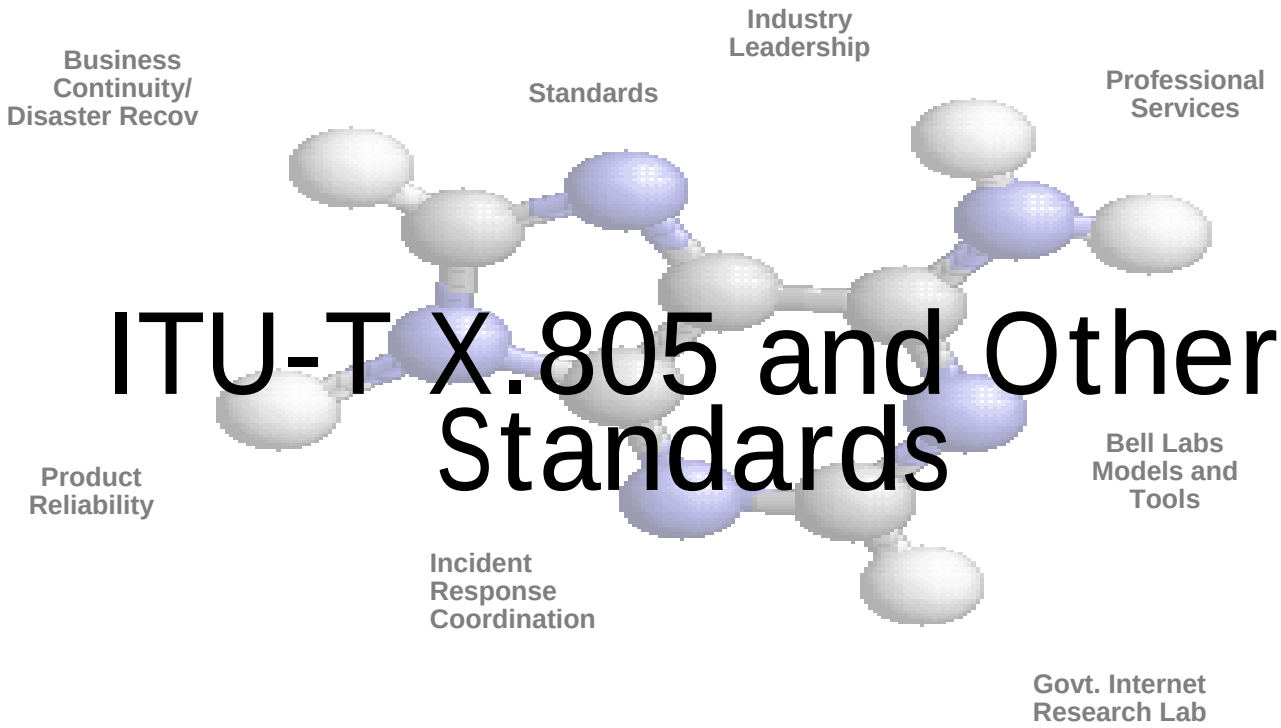
All Rights Reserved © Alcatel-Lucent 2006, 2007

Countermeasures and Recommendations

-Sample illustration

Asset/Threat	Analysis	Countermeasures
1. **AP GUI** **Disclosure** **Interruption**	Use of HTTP for web-based access Physical access of AP or password compromise	- Use secure HTTP (HTTPS). Password protection best practices. If AP does not support https, then use secure VPN using an additional VPN gateway. - Physical access to the AP should be limited and protected by using site surveillance
2. **AP Management Traffic** **Corruption** **Removal** **Disclosure** **Interruption**	Forged management commands (protocol weakness) Spoofed ARP Response (low probability vulnerability) Eavesdropping (SNMP v1, v2) DoS attack on the management port of the AP	-Since the AP is primarily a bridge device, the management port for the AP can be on a separate subnet (assign it a different network from the users) Use ACLs to control access. - Encryption of the community string while in-transit forces the attacker to know the encryption key in addition to successfully guessing the password in order to gain access. SNMPv3 should be configured with community string encryption enabled.
3. **Association Table in AP** **Destruction** **Disclosure**	Weak access control, lack of software integrity	-Change default AP configuration, such as SSID -Disable SSID broadcasts -Software integrity checks

All Rights Reserved © Alcatel-Lucent 2006, 2007



ITU-T X.805 and Other Standards

All Rights Reserved © Alcatel-Lucent 2006, 2007

Security Standardization Issues

Key Distribution (for end-users and network elements) and Public Key Infrastructure

"Network Privacy" – topology hiding and NAT/Firewall traversal for real-time applications

Convergence with IT security

Management of security functions (e.g. policy)

Guidelines on the implementation of the IETF protocols (e.g. IPSec options)

Security for supporting access: DSL, WLAN, and cable access scenarios

Guidelines for handling 3GPP vs. 3GPP2 differences in IMS security

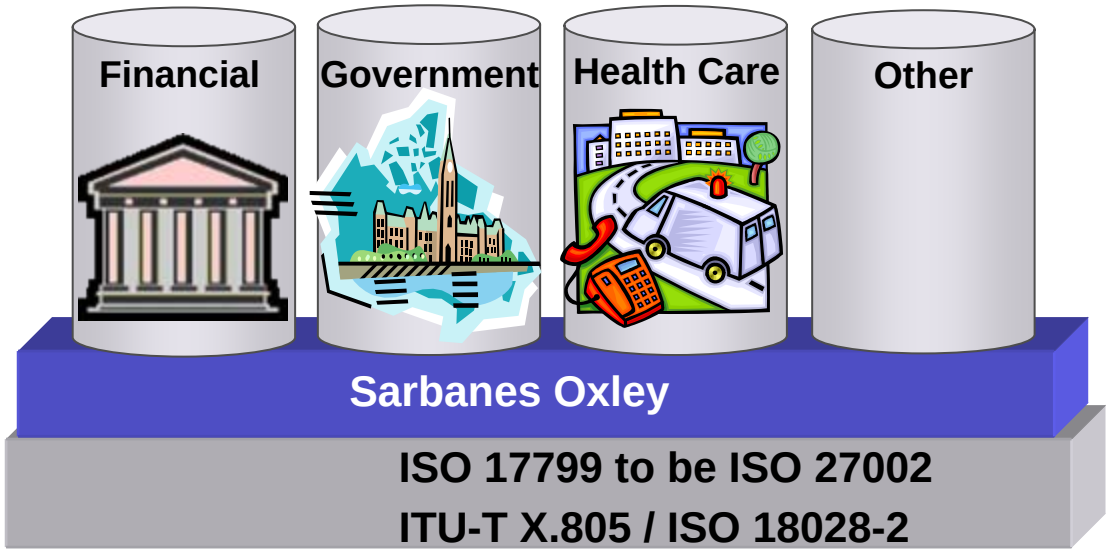
Both – network assets and network traffic – must be protected.
Proper management procedures will prevent attacks from within

All Rights Reserved © Alcatel-Lucent 2006, 2007

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;



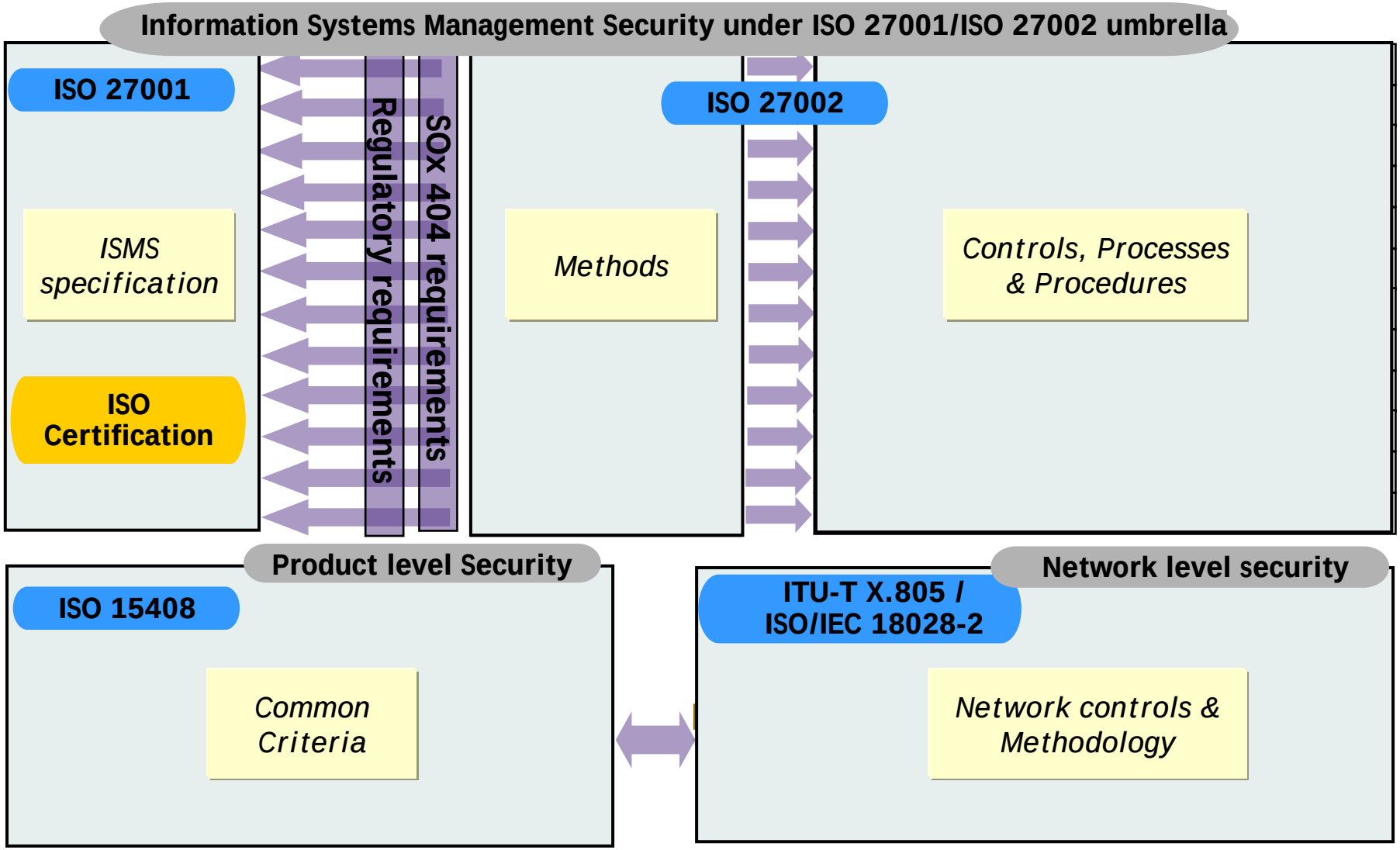
A common framework to adapt to emerging industry requirements

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

Standards approach provides foundation

All Rights Reserved © Alcatel-Lucent 2006, 2007

Security Framework



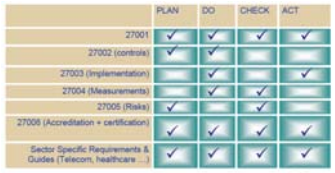
All Rights Reserved © Alcatel-Lucent 2006, 2007

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

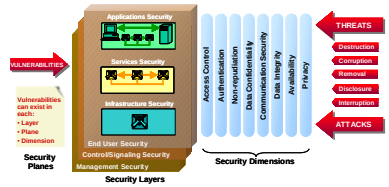
ISO/IEC 27001:27005

- 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.



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

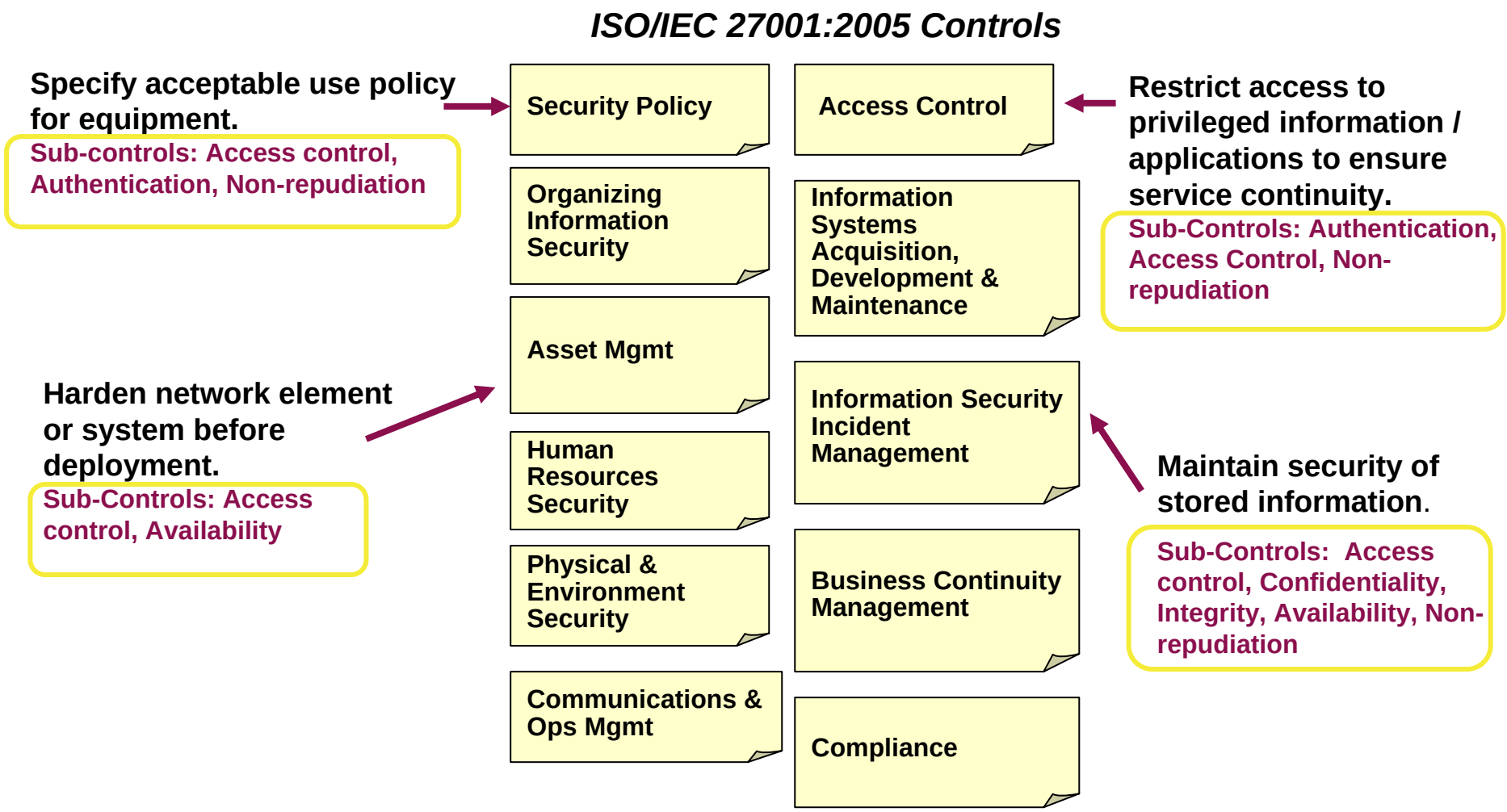
- Provides standards for detailed technical design, architecture, requirements, and test plans for the end-to-end network security solutions or individual products



ISMS = Information Security Management Systems

All Rights Reserved © Alcatel-Lucent 2006, 2007

ISO/IEC 27001 enhanced by ITU-T X.805 / ISO 18028-2



All Rights Reserved © Alcatel-Lucent 2006, 2007

eHealth or Health Insurance Portability and Accountability Act (HIPAA)

Privacy & Cyber Security Requirements

What:

- Security of individually identifiable health information in electronic form – referred to as Electronic Protected Health Information (ePHI)

Who:

- Healthcare providers, health care clearinghouses, health plan providers who transmit any protected health information in electronic form

How:

- By maintaining reasonable and appropriate administrative, physical, and technical safeguards to protect against any threats to the security and integrity of ePHI

Why:

- To protect confidentiality, integrity and availability of ePHI when it is stored, maintained or transmitted.

All Rights Reserved © Alcatel-Lucent 2006, 2007

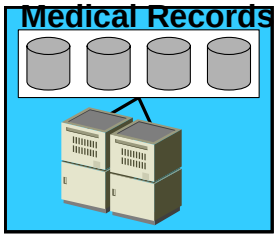
Utilizing ITU-T X.805 for Security Safeguards in Health Sector

End-users are:
- Plan Provider
- Clearinghouse
- Caregiver

ITU-T X.805 Safeguards in depth

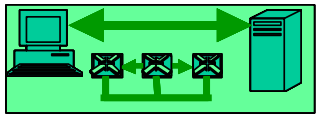
Electronic Protected Health Information (ePHI)

Securing the patient data provided to the network-based application (social security number etc.)



Enterprise Data Center

Application Security



End User Security

Infrastructure Security

End User Security

X.805 can be leveraged to Identify Cyber Security Requirements of eHealth/HIPAA

Securing the patient data as it resides in or is transported through network elements and while it is being transported across communications links. (medical history)

HIPAA Safeguards

Access Control
- Unique User Identification
- Emergency Access Procedure
- Encryption and Decryption
- Automatic Logoff

Audit Control
(logging and monitoring)

Integrity
(Integrity of ePHI)

Person or Entity Authentication

Transmission Security
- Message Integrity Controls
- Encryption Controls

End-users are IT for:
- Batch Transfers for Billing
- Mirrored Backup
- Disposal

Privacy - IPSec VPNs

Communications Security - Use VPNs

Data Confidentiality - SSL/TLS for end-to-end application security

Non - Repudiation - Digital Signatures

Data Integrity - Protect files w/ checksums

Data Confidentiality - Encrypt files

Access Control - Use file system ACLs

Non - Repudiation – Role Based Access Control

All Rights Reserved © Alcatel-Lucent 2006, 2007

Alcatel·Lucent

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

All Rights Reserved © Alcatel-Lucent 2006, 2007

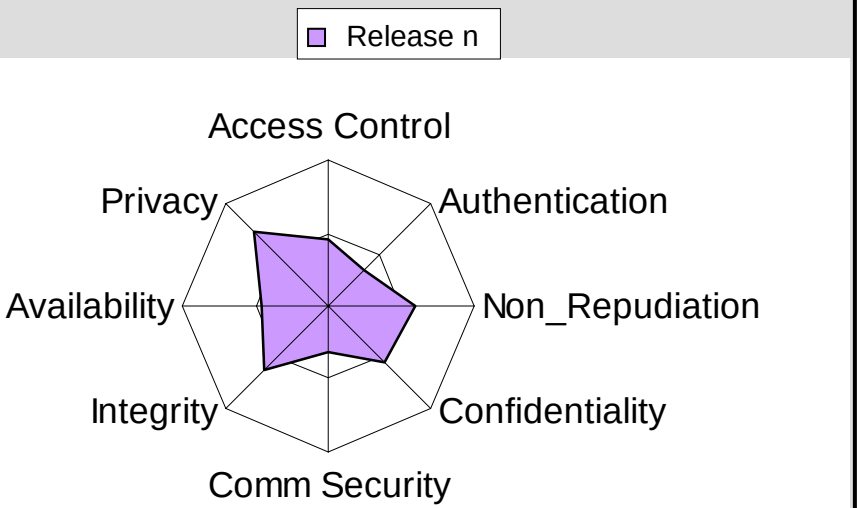
Standards Summary

Using ITU –T X.805/ISO 18028-2 as your overall network security model will

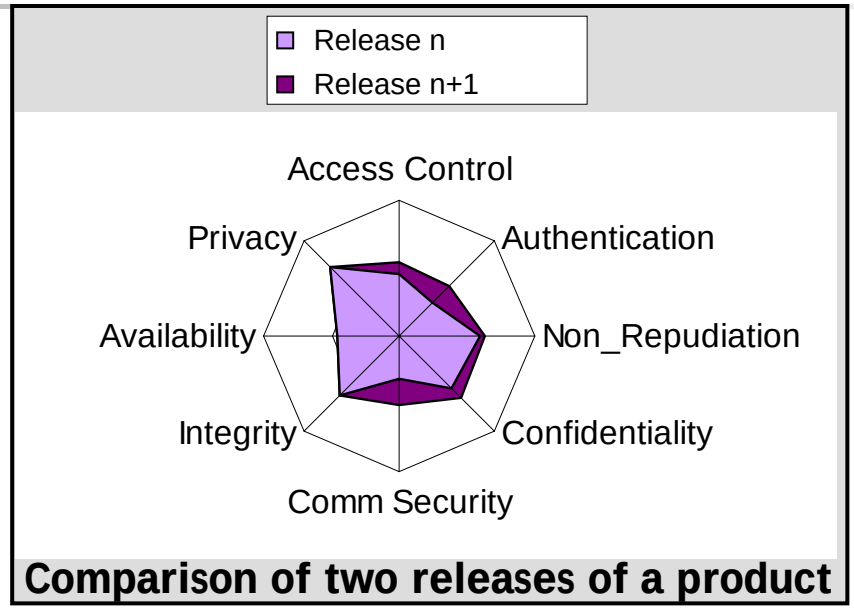
- Drive common security policies & requirements for your customer service offerings
- Build in quantification of security threats and associated risk
- Ensure security is built in from service concept through deployment.
- Continue to drive the end-to-end network security

All Rights Reserved © Alcatel-Lucent 2006, 2007

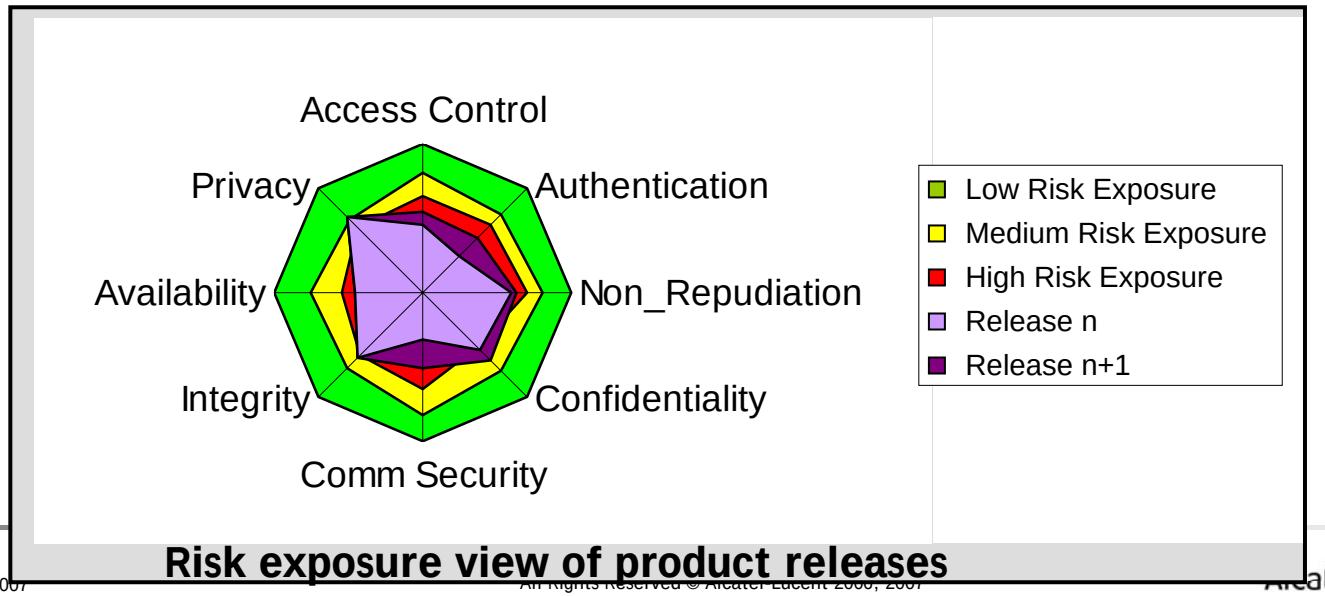
Using ITU-T X.805 for Measuring Security



View of a single product release



Comparison of two releases of a product



Risk exposure view of product releases

All Rights Reserved © Alcatel-Lucent 2006, 2007

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"

All Rights Reserved © Alcatel-Lucent 2006, 2007

Backup

All Rights Reserved © Alcatel-Lucent 2006, 2007

What ITU -T X.805 is Not by Itself?

- One Answer to Architecture
- Implementation Specification
- A set of Organizational Controls
- A Procedure or Specification of Evaluation Criteria
- Implementation of Risk Management
- A Protocol Verification Algorithm
- Operations Management Guide
- Organizational or Personnel Management Guide
- Physical Security Standard
- Product or Technology or Industry Dependent

- May be just a talking point slide

X.805 can be used as an enabler for any of the items and more

All Rights Reserved © Alcatel-Lucent 2006, 2007