Lucent Worldwide Services
Network Security Assessment Service

Introduction to ITU-T X.805 standard

Ching Tim Meng (CISSP, CISA)
Regional Security Consultant, Asia Pacific

25 September 2006

Lucent Technologies
Bell Labs Innovations

Overview

- Origins
- What is it all about
- Relevance and applications
- The future

Current situation

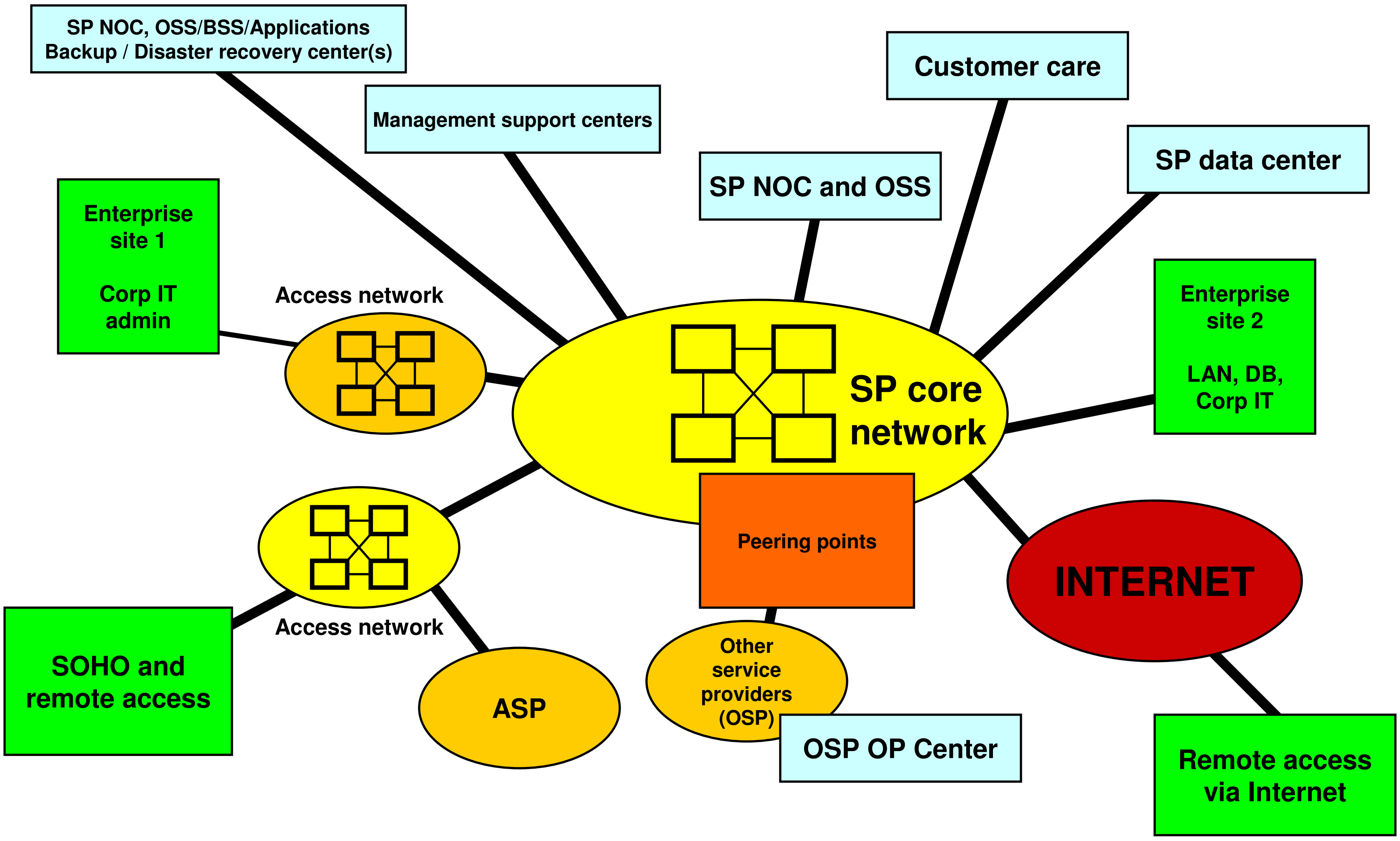
- Heard of anything network security standard?
- No standard that guides an organisation on securing the network architecture
- Checklist method used traditionally by auditors not providing business value to customer
    - Same control cannot be applied in a similar manner for different organisations
    - Not dynamic enough to address ever-changing technology progress

Different business requirements warrant different controls

Introducing ITU-T X.805 standard

- Developed by Bell Labs, research arm of Lucent.
- Formerly known as Bell Labs Security Framework.
- Developed to address robustness of network security framework.
- Address end-to-end network security for the following kinds of networks:
  - Wireline voice and data
  - Wireless
  - Optical
  - Converged networks
- Can be applied to all types of service provider and enterprise networks, across all layers of the protocol stack.

Typical service provider network architecture



Bell Labs Security Framework

Security Threats

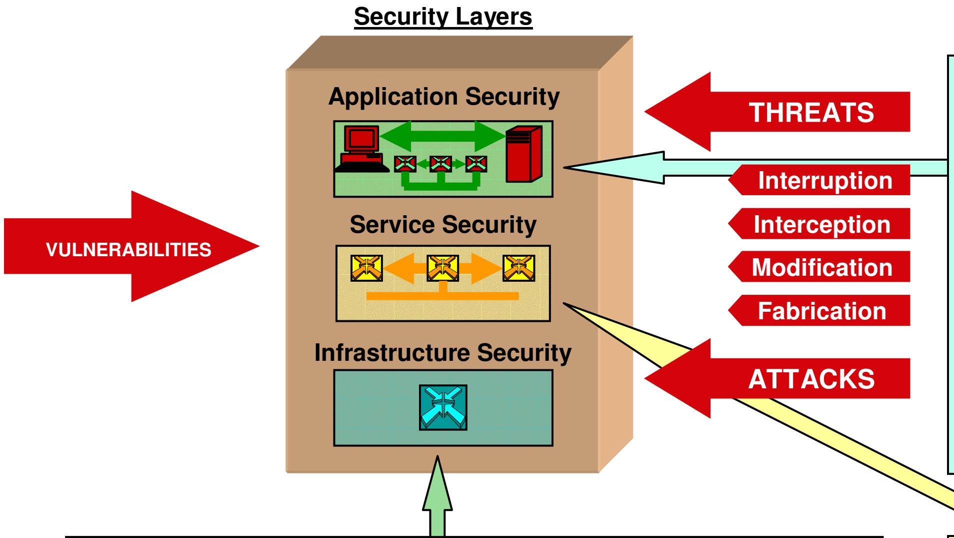
- Framework identifies issues that need to be addressed to detect, correct and prevent both intentional and accidental threats originating from inside or outside the network.
- Four threats identified in this framework:
  - Interruption
  - Interception
  - Modification
  - Fabrication

Bell Labs Security Framework (Cont'd)

Security Layers

- Three security layers consisting of hierarchy of network equipment and facility groupings, where they build on one another to provide comprehensive, end-to-end security.
- Three security layers defined as:
  - Infrastructure
  - Services
  - Applications

Bell Labs Security Framework (Cont'd)



3 - Applications Security Layer:

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

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, WiMax
  - VoIP, QoS, IM, Location services
  - Toll free call services

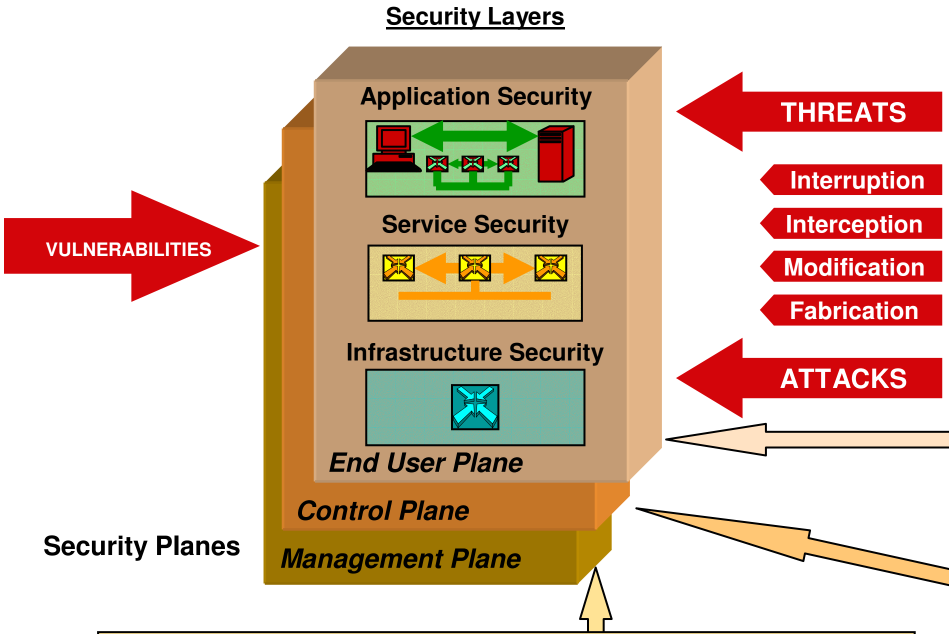
- **Security Layers are a hierarchy of equipment and facilities groupings**
- **Each Security Layer has unique vulnerabilities, threats, and mitigations**
- **Infrastructure security enables services security enables applications security**

Bell Labs Security Framework (Cont'd)

Security Planes

- Three security planes represent the activities that take place on a network.
- Three security layers defined as:
  - Management
  - Control
  - End-User
- Networks should be design such that events on one security plane are kept totally isolated from the other security planes.

Bell Labs Security Framework (Cont’d)



3 - 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)

1 - 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**

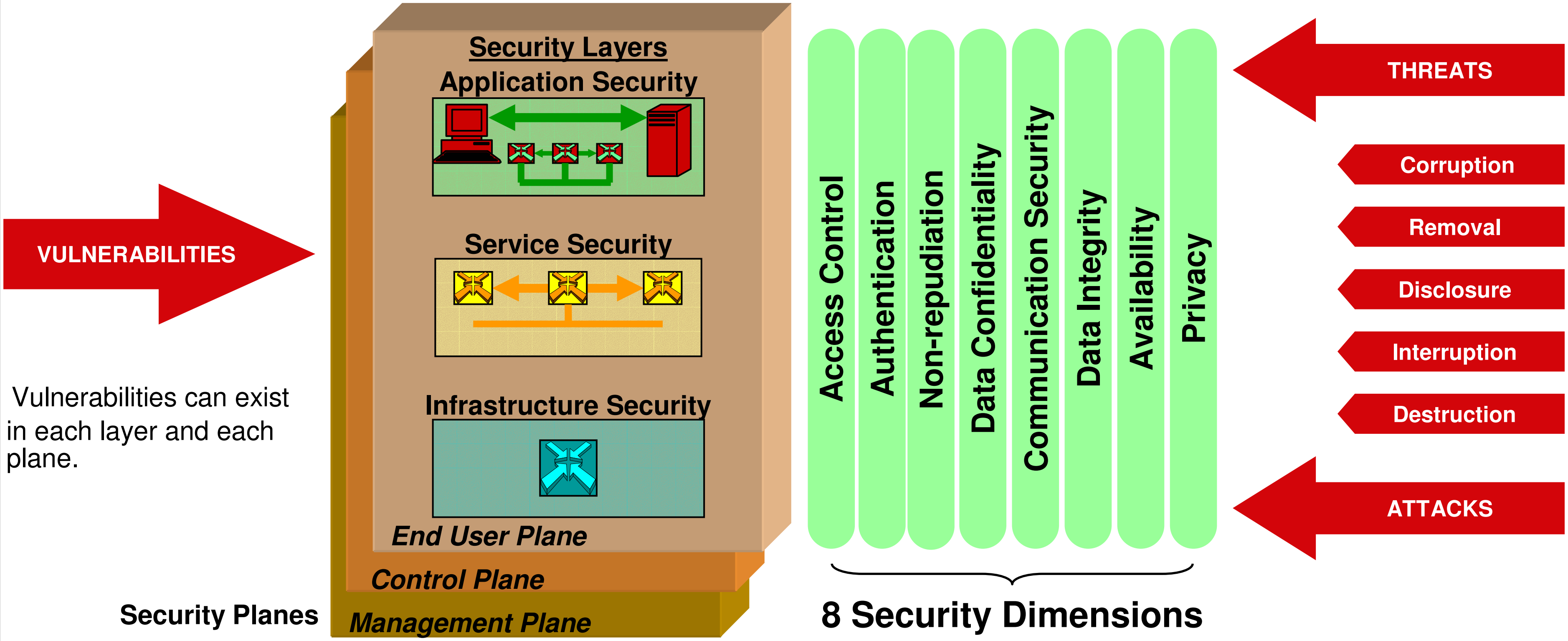
Transition to ITU-T X.805

- Bell Labs Security Framework has been tested and verified by following bodies:
  - ITU (International Telecommunication Union)
  - NSIE (National Safety Information Exchange)
  - NSTAC (National Security Telecommunications Advisory Committee)
  - IES (Institute of Environmental Sciences)
  - NCC (National Computing Centre)
  - NRIC VI (Network Reliability and Interoperability Council)
  - Industry Canada (A government body from Canada)

Transition to ITU-T X.805 (Cont’d)

- Proven framework submitted to ITU-T for ratification.
- Ratification process includes a few changes:
  - Utilises standard security services and mechanisms from ITU-T X.800 which define eight basic dimensions of security that must be addressed.
  - Four threats have been renamed, and added a new threat into the framework.
- Standard named as “Security architecture for systems providing end-to-end communications”.
- Ratified by ITU on October 2003.

ITU-T X.805 network security framework



Vulnerabilities can exist in each layer and each plane.

Security architecture for end-to-end network security

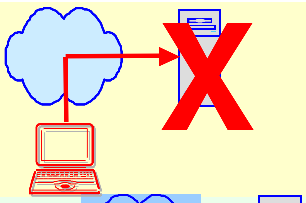
ITU-T X.800 Threat Model

- Five security threats defined:
  - Destruction
  - Corruption (Formerly Modification)
  - Removal (New threat defined)
  - Disclosure (Formerly Interception)
  - Interruption
- The threat “Fabrication” has been incorporated as part of “Corruption”.

ITU-T X.800 Threat Model (Cont'd)

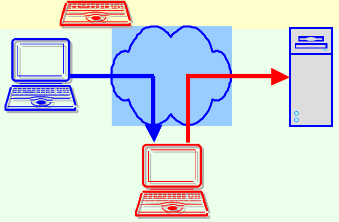
1 - Destruction (an attack on availability):

– Destruction of information and/or network resources



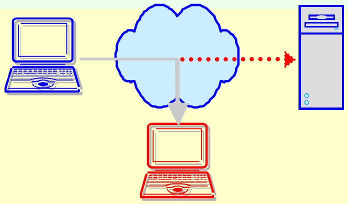
2 - Corruption (an attack on integrity):

– Unauthorized tampering with an asset



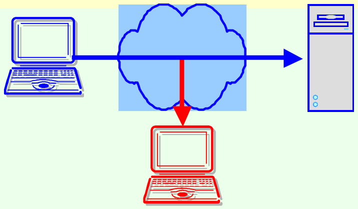
3 - Removal (an attack on availability):

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



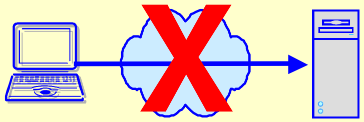
4 - Disclosure (an attack on confidentiality):

– Unauthorized access to an asset



5 - Interruption (an attack on availability):

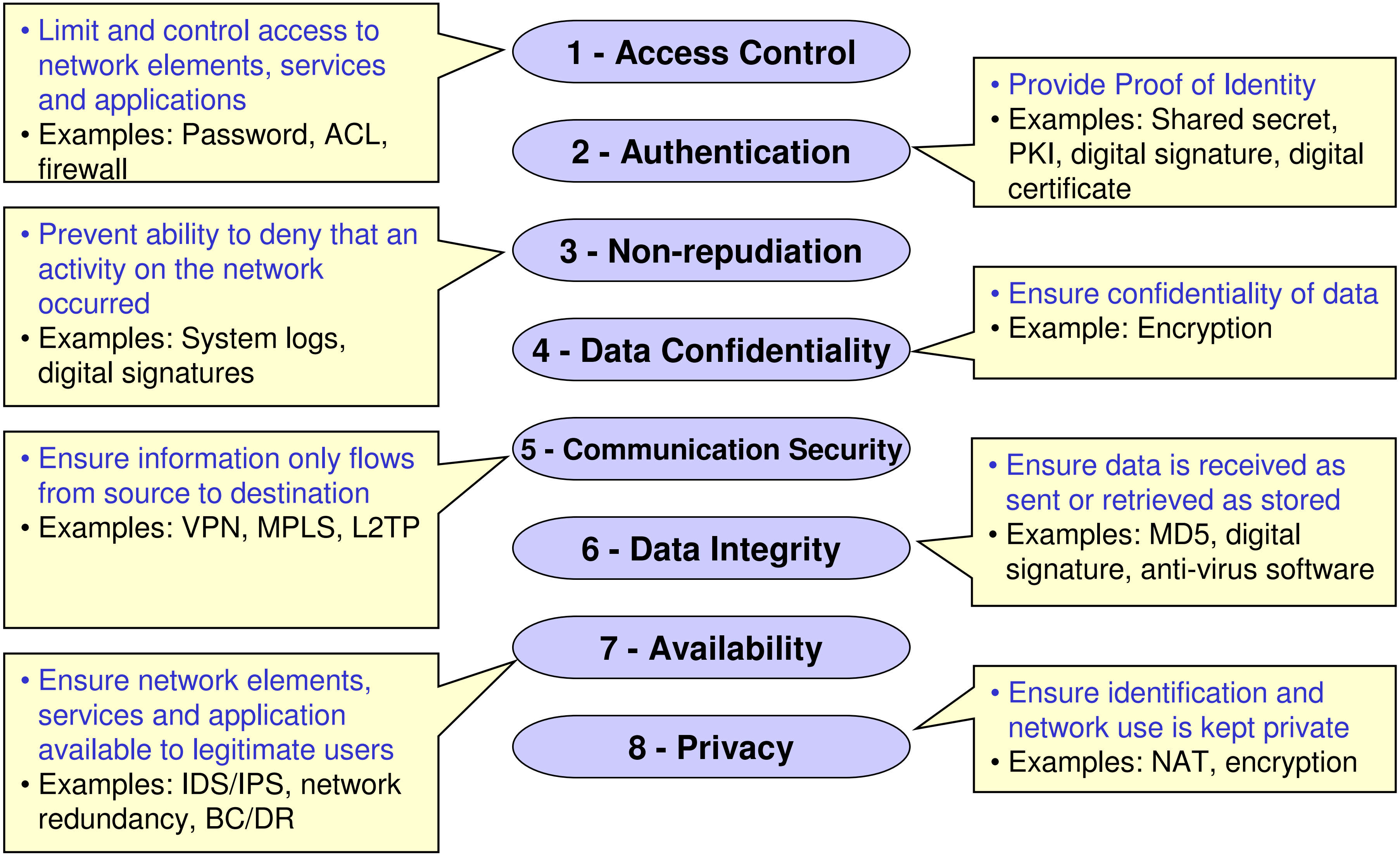
– Network becomes unavailable or unusable



Security Dimensions

- A security dimension is a set of security measures designed to address a particular aspect of the network security
- ITU-T X.805 identifies eight sets of security dimensions that protect against all threats defined.
- Applicable to the network, applications and end-user information

Security Dimensions (Cont'd)



1 - Access Control

- Limit and control access to network elements, services and 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 information only flows from source to destination
- Examples: VPN, MPLS, L2TP

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

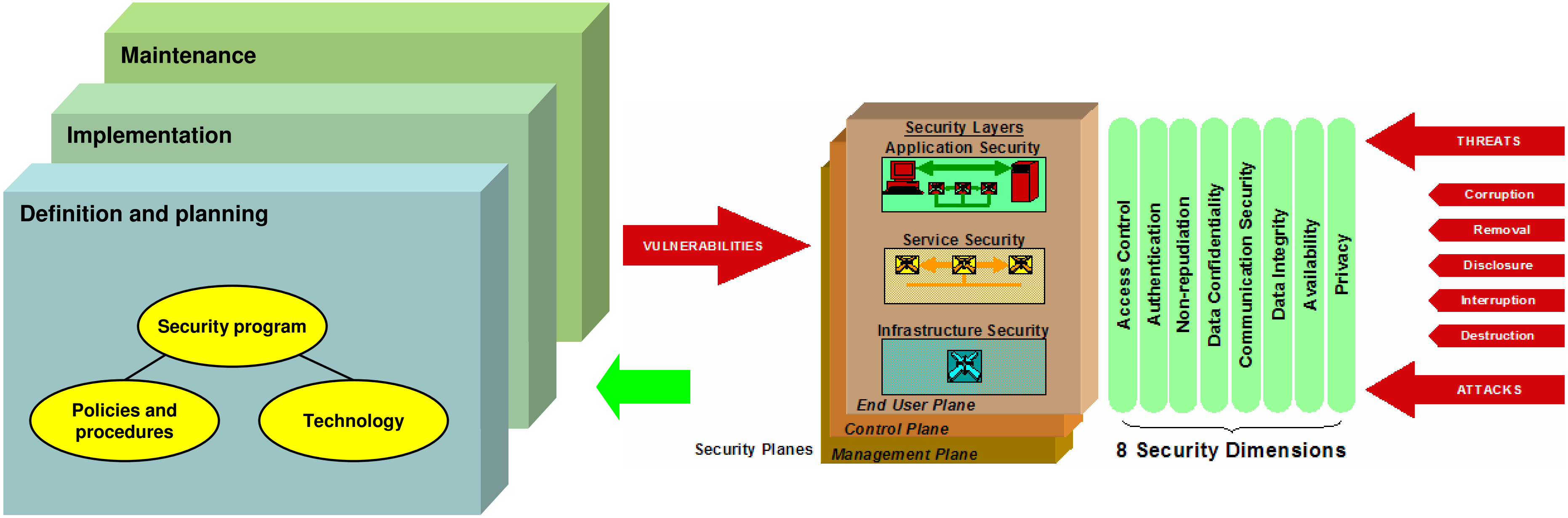
- Ensure identification and network use is kept private
- Examples: NAT, encryption

8 Security Dimensions applied to each Security Perspective (layer and plane)

Mapping Security Dimensions to Security Threats

Security Dimension	ITU-T X.800 Security Threats				
	Destruction of Information or Other Resources	Corruption or Modification Of Information	Theft, Removal or Loss of Information and Other Resources	Disclosure of Information	Interruption of Services
Access Control	Y	Y	Y	Y	
Authentication			Y	Y	
Non-repudiation	Y	Y	Y	Y	Y
Data Confidentiality			Y	Y	
Communication Security			Y	Y	
Data Integrity	Y	Y			
Availability	Y				Y
Privacy				Y	

Applying the standard to security programs

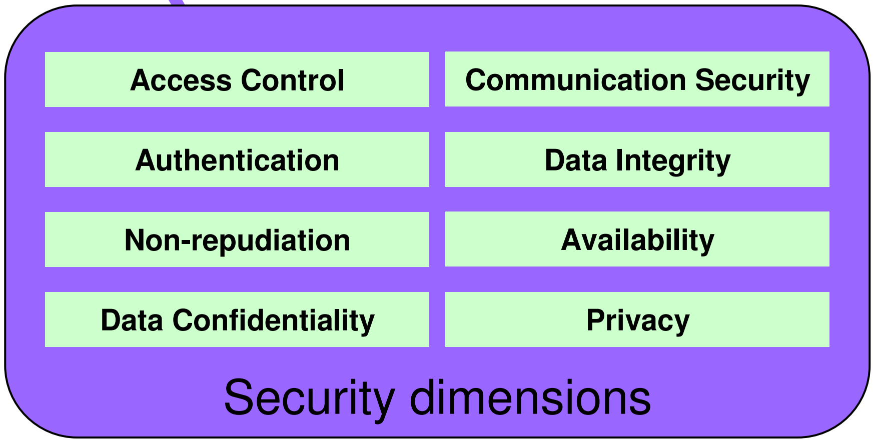


Modular Approach to Network Security Analysis

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

The 8 security dimensions are applied to each security perspective

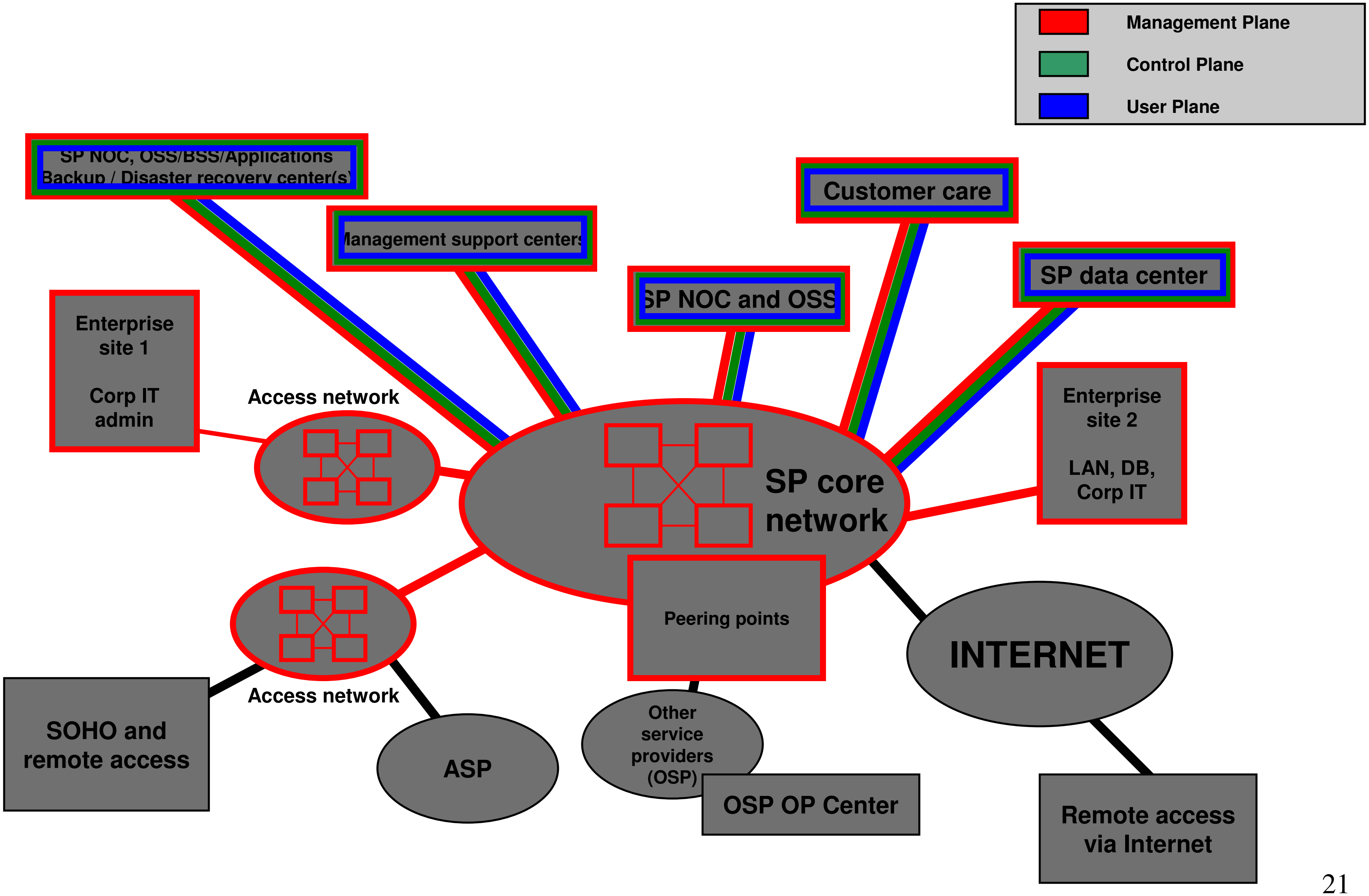
Security Dimensions of different modules have different objectives and comprise different sets of security measures.



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

Security dimensions

Management/Administrative Networks



Modules’ objectives

- Module 1 (Infrastructure, Management)
  - Concerned with securing the operations, administration, maintenance, and provisioning (OAM&P) of the individual network elements, communication links, and server platforms that comprise the network.
- Module 2 (Infrastructure, Control)
  - Consists of securing the control or signaling information that resides in the network elements and server platforms that comprise the network, and in the receipt and transmission of control or signaling information by the network, elements and server platforms.

Modules' objectives (Cont'd)

- Module 3 (Infrastructure, End-User)
  - Consists of securing user data and voice as it resides in or is transported through network elements, as well as while it is being transported across communications links.
- Module 4 (Services, Management)
  - Concerned with securing the OAM&P functions of network services.
- Module 5 (Services, Control)
  - Consists of securing the control or signaling information used by the network service.

Modules' objectives (Cont'd)

- Module 6 (Services, End-User)
  - Consists of securing user data and voice as it uses the network service.
- Module 7 (Applications, Management)
  - Concerned with securing the OAM&P functions of the network-based application.
- Module 8 (Applications, Control)
  - Consists of securing the control or signaling information used by the network-based applications.

Modules' objectives (Cont'd)

- Module 9 (Applications, End-User)
  - Consists of securing user data provided to the network-based application.
    - Authenticate user using the banking system.
    - Protect passwords entered in a banking application at the application level.

Example 1: Internet Service Provider

Layer Plane	Infrastructure	Services	Applications
Management	Router Distribution switch RAS	RADIUS SNMP	Email accounts Web page
Control	BGP OSPF	DHCP	SMTP POP3 HTTP
End-User	Management software Email protection	DNS Finger WHOIS	Email client Web browser

Example 2: A Multi-National Company

Layer Plane	Infrastructure	Services	Applications
Management	Router Distribution switch	RADIUS SNMP	User accounts File directories
Control	RIPv2	DHCP IPSec SIP	NETBIOS
End-User	Management software Database encryption	DNS VoIP	Email client Web browser Database client VoIP client

Example 3: Application Service Provider

Layer Plane	Infrastructure	Services	Applications
Management	Router Distribution switch	SNMP	Email accounts Web page User accounts File directories
Control	N/A	N/A	N/A
End-User	N/A	N/A	N/A

Example 4: Small Business Company

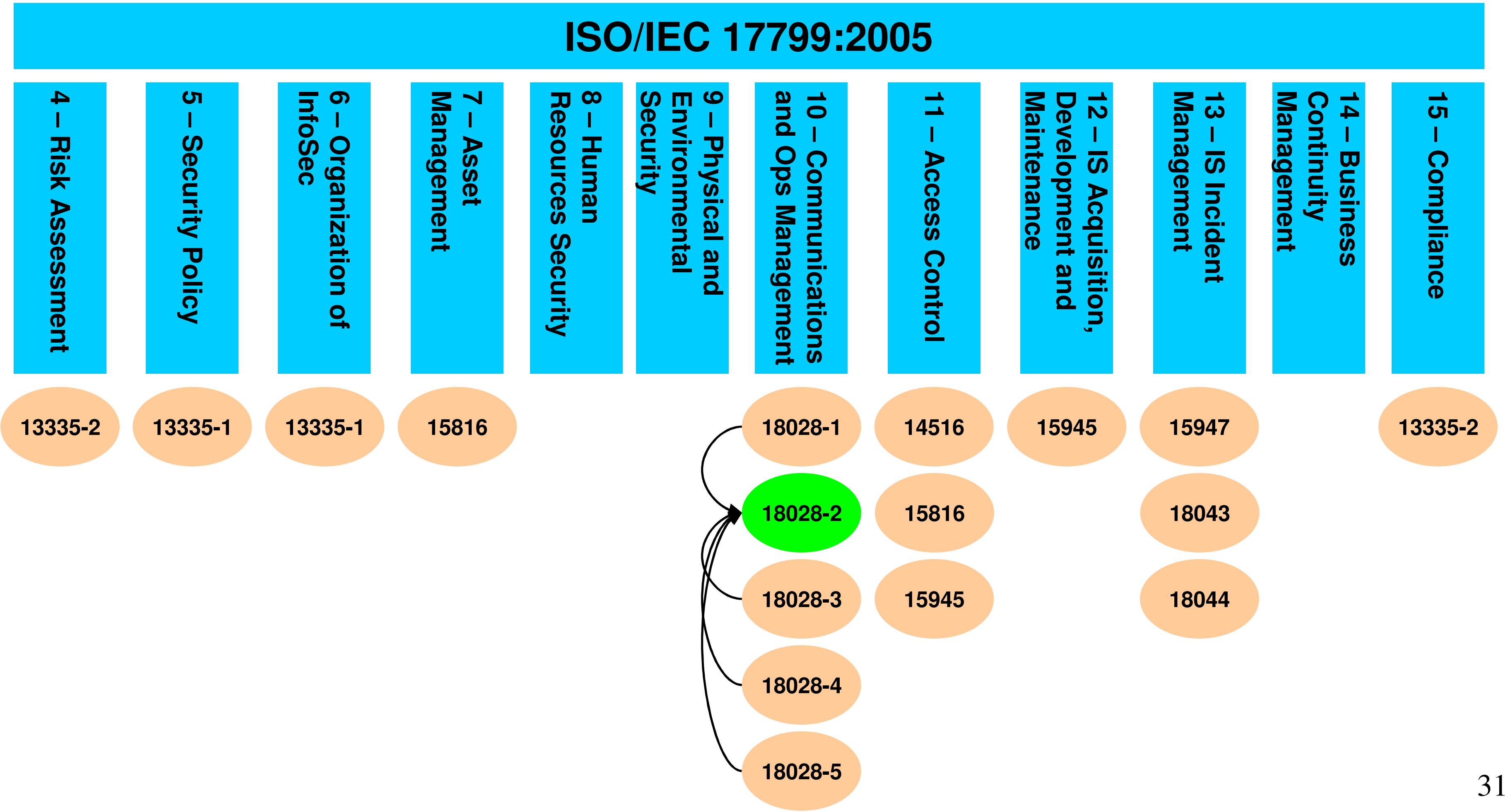
Layer Plane	Infrastructure	Services	Applications
Management	N/A	N/A	N/A
Control	N/A	N/A	N/A
End-User	Management software Email protection	DNS	Email client Web browser

Relevance of ITU-T X.805 to today's networks

- Comprehensive, end-to-end network view of security
- Applies to any network technology
  - Any layer of the protocol stack
  - 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 and service provider, government needs

Relevance of ITU-T X.805 to ISO/IEC 17799

- Complements ISO/IEC 17799:2005



ISO/IEC 17799:2005

4 – Risk Assessment	5 – Security Policy	6 – Organization of InfoSec	7 – Asset Management	8 – Human Resources Security	9 – Physical and Environmental Security	10 – Communications and Ops Management	11 – Access Control	12 – IS Acquisition, Development and Maintenance	13 – IS Incident Management	14 – Business Continuity Management	15 – Compliance
13335-2	13335-1	13335-1	15816			18028-1	14516	15945	15947		13335-2
						18028-2	15816		18043		
						18028-3	15945		18044		
						18028-4					
						18028-5					

How the industry benefits

- End-user
  - A framework to help CIO to see where are the essential areas of the network to secure.
- Consultant
  - Use it to design a secure design based on industry best practices, taking all perspectives into consideration.
- Auditor
  - Use it to review the security design of the network.
- Vendor
  - Leverage it to assure customers that following this standard will not lead to a compromise their network.

ITU-T X.805 current and future roadmap

- Officially adopted as ISO/IEC 18028 Part 2 on 1 Feb 2006.
- More X.805 standards going to be produced:
  - Network security certification
  - Division the security features between the network and the users (To be known as X.805+)
- Lucent has done a PCI mapping to ISO 18028 Part 2.
- Lucent going to roll out X.805 certification and training in the near future.

To know more about ITU-T X.805 …

- Please email me at
  - timmeng@lucent.com

THANK YOU.