T1M1/2003-039 R3
July 9, 2003

T1M1: Management Plane Security Standard (T1.276)

Presentation Contributors and Liaison Representatives:

Mike Fargano - T1M1 Chair, **michael.fargano@qwest.com**

Jim Stanco - T1M1 Vice Chair (previous), **jim.stanco@aol.com**

Lakshmi Raman - T1M1.5 Chair, **lraman@sunreyes.com**

Mike McGuire - T1M1 Security Team Lead, **mm8631@sbc.com**

Rod Wallace - T1M1 Security SME, **rod.wallace@nortelnetworks.com**

Chris Lonvick - T1M1 Security SME, **clonvick@cisco.com**

Note: This presentation is for general information sharing purposed only – refer to T1.276 American National Standard (and/or latest draft proposed ANS) for details and clarifications.

Outline

- Why Care?
- T1M1 Overview
- OAM&P Simplified Reference Model
- T1M1 History in Security
- Management Plane Security:
  - Business Drivers/Case and Motivation
  - Objective
  - Driving Principles
  - Network Mgt Security Reference Model
  - Summary/Status, Challenges, Contributors

Why Care?

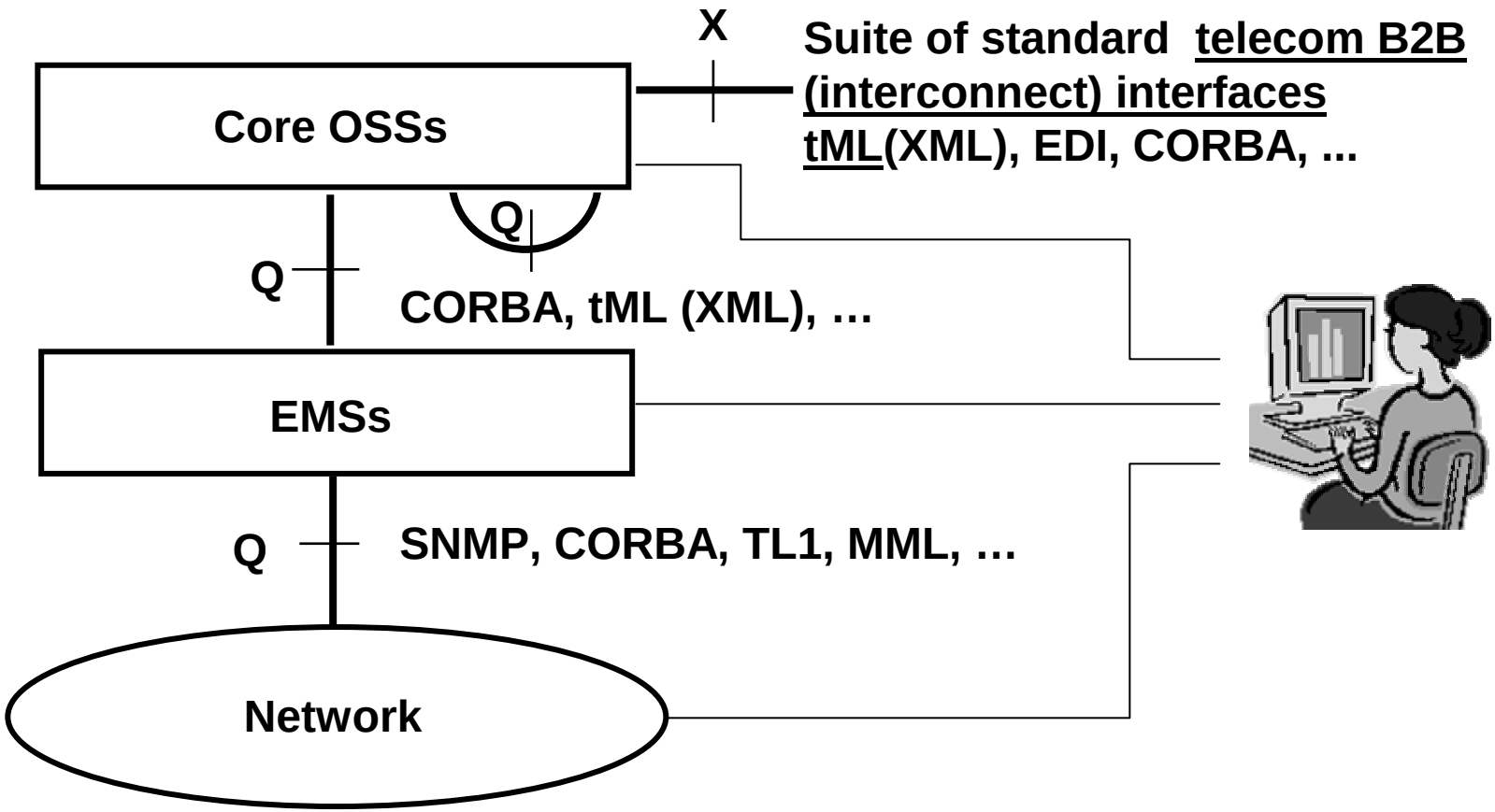
Network Management Security Risk

- From ATIS/T1 Press Release on T1M1 Security Work (http://www.atis.org/atis/press/pressreleases2002/100202.htm):
  - "A **security breach of a NE or OSS at the Management Plane** could include a major **incursion into the network** by an intruder, leading to **loss of integrity and service** of the elements and a **major network outage or disruption."**

T1M1 - Overview

- Telecom Network Management – Operations, Administration, Maintenance, and Provisioning (OAM&P); Technical Subcommittee of *Committee T1* – ANSI Accredited USA SDO
- Major Programs:
  - Common OAM&P Functionality and Technology
  - Inter-Administration OAM&P (OSS Interconnect)
  - Network Technology-Specific OAM&P
- **OAM&P Security: Part of each major program; bulk of work in Common OAM&P Functionality and Technology program**

OAM&P Simplified Systems Interface Reference Model



T1M1 History in Security

- Network Management Security Areas:
  - NEs and OSSs OAM&P interfaces
  - NS/EP, Emergency Telecom Services (ETS), Lawfully Authorized Electronic Surveillance
- 1980's to 2001: Many standards per above (see document *T1M1/2002-006* for history to 2001 ftp://ftp.t1.org/T1M1/M1.0/2002/2m100060.pdf)
- **2002/2003: *Management Plane Security Standard* – Collaboration with T1M1, NSTAC NSIE, Gov NSIE, + liaisons**

Mgt Plane Sec – Business Drivers

- Net Mgt Security Standard ***Business Drivers***:
  - ***Efficiency:*** **Reduced costs via commonality - economies of scale**
  - ***Effectiveness:*** **Common baseline for security functionality - reasonable risk management**
- Common baseline network management security requirements for NEs and OSSs to build network technology specific OAM&P security specifications and standards upon (e.g., optical network OAM&P security)

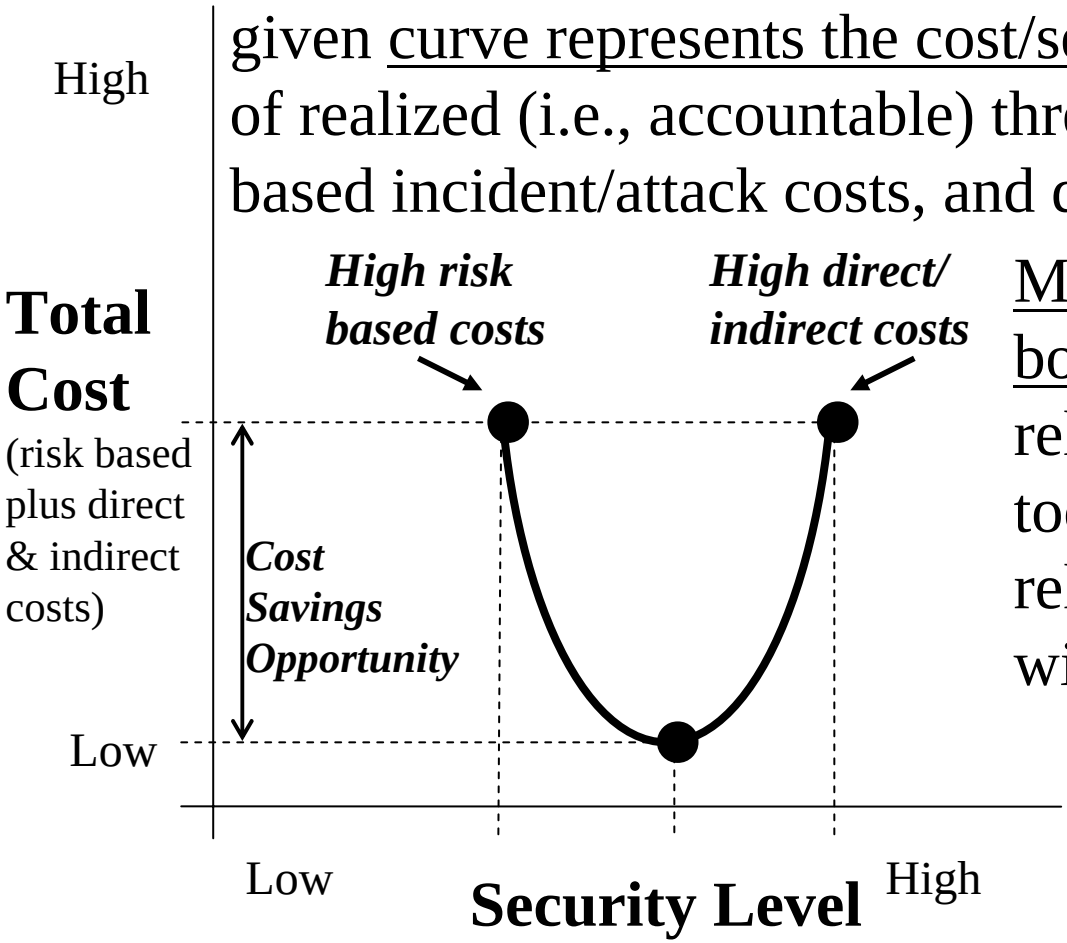
Mgt Plane Sec – Business Case

The general business rational to implement the Management Plane Security Standard is that it:

1. Raises the baseline OAM&P security requirements to meet the new (current) realized security risks and;
2. Provides for the new minimum cost zone between relatively too little security and too much security (with the relative high costs that come with these two extremes).

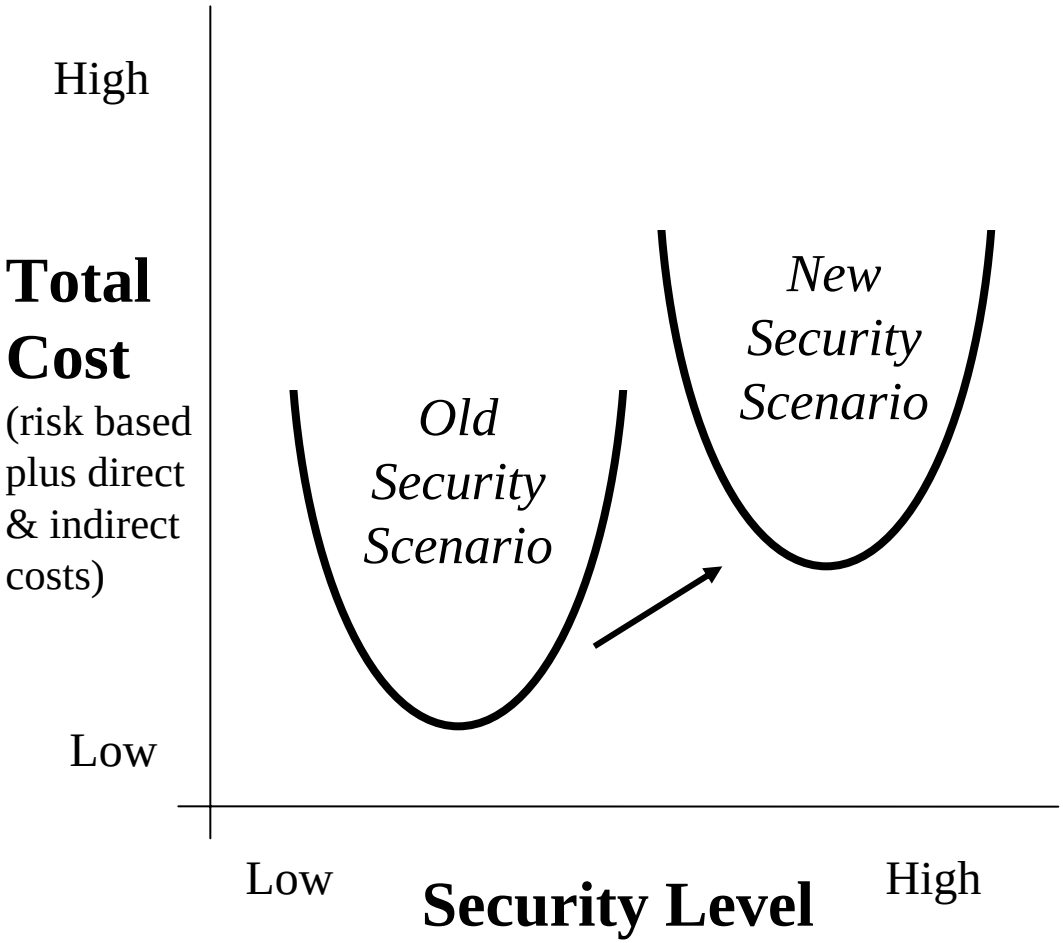
Mgt Plane Sec – Business Case Framework

Generic security business case is Risk Management based. A given curve represents the cost/security tradeoffs given a set of realized (i.e., accountable) threats, vulnerabilities, risk based incident/attack costs, and direct/indirect security costs.



Minimum cost zone is at the bottom of the curve - between relatively too little security and too much security (with the relative high costs that come with these two extremes).

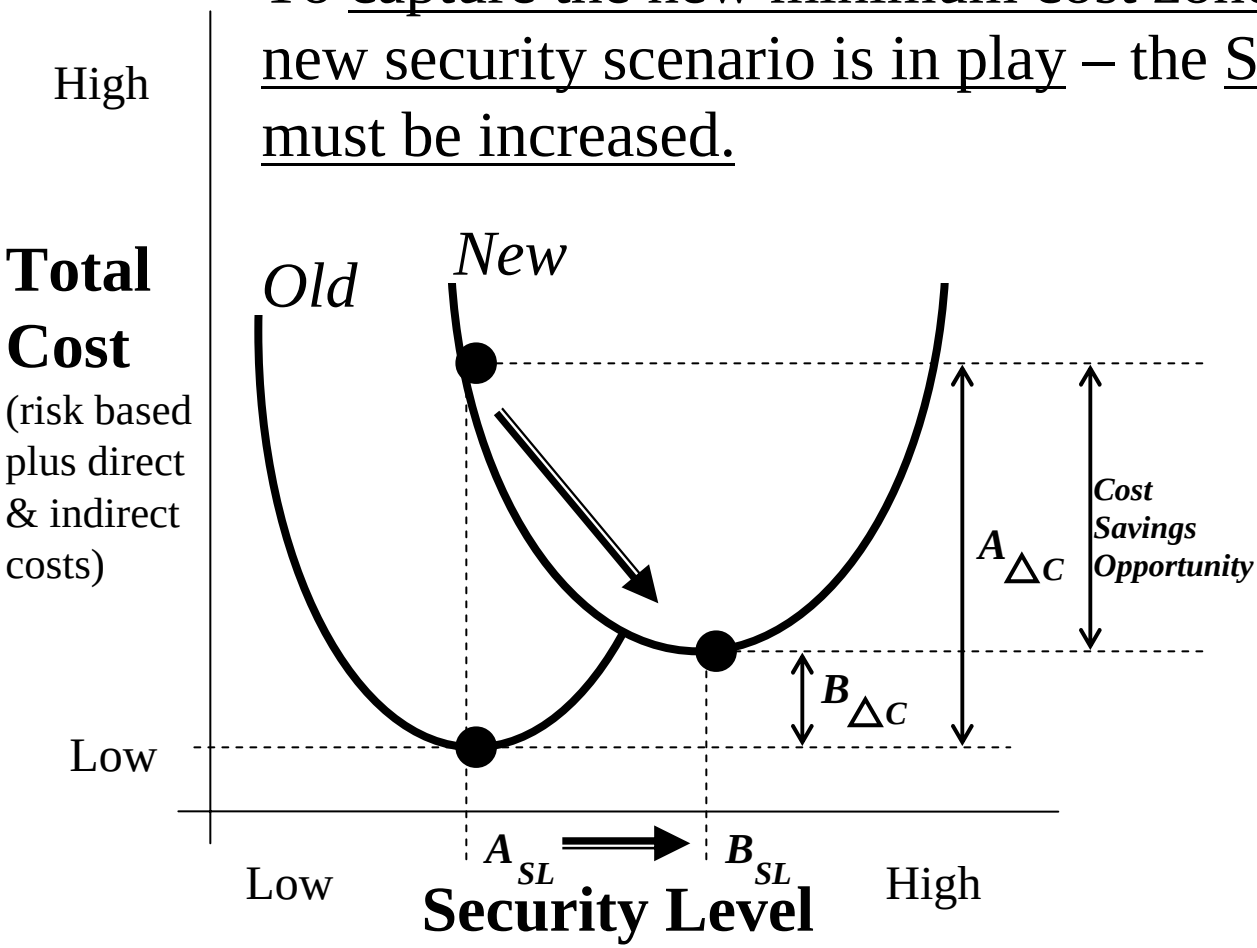
Mgt Plane Sec – Business Case with Increased Security Risks



New curve based on realization of new set of increased threats, vulnerabilities, incident/attack costs, and security costs – e.g., post 9/11

Mgt Plane Sec – Business Case: Cost Shifts w/ Increased Security Risks

To capture the new minimum cost zone while the new security scenario is in play – the Security Level must be increased.



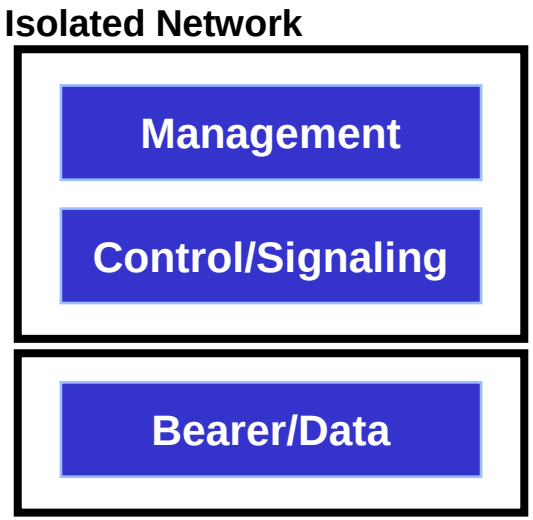
Being at the old minimum cost Security Level while the new security scenario is in play puts an organization in a relatively high Total Cost position.

Mgt Plane Sec – Motivation

- **A major concern to NSIE and T1M1 is that network infrastructure is a terrorist target, identified as part of National Critical Infrastructure.**
- **Our industry is transitioning to converged packet networks resulting in an increased sense of vulnerability.**
- **Service providers are specifying similar but different security requirements for products resulting in inconsistent vendor feature sets.**
- **System Integration and operations costs increase when dealing with vendors products that have differing security features and functionality.**
- **Infrastructure Security adds cost without generating additional revenue for both vendors and service providers alike.**

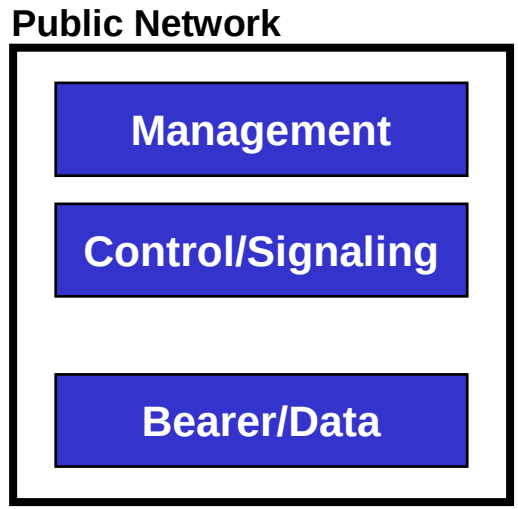
Mgt Plane Sec - Network (NGN) Security Challenges

Then



- Public traffic and management/control traffic were sent on separate networks.
- Threats in Public network were insulated from network management and control
- Management and Control network was easier to secure – e.g., known users.

Now



- Public traffic and management/control traffic are sent on the same network.
- Threats in Public network are now threats to network management and control
- Management and Control network now needs higher security level, e.g., security level that is applied to secure Public traffic.

Mgt Plane Sec - Objective

Define a consistent and standardized set of baseline network element and network management security requirements.

Standardize this set of security requirements within standards organizations such as T1M1 and ITU-T (SG4).

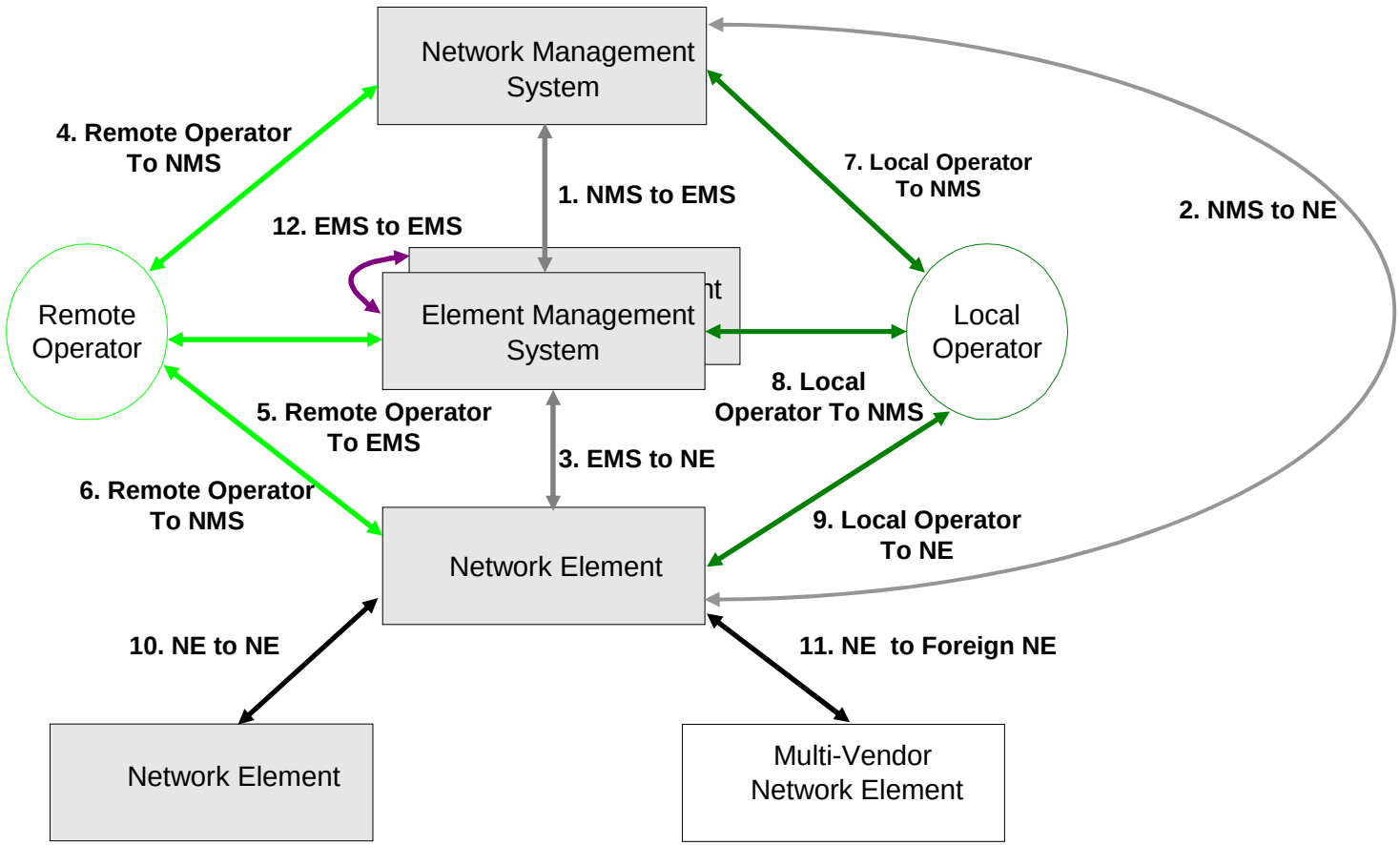
<u>These requirements will:</u>

- Ensure a minimal baseline of security throughout the industry.
- Provide vendors with a standard set of design objectives in relation to product and network security features.
- Make it easier for service providers to procure & build a secure infrastructure comprised of multiple vendor platforms.

Mgt Plane Sec - Key Principles

- **Secure management traffic with strong encryption and authentication.**
- **Authenticate and attribute all management actions.**
- **Maintain secure logs for all of the above.**

Network Management Security Reference Model



Mgt Plane Sec - Summary/Status

- Started work in NSIE with intent to make OAM&P security best practice recommendations public. NSIE and T1M1 agreed that T1M1 adoption was an effective means to make document public and standard.
  - **Status: Draft Standard (T1.276) Letter Ballot process <u>completed</u> - see document T1M1.5/2003-007R5 – Final (official) publication version should be available by end of July 2003.**
- Recommendations brought to the NRIC VI Workgroup 1B for inclusion in Cyber-security OAM Best Practices.
- Submitted to the ITU-T (SG4) for adoption as an International Standard (ITU-T Recommendation).

Mgt Plane Sec – Challenges

- To have the standard used and implemented - ASAP
  - There is evidence that this is happening.

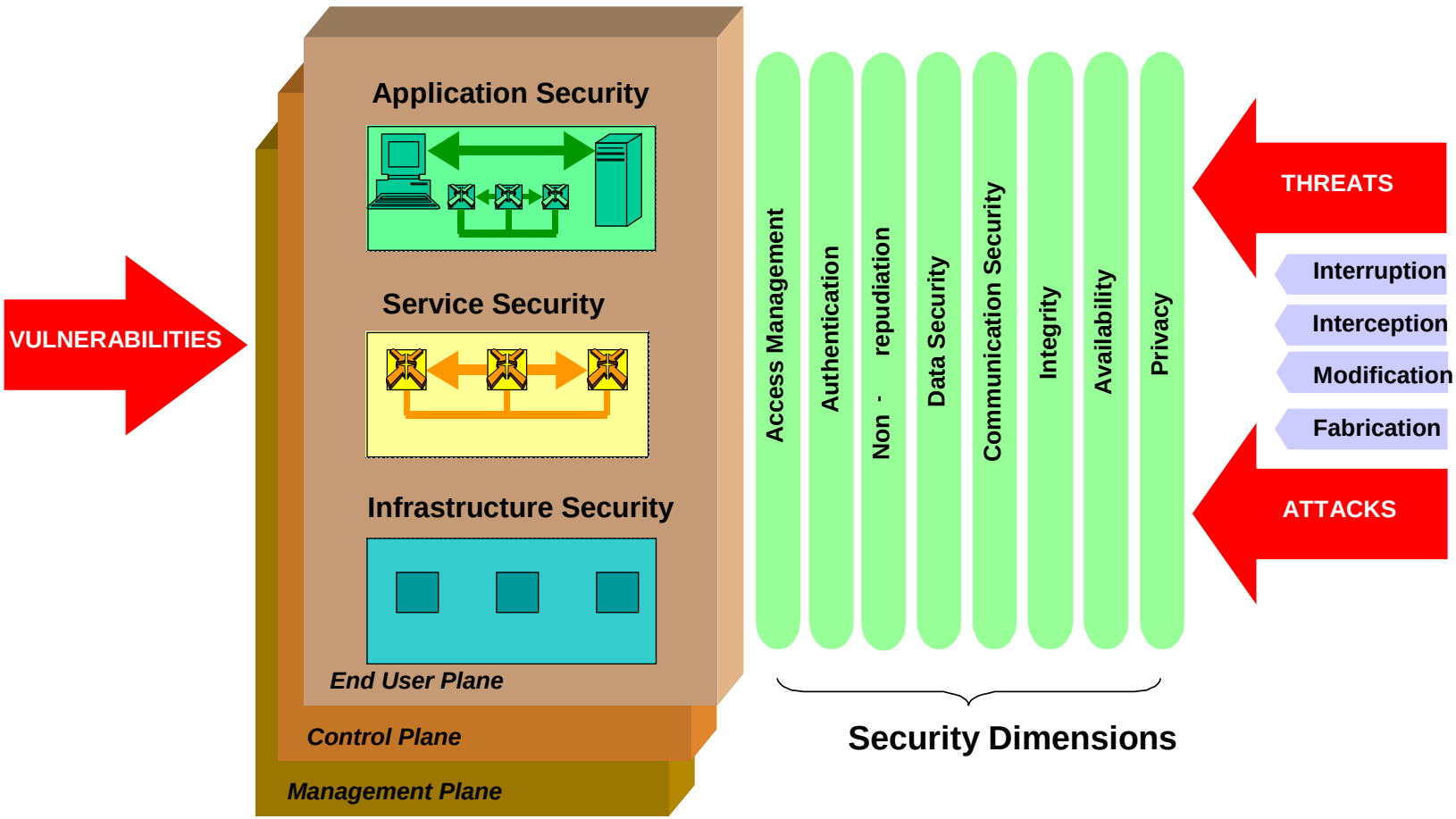
- Wide spread adoption of the standard.
  - Vendors and Service Provider contributors are working this now.

Mgt Plane Sec – Key Contributors

BellSouth	Booz-Allen Hamilton
BT	Cisco
DoD/NorAD	Harris
Lucent	Nortel Networks
Qwest	SBC
Siemens	Telcordia
Verizon	Worldcom

Management Plane Security
Appendix: Backup Slides

Security Framework Model



Document Contents

Background and Scope

59 Mandatory Security Requirements

Examples

Document Annex

B	**ADDITIONAL SECURITY CONSIDERATIONS**	
B.1	**Applicability to Enterprise OAM&P**	
B.2	**CORBA, SNMP, XML, and SOAP**	
	B.2.1	CORBA
	B.2.2	SNMP Security
	B.2.3	XML
	B.2.4	SOAP
B.3	**Communications Assistance to Law Enforcement Act**	
B.4	**Physical Security Considerations**	
	B.4.1	Physical Premises Security
	B.4.2	Building Services
	B.4.3	Environmental and Geographical Threats
	B.4.4	Co-location Procedures
B.5	**Development Process**	
	B.5.1	Bootstrapping, Installation, and Failure Modes
	B.5.2	Patching Process
B.5.3	**Development Life Cycle Security**	
	B.5.3.1	Personnel Management
	B.5.3.2	Security Awareness and Training
	B.5.3.3	Risk Management
	B.5.3.4	Requirements
	B.5.3.5	Design
	B.5.3.6	Separation of Duty
	B.5.3.7	Implementation
	B.5.3.8	Documentation
	B.5.3.9	Operating System……
	B.5.3.19	Secure Installation, Configuration, and Operation

Additional Security Considerations (Informational, outside the scope of the detailed security requirements)

Example Mandatory Requirements

Secure management traffic with STRONG ENCRYPTION and authentication:

M55: For each physical or logical interface that carries any MANAGEMENT TRAFFIC in an NE/MS, the NE/MS shall be configurable to secure MANAGEMENT TRAFFIC with STRONG AUTHENTICATION and symmetric or asymmetric encryption in order to provide confidentiality and integrity.

Authenticate and attribute all MANAGEMENT ACTIONS:

M12: Client AUTHENTICATION for logging in, logging, and auditing on each NE/MS shall be at least as strong as a User ID with a COMPLEX PASSWORD over a previously established TRUSTED PATH.

Manage security resources and configurations with integrity:

M25: On each NE/MS, a SYSTEM SECURITY ADMINISTRATOR shall be able to execute all of the CRITICAL SECURITY MANAGEMENT ACTIONS.

Maintain secure logs for all of the above:

M31: Each NE/MS shall be able to log each CRITICAL SECURITY ADMINISTRATION ACTION, each login attempt and its result, and each logout or SESSION termination.

Link to the Draft Standard (T1.276)

Final *Working* Document Number: T1M1.5/2003-007R5

Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane

“New File” (pre-archived) at:

ftp://ftp.t1.org/T1M1/NEW-T1M1.5/3m150075.pdf

Or, moved to archive at:

ftp://ftp.t1.org/T1M1/M1.5/2003/3m150075.pdf