THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

Operations, Administration, Maintenance, and Provisioning (OAM&P) Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane

August 28, 2003

1.0 INTRODUCTION

Executive Orders, Presidential directives, and Presidential commissions (e.g., the President's Commission on Critical Infrastructure Protection [PCCIP]), have specified infrastructures as national assets that are critical to the defense and economic security of the United States. Telecommunications is one of these critical infrastructures, as cited in the PCCIP report. As such, security for the network management functions controlling this infrastructure is essential. Many standards for network management security exist; however, compliance is low and implementations are inconsistent across the various telecommunications equipment and software providers. In addition, service providers are specifying similar but different requirements for products, which results in inconsistent vendor feature sets and potentially higher costs for vendors. Finally, as the telecommunications industry transitions to a converged network environment, new security challenges are introduced; and threats in the public network now become threats in the management and control planes.

Recognizing these trends, the President's National Security Telecommunications Advisory Committee (NSTAC) Network Security Information Exchange (NSIE) and the Government NSIE established the Security Requirements Working Group (SRWG) in 2002 to examine the security requirements for controlling access to the public switched network, in particular with respect to the emerging next generation network. In the telecommunications industry, this access incorporates operation, administration, maintenance, and provisioning (OAM&P) for network elements and various supporting systems and databases (i.e., operational support system).

Members of the SRWG, representing a cross-section of telecommunications carriers and vendors, developed an initial list of security requirements that would allow vendors, Government departments and agencies, and service providers to implement a secure telecommunications network management infrastructure. This initial list of security requirements was developed as a consensus document and submitted as a contribution to the Alliance for Telecommunications Industry Solutions (ATIS) Committee T1 – Telecommunications, Working Group T1M1.5 OAM&P Architecture, Interface and Protocols for consideration as a standard.

Representatives from T1M1.5, the NSTAC NSIE, the Government NSIE, and T1M1 liaison organizations further refined the initial document and developed the standard entitled *Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane*. Committee T1 approved the standard (T1.276-2003) in July 2003. An extract of T1.276-2003 is attached as Appendix B; it is included here for informational purposes only. A business case presentation developed in support of the OAM&P Security Requirements standard is attached as Appendix C. Future plans for the standard include submitting it to the International Telecommunication Union for consideration as an international standard.

Previous NSIE public network risk assessments have also documented the management plane's vulnerabilities and susceptibility to intruder attacks. Because an increasing number of networks are closely tied to intranets, these networks are susceptible to hacker threats. Furthermore, the lack of standards to address this issue enables intruders to penetrate vulnerabilities and further

deteriorate the telecommunications networks. Therefore, an urgent need exists for this baseline standard to provide much-needed security mechanisms for telecommunications carriers and vendors to implement.

The current standard addresses only one aspect (i.e., the management plane) of an overall end-to-end security solution. T1.276-2003 addresses security for network element, management system, and element management system equipment only; it does not specifically address security for other equipment, such as customer premises equipment. Separate and apart from the T1.276-2003 requirements, the current standard assumes that effective hardware and software controls provided by the operating system (OS) protect the data and resources being managed.

Authors of the standard were especially concerned with security of management traffic as it traverses networks mixed with end-user traffic. This was a driving factor in focusing the standard, which was ultimately developed around the following design principles—

- Isolation of management traffic from customer traffic
- Effective security policies that are definable, flexible, enforceable, auditable, verifiable, reliable, and usable,
- Strong authentication, authorization, and accounting
- Implementation of available security mechanisms
- Path for improvement
- Technical feasibility
- Consistent with standard operating procedures of well-run network management operations
- Use of ideas and concepts that are already standardized.

Finally, as indicated in the appendix to T1.276-2003, security is an integral part of software engineering. To develop a secure product, secure programming techniques and secure protocols must be used. Non-secure programming techniques can circumvent the best security protocols and mechanisms. For example, if a programmer does not manage buffers properly, a buffer overflow may occur and provide more privilege to a user than is appropriate. Vendors should follow formal documented development processes. Secure programming best practices must be followed in design, development, testing, and distribution of software. As the T1.276-2003 standard is developed, this concept could be incorporated into the standard or a companion standard.

2.0 CONCLUSIONS AND RECOMMENDATIONS

2.1 Coordination of the Standard with Other Standards and Further Development of the Standard

The T1.276-2003 standard focuses on the broad telecommunications sector needs, including technical, operational, and management issues. The underlying security postures espoused by the T1.276-2003 standard are aligned with the principles outlined in the ISO/IEC 15408 Common Criteria. Successful application of the standard will provide a baseline security model for the OS. Further security of the OS and related components must be reviewed using a

standard designed for that purpose and appropriate to the specific service provider's needs. In particular, the degree to which an OS complies with the ISO/IEC 15408 Common Criteria protection profiles may be applied in evaluating security for the computing environment.

Nevertheless, some overlap may exist between the requirements suggested by the T1.276-2003 standard and other standards, including Common Criteria profiles and various Federal Information Processing Standards (FIPS). As the standard matures, standards bodies should refine it to avoid possible conflicts resulting from unnecessary overlap in the areas of the organizations, information technology systems, or applications covered therein.

Therefore, the President should:

> Direct the National Institute of Standards and Technology (NIST) to review the T1.276-2003 standard. If a review finds a conflict between the T1.276-2003 standard and existing FIPS standards and NIST publications, NIST should make these conflicts known to the appropriate standards bodies.

2.2 Adoption of the Standard for Telecommunications Use

As customers and vendors implement T1.276-2003, OAM&P security will improve and they will be better positioned to address current security threats and risks. The standard provides vendors with a common set of requirements to build against and provides Government and commercial customers with a standard set of requirements that can be used to specify the minimum security specifications that providers must meet to implement a secure network management infrastructure.

Therefore, the President should:

> Encourage Federal departments and agencies to use the T1.276-2003 standard in requests for proposals, as appropriate.

2.3 Adaptation of the Standard to Other Critical Infrastructures

Although the requirements outlined in the standard employ telecommunications terms and formats, the underlying principles should apply equally to the management of computing elements in the other infrastructures. Other critical infrastructures may wish to modify and apply those recommendations that are appropriate to their respective infrastructure.

Therefore, the President should:

> Encourage other infrastructures through the Department of Homeland Security to consider the elements of the T1.276-2003 standard as a baseline for security requirements and adapt appropriate requirements for their respective infrastructure.

APPENDIX A

NSTAC OAM&P STANDARD WORKING GROUP MEMBERSHIP

Chair:

Jack Edwards	Nortel Networks

Members:

Jonathan Boynton	SBC
Kathryn Condello	CTIA
Anne Frantzen	Lucent
Vernon Joyner	Raytheon
Rick Kemper	CTIA
Hank Kluepfel	SAIC
Phil Reitinger	Microsoft

Other Participants:

Rick Kuhn	NIST

APPENDIX B

EXTRACT of T1.276-2003

An extract of the T1.276-2003 standard entitled *OAM&P Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane* is attached below. This extract includes the table of contents, key paragraphs, and a few requirements contained within the T1.276-2003 standard. T1.276-2003 can be purchased through the Alliance for Telecommunications Industry Solutions Document Center, https://www.atis.org/atis/docstore/doc_display.asp?ID=1924 or http://www.atis.org/doccenter.shtml. The standard is approximately 60 pages in length; and a paper copy can be purchased for $166, while the electronic download costs $151. Individuals from the member companies/organizations of Committee T1 can obtain a complimentary download of the standard.

T1.276-2003 TABLE OF CONTENTS

T1.276-2003 EXTRACTED TEXT

In some telecommunications networks, management traffic is often transmitted on a separate network from that carrying the service provider's end-user traffic. In these networks, security threats to the management plane are completely isolated from any malicious activity on the end-user plane. The management plane is relatively easy to secure because access to this plane is restricted to known administrators and traffic is restricted to known management activities. However, in some cases management traffic is combined on a single network with the service provider's end-user traffic. Combining traffic in this manner minimizes costs by requiring only a single integrated network infrastructure; however, many new security challenges are introduced. Threats in the end-user plane now become threats to the management and control planes. The management plane now becomes accessible to the multitude of end-users and many types of malicious activities become possible. The purpose of this document is to recommend minimum baseline security mechanisms to help mitigate security risks in the management of telecommunications networks.

To provide a complete end-to-end solution, all security measures (e.g., access control, authentication) should be applied to each type of network activity (i.e., management plane activity, control plane activity, and end user plane activity) for the network infrastructure, network services, and network applications. This document focuses specifically on the security aspect of the management plane for network elements (NE) and management systems (MS), which are part of the network infrastructure. As such, the document addresses only one aspect of an overall end-to-end security solution, but may be used as a starting point for subsequent documents addressing the security of "control" and "end user" planes, as appropriate.

The requirements in this standard are applicable to NEs and MSs to be deployed in the future. For NEs in the network that do not meet all the mandatory security requirements, the overall security requirements at the network architecture design should be supported. This document addresses security for NE, MS, and element management system (EMS) equipment, and does not specifically address security for other equipment such as customer premises equipment (e.g., voice over Internet Protocol [IP] telephones) or independent test gear. For such other equipment, all mandatory requirements in this document should be considered objective recommendations.

T1.276-2003 EXTRACTED REQUIREMENTS

M-23: Each NE/MS shall store login passwords in a nonvolatile and one-way encrypted manner. As an exception to one-way encryption, symmetrically encrypted passwords may be used for passwords that need to be decrypted for internal, transient use in trusted system-to-system communication or single sign-on.

M-24: Each NE/MS shall have at least five types of user roles: a SYSTEM SECURITY ADMINISTRATOR, an APPLICATION SECURITY ADMINISTRATOR, a SYSTEM ADMINISTRATOR, an APPLICATION ADMINISTRATOR, and an APPLICATION USER/OPERATOR. In the case of embedded systems without a separation of system and application, the NE shall support at least three

types of user roles: a combined SYSTEM SECURITY ADMINISTRATOR and APPLICATION SECURITY ADMINISTRATOR, a combined SYSTEM ADMINISTRATOR and APPLICATION ADMINISTRATOR, and an APPLICATION USER/OPERATOR.

APPENDIX C

T1M1: MANAGEMENT PLANE SECURITY STANDARD (T1.276) PRESENTATION

The following is a business case presentation developed in support of the T1.276-2003 standard.

T1M1/2003-039 R4
August 1, 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.

1

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

2

Why Care?

Network Management Security Risk

- Pre-work motivation from Oct 2, 2002 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."**

3

Why Care?

Network Management Security Risk (Cont.)

- From July 31, 2003 (post-work) ATIS/T1 Press Release on T1M1 Security Standard (http://www.atis.org/PRESS/pressreleases2003/073103.htm):
  - "In an age when the communications industry is **transitioning to next generation networks** with the **backdrop of terrorist threats** to America's critical infrastructure, it was **essential to develop a standard to drive the implementation of a common baseline for management plane security** to secure the management of the public telecommunications network."
  - "T1.276-2003 will be highlighted in a report by the NSTAC to President Bush…"

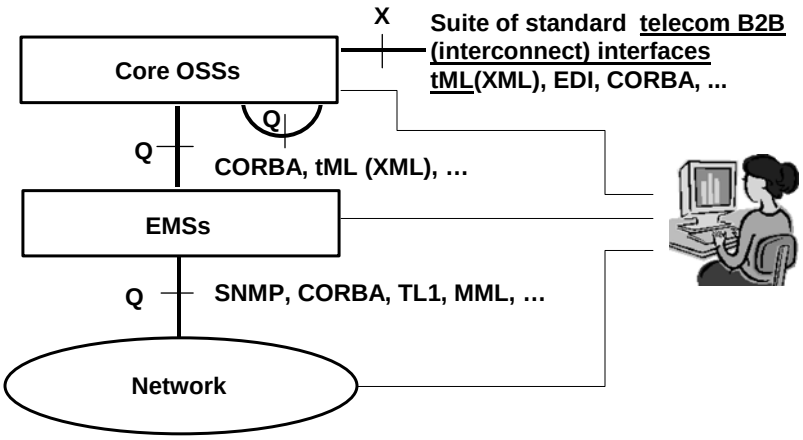
4

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**

4

OAM&P Simplified Systems Interface Reference Model



5

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**

6

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)

7

Mgt Plane Sec – Business Case

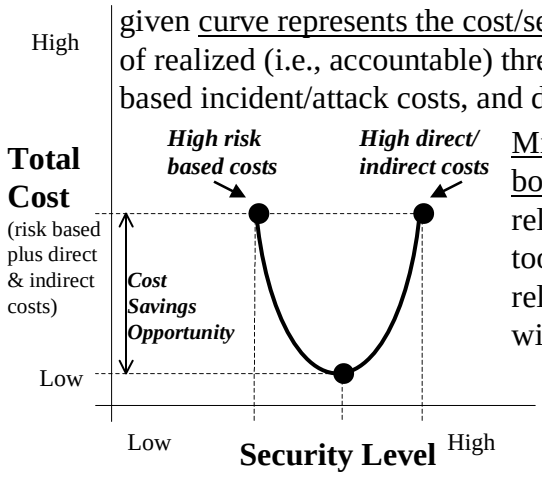
The general business rational to implement the Management Plane Security Standard is that it:

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).

8

Mgt Plane Sec – Business Case Framework

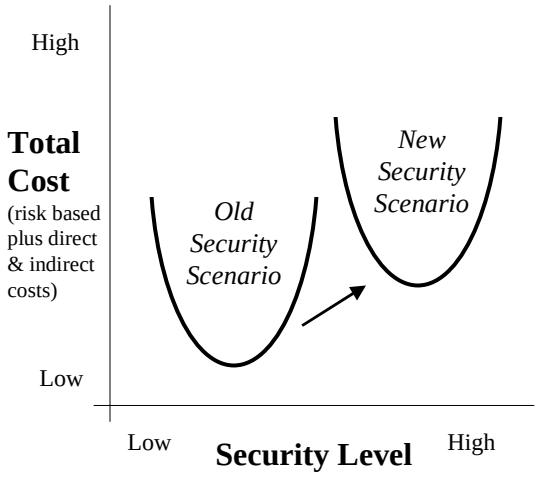
Generic security business case is Risk Management based. A given curve represents the cost/security tradeoffs given a set of realized (i.e., accountable) threats, vulnerabilities, risk based incident/attack costs, and direct/indirect security costs.



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).

9

Mgt Plane Sec – Business Case with Increased Security Risks

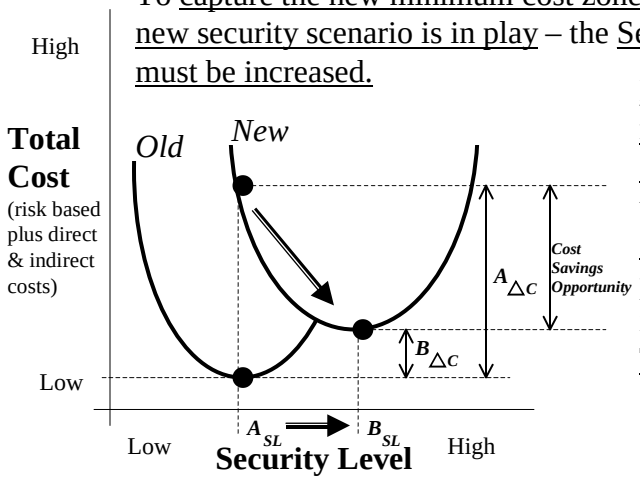


New curve based on realization of new set of increased threats, vulnerabilities, incident/attack costs, and security costs – e.g., post 9/11

10

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.

11

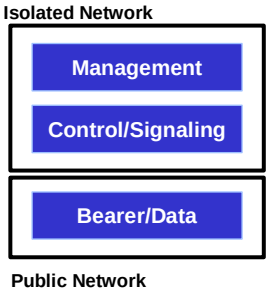
Mgt Plane Sec – Motivation

- **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.**

12

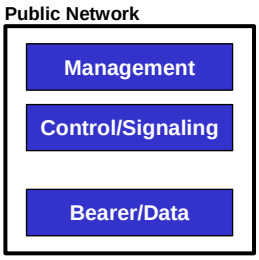
Mgt Plane Sec - Network (NGN) Security Challenges

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.

13

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.

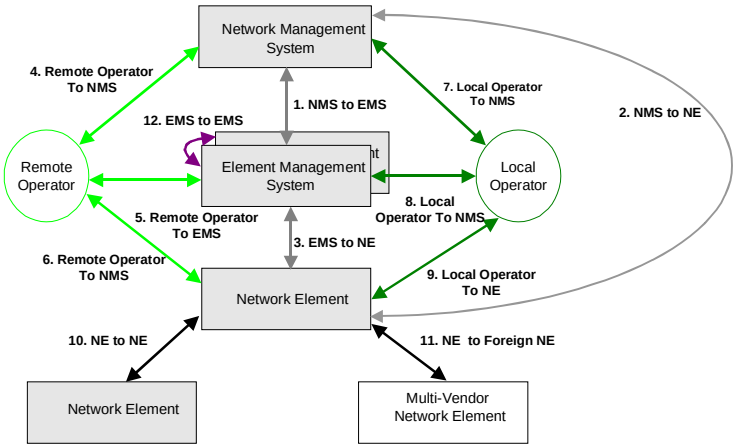
14

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.

15

Network Management Security Reference Model



16

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: Standard is Published – See next slide.**
- 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).

18

T1.276-2003 Reference and Link

- **T1.276-2003, *OAM&P Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane***
- The standards document can be purchased through the ATIS Document Center, **http://www.atis.org/doccenter.shtml** (a complementary download is available to Committee T1 Members)
- Direct Link to Standards Document: **https://www.atis.org/atis/docstore/doc_display.asp?ID=1924**

19

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.

18

Mgt Plane Sec – Key Contributors

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

19