

Network Working Group
Internet-Draft
Expires: October 21, 2006

C. Lonvick
D. Spak
Cisco Systems
April 19, 2006

Security Best Practices Efforts and Documents
draft-ietf-opsec-efforts-03.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on October 21, 2006.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This document provides a snapshot of the current efforts to define or apply security requirements in various Standards Developing Organizations (SDO).

Table of Contents

1.	Introduction	5
2.	Conventions Used in This Document	7
3.	Format of this Document	8
4.	Online Security Glossaries	9
4.1.	ATIS Telecom Glossary 2000	9
4.2.	Critical Infrastructure Glossary of Terms and Acronyms	9
4.3.	Internet Security Glossary - RFC 2828	9
4.4.	Compendium of Approved ITU-T Security Definitions	10
4.5.	Microsoft Solutions for Security Glossary	10
4.6.	SANS Glossary of Security Terms	10
4.7.	USC InfoSec Glossary	10
5.	Standards Developing Organizations	11
5.1.	3GPP - Third Generation Partnership Project	11
5.2.	3GPP2 - Third Generation Partnership Project 2	11
5.3.	ANSI - The American National Standards Institute	11
5.4.	ATIS - Alliance for Telecommunications Industry Solutions	11
5.4.1.	ATIS Network Performance, Reliability and Quality of Service Committee, formerly T1A1	12
5.4.2.	ATIS Network Interface, Power, and Protection Committee, formerly T1E1	12
5.4.3.	ATIS Telecom Management and Operations Committee, formerly T1M1 OAM&P	12
5.4.4.	ATIS Ordering and Billing Forum regarding T1M1 O&B	12
5.4.5.	ATIS Wireless Technologies and Systems Committee, formerly T1P1	13
5.4.6.	ATIS Packet Technologies and Systems Committee, formerly T1S1	13
5.4.7.	ATIS Protocol Interworking Committee, regarding T1S1	13
5.4.8.	ATIS Optical Transport and Synchronization Committee, formerly T1X1	13
5.5.	CC - Common Criteria	13
5.6.	DMTF - Distributed Management Task Force, Inc.	14
5.7.	ETSI - The European Telecommunications Standard Institute	14
5.8.	GGF - Global Grid Forum	14
5.9.	IEEE - The Institute of Electrical and Electronics Engineers, Inc.	14
5.10.	IETF - The Internet Engineering Task Force	14
5.11.	INCITS - InterNational Committee for Information Technology Standards	15
5.12.	INCITS Technical Committee T11 - Fibre Channel Interfaces	15
5.13.	ISO - The International Organization for Standardization	15

5.14.	ITU - International Telecommunication Union	15
5.14.1.	ITU Telecommunication Standardization Sector - ITU-T	15
5.14.2.	ITU Radiocommunication Sector - ITU-R	16
5.14.3.	ITU Telecom Development - ITU-D	16
5.15.	OASIS - Organization for the Advancement of Structured Information Standards	16
5.16.	OIF - Optical Internetworking Forum	16
5.17.	NRIC - The Network Reliability and Interoperability Council	16
5.18.	National Security Telecommunications Advisory Committee (NSTAC)	17
5.19.	TIA - The Telecommunications Industry Association	17
5.20.	Web Services Interoperability Organization (WS-I)	17
6.	Security Best Practices Efforts and Documents	18
6.1.	3GPP - TSG SA WG3 (Security)	18
6.2.	3GPP2 - TSG-S Working Group 4 (Security)	18
6.3.	American National Standard T1.276-2003 - Baseline Security Requirements for the Management Plane	18
6.4.	DMTF - Security Protection and Management (SPAM) Working Group	19
6.5.	DMTF - User and Security Working Group	19
6.6.	ATIS Security & Emergency Preparedness Activities	19
6.7.	ATIS Work-Plan to Achieve Interoperable, Implementable, End-To-End Standards and Solutions	19
6.7.1.	ATIS Work on Packet Filtering	20
6.8.	ATIS Work on the NGN	20
6.9.	Common Criteria	20
6.10.	ETSI	21
6.11.	GGF Security Area (SEC)	21
6.12.	Information System Security Assurance Architecture	21
6.13.	Operational Security Requirements for IP Network Infrastructure : Advanced Requirements	22
6.14.	INCITS Technical Committee T4 - Security Techniques	22
6.15.	INCITS CS1 - Cyber Security	22
6.16.	ISO Guidelines for the Management of IT Security - GMITS	22
6.17.	ISO JTC 1/SC 27	23
6.18.	ITU-T Study Group 2	24
6.19.	ITU-T Recommendation M.3016	24
6.20.	ITU-T Recommendation X.805	25
6.21.	ITU-T Study Group 16	25
6.22.	ITU-T Study Group 17	25
6.23.	Catalogue of ITU-T Recommendations related to Communications System Security	25
6.24.	ITU-T Security Manual	26
6.25.	ITU-T NGN Effort	26
6.26.	NRIC VI Focus Groups	26

6.27.	OASIS Security Joint Committee	27
6.28.	OASIS Security Services TC	27
6.29.	OIF Implementation Agreements	27
6.30.	TIA	28
6.31.	WS-I Basic Security Profile	28
7.	Security Considerations	29
8.	IANA Considerations	30
9.	Acknowledgments	31
10.	Changes from Prior Drafts	32
11.	Normative References	33
	Authors' Addresses	34
	Intellectual Property and Copyright Statements	35

1. Introduction

The Internet is being recognized as a critical infrastructure similar in nature to the power grid and a potable water supply. Just like those infrastructures, means are needed to provide resiliency and adaptability to the Internet so that it remains consistently available to the public throughout the world even during times of duress or attack. For this reason, many SDOs are developing standards with hopes of retaining an acceptable level, or even improving this availability, to its users. These SDO efforts usually define themselves as "security" efforts. It is the opinion of the authors that there are many different definitions of the term "security" and it may be applied in many diverse ways. As such, we offer no assurance that the term is applied consistently throughout this document.

Many of these SDOs have diverse charters and goals and will take entirely different directions in their efforts to provide standards. However, even with that, there will be overlaps in their produced works. If there are overlaps then there is a potential for conflicts and confusion. This may result in:

Vendors of networking equipment who are unsure of which standard to follow.

Purchasers of networking equipment who are unsure of which standard will best apply to the needs of their business or organization.

Network Administrators and Operators unsure of which standard to follow to attain the best security for their network.

For these reasons, the authors wish to encourage all SDOs who have an interest in producing or in consuming standards relating to good security practices to be consistent in their approach and their recommendations. In many cases, the authors are aware that the SDOs are making good efforts along these lines. However, the authors do not participate in all SDO efforts and cannot know everything that is happening.

The OpSec Working Group met at the 61st IETF and agreed that this document could be a useful reference in producing the documents described in the Working Group Charter. The authors have agreed to keep this document current and request that those who read it will submit corrections or comments.

Comments on this document may be addressed to the OpSec Working Group or directly to the authors.

opsec@ops.ietf.org

2. Conventions Used in This Document

This document shall use the keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" to describe requirements. These keywords are to be interpreted as described in [[1](#)].

3. Format of this Document

The body of this document has three sections.

The first part of the body of this document, [Section 4](#), contains a listing of online glossaries relating to networking and security. It is very important that the definitions of words relating to security and security events be consistent. Inconsistencies between the useage of words on standards is unacceptable as it would prevent a reader of two standards to appropriately relate their recommendations. The authors of this document have not reviewed the definitions of the words in the listed glossaries so can offer no assurance of their alignment.

The second part, [Section 5](#), contains a listing of SDOs that appear to be working on security standards.

The third part, [Section 6](#), lists the documents which have been found to offer good practices or recommendations for securing networks and networking devices.

4. Online Security Glossaries

This section contains references to glossaries of network and computer security terms

4.1. ATIS Telecom Glossary 2000

<http://www.atis.org/tg2k/>

Under an approved T1 standards project (T1A1-20), an existing 5800-entry, search-enabled hypertext telecommunications glossary titled Federal Standard 1037C, Glossary of Telecommunication Terms was updated and matured into this glossary, T1.523-2001, Telecom Glossary 2000. This updated glossary was posted on the Web as a American National Standard (ANS).

4.2. Critical Infrastructure Glossary of Terms and Acronyms

http://www.ciao.gov/ciao_document_library/glossary/a.htm

The Critical Infrastructure Assurance Office (CIAO) was created to coordinate the Federal Government's initiatives on critical infrastructure assurance. While the glossary was not created as a glossary specifically for security terms, it is populated with many security related definitions, abbreviations, organizations, and concepts.

4.3. Internet Security Glossary - [RFC 2828](#)

<http://www.ietf.org/rfc/rfc2828.txt>

Created in May 2000, the document defines itself to be, "an internally consistent, complementary set of abbreviations, definitions, explanations, and recommendations for use of terminology related to information system security." The glossary makes the distinction of the listed definitions throughout the document as being:

- o a recommended Internet definition
- o a recommended non-Internet definition
- o not recommended as the first choice for Internet documents but something that an author of an Internet document would need to know
- o a definition that shouldn't be used in Internet documents

- o additional commentary or usage guidance

4.4. Compendium of Approved ITU-T Security Definitions

<http://www.itu.int/itudoc/itu-t/com17/activity/def004.html>

Addendum to the Compendium of the Approved ITU-T Security-related Definitions

<http://www.itu.int/itudoc/itu-t/com17/activity/add002.html>

These extensive materials were created from approved ITU-T Recommendations with a view toward establishing a common understanding and use of security terms within ITU-T.

4.5. Microsoft Solutions for Security Glossary

<http://www.microsoft.com/security/glossary/>

The Microsoft Solutions for Security Glossary was created to explain the concepts, technologies, and products associated with computer security. This glossary contains several definitions specific to Microsoft proprietary technologies and product solutions.

4.6. SANS Glossary of Security Terms

<http://www.sans.org/resources/glossary.php>

The SANS Institute (SysAdmin, Audit, Network, Security) was created in 1989 as, "a cooperative research and education organization." Updated in May 2003, SANS cites the NSA for their help in creating the online glossary of security terms. The SANS Institute is also home to many other resources including the SANS Intrusion Detection FAQ and the SANS/FBI Top 20 Vulnerabilities List.

4.7. USC InfoSec Glossary

http://www.usc.edu/org/infosec/resources/glossary_a.html

A glossary of Information Systems security terms compiled by the University of Southern California Office of Information Security.

5. Standards Developing Organizations

This section of this document lists the SDOs, or organizations that appear to be developing security related standards. These SDOs are listed in alphabetical order.

Note: The authors would appreciate corrections and additions. This note will be removed before publication as an RFC.

5.1. 3GPP - Third Generation Partnership Project

<http://www.3gpp.org/>

The 3rd Generation Partnership Project (3GPP) is a collaboration agreement formed in December 1998. The collaboration agreement is comprised of several telecommunications standards bodies which are known as "Organizational Partners". The current Organizational Partners involved with 3GPP are ARIB, CCSA, ETSI, ATIS, TTA, and TTC.

5.2. 3GPP2 - Third Generation Partnership Project 2

<http://www.3gpp2.org/>

Third Generation Partnership Project 2 (3GPP2) is a collaboration among Organizational Partners much like its sister project 3GPP. The Organizational Partners (OPs) currently involved with 3GPP2 are ARIB, CCSA, TTA, TTA, and TTC. In addition to the OPs, 3GPP2 also welcomes the CDMA Development Group and IPv6 Forum as Market Representation Partners for market advice.

5.3. ANSI - The American National Standards Institute

<http://www.ansi.org/>

ANSI is a private, non-profit organization that organizes and oversees the U.S. voluntary standardization and conformity assessment system. ANSI was founded October 19, 1918.

5.4. ATIS - Alliance for Telecommunications Industry Solutions

<http://www.atis.org/>

ATIS is a United States based body that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using pragmatic, flexible and open approach. Committee T1 as a group no longer exists as a result of the recent ATIS reorganization on January 1, 2004. ATIS has restructured the former

T1 technical subcommittees into full ATIS standards committees to easily identify and promote the nature of standards work each committee performs. Due to the reorganization, some groups may have a new mission and scope statement.

5.4.1. ATIS Network Performance, Reliability and Quality of Service Committee, formerly T1A1

<http://www.atis.org/0010/index.asp>

ATIS Network Performance, Reliability and Quality of Service Committee develops and recommends standards, requirements, and technical reports related to the performance, reliability, and associated security aspects of communications networks, as well as the processing of voice, audio, data, image, and video signals, and their multimedia integration.

5.4.2. ATIS Network Interface, Power, and Protection Committee, formerly T1E1

<http://www.atis.org/0050/index.asp>

ATIS Network Interface, Power, and Protection Committee develops and recommends standards and technical reports related to power systems, electrical and physical protection for the exchange and interexchange carrier networks, and interfaces associated with user access to telecommunications networks.

5.4.3. ATIS Telecom Management and Operations Committee, formerly T1M1 OAM&P

<http://www.atis.org/0130/index.asp>

ATIS Telecom Management and Operations Committee develops internetwork operations, administration, maintenance and provisioning standards, and technical reports related to interfaces for telecommunications networks.

5.4.4. ATIS Ordering and Billing Forum regarding T1M1 O&B

<http://www.atis.org/obf/index.asp>

The T1M1 O&B subcommittee has become part of the ATIS Ordering and Billing Forum.

The ATIS-sponsored Ordering and Billing Forum (OBF) provides a forum for customers and providers in the telecommunications industry to identify, discuss and resolve national issues which affect ordering,

billing, provisioning and exchange of information about access services, other connectivity and related matters.

5.4.5. ATIS Wireless Technologies and Systems Committee, formerly T1P1

<http://www.atis.org/0160/index.asp>

ATIS Wireless Technologies and Systems Committee develops and recommends standards and technical reports related to wireless and/or mobile services and systems, including service descriptions and wireless technologies.

5.4.6. ATIS Packet Technologies and Systems Committee, formerly T1S1

T1S1 was split into two separate ATIS committees: the ATIS Packet Technologies and Systems Committee and the ATIS Protocol Interworking Committee. PTSC is responsible for producing standards to secure signalling.

The basic document is PTSC-SEC-2005-059.doc which is in Letter Ballot at this time. It is expected to move to an ANSI standard.

5.4.7. ATIS Protocol Interworking Committee, regarding T1S1

T1S1 was split into two separate ATIS committees: the ATIS Packet Technologies and Systems Committee and the ATIS Protocol Interworking Committee. As a result of the reorganization of T1S1, these groups will also probably have a new mission and scope.

5.4.8. ATIS Optical Transport and Synchronization Committee, formerly T1X1

<http://www.atis.org/0240/index.asp>

ATIS Optical Transport and Synchronization Committee develops and recommends standards and prepares technical reports related to telecommunications network technology pertaining to network synchronization interfaces and hierarchical structures including optical technology.

5.5. CC - Common Criteria

<http://www.commoncriteriaportal.org/>

In June 1993, the sponsoring organizations of the existing US, Canadian, and European criterias (TCSEC, ITSEC, and similar) started the Common Criteria Project to align their separate criteria into a single set of IT security criteria.

5.6. DMTF - Distributed Management Task Force, Inc.

<http://www.dmtf.org/>

Founded in 1992, the DMTF brings the technology industry's customers and top vendors together in a collaborative, working group approach that involves DMTF members in all aspects of specification development and refinement.

5.7. ETSI - The European Telecommunications Standard Institute

<http://www.etsi.org/>

ETSI is an independent, non-profit organization which produces telecommunications standards. ETSI is based in Sophia-Antipolis in the south of France and maintains a membership from 55 countries.

Joint work between ETSI and ITU-T SG-17

http://docbox.etsi.org/OCG/OCG/GSC9/GSC9_JointT%26R/GSC9_Joint_011_Security_Standardization_in_ITU.ppt

5.8. GGF - Global Grid Forum

<http://www.gridforum.org/>

The Global Grid Forum (GGF) is a community-initiated forum of thousands of individuals from industry and research leading the global standardization effort for grid computing. GGF's primary objectives are to promote and support the development, deployment, and implementation of Grid technologies and applications via the creation and documentation of "best practices" - technical specifications, user experiences, and implementation guidelines.

5.9. IEEE - The Institute of Electrical and Electronics Engineers, Inc.

<http://www.ieee.org/>

IEEE is a non-profit, technical professional association of more than 360,000 individual members in approximately 175 countries. The IEEE produces 30 percent of the world's published literature in electrical engineering, computers and control technology through its technical publishing, conferences and consensus-based standards activities.

5.10. IETF - The Internet Engineering Task Force

<http://www.ietf.org/>

IETF is a large, international community open to any interested individual concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

5.11. INCITS - InterNational Committee for Information Technology Standards

<http://www.incits.org/>

INCITS focuses upon standardization in the field of Information and Communications Technologies (ICT), encompassing storage, processing, transfer, display, management, organization, and retrieval of information.

5.12. INCITS Technical Committee T11 - Fibre Channel Interfaces

<http://www.t11.org/index.htm>

T11 is responsible for standards development in the areas of Intelligent Peripheral Interface (IPI), High-Performance Parallel Interface (HIPPI) and Fibre Channel (FC). T11 has a project called FC-SP to define Security Protocols for Fibre Channel.

FC-SP Project Proposal:

ftp://ftp.t11.org/t11/admin/project_proposals/02-036v2.pdf

5.13. ISO - The International Organization for Standardization

<http://www.iso.org/>

ISO is a network of the national standards institutes of 148 countries, on the basis of one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. ISO officially began operations on February 23, 1947.

5.14. ITU - International Telecommunication Union

<http://www.itu.int/>

The ITU is an international organization within the United Nations System headquartered in Geneva, Switzerland. The ITU is comprised of three sectors:

5.14.1. ITU Telecommunication Standardization Sector - ITU-T

<http://www.itu.int/ITU-T/>

ITU-T's mission is to ensure an efficient and on-time production of

high quality standards covering all fields of telecommunications.

5.14.2. ITU Radiocommunication Sector - ITU-R

<http://www.itu.int/ITU-R/>

The ITU-R plays a vital role in the management of the radio-frequency spectrum and satellite orbits.

5.14.3. ITU Telecom Development - ITU-D

(also referred as ITU Telecommunication Development Bureau - BDT)

<http://www.itu.int/ITU-D/>

The Telecommunication Development Bureau (BDT) is the executive arm of the Telecommunication Development Sector. Its duties and responsibilities cover a variety of functions ranging from programme supervision and technical advice to the collection, processing and publication of information relevant to telecommunication development.

5.15. OASIS - Organization for the Advancement of Structured Information Standards

<http://www.oasis-open.org/>

OASIS is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards.

5.16. OIF - Optical Internetworking Forum

<http://www.oiforum.com/>

On April 20, 1998 Cisco Systems and Ciena Corporation announced an industry-wide initiative to create the Optical Internetworking Forum, an open forum focused on accelerating the deployment of optical internetworks.

5.17. NRIC - The Network Reliability and Interoperability Council

<http://www.nric.org/>

The purposes of the Committee are to give telecommunications industry leaders the opportunity to provide recommendations to the FCC and to the industry that assure optimal reliability and interoperability of telecommunications networks. The Committee addresses topics in the area of Homeland Security, reliability, interoperability, and broadband deployment.

5.18. National Security Telecommunications Advisory Committee (NSTAC)

<http://www.ncs.gov/nstac/nstac.html>

President Ronald Reagan created the National Security Telecommunications Advisory Committee (NSTAC) by Executive Order 12382 in September 1982. Since then, the NSTAC has served four presidents. Composed of up to 30 industry chief executives representing the major communications and network service providers and information technology, finance, and aerospace companies, the NSTAC provides industry-based advice and expertise to the President on issues and problems related to implementing national security and emergency preparedness (NS/EP) communications policy. Since its inception, the NSTAC has addressed a wide range of policy and technical issues regarding communications, information systems, information assurance, critical infrastructure protection, and other NS/EP communications concerns.

5.19. TIA - The Telecommunications Industry Association

<http://www.tiaonline.org/>

TIA is accredited by ANSI to develop voluntary industry standards for a wide variety of telecommunications products. TIA's Standards and Technology Department is composed of five divisions: Fiber Optics, User Premises Equipment, Network Equipment, Wireless Communications and Satellite Communications.

5.20. Web Services Interoperability Organization (WS-I)

<http://www.ws-i.org/>

WS-I is an open, industry organization chartered to promote Web services interoperability across platforms, operating systems, and programming languages. The organization works across the industry and standards organizations to respond to customer needs by providing guidance, best practices, and resources for developing Web services solutions.

6. Security Best Practices Efforts and Documents

This section lists the works produced by the SDOs.

6.1. 3GPP - TSG SA WG3 (Security)

<http://www.3gpp.org/TB/SA/SA3/SA3.htm>

TSG SA WG3 Security is responsible for the security of the 3GPP system, performing analyses of potential security threats to the system, considering the new threats introduced by the IP based services and systems and setting the security requirements for the overall 3GPP system.

Specifications:

<http://www.3gpp.org/ftp/Specs/html-info/TSG-WG--S3.htm>

Work Items:

<http://www.3gpp.org/ftp/Specs/html-info/TSG-WG--s3--wis.htm>

3GPP Confidentiality and Integrity algorithms:

<http://www.3gpp.org/TB/Other/algorithms.htm>

6.2. 3GPP2 - TSG-S Working Group 4 (Security)

http://www.3gpp2.org/Public_html/S/index.cfm

The Services and Systems Aspects TSG (TSG-S) is responsible for the development of service capability requirements for systems based on 3GPP2 specifications. Among its responsibilities TSG-S is addressing management, technical coordination, as well as architectural and requirements development associated with all end-to-end features, services and system capabilities including, but not limited to, security and QoS.

TSG-S Specifications:

http://www.3gpp2.org/Public_html/specs/index.cfm#tsgs

6.3. American National Standard T1.276-2003 - Baseline Security Requirements for the Management Plane

Abstract: This standard contains a set of baseline security requirements for the management plane. The President's National Security Telecommunications Advisory Committee Network Security Information Exchange (NSIE) and Government NSIE jointly established a Security Requirements Working Group (SRWG) 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 for network elements and various supporting systems and databases. Members of the SRWG, from 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 submitted as a contribution to Committee T1 - Telecommunications, Working Group T1M1.5 for consideration as a standard. The requirements outlined in this document will allow vendors, government departments and agencies, and service providers to implement a secure telecommunications network management infrastructure.

Documents:

<http://webstore.ansi.org/ansidocstore/product.asp?sku=T1%2E276%2D2003>

6.4. DMTF - Security Protection and Management (SPAM) Working Group

<http://www.dmtf.org/about/committees/spamWGCharter.pdf>

The Working Group will define a CIM Common Model that addresses security protection and detection technologies, which may include devices and services, and classifies security information, attacks and responses.

6.5. DMTF - User and Security Working Group

<http://www.dmtf.org/about/committees/userWGCharter.pdf>

The User and Security Working Group defines objects and access methods required for principals - where principals include users, groups, software agents, systems, and organizations.

6.6. ATIS Security & Emergency Preparedness Activities

[http://www.atis.org/atis/atisinfo/emergency/
security_committee_activities_T1.htm](http://www.atis.org/atis/atisinfo/emergency/security_committee_activities_T1.htm)

The link above contains the description of the ATIS Communications Security Model, the scopes of the Technical Subcommittees in relation to the security model, and a list of published documents produced by ATIS addressed to various aspects of network security.

6.7. ATIS Work-Plan to Achieve Interoperable, Implementable, End-To-End Standards and Solutions

<ftp://ftp.t1.org/T1M1/NEW-T1M1.0/3M101940.pdf>

The ATIS TOPS Security Focus Group has made recommendations on work items needed to be performed by other SDOs.

6.7.1. ATIS Work on Packet Filtering

A part of the ATIS Work Plan was to define how disruptions may be prevented by filtering unwanted traffic at the edges of the network. ATIS is developing this work in a document titled, "Traffic Filtering for the Prevention of Unwanted Traffic".

6.8. ATIS Work on the NGN

http://www.atis.org/tops/WebsiteDocuments/NGN/Working%20Docs/Part%20I/ATIS_NGN_Part_1_Issue1.pdf

In November 2004, ATIS released Part I of the ATIS NGN-FG efforts entitled, "ATIS Next Generation Network (NGN) Framework Part I: NGN Definitions, Requirements, and Architecture, Issue 1.0, November 2004."

6.9. Common Criteria

<http://www.commoncriteriaportal.org/>

Version 1.0 of the CC was completed in January 1996. Based on a number of trial evaluations and an extensive public review, Version 1.0 was extensively revised and CC Version 2.0 was produced in April of 1998. This became ISO International Standard 15408 in 1999. The CC Project subsequently incorporated the minor changes that had resulted in the ISO process, producing CC version 2.1 in August 1999. Version 3.0 was published in June 2005 and is available for comment.

The official version of the Common Criteria and of the Common Evaluation Methodology is v2.3 which was published in August 2005.

All Common Criteria publications contain:

Part 1: Introduction and general model

Part 2: Security functional components

Part 3: Security assurance components

Documents: Common Criteria V2.3

<http://www.commoncriteriaportal.org/public/expert/index.php?menu=2>

6.10. ETSI

<http://www.etsi.org/>

The ETSI hosted the ETSI Global Security Conference in late November, 2003, which could lead to a standard.

Groups related to security located from the ETSI Groups Portal:

OCG Security

3GPP SA3

TISPAN WG7

6.11. GGF Security Area (SEC)

<https://forge.gridforum.org/projects/sec/>

The Security Area (SEC) is concerned with various issues relating to authentication and authorization in Grid environments.

Working groups:

Authorization Frameworks and Mechanisms WG (AuthZ-WG) -

<https://forge.gridforum.org/projects/authz-wg>

Certificate Authority Operations Working Group (CAOPS-WG) -

<https://forge.gridforum.org/projects/caops-wg>

OGSA Authorization Working Group (OGSA-AUTHZ) -

<https://forge.gridforum.org/projects/ogsa-authz>

Grid Security Infrastructure (GSI-WG) -

<https://forge.gridforum.org/projects/gsi-wg>

6.12. Information System Security Assurance Architecture

IEEE Working Group - <http://issaa.org/>

Formerly the Security Certification and Accreditation of Information Systems (SCAISWG), IEEE Project 1700's purpose is to develop a draft Standard for Information System Security Assurance Architecture for ballot and during the process begin development of a suite of associated standards for components of that architecture.

Documents: <http://issaa.org/documents/index.html>

6.13. Operational Security Requirements for IP Network Infrastructure : Advanced Requirements

IETF [RFC 3871](#)

Abstract: This document defines a list of operational security requirements for the infrastructure of large ISP IP networks (routers and switches). A framework is defined for specifying "profiles", which are collections of requirements applicable to certain network topology contexts (all, core-only, edge-only...). The goal is to provide network operators a clear, concise way of communicating their security requirements to vendors.

Documents:

<ftp://ftp.rfc-editor.org/in-notes/rfc3871.txt>

6.14. INCITS Technical Committee T4 - Security Techniques

http://www.incits.org/tc_home/t4.htm

Technical Committee T4, Security Techniques, participates in the standardization of generic methods for information technology security. This includes development of: security techniques and mechanisms; security guidelines; security evaluation criteria; and identification of generic requirements for information technology system security services.

6.15. INCITS CS1 - Cyber Security

http://www.incits.org/tc_home/cs1.htm

INCITS/CS1 was established in April 2005 to serve as the US TAG for ISO/IEC JTC 1/SC 27 and all SC 27 Working Groups except WG 2 (INCITS/T4 serves as the US TAG to SC 27/WG 2).

The scope of CS1 explicitly excludes the areas of work on cyber security standardization presently underway in INCITS B10, M1 and T3; as well as other standard groups, such as ATIS, IEEE, IETF, TIA, and X9. INCITS T4's area of work would be narrowed to cryptography projects in ISO/IEC JTC 1/SC 27 WG 2 (Security techniques and mechanisms).

6.16. ISO Guidelines for the Management of IT Security - GMITS

Guidelines for the Management of IT Security -- Part 1: Concepts and models for IT Security

[http://www.iso.ch/iso/en/
CatalogueDetailPage.CatalogueDetail?CSNUMBER=21733&ICS1=35](http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=21733&ICS1=35)

Guidelines for the Management of IT Security -- Part 2: Managing and planning IT Security

[http://www.iso.org/iso/en/
CatalogueDetailPage.CatalogueDetail?CSNUMBER=21755&ICS1=35&ICS2=40&
ICS3=](http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=21755&ICS1=35&ICS2=40&ICS3=)

Guidelines for the Management of IT Security -- Part 3: Techniques for the management of IT Security

[http://www.iso.org/iso/en/
CatalogueDetailPage.CatalogueDetail?CSNUMBER=21756&ICS1=35&ICS2=40&
ICS3=](http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=21756&ICS1=35&ICS2=40&ICS3=)

Guidelines for the Management of IT Security -- Part 4: Selection of safeguards

[http://www.iso.org/iso/en/
CatalogueDetailPage.CatalogueDetail?CSNUMBER=29240&ICS1=35&ICS2=40&
ICS3=](http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=29240&ICS1=35&ICS2=40&ICS3=)

Guidelines for the Management of IT Security - Part 5: Management guidance on network security

[http://www.iso.org/iso/en/
CatalogueDetailPage.CatalogueDetail?CSNUMBER=31142&ICS1=35&ICS2=40&
ICS3=](http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=31142&ICS1=35&ICS2=40&ICS3=)

Open Systems Interconnection -- Network layer security protocol

[http://www.iso.org/iso/en/
CatalogueDetailPage.CatalogueDetail?CSNUMBER=22084&ICS1=35&ICS2=100&
ICS3=30](http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=22084&ICS1=35&ICS2=100&ICS3=30)

6.17. ISO JTC 1/SC 27

[http://www.iso.ch/iso/en/stdsdevelopment/techprog/workprog/
TechnicalProgrammeSCDetailPage.TechnicalProgrammeSCDetail?COMMID=143](http://www.iso.ch/iso/en/stdsdevelopment/techprog/workprog/TechnicalProgrammeSCDetailPage.TechnicalProgrammeSCDetail?COMMID=143)

Several security related ISO projects under JTC 1/SC 27 are listed here such as:

IT security techniques -- Entity authentication

Security techniques -- Key management

Security techniques -- Evaluation criteria for IT security

Security techniques -- A framework for IT security assurance

IT Security techniques -- Code of practice for information security management

Security techniques -- IT network security

Guidelines for the implementation, operation and management of Intrusion Detection Systems (IDS)

International Security, Trust, and Privacy Alliance -- Privacy Framework

6.18. ITU-T Study Group 2

<http://www.itu.int/ITU-T/studygroups/com02/index.asp>

Security related recommendations currently under study:

E.408 Telecommunication networks security requirements Q.5/2 (was E.sec1)

E.409 Incident Organisation and Security Incident Handling Q.5/2 (was E.sec2)

Note: Access requires TIES account.

6.19. ITU-T Recommendation M.3016

<http://www.itu.int/itudoc/itu-t/com4/contr/068.html>

This recommendation provides an overview and framework that identifies the security requirements of a TMN and outlines how available security services and mechanisms can be applied within the context of the TMN functional architecture.

Question 18 of Study Group 3 is revising Recommendation M.3016. They have taken the original document and are incorporating thoughts from ITU-T Recommendation X.805 and from ANSI T1.276-2003. The group has produced a new series of documents.

M.3016.0 - Overview

M.3016.1 - Requirements

M.3016.2 - Services

M.3016.3 - Mechanisms

M.3016.4 - Profiles

6.20. ITU-T Recommendation X.805

<http://www.itu.int/itudoc/itu-t/aap/sg17aap/history/x805/x805.html>

This Recommendation defines the general security-related architectural elements that, when appropriately applied, can provide end-to-end network security.

6.21. ITU-T Study Group 16

<http://www.itu.int/ITU-T/studygroups/com16/index.asp>

Security of Multimedia Systems and Services - Question G/16

<http://www.itu.int/ITU-T/studygroups/com16/sg16-qg.html>

6.22. ITU-T Study Group 17

<http://www.itu.int/ITU-T/studygroups/com17/index.asp>

ITU-T Study Group 17 is the Lead Study Group on Communication System Security

<http://www.itu.int/ITU-T/studygroups/com17/cssecurity.html>

Study Group 17 Security Project:

<http://www.itu.int/ITU-T/studygroups/com17/security/index.html>

During its November 2002 meeting, Study Group 17 agreed to establish a new project entitled "Security Project" under the leadership of Q.10/17 to coordinate the ITU-T standardization effort on security. An analysis of the status on ITU-T Study Group action on information and communication network security may be found in TSB Circular 147 of 14 February 2003.

6.23. Catalogue of ITU-T Recommendations related to Communications System Security

<http://www.itu.int/itudoc/itu-t/com17/activity/cat004.html>

The Catalogue of the approved security Recommendations include those, designed for security purposes and those, which describe or use of functions of security interest and need. Although some of the security related Recommendations includes the phrase "Open Systems Interconnection", much of the information contained in them is pertinent to the establishment of security functionality in any communicating system.

6.24. ITU-T Security Manual

<http://www.itu.int/ITU-T/edh/files/security-manual.pdf>

TSB is preparing an "ITU-T Security Manual" to provide an overview on security in telecommunications and information technologies, describe practical issues, and indicate how the different aspects of security in today's applications are addressed by ITU-T Recommendations. This manual has a tutorial character: it collects security related material from ITU-T Recommendations into one place and explains the respective relationships. The intended audience for this manual is engineers and product managers, students and academia, as well as regulators who want to better understand security aspects in practical applications.

6.25. ITU-T NGN Effort

<http://www.itu.int/ITU-T/2001-2004/com13/ngn2004/index.html>

During its January 2002 meeting, SG13 decided to undertake the preparation of a new ITU-T Project entitled "NGN 2004 Project". At the November 2002 SG13 meeting, a preliminary description of the Project was achieved and endorsed by SG13 with the goal to launch the Project. It is regularly updated since then.

The role of the NGN 2004 Project is to organize and to coordinate ITU-T activities on Next Generation Networks. Its target is to produce a first set of Recommendations on NGN by the end of this study period, i.e. mid-2004.

6.26. NRIC VI Focus Groups

<http://www.nric.org/fg/index.html>

The Network Reliability and Interoperability Council (NRIC) was formed with the purpose to provide recommendations to the FCC and to the industry to assure the reliability and interoperability of wireless, wireline, satellite, and cable public telecommunications networks. These documents provide general information and guidance on NRIC Focus Group 1B (Cybersecurity) Best Practices for the

prevention of cyberattack and for restoration following a cyberattack.

Documents:

Homeland Defense - Recommendations Published 14-Mar-03

Preventative Best Practices - Recommendations Published 14-Mar-03

Recovery Best Practices - Recommendations Published 14-Mar-03

Best Practice Appendices - Recommendations Published 14-Mar-03

6.27. OASIS Security Joint Committee

[http://www.oasis-open.org/committees/
tc_home.php?wg_abbrev=security-jc](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security-jc)

The purpose of the Security JC is to coordinate the technical activities of multiple security related TCs. The SJC is advisory only, and has no deliverables. The Security JC will promote the use of consistent terms, promote re-use, champion an OASIS security standards model, provide consistent PR, and promote mutuality, operational independence and ethics.

6.28. OASIS Security Services TC

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

The Security Services TC is working to advance the Security Assertion Markup Language (SAML) as an OASIS standard. SAML is an XML framework for exchanging authentication and authorization information.

6.29. OIF Implementation Agreements

The OIF has 2 approved Implementation Agreements (IAs) relating to security. They are:

OIF-SMI-01.0 - Security Management Interfaces to Network Elements

This Implementation Agreement lists objectives for securing OAM&P interfaces to a Network Element and then specifies ways of using security systems (e.g., IPsec or TLS) for securing these interfaces. It summarizes how well each of the systems, used as specified, satisfies the objectives.

OIF - SEP - 01.1 - Security Extension for UNI and NNI

This Implementation Agreement defines a common Security Extension for securing the protocols used in UNI 1.0, UNI 2.0, and NNI.

Documents: <http://www.oiforum.com/public/documents/Security-IA.pdf>

6.30. TIA

The TIA has produced the "Compendium of Emergency Communications and Communications Network Security-related Work Activities". This document identifies standards, or other technical documents and ongoing Emergency/Public Safety Communications and Communications Network Security-related work activities within TIA and it's Engineering Committees. Many P25 documents are specifically detailed. This "living document" is presented for information, coordination and reference.

Documents: http://www.tiaonline.org/standards/cip/EMTEL_sec.pdf

6.31. WS-I Basic Security Profile

<http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html>

The WS-I Basic Security Profile 1.0 consists of a set of non-proprietary Web services specifications, along with clarifications and amendments to those specifications which promote interoperability.

7. Security Considerations

This document describes efforts to standardize security practices and documents. As such this document offers no security guidance whatsoever.

Readers of this document should be aware of the date of publication of this document. It is feared that they may assume that the efforts, on-line material, and documents are current whereas they may not be. Please consider this when reading this document.

8. IANA Considerations

This document does not propose a standard and does not require the IANA to do anything.

9. Acknowledgments

The following people have contributed to this document. Listing their names here does not mean that they endorse the document, but that they have contributed to its substance.

David Black, Mark Ellison, George Jones, Keith McCloghrie, John McDonough, Art Reilly, Chip Sharp, Dane Skow, Michael Hammer, Bruce Moon.

10. Changes from Prior Drafts

-00 : Initial draft published as [draft-lonvick-sec-efforts-01.txt](#)

-01 : Security Glossaries:

Added ATIS Telecom Glossary 2000, Critical Infrastructure Glossary of Terms and Acronyms, Microsoft Solutions for Security Glossary, and USC InfoSec Glossary.

Standards Developing Organizations:

Added DMTF, GGF, INCITS, OASIS, and WS-I

Removal of Committee T1 and modifications to ATIS and former T1 technical subcommittees due to the recent ATIS reorganization.

Efforts and Documents:

Added DMTF User and Security WG, DMTF SPAM WG, GGF Security Area (SEC), INCITS Technical Committee T4 - Security Techniques, INCITS Technical Committee T11 - Fibre Channel Interfaces, ISO JTC 1/SC 27 projects, OASIS Security Joint Committee, OASIS Security Services TC, and WS-I Basic Security Profile.

Updated Operational Security Requirements for IP Network Infrastructure : Advanced Requirements.

-00 : as the WG ID

Added more information about the ITU-T SG3 Q18 effort to modify ITU-T Recommendation M.3016.

-01 : First revision as the WG ID.

Added information about the NGN in the sections about ATIS, the NSTAC, and ITU-T.

-02 : Second revision as the WG ID.

Updated the date.

Corrected some url's and the reference to George's RFC.

-03 : Third revision of the WG ID.

Updated the date.

Updated the information about the CC

Added a Conventions section (not sure how this document got to where it is without that)

Note: This section will be removed before publication as an RFC.

11. Normative References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), STD 14, March 1997.

Authors' Addresses

Chris Lonvick
Cisco Systems
12515 Research Blvd.
Austin, Texas 78759
US

Phone: +1 512 378 1182
Email: clonvick@cisco.com

David Spak
Cisco Systems
12515 Research Blvd.
Austin, Texas 78759
US

Phone: +1 512 378 1720
Email: dspak@cisco.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2006). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

