Network Working Group	C. Lonvick	
Internet-Draft	D. Spak	
Expires: October 16, 2009	Cisco Systems	
	April 14, 2009	

TOC

Security Best Practices Efforts and Documents
draft-ietf-opsec-efforts-10.txt

Status of this Memo

Copyright Notice

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

TOC

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 ogranization.
>
> 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. Format of this Document

TOC

The body of this document has three sections.
The first part of the body of this document, Section 3 (Online Security Glossaries), 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 4 (Standards Developing Organizations), contains a listing of SDOs that appear to be working on security standards.
The third part, Section 5 (Security Best Practices Efforts and Documents), lists the documents which have been found to offer good practices or recommendations for securing networks and networking devices.

---

3. Online Security Glossaries

TOC

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

---

3.1. ATIS Telecom Glossary 2000

TOC

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 an American National Standard (ANS).

3.2. Internet Security Glossary - RFC 4949

TOC

http://www.ietf.org/rfc/rfc4949.txt
This document was originally created as RFC 2828 in May 2000. It was revised as RFC 4949 and 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."

3.3. Compendium of Approved ITU-T Security Definitions

TOC

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.

3.4. Microsoft Solutions for Security Glossary

TOC

http://www.microsoft.com/security/glossary.mspx
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.

3.5. SANS Glossary of Security Terms

TOC

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.

TOC

3.6. Security Taxonomy and Glossary - Anne & Lynn Wheeler

http://www.garlic.com/~lynn/secure.htm
Anne and Lynn Wheeler maintain a security taxonomy and glossary with terms merged from AFSEC, AJP, CC1, CC2, CC21 (CC site), CIAO, FCv1, FFIEC, FJC, FTC, IATF V3 (IATF site), IEEE610, ITSEC, Intel, JTC1/SC27 (SC27 site), KeyAll, MSC, NIST 800-30, 800-33, 800-37, 800-53, 800-61, 800-77, 800-83 FIPS140, NASA, NCSC/TG004, NIAP, NSA Intrusion, CNSSI 4009, online security study, RFC1983, RFC2504, RFC2647, RFC2828, TCSEC, TDI, and TNI.

---

4. Standards Developing Organizations

TOC

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.

4.1. 3GPP - Third Generation Partnership Project

TOC

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.

4.2. 3GPP2 - Third Generation Partnership Project 2

TOC

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, TIA, 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.

TOC

4.3. 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.

4.3.1. Accredited Standards Committee X9 (ASC X9)

TOC

http://www.x9.org/
The Accredited Standards Committee X9 (ASC X9) has the mission to develop, establish, maintain, and promote standards for the Financial Services Industry in order to facilitate delivery of financial services and products.

4.4. ATIS - Alliance for Telecommunications Industry Solutions

TOC

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.

4.4.1. ATIS NIPP - Network Interface, Power, and Protection Committee, formerly T1E1

TOC

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.

TOC

4.4.2. ATIS NPRQ - 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.

4.4.3. ATIS OBF - Ordering and Billing Forum, formerly regarding T1M1 O&B

TOC

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.

4.4.4. ATIS OPTXS - Optical Transport and Synchronization Committee, formerly T1X1

TOC

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.

4.4.5. ATIS TMOC - Telecom Management and Operations Committee, formerly T1M1 OAM&P

TOC

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.

4.4.6. ATIS WTSC - Wireless Technologies and Systems Committee, formerly T1P1

TOC

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.

4.4.7. ATIS PTSC - Packet Technologies and Systems Committee, formerly T1S1

TOC

http://www.atis.org/0191/index.asp
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.

4.4.8. ATIS Protocol Interworking Committee, regarding T1S1

TOC

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.

4.5. CC - Common Criteria

TOC

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.

TOC

4.6. 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.

4.7. ETSI - The European Telecommunications Standard Institute

TOC

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://www.tta.or.kr/gsc/upload/
GSC9_Joint_011_Security_Standardization_in_ITU.ppt

4.8. GGF - Global Grid Forum

TOC

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.

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

TOC

http://www.ieee.org/
IEEE is a non-profit, 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.

TOC

4.10. 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.

4.11. INCITS - InterNational Committee for Information Technology Standards

TOC

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.

4.11.1. INCITS Technical Committee T11 - Fibre Channel Interfaces

TOC

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

---

4.12. ISO - The International Organization for Standardization

TOC

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.

4.13. ITU - International Telecommunication Union

TOC

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:

4.13.1. ITU Telecommunication Standardization Sector - ITU-T

TOC

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.

4.13.2. ITU Radiocommunication Sector - ITU-R

TOC

http://www.itu.int/ITU-R/
The ITU-R plays a vital role in the management of the radio-frequency spectrum and satellite orbits.

4.13.3. ITU Telecom Development - ITU-D

TOC

(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.

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

TOC

http://www.oasis-open.org/
OASIS is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards.

4.15. OIF - Optical Internetworking Forum

TOC

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.

4.16. NRIC - The Network Reliability and Interoperability Council

TOC

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.

4.17. National Security Telecommunications Advisory Committee (NSTAC)

TOC

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.

4.18. TIA - The Telecommunications Industry Association

TOC

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.

4.19. TTA - Telecommunications Technology Association

TOC

http://www.tta.or.kr/Home2003/main/index.jsp http://www.tta.or.kr/English/new/main/index.htm (English)
TTA (Telecommunications Technology Association) is a IT standards organization that develops new standards and provides one-stop services for the establishment of IT standards as well as providing testing and certification for IT products.

4.20. The World Wide Web Consortium

TOC

http://www.w3.org/Consortium/
The World Wide Web Consortium (W3C) is an international consortium where Member organizations, a full-time staff, and the public work together to develop Web standards. W3C's mission is: To lead the World Wide Web to its full potential by developing protocols and guidelines that ensure long-term growth for the Web.
The security work within the W3C
http://www.w3.org/Security/Activity

4.21. Web Services Interoperability Organization (WS-I)

TOC

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.

---

5. Security Best Practices Efforts and Documents

TOC

This section lists the works produced by the SDOs.

5.1. 3GPP - TSG SA WG3 (Security)

TOC

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

---

5.2. 3GPP2 - TSG-S Working Group 4 (Security)

TOC

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

---

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

TOC

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

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

TOC

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.

5.5. DMTF - User and Security Working Group

TOC

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.

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

TOC

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.

5.6.1. ATIS Work on Packet Filtering

TOC

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".

5.7. ATIS Work on the NGN

TOC

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."

5.8. Common Criteria

TOC

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

5.9. ETSI

TOC

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

5.10. GGF Security Area (SEC)

TOC

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

---

5.11. Information System Security Assurance Architecture

TOC

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

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

TOC

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

5.13. INCITS CS1 - Cyber Security

TOC

http://cs1.incits.org/
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).

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

TOC

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
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=
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=
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=
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=
Open Systems Interconnection -- Network layer security protocol
http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=22084&ICS1=35&ICS2=100&ICS3=30

5.15. ISO JTC 1/SC 27

TOC

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

---

5.16. ITU-T Study Group 2

TOC

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.

5.17. ITU-T Recommendation M.3016

TOC

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

5.18. ITU-T Recommendation X.805

TOC

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.

5.19. ITU-T Study Group 16

TOC

http://www.itu.int/ITU-T/studygroups/com16/index.asp
Multimedia Security in Next-Generation Networks (NGN-MM-SEC)
http://www.itu.int/ITU-T/studygroups/com16/sg16-q25.html

5.20. ITU-T Study Group 17

TOC

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.

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

TOC

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.

5.22. ITU-T Security Manual

TOC

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 are engineers and product managers, students and academia, as well as regulators who want to better understand security aspects in practical applications.

5.23. ITU-T NGN Effort

TOC

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.

5.24. NRIC VI Focus Groups

TOC

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

5.25. OASIS Security Joint Committee

TOC

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.

5.26. OASIS Security Services (SAML) TC

TOC

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.

5.27. OIF Implementation Agreements

TOC

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

---

5.28. TIA

TOC

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/technology/ciphs/documents/EMTEL_sec.pdf

---

5.29. WS-I Basic Security Profile

TOC

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.

5.30. NIST Special Publications (800 Series)

TOC

http://csrc.nist.gov/publications/PubsSPs.html

Special Publications in the 800 series present documents of general interest to the computer security community. The Special Publication 800 series was established in 1990 to provide a separate identity for information technology security publications. This Special Publication 800 series reports on ITL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

5.31. NIST Interagency or Internal Reports (NISTIRs)

TOC

http://csrc.nist.gov/publications/PubsNISTIRs.html
NIST Interagency or Internal Reports (NISTIRs) describe research of a technical nature of interest to a specialized audience. The series includes interim or final reports on work performed by NIST for outside sponsors (both government and nongovernment). NISTIRs may also report results of NIST projects of transitory or limited interest, including those that will be published subsequently in more comprehensive form.

5.32. NIST ITL Security Bulletins

TOC

http://csrc.nist.gov/publications/PubsITLSB.html
ITL Bulletins are published by NIST's Information Technology Laboratory, with most bulletins written by the Computer Security Division. These bulletins are published on the average of six times a year. Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Not all of ITL Bulletins that are published relate to computer / network security. Only the computer security ITL Bulletins are found here.

---

6. Security Considerations

TOC

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.

---

7. IANA Considerations

TOC

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

---

8. Acknowledgments

TOC

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.

---

9. Changes from Prior Drafts

TOC

-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)

-04 : Fourth revision of the WG ID.

Updated the date.

Added Anne & Lynn Wheeler Taxonomy & Security Glossary

CIAO glossary removed. CIAO has been absorbed by DHS and the glossary is no longer available.

USC glossary removed, could not find it on the site or a reference to it elsewhere.

Added TTA - Telecommunications Technology Association to SDO section.

Removed ATIS Security & Emergency Preparedness Activities from Documents section. Could not find it or a reference to it.

INCITS T4 incorporated into CS1 - T4 section removed

X9 Added to SDO list under ANSI

Various link or grammar fixes.

-05 : Fifth revision of the WG ID.

Updated the date.

Removed the 2119 definitions; this is an informational document.

-06 : Sixth revision of the WG ID.

Updated the date.

Added W3C information.

-07 : Seventh revision of the WG ID.

Updated the date.

-08 : Eighth revision of the WG ID.

Updated the reference to RFC 4949, found by Stephen Kent.

-09 : Nineth revision of the WG ID.

Updated the date.

-10 : Tenth revision of the WG ID.

Added references to NIST documents, recommended by Steve Wolff.
Updated the date.

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

Authors' Addresses

TOC

	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