Network Working Group
Internet-Draft
Expires: March 21, 2005

C. Lonvick
D. Spak
Cisco Systems
September 20, 2004

Security Best Practices Efforts and Documents
draft-lonvick-sec-efforts-01.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

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 authors of this document would like to keep it open as an Internet Draft for approximately 6 months for the date of the first submission. We hope that it will be spread far and wide and that the leaders of SDO efforts will contact us with updated information so that their own effort may be listed in this document, or so that corrections may be made.

Comments on this document may be addressed to the authors.

2. Format of this Document

The body of this document has three sections.

The first part of the body of this document, Section 3, 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, contains a listing of SDOs that appear to be working on security standards.

The third part, Section 5, lists the documents which have been found to offer good practices or recommendations for securing networks and networking devices.

3. Online Security Glossaries

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

3.1 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).

3.2 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.

3.3 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:

- a recommended Internet definition

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

3.4 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.

3.5 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.

3.6 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.

3.7 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.

4. 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.

4.1 3GPP - Third Generation P P

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 P P 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, 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.

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.

4.4 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.

4.4.1 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.

4.4.2 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.

4.4.3 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.

4.4.4 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 authors are investigating this and hope to provide a clear scope of their effort.

4.4.5 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.

4.4.6 ATIS Packet Technologies and Systems 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.

4.4.7 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.

4.4.8 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.

4.5 CC - Common Criteria

http://csrc.nist.gov/cc/

Note: The URL for the Common Criteria organization was http://www.commoncriteria.org/ however, they have elected to take their web site offline for the time being. It is hoped that the proper URL will be available before this document becomes an RFC. This note will be removed prior to publication as an RFC.

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.

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

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

4.8 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.

4.9 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.

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

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.

4.12 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.

4.13 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:

4.13.1 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.

4.13.2 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.

4.13.3 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.

4.14 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.

4.15 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.

4.16 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.

4.17 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.

4.18 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.

5. Security Best Practices Efforts and Documents

This section lists the works produced by the SDOs.

5.1 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

5.2 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

5.3 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

5.4 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.

5.5 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.

5.6 ATIS Security & Emergency Preparedness Activities

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.

5.7 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.

5.8 Common Criteria

http://csrc.nist.gov/cc/

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.

Common Criteria v2.1 contains:
- Part 1 - Intro & General Model
- Part 2 - Functional Requirements (including Annexes)
- Part 3 - Assurance Requirements

Documents: Common Criteria V2.1
http://csrc.nist.gov/cc/CC-v2.1.html

5.9 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

5.10 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

5.11 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

5.12 Operational Security Requirements for IP Network Infrastructure : Advanced Requirements

IETF Internet-Draft

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:
http://www.ietf.org/internet-drafts/draft-jones-opsec-06.txt

5.13 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.

5.14 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

5.15 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

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

5.16 ISO JTC 1/SC 27

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

5.17 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.

5.18 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 security threats to a TMN and outlines how available security services can be applied within the context of the TMN functional architecture.

5.19 **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.

5.20 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

5.21 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.

5.22 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.

5.23 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.

5.24 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

5.25 OASIS Security Joint Committee

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 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.

5.27 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

5.28 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

5.29 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.

6. 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.

7. IANA Considerations

This Internet Draft does not propose a standard but is trying to pull together information about the security related efforts of all Standards Developing Organizations and some other efforts which provide good secuirty methods, practices or recommendations.

8. 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.

9. Changes from Prior Drafts

-00 : Initial draft

-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.

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

10. References

10.1 Normative References

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

10.2 Informative References

[2] Narten, T. and H. Alvestrand, "Guidelines for writing an IANA Considerations Section in RFCs", RFC 2869, BCP 26, October 1998.

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

Disclaimer of Validity

Copyright Statement

Acknowledgment

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