Network Working Group
Internet-Draft
Intended status: Informational
Expires: October 15, 2013

C. Lonvick
D. Spak
Cisco Systems
April 13, 2013

Security Best Practices Efforts and Documents
draft-ietf-opsec-efforts-20.txt

Abstract

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

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on October 15, 2013.

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 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

This document will be updated in sections. The most recently updated part of this document is Section 4.

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.

The text used in sections 3, 4, and 5 have been copied from their referring web sites. The authors make no claim about the validity or accuracy of the information listed.

3. Online Security Glossaries

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

3.1. ATIS Telecom Glossary 2007

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

This Glossary began as a 5800-entry, search-enabled hypertext telecommunications glossary titled Federal Standard 1037C, Glossary of Telecommunication Terms . Federal Standard 1037C was updated and matured into an American National Standard (ANS): T1.523-2001, Telecom Glossary 2000 , under the aegis of ASC T1. In turn, T1.523-2001 has been revised and redesignated under the ATIS procedures for ANS development as ATIS-0100523.2007, ATIS Telecom Glossary 2007.

Date published: 2007

3.2. Internet Security Glossary - RFC 4949

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."

Date published: August 2007

3.3. Compendium of Approved ITU-T Security Definitions

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

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

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. The original Compendium was compiled by SG 17, Lead Study Group on Communication Systems Security (LSG-CSS).
http://www.itu.int/itudoc/itu-t/com17/activity/def004.html

Date published: 2003

3.4. Microsoft Malware Protection Center

http://www.microsoft.com/security/portal/threat/encyclopedia/glossary.aspx

The Microsoft Malware Protection Center, Threat Research and Response Glossary was created to explain the concepts, technologies, and products associated with computer security.

Date published: indeterminate

3.5. SANS Glossary of Security Terms

http://www.sans.org/security-resources/glossary-of-terms/

The SANS Institute (SysAdmin, Audit, Network, Security) was created in 1989 as, "a cooperative research and education organization." This glossary was updated in May 2003. The SANS Institute is also home to many other resources including the SANS Intrusion Detection FAQ and the SANS/FBI Top 20 Vulnerabilities List.

Date published: indeterminate

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.

Date updated: October 2010

3.7. NIST - Glossary of Key Information Security Terms

http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf

This glossary of basic security terms has been extracted from NIST Federal Information Processing Standards (FIPS) and the Special Publication (SP) 800 series. The terms included are not all inclusive of terms found in these publications, but are a subset of basic terms that are most frequently used. The purpose of this glossary is to provide a central resource of definitions most

commonly used in NIST security publications.

Date originally published: April 2006

Date of this update: February 2010

3.8. RSA Information Security Glossary

http://www.rsa.com/glossary/

Welcome to the RSA Security Information Security Glossary. This glossary is offered as an aid to understanding current concepts and initiatives in the realm of Information Security. The terms were chosen based on their importance in understanding the solutions, services and products that RSA security provides for its customers.

Date originally published: 2005

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 Partnership Project

http://www.3gpp.org/

The 3rd Generation Partnership Project (3GPP) unites [Six] telecommunications standards bodies, known as "Organizational Partners" and provides their members with a stable environment to produce the highly successful Reports and Specifications that define 3GPP technologies.

4.2. 3GPP2 - Third Generation Partnership Project 2

http://www.3gpp2.org/

The Third Generation Partnership Project 2 (3GPP2) is:

> a collaborative third generation (3G) telecommunications specifications-setting project
>
> comprising North American and Asian interests developing global specifications for ANSI/TIA/EIA-41 Cellular Radiotelecommunication Intersystem Operations network evolution to 3G
>
> and global specifications for the radio transmission technologies (RTTs) supported by ANSI/TIA/EIA-41.

3GPP2 was born out of the International Telecommunication Union's (ITU) International Mobile Telecommunications "IMT-2000" initiative, covering high speed, broadband, and Internet Protocol (IP)-based mobile systems featuring network-to-network interconnection, feature/service transparency, global roaming and seamless services independent of location. IMT-2000 is intended to bring high-quality mobile multimedia telecommunications to a worldwide mass market by achieving the goals of increasing the speed and ease of wireless communications, responding to the problems faced by the increased demand to pass data via telecommunications, and providing "anytime, anywhere" services.

4.3. ANSI - The American National Standards Institute

http://www.ansi.org/

As the voice of the U.S. standards and conformity assessment system, the American National Standards Institute (ANSI) empowers its members and constituents to strengthen the U.S. marketplace position in the global economy while helping to assure the safety and health of consumers and the protection of the environment.

The Institute oversees the creation, promulgation and use of thousands of norms and guidelines that directly impact businesses in nearly every sector: from acoustical devices to construction equipment, from dairy and livestock production to energy distribution, and many more. ANSI is also actively engaged in accrediting programs that assess conformance to standards - including globally-recognized cross-sector programs such as the ISO 9000 (quality) and ISO 14000 (environmental) management systems.

4.3.1. Accredited Standards Committee X9 (ASC X9)

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 the delivery of financial services and products. Under this mission ASC X9 fulfills the objectives of: (1) Supporting (maintain, enhance, and promote use of) existing standards; (2) Facilitating development of new, open standards based upon consensus; (3) Providing a common source for all standards affecting the Financial Services Industry; (4) Focusing on current and future standards needs of the Financial Services Industry; (5) Promoting use of Financial Services Industry standards; and (6) Participating and promoting the development of international standards.

4.4. ATIS - Alliance for Telecommunications Industry Solutions

http://www.atis.org/

ATIS member companies develop the standards and solutions that are creating the future of the information and communications technology (ICT) industry. From efforts to realize the cost benefits of cloud services, to standards underpinning the nation's emergency communications system, to improvements in data access to support health care delivery, or developing new avenues to interactive sources of entertainment, ATIS' work makes ICT innovation possible.

Through involvement in our committees and forums, ATIS member companies achieve their technical potential and business objectives. They also get a strategic view of the future of technology to help them better position their products and services. ATIS members further benefit from valuable networking opportunities with other companies leading change in our industry, as well as the insights of leading CIOs, CTOs and other thought leaders.

ATIS gives our members a place at the table where today's ICT standards decisions are being made. Our work helps members prepare for when the future becomes today. And, with the fast pace of innovation, the gap between today's technologies and tomorrow's networks is all but disappearing.

ATIS creates solutions that support the rollout of new products and services into the information, entertainment and communications marketplace. Its activities provide the basis for the industry's delivery of:

Existing and next generation IP-based infrastructures;

Reliable converged multimedia services, including IPTV;

Enhanced Operations Support Systems and Business Support Systems; and

Greater levels of service quality and performance.

ATIS is accredited by the American National Standards Institute (ANSI).

4.4.1. ATIS NPRQ - Network Performance, Reliability, and Quality of Service Committee, formerly T1A1

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

PRQC 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. PRQC alsodevelops andrecommends positions on, and foster consistency with, standards and related subjects under consideration in other North American and international standards bodies.

PRQC Focus Areas are:

Performance and Reliability of Networks (e.g. IP, ATM, OTN, and PSTN), and Services (e.g. Frame Relay, Dedicated and Switched Data),

Security-related aspects,

Emergency communications-related aspects,

Coding (e.g. video and speech), at and between carrier-to-carrier and carrier-to-customer interfaces, with due consideration of end-user applications.

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

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

The Telecom Management and Operations Committee (TMOC) develops operations, administration, maintenance and provisioning standards, and other documentation related to Operations Support System (OSS) and Network Element (NE) functions and interfaces for communications networks - with an emphasis on standards development related to U.S.A. communication networks in coordination with the development of international standards.

The scope of the work in TMOC includes the development of standards and other documentation for communications network operations and management areas, such as: Configuration Management, Performance Management (including in-service transport performance management), Fault Management, Security Management (including management plane security), Accounting Management, Coding/Language Data Representation, Common/Underlying Management Functionality/ Technology, and Ancillary Functions (such as network tones and announcements). This work requires close and coordinated working relationships with other domestic and international standards development organizations and industry forums.

4.5. CC - Common Criteria

http://www.commoncriteriaportal.org/

The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that:

Products can be evaluated by competent and independent licensed laboratories so as to determine the fulfilment of particular security properties, to a certain extent or assurance;

Supporting documents, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies;

The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation;

These certificates are recognized by all the signatories of the CCRA.

The CC is the driving force for the widest available mutual recognition of secure IT products. This web portal is available to support the information on the status of the CCRA, the CC and the certification schemes, licensed laboratories, certified products and related information, news and events.

4.6. DMTF - Distributed Management Task Force, Inc.

http://www.dmtf.org/

DMTF enables more effective management of millions of IT systems worldwide by bringing the IT industry together to collaborate on the development, validation and promotion of systems management standards.

The group spans the industry with 160 member companies and organizations, and more than 4,000 active participants crossing 43 countries. The DMTF board of directors is led by 15 innovative, industry-leading technology companies. They include Advanced Micro Devices (AMD); Broadcom Corporation; CA, Inc.; Cisco; Citrix Systems, Inc.; EMC; Fujitsu; HP; Huawei; IBM; Intel Corporation; Microsoft Corporation; Oracle; RedHat and VMware, Inc.

With this deep and broad reach, DMTF creates standards that enable interoperable IT management. DMTF management standards are critical to enabling management interoperability among multi-vendor systems, tools and solutions within the enterprise.

4.7. ETSI - The European Telecommunications Standard Institute

http://www.etsi.org/

The European Telecommunications Standards Institute (ETSI) produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies.

We are officially recognized by the European Union as a European Standards Organization. The high quality of our work and our open approach to standardization has helped us evolve into a European roots - global branches operation with a solid reputation for technical excellence.

4.7.1. ETSI SEC

http://portal.etsi.org/portal/server.pt/gateway/PTARGS_0_13938_491_312_425_43/tb/closed_tb/sec.asp

Board#38 confirmed the closure of TC SEC.

At the same time it approved the creation of an OCG Ad Hoc group OCG Security

TC SEC documents can be found in the SEC archive

The SEC Working groups (ESI and LI) were closed and TC ESI and a TC LI were created to continue the work.

All documents and information relevant to ESI and LI are available from the TC ESI and TC LI sites

4.7.2. ETSI OCG SEC

http://portal.etsi.org/ocgsecurity/OCG_security_ToR.asp

The creation of the OCG SEC was decided at the Board #38 on 30 May 2002. The group's primary role is to provide a horizontal co-ordination structure for security issues that will ensure this work is seriously considered in each ETSI TB and that any duplicate or conflicting work is detected. To achieve this aim the group should mainly conduct its work via email and, where appropriate, co-sited "joint security" technical working meetings.

When scheduled, appropriate time at each "joint SEC" meeting should be allocated during the meetings to allow for:

- Individual committee activities as well as common work;

- Coordination between the committees; and

Experts to contribute to more than one committee.

4.8. GGF - Global Grid Forum

http://www.gridforum.org/

OGF is an open community committed to driving the rapid evolution and adoption of applied distributed computing. Applied Distributed Computing is critical to developing new, innovative and scalable applications and infrastructures that are essential to productivity in the enterprise and within the science community. OGF accomplishes its work through open forums that build the community, explore trends, share best practices and consolidate these best practices into standards.

4.8.1. Global Grid Forum Security Area

http://www.ogf.org/gf/group_info/areasgroups.php?area_id=7

The Security Area is concerned with technical and operational security issues in Grid environments, including authentication, authorization, privacy, confidentiality, auditing, firewalls, trust establishment, policy establishment, and dynamics, scalability and management aspects of all of the above.

The Security Area is comprised of the following Working Groups and Research Groups.

Certificate Authority Operations WG (CAOPS-WG)

Firewall Issues RG (FI-RG)

Levels Of Authentication Assurance Research Group (LOA-RG)

OGSA Authorization WG (OGSA-AUTHZ-WG)

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

http://www.ieee.org/

IEEE is the world's largest professional association dedicated to advancing technological innovation and excellence for the benefit of humanity. IEEE and its members inspire a global community through IEEE's highly cited publications, conferences, technology standards, and professional and educational activities.

4.9.1. IEEE Computer Society's Technical Committee on Security and Privacy

http://www.ieee-security.org/

4.10. IETF - The Internet Engineering Task Force

http://www.ietf.org/

The goal of the IETF is to make the Internet work better.

The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.

4.10.1. IETF Security Area

The Working Groups in the Security Area may be found from this page.

http://datatracker.ietf.org/wg/

The wiki page for the IETF Security Area may be found here.

http://trac.tools.ietf.org/area/sec/trac/wiki

4.11. INCITS - InterNational Committee for Information Technology Standards

http://www.incits.org/

INCITS is the primary U.S. focus of standardization in the field of Information and Communications Technologies (ICT), encompassing storage, processing, transfer, display, management, organization, and retrieval of information. As such, INCITS also serves as ANSI's Technical Advisory Group for ISO/IEC Joint Technical Committee 1. JTC 1 is responsible for International standardization in the field of Information Technology.

There are three active Groups in the Security / ID Technical Committee.

4.11.1. Identification Cards and Related Devices (B10)

http://standards.incits.org/a/public/group/b10

Development of national and international standards in the area of identification cards and related devices for use in inter-industry applications and international interchange.

4.11.2. Cyber Security (CS1)

http://standards.incits.org/a/public/group/cs1

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.

The scope of CS1 explicitly excludes the areas of work on cyber security standardization presently underway in INCITS B10, M1, T3, T10 and T11; as well as other standard groups, such as ATIS, IEEE, IETF, TIA, and X9.

4.11.3. Biometrics (M1)

http://standards.incits.org/a/public/group/m1

INCITS/M1, Biometrics Technical Committee was established by the Executive Board of INCITS in November 2001 to ensure a high priority, focused, and comprehensive approach in the United States for the rapid development and approval of formal national and international generic biometric standards. The M1 program of work includes biometric standards for data interchange formats, common file formats, application program interfaces, profiles, and performance testing and reporting. The goal of M1's work is to accelerate the deployment of significantly better, standards-based security solutions for purposes, such as, homeland defense and the prevention of identity theft as well as other government and commercial applications based on biometric personal authentication.

4.12. ISO - The International Organization for Standardization

http://www.iso.org/

ISO (International Organization for Standardization) is the world's largest developer and publisher of International Standards.

ISO is a network of the national standards institutes of 163 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system.

ISO is a non-governmental organization that forms a bridge between the public and private sectors. On the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations.

Therefore, ISO enables a consensus to be reached on solutions that

meet both the requirements of business and the broader needs of society.

4.13. ITU - International Telecommunication Union

http://www.itu.int/

ITU (International Telecommunication Union) is the United Nations specialized agency for information and communication technologies - ICTs.

We allocate global radio spectrum and satellite orbits, develop the technical standards that ensure networks and technologies seamlessly interconnect, and strive to improve access to ICTs to underserved communities worldwide.

ITU is committed to connecting all the world's people - wherever they live and whatever their means. Through our work, we protect and support everyone's fundamental right to communicate.

The ITU is comprised of three sectors:

4.13.1. ITU Telecommunication Standardization Sector - ITU-T

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

ITU-T Recommendations are defining elements in information and communication technologies (ICTs) infrastructure. Whether we exchange voice, data or video messages, communications cannot take place without standards linking the sender and the receiver. Today's work extends well beyond the traditional areas of telephony to encompass a far wider range of information and communications technologies.

4.13.2. ITU Radiocommunication Sector - ITU-R

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

The ITU Radiocommunication Sector (ITU-R) plays a vital role in the global management of the radio-frequency spectrum and satellite orbits - limited natural resources which are increasingly in demand from a large and growing number of services such as fixed, mobile, broadcasting, amateur, space research, emergency telecommunications, meteorology, global positioning systems, environmental monitoring and communication services - that ensure safety of life on land, at sea and in the skies.

4.13.3. ITU Telecom Development - ITU-D

(also referred as ITU Telecommunication Development Bureau - BDT)

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

The mission of the Telecommunication Development Sector (ITU-D) aims at achieving the Sector's objectives based on the right to communicate of all inhabitants of the planet through access to infrastructure and information and communication services.

In this regard, the mission is to:

Assist countries in the field of information and communication technologies (ICTs), in facilitating the mobilization of technical, human and financial resources needed for their implementation, as well as in promoting access to ICTs.

Promote the extension of the benefits of ICTs to all the world's inhabitants.

Promote and participate in actions that contribute towards narrowing the digital divide.

Develop and manage programmes that facilitate information flow geared to the needs of developing countries.

The mission encompasses ITU's dual responsibility as a United Nations specialized agency and an executing agency for implementing projects under the United Nations development system or other funding arrangements.

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

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

OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society. The consortium produces more Web services standards than any other organization along with standards for security, e-business, and standardization efforts in the public sector and for application-specific markets. Founded in 1993, OASIS has more than 5,000 participants representing over 600 organizations and individual members in 100 countries.

OASIS promotes industry consensus and produces worldwide standards

for security, Cloud computing, SOA, Web services, the Smart Grid, electronic publishing, emergency management, and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology.

OASIS has several Technical Committees in the Security Category.

http://www.oasis-open.org/committees/tc_cat.php?cat=security

4.15. OIF - Optical Internetworking Forum

http://www.oiforum.com/

"The Optical Internetworking Forum (OIF) promotes the development and deployment of interoperable networking solutions and services through the creation of Implementation Agreements (IAs) for optical networking products, network processing elements, and component technologies. Implementation agreements will be based on requirements developed cooperatively by end-users, service providers, equipment vendors and technology providers, and aligned with worldwide standards, augmented if necessary. This is accomplished through industry member participation working together to develop specifications (IAs) for:

External network element interfaces

Software interfaces internal to network elements

Hardware component interfaces internal to network elements

The OIF will create Benchmarks, perform worldwide interoperability testing, build market awareness and promote education for technologies, services and solutions. The OIF will provide feedback to worldwide standards organizations to help achieve a set of implementable, interoperable solutions."

4.15.1. OAM&P Working Group

http://www.oiforum.com/public/oamp.html

In concert with the Carrier, Architecture & Signaling and other OIF working groups, the Operations, Administration, Maintenance, & Provisioning (OAM&P) working group develops architectures, requirements, guidelines, and implementation agreements critical to widespread deployment of interoperable optical networks by carriers. The scope includes but is not limited to a) planning, engineering and provisioning of network resources; b) operations, maintenance or

administration use cases and processes; and c) management functionality and interfaces for operations support systems and interoperable network equipment. Within its scope are Fault, Configuration, Accounting, Performance and Security Management (FCAPS) and Security. The OAM&P working group will also account for work by related standards development organizations (SDOs), identify gaps and formulate OIF input to other SDOs as may be appropriate.

4.16. National Security Telecommunications Advisory Committee (NSTAC)

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

Meeting our Nation's critical national security and emergency preparedness (NS/EP) challenges demands attention to many issues. Among these, none could be more important than the availability and reliability of telecommunication services. The President's National Security Telecommunications Advisory Committee (NSTAC) mission is to provide the U.S. Government the best possible industry advice in these areas.

4.17. TIA - The Telecommunications Industry Association

http://www.tiaonline.org/

The Telecommunications Industry Association (TIA) is the leading trade association representing the global information and communications technology (ICT) industry through Standards development, Policy initiatives, business opportunities, market intelligence and networking events. With support from hundreds of members, TIA enhances the business environment for companies involved in telecom, broadband, mobile wireless, information technology, networks, cable, satellite, unified communications, emergency communications and the greening of technology. TIA is accredited by ANSI.

4.17.1. APCO Project 25 Public Safety Standards

http://www.tiaonline.org/all-standards/committees/tr-8

Recognizing the need for common standards for first responders and homeland security/emergency response professionals, representatives from the Association of Public Safety Communications Officials International (APCO), the National Association of State Telecommunications Directors (NASTD), selected federal agencies and the National Communications System (NCS) established Project 25 (PDF), a steering committee for selecting voluntary common system standards for digital public safety radio communications. TIA TR-8 facilitates such work through its role as an ANSI-accredited

Standards Development Organization (SDO) and has developed in TR-8 the 102 series of technical documents. These standards directly address the guidelines of the Communications Assistance for Law Enforcement Act (CALEA).

4.18. TTA - Telecommunications Technology Association

http://www.tta.or.kr/

http://www.tta.or.kr/English/index.jsp (English)

The purpose of TTA is to contribute to the advancement of technology and the promotion of information and telecommunications services and industry as well as the development of national economy, by effectively stablishing and providing technical standards that reflect the latest domestic and international technological advances, needed for the planning, design and operation of global end-to-end telecommunications and related information services, in close collaboration with companies, organizations and groups concerned with information and telecommunications such as network operators, service providers, equipment manufacturers, academia, R&D institutes, etc.

4.19. The World Wide Web Consortium

http://www.w3.org/Consortium/

The World Wide Web Consortium (W3C) is an international community where Member organizations, a full-time staff, and the public work together to develop Web standards. Led by Web inventor Tim Berners-Lee and CEO Jeffrey Jaffe, W3C's mission is to lead the Web to its full potential.

http://www.w3.org/Security/

Security online is a vast field that is being worked on by a number of organizations, including W3C. Mapping the entire field would be a huge endeavor; hence, this page focuses on work that W3C is involved in.

The traditional W3C Security Resources page is no longer maintained, but remains online for archival purposes.

The Web Security Wiki serves as a place for interested parties in the Web security community to collect information about security aspects of specifications and implementations of Web technologies.

4.20. TM Forum

http://www.tmforum.org/

TM Forum is a global, non-profit industry association focused on simplifying the complexity of running a service provider's business. As an established industry thought-leader, the Forum serves as a unifying force, enabling more than 850 companies across 195 countries to solve critical business issues through access to a wealth of knowledge, intellectual capital and standards.

4.20.1. Security Management

http://www.tmforum.org/SecurityManagement/9152/home.html

Securing networks, cyber, clouds, and identity against evolving and ever present threats has emerged as a top priority for TM Forum members. In response, the TM Forum's Security Management Initiative was formally launched in 2009. While some of our Security Management efforts, such as Identity Management, are well established and boast mature Business Agreements and Interfaces, a series of presentations, contributions, and multi-vendor technology demonstrations have jumped started work efforts on industry hot topics Network Defense, Cyber Security, and security for single and multi-regional enterprise application cloud bursting. Our aim is to produce Security Management rich frameworks, best practices, and guidebooks.

5. Security Best Practices Efforts and Documents

This section lists the works produced by the SDOs.

5.1. 3GPP - SA3 - Security

http://www.3gpp.org/SA3-Security

The WG is responsible for security in 3GPP systems, determining the security requirements, and specifying the security architectures and protocols. The WG also ensures the availability of cryptographic algorithms which need to be part of the specifications. The sub-WG SA3-LI provides the requirements and specifications for lawful interception in 3GPP systems.

Specifications:
http://www.3gpp.org/ftp/Specs/html-info/TSG-WG--S3.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. It is also responsible for high level architectural issues, as required, to coordinate service development across the various TSGs. In this role, the Services and Systems TSG shall track the activities within the various TSGs, as required, to meet the above service requirements.

More specifically, TSG-S will address the following areas of work: 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/tsgs.cfm

5.3. ATIS-0300276.2008 - Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane

This document contains both the published and redline versions of ATIS-0300276.2008. This standard contains a set of baseline security requirements for the management plane. The requirements outlined in this standard allow equipment/system suppliers, government departments and agencies, and service providers to implement a secure

telecommunications management infrastructure.

Documents: http://www.atis.org/docstore/product.aspx?id=24660

5.4. DMTF - Security Modeling Working Group

http://www.dmtf.org/sites/default/files/SecurityWGCharter.pdf

The Security Modeling Working Group of the Schema Subcommittee is responsible for developing the models and profiles required to provide interoperable security management interfaces for implementations, including the enabling of configuration and management of authentication, authorization, and auditing services.

The operational security requirements for protocols and management initiatives are not addressed by this work group and should be addressed by the working groups responsible for them. Management of the underlying security capabilities utilized by such protocols and initiatives are addressed by this work group, (for example: interfaces for the management of keys and certificates).

5.5. Common Criteria

http://www.commoncriteriaportal.org/

The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Agreement (CCRA), which ensures that:

Products can be evaluated by competent and independent licensed laboratories so as to determine the fulfilment of particular security properties, to a certain extent or assurance;

Supporting documents, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies;

The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation;

These certificates are recognized by all the signatories of the CCRA.

The CC is the driving force for the widest available mutual

recognition of secure IT products. This web portal is available to support the information on the status of the CCRA, the CC and the certification schemes, licensed laboratories, certified products and related information, news and events.

5.6. ETSI

TC SEC

http://portal.etsi.org/portal/server.pt/gateway/PTARGS_0_13938_491_312_425_43/tb/closed_tb/sec.asp

Board#38 confirmed the closure of TC SEC.

At the same time it approved the creation of an OCG Ad Hoc group OCG Security

TC SEC documents can be found in the SEC archive (members login required)

The SEC Working groups (ESI and LI) were closed and TC ESI and a TC LI were created to continue the work.

All documents and information relevant to ESI and LI are available from the TC ESI and TC LI sites

TC ESI: http://portal.etsi.org/portal/server.pt/community/ESI/307

TC LI: http://portal.etsi.org/portal/server.pt/community/LI/318

OCG SEC

http://portal.etsi.org/ocgsecurity/OCG_security_ToR.asp

The group's primary role is to provide a light-weight horizontal co-ordination structure for security issues that will ensure this work is seriously considered in each ETSI TB and that any duplicate or conflicting work is detected. To achieve this aim the group should mainly conduct its work via email and, where appropriate, co-sited "joint security" technical working meetings.

OCG documents may be found here:

http://portal.etsi.org/ocg/Summary.asp (members login required)

5.7. 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:

http://www.rfc-editor.org/rfc/rfc3871.txt

5.8. ISO JTC 1/SC 27 - Information security Technology techniques

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306

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

IT security techniques -- Message Authentication Codes (MACs)

IT Security techniques -- Key management

IT Security techniques -- Entity authentication

IT Security techniques -- Hash-functions

IT Security techniques -- Non-repudiation

IT Security techniques -- IT network security

5.9. ITU-T Study Group 2

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

Security related recommendations currently under study:
http://www.itu.int/ITU-T/recommendations/index_sg.aspx?sg=2

5.10. ITU-T Study Group 17

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

Security related recommendations currently under study:
http://www.itu.int/ITU-T/recommendations/index_sg.aspx?sg=17

The ICT Security Standards Roadmap
http://www.itu.int/ITU-T/studygroups/com17/ict/index.html

This ICT Security Standards Roadmap has been developed to assist in the development of security standards by bringing together information about existing standards and current standards work in key standards development organizations.

In addition to aiding the process of standards development, the Roadmap will provide information that will help potential users of security standards, and other standards stakeholders, gain an understanding of what standards are available or under development as well as the key organizations that are working on these standards.

The Roadmap was initiated by ITU-T Study Group 17. In January 2007 the initiative became a collaborative effort when the European Network and Information Security Agency (ENISA) and the Network and Information Security Steering Group (NISSG) joined Study Group 17 in the project.

The Roadmap is in five parts:

Part 1: ICT Standards Development Organizations and Their Work
http://www.itu.int/ITU-T/studygroups/com17/ict/part01.html

Part 1 contains information about the Roadmap structure and about each of the listed standards organizations, their structure and the security standards work being undertaken. In addition it contains information on terminology by providing links to existing security glossaries and vocabularies.

Part 2: Approved ICT Security Standards
http://www.itu.int/ITU-T/studygroups/com17/ict/part02.html

Part 2 contains a summary catalogue of approved standards.

Part 3: Security standards under development
http://www.itu.int/ITU-T/studygroups/com17/ict/part03.html

Part 3 is structured with the same taxonomy as Part 2 but contains work in progress, rather than standards that have already been approved and published. Part 3 will also contain information on inter-relationships between groups undertaking the work and on potential overlaps between existing projects.

Part 4: Future needs and proposed new security standards
http://www.itu.int/ITU-T/studygroups/com17/ict/part04.html

Part 4 is intended to capture possible future areas of security standards work where gaps or needs have been identified as well as areas where proposals have been made for specific new standards work.

Part 4 includes provision for direct feedback, comments and suggestions.

Part 5: Best practices
http://www.itu.int/ITU-T/studygroups/com17/ict/part05.html

Part 5 is a recent addition to the Roadmap (May 2007). It is intended to be a repository of security-related best practices contributed by our community of members.

This section will be based on contributions from the security community.

Where possible contributions should refer to best practices relating to standards-based security but other best practices will be considered for inclusion.

It is important to note that the Roadmap is a work-in-progress. It is intended that it be developed and enhanced to include other standards organizations as well as a broader representation of the work from organizations already included. It is hoped that standards organizations whose work is not represented in this version of the Roadmap will provide information to ITU-T about their work so that it may be included in future editions.

In May 2007, Part 2 of the Roadmap was converted to a searchable database format that allows direct links to the information of participating standards organizations. The database format will allow each participating organization to manage its own data within the Roadmap. This will enable more timely updating of the information and will also reduce the overhead in maintaining the information.

http://www.itu.int/ITU-T/security/main_table.aspx

5.11. NRIC VII Focus Groups

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

The mission of the NRIC is partner with the Federal Communications Commission, the communications industry and public safety to

facilitate enhancement of emergency communications networks, homeland security, and best practices across the burgeoning telecommunications industry.

By December 16, 2005, the Council shall present a final report that describes, in detail, any additions, deletions, or modifications that should be made to the Homeland Security Best Practices that were adopted by the preceding Council.

Documents in Focus Group 2: Homeland Security, Subcommittee 2.B: Cyber Security:

Focus Group 2B Report - Homeland Security Cyber Security Best Practices Published 06-Dec-2004

Focus Group 2B Report Appendices Published 06-Dec-2004

Focus Group 2B Final Report - Summary of Activities, Guidance and Cybersecurity Issues Published 16-Dec-2005

Focus Group 2B Final Best Practices Published 16-Dec-2005

5.12. OASIS Security Technical Committees

Many Technical Committees have produced standards.

http://www.oasis-open.org/committees/tc_cat.php?cat=security

5.13. OIF Implementation Agreements

The OIF has 3 approved, and in-force Implementation Agreements (IAs) relating to security. They are:

OIF-SEP-03.0 - Security Extension for UNI and E-NNI 2.0 (Nov 2010)
http://www.oiforum.com/public/documents/OIF-SEP-03.0.pdf

OIF-SMI-01.0 - Security for Management Interfaces to Network Elements (September 2003)
http://www.oiforum.com/public/documents/SecurityMgmt-IA.pdf

OIF-SMI-02.1 - Addendum to the Security for Management Interfaces to Network Elements (March 2006)
http://www.oiforum.com/public/documents/OIF-SMI-02_1.pdf

5.14. TIA - Critical Infrastructure Protection (CIP) and Homeland Security (HS)

The TIA Cybersecurity Working Group advocates public policy positions

related to the security of ICT equipment and services from a vendor perspective as it relates to critical infrastructure, supply chain and information sharing.

http://www.tiaonline.org/policy/cybersecurity

5.15. NIST Special Publications (800 Series)

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.

5.16. NIST Interagency or Internal Reports (NISTIRs)

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.

5.17. NIST ITL Security Bulletins

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.

5.18. SANS Information Security Reading Room

http://www.sans.org/reading_room/

Featuring over 1,969 original computer security white papers in 77

different categories

Most of the computer security white papers in the Reading Room have been written by students seeking GIAC certification to fulfill part of their certification requirements and are provided by SANS as a resource to benefit the security community at large. SANS attempts to ensure the accuracy of information, but papers are published "as is". Errors or inconsistencies may exist or may be introduced over time as material becomes dated.

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

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, Michael Hammer, Bruce Moon, Stephen Kent, Steve Wolff, Bob Natale, Marek Lukaszuk.

9. 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)

-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.

-11 : Eleventh revision of the WG ID.

Updated the date.

-12 : Twelfth revision of the WG ID.

Updated the date.

-13 : Nothing new.

Updated the date.

-14 : Fourteenth revision of the WG ID.

Updated the date and reviewed the accuracy of Section 3.

Updated the section on Compendium of Approved ITU-T Security Definitions

Updated the section on the Microsoft glossary.

Updated the section on the SANS glossary.

Added the NIST Security glossary.

Added dates to all glossaries - where I could find them.

Added the SANS Reading Room material to Section 5.

-15 : Fifteenth revision of the WG ID.

Updated the date and reviewed the accuracy of Section 4. Several changes made.

Removed WS-I as they have merged with OASIS.

Added TM Forum.

-16 : Sixteenth revision of the WG ID.

Updated the date and reviewed the accuracy of Section 5. Several changes made.

-17 : Seventeenth revision of the WG ID.

Updated the date and reviewed the accuracy of Section 3. A couple of changes made.

-18 : Eighteenth revision of the WG ID.

Updated the date and reviewed the accuracy of Section 4. Some changes made.

-19 : Ninteenth revision of the WG ID.

Updated the date and reviewed the accuracy of Section 5. Some changes made.

-20 : Twentieth revision of the WG ID.

Updated the date and reviewed the accuracy of Section 3. Some changes made.

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

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