Applicability of the Security Control Automation Protocol (SCAP) to Voice over Internet Protocol (VoIP) Systems

Version 0.9

This publication is for informational purposes and presents a view on how practical it could be to use the Security Content Automation Protocol (defined in NIST Special Publication 800-126) to an implemented Voice over Internet Protocol (VoIP) System. While a view of a hypothetical security assessment of a generic implemented VoIP System is presented in this publication it is presented just as a rough guide, is not a substitute for a rigorous security assessment on a particular VoIP system or implementation.

Participation in the development of this publication does not represent an endorsement of the content of this publication on the part of any specific individual, company, or corporation. Any reference made to existing commercial products or services is not intended as, and does not constitute, and endorsement or approval of such products or services.

This publication is protected by copyright, all rights reserved. The scanning, uploading and distribution of this book by electronic means, including the Internet, without the permission of the Internet Security Alliance, is illegal and punishable by law.

If you wish to acquire printed copies of this publication, or distribute portions of this publication in any media, please contact Internet Security Alliance by calling (703)907-7799.

© 2010 Internet Security Alliance. All rights reserved.

Applicability of the Security Control Automation Protocol (SCAP) to Voice over Internet Protocol (VoIP) Systems

Version 0.9

Board of Directors

Larry Clinton
President, Internet Security Alliance

Ty Sagalow
IS Alliance Board Chair,
Executive Vice-President and Chief Innovation Officer, Zurich North America

Mike Hickey
First Vice Board Chair
VP, Government Affairs & National Security Policy, Verizon

Dr. Sagar Vidyasagar
Second vice Board Chair
Executive VP, Advanced Technology, Tata Consultancy Services

Marc-Anthony Signorino
Secretary/Treasurer
Director of Technology Policy, National Association of Manufacturers

Bruno Mahlman
Vice President, National Security, Perot Systems Corporation

Tim McKnight
Vice President & Chief Information Security Officer, Northrup Grumman

Ken Silva
Chief Technology Office, Verisign

Charlie Croom
Vice President, Cyber Security Strategy, Lockheed Martin

Joe Buonomo
President, Direct Computer Resources, Inc.

Jeff Brown
Director, Infrastructure Services and CISO Information Technology, Raytheon

Lawrence Dobranski
Leader, Advanced Security Solutions Research & Development Nortel

Eric Guerrino
Managing Director Systems and Technology, Bank of New York Mellon

Dr. Pradeep Kohsla
Dean, School of Engineering and Computer Sciences, Co-Director – Cylab, Carnegie Mellon University

WHAT IS THE INTERNET SECURITY ALLIANCE?

Virtually every corporation integrates use of the Internet into their business plan. However, the use of the Internet also exposes corporations to continuing and persistent threats, putting at risk corporate intellectual property, business operations, and overall enterprise security. These risks confront any business, as well as all of their respective suppliers, business partners and customers.

The Internet Security Alliance (ISAlliance) is a non-traditional trade association that serves to understand, integrate and help manage the multi-dimensional and international issues that operating in the Internet creates. The ISAlliance website is www.isalliance.org.

WHAT DOES THE INTERENT SECURITY ALLIANCE DO?

ISAlliance provides tangible benefits to its membership by creating cutting edge services and applicable publications useful across the various industry sectors that use the Internet. ISAlliance was conceived in conjunction with Carnegie Mellon University to integrate technological issues with the membership's pragmatic business concerns and align public policy to facilitate business growth and resilience.

The ISAlliance provides a broad range of ongoing technological, business and policy services to its membership, all of which can be reviewed in more detail at the ISAlliance web site. In addition, the ISAlliance Board identifies a select set of priority projects each year for intensive work.

This report is a new contribution to a continuing series of publications produced by ISAlliance that address the substantive issues that arise at the intersections of business, law and information security. Previous titles include:

Navigating Compliance and Security for Unified Communications

The Cyber Security Social Contract: A Twenty-First Century Model for Protecting and Defending Critical Technology Systems and Infrastructure.

The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask

Contracting for Information Security in Commercial Transactions, Volume I: An Introductory Guide

Contracting for Information Security in Commercial Transactions, Volume II: Model Contract Terms for Certified Information Management Systems

Common Sense Guide for Senior Managers: Top Ten Recommended Security Practices

Copies of these publications can be obtained or purchased from the ISAlliance.

About the Editor

Paul Sand is the President and CEO of Salare Security LLC. Salare Security is committed to providing products and services that prevent covert channel communications that are exploited to propagate malware and that are used to exfiltrate information from an enterprise. Salare was founded to commercialize technology licensed from the Illinois Institute of Technology (IIT) developed as the result of IIT's involvement in the National Security Agency's Academic Center of Excellence in Information Assurance program.

Paul Sand is a member of the Board of Directors of the Chicago Infragard Members Alliance Chapter, a member of the US Secret Service's Electronic Crimes Task Force, a senior member of the IEEE, a member of the Information Systems Security Association, and an adjunct faculty member at the Keller Graduate School of Management. He has previously worked at Bell Laboratories, AT&T Network Systems, and Lucent Technologies. He holds 21 awarded US Patents in the areas of voice and data communications and public safety.

Paul is a frequent industry speaker and may be reached at paul.sand@salaresecurity.com or 312.994.2336.

Special Thanks

Special thanks are given to all of the SCAP Applicability Working Group for the ISAlliance VoIP Security Project. This paper presents the results of a year long effort that would not have been possible with out the countless hours of contributions and efforts these individuals have made to this effort.

In particular, special thanks are given to the authors of the each of the individual sections of this whitepaper:

Chapter 1 – History & Background of the ISAlliance Voice Security Project
Lawrence Dobranski, Nortel Networks
Chapter 2 – ISAlliance Voice Security Project Goals and Objectives
Lawrence Dobranski, Nortel Networks
Chapter 3 – Scope of the SCAP Applicability Working Group Project
Paul R. Sand, Salare Security
Chapter 4 – VoIP Architecture
Matt Trainor, Nortel Networks
Chapter 5 – VoIP Threat Risk Assessment
Tom Grill, Verisign
Ken Stavinoha, Microsoft
Chapter 6 – VoIP Security Checklist and Mapping to SP 800-53 R3
Dawn Adams, EWA-Canada
Peter Thermos, Palindrome Technologies
Chapter 7 – Use of Security Content Automation Program (SCAP) for VoIP Security
Scott Armstrong, Gideon Technologies

The entire group consisted of 50 individuals representing 43 organizations.

AJ West, Boeing
Alex Fielding, Ripcord Networks
Allie Larman, Oklahoma Office of State Finance
Andrew Bove, Secure Acuity Networks, LLC
Andriy Markov, VoIPshield Systems Inc.
Barry Wasser, Department of Homeland Security
Blake Frantz, Center For Internet Security
Bob Moskowitz, ICSAlabs, an Independent Division of Verizon Business Systems
Bogdan Materna, VoIPshield Systems Inc.
Calvin Bowditch, Joint Task Force-Global Network Operations

Carl Herberger, Evolve IP
Cheri Sigmon, Department of Defense
Cynthia Reese, Science Applications International Corporation (SAIC)
David Lukasik, Department of Veterans Affairs
Dawn Adams, EWA-Canada
Denise Walker, DBA, Lone Star College System
Ed Stull, Direct Computer Resources
Ed White, McAfee
Edward Cummins, Raytheon
Gary Gapinski, National Aeronautics and Space Administration
Imran Khan, Consultant
James Mesta, Agilent Technologies, Inc.
Jeffrey Ritter, Waters Edge Consulting
Jim Meyer, Institute for Defense Analyses
John Fulater, HSBC North America
Joseph Dalessandro, Withheld
Ken Fee, Firefly Communications
Ken Stavinoha, Microsoft
Kenneth Kousky, Salare Security, LLC
Kevin Watkins, McAfee
Laurie Hestor, Defense Information Systems Agency
Linda Kostic, eTrade Financial
Lorelei Knight, ICSAlabs, an Independent Division of Verizon Business Systems
Lynn Hitchcock, Raytheon
Mark Humphrey, Boeing
Matt Trainor, Nortel Networks
Paul Salva, HSBC North America
Pete Eisele, Northrop Grumman
Peter Thermos, Palindrome Technologies
Rick Mellendick, Food and Drug Administration
Robert Smith, Global UniDocs Company
Ronald Rice, Defense Information Systems Agency
Scott Armstrong, Gideon Technologies
Shawn Dickson, Raytheon
Sheila Christman, National Security Agency
Steve Carver, FAA (Retired)
Steven Draper, National Security Agency
Terry Rimmer, Oklahoma Office of State Finance
Tom Grill, VeriSign

Table of Contents

Executive Summary

This white paper presents the findings of efforts in 2009 of the Security Content Automation Protocol (SCAP) Applicability Working Group of the Internet Security Alliance's VoIP Security Project. This VoIP Security Project was initiated by the ISAlliance in 2007 after the weakness of cyber security around VoIP and the potential critical impact of the exploitation or those weaknesses was understood. The project has received support from both by the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS) as well as many private sector companies.

The SCAP Applicability Working Group has been focused on determining the practicality of using SCAP to automate evaluation of security controls in a VoIP Network. Taking SCAP, which was designed for the evaluation of desktop computer's configuration compliance with the Federal Desktop Core Configuration (FDCC), and applying it to non-desktop components spread across a large network to implement a complex service is a significant undertaking. VoIP was a challenging service to attempt such automation because it is still an evolving technology and that no clear, universally accepted security controls has yet emerged. As a result, the project was carefully scope to address the challenging technological challenges without having to develop an encompassing and complete view of appropriate VoIP security controls.

A security assessment was conducted on a reference voip system (the Reference Architecture) that led to the definition of a set of security controls for VoIP. The security assessment was not complete, did serve to define a set of security controls for a VoIP system. Then, the use of SCAP was studied to evaluate that set of controls.

This whitepaper concludes that much of SCAP can easily be extended to a VoIP system. Specifically, Common Vulnerabilites and Exposures (CVE), Common Configuration Enumeration (CCE), and the Common Vulnerability Scoring System (CVSS) are those parts that are easily extended. The Extensible Configuration Checklist Description Format (XCCDF) and the Open Vulnerability and Assessment Language (OVAL) will be much harder to extend, though probably not impossible to extend. The challenge for XCCDF is that commonality and diversity of devices in a VoIP system begs for an object oriented approach that allows for checklist to be developed from a high-level class down toward a specific device model and firmware version. The challenge for OVAL is that the language is not functional enough to handle the multitude of devices and their corresponding controls.

Chapter 1 - History & Background of the ISAlliance Voice Security Project

The proliferation of network enabled devices has exploded. Unified Communication (UC) networks likely face the greatest challenge today in managing a diverse, large set of mobile and fixed devices. Ensuring that all of these numerous devices have the most up to date patches, present no known security vulnerabilities, and are configured to represent the organization's security policy, is a significant and growing challenge for the operational security leaders responsible for managing the risk in a UC Network.

UC Networks can be attacked via the notoriously old and well known data network exploits as well as via new exploits targeting VoIP vulnerabilities. A large U.S. retailer's VoIP system was successfully compromised via a simple password cracking attack because of a failure to validate compliance with the retailer's security policy. This compromise took place after an operator inadvertently mis-configured the VoIP PBX. The operator attempted to increase the password complexity setting on the PBX, but instead mistakenly turned off all password complexity rules. As can be expected, within hours the PBX was compromised, resulting in the lost of VoIP service to all the retailer's locations. This resulted in a significant financial loss due to the inability to process credit card and debit transactions. An automatic, periodic validation of the IP PBX configuration could clearly have detected and allowed correction before the IP PBX was compromised.

The Internet Security Alliance's Board of Directors acknowledged that this incident represented the significant potentials for malicious activity that exist within the VoIP solutions deployed or planned in many private and public sector organizations. The National Institute of Standards and Technology "Security Content Automation Protocol" (SCAP) program was developed to provide patch and configuration management for desktop computers. The IA Alliance Board immediately then raised the question: Would SCAP help address this and other security issues identified with enterprise VoIP deployments?

SCAP is a recommended approach for U.S. Federal Government Organizations to demonstrate compliance with security requirements in mandates such as the Federal Information Security management Act (FISMA). SCAP consists of two elements. First, SCAP is a protocol: it consists of six specifications that standardize how security software communicates information about software flaws and security configurations. These standards are the SCAP components. Second, SCAP provides software vulnerabilities and security configuration reference data. These are the SCAP content.

SCAP can be used for security configuration verification, requirements traceability, standardized security enumerations, and vulnerability measurement. From an enterprise voice perspective SCAP addresses three critical areas in providing a solutions level of assurance, namely, the

management of security vulnerabilities, the management of corrective content (patches), and the management of security configuration.

The ISAlliance reached out to NIST and DSH seeking their support of an ISAlliance lead program to assess the applicability of the SCAP program to enterprise VoIP solutions, and develop the appropriate SCAP content. NIST and DHS expressed extreme support of the proposal and encouraged the ISAlliance to continue with the incubation of their idea.

ISAlliance continued their work and presented their VoIP SCAP proposal to the The Fourth Annual Information Security Automation Conference in Gaithersburg, MD in September, 2008. In addition, a daylong workshop was proposed to further develop the ISAlliance's proposal and solicit feedback and approaches on how to assess the applicability of the SCAP approach to real-time systems such as enterprise VoIP solutions, and how to develop reference SCAP content to establish a minimum baseline for appropriate VoIP configurations.

The result of the workshop was the realization to properly assess the applicability of SCAP to VoIP required an industry-working group. ISAlliance established such a group in early 2009 with the primary objectives of assessing the appropriateness of the SCAP Program to enterprise voice solutions and, if appropriate, the development of appropriate benchmark SCAP content.

Chapter 2 - ISAlliance Voice Security Project Goals and Objectives

Originally, the initial goal of the ISAlliance VoIP Security Project was to develop SCAP baseline content to enable VoIP developers to develop product specific SCAP content. This goal was the distillation of the realization that with the proliferation of network enabled devices in the enterprise, there was s need to ensure that the network enabled devices introduce no known vulnerabilities, are properly patched, and are securely configured. These activities are critical; this is especially so with enterprise voice services. The ability to do these automatically on a periodic basis will improve the overall assurance of the organizations' voice solution, and provide an increase in security posture of voice services.

The SCAP for VoIP workshop held at the Fourth Annual Security Automation Conference was very successful. One of the most important conclusions that was reached was to properly assess the applicability of SCAP to VoIP would require a detailed review of SCAP from a voice perspective by an industry working group. ISAlliance established such a group in early 2009 with the primary objectives of assessing the appropriateness of the SCAP Program to enterprise voice solutions and if appropriate, the development of appropriate benchmark SCAP content. To achieve the objective of providing a report on the ISAlliance VoIP Security Project at the fifth Annual Security Automation Conference, the working group was split into two sub groups. The first was charged with determining the applicability of the SCAP program to VoIP; the second was assigned to develop a list of applicable VoIP Security standards that could be used as references to developed baseline SCAP content for VoIP security. This whitepaper represents the findings of the first working group: Applicability of SCAP To VoIP.

Chapter 3 -- Scope of the SCAP Applicability Working Group

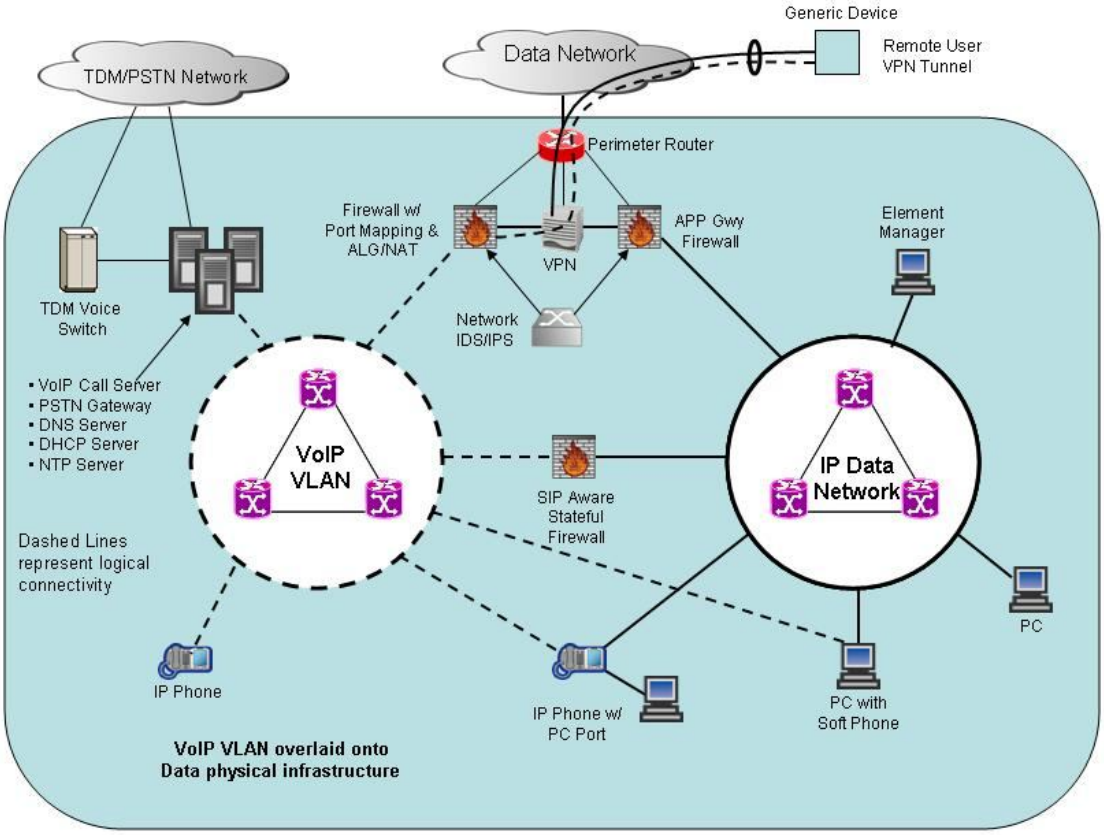
Accomplishing the objectives and goals of the VoIP Security Project required strict consideration of challenges from two very distinct directions. First, application of SCAP from a desktop environment to a network-wide, complex application is a challenge in and of itself. Second, defining a complete, comprehensive, broadly applicable set of VoIP Security controls is a challenge in its own right. VoIP continues to evolve as a technology and security approaches have not yet converged to the point that a single view of the architecture, threats and risks can be reasonably asserted to lead to a common set of controls. As a result, there is tremendous conflict in moving a project aimed at automating validation of security controls of a VoIP system using SCAP in a relatively short amount of time. Firmly fixing the scope of work is our solution to working through these conflicts.

The most important outcome of this project is an assessment of the viability and ease of use of SCAP to automate a network wide application. Secondly, it is to specifically judge the viability and ease of use of SCAP to automate the verification of security controls implemented on a VoIP system. Thirdly, it is to define a reasonably comprehensive set of security controls required by VoIP systems commonly deployed today.

In order to complete our work within 6 months of our kick-off, much thought was given to what comprised a “reasonably comprehensive set of security controls required by VoIP systems commonly deployed today.” We arrived at the following approach: define a reference VoIP reference architecture, conduct a threat risk analysis, develop a list of security controls, and then examine use of SCAP to validate the controls. To reduce the effort, but still achieve that primary goal of examining the use of SCAP to validate VoIP security controls, the logical and physical architecture was limited. In particular, we chose to focus on SIP deployments exclusively, to ignore the use of SIP trunks (external VoIP connections are always assumed to be through a media gateway), and to ignore the existence of voice mail systems and audio conferencing systems. While we readily admit that this position reduces the utility of the reference VoIP system, this was necessary to constrain the work effort to an achievable level while not making the reference architecture too simple and thereby potentially skewing results. Additional functionality, signaling and network interconnect are important considerations and are considerations we expect to address in a subsequent effort as this project continues in more phases.

Chapter 4 - VoIP Architecture

Our chosen Reference VoIP Architecture (RA) is shown in Figure 1 and represents a typical single-site generic enterprise VoIP deployment. This RA establishes a common terminology and sets the groundwork for the discussions and analysis that follows later in this paper. This RA is closely based on the VoIP Architecture documented in the DoD/DISA document titled "*Internet Protocol Telephony & Voice Over Internet Protocol – Security Technical Implementation Guide Version 2, Release 2*".



Note – This generic architecture is based on the VoIP Security Architecture captured in the DoD/DISA document titled "INTERNET PROTOCOL TELEPHONY & VOICE OVER INTERNET PROTOCOL – SECURITY TECHNICAL IMPLEMENTATION GUIDE Version 2, Release 2" (Figure 3-1)

Figure 4.1 – The Reference VoIP Architecture

A typical VoIP deployment makes use of the existing IP infrastructure for business and economic reasons. VoIP services overlay onto the IP network already in place, with special consideration given to Quality of Service (QoS), Availability, and Security. The convergence of Voice and Data onto a single IP network to form a UC network has blurred the division between traditional telephony and data services from both operations and support perspectives. However, because of the special needs of a real-time service such as VoIP, there are additional considerations to ensure a successful and robust deployment.

Duplication of physical networking components would make the business case for VoIP uneconomical. But, separate networks for voice and data are required to deliver the substantially different Quality of Service (QoS) Requirements of voice. For this reason, the Switch Routers depicted as part of the IP Data Network and the Core VoIP Virtual LAN (VLAN) could very well the same physical devices, with logical separation between traditional data services and VoIP services being provided using VLAN technology. The dashed lines in the RA are used to depict network element connectivity to the VoIP VLAN.

The VoIP Servers, VoIP Clients, traditional data devices, and servers that provide Network Services (DNS, DHCP etc.) are all logically separated into Security Zones to provide differing treatment. Using different Security Zones for devices that share common functionality provides a coarse level of protection and enables the application of specific policies and procedures specific to the common functionality. All of the VoIP elements are connected to a VLAN configured to support the QoS, Security, and Availability requirements for VoIP traffic.

A TDM Gateway provides connectivity to and from the VoIP domain to support PSTN calls and calls to/from traditional telephony sets, potentially deployed in the same Enterprise. Also depicted in the RA is a Session Border Controller that, although out of scope for this paper, would secure SIP trunks to a VoIP Service Provider.

Also included in the RA is a Generic Device that makes use of VPN Tunneling to connect to the Enterprise, since this is a very common deployment for teleworkers and "road warriors". The VPN tunnel is terminated as usual in the data network and the VoIP specific traffic is routed though a VoIP aware firewall.

Throughout this paper the various Security Controls will be discussed as they relate to Security Planes. The requirements at the various planes can differ and this will be evident in the upcoming Chapter 5 - Threat Risk Assessment. The three Security Planes are (1) Media Plane (also called End-User Plane or Bearer Plane), (2) Signaling & Control Plane, and (3) Management Plane. These Security Planes are well defined in a document titled "*Draft ITU-T Recommendation X.805 (Formerly X.css), Security architecture for systems providing end-to-end communications*" and in the ATIS Standard *ATIS-1000007.2006 – Generic Signaling and Control Plane Security Requirements for Evolving Networks*[1].

The Media Security Plane addresses the user data flows. Specifically, in a VoIP deployment this would be the RTP/RTCP media flows. Other generic Protocols of concern are HTTP/HTTPS, POP, IMAP, TCP, UDP, FTP, IPSec, and TLS.

The Signaling & Control Security Plane typically involve the security of machine-to-machine communications and call set-up and teardown. In the context of this paper, the primary protocol for consideration is SIP. Other generic Protocols to be considered at this plane are BGP, OSPF, IS-IS, RIP, PIM, RSVP, H.323, SS7, IKE, ICMP, PKI, DNS, DHCP, SMTP.

1
© Copyright 2009 by the Alliance for Telecommunications Industry Solutions, Inc. ATIS publications are available from the ATIS Document Center at https://www.atis.org/docstore/default.aspx Version DRAFT .

The Management Security Plane involves the protection of Operations, Administration, Management and Provisioning of network elements and back-office systems. Generic Protocols of concern are SNMP, Telnet, S/FTP, TFTP, and HTTP/S.

The major VoIP specific elements are identified in Table 1, along with basic information regarding functionality.

Device	Functionality
IP Phone	IP based telephony device
IP Phone with PC Port	IP based telephony device with integrated Layer 2 Ethernet switch
PC with Soft Phone	Personal Computer with software based IP telephony client
Session Border Controller	A device (or collection of devices) that controls real-time session traffic at the signaling, call-control, and packet layers as they cross between networks or between network segments
Call Manager	A hardware/software based VoIP component (or components) that provide registration, configuration and call control functionality for VoIP end devices
TDM/PSTN Gateway	Network element that provides protocol/signaling translation between an IP based telephony service and a traditional TDM based telephony service
VoIP Aware Firewall	A firewall that is SIP-aware, meaning that it has the capability to discover the RTP/RTCP port information that SIP dynamically assigns to the media stream. The VoIP aware firewall must have the ability to parse the SIP exchanges in order to discover which packets contain the media streams.

Table 4.1 Major VoIP Elements

Chapter 5 - VoIP Threat Risk Assessment

Overview

This section discusses security threats and vulnerabilities encountered in the VoIP Reference Architecture and a high level overview of security controls to mitigate the risk of such threats which adversely impact the operations, assets and overall voice services of the organization.

Numerous approaches have been used by information security personnel to evaluate the security risk of an organization and its IP communication infrastructure. Security risk assessments range from strictly a technical evaluation of the infrastructure to an all encompassing assessment from a technical, organizational and business perspective. In general, such assessments are comprised of:

(i) identification of information-related assets that are critical to the organization and infrastructure, in this case the VoIP Reference Architecture

(ii) identification of potential threat sources and corresponding risk likelihood against each asset

(iii) identification of security controls in place to protect the assets

(iv) identification of the presence of vulnerabilities due to missing or insufficient security measures

(v) determination of the acceptable level of risk for each asset – threat pair

(vi) determination of an organizational defined ranking of its informational assets so that sufficient security controls can be deployed to mitigate against the highest impacts to the organization.

Security risk assessment (or threat risk analysis) is typically a very lengthy, detailed process. The assessment described in this chapter will provide a high level examination of threat sources, vulnerabilities and risks that may be encountered in the VoIP Reference Architecture; leading towards guidance on the mitigation of such threats. The assessment is focused on the critical system elements, protocols and applications defined as in scope for this effort. The assessment does not examine the underlying IP network infrastructure except where it directly impacts VoIP services, any specific vendor implementation, operating system, organizational policy and business objectives. Furthermore, the analysis does not develop relative probabilities and priorities among the list of possible threats and vulnerabilities. Rather it is for the reader to rank the probabilities and priorities according to organization and business objectives.

Asset Classification

A key aspect to the security risk assessment is the identification of assets which define the VoIP Reference Architecture, and in particular selection of those assets which are considered most critical to be protected from compromise, exploitation, interruption or loss. Assets may be physical systems, information, service level agreements, regulatory commitments, staff and any other physical or logical element that is important for the organization to protect.

The number of critical assets for an organization may easily exceed one hundred. To make the analysis more manageable, only the most common assets will be reviewed in this document. High level asset groups or asset containers have been defined to categorize the various assets which comprise the basic VoIP architecture. These high-level asset groups are:

- **Hardware systems** which include the IP PBX, Call Controller or call manager, media gateway, IP phone handset, desktops, databases, and supplemental servers.
- **Software** such as operating systems, VoIP related application software (i.e. soft phone) and third-party security software such as malicious code detection/removal, anti-virus, host based firewall applications.
- **Network infrastructure** comprised of routers, switches, firewalls, VPN devices, Intrusion detection / prevention systems.
- **Staff personnel** responsible for the architecture, network and security operations, system administration and software development; including the enforcement of policies and processes critical to the security of the organization.

As noted earlier in the document the only most basic elements of a VoIP service infrastructure is defined in our VoIP Reference Architecture. Platforms such as voicemail, audio conferencing server (or media servers), application servers, fax over IP, email integration for unified messaging, session border controllers, SIP trunks, and other elements present in a comprehensive unified communication solution will be assessed in the future.

It is important to understand the security requirements of each critical asset so one may understand how a particular threat will adversely impact the VoIP Reference Architecture. The core principles of information security – confidentiality, integrity and availability, are asked upon each critical asset to identify the importance of the requirements on the asset (i.e., low, moderate and critical). This evaluation of each asset will help to identify the security controls to best protect the particular asset described later in the section. The core principles (or requirements) of information security are defined as follows:

- **Confidentiality**. The "property of preventing disclosure of information to unauthorized individuals, processed or systems." Typically some form of encryption is used to satisfy this security requirement.
- **Integrity**. The accuracy of information created, modified, stored and delivered within and possibly outside of the organization with proper authentication and authorization to do so.

- **Availability**. The property of ensuring the network, information, service or application is accessible when needed by an authorized entity.

Other well-known security requirements such as authentication, authorization, accountability and non-repudiation are not ranked for its importance on each critical asset in this version of the white paper. The following classifications of security importance are used for this assessment:

Security Importance	Definition
Low	The compromise or loss of the security principle from the asset will result in no loss of confidence or risk seen by the organization.
Moderate	The compromise or loss of the security principle from the asset will cause loss of confidence and risk to the VoIP service infrastructure with service degradation experienced by many individuals however no loss of availability or critical data.
Critical	The compromise or loss of the security principle from the asset will cause loss of availability and/or complete compromise resulting in the VoIP service not being useable.

Table 5.0 – Security Importance Definition

Table 5.1 below identifies system assets and corresponding informational assets which are considered critical to the VoIP Reference Architecture, including the degree of importance each core security requirement or principle has on each asset.

System Asset	Informational Asset	Importance Of Security Requirement		
		Confidentiality	Integrity	Availability
IP Phone Handset	Operating System	Low	Moderate	Moderate
	Configuration	Low - Moderate	Moderate	Moderate
	Media	Moderate	Moderate	Critical
	Signalling	Moderate	Critical	Critical
	Management	Critical	Critical	Critical

1

System Asset	Informational Asset	Importance Of Security Requirement		
		Confidentiality	**Integrity**	**Availability**
Desktop	Operating System	Low	Moderate	Moderate
	VoIP Application (i.e., Soft phone)	Low	Moderate	Moderate
	Media	Moderate	Moderate	Critical
	Signalling	Moderate	Critical	Critical
	Management	Critical	Critical	Critical
System Asset	**Informational Asset**	**Importance Of Security Requirement**		
		Confidentiality	**Integrity**	**Availability**
IP PBX (includes media gateway, Call Controller / call manager) *[Note 1]*	Operating System	Low	Critical	Critical
	Configuration	Moderate	Critical	Critical
	Dial Plan	Moderate	Critical	Critical
	Call Detail Records (and Billing Info)	Critical	Critical	Critical
	Software Licenses	Low	Moderate	Critical
	Media	Moderate	Moderate	Critical
	Signalling	Moderate	Critical	Critical
	Management	Critical	Critical	Critical
System Asset	**Informational Asset**	**Importance Of Security Requirement**		
		Confidentiality	**Integrity**	**Availability**
Element Manager	Operating System	Low	Critical	Moderate
	Configuration and Management	Moderate	Critical	Moderate

2

System Asset	Informational Asset	Importance Of Security Requirement		
		Confidentiality	Integrity	Availability
Network (i.e., router, switch, firewall, VPN, IPS)	OS / Firmware	Low	Critical	Critical
	Media	Moderate	Moderate	Critical
	Signalling	Moderate	Critical	Critical
	Management	Critical	Critical	Critical
System Asset	**Informational Asset**	**Importance Of Security Requirement**		
		Confidentiality	**Integrity**	**Availability**
DNS, DHCP, TFTP, RADIUS	Operating System	Low	Critical	Critical
	User Identification	Low	Critical	Critical
	User Profiles	Moderate	Critical	Critical
	Configurations (phones)	Low - Moderate	Critical	Critical

Table 5.1 Critical System and Informational Assets

[Note 1] The call processing and media gateway functionality may be composed of a distributed or centralized (appliance) architecture dependent on the specific vendor.

Threats on Critical Assets

Once critical assets are identified, the next step in a security risk assessment is to identify potential threats and likelihood for the threat to occur in the organization. The security risk assessment reviewed possible threats to the critical assets of our VoIP Reference Architecture by identifying potential threat sources. A security threat is an entity with the capability, intent and method to compromise, damage or alter an information system or information by taking advantage of a weakness or vulnerability inherent to the exploited system or information. The organization must understand how to profile a threat on its network infrastructure, devices and data; and only afterwards can the organization properly develop a security strategy to protect against potential threats.

A threat profile is defined by a specific entity or situation as the source of the security risk, method of access into the organization, the entity's authorized role in the organization, and action taken by the entity to exploit a vulnerability to the asset in the organization. Many threats will be initiated in a malicious and illegal manner however accidental threats will occur and must be considered in the assessment and overall security mitigation strategy. Examples of deliberate threat sources include malicious users residing inside and outside the VoIP service infrastructure, downloadable software with malicious code, and physical disruptions. Accidental threat sources may include power outage, fire, flood, software, hardware and firmware failures, and mis-configurations of phones and servers; although these too may be deliberate. Furthermore, such threat sources may access an organization's network infrastructure via numerous methods from communication channels such as the Internet, LAN, WAN, wireless and modem, to physical access methods such as laptops, USB memory sticks and drives, and third-party software.

It is threat sources with the possibility to exploit the vulnerabilities of each asset which leads to consequences adversely impacting the organization and business objectives that must be examined in the assessment. The following identifies common threat sources which may compromise and exploit one or more critical assets to an organization. Some of these threat sources are accidental whereas other threat sources are deliberate or intentional. Here are the potential threat sources:

- **Malicious users** such as disgruntled employees, contractors, hackers which may establish an attack vector from either inside or outside the organization.
- **Accidental users** such as trusted employees and contractors whose actions or inactions may have caused an exploitable vulnerability.
- **Configuration weaknesses and mistakes** from trusted actors.
- **Social engineering** where confidential/sensitive information on the organization, infrastructure and services is discovered using deception or misrepresentation.
- **Email** with embedded Web links and malicious attachments.
- **Software** such as flaws in the implementation of an application, protocol or operating system, or delivery of malicious code (i.e., malware, virus, trojan, worm) into the organization.
- **Hardware** such as a defect in the hardware or delivery of confidential / sensitive information to unauthorized personnel (i.e., USB memory sticks, used laptops and hard drives).
- **Data leakage** where confidential/sensitive information on a laptop and removable media with the possibility of being stolen and/or discovered by malicious actors.
- **Third party providers** providing an access conduit into the organization for deliberate and accidental threats.
- **Physical interruption** due to accidental or deliberate causes (i.e., power outage, flood, severed Internet or PSTN circuit/cable, system upgrades, etc)
- **Unknown threats** – thus risk assessment is an ongoing process.

Every organization has limited resource capabilities (i.e., personnel, budget) to implement the ideal security strategy to address all potential threats. It is important to determine the potential risk (or product of likelihood and impact) for a threat to actually exploit a vulnerability and cause damage to the organization. The damage or impact may be qualified as a loss of availability, integrity and confidentiality; including other possible losses. It is not possible to identify all risks, nor is it possible to eliminate all risks. Therefore the organization must develop criteria to prioritize such risks, and apply more resources to protect higher risk assets above lower risk assets. Calculation of the threat likelihood may range from a simple qualitative classification to a more in depth quantitative approach using historical data and trend analysis. Selection of the most appropriate measurement for threat likelihood is out-of-scope for this white paper. The white paper will utilize a coarse qualitative classification to illustrate the assessment performed on our VoIP Reference Architecture. The classification is based on two key factors – time frame of threat occurrence and location of threat source. Other factors such as access method, accidental versus deliberate intention, and other dependencies can provide further granularity to determine the threat likelihood, however, these factors were not used for this assessment. The following scoring (or ranking) criteria should be used to determine the likelihood of a threat on the VoIP Reference Architecture; the criteria is based on the ETSI TIPHON Threat Likelihood Scoring Criteria [2].

- **Low** means (i) threat needs to bypass strong technical controls to exploit an organization, or (ii) motivation for the threat is very low.
- **Medium** means (i) threat needs to bypass less than strong technical controls without significant effort, or (ii) motivation for the threat is reasonable.
- **High** means (i) there are not sufficient controls to mitigate or prevent the threat, or (ii) motivation for the threat is high.

Basic threat sources such malicious users, configuration weaknesses, hardware and software flaws, and physical disruptions were considered in the assessment of our VoIP Reference Architecture and are depicted in Table 5.2 below. Other threat sources were not considered for this whitepaper.

With the convergence of voice and data across a common IP network, it is anticipated the likelihood for a threat source to adversely impact the organization is higher from the IP / data network than PSTN (i.e., POTS). Thus the primary focus of this risk assessment will be with LAN/WAN/Internet residing actors attempting to use these threats sources against the organization. However threats from PSTN initiated weaknesses such as modems to gain unauthorized access to systems are common enough that appropriate security controls will be identified later in the document. Furthermore, as IP connectivity to the Public VoIP Network (i.e., SIP trunks) becomes readily available, threats from the Public VoIP Network may certainly increase. For purposes of simplicity, wireless IP access and remote VPN access (i.e., SSH, IPSec) are considered an external method of access with threats similar to attacks from the Internet.

Threat Sources	Threat Likelihood Based on Access Vector		
	Internal Network	**External / Internet**	**External / PSTN**
Malicious or Accidental Users	High	High	Medium
Configuration weaknesses	High	High	Medium
Hardware flaws	High	Medium	Low
Software flaws	High	High	Low
Physical Interruptions	High	Medium	Low

Table 5.2 Threat Sources and Likelihood

Threat likelihood and threat impact are not the same. It is possible that a high probability threat (i.e., hardware failure) may have a very low impact to the organization which implements system redundancy. In other circumstances a threat with a smaller likelihood to occur, such as the loss of a PSTN circuit, will have a critical impact to the organization.

The next step to the security risk assessment is to identify for each critical asset those threats which potentially have a high likelihood and high adverse impact to the organization. The following threat impact criteria have been identified; based on the ETSI TIPHON Threat Impact Scoring Criteria [2].

:

- Minor (or Low) – impact will result in no loss of confidence seen by the organization. A few individuals may be temporarily impacted. Potential damage will remain low.
- Major (or Medium) – impact will cause loss of confidence to the VoIP service infrastructure with service degradation experienced by many individuals however no loss of availability or critical data. Potential damage can not be neglected.
- Critical (or High) – impact will cause loss of availability and/or complete compromise resulting in the VoIP service not useable. Potential damage may be severe.

Risk is a product of potential impact of threat on organization and likelihood for threat to occur. Table 5.3 illustrates the threat risk scoring criteria used by ETSI TIPHON [2]. Low is scored 1, Medium scored 2 and High scored 3; and thus a risk from 1 (lowest) to 9 (highest). Countermeasures should always be implemented for higher risk threats before lower risks.

Threat Impact	Threat Likelihood		
	Low	**Medium**	**High**
Low	Minor Risk	Minor Risk	Major Risk
Medium	Minor Risk	Major Risk	Critical Risk
High	Major Risk	Critical Risk	Critical Risk

Table 5.3 ETSI TIPHON Threat Risk Score

Next is to apply the threat impact, likelihood and risk scoring methodology defined above to the critical assets identified for the VoIP Reference Architecture in Table 5.1. As described earlier certain threat sources are more likely to occur inside the organization as oppose to outside. Table 5.4 illustrates the risk to the assets from threats originating from inside the organization; however risk of exploitation is based on organization's deployment of security controls. The same methodology may be applied to threats originating from outside.

System Asset	Informational Asset	Threat Impact	Threat Likelihood	Risk
IP Phone Handset	Operating System	Low	Medium	Minor
	Configuration	Low	High	Major
	Media	Low	Low	Minor
	Signalling	Low	Low	Minor
	Management	Low	Medium	Minor
Desktop	Operating System	Low	High	Major

	VoIP Application (i.e., Soft phone)	Low	High	Major
	Media	Low	Low	Minor
	Signalling	Low	Low	Minor
	Management	Low	Medium	Minor
Call Controller and Media Gateway (or IP PBX) Note 1	Operating System	High	High	Critical
	Configuration	High	High	Critical
	Dial Plan	High	High	Critical
	Call Detail Records (and Billing Info)	Medium	High	Critical
	Software Licenses	Medium	High	Critical
	Media	Medium	Low	Minor
	Signalling	Medium	Low	Minor
	Management	Medium	Medium	Major
Element Manager	Operating System	Low	High	Major
	Configuration and Management	Low	High	Major
Network (i.e., router, switch, firewall, VPN, IPS)	OS / Firmware	High	Medium	Critical
	Media	Medium	Medium	Major
	Signalling	Medium	Medium	Major
	Management	Medium	Medium	Major

DNS, DHCP, TFTP, RADIUS	Operating System	High	High	Critical
	User Identification	Medium	High	Critical
	User Profiles	Medium	High	Critical
	Configurations (phones)	Medium	High	Critical

Table 5.4 Threat Risk Score of Critical Assets From Internal Threats

Vulnerabilities Exploited By Threats

With threats identified for each critical asset, the next step is to identify what possible vulnerabilities may exist for each asset. As performed with threat sources, the exhaustive list of vulnerabilities will need to be prioritized (or ranked) based on the likelihood or risk for the vulnerability to be exploited by a threat and its adverse impact or consequence on the organization. Such consequences include disclosure or viewing of sensitive information, modification of important or sensitive information, loss of important information, and interruption of access to information, applications and services. This section will discuss vulnerabilities which may exist in the VoIP Reference Architecture and its impact to the organization should appropriate security controls not be implement to protect the applicable assets.

Vulnerability is a weakness or flaw in the design and implementation of the VoIP protocols and applications, operating system, supplemental services (i.e., DNS, DHCP), network, physical infrastructure, policies and procedures which may be exploited. Not only is the risk of a vulnerability specific to the asset and information associated with the asset, the network location of where the vulnerability is exploited is also of importance. Typically, an organization's network is partitioned into various security zones (i.e. trusted, DMZ and untrusted), each with its unique security requirements. It is part of the security risk assessment to determine what risk the vulnerability has on a specific asset in a particular security zone within the network.

As a threat gains access into the organization's network, the threat attempts to discover assets with exploitable vulnerabilities. Fundamentally, this is performed by scanning for specific services and known ports (aka, footprinting), identify the device based on the running services,

ports and vendor ID in MAC address, and afterwards attempt to compromise the device based on vulnerabilities known to exist for the device.

A threat may attempt to exploit numerous logical elements (i.e., module, process) of an asset or focus on a single specific element. From an operational perspective, each element can be viewed in terms of how the asset is involved with the VoIP service. The asset may be involved with the signaling, media or management aspect of the VoIP service. Each type of traffic or 'plane' has its own protocols.

- **Media or Bearer Plane** is responsible to deliver the voice packets between IP endpoints such as IP phones and media gateways. RealTime Protocol (RTP) and RealTime Control Protocol (RTCP) are the key protocols used for media.
- **Signalling or Control** Plane is responsible to deliver the call setup, teardown and mid-call information between IP endpoints, Call Controllers/call managers, and supplemental servers such as DNS, DHCP, TFTP. The signalling plane is used to initiate traffic across the media plane. For this assessment Session Initiation Protocol (SIP) is the primary VoIP signalling protocol.
- **Management Plane** is responsible to deliver the administration, management and monitoring traffic out-of-band with respect to the actual voice call. The management plane may use the same network as the signalling and media planes, or a separate network may be provided for management purposes only. Various remote terminal (i.e., Telnet, SSH), Web/GUI console (i.e., HTTP/HTTPS), file transfer (i.e., FTP, TFTP, SFTP, SCP), configuration and monitoring (i.e., SNMP) and management user authentication (i.e., RADIUS, TACACS) protocols are used across the management plane.

The following are common types of vulnerabilities possible in the VoIP Reference Architecture.

Configuration weakness of the operating system and VoIP applications results in the use of unnecessary services and open TCP/UDP ports, insecure management and file transfer protocols, default service settings (i.e., use of 'public' community string for SNMP), and other vendor assigned default settings simply enabled for ease of deployment. A weak configuration may allow the attacker to exploit other vulnerabilities such as unauthorized access, reconnaissance and denial-of-service.

Unauthorized access due to weak authentication typically results from use of credentials such as a source IP address, default vendor passwords, simple passwords, and unencrypted (or cleartext) passwords as the sole mechanism for validating identities and providing authorization for a user or device to access resources. Failure to properly authenticate users can allow the realization of additional threats including tampering, fraudulent use of the asset, eavesdropping, denial of service, or compromise of system integrity.

Malicious Code is defined in NIST IR 7298 as "Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host." Malicious code can be used to gather information on system management and/or signalling and control for fraudulent use, denial of service, or further compromise of the system.

Reconnaissance and Enumeration occur when a potential attacker seeks information about an asset or system to cause an exploit or compromise. IP and MAC addresses, operating system and application versions, open ports, and services used by the assets are some types of information which can be harvested. Information may be gathered using any number of common protocols and services such as BOOTP, TFTP, SNMP, HTTP, and SIP, including social engineering techniques. As the attacker understands the organization's VoIP deployment, the attacker can probe or enumerate the organization for specific VoIP vulnerabilities.

Spoofing (or masquerading) involves presenting falsified identity information to gain unauthorized access to a system; including a means to bypass access control measures. The falsified identity may be a MAC or IP address, SIP Uniform Resource Identifier (URI), caller ID, or other form of identity. FIPS 191 notes spoofing involves: (i) the ability to receive a message by masquerading as the legitimate receiving destination, or (ii) masquerading as the sending machine and sending a message to a destination. Attackers can use spoofing to launch further attacks such as unauthorized access, fraudulent calls, denial-of-service, and man-in-the-middle attacks.

Impersonation involves the pretence of legitimacy using falsified or captured credentials, such as a rogue call server pretending to be the authorized call server. Impersonation relies heavily on spoofing and eavesdropping to acquire the information needed. Impersonation can facilitate registration and media session hijacking, toll fraud, denial of service, and system compromise.

Eavesdropping occur when an attacker can capture media, signalling or management traffic without authorization. An attacker may use network assets to 'sniff' and forward duplicated packets or redirect the signalling and media packets to a rogue device so the attacker may capture the targeted traffic. Eavesdropping affects the confidentiality of a voice conversation delivered across the media plane. When applied against the Signalling and Management planes, eavesdropping can provide the attacker with sensitive information such as credentials (i.e., user ID, password, PIN, telephone number) for use in more complex system intrusions such as unauthorized access, toll fraud and man-in-the-middle attacks.

Signalling and Media Manipulation can lead to threats to communication integrity. Media manipulation can include deletion, insertion, redirection and replay of media. Signalling manipulation can result in denial of service via the generation of false registration packets which tie up phone operations, the generation of invite packets which cause the phone to ring, and sending "bye" packets which disconnect calls. It can also result in unauthorized redirection of calls and facilitate the implementation of a rogue proxy onto the network.

Fuzzing occurs when an attacker sends messages with malformed syntax, incorrect or unexpected message sequence to a system with the intent to crash it. This vulnerability may lead to a type of DoS attack causing buffer overflows without the need for excessive flooding of packets. Fuzzing may impact the availability and possibly the integrity or accountability of organization's VoIP service.

Man-in-the-middle attacks use interception, impersonation and spoofing to insert a rogue device into the communications path as a legitimate server or endpoint. The impacts include eavesdropping on a conversation, the deletion, injection or replay of media or signalling content, reconstruction of DTMF tones, and redirection of a conversation. Interception of the traffic may be performed at the network level (i.e., ARP poisoning) or application level (i.e., SIP registration hijacking).

Denial-of-Service (DoS) attacks result in the disruption to the network, system or service through the use of packets designed to overwhelm it. Packets may be carefully crafted payloads to exploit an operating system or application, or a flood of packets to overburden the target. Impacts range from ability to block legitimate calls, degradation of call quality, to crashing segments of the network, system or application. Types of packet flooding range from ICMP, UDP and TCP packets to application flooding such as various SIP protocol messages (i.e., Invite, Register, Notify, Info, Option, Bye). Some flooding attacks may be unintentional such as SIP endpoints configured with very short registration intervals, problematic software, and high traffic circumstances (i.e., simultaneous reboot). Regardless, DoS attacks against VoIP/IP PBX systems, DHCP, TFTP, DNS, and network-security devices can adversely impact the overall VoIP service.

Theft of Service/Toll Fraud involves the unauthorized use of assets to place a call without approval or payment. Typically a malicious actor gains access to a VoIP asset due to weak authentication, spoofing, eavesdropping and impersonation.

VOIP Spam (or Spam over Internet Telephony – SPIT) and Phishing involve the unsolicited use of email messages, voice messages or phone calls to gain credentials or other sensitive data through social engineering. At some point, the volume of VOIP Spam can also degrade system performance.

Table 5.5 identifies how each vulnerability classification will typically impact the organization with respect to its signalling, media and management traffic.

Vulnerability	Impact To Traffic Plane		
	Media	**Signalling / Control**	**Management**
Unauthorized Access - Weak Authentication	Compromise, Loss of confidentiality	Compromise, Loss of integrity	Compromise, Loss of integrity
Configuration Weakness	Degrade Call Quality, Disclosure	Compromise, Disclosure	Compromise, Disclosure
Malicious Code	Degrade System Performance	Compromise, Degrade System Performance	Compromise, Degrade System Performance
Reconnaissance, Enumeration	Host Discovery - Disclosure	Host Discovery - Disclosure	Host Discovery – Disclosure
Spoofing (masquerading)	Confidentiality	Loss of availability, Integrity	Integrity
Eavesdropping	Confidentiality	Integrity	Integrity
Signalling And Media Manipulation / Hijacking	Integrity	Integrity, Disruption, Degrade Performance	N/A
Fuzzing	Degrade System Performance	Loss of availability, Degrade Performance	Degrade System Performance
Impersonation	Confidentiality	Integrity	Integrity

Vulnerability	Impact To Traffic Plane		
	Media	**Signalling / Control**	**Management**
Man-In-The-Middle Attacks	Intercept and manipulate to impact confidentiality	Intercept and manipulate to impact integrity	Intercept and manipulate to impact integrity
Denial-Of-Service Attacks	Degrade Call Quality & System Performance	Loss of Availability, Resource exhaustion	Loss of Reliable In-band Management
Theft of Service / Toll Fraud	Unauthorized or fraudulent calls	N/A	N/A
VoIP Spam And Phishing	Degrade System Performance	Identity Theft, Disclosure	Disclosure

Table 5.5 Vulnerability Impact on Traffic Plane

A threat which has successfully exploited a vulnerability of a critical asset will have adversely impacted the VoIP Reference Architecture. This impact or consequence will broadly result in the unauthorized disclosure of information, the modification of information or operation for unauthorized purposes, interruption of an asset, service or network without cause, or loss of an asset, service or network. The following vulnerability impact classifications on assets have been identified:

- **Low** – impact will result in no loss of confidence or degradation of service seen by the organization. A few individuals may be temporarily impacted.
- **Medium** – impact will cause loss of confidence to the VoIP service infrastructure with service degradation experienced by many individuals however no loss of availability or critical data.
- **High** – impact will cause loss of availability and/or complete compromise resulting in the VoIP service not useable.

Table 5.6 shows the potential impacts of select vulnerabilities in four consequential areas: disclosure, modification, interruption, and loss. These are average impacts and not necessarily the worst case impact.

Vulnerability	Impact of Vulnerability on Asset (= Consequence)			
	Disclosure	**Modification**	**Interruption**	**Loss**
Unauthorized Access - Weak Authentication	High	High	High	High
Configuration Weaknesses	Low-Medium	High	Medium	Medium
Malicious Code	Low	High	Medium	Low
Reconnaissance	Low	Low	Low	Low
Spoofing	Low	Medium	Low	Low
Eavesdropping	Low	Low	Low	Low
Signalling And Media Manipulation / Hijacking	Low	High	Medium	Medium
Fuzzing	Low	Medium	Medium	Low
Impersonation	Medium	High	Low	Low
Man-In-The-Middle Attacks	Low	High	Medium	Medium
Denial-Of-Service Attacks	Low	Low	High	Medium - High
Theft of Service / Toll Fraud	Low	Low	Low	High
VoIP Spam And Phishing	Medium	Low	Low	Low

Table 5.6 Vulnerability Impact on Asset

Table 5.7 shows the most critical security requirements, most critical impacts, and most likely threat vulnerabilities for selected system assets.

System Asset	Informational Asset	Most Critical Security Req	Most Critical Impact	Most Likely Threat-Vulnerabilities
IP Phone Handset	Operating System	Integrity	Modification	Traditional Data Exploits
	Configuration	Integrity	Loss of Avail.	Weak Authentication
	Media	Integrity	Call Quality Degradation / Loss of Avail.	DoS Attack
	Signalling	Integrity	Interception	Eavesdropping
	Management	Integrity	Interception	Eavesdropping
System Asset	**Informational Asset**	**Most Critical Security Req**	**Most Critical Impact**	**Most Likely Threat-Vulnerabilities**
Desktop	Operating System	Integrity	Loss of Avail.	Malicious Code, Traditionnel Data Exploits
	VoIP Application (i.e., Soft phone)	Integrity	Loss of Avail.	Configuration Weakness
	Media	Integrity	Call Quality Degradation / Loss of Avail.	DoS Attack
	Signalling	Integrity	Interception	Eavesdropping
	Management	Integrity	Interception	Eavesdropping

1

System Asset	Informational Asset	Most Critical Security Req	Most Critical Impact	Most Likely Threat-Vulnerabilities
Call Controller and Media Gateway (or IP PBX)	Operating System	Integrity	Modification	Malicious Code, Traditionnel Data Exploits
	Configuration	Integrity	Loss of Avail.	Configuration Weakness
	Dial Plan	Integrity	Loss of Avail	Theft of Service / Toll Fraud
	Call Detail Records (and Billing Info)	Integrity and Confidentiality	Loss of Avail., Repudiation	Weak Authentication, Configuration Weakness
	Software Licenses and Operational Service	Availability	Loss of Avail.	Weak Authentication
	Media	Integrity	Call Quality Degradation / Loss of Avail.	DoS Attack
	Signalling	Integrity	Interception	Eavesdropping
	Management	Integrity	Interception	Eavesdropping
System Asset	**Informational Asset**	**Most Critical Security Req**	**Most Critical Impact**	**Most Likely Threat-Vulnerabilities**
Element Manager	Operating System	Integrity	Modification	Malicious Code, Traditionnel Data Exploits
	Configuration and Management	Availability	Unauthorized Access	Weak Authentication

2

1

System Asset	Informational Asset	Most Critical Security Req	Most Critical Impact	Most Likely Threat-Vulnerabilities
Network (i.e., router, switch, firewall, VPN, IPS)	Operating System	Integrity	Modification	Traditional Data Exploits
	Media	Integrity	Call Quality Degradation / Loss of Avail.	DoS Attack
	Signalling	Integrity	Interception	Eavesdropping
	Management	Integrity	Interception	Eavesdropping
System Asset	**Informational Asset**	**Most Critical Security Req**	**Most Critical Impact**	**Most Likely Threat-Vulnerabilities**
DNS, DHCP, TFTP, RADIUS	Operating System	Integrity	Modification	Malicious Code, Traditionnel Data Exploits
	User Identification (i.e., IP Address)	Integrity	Compromise, Loss of Avail	Configuration Weakness, Malicious Code, DoS
	User Profiles	Integrity	Compromise	Weak Authentication, Configuration Weakness
	Configurations (i.e., Phones)	Integrity	Compromise	Weak Authentication, Configuration Weakness

2 *Table 5.7 Most Critical Impact and Mostly Likely Threat Vulnerabilities*

3

Security Controls To Mitigate Threats and Vulnerabilities

Organizations can perform frequent security risk assessments and implement a defense-in-depth security strategy of security controls and countermeasures to prevent, protect and mitigate against threats and vulnerabilities. However the risk remains for a malicious actor to gain access to the network and successfully initiate an attack against the VoIP service infrastructure. As a result, security must be viewed as an ongoing process of security audits, identification of new threats and vulnerabilities, testing, hardware and software upgrades, and implementation of new security mitigation controls.

This section provides a high level overview of typical security controls and countermeasures to protect the VoIP Reference Architecture from threats and vulnerabilities identified earlier in the document.

The following highlights common classifications of security controls applicable to VoIP:

Hardening of Operating System / Firmware – securing the operating system / firmware including configuration files for all elements of a VoIP service infrastructure. Disable all unnecessary services and ports which are not required for the device. Required services to be bound to specific interface, and not unnecessary interfaces. Logging should be enabled. It is recommended to use secure protocols which encrypt the payload. Host based intrusion detection, anti-virus, malware protection are recommended. Other mitigation techniques include up-to-date patches installed on the device.

Strong Authentication – the process to identify an individual, message, device or information as authentic and not altered or forged. Simple authentication may be performed using a username and password however this common method provides a weak form of identity. Basic and message digest authentication using MD5 checksum defined for HTTP and SIP are also considered weak methods of authentication. Digital certificates, as defined in ITU X.509 standard, may be used to establish the validity of a message or device. Public Key Infrastructure (PKI) is a well known trusted method to create, manage, store, distribute and revoke certificates. Unilateral authentication occurs when the server is authenticated but not the client, whereas bilateral (or mutual) authentication occurs when both parties of the session (or conversation) are authenticated. Transport Layer Security (TLS) using digital certificates is considered as a strong authentication mechanism for signalling and management. And Secure RTP (SRTP) using digital certifications is considered a strong authentication mechanism for delivery of media. Other forms of authentication such as Secure Shell version 2 (SSHv2) and one-time password tokens are also used for authentication of management sessions.

Access Control in the context of this document refers to a software element which provides a controlled access to resources. Physical devices such as firewalls, intrusion prevention system or routers employed with Access Control Lists (ACLs) are typically used to restrict access based on IP addresses and TCP/UDP ports. Capabilities such as packet filtering, deep packet inspection, white- and black listing are commonly used by these devices. Call Admission Control (CAC) is used to control the number of concurrent calls that may be delivered across the network; typically supported on the Call Controller (or IP PBX).

Authorization – the process to specify access rights to an individual, message, device or information using a defined Role Based Access Control (RBAC) model and adhere to Least Access Principle where access to services, devices and networks is restricted unless otherwise permitted.

Encryption – the process to transform clear or plaintext information into an unreadable format for all users and devices except those possessing the proper credentials. Encryption can protect the confidentiality of the information however additional techniques are required to protect the integrity of the information. It is recommended encryption be performed at the endpoints (i.e., IP phone, media gateway) and not in the network using IPSec tunnels in order to ensure end-to-end integrity and confidentiality. Secure RTP (SRTP) encrypts the RTP and RTCP protocols used to encapsulate media, protecting the media from disclosure, modification and replay. SIP over TLS is used to encrypt the SIP signalling protocol. And the SSL protocol is used to encrypt management protocols such as SSH, SFP, SCP and HTTPS. Encryption of files should be performed to ensure integrity (i.e., configuration, firmware) and privacy of confidential or sensitive data (i.e., call detail records). 168-bit Triple Data Encryption Standard (3DES) or 128-bit Advanced Encryption Standard (AES) typically used for encryption.

Voice and Data Segregation Using VLANs – Virtual LANs are used to segment the network broadcast domains logically across a switched network. Separate VLANs should be used for voice and data traffic to minimize the impact of data leakage on voice traffic. VLANs provide some basic protection against ARP based eavesdropping, denial-of-service, reconnaissance and toll fraud attacks. Use of soft phones violates this security control and thus increases risk of a data originating vulnerability to impact VoIP.

Topology Hiding – assignment of private IP address space (RFC 1918) for the critical VoIP systems to ensure direct access from the Internet is not possible. Typically these privately addressed VoIP systems would be behind a firewall. Network Address Translation (NAT) including NAT Traversal for VoIP is out-of-scope with respect to this document.

Denial of Service Protection – mechanism to block or rate limit packets based on protocol type, IP address, UDP/TCP port or specific application payload content. From a server perspective, the resource processing overhead may be reduced by configuring the SIP server not to process and respond to illegitimate requests with an error code.

Call Pattern Analysis – use of VoIP aware firewall and intrusion detection / prevention software and systems to check for malformed packets with respect to the syntax and semantics, and abnormal traffic patterns which may be considered as a malicious threat. This security control protects against fuzzing and toll fraud.

Monitoring, Logging and Reporting – Monitoring involves real time oversight and analysis of events on systems and networks. Logging is the capture of event data for further review to ensure quality and for the facilitation of incident response. Reporting captures event information and formulates it to assist in compliance, benchmarking, and trend analysis.

Auditing – the use of audit trails to record access, modification, and deletion activities. Auditing must be enabled on the desired devices and the audit logs should be written to a secure location to prevent tampering or destruction.

Patch Management – software patch upgrades to operating systems, firmware and applications used across the VoIP service infrastructure.

Backup and Restore – copies of configurations and critical data should be stored in a secure area, with a copy preferably off-site in the event of a disaster. System and data restoration should be tested periodically to ensure the backup is saving useful data.

Vulnerability Testing – the examination of applications, systems, and networks to identify potential weaknesses which could be exploited by an intruder.

Security Code Review – any new software application or device to be installed in the network should be tested to ensure the software code is free of malicious code and known vulnerabilities.

Table 5.8 below identifies several security controls and countermeasures specific to VoIP devices, applications and traffic content for each vulnerability classification.

Vulnerability	Security Controls / Countermeasures
Configuration Weakness	• Hardening of Operating System / Firmware
Unauthorized Access - Weak Authentication	• Hardening of Operating System / Firmware, • Strong Authentication
Malicious Code	• Anti-malware, Anti-virus, File Integrity Monitoring, • Remove applications not VoIP related to server/appliance
Reconnaissance and Enumeration	• Hardening of Operating System / Firmware, • Restrict local configuration access on phones, • Use secure file transfer protocols (and not TFTP) • Authenticate SIP requests using TLS, • Effective patch management, • Access control using firewall and IPS to detect port scans, black- and whitelisting; apply network base ACLs. • Logical network separation of data and voice using VLANs
Spoofing	• Strong Authentication, • SIP over TLS for signalling, S/MIME • Secure management channel (i.e., SSH/SSL/TLS, IPSec)

1

Vulnerability	Security Controls / Countermeasures
Eavesdropping - Interception	• SIP over TLS for signalling , Secure RTP (SRTP) and ZRTP for media, • SSH/SSL for management, • IPSec tunnels for all traffic content.
Signalling And Media Manipulation	• Authentication of the signalling, • Encryption of the signalling and media,
Fuzzing	• Hardening of the VoIP application with robust SIP parsing capability, • Security Code Reviews, • Ensure vendor of VoIP systems has performed sufficient testing using fuzzing tools (ie. Protos, Codenomicon, SIPp, etc), • Use of a VoIP aware firewall and IPS,
Impersonation	• Strong Mutual Authentication
Man-In-The-Middle Attacks	• Use of 802.1x network port authentication, • Authentication of the signalling, • Encryption of the signalling (SIP over TLS) and media (SRTP, ZRTP), • Logical network separation of data and voice using VLANs, • Detection of ARP poisoning and disable gratuitous ARP

2

3

1

Vulnerability	Security Controls / Countermeasures
Denial-Of-Service Attacks (network, application, OS)	• Hardening of Operating System / Firmware, • Packet filtering, rate limiting, traffic shaping and other QoS across network, • Authentication of SIP requests, • Configure SIP server not to respond to illegitimate requests, • Use of VoIP aware firewall and IPS to detect and block, • Effective patch management to remove flaw / vulnerability, • Ensure DoS mitigation supported natively on VoIP systems,
Theft of Service / Toll Fraud	• Access control on the IP PBX, Call Controller and/or media gateway • Call pattern analysis / deep packet inspection by firewall, IPS
VoIP Spam and Phishing	• Identity Management (of Caller), • Black list of known attackers, • White list of known good addresses/users,
Traditional Data Exploits To Impact Operating System	• Hardening of Operating System / Firmware, • Patch Management and vendor support coordination, • Anti-virus and host based IPS software

2 *Table 5.8 Security Controls and Countermeasures*

3

Table 5.9 summarizes recommended security controls to mitigate threat – vulnerability from the perspective exploitation of the signalling, media and management plane. In general, the same security controls can be applied across the various traffic planes.

Threat – Vulnerability	**Mitigation Techniques Across Traffic Planes**		
	Media	**Signalling / Control**	**Management**
Configuration Weakness	Hardening OS/Firmware	Hardening OS/Firmware	Hardening OS/Firmware
Unauthorized Access - Weak Authentication	Strong Authentication	Strong Authentication	Strong Authentication
Malicious Code	Anti-malware, Anti-Virus	Anti-malware, Anti-Virus	Anti-malware, Anti-Virus
Reconnaissance and Enumeration	Hardening OS/Firmware Firewall, ACLs	Hardening OS/Firmware Firewall, ACLs, SIP over TLS	Hardening OS/Firmware Firewall, ACLs, Secure mgmt channel
Spoofing	Secure RTP	SIP over TLS	Secure mgmt channel
Eavesdropping	Secure RTP	SIP over TLS	Secure mgmt channel
Signalling And Media Manipulation	Strong Authentication, Encryption	Strong Authentication, Encryption	Strong Authentication, Encryption
Fuzzing	VoIP aware firewall	VoIP aware firewall, Security code reviews with vulnerability testing	OS / Firmware Hardening

Threat – Vulnerability	Mitigation Techniques Across Traffic Planes		
	Media	**Signalling / Control**	**Management**
Impersonation	Strong Authentication	Strong Authentication	Strong Authentication
Man-In-The-Middle Attacks	Strong Authentication, Encryption	Strong Authentication, Encryption	Strong Authentication, Encryption
Denial-Of-Service Attacks	Network based mitigation	Network based mitigation	
Toll Fraud	Strong Authentication	Strong Authentication	Strong Authentication
VoIP Spam And Phishing	N/A	Blacklisting	Blacklisting
Traditional Data Exploits To Impact Operating System	OS Hardening, Patch Management	OS Hardening, Patch Management	OS Hardening, Patch Management

Table 5.9 Mitigation Techniques Applied Across Traffic Planes

Based on the results formulated in table 5-7 depicting the most critical impact – most likely threat vulnerabilities for each asset, table 5-10 identifies recommended security controls to protect and mitigate against them. This is not an exhaustive list of security controls and countermeasures to implement for each asset, but simply a general set of controls in support of the VoIP Reference Architecture.

1

System Asset	Informational Asset	Most Likely Threat-Vulnerabilities	Security Controls - Mitigation
IP Phone Handset	Operating System	Enumeration	OS/Firmware Hardening
	Configuration	Weak Authentication	Strong Authentication and Identity Management
	Media	DoS Attack	OS/Firmware Hardening
	Signalling	Eavesdropping	SIP over TLS
	Management	Eavesdropping	Secure mgmt channel
System Asset	**Informational Asset**	**Most Likely Threat-Vulnerabilities**	**Security Controls - Mitigation**
Desktop	Operating System	Malicious Code, Enumeration	OS/Firmware Hardening
	VoIP Application (i.e., Soft phone)	Configuration Weakness	Strong Authentication and Identity Management
	Media	DoS Attack	OS/Firmware Hardening
	Signalling	Eavesdropping	SIP over TLS
	Management	Weak Authentication	Secure mgmt channel

2

1

System Asset	Informational Asset	Most Likely Threat-Vulnerabilities	Security Controls - Mitigation
Call Controller and Media Gateway (or IP PBX)	Operating System	Enumeration	OS/Firmware Hardening
	Configuration	Configuration Weakness	Strong Authentication and Identity Management
	Dial Plan	Theft of Service / Toll Fraud	Strong Authentication and Identity Management
	Call Detail Records (and Billing Info)	Weak Authentication, Configuration Weakness	Strong Authentication and Identity Management
	Software Licenses	DoS Attacks	DoS Mitigation
	Media	DoS Attack	OS/Firmware Hardening, Network based DoS Mitigation
	Signalling	Eavesdropping and Impersonation	SIP over TLS
	Management	Weak Authentication	Secure mgmt channel
System Asset	**Informational Asset**	**Most Likely Threat-Vulnerabilities**	**Security Controls - Mitigation**
Element Manager	Operating System	Malicious Code, Enumeration	OS/Firmware Hardening
	Configuration and Management	Weak Authentication	Strong Authentication , Secure mgmt channel

2

System Asset	Informational Asset	Most Likely Threat-Vulnerabilities	Security Controls - Mitigation
Network (i.e., router, switch, firewall, VPN, IPS)	OS / Firmware	Enumeration	OS/Firmware Hardening
	Signalling	Eavesdropping	Encryption
	Media	DoS Attack	DoS Mitigation
	Management	Eavesdropping	Encryption
System Asset	**Informational Asset**	**Most Likely Threat-Vulnerabilities**	**Security Controls - Mitigation**
DNS, DHCP, TFTP, RADIUS	Operating System	Malicious Code, Enumeration	OS/Firmware Hardening
	User Identification (i.e., IP Address)	DoS Attacks (i.e., DHCP exhaustion)	DoS Mitigation
	User Profiles	Weak Authentication, Configuration Weakness	Strong Authentication and Identity Management
	Configurations (i.e., Phones)	Weak Authentication, Configuration Weakness	Strong Authentication and Identity Management

Table 5.10 Mitigation Techniques For Most Likely Threat Vulnerabilities

Summary

A security risk assessment can be a very lengthy, detailed process that may require several iterations before the organization is ready to implement the necessary security controls to protect its operations, assets and overall voice services. Section 5 is meant to provide an understanding of how to develop a security risk assessment (or threat risk analysis) for a VoIP deployment. The assessment developed in this section will be used in Section 6 to establish a security checklist for the VoIP Reference Architecture that can be translated into a Security Content Automation Protocol (SCAP) benchmark.

Chapter 6 - VoIP Security Checklist and Mapping to SP 800-53 R3

Purpose

The purpose of this section is to establish a high level security checklist for the VoIP solution described previously in this document. The intent is not to produce a vendor specific set of requirements, such as that appropriate for *system-specific controls* or *hybrid controls*[1], but rather to specify a minimum set of security requirements for a generic VoIP solution.

"Security controls not designated as common controls are considered *system-specific controls* or *hybrid controls*. System-specific controls are the primary responsibility of information system owners and their respective authorizing officials. Organizations assign a *hybrid* status to a security control when one part of the control is deemed to be common and another part of the control is deemed to be system-specific."

This minimum set of security requirements could then be used by a VoIP solution provider to create a vendor specific lower level security checklist, consistent with the system-specific control guidance in SP 800-53-R3, that can be translated into a tailored, hybrid set of controls consistent with the framework set forth in the Security Content Automation Protocol (SCAP) benchmark

Checklist

A security checklist is a prose description of the steps that are required to be taken to configure a product to ensure that it is operating in a secure manner. This is generally known as a "hardening" of a product into a secure configuration appropriate for that product.

The VoIP security checklist will be written according to the specifications of the NIST Special Publication 800-70-R1 National Checklist Program for IT Products – Guidelines for Checklist Users and Developers. The National Checklist Program (NCP) is a NIST program that hosts product security checklists. These are intended to be used to develop SCAP content (i.e. data streams) that can be used by SCAP validated tools to verify the product configuration).

[1] NIST Special Publication (SP) 800-53-R3, August 2009, paragraph 2.3 Common Controls, page 11.

SCAP

The Security Content Automation Protocol (SCAP) program is a NIST validation program that allows scanning tools to be validated using SCAP content. These tools are then used to scan products to verify that they are in the security configuration designated by the checklist. SCAP uses a set of six open standards working together to standardize a method of determining a product's configuration settings and vulnerability / patch status. The US federal government requires that every agency use an SCAP validated tool to show FISMA compliance. Currently, the focus of SCAP is the Federal Desktop Core Configuration (FDCC) requirements for Microsoft XP and Vista platforms as prescribed by the Office of Management and Budget (OMB). Because FAR 38 requiring the use of NCP checklists was published in March 2008, the need for SCAP data streams for each product has intensified. The ultimate goal of this section is to demonstrate that SCAP data stream(s) can be written, and further refined through appropriate tailoring as indicated, for a VoIP solution.

SCAP data streams are usually developed on a product basis. One challenge for the VoIP solution is to determine a security checklist for what is essentially a system. This is not unlike a certification and authorization activity. A second challenge is to ensure that this baseline security is generic enough and extensible enough to allow both differences in solution types and innovations in future solutions. The SCAP baseline security checklist is not presently based on a specific set of standards, but rather on industry best-practices. There are other initiatives that are incorporating VoIP solutions (e.g. DISA for use in the DoD) for which this baseline checklist can be used. Specific solutions and/or requirements are not within scope of this paper, but it is intended to provide a generic VoIP solution and can be modified to suit other system-specific controls that are more appropriate for diverging VoIP vendor proprietary solutions, and reflect areas where more convergence in future products would accomplish the goal of building-in security by commercial interests. The checklist will then be able to enhance designed-in security while allowing each solution provider to focus on the converging solution strategies that they agree will afford the capability to achieve the SCAP goals over time, with attendant refinements in their product as well as through the establishment of verifiable and measurable checklist compliance tools that fit suit each vendor's tailored SCAP approach and solution.

The security checklist incorporates the reference architecture set forth in Section 4 of this paper. The architecture is discussed here in terms of subsystems that provide specific security functionality. The environment is also briefly discussed in the following paragraphs. The purpose of the threat scenario description is to identify threats that need to be countered or mitigated to ensure a secure configuration of the VoIP solution. The mitigations, or controls, are then mapped to the controls found in the NIST SP 800-53-R3 Security Controls.

VoIP Solution Architecture and Subsystems

The reference architecture, upon which the security checklist is based, is vendor agnostic. There will be differences in implementation of protocols, software/firmware/hardware types and specialty features between solutions. The baseline is intended to give a minimum set of requirements for any VoIP solution which the vendor can tailor to suit their unique proprietary solution. This is felt to be a development path that may still afford future reliance upon common controls as the proprietary portions are re-engineered to be interoperable where they are not so today. The benefit encourages standardization growth to be more VoIP solution diverse, yet friendly and mutually inclusive, not exclusive. Through vendor implementations that are initially tolerant of system-specific components, it is hoped that future evolutionary VoIP growth towards common controls will permit them to be better integrated into larger system architectural solutions.

Prior to discussion of the functional subsystems of the VoIP solution, some operational and procedural assumptions are made. This will likely be refined as this endeavour progresses but for this paper the following assumptions are made:

1. The VoIP solution will be integrated into a data network.
2. A VoIP VLAN will be implemented in the solution.
3. Any PC operating systems that fall under the OMB requirement for FDCC compliance will be FDCC compliant and the relevant FDCC SCAP data stream will be used in conjunction with any SCAP data stream derived from this checklist.
4. Vendors using proprietary operating systems in the solution will be required to produce the appropriate checklist and SCAP data stream for the OS. Current FDCC compliant operating systems will be used as a guide for the development of said data streams and these will be used in conjunction with any data streams derived from the VoIP checklist.
5. Since the VoIP solution is integrated into an existing data network, it is assumed that the network will provide appropriate security controls to protect the network.
6. Security checklists require a mapping to relevant standards and this checklist will use the NIST SP 800-53 R3 9(Security Controls) as the standard to which it maps. In the future it is anticipated that the mapping scope will broaden to include other relevant standards.
7. Every security checklist conforming to the NCP requirements must discuss a threat scenario. This checklist is based on the Managed Environment scenario in SP 800-70-R1.The threat scenario is been discussed in depth in section 5 of this paper, and the results of the threat scenario discussion will be used in this section.
8. The Managed Environment scenario must include a discussion on insider threats. This is discussed in section 4 but there is no intention to include any specific procedural mitigation in this checklist though such mitigations are highly advised. Physical security

procedures and protections are not within scope for the security checklist though these are highly advisable.

9. Some well defined components of a VoIP solution are also expected to be manifest as part of a data network, and where these shared converged components are extant it is presumed that they will be "hardened," or at least provisioned with an appropriate level of protection for the most sensitive content of both the data network and the VoIP content borne over the same infrastructure.. These components are neither enumerated nor discussed in the checklist, but they are seen to include such elements as a DNS server, a DHCP server, NTP server, etc. Required security functionality expectations from these data network components are only cited when there are parallel VoIP specific configuration needs that bear consideration and inclusive treatment.

VoIP Subsystems

There are four defined subsystems for the VoIP reference architecture for the purposes of this paper. They are:

1. The Call Controller Subsystem
2. The Element Manager Subsystem
3. The IP Phone Subsystem
4. The SIP Aware Firewall and IPS Subsystem

The purpose of each subsystem will be discussed and the security functionality expected to be provided by the subsystem will be given. This functionality will then be mapped to the security controls in SP 800-53 R3. The intent is to describe what functionality is required without prescribing how it must be implemented. This is left to the individual vendor to make the checklist more granular to suit their specific solution.

The Call Controller Subsystem

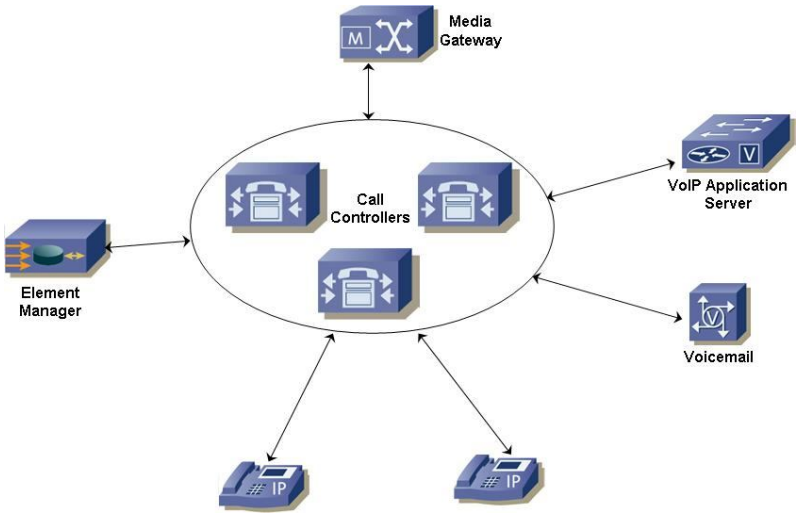


Figure 6.1 – The Call Controller Subsystem.

The Call Controller Subsystem can be further divided into specific functional areas. These have been identified as:

1. Call Controller to IP Phones Functional Area
2. Call Controller to Media Gateway Functional Area
3. Call Controller to Element Manager Functional Area
4. Call Controller to Call Controller Functional Area

It should be noted here that the Call Controller to Voice Mail and Application Server functional areas are out of scope for this document and will not be discussed at this time. Each of the covered functional areas are discussed in terms of the connectivity, purpose and security functionality required by that functional area.

The Call Controller to IP Phones Funtional Area

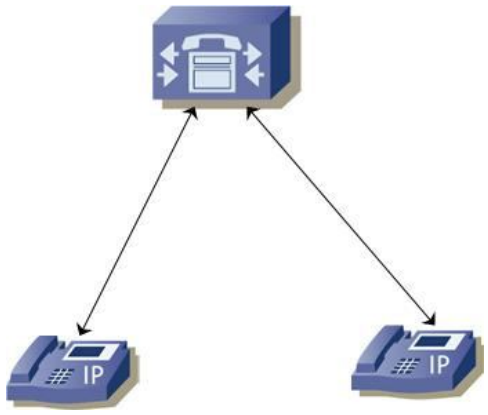


Figure 6.2 – The Call Controller to IP Phones Functional Area

Connectivity of the Functional Area

The Call Controller connects to the IP Phones via the VoIP VLAN and the same physical LAN as the data network.

Purpose of the Functional Area Components

The main purpose of the Call Controller is to handle VoIP SIP signalling such as registering users, keeping track of registered users, users' locations, and establishing and terminating media sessions. The Call Controller also serves as a VoIP media proxy (forwarding RTP/SRTP packets on conference calls and similar functions), allowing users to check call logs and access their contacts, and pushing configuration and firmware files to the IP phones.

Security Functionality Required by the Functional Area

Security functionality specifically required to be implemented in this Functional Area of the Call Controller Subsystem consists of:

1. Endpoint registration
2. Location discovery (DNS)
3. Signalling session establishment and termination management
4. Session and media proxy (voicemail, conferencing)
5. Dial plan management

6. Call admission control
7. Phone firmware management
8. Endpoint configuration management
9. CDR creation

The Call Controller to Media Gateway Functional Area

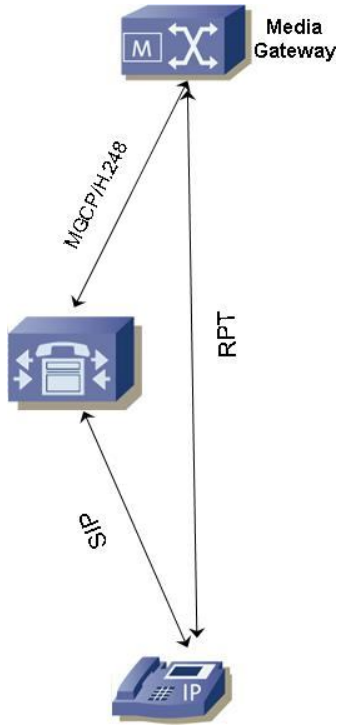


Figure 6.3 - The Call Controller to Media Gateway Functional Area

The Connectivity of the Functional Area

It is anticipated that this will be a physically separated network used to carry MGCP or H.248 messages. It is also anticipated that IPSec will be implemented.

The Purpose of the Functional Area

The main purpose is to handle VoIP signalling using MGCP or H.248 such as establishing and terminating media sessions and keeping track of established sessions.

The Security Functionality Required by the Functional Area

Security functionality specifically required to be implemented in this Functional area of the Call Controller Subsystem consists of:

1. Registration with device and user authentication

2. Location discovery using DNS
3. Session creation and termination management
4. Session and media proxy
5. Call admission control
6. Phone firmware management
7. Dial plan management
8. Management of endpoint configuration
9. PSTN routing
10. Emergency services
11. CDR creation

The Call Controller to Element Manager Functional Area

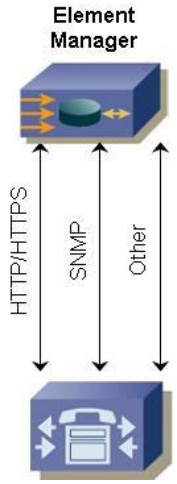


Figure 6.4 - The Call Controller to Element Manager Functional Area

The Connectivity of the Functional Area

It is anticipated that this will be a physically separated network using only local access and requiring the implementation of IPSec and protocols that implement strong authentication and encryption such as HTTPS.

The Purpose of the Functional Area

The main purpose of this functional area of the Call Controller Subsystem is configuration and management of:

1. Users (add, delete, modify)
2. Dial plans (local, long distance, between branches)
3. Performance monitoring
4. Firmware updates and patches management
5. Phone configuration management

6. Backup and restore

The Security Functions Required by the Functional Area

Security functionality specifically required to be implemented in this functional area of the Call Controller Subsystem consists of:

1. Location discovery
2. Session creation and termination management

The Call Controller to Call Controller Functional Area

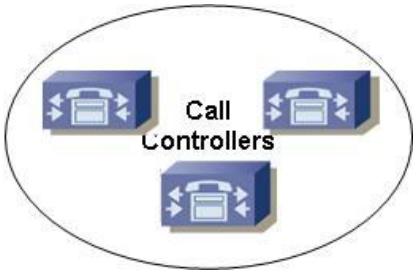


Figure 6.5 - The Call Controller to Call Controller Functional Area

The Connectivity of the Functional Area

It is anticipated that this will be physically separated networks requiring the implementation of IPSec and protocols that implement strong authentication and encryption such as HTTPS.

The Purpose of the Functional Area

The main purpose of this functional are of the Call Controller Subsystem is to provide redundancy, load balancing and inter-branch communication.

The Security Functionality Required by the Functional Area

Security functionality specifically required to be implemented in this functional area of the Call Controller Subsystem consists of:

1. Authentication of Call Controller
2. Location discovery
3. Session creation and termination management

The Element Manager Subsystem

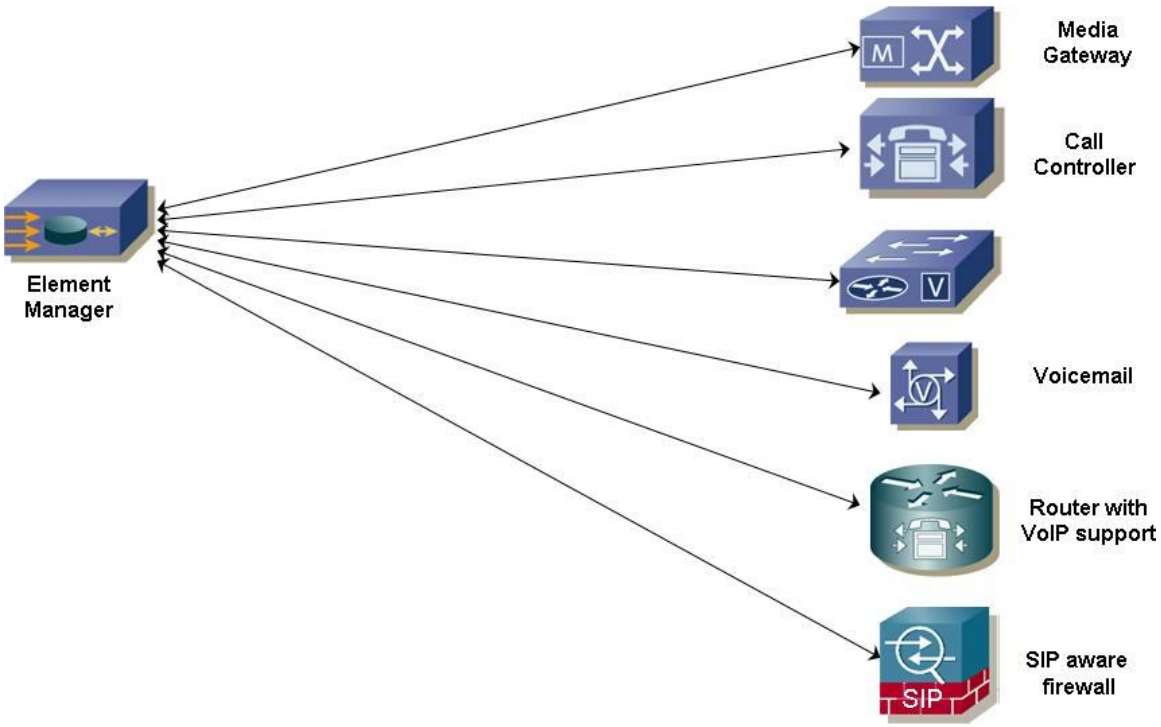


Figure 6.6 – The Element Manager Subsystem

The Element Manager Subsystem usually consists of a graphical configuration tool that helps to simplify or streamline the management and provisioning processes for different types of devices such as gateways, firewalls and Call Controllers.

The Connectivity of the Subsystem

It is anticipated that this will be a physically separated network using local access only and requiring the implementation of IPSec and protocols that implement strong authentication and encryption such as HTTPS.

The Purpose of the Subsystem

The main purpose of the Element Manager Subsystem is configuration and management of:

1. Users (add, delete, modify)
2. Performance monitoring
3. Firmware updates and patches management
4. Device specific features configuration
5. Backup and restore

The Security Functions Required by the Subsystem

Security functionality specifically required to be implemented in the Element Manager Subsystem consists of:

1. Strong authentication for administrators
2. Authorization
3. Encryption and integrity
4. Confidentiality

The IP Phone Subsystem

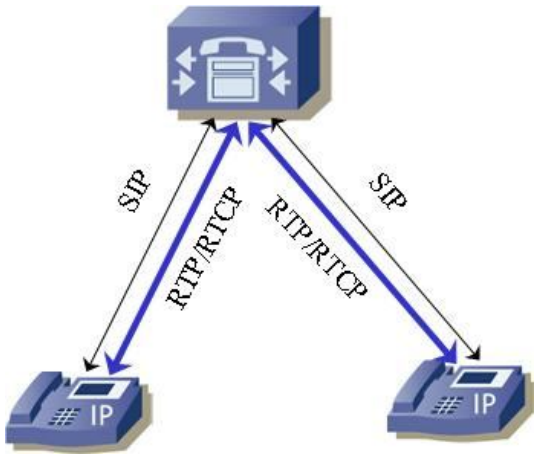


Figure 6.7 – The IP Phones Subsystem

The IP Phone Subsystem can be further divided into specific functional areas. These have been identified as:

1. The IP Phone to Call Controller Functional Area
2. The IP Phone to Media Gateway Functional Area
3. The IP Phone to IP Phone Functional Area
4. The IP Phone to User Functions Functional Area

The IP Phone to Call Controller Functional Area

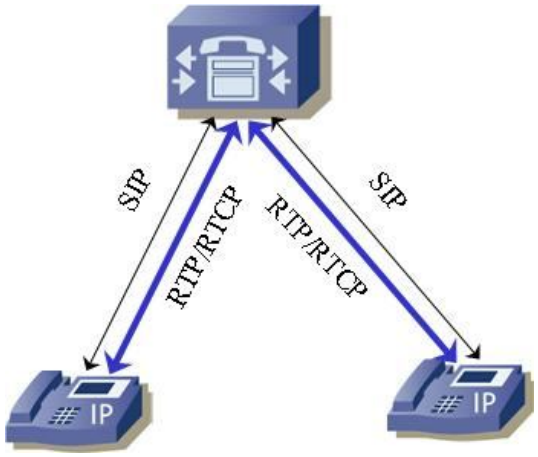


Figure 6.8 – The IP Phones to Call Controller Functional Area

The Connectivity of the Functional Area

The IP phone has connectivity to the VoIP VLAN and the same physical LAN as the data network.

The Purpose of the Functional Area

The main purpose of this functional area of the IP Phone Subsystem is to handle VoIP SIP signalling such as registering with the Call Controller, providing an IP address and port to receive messages, and initiating, establishing and terminating media sessions (i.e. make call, receive call and terminate call). Other purposes are to get configuration updates from the Call Controller, get firmware updates from the Call Controller, and exchange RTP/RTCP packets in the case of conference calling.

The Security Functions Required by the Functional Area

Security functionality specifically required to be implemented in this functional area of the IP Phone Subsystem consists of:

1. Authentication of phone to Call Controller
2. Authorization of SIP requests
3. Encryption and Integrity
4. Access Control

The IP Phone to Media Gateway Functional Area

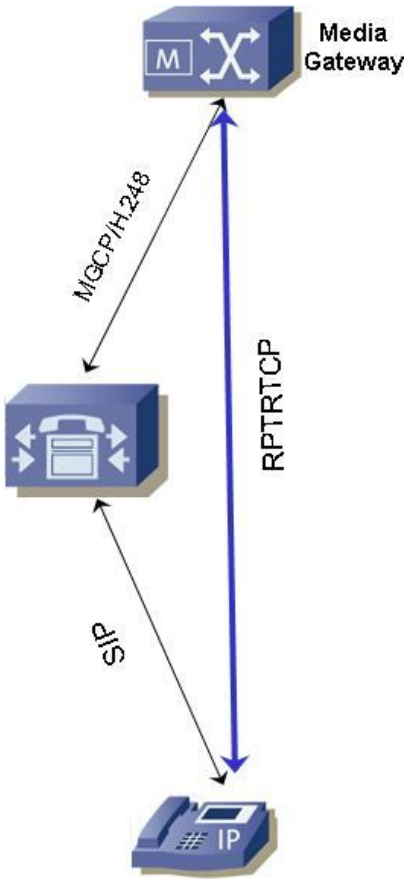


Figure 6.9 - The IP Phone to Media Gateway Functional Area

The Connectivity of the Functional Area

This functional area of the IP Phone Subsystem has connectivity to the VoIP VLAN and the data network.

The Purpose of the Functional Area

The main purpose of this functional area of the IP Phone Subsystem is to handle RTP and RTCP packets for external calls.

The Security Functions Required by the Functional Area

Security functionality specifically required to be implemented in this element of the IP Phone Subsystem consists of:

1. Availability; and,
2. Confidentiality by RTP encryption (if used)

The IP Phone to IP Phone Functional Area

Figure 6.10 - The IP Phone to IP Phone Functional Area

The Connectivity of the Functional Area

This functional are of the IP Phone Subsystem has connectivity to the VoIP VLAN and the data network.

The Purpose of the Functional Area

The main purpose of this element of the IP Phone Subsystem is to handle a media session by receiving and decoding RTP packets, encoding and sending RTP packets, and handling RTP control messages.

The Security Functions Required by the Functional Area

Security functionality specifically required to be implemented in this functional area of the IP Phone Subsystem consists of:

Confidentiality by RTP encryption

The IP Phone to User Functional Area

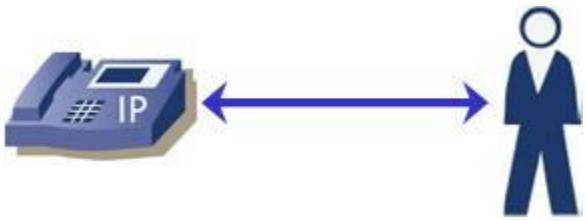


Figure 6.11 - The IP Phone to User Functional Area

The Connectivity of the Functional Area

This functional area of the IP Phone Subsystem has connectivity to the same physical data network and also has a manual aspect.

The Purpose of the Functional Area

The main purpose of this functional are of the IP Phone Subsystem is configuration and usage of the IP phone such as reconfiguring the phone using special key combinations, making and receiving calls, and remote management using HTTPS for reconfiguration of the phone.

The Security Function Requirements of the Functional Area

Security functionality specifically required to be implemented in this functional area of the IP Phone Subsystem consists of:

Confidentiality by RTP encryption

The SIP Aware Firewall and VoIP IPS Subsystem

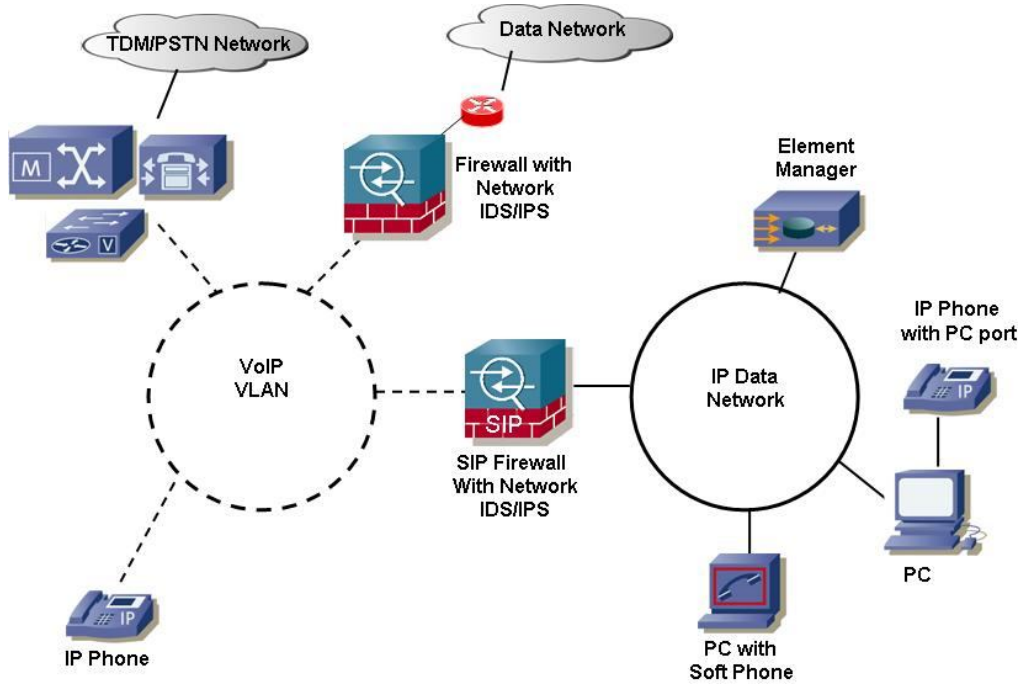


Figure 6.12 -- The SIP Aware Firewall and VoIP IPS Subsystem

Firewall and IPS are inline devices that take place in the network, sometimes run on one appliance, however, the purposes are different. The SIP Aware Firewall and VoIP IPS Subsystem can be further divided into specific functional areas. These have been identified as:

1. The SIP Aware Firewall Inline Operation Functional Area
2. IDS/IPS Inline Operation Functional Area
3. IP Aware Firewall and IPS Management Functional Area

The SIP Aware Firewall Inline Operation Functional Area

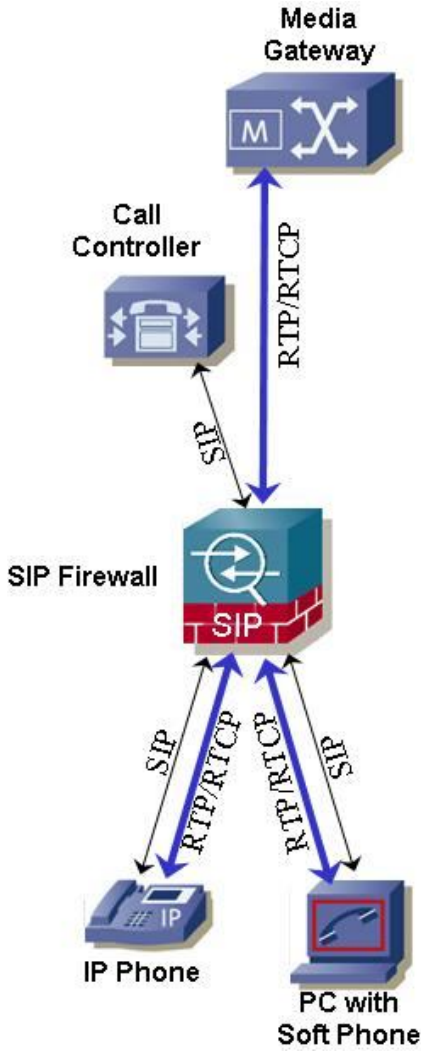


Figure 6.13 -- The SIP Aware Firewall Inline Operation Functional Area

The Connectivity of the Functional Area

The SIP aware firewall is inline between the data network and the VoIP VLAN.

The Purpose of the Functional Area

The main purpose of this functional area of the SIP Aware Firewall and VoIP IPS Subsystem is to provide firewall functionality. The firewall opens “pinholes” for RTP/RTCP packets based on SIP signalling. The firewall provides stateful SIP signalling inspection, closes all unnecessary ports and opens dynamic RTP/RTCP ports.

The Security Function Requirements of the Functional Area

Security functionality specifically required to be implemented in this functional area of the SIP Aware Firewall and VoIP IPS Subsystem consists of:

1. Security Audit
2. Non-repudiation

The IDS/IPS Inline Operation Functional Area

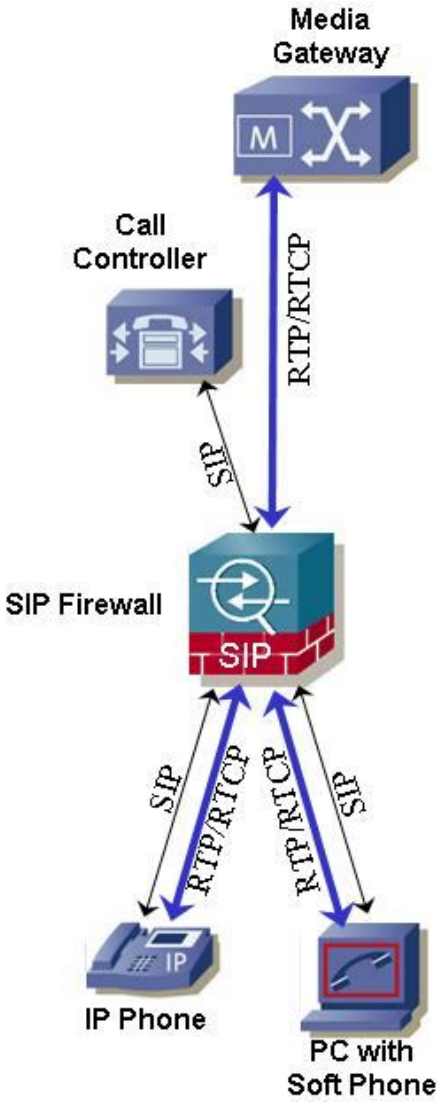


Figure 6.14 -- The IDS/IPS Inline Operation Functional Area

The Connectivity of the Functional Area

The IDS/IPS is inline between the data network and the VoIP VLAN.

The Purpose of the Functional Area

The main purpose of this funcational area of the SIP Aware Firewall and VoIP IPS Subsystem is to provide IPS/IDS functionality. The IDS/IPS detects and prevents attacks on the VoIP server components by performing malicious attack detection, known attacks detection, behavior based anomalies detection, SPIT detection, and DoS prevention.

The Security Function Requirements of the Functional Area

Security functionality specifically required to be implemented in this functional area of the SIP Aware Firewall and VoIP IPS Subsystem consists of:

1. Security Audit
2. Availability
3. Non-repudiation

The SIP Aware Firewall and IPS Management Functional Area

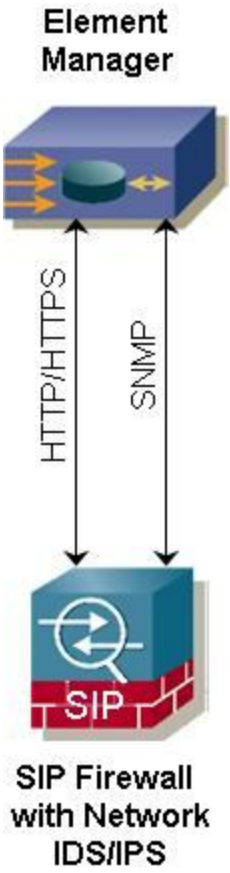


Figure 6.15 - The SIP Aware Firewall and IPS Management Functional Area

The Connectivity of the Functional Area

It is anticipated that there will be physical network separation (i.e. using only local access), implementing IPSec, and using strong authentication and encryption protocols such as HTTPS.

The Purpose of the Functional Area

The main purpose of this functional are of the SIP Aware Firewall and VoIP IPS Subsystem is configuration and management of the firewall, performance monitoring, and firmware updates and patches.

The Security Function Requirements of the Functional Area

Security functionality specifically required to be implemented in this functional are of the SIP Aware Firewall and VoIP IPS Subsystem consists of:

1. Security Audit
2. Authentication of administrators and users
3. Authorization

Mapping of Functionality to SP 800-53 R3 Controls

Having determined the essential security functionality for the checklist, the appropriate controls to be implemented can be determined and matched to the security functionality provided by the VoIP solution.

Call Controller Subsystem **Call Controller to IP Phones**				
Security Function	**SP 800-53 R3 Control**	**Low**	**Moderate**	**High**
Endpoint registration	AC-2	AC-2	AC-2 (1), (2), (3), (4), (5), (6)	AC-2 (1), (2), (3), (4), (5), (6)
	AC-3	AC-3	AC-3	AC-3
	AC-4	AC-4	AC-4	AC-4
	AC-7	AC-7	AC-7	AC-7
	AC-10	AC-10	AC-10	AC-10
		Not selected	Not selected	
	AC-11	AC-11	AC-11	AC-11
		Not selected		
	AU-8	AU-8	AU-8 (1)	AU-8 (1)
	AU-9	AU-9	AU-9	AU-9
	AU-10	AU-10	AU-10	AU-10
		Not Selected	Not Selected	
	AU-12	AU-12	AU-12	AU-12 (1)

	IA-2	IA-2 (1)	IA-2 (2)	IA-2 (3)
	IA-3	IA-3	IA-3	IA-3
		Not Selected		
	IA-6	IA-6	IA-6	IA-6
	IA-8	IA-8	IA-8	IA-8
	SI-7	SI-7	SI-7	SI-7 (1), (2)
		Not Selected	Not Selected	
	SI-11	SI-11	SI-11	SI-11
		Not Selected		
	SC-8	SC-8	SC-8 (1)	SC-8 (1)
		Not Selected		
	SC-9	SC-9	SC-9 (1)	SC-9 (1)
		Not Selected		
	SC-10	SC-10	SC-10	SC-10
		Not Selected		
	SC-23	SC-23	SC-23	SC-23
		Not Selected		
Location discovery (DNS)	SC-20	SC-20 (1)	SC-20 (1)	SC-20 (1)
	SC-21	SC-21	Not selected	SC-21
		Not selected		
Signalling	SC-8	SC-8	SC-8 (1)	SC-8 (1)

session establishment and termination management		Not Selected		
	SC-9	SC-9	SC-9 (1)	SC-9 (1)
		Not Selected		
	SC-10	SC-10	SC-10	SC-10
		Not Selected		
Session and media proxy (voicemail, conferencing)	SC-8	SC-8	SC-8 (1)	SC-8 (1)
		Not Selected		
	SC-9	SC-9	SC-9 (1)	SC-9 (1)
		Not Selected		
	SC-10	SC-10	SC-10	SC-10
		Not Selected		
Dial plan management	SI-7	SI-7	SI-7	SI-7 (1), (2)
		Not Selected	Not Selected	
	SI-10	SI-10	SI-10	SI-10
		Not Selected		
	SI-11	SI-11	SI-11	SI-11
		Not Selected		
	SC-28	SC-28	SC-28	SC-28
Call admission control	AU-8	AU-8	AU-8 (1)	AU-8 (1)
	AU-9	AU-9	AU-9	AU-9
	AU-12	AU-12	AU-12	AU-12 (1)

Phone firmware management	SI-7	SI-7 Not Selected	Not Selected	SI-7 (1), (2)
	SI-10	SI-10 Not Selected	SI-10	SI-10
	SI-11	SI-11 Not Selected	SI-11	SI-11
	SC-23	SC-23 Not Selected	SC-23	SC-23
Endpoint configuration management	SI-7	SI-7 Not Selected	Not Selected	SI-7 (1), (2)
	SI-10	SI-10 Not Selected	SI-10	SI-10
	SI-11	SI-11 Not Selected	SI-11	SI-11
	SC-23	SC-23 Not Selected	SC-23	SC-23
CDR creation	SC-28	SC-28	SC-28	SC-28

Table 6.1a

1

Call Controller Subsystem				
Call Controller to Media Gateway				
Security Function	**SP 800-53 R3 Control**	**Low**	**Moderate**	**High**
Registration with device / user authentication	AC-2	AC-2	AC-2 (1), (2), (3), (4), (5), (6)	AC-2 (1), (2), (3), (4), (5), (6)
	AC-3	AC-3	AC-3	AC-3
	AC-4	AC-4	AC-4	AC-4
	AC-7	AC-7	AC-7	AC-7
	AC-10	AC-10 Not selected	AC-10 Not selected	AC-10
	AC-11	AC-11 Not selected	AC-11	AC-11
	AU-8	AU-8	AU-8 (1)	AU-8 (1)
	AU-9	AU-9	AU-9	AU-9
	AU-12	AU-12	AU-12	AU-12 (1)
	AU-12	AU-12	AU-12	AU-12 (1)
	IA-2	IA-2 (1)	IA-2 (2)	IA-2 (3)
	IA-3	IA-3 Not Selected	IA-3	IA-3
	IA-6	IA-6	IA-6	IA-6
	IA-8	IA-8	IA-8	IA-8

	SI-7	SI-7 Not Selected	SI-7 Not Selected	SI-7 (1), (2)
	SI-11	SI-11 Not Selected	SI-11	SI-11
	SC-8	SC-8 Not Selected	SC-8 (1)	SC-8 (1)
	SC-9	SC-9 Not Selected	SC-9 (1)	SC-9 (1)
	SC-10	SC-10 Not Selected	SC-10	SC-10
	SC-23	SC-23 Not Selected	SC-23	SC-23
Location discovery using DNS	SC-20	SC-20 (1)	SC-20 (1)	SC-20 (1)
	SC-21	SC-21 Not selected	SC-21 Not selected	SC-21
Session creation and termination management	SC-8	SC-8 Not Selected	SC-8 (1)	SC-8 (1)
	SC-9	SC-9 Not Selected	SC-9 (1)	SC-9 (1)
	SC-10	SC-10	SC-10	SC-10

		Not Selected		
Session and media proxy	SC-8	SC-8 Not Selected	SC-8 (1)	SC-8 (1)
	SC-9	SC-9 Not Selected	SC-9 (1)	SC-9 (1)
	SC-10	SC-10 Not Selected	SC-10	SC-10
Call admission control	AU-8	AU-8	AU-8 (1)	AU-8 (1)
	AU-9	AU-9	AU-9	AU-9
	AU-12	AU-12	AU-12	AU-12 (1)
Phone firmware management	SI-7	SI-7 Not Selected	Not Selected	SI-7 (1), (2)
	SI-10	SI-10 Not Selected	SI-10	SI-10
	SI-11	SI-11 Not Selected	SI-11	SI-11
Dial plan management	SI-7	SI-7 Not Selected	SI-7 Not Selected	SI-7 (1), (2)
	SI-10	SI-10 Not Selected	SI-10	SI-10

	SI-11	SI-11 Not Selected	SI-11	SI-11
Management of endpoint configuration	SI-7	SI-7 Not Selected	Not Selected	SI-7 (1), (2)
	SI-10	SI-10 Not Selected	SI-10	SI-10
	SI-11	SI-11 Not Selected	SI-11	SI-11
	SC-28	SC-28	SC-28	SC-28
PSTN routing	SI-7	SI-7 Not Selected	SI-7 Not Selected	SI-7 (1), (2)
	SI-10	SI-10 Not Selected	SI-10	SI-10
	SI-11	SI-11 Not Selected	SI-11	SI-11
Emergency services				
CDR creation	SC-28	SC-28	SC-28	SC-28

Table 6.1b

1

Call Controller Subsystem				
Call Controller to Element Manager				
Security Function	**SP 800-53 R3 Control**	**Low**	**Moderate**	**High**
Location discovery	SC-20	SC-20 (1)	SC-20 (1)	SC-20 (1)
	SC-21	SC-21 Not selected	SC-21 Not selected	SC-21
Session creation and termination management	SC-8	SC-8 Not Selected	SC-8 (1)	SC-8 (1)
	SC-9	SC-9 Not Selected	SC-9 (1)	SC-9 (1)
	SC-10	SC-10 Not Selected	SC-10	SC-10

2 *Table 6.1c*

Call Controller Subsystem				
Call Controller to Call Controller				
Security Function	**SP 800-53 R3 Control**	**Low**	**Moderate**	**High**
Authentication of Call Controller	AC-2	AC-2	AC-2 (1), (2), (3), (4), (5), (6)	AC-2 (1), (2), (3), (4), (5), (6)
	AC-3	AC-3	AC-3	AC-3
	AC-4	AC-4	AC-4	AC-4
	AC-7	AC-7	AC-7	AC-7
	AC-10	AC-10	AC-10	AC-10

		Not selected	Not selected	
	AC-11	AC-11 Not selected	AC-11	AC-11
	AU-8	AU-8	AU-8 (1)	AU-8 (1)
	AU-9	AU-9	AU-9	AU-9
	AU-12	AU-12	AU-12	AU-12 (1)
	AU-12	AU-12	AU-12	AU-12 (1)
	IA-2	IA-2 (1)	IA-2 (2)	IA-2 (3)
	IA-3	IA-3 Not Selected	IA-3	IA-3
	IA-6	IA-6	IA-6	IA-6
	IA-8	IA-8	IA-8	IA-8
	SI-7	SI-7 Not Selected	SI-7 Not Selected	SI-7 (1), (2)
	SI-11	SI-11 Not Selected	SI-11	SI-11
	SC-8	SC-8 Not Selected	SC-8 (1)	SC-8 (1)
	SC-9	SC-9 Not Selected	SC-9 (1)	SC-9 (1)

	SC-10	SC-10 Not Selected	SC-10	SC-10
	SC-23	SC-23 Not Selected	SC-23	SC-23
Location discovery	SC-20	SC-20 (1)	SC-20 (1)	SC-20 (1)
	SC-21	SC-21 Not selected	SC-21 Not selected	SC-21
Session creation and termination management	SC-8	SC-8 Not Selected	SC-8 (1)	SC-8 (1)
	SC-9	SC-9 Not Selected	SC-9 (1)	SC-9 (1)
	SC-10	SC-10 Not Selected	SC-10	SC-10

Table 6.1d

Element Manager Subsystem				
Security Function	**SP 800-53 R3 Control**	**Low**	**Moderate**	**High**
Strong authentication for administrators	IA-2	IA-2 (1)	IA-2 (2)	IA-2 (3)
	IA-3	IA-3 Not Selected	IA-3	IA-3
	IA-6	IA-6	IA-6	IA-6
	IA-8	IA-8	IA-8	IA-8

Authorization	AC-2	AC-2	AC-2 (1), (2), (3), (4), (5), (6)	AC-2 (1), (2), (3), (4), (5), (6)
	AC-3	AC-3	AC-3	AC-3
	AC-4	AC-4	AC-4	AC-4
	SI-7	SI-7 Not Selected	SI-7 Not Selected	SI-7 (1), (2)
	SI-10	SI-10 Not Selected	SI-10	SI-10
	SI-11	SI-11 Not Selected	SI-11	SI-11
Encryption and integrity	SC-8	SC-8 Not Selected	SC-8 (1)	SC-8 (1)
	SC-9	SC-9 Not Selected	SC-9 (1)	SC-9 (1)
	SC-10	SC-10 Not Selected	SC-10	SC-10
Confidentiality	SC-28	SC-28	SC-28	SC-28

Table 6.2

IP Phone Subsystem				
IP Phone to Call Controller				
Security Function	**SP 800-53 R3 Control**	**Low**	**Moderate**	**High**
Authentication of phone to Call Controller	IA-2	IA-2 (1)	IA-2 (2)	IA-2 (3)
	IA-3	IA-3 Not Selected	IA-3	IA-3
	IA-6	IA-6	IA-6	IA-6
	IA-8	IA-8	IA-8	IA-8
Authorization of SIP requests	IA-3	IA-3 Not Selected	IA-3	IA-3
	SI-7	SI-7 Not Selected	SI-7 Not Selected	SI-7 (1), (2)
Encryption and Integrity	SC-8	SC-8 Not Selected	SC-8 (1)	SC-8 (1)
	SC-9	SC-9 Not Selected	SC-9 (1)	SC-9 (1)
	SC-28	SC-28	SC-28	SC-28
Access Control	AC-2	AC-2	AC-2 (1), (2), (3), (4), (5), (6)	AC-2 (1), (2), (3), (4), (5), (6)
	AC-3	AC-3	AC-3	AC-3
	AC-4	AC-4	AC-4	AC-4

Table 6.3a

IP Phone Subsystem				
IP Phone to Media Gateway				
Security Function	**SP 800-53 R3 Control**	**Low**	**Moderate**	**High**
Confidentiality by RTP encryption	SC-8	SC-8 Not Selected	SC-8 (1)	SC-8 (1)
	SC-9	SC-9 Not Selected	SC-9 (1)	SC-9 (1)

Table 6.3b

IP Phone Subsystem				
IP Phone to IP Phone				
Security Function	**SP 800-53 R3 Control**	**Low**	**Moderate**	**High**
Confidentiality - RTP encryption	SC-8	SC-8 Not Selected	SC-8 (1)	SC-8 (1)
	SC-9	SC-9 Not Selected	SC-9 (1)	SC-9 (1)

Table 6.3c

IP Phone Subsystem				
IP Phone to User				
Security Function	**SP 800-53 R3 Control**	**Low**	**Moderate**	**High**
Authentication	IA-2	IA-2 (1)	IA-2 (2)	IA-2 (3)
	IA-3	IA-3 Not Selected	IA-3	IA-3
	IA-6	IA-6	IA-6	IA-6
	IA-8	IA-8	IA-8	IA-8

Table 6.3d

SIP Aware Firewall and VoIP IPS Subsystem				
SIP Aware Firewall Inline Operation				
Security Function	**SP 800-53 R3 Control**	**Low**	**Moderate**	**High**
Security Audit	AU-8	AU-8	AU-8 (1)	AU-8 (1)
	AU-9	AU-9	AU-9	AU-9
	AU-12	AU-12	AU-12	AU-12 (1)
Non-repudiation	AU-10 Not selected	AU-10 Not selected	AU-10 Not selected	AU-10 Not selected

Table 6.4a

SIP Aware Firewall and VoIP IPS Subsystem				
IDS/IPS Inline Operation				
Security Function	**SP 800-53 R3 Control**	**Low**	**Moderate**	**High**
Security Audit	AU-8	AU-8	AU-8 (1)	AU-8 (1)
	AU-9	AU-9	AU-9	AU-9
	AU-12	AU-12	AU-12	AU-12 (1)
Non-repudiation	AU-10 Not selected	AU-10 Not selected	AU-10 Not selected	AU-10 Not selected

Table 6.4b

SIP Aware Firewall and VoIP IPS Subsystem				
SIP Aware Firewall and IPS Management				
Security Function	**SP 800-53 R3 Control**	**Low**	**Moderate**	**High**
Security Audit	AU-8	AU-8	AU-8 (1)	AU-8 (1)
	AU-9	AU-9	AU-9	AU-9
	AU-12	AU-12	AU-12	AU-12 (1)
Authentication of administrators and users	AC-2	AC-2	AC-2 (1), (2), (3), (4), (5), (6)	AC-2 (1), (2), (3), (4), (5), (6)
	AC-3	AC-3	AC-3	AC-3
	AC-4	AC-4	AC-4	AC-4

Authorization	IA-2	IA-2 (1)	IA-2 (2)	IA-2 (3)
	IA-3	IA-3 Not Selected	IA-3	IA-3
	IA-6	IA-6	IA-6	IA-6
	IA-8	IA-8	IA-8	IA-8
	SI-7	SI-7 Not Selected	SI-7 Not Selected	SI-7 (1), (2)
	SI-10	SI-10 Not Selected	SI-10	SI-10
	SI-11	SI-11 Not Selected	SI-11	SI-11
	SC-8	SC-8 Not Selected	SC-8 (1)	SC-8 (1)
	SC-9	SC-9 Not Selected	SC-9 (1)	SC-9 (1)
	SC-10	SC-10 Not Selected	SC-10	SC-10

Table 6.4c

Security Checklist

Each security function can be expressed as a rule or a series of rules that will enforce the security functionality. This leads to the development of an SCAP expressed checklist (in XML) to be used to check and / or verify that the secure configuration is being maintained and used.

The security checklist is strawman at this point. The checklist is intended to be a high level statement of desired controls / mechanisms in any best practices VoIP solution and is not intended to be limiting in any way to a more robust implementation. This is a minimum set of requirements and is intended to be modified by a solution provider to more fully describe a particular solution. It is expected that each rule may be further sub-divided to fully express the specific mechanisms of a particular VoIP solution.

The NIST SP 800-53 R3 controls have been listed for systems that are classified as Low, Moderate and High. For the purposes of this checklist, however, the classification of Low is being used. In some instances, for the Low classification, the SP 800-53 R3 controls specify "Not Selected". In these instances the VoIP checklist is including the minimum control requirement for the Low classification. Otherwise, the control set is applied as indicated in SP 800-53 R3.

Rules for The Call Controller Subsystem

AC-2 Call Controller account management

Rule CC-1: Verify Call Controller (type, version and any other unique identifier)

Rule CC-2: Verify that administrator account exists, is valid and has valid credentials and access to other account types.

Rule CC-3: Verify user accounts are maintained according to policy.

Rule CC-4: Verify only authorized endpoints can be registered.

AC-3 Access control enforcement

Rule CC-5a: Verify local access control policy (rule set) is implemented in Call Controller.

Rule CC-5b: Verify remote access control policy implemented in Call Controller.

AC-4 Information flow enforcement

Rule CC-6a: Verify Call Controller only allows authorized endpoint to communicate with itself.

Rule CC-6b: Verify Call Controller only allows authorized media gateway to communicate with itself.

Rule CC-6c: Verify Call Controller only allows an authorized Call Controller to communicate with itself.

Rule CC-6d: Verify Call Controller only allows an authorized PSTN to communicate with itself.

Rule CC-7a: Verify Call Controller only allows authorized endpoint to communicate with other system components.

Rule CC-7b: Verify Call Controller only allows authorized media gateway to communicate with other system components.

AC-7 Unsuccessful login attempts

Rule CC-8: Verify that the Call Controller enforces a limit of [x] consecutive invalid login attempts during a time period of [y].

Rule CC-9: Verify that the Call Controller locks the account when the maximum number of unsuccessful logins has been reached.

AC-10 Concurrent Session Control

Rule CC-10: Verify that the Call Controller limits the number of concurrent sessions to [x].

AC-11 Session lock

Rule CC-11: Verify that the Call Controller prevents further access to the system by locking the session after a specified time [x] period of inactivity.

Rule CC-12: Verify that the Call Controller retains the session lock until appropriate credentials have been supplied by the user.

AU-8 Time stamps

Rule CC-13: Verify that the Call Controller uses internal system clocks for audit time stamps which include both date and time.

AU-9 Protection of audit information

Rule CC-14: Verify that c maintains audit records.

Rule CC-15: Verify that Verify Call Controller protects audit records from unauthorized access.

Rule CC-16: Verify that Verify Call Controller protects audit records from unauthorized modification.

Rule CC-17: Verify that Verify Call Controller protects audit records from unauthorized deletion.

AU-10 Non-repudiation

Rule CC-18: Verify that the Call Controller protects against an individual falsely denying having performed an action.

AU-12 Audit generation

Rule CC-19: Verify that the Call Controller audits events defined by policy.

Rule CC-20: Verify that only authorized users can determine which audit records are generated.

Rule CC-21: Verify that audit records for the auditable events are generated.

IA-2 Identification and authorization

Rule CC-22: Verify that the Call Controller uniquely identifies organizational users.

Rule CC-23: Verify that the Call Controller authenticates organizational users.

Rule CC-24: Verify that the Call Controller authenticates processes acting on behalf of a user.

Rule CC-25: Verify that multifactor authentication is used for remote access.

Rule CC-26: Verify that multifactor authentication is used for access to privileged accounts.

IA-3 Device identification and authentication

Rule CC-27a: Verify that the Call Controller identifies and authenticates an endpoint before a session is established.

Rule CC-27b: Verify that the Call Controller identifies and authenticates a Media gateway before a session is established.

Rule CC-27c: Verify that the Call Controller identifies and authenticates an Element Manager before a session is established.

Rule CC-27d: Verify that the Call Controller identifies and authenticates another Call Controller before a session is established.

IA-6 Authenticator feedback

Rule CC-28: Verify that the Call Controller obscures feedback of authentication information during the authentication process of a user.

Rule CC-29: Verify that the Call Controller obscures feedback of authentication information during the authentication process of a process acting on behalf of a user.

Rule CC-30: Verify that the Call Controller obscures feedback of authentication information during the authentication process of an endpoint, media gateway or Call Controller.

IA-8 Identification and authentication of non-organizational users

Rule CC-31: Verify that the Call Controller uniquely identifies a non-organizational user for remote access.

Rule CC-32: Verify that the Call Controller authenticates a non-organizational user for remote access.

Rule CC-33: Verify that the Call Controller identifies a process acting on behalf of a non-organizational user for remote access.

Rule CC-34: Verify that the Call Controller authenticates a process acting on behalf of a non-organizational user for remote access.

SI-7 Software and information integrity

Rule CC-35: Verify that the Call Controller detects unauthorized changes to software.

Rule CC-36: Verify that the Call Controller detects unauthorized changes to information.

SI-10 Information accuracy, completeness, validity and authenticity

Rule CC-37: Verify that the Call Controller checks information for accuracy, completeness, validity and authenticity as close to source as possible.

SI-11 Error handling

Rule CC-38: Verify that the Call Controller identifies error conditions.

Rule CC-39: Verify that the Call Controller generates error messages.

Rule CC-40: Verity that the Call Controller gives error messages only to authorized users.

Rule CC-41: Verify that the Call Controller prohibits inclusion of sensitive information in error logs.

Rule CC-42: Verify that the Call Controller prohibits inclusion of sensitive information in administrative messages.

SC-8 Transmission integrity

Rule CC-43: Verify that the Call Controller protects the integrity of transmitted data.

SC-9 Transmission confidentiality

Rule CC-44: Verify that the Call Controller protects the confidentiality of transmitted data.

SC-10 Network disconnect

Rule CC-45a: Verify that the Call Controller terminates a network connection at the end of an endpoint session.

Rule CC-45a: Verify that the Call Controller terminates a network connection at the end of a media gateway session.

Rule CC-45c: Verify that the Call Controller terminates a network connection at the end of an element manager session.

Rule CC-46a: Verify that the Call Controller terminates a network connection at the end of a specified time [x] of endpoint session inactivity.

Rule CC-46b: Verify that the Call Controller terminates a network connection at the end of a specified time [x] of media gateway session inactivity.

Rule CC-46b: Verify that the Call Controller terminates a network connection at the end of a specified time [x] of element manager session inactivity.

SC-20 Secure name / address resolution

Rule CC-47: Verify that the Call Controller provides additional data origin and integrity artifacts in response to name/address resolution queries.

SC-21 Secure name/address resolution service

Rule CC-48: Verify that the Call Controller performs data origin authentication and data integrity verification on name/address resolution responses requested by client systems.

SC-23 Session authenticity

Rule CC-49: Verify that the Call Controller provides session level authenticity protection.

SC-28 Confidentiality of information at rest

Rule CC-50: Verify that the Call Controller protects the confidentiality of information at rest.

Rule CC-51: Verify patches up to date.

Rules for The Element Manager Subsystem

AC-2

Rule EM-1: Verify Element manager (type, version and any other unique identifier).

Rule EM-2: Verify that administrator account exists, is valid and has valid credentials and access to other account types.

Rule EM-3: Verify user accounts are maintained according to policy.

AC-3 Access control enforcement

Rule EM-4a: Verify local access control policy (rule set) is implemented in Element Manager.

Rule EM-4b: Verify remote access control policy implemented in Element Manager.

AC-4 Information flow enforcement

Rule EM-5a: Verify Element Manager only allows authorized Call Controller to communicate with itself.

Rule EM-5b: Verify Element Manager only allows authorized Media Gateway to communicate with itself.

Rule EM-5c: Verify Element Manager only allows an authorized Endpoint to communicate with itself.

IA-2 Identification and authorization

Rule EM-6: Verify that the Element Manager uniquely identifies organizational users.

Rule EM-7: Verify that the Element Manager authenticates organizational users.

Rule EM-8: Verify that the Element Manager authenticates processes acting on behalf of a user.

Rule EM-9: Verify that multifactor authentication is used for remote access.

Rule EM-10: Verify that multifactor authentication is used for access to privileged accounts.

IA-3 Device identification and authentication

Rule EM-11: Verify that the Element Manager identifies and authenticates an endpoint before a session is established.

IA-6 Authenticator feedback

Rule EM-12: Verify that the Element Manager obscures feedback of authentication information during the authentication process of a user.

Rule EM-13: Verify that the Element Manager obscures feedback of authentication information during the authentication process of a process acting on behalf of a user.

Rule EM-14: Verify that the Element Manager obscures feedback of authentication information during the authentication process of an endpoint.

IA-8 Identification and authentication of non-organizational users

Rule EM-15: Verify that the Element Manager uniquely identifies a non-organizational user for remote access.

Rule EM-16: Verify that the Element Manager authenticates a non-organizational user for remote access.

Rule EM-17: Verify that the Element Manager identifies a process acting on behalf of a non-organizational user for remote access.

Rule EM-18: Verify that the Element Manager authenticates a process acting on behalf of a non-organizational user for remote access.

SI-7 Software and information integrity

Rule Em-19 Verify that the Element Manager detects unauthorized changes to software.

Rule EM-20: Verify that the Element Manager detects unauthorized changes to information.

SI-10 Information accuracy, completeness, validity and authenticity

Rule EM-21: Verify that the Element Manager checks information for accuracy, completeness, validity and authenticity as close to source as possible.

SI-11 Error handling

Rule EM-22: Verify that the Element Manager identifies error conditions.

Rule EM-23: Verify that the Element Manager generates error messages.

Rule EM-24: Verity that the Element Manager gives error messages only to authorized users.

Rule EM-25: Verify that the Element Manager prohibits inclusion of sensitive information in error logs.

Rule EM-26: Verify that the Element Manager prohibits inclusion of sensitive information in administrative messages.

SC-8 Transmission integrity

Rule EM-27: Verify that the Element Manager protects the integrity of transmitted data.

SC-9 Transmission confidentiality

Rule EM-28: Verify that the Element Manager protects the confidentiality of transmitted data.

SC-10 Network disconnect

Rule EM-29: Verify that the Element Manager terminates a network connection at the end of a session.

SC-28 Confidentiality of information at rest

Rule EM-30: Verify that the Element Manager protects the confidentiality of information at rest.

Rule EM-31:Verify patches up to date.

Rules for The IP Phone Subsystem

AC-2 Call Controller account management

Rule PH-1: Verify IP phone (type, version and any other unique identifier).

Rule PH-2: Verify user accounts are maintained according to policy.

Rule PH-3: Verify phone is registered to authorized Call Controller.

AC-3 Access control enforcement

Rule PH-4a: Verify local access control policy (rule set) is implemented in IP Phone.

Rule PH-4b: Verify remote access control policy implemented in IP Phone.

AC-4 Information flow enforcement

Rule PH-5: Verify IP Phone only allows authorized Call Controller to communicate with itself.

IA-2 Identification and authorization

Rule PH-6: Verify that the IP Phone uniquely identifies user.

Rule PH-7: Verify that the IP Phone authenticates processes acting on behalf of a user.

Rule PH-8: Verify that multifactor authentication is used for remote access.

Rule PH-9: Verify that multifactor authentication is used for access to privileged accounts.

IA-3 Device identification and authentication

Rule PH-10: Verify that the IP Phone uniquely identifies and authenticates the Call Controller before a session is established.

Rule PH-11: Verify SIP requests are authenticated.

IA-6 Authenticator feedback

Rule PH-12: Verify that the IP Phone obscures feedback of authentication information during the authentication process of a user.

Rule PH-13: Verify that the IP Phone obscures feedback of authentication information during the authentication process of a process, acting on behalf of a user.

IA-8 Identification and authentication of non-organizational users

Rule PH-14: Verify that the IP Phone uniquely identifies a non-organizational user for remote access.

Rule PH-15: Verify that the IP Phone identifies a process acting on behalf of a non-organizational user for remote access.

Rule PH-16: Verify that the IP Phone authenticates a process acting on behalf of a non-organizational user for remote access.

SC-8 Transmission integrity

Rule PH-17: Verify that the IP phone protects the integrity of transmitted data.

SC-9 Transmission confidentiality

Rule PH-18: Verify that the IP Phone protects the confidentiality of transmitted data.

SC-28 Confidentiality of information at rest

Rule PH-19: Verify that the IP Phone protects the confidentiality of information at rest.

SI-7 Software and information integrity

Rule PH-21: Verify that the IP Phone detects unauthorized changes to software.

Rule PH-22: Verify that the IP Phone detects unauthorized changes to information.

RulePH-23: Verify patches up to date.

Rules for The Firewall/IDS Subsystem

AC-2

Rule FW-1: Verify FW/IDS (type, version and any other unique identifier).

Rule FW-2: Verify that administrator account exists, is valid and has valid credentials and access to other account types.

Rule FW-3: Verify user accounts are maintained according to policy.

AC-3 Access control enforcement

Rule FW-4a: Verify local access control policy (rule set) is implemented in Firewall / IDs.

Rule FW-4b: Verify remote access control policy implemented in Firewall / IDs.

AC-4 Information flow enforcement

Rule FW-5a: Verify Firewall / IDS only allows authorized Call Controller to communicate with itself.

Rule FW-5b: Verify Firewall / IDS only allows authorized Media Gateway to communicate with itself.

Rule FW-5c: Verify Firewall / IDS only allows an authorized Endpoint to communicate with itself.

AU-8 Time stamps

Rule FW-6: Verify that the Firewall / IDS uses internal system clocks for audit time stamps which include both date and time.

AU-9 Protection of audit information

Rule FW-7: Verify that Firewall / IDS maintains audit records.

Rule FW-8: Verify that Firewall / IDS protects audit records from unauthorized access.

Rule FW-9: Verify that Verify Firewall / IDS protects audit records from unauthorized modification.

Rule FW-10: Verify that Verify Firewall / IDS protects audit records from unauthorized deletion.

AU-10 Non-repudiation

Rule FW-11: Verify that the Firewall / IDS protects against an individual falsely denying having performed an action.

AU-12 Audit generation

Rule FW-12: Verify that the Firewall / IDS audits events defined by policy.

Rule FW-13: Verify that only authorized users can determine which audit records are generated.

Rule FW-14: Verify that audit records for the auditable events are generated.

IA-2 Identification and authorization

Rule FW-15: Verify that the Firewall / IDS uniquely identifies organizational users.

Rule FW-16: Verify that the Firewall / IDS authenticates organizational users.

Rule FW-17: Verify that the Firewall / IDS authenticates processes acting on behalf of a user.

Rule FW-18: Verify that multifactor authentication is used for remote access.

Rule FW-19: Verify that multifactor authentication is used for access to privileged accounts.

IA-3 Device identification and authentication

Rule FW-20a: Verify that the Firewall / IDS identifies and authenticates an endpoint before a session is established.

Rule FW-20b: Verify that the Firewall / IDS identifies and authenticates a Media gateway before a session is established.

Rule FW-20c: Verify that the Firewall / IDS identifies and authenticates an Element Manager before a session is established.

Rule FW-20d: Verify that the Firewall / IDS identifies and authenticates a Call Controller before a session is established.

IA-6 Authenticator feedback

Rule FW-21: Verify that the Firewall / IDS obscures feedback of authentication information during the authentication process of a user.

Rule FW-22: Verify that the Firewall / IDS obscures feedback of authentication information during the authentication process of a process acting on behalf of a user.

Rule FW-23: Verify that the Firewall / IDS obscures feedback of authentication information during the authentication process of an endpoint, media gateway or Call Controller.

IA-8 Identification and authentication of non-organizational users

Rule FW-24: Verify that the Firewall / IDS uniquely identifies a non-organizational user for remote access.

Rule FW-25: Verify that the Firewall / IDS authenticates a non-organizational user for remote access.

Rule FW-26: Verify that the Firewall / IDS identifies a process acting on behalf of a non-organizational user for remote access.

Rule FW-27: Verify that the Firewall / IDS authenticates a process acting on behalf of a non-organizational user for remote access.

SI-7 Software and information integrity

Rule FE-28: Verify that the Firewall / IDS detects unauthorized changes to software.

Rule FW-29: Verify that the Firewall / IDS detects unauthorized changes to information.

SI-10 Information accuracy, completeness, validity and authenticity

Rule FW-30: Verify that the Firewall / IDS checks information for accuracy, completeness, validity and authenticity as close to source as possible.

SI-11 Error handling

Rule FW-31: Verify that the Firewall / IDS identifies error conditions.

Rule FW-32: Verify that the Firewall / IDS generates error messages.

Rule FW-33: Verity that the Firewall / IDS gives error messages only to authorized users.

Rule FW-34: Verify that the Firewall / IDS prohibits inclusion of sensitive information in error logs.

Rule FW-35: Verify that the Firewall / IDS prohibits inclusion of sensitive information in administrative messages.

SC-8 Transmission integrity

Rule FW-36: Verify that the Firewall / IDS protects the integrity of transmitted data.

SC-9 Transmission confidentiality

Rule FW-37: Verify that the Firewall / IDS protects the confidentiality of transmitted data.

SC-10 Network disconnect

Rule FW-38a: Verify that the Firewall / IDS terminates a network connection at the end of an endpoint session.

Rule FW-38b: Verify that the Firewall / IDS terminates a network connection at the end of a media gateway session.

Rule FW-38c: Verify that the Firewall / IDS terminates a network connection at the end of an element manager session.

Rule FW-38d: Verify that the Firewall / IDS terminates a network connection at the end of a Call Controller session.

Rule FW-39a: Verify that the Firewall / IDS terminates a network connection at the end of a specified time [x] of endpoint session inactivity.

Rule FW-39b: Verify that the Firewall / IDS terminates a network connection at the end of a specified time [x] of media gateway session inactivity.

Rule FW-39c: Verify that the Firewall / IDS terminates a network connection at the end of a specified time [x] of element manager session inactivity.

Rule FW-39d: Verify that the Firewall / IDS terminates a network connection at the end of a specified time [x] of Call Controller session inactivity.

Rule FW-40: Verify patches up to date.

Chapter 7 – Use of Security Content Automation Program (SCAP) for VOIP Security

Overview

This chapter focuses on the subset of standards that are encapsulated within the Security Content Automation Protocol (SCAP). As of September 2009, SCAP is considered to be at version "1.0" (http://scap.nist.gov/revision/1.0/index.html), with future iterations modifying and or enhancing existing SCAP components, or adding additional components that may be added from candidates that are considered "Emerging Specifications" (http://scap.nist.gov/emerging-specs/index.html).

In publishing the NIST Draft Special Publication (SP) 800-126, The Technical Specification for the Security Content Automation Protocol (SCAP), NIST is defining the specifications for organizing and expressing security-related information in standardized ways, as well as related reference data such as unique identifiers for vulnerabilities. SP 800-126 also provides an overview of SCAP, focusing on how software developers can integrate SCAP technology into their product offerings and interfaces.

SCAP seeks to encourage the interoperability and automation information security processes and data exchanges. SCAP is a suite of: selected open standards; enumerations of software vulnerabilities; security related mis-configuration and/or inconsistency detection names; standardized vulnerability names; standardized product platform host (operating systems, databases) names; standardized metrics and tools that afford the measurement of systems for vulnerabilities present; and methods for use of scoring mechanisms to rank the results of these measurements in order of criticality, to evaluate the degree of adverse impact of the discoveries upon network as well as desktop system security. SCAP also strives defines how these standards are combined (please reference NIST Draft Special Publication (SP) 800-126, The Technical Specification for the Security Content Automation Protocol (SCAP)).

As recently as 2006, only the XCCDF and OVAL specifications were considered a part of SCAP. NIST currently has encapsulated six (6) different standards initiatives through the SCAP. Now the following additional standards have been included:

- Common Vulnerabilities and Exposures (CVE)
- Common Configuration Enumeration (CCE)
- Common Platform Enumeration (CPE)
- Common Vulnerability Scoring System (CVSS)

This suite of standards is expected to grow over time to address emerging issues that face the vulnerability management and security compliance community. To this end NIST has developed a SCAP Release Cycle to help guide the evolution of the standard (http://scap.nist.gov/timeline.html).

There may be an infinite number of potential use cases for application of one or more

components of SCAP. To date, NIST has focused on a few specific use cases, with the most prominent being the evaluation of security configurations of Microsoft XP and VISTA operating systems in conjunction with the OMB mandate for the Federal Desktop Core Configuration (FDCC).

In FDCC use case, all six components of SCAP were utilized. However, many use cases may only involve one or more components, and as the applicability of SCAP to VOIP applications is considered, the applicability of the specific SCAP components must be considered as well as applicability of a sub-set, or the complete set, of the SCAP components utilized.

Currently, for use cases that NIST has defined a specific functional capability requirement involving a specified set of SCAP components and specific verifiable functionality that can be confirmed through a the NIST SCAP Validation Program (http://scap.nist.gov/validation/index.html). To date, the functional categories are not directly VOIP related, but – for the most part - do not exclude use of that capability within the scope of VOIP security.

Whether or not one relies on a "NIST SCAP Validated" tool, SCAP has many useful applications in securing information technology assets as described below.

Secure Configurations

Agencies and other organizations should consistently monitor their operating systems and applications, using SCAP tools and content, to ensure that they maintain a secure configuration. Such tools can also assist with automating implementation of an initial secure configuration for new assets (secure images may also be used for this purpose in some cases).

Regulatory Technical Control Compliance Automation

Agencies and other organizations can automate much of their regulatory technical security control compliance activities by regularly scanning information technology assets using SCAP checklists. SCAP checklists often have regulatory compliance mappings embedded within the checklist so that SCAP-compatible tools can automatically generate compliance evidence after running an assessment. In this scenario each low level security configuration check is mapped to an associated high level "regulatory" technical security controls. In addition, the SCAP checklists also often contain mappings to other high level policies (e.g., FISMA, ISO, DOD 8500, FISCAM) and SCAP tools may also output those compliance mappings.

Customization of Recommended Secure Configurations

Agencies and other organizations can customize recommended SCAP secure configurations (e.g., NIST checklists) to tailor them to specific environments. SCAP checklists, being represented in standards based XML formats, are an ideal format for customization. Organizations can modify checks, delete checks, add new checks, and digitally sign their changes. Then SCAP compatible tools will be able to automatically process the customized checklists without any additional coding being required or even any involvement from the SCAP tool vendor.

Integration and Automation of Security Operations

Agencies and other organizations can integrate and automate disjoint security operations activities and databases through adoption of SCAP. This can be achieved by integrating interoperable tools, such as vulnerability databases, incident databases, intrusion detection databases, and asset databases using SCAP data as primary keying material. For example, all security products and databases should use standard names for software flaws, configuration issues, and product names.

Vulnerability Assessment and Reporting

Agencies and other organizations can use SCAP vulnerability and product naming enumeration standards when assessing and communicating about vulnerabilities (security related software flaws and mis-configurations). Agencies and other organizations can report incident details (both internally and externally) using SCAP vulnerability and product names to the greatest extent possible. This ensures that all vulnerability communications precisely identify the relevant low level issues, enable integration of data feeds using this same standardized language, and enable easy correlation with other data repositories that may have additional information on the relevant vulnerabilities.

SCAP 1.0 Components

XCCDF

Extensible Configuration Checklist Description Format (XCCDF) from the NSA's National Vulnerability Database is a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. The specification also defines a data model and format for storing results of benchmark compliance testing. The intent of XCCDF is to provide a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance, and thereby foster more widespread application of good security practices. Development of the XCCDF specification is being led by NSA, with contributions from other agencies and organizations.
The motivation for this is improvement of security for IT systems, including the Internet, by better application of known security practices and configuration settings.

An XCCDF document is composed of one or more XCCDF rules. An XCCDF rule is a high-level definition of a technical check on a system. A rule does not directly specify how a check should be performed, but instead points to other XML documents (such as OVAL definition files) that contain the actual instructions for performing the check.

One potential use for XCCDF is streamlining compliance to FISMA and Department of Defense (DOD) STIGs. XCCDF proposes to automate certain technical aspects of security by converting English text contained in various publications (e.g., configuration guides, checklists, the National Vulnerability Database [NVD]) into a machine-readable XML format such that the various audiences (e.g., scanning vendors, checklist/configuration guide, auditors) will be operating in the same semantic context. The end result will allow organizations to use commercial off-the-

shelf (COTS) tools to automatically check their security and map to technical compliance requirement.

OVAL ™

OVAL™ is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. The OVAL Language is a collection of XML schema for representing system information, expressing specific machine states, and reporting the results of an assessment. The OVAL repository is the central meeting place for the OVAL Community to discuss, analyze, store, and disseminate OVAL Definitions.

Open Vulnerability and Assessment Language (OVAL) is used to specify the technical details for checking systems for the presence of vulnerabilities and configuration issues. A set of instructions used to check for a security problem, such as an incorrect minimum password length setting, is known as an OVAL definition. A file containing one or more OVAL definitions (often hundreds or even thousands) is known as an OVAL definition file.

OVAL definitions are standardized, machine-readable tests written in the Open Vulnerability and Assessment Language (OVAL™) that check the machine state of computer systems for the presence of software vulnerabilities, configuration issues, programs, and patches. OVAL definitions, which are free to use and implement in information security products and services, are written in Extensible Mark-up Language (XML) and are available for most major platforms.

There are four types of OVAL definitions:

- Vulnerability definitions, which define “the conditions that must exist for a specific vulnerability to be present”
- Patch definitions, which define “the conditions that determine whether a particular patch is appropriate for a system”
- Inventory definitions, which define “the conditions that determine whether a specific piece of software is installed on the system”
- Compliance definitions, which define “the conditions that determine compliance with a specific policy or configuration statement.”

CVE and NVD

The Common Vulnerabilities and Exposures (CVE) vulnerability naming standard is a dictionary of names for most publicly known security flaws in IT software. The CVE industry standard has achieved wide acceptance by the security industry and a number of government organizations. It is funded by US-CERT and the technical analysis work is done at MITRE Corporation. General CVE information is available at http://cve.mitre.org/.

CVE provides the computer security community with the following:

- A comprehensive list of publicly known vulnerabilities
- An analysis of the authenticity of newly published vulnerabilities
- A unique name to enumerate and describe each vulnerability.

The vulnerabilities listed in CVE can be best viewed using the National Vulnerability Database (NVD), which provides summaries for all CVE vulnerabilities. Each summary contains attributes of the vulnerability (including a short summary and vulnerable version numbers) and links to advisories, patches, and other resources related to the vulnerability. NVD offers a fine-grained search engine that allows users to search for vulnerabilities containing a variety of characteristics. For example, users can search on product characteristics such as vendor name, product name, and version number, or on vulnerability characteristics such as severity, related exploited range, and type of vulnerability. NVD also supports queries in OVAL format. NVD is available at http://nvd.nist.gov/.

CVE has not been adopted by any formal standards body, but it is a widely used self-declared standard. NIST SP 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme, is available at http://csrc.nist.gov/publications/nistpubs/800-51/sp800-51.pdf.
Any product containing NVD or CVE data can be integrated with the NVD web site vulnerability summaries. To link to a particular vulnerability summary, simply use the hyperlink format http://nvd.nist.gov/nvd.cfm?cvename=CVE-2001-0322 where "CVE-2001-0322" to see that vulnerability name actually replaced with the name of the vulnerability of interest.

CCE

In mid-2006, plans for a Common Configuration Enumeration (CCE) standard were announced. It is very similar to CVE, but it addresses security mis-configurations in software deployments instead of flaws with the software itself. Checklists could refer to CCE names for mis-configurations just as they refer to CVE names for software flaws. More information on CCE is available at: http://cve.mitre.org/cce/.

CPE

CPE™ is a structured naming scheme for information technology systems, platforms, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name. The power of the CPE standard is in the uniformity in defining a particular component of the IT system that can then be linked to recommended configuration data defined in CCE and security vulnerabilities defined in CVE.

CVSS

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores. Two common uses of CVSS are prioritization of vulnerability remediation activities and in calculating the severity of vulnerabilities discovered on one's systems. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

In particular, NVD supports the Common Vulnerability Scoring System (CVSS) version 2 standard for all CVE vulnerabilities. NVD provides CVSS 'base scores' which represents the innate characteristics of every included vulnerability. We do not currently provide 'temporal scores' (scores that change over time due to events external to the vulnerability). However, NVD does provide a CVSS score calculator to allow you to add temporal data and to even calculate environmental scores (scores customized to reflect the impact of the vulnerability on your organization). This calculator contains support for U.S. government agencies to customize vulnerability impact scores based on FIPS 199 System ratings. An expert version of this calculator is also provided by the NVD.

Many organizations are using CVSS, and each are finding value in different ways. Below are some examples:

Vulnerability Bulletin Providers: Both non-profit and commercial organizations are publishing CVSS base and temporal scores and vectors in their free vulnerability bulletins. These bulletins offer much information, including the date of discovery, systems affected and links to vendors for patching recommendations.

Software Application Vendors: Software application vendors are providing CVSS base scores and vectors to their customers. This helps them properly communicate the severity of vulnerabilities in their products and helps their customers effectively manage their IT risk.

User Organizations: Many private-sector organizations are using CVSS internally to make informed vulnerability management decisions. They use scanners or monitoring technologies to first locate host and application vulnerabilities. They combine this data with CVSS base, temporal and environmental scores to obtain more contextual risk information and remediate those vulnerabilities that pose the greatest risk to their systems.

- Vulnerability Scanning and Management: Vulnerability management organizations scan networks for IT vulnerabilities. They provide the CVSS base score for every vulnerability observed for each network device. User organizations use this critical data stream to more effectively manage their IT infrastructures by reducing outages and protecting against malicious and accidental IT threats.
- Security (Risk) Management: Security Risk Management firms use CVSS scores as input to calculating an organization's risk or threat level. These firms use sophisticated applications that often integrate with an organization's network topology, vulnerability data, and asset database to provide their customers with a more informed perspective of their risk level.
- Researchers: The open framework of CVSS enables researches to perform statistical analysis on vulnerabilities and vulnerability properties.

Emerging Specifications

Many emerging specifications may be considered for adoption and inclusion in a future version of SCAP, and the sources of these specifications may come from industry, government, or

elsewhere. MITRE tracks many standards that may someday evolve into a future version of SCAP, and consolidates their efforts under an initiative termed “Making Security Measureable”. (http://measurablesecurity.mitre.org/ , http://measurablesecurity.mitre.org/list/index.html). NIST has published some guidelines and FAQs to help guide the evolution process as well (http://scap.nist.gov/emerging-specs/index.html). While there are no guarantees that a specification that is officially considered an emerging specification, a few may warrant review due to indications that they may have matured enough for near term consideration (http://scap.nist.gov/emerging-specs/listing.html).

The following listing represents specifications for emerging security automation capabilities includes 3 XML languages, and two metrics capabilities:

Asset Reporting Format (ARF): The ARF language is a general security automation results reporting language developed by the DoD in conjunction with NIST and members of the SCAP vendor community. It provides a structured language for exchanging and exporting detailed, per-device assessment data between network assessment tools. ARF is intended to be used by vulnerability scanners, eXtensible Configuration Checklist Description Format (XCCDF) scanners, and other tools that collect detailed configuration data about Internet Protocol-based networked devices. Detailed information about ARF can be found in the ARF specification and data dictionary.

Website: http://metadata.dod.mil/mdr/ns/netops/shared_data/arf_index_page/0.41).

Common Configuration Scoring System (CCSS): A set of standardized measures for the characteristics and impacts of software security configuration issues. NIST IR 7502 also provides several examples of how CCSS measures and scores would be determined for a diverse set of configuration issues. Once CCSS is finalized, CCSS data can assist organizations in making sound decisions as to how configuration issues should be addressed and can provide data to be used in quantitative assessments of host security.

Web site: NIST CSRC Publications: NIST IR 7502

Common Misuse Scoring System (CMSS)

A set of standardized measures for the characteristics of software feature misuse vulnerabilities. A software feature misuse vulnerability is present when the trust assumptions made when designing software features can be abused in a way that violates security. NIST IR 7517 defines the CMSS specification, and it also provides examples of how CMSS measures and scores would be determined for software feature misuse vulnerabilities. Once CMSS is finalized, CMSS data

can be used along with CVSS and CCSS data to assist organizations in making sound decisions as to how their host vulnerabilities should be addressed. CMSS data can also be used in quantitative assessments of host security.
Web site: NIST CSRC Publications: NIST IR 7517

Open Checklist Interactive Language (OCIL)

The Open Checklist Interactive Language defines a framework for expressing a set of questions to be presented to a user and corresponding procedures to interpret responses to these questions. Although the OCIL specification was developed for use with IT security checklists, the uses of OCIL are by no means confined to IT security. Other possible use cases include research surveys, academic course exams, and instructional walkthroughs.

Web site: http://scap.nist.gov/specifications/ocil/

Open Checklist Reporting Language (OCRL™)

Open Checklist Reporting Language is a language for writing machine-readable XML definitions that gather information from systems and present it as a standardized report for human evaluation of policy compliance. Each generated report file corresponds to a single policy recommendation.

OCRL complements existing benchmark languages such as eXtensible Configuration Checklist Description Format (XCCDF) and Open Vulnerability and Assessment Language (OVAL®) — which already provide capabilities for structuring security guidance in a machine-understandable way and describing how to gather and evaluate system information to determine compliance — by addressing those instances where a human is necessary to determine compliance with a given policy recommendation, or where XCCDF and OVAL do not have the necessary capability to evaluate collected information for compliance with a recommendation. For example, a policy recommendation that states, “The user should disable unnecessary services on the computer,” requires human judgment to determine what services are unnecessary. An OCRL Definition could be written to provide a report of all the services running on the computer, which could then be used by a person to determine whether any unwanted services are present.

OCRL was specifically designed to work with the XCCDF and OVAL benchmark authoring languages. While OCRL documents can be used alone by a software program to create one or more reports, by using OCRL in conjunction with OVAL more automation can be called out from an XCCDF document than using OVAL alone, resulting in significantly enhanced capabilities for benchmark automation.

Web site: http://ocrl.mitre.org/

Bibliography (Editor's Note this needs a little more work!)

- Internet Protocol Telephony & Voice Over Internet Protocol – Security Technical Implementation Guide Version 2, Release 2
- http://iase.disa.mil/stigs/stig/VoIP-STIG-V2R2.pdf
- Draft ITU-T Recommendation X.805 (Formerly X.css), Security architecture for systems providing end-to-end communications
- https://datatracker.ietf.org/documents/LIAISON/itut-sg17-ls-x805-end2end-communications.pdf
- ATIS-1000007.2006 – Generic Signaling and Control Plane Security Requirements for Evolving Networks https://www.atis.org/docstore/default.aspx
- the ETSI TIPHON Threat Likelihood Scoring Criteria [2].
- AllianceAnalysis of Information Assurance Requirements and Threats for the DOD Real-Time Services Environment, May 22, 2009VoIP Security and Privacy Threat Taxonomy – Public Release 1.0, VoIP Security