INTERNET SECURITY ALLIANCE

SCAP for VoIP

Automating Configuration Compliance

6th Annual IT Security Automation Conference

SALARE SECURITY™
Stopping Covert Communication

VeriSign®

Presentation Overview

1. The Business Challenge
2. Securing Voice over IP Networks
3. The ISA VoIP Security Project
4. Next Steps With SCAP
5. Summary

The Business Challenge

- Cyber Security Operations:
  - Expensive
  - Prone to Failure

96% of Breaches Avoidable through Simple or Intermediate Controls
Verizon 2010 Data Breach Report

- Cyber Security Industry is Caught in "Too Busy to Get Better" Trap

"I have additional risk to manage. I have capital budget. There are great new solutions. I don't have more people to manage them."
Paraphrase of leading CISOs

INTERNET SECURITY ALLIANCE

VoIP Enterprise Risk

Network convergence and channel consolidation potentially increase vulnerabilities and the consequences of failure in security.

Dennis Blair, Former Director of National Intelligence, Feb. 2010 (paraphrase)

- Impact of Convergence
  - Silo Approaches to Security Understood
  - Cross-Silo Vulnerabilities and Attacks Ignored
  - VLANs have vulnerabilities
- Impact of Channel Consolidation
  - Voice Used as an Out-Of-Band Channel
  - Voice Can be Used to Carry Data

SALARE SECURITY™ Stopping Covert Communication

VeriSign®

VoIP Security Today

- Guidance
  - NSA Security Guidance for IPT
  - DISA VVoIP
  - NIST SP 800-58
  - Best Practices from Vendors
- Security Devices
  - SBC
  - Firewall
  - IPS/IDS
- Assessments & Controls
  - Pen testing
  - Monitoring
  - Configuration Management
  - Change Control

New Vulnerabilities
New Devices
New Controls
New Assessments

Who has time?

FISMA and FDCC

- FISMA VoIP Coverage
  - FIPS 199 and 200 Point to NIST SP-800 Series
  - Implementation of SP-800-53 Controls Required for Compliance
  - SP 800-58 Defines VoIP Controls
- FDCC does not Address VoIP
  - SP-800-58 Recommends No Soft Phones
  - Only covers Vista and XP OSs

ISA VoIP Charter

ISA Mission

ISA is to combine advanced technology with the economic realities and help create effective public policy leading to a sustainable system of world-wide cyber security.

ISA VoIP Project Objective

Increase cyber security posture and reduce operational expense through automated VoIP security configuration and compliance.

ISA VoIP Security Project

Focus on automation of configuration management and compliance

2010 Objective
IP Phone
Soft Phone

2011 Objective
IP PBX
Call Manager

Final Objective
IP Phone
Soft Phone
IP PBX
Call Manager
Session Border Controller
And more…

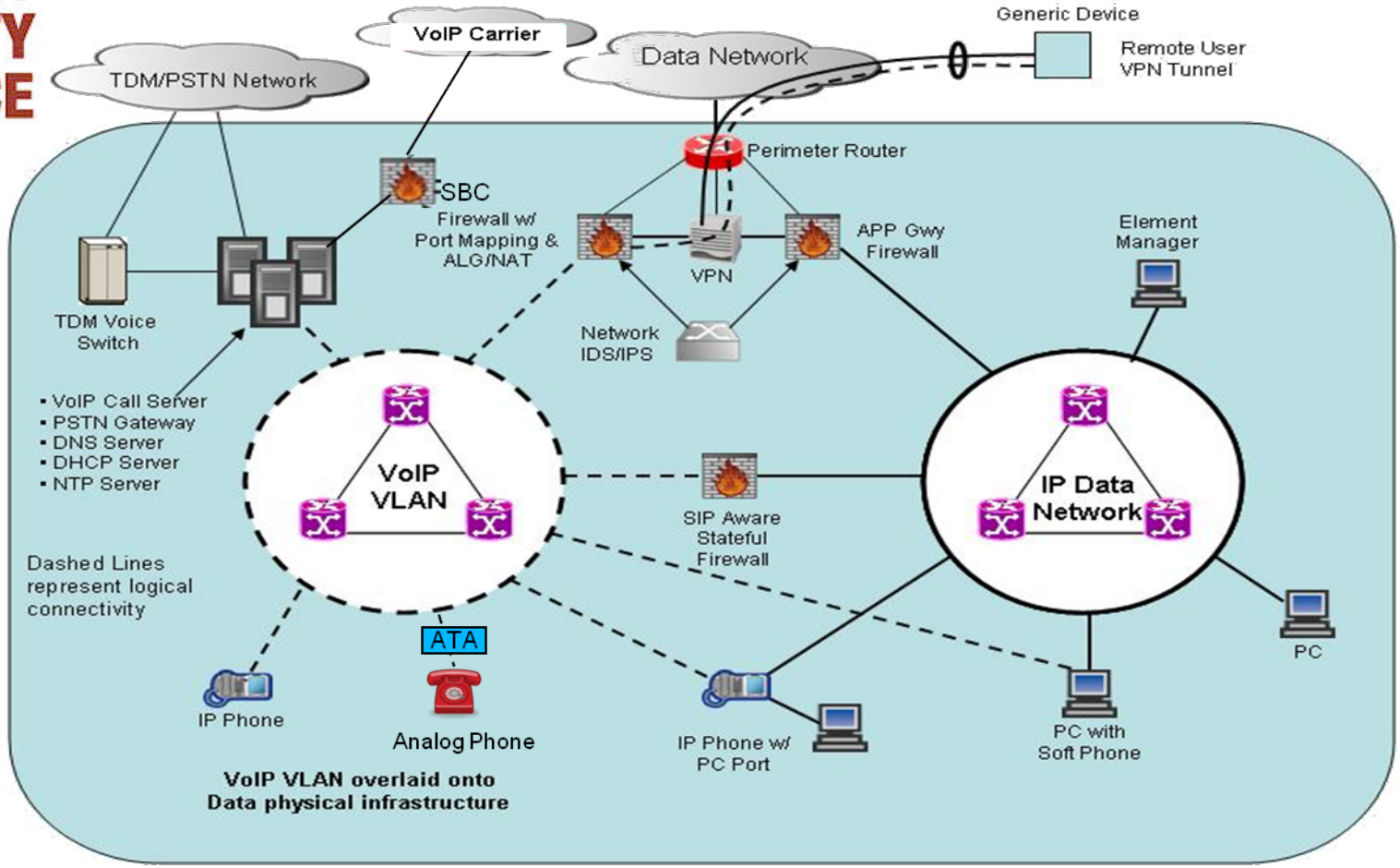
NIST SP 800-53, 800-70, 800-126, 800-58, NCP

SALARE SECURITY™ Stopping Covert Communication

VeriSign

INTERNET SECURITY ALLIANCE

Reference VoIP Network



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)

SALARE SECURITY™ Stopping Covert Communication

VeriSign®

Need To Automate IP Phone Configuration Compliance

- Widely Distributed
- New Access Vector
- Perimeter Security Not Sufficient
- Default Configuration Weak
- Will Drift from Baseline
  - Changes to phone settings undetected
  - Manual assessment not practical
- Convergence with Data Network

❖**At Least One Phone Will Be Altered!**

Typical Automation For Configuration Compliance

Access Methods

- Telnet / SSH
- HTTP / HTTPS
- SNMP
- Console
- Element Manager
- LLDP/CDP

Issues

- Vendor specific
- Inconsistency across data formats and mechanism
- Lack of open standards
- Incomplete retrieval of 'running' configuration information / state
- May conflict with security best practices (i.e., disable protocol)

INTERNET SECURITY ALLIANCE

SCAP For VoIP: Today

SCAP Component	Description	Keyword 'VoIP' Search	Keyword 'Phone' Search
Common Vulnerability Enumeration (CVE)	Standard nomenclature and dictionary of security related software flaws	96 matches	336 matches, out of which 102 (Apple iPhone), 27 (Cisco), 7(Avaya), 6 (Nortel), 5 (Microsoft), 5 (Snom)
Common Configuration Enumeration (CCE)	Standard nomenclature and dictionary of software mis-configurations	0 (under development)	0 (under development)
Common Platform Enumeration (CPE)	Standard nomenclature and dictionary of product naming	22 matches (nortel and cisco)	146 matches
Common Vulnerability Scoring System (CVSS)	Standard for measuring the impact of vulnerabilities	0	0
eXtensible Checklist Configuration Description Format (XCCDF)	Standard XML for specifying checklists and for reporting results of checklist evaluation	0	0
Open Vulnerability and Assessment Language (OVAL)	Standard XML for test procedures	5 matches – cisco (V)	16 matches - 13 (V), 3 (I)

SCAP For VoIP: Today

- Several CPE IDs available for IP phones
- Focus on software flaws / vulnerabilities (CVE)
  - ➢ A few systems identify firmware version and do very basic penetration / vulnerability test
- No CCE IDs
- No Checklists for VoIP in NCP
- All configuration settings not accessible for SCAP
- Few OVAL test definitions available for VoIP
- No OVAL definitions for configuration compliance

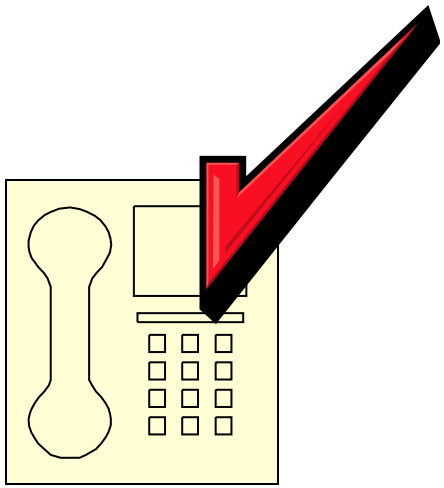
❖ **Much work remains to SCAP-enable VoIP**

Status on the VoIP Security Project at ISA

- Focus: Configuration Compliance & Validation
- IP Phone is First to be Evaluated
- Baseline Security Configuration Checklist – Done
  - NIST 800-53 controls mapped to IP phone
  - XCCDF document available
  - In process to submit checklist to National Checklist Program for review
- Vendor Specific IP Phone Checklists Under Development

IP Phone Baseline Security Checklist

- Assure Baseline Security
- Signaling Protocol: SIP
- Media Protocol: RTP/RTCP
- Configuration Controls For
  - 7 Security Principles
  - 3 Traffic Planes
- Automated and Manual Rules
- Expressed using XCCDF
- “One size does not fit all”



Challenges With SCAP Enabling The IP Phone

- Perpetual Configuration Drift
- IP Phone Uses an Embedded OS
  - Today's authenticated configuration scanners focus on Windows and Unix/Linux
- Retrieval of Entire Running State Not Available
  - Use of remote access protocols varies between vendors
- No OVAL definition schema available for IP phone configuration compliance

Host Based Configuration Scanner

Host based agent installed on the phone

- OVAL definition file to be downloaded to agent
- Gather, analyze configuration locally
- Generate and report results

Pros

- Direct access to configuration
- Standard reporting format available with OVAL

Cons

- Regular updates for IP phones across enterprise
- Resource consumption could impact call quality

Network Based Configuration Scanner

Centralized platform probes IP phones for configurations

- No agent on phone
- Gather configuration from phone
- Analyze and generate report on centralized scanner

Pros

- Eliminate need to update agent on all phones

Cons

- Visibility of entire configuration questionable
- Lack of common data structure & remote access method

Hybrid Based Configuration Scanner

Lightweight, host based agent installed on each phone

- Configuration gathered within each phone
- Centralized assessment platform to analyze/report results

Pros

- Small memory (resource) footprint required for agent
- Eliminate need to update agent on all phones
- Direct access to configuration
- Extensive analysis and reporting available
- No significant impact to functionality and performance

Cons

- None

Next Steps – Automation Using OVAL

- Preliminary XCCDF content completed
- OVAL definitions for IP phone
- Apply OVAL compliance check to static phone configuration file stored on IPT server
- Ability to query entire configuration running state
- Apply OVAL compliance check to running state configuration on IP phone
- Report the results of the assessment

Industry Adoption

- Using SCAP to automate configuration compliance of IP phone is possible
- Vendor support is needed to make this a reality
  - Develop specific product checklists based on an industry developed IP phone baseline checklist (i.e., ISA VoIP checklist).
  - Develop an industry standard interface to query the entire running state of the phone configuration.
  - Possibility of a standard data format structure for IP phone configuration

Summary

- Challenge today is VoIP configuration compliance rely on manual processes with limited operational resources
  - Numerous VoIP security guidelines but no master list of all security requirements (i.e., IP phone checklist) focus on automation
- Adoption of standard based approach using SCAP is right tool to address VoIP configuration compliance challenge
- Configuration compliance must be a fundamental capability of an IP phone, not an optional 'nice-to-have' feature
- NIST 800-70 review & National Checklist Program
- VoIP vendor involvement is critical

Contact Information

Internet Security Alliance

(703)907-7090
mmorgan@isalliance.org

Co-chair of ISA VoIP Project and
CEO of Salare Security

Paul Sand

(312) 994-2336
paul.sand@salaresecurity.com

Co-chair of ISA VoIP Project and
Technical Director at VeriSign

Thomas Grill

(703) 948-3287
tgrill@verisign.com