INTERNET SECURITY ALLIANCE

Application of SCAP to Secure Unified Communications

INTERNET
SECURITY
ALLIANCE

Baseline Standards Participants

Co-Chairs of the Baseline Standards Group
Mark Humphrey, Boeing and Scott Armstrong, Gideon Technologies

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 Archer, American Century Investments
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
Chad Lorenc, Agilent Technologies, Inc.
Cheri Sigmon, Department of Defense
Dawn Adams, EWA-Canada
Denise Walker, DBA, Lone Star College System
Ed White, McAfee
Edward Cummins, Raytheon
Faisal Naqvi, Expedia
Gary Humphrey, AT&T
Greg Pulos, Department of Commerce
Imran Khan, Consultant
James Mesta, Agilent Technologies, Inc.
Jeff Pound, US Department of Transportation
Jeffrey Ritter, Waters Edge Consulting
Jim Meyer, Institute for Defense Analyses
Joe Grettenberger, Compliance Collaborators, Inc.
John Poff, Pearl Technology
John Fulater, HSBC North America
John Wurzler, CNA Insurance
Kathleen Blasco, Department of Homeland Security
Ken Fee, Firefly Communications
Ken Stavinoha, Microsoft
Kenneth Kousky, Salare Security, LLC
Kevin Watkins, McAfee
Leighton Johnson, Information Security and Forensics Management Team
Linda Kostic, eTrade Financial
Lorelei Knight, ICSAlabs, an Independent Division of Verizon Business Systems
Lynn Hitchcock, Raytheon
Martha Soles, US-CERT
Matt Trainor, Nortel Networks
Michael Hamilton, City of Seattle
Paul Salva, HSBC North America
Pete Eisele, Northrop Grumman
Richard Austin, Kennesaw State University
Rick Mellendick, Food and Drug Administration
Robert Kennedy, Disney
Robert Smith, Global UniDocs Company
Ronald Rice, Defense Information Systems Agency
Shawn Dickson, Raytheon
Sheila Christman, National Security Agency
Steve Carver, FAA (Retired)
Steven Bennett, Jones Day
Steven Draper, National Security Agency
Terry Rimmer, Oklahoma Office of State Finance
Tom Grill, VeriSign

INTERNET SECURITY ALLIANCE

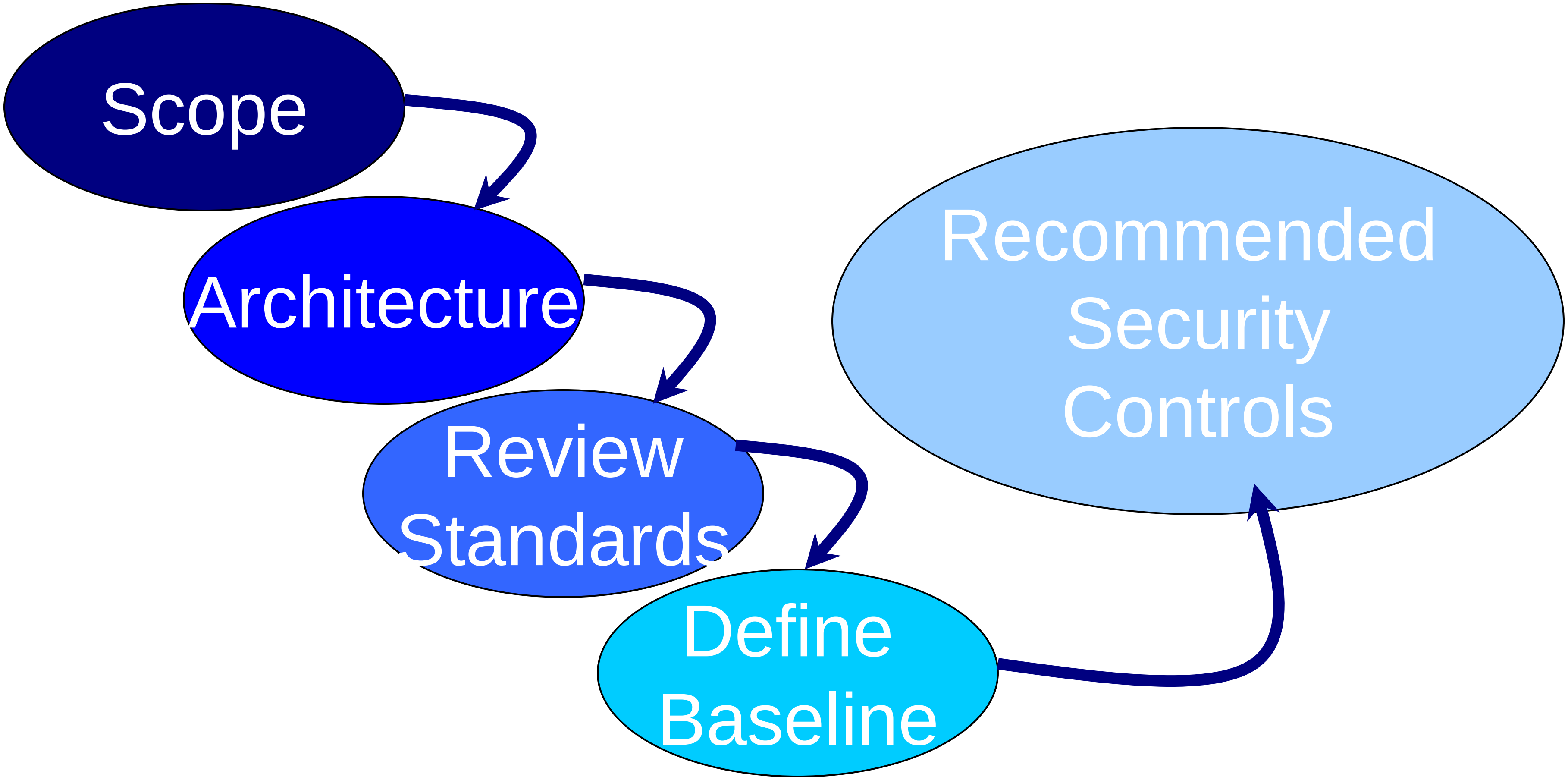
Special Thanks

AJ West, Boeing
Andriy Markov, VoIPshield Systems Inc.
Barry Wasser, DHS
Bogdan Materna, VoIPshield Systems Inc.
Dawn Adams, EWA-Canada
Ed Cummins, Raytheon
Gary Gapinski, NASA
John Fulater, HSBC North America
Ken Stavinoha, Microsoft
Leighton Johnson, ISFMT
Paul Salva, HSBC North America
Peter Thermos, Palindrome Technologies
Rick Mellendick, FDA
Terry Rimmer, Oklahoma Office of State Finance

Andrew Bove, Secure Acuity Networks, LLC
Barry Archer, American Century Investments
Bob Moskowitz, ICSAlabs
David Lukasik, Dept of Veterans Affairs
Denise Walker, DBA, Lone Star College Sys.
Ed White, McAfee
Joe Grettenberger, Compliance Collaborators
Ken Kousky, IP3, Inc.
Kevin Watkins, McAfee
Matt Trainor, Nortel Networks
Pete Eisele, Northrop Grumman
Richard Austin, Kennesaw State University
Ronald Rice, DISA
Tom Grill, VeriSign

INTERNET
SECURITY
ALLIANCE

Baseline Standards Process



Scope

Architecture

Review Standards

Define Baseline

Recommended Security Controls

INTERNET SECURITY ALLIANCE

Baseline Standards Defined Areas

- Phone Security Overview - Hypertext Transfer Protocol Secure (**HTTPS**)
- Using the Certificate Authority Proxy Function
- Encrypting Phone Configuration Files
- Configuring Digest & Phone Hardening
- Call Controller Hardening
- Firewalls and Intrusion Prevention Systems (**IPS**)
- Security at Different Planes and Other Relevant Controls
- Signaling and Media Protection Mechanisms

Baseline Standards Basis for SCAP

- Why SCAP?
- VoIP Community Today
  - Distinct Groups and Perspectives
    - Common Carrier
    - Vendors
    - Enterprise/ Business

Baseline Standards Basis for SCAP

Key Resources

- DraftTelecommunication Standardization Sector (**ITU**-**T**) Recommendation X.805 (Formerly X.css), Security architecture for systems providing end-to-end communications
- Internet Protocol Telephony & Voice Over Internet Protocol – Security Technical Implementation Guide Version 2, Release 2
- Alliance for Telecommunications Industry Solutions (ATIS) -1000007.2006 - Generic Signaling and Control Plane Security Requirements for Evolving Networks
- Federal Information Security Management Act (FISMA).
- NIST SP 800-32, "Introduction to Public Key Technology and the Federal PKI Infrastructure",
- Security Guidance for Deploying IP Telephony Systems. http://www.isalliance.org/images/stories/I332-016R-2005.pdf
- Defence Information Systems Agency (DISA) Security Technical Implementation Guides.

Baseline Standards Basis for SCAP

Key Resources (Cont.)

- Federal Information Processing Standards (FIPS) PUB 140-2, Security Requirements for Cryptographic Modules
- NIST SP 800-53 Rev. 3, “Recommended Security Controls for Federal Information Systems
- Jonathan Rosenberg, et. al., “SIP: Session Initiation Protocol”

  Internet Engineering Task Force (IETF) Request for Comments (RFC) 3261.
- Peter Thermos, Ari Takanen, “Securing VoIP Networks; Threats, Vulnerabilities and Countermeasures”, Addison-Wesley 2007, ISBN:978-0321437341
- S. Kent, K. Seo, “Security Architecture for the Internet Protocol”, RFC 4301, December 2005

Baseline Standards Strategy

- Configurations and Compliance Testing
- Minimum Baseline Controls
- Security Considerations
  - – Defense in Breadth
  - – Defense in Depth
- Automated Processes

Baseline Standards

Phone Security Overview

- Match Baseline to Organization’s needs
  - Appropriate Assurance Level
  - Flexible
  - Adaptable
  - Currently Available Solution
- Adequate Service Continuity

  (Switched Network Equivalent)

Baseline Standards

Certificate Authority Proxy Function

- Enable Certificates and Public Key Infrastructure (**PKI**)
  - – Identity Management
  - – Confidentiality
  - – Integrity
  - – Availability

Baseline Standards

Encrypting Phone Configuration Files

- Encryption/Decryption Process
- Security Controls
  - Symmetric Encryption Algorithms
  - Asymmetric Encryption Algorithms
  - Key Management
- Security Considerations
  - Public Key Infrastructure (**PKI**)
  - Key Management Infrastructure (**KMI**)
  - Trivial File Transfer Protocol (**TFTP**)
  - Passwords

Baseline Standards

Configuring Digest – Phone Hardening

- Digest Authentication
  - – Users-to-Proxy
  - – Proxy- to-Proxy
  - – Proxy-to-Server
- Phone Hardening
  - – Device Update Assurance
  - – Data-at-Rest (minimize Attack surface)
  - – Data-in-Transit **(CIA)**

INTERNET
SECURITY
ALLIANCE

Baseline Standards

Call Controller Hardening

- Minimize Attack Surface
- Delete Unnecessary Services & Utilities
- Enable Incident Management
  - Detection
  - Analysis
  - Response

Baseline Standards

Firewalls and IPS

- Segment & Isolate Infrastructure
  - Pass Allowed Traffic
  - Block Attacks
- Monitor and Manage Network
  - Network & Situational Awareness
  - Audit and Accountability

Baseline Standards

Security at Different Planes & Other Relevant Controls

- Management Plane
- Signaling Plane
- Media/Control Media Plane
- Attack Vectors and Exposures
  - MITM, Replay, Impersonation, TFTP…..

INTERNET
SECURITY
ALLIANCE

Request the White Paper

Please email bfoer@isalliance.org

to request a free copy of

Application of SCAP to Secure Unified Communications

INTERNET
SECURITY
ALLIANCE

Baseline Standards

Questions?

Baseline Standards

Phone Security Overview

- Technology Changed
- VoIP Quickly Adopted
  - Commercial Market
  - Government
- Regulation and Legal Issue Also Following
  - ISAlliance Leading Effort to Assist Definition
  - Others