INTERNET SECURITY ALLIANCE

VoIP Security Project:
SCAP Applicability Work Group

INTERNET SECURITY ALLIANCE

Outline

- Introductions
- The Challenge
- Working Group Process
- Applicability of the SCAP Standards
- Future Needs
- Q&A

Applicability Participants

Chair of the Applicability Group
Paul Sand, Salare Security

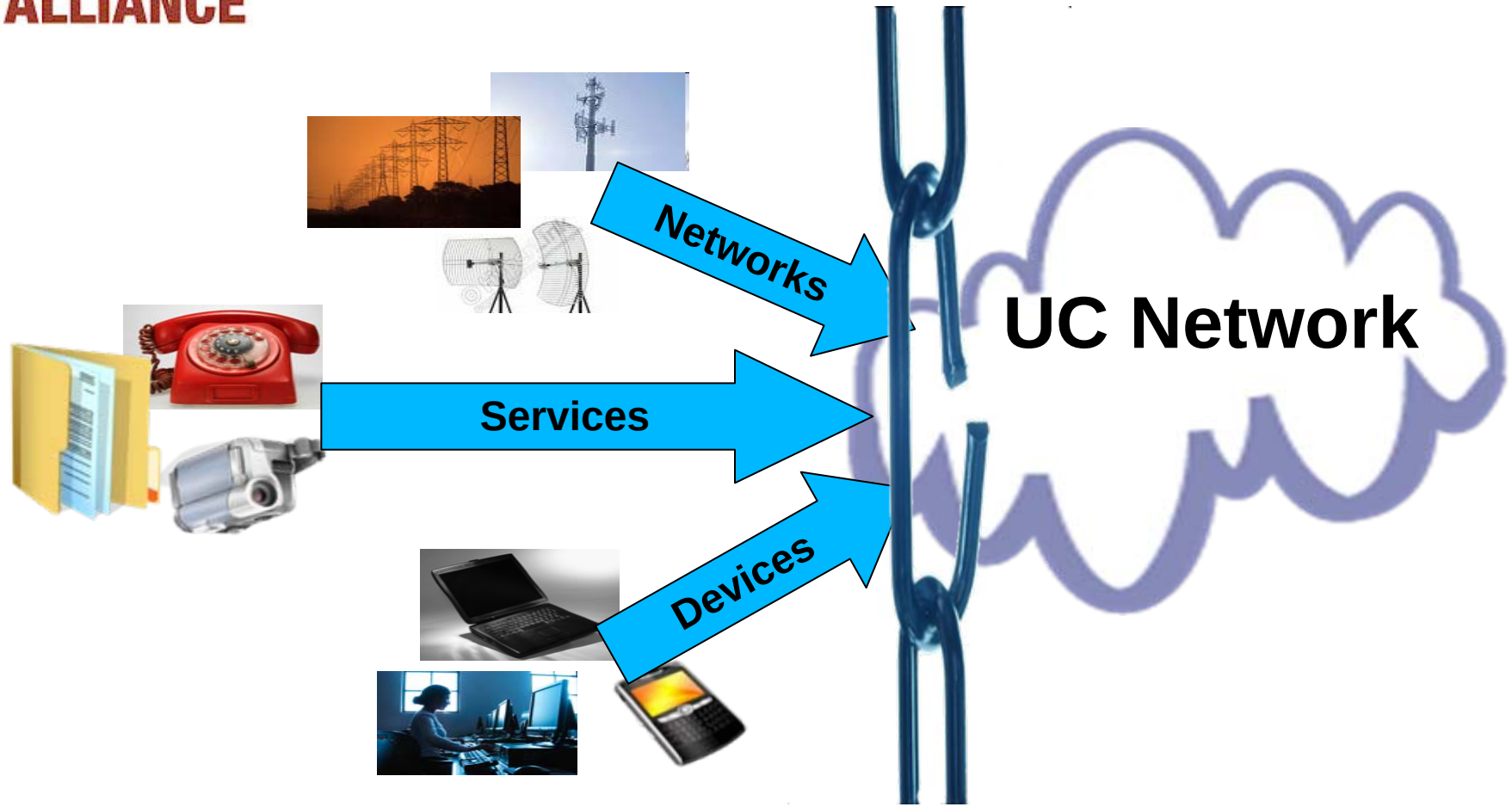
AJ West, Boeing
Alex Fielding, Ripcord Networks
Allie Larman, Oklahoma Office of State Finance
Andrew Bove, Secure Acuity Networks, LLC
Andriy Markov, VoIPshield Systems Inc.
Barry Wasser, Department of Homeland Security
Blake Frantz, Center For Internet Security
Bob Moskowitz, ICSAlabs, an Independent 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

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

The Unified Communications Challenge



INTERNET SECURITY ALLIANCE

The SCAP Challenge

SCAP Today

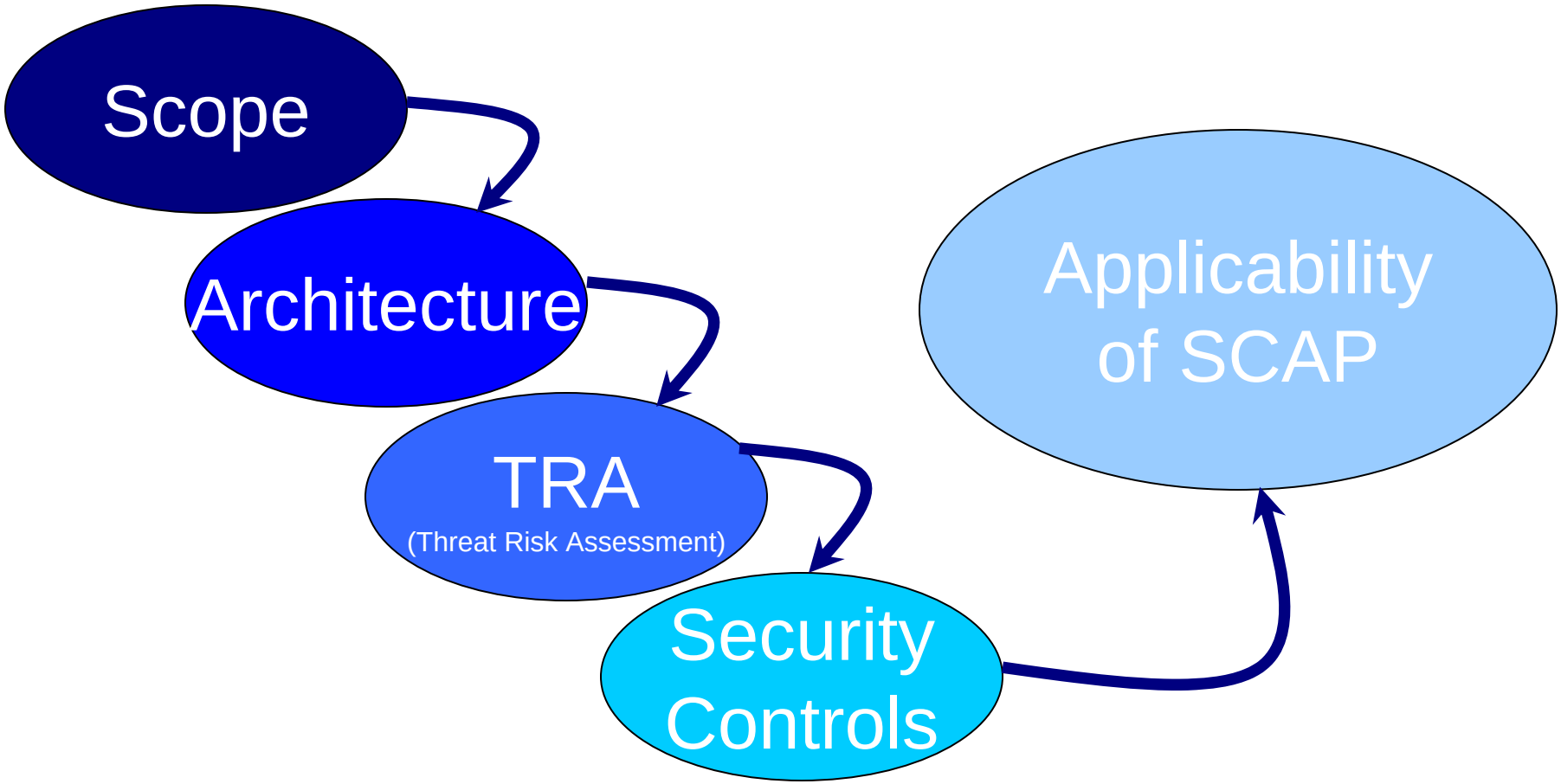
- Federal Desktop Core Configuration (FDCC)
  - One Vendor
  - Just Desktops
- Just Evaluation

SCAP Tomorrow

- Set Configuration
- More Applications
- More Vendors
- More Tools

INTERNET SECURITY ALLIANCE

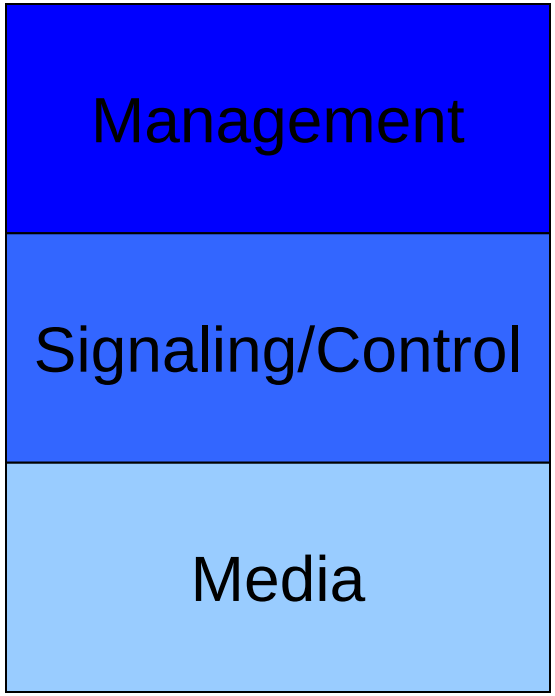
Applicability Workgroup Approach



Scope of Phase I Effort

- **Management**
  Virtual Local Area Network (VLAN's) and virtual private network (VPN's)
- **Signaling**
  Session Initiation Protocol (SIP/SIPS)
- **Media**
  Secure Real-time Transport Protocol (RTP/SRTP) [requires industry adoption]
- **Network**
  Routers, Switches, firewalls, VPNs, VLANs
  Traditional Voice Services Interconnection
- **Features**
  Voice Calls
- **User Devices**
  IP Phones, Soft phones

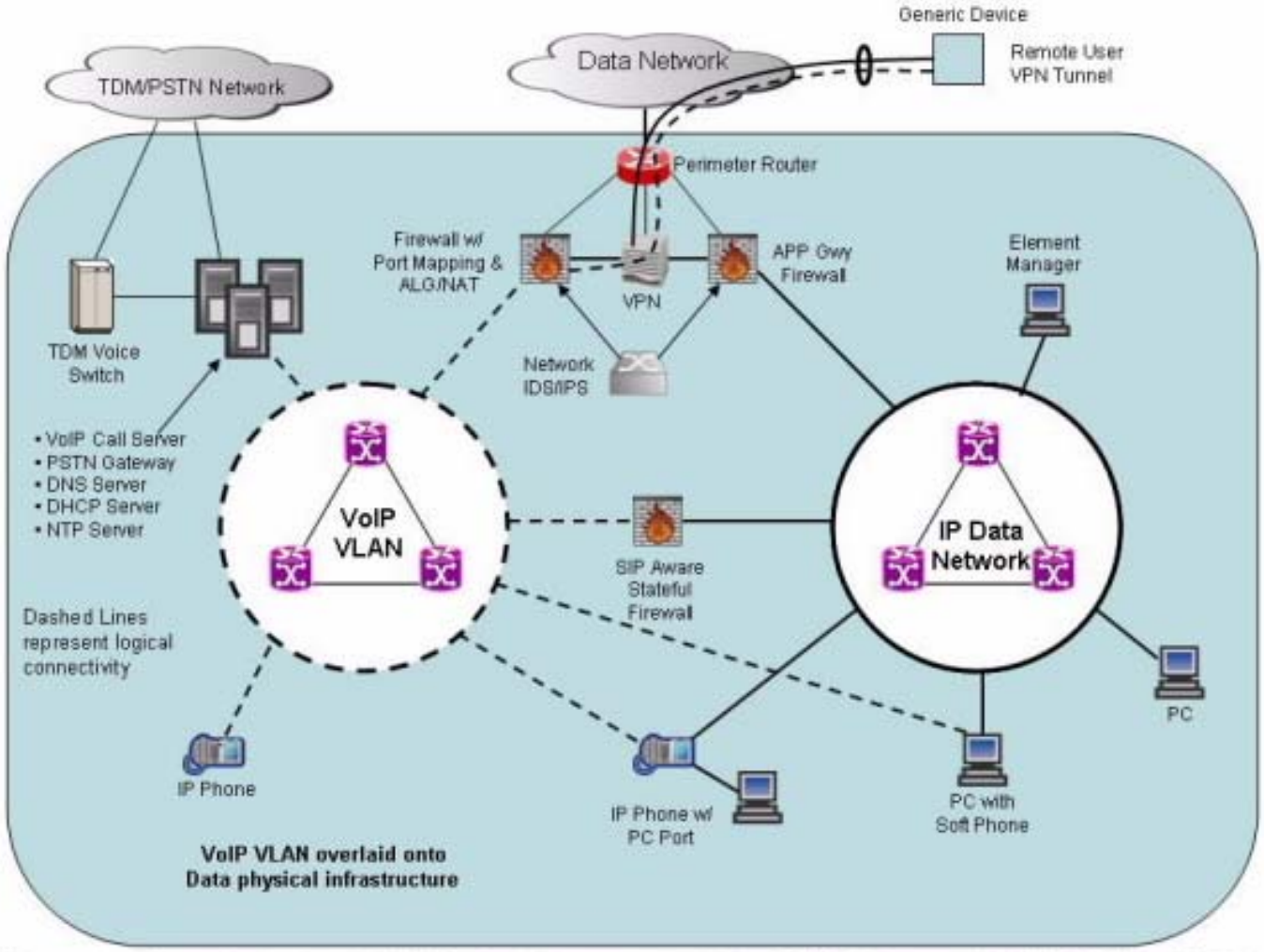
The Traffic Planes



VoIP Architecture

Legend

•Time-division multiplexing (TDM)
•Public switched telephone network (PSTN)
•Domain Name System (DNS)
•Dynamic Host Configuration Protocol (DHCP)
•Network Time Protocol (NTP)
•Implicit dynamically secured application protocols (IDSAP)
•Application-level gateway (ALG)
•Network address translation (NAT)
•Intrusion detection system (IDS)
•Intrusion prevention system (IPS)



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)

VoIP Mini-TRA: Assets

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
	Signaling	Moderate	Critical	Critical
	Management	Critical	Critical	Critical
Desktop	Operating System	Low	Moderate	Moderate
	VoIP Application (i.e., Soft phone)	Low	Moderate	Moderate
	Media	Moderate	Moderate	Critical
	Signaling	Moderate	Critical	Critical
	Management	Critical	Critical	Critical

Importance of security requirements listed are subjective and based on the requirements of the enterprise

VoIP Mini-TRA: Threat Sources & Likelihood

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

VoIP Mini-TRA: Threat Risk Score

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
	Signaling	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
	Signaling	Low	Low	Minor
	Management	Low	Medium	Minor

VoIP Security Controls: SP 800-53

Call Controller Subsystem				
Call Controller to IP Phones				
Security Function	**SP 800-53 R3 Control**	**Low**	**Moderate**	**High**
Location discovery (DNS)	SC-20	SC-20 (1)	SC-20 (1)	SC-20 (1)
	SC-21	SC-21 Not selected	Not selected	SC-21
Signaling session establishment 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
	SC-23	SC-23 Not Selected	SC-23	SC-23

Applying SCAP to VoIP

Standard	Description	Assessment
XCCDF	Extensible Configuration Checklist Description Format	OK
OVAL	Open Vulnerability and Assessment Language	Need More Device Support Need More OS Support Need More Expressiveness
CVE	Common Vulnerabilities and Exposures	OK

Applying SCAP to VoIP

Standard	Description	Assessment
CCE	Common Configuration Enumeration	No Configurations for VoIP Elements
CPE	Common Platform Enumeration	No VoIP Element Definitions
CVSS	Common Vulnerability Scoring System	OK

Other SCAP Improvements

- Need Multiple Classification Zones
- Need System View

Other Critical Success Factors

- Need Major VoIP Vendor Involvement
- Need SCAP Business Case
- Increased Collaboration/Sharing of Checklist Information (NCP)

Phase II

- ISA & NIST to Lead Effort Encouraging Vendor Participation
- Comprehensive Reference Architecture
- More VoIP Features
  - Voice Mail
  - Conferencing
  - Instant Messaging
  - Identity Management
  - Video
  - Encryption/Decryption

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

Q&A