Enterprise Security and VoIP

Dan York, CISSP
VOIPSA Best Practices Chair

VOIPSA

September 11, 2007

The Challenge of VoIP Security

VOIPSA

The Implications are Clear

Privacy

Availability

Compliance

Confidence

Mobility

Cost Avoidance

Business Continuity

© 2007 VOIPSA and Owners as Marked

VOIPSA

The Noise is Deafening

2006 COMPUTERWORLD Security

SEARCH

VOIP: Don't overlook security

Jaikumar Vijayan Today's Top Stories ▸ or Other Security Stor

SECURITY

LIGHT READING

NEWS ANALYSIS

Go to a section GO

Home > News Analysis > VOIP

Discuss Print Email License content Reprint Article

Two Charged in VOIP Hacking Scandal

JUNE 09, 2006

Discuss >

Federal authorities pressed charges Thursday against a second mar

VoIP Systems Vulnerable To Attack

By **Kevin McLaughlin**, *CRN*
3:00 PM EDT Fri. Aug. 25, 2006
From the August 28, 2006 *CRN*

VoIP is well on its way to widespread adoption, but the fact that many companies ecurity on their VoIP systems could

oing so without fully considering the applications, operating systems, and pportunity for hackers, said David h, Mass.-based 3Com and its

TECHWORLD site-wide navigation

News
Insight
How-tos
White papers
Case studies
Briefings
Interviews

Networking Storage Security Mobility & Wireless Ap

Home | News | Insight | How-tos | Whitepapers | Case studies | Interviews | Bri

Print-friendly page

July 17, 06

The security pitfalls of VoIP

ECONOMICS HAS GONE TO PEOPLE'S HEADS - AGAIN.

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publicati
800-58

Security Considerations for Voice Over IP Systems

Recommendations of the National Institute of Standards and Technology

Phishing Scams – Don't Get Hooked!

(5 Comments)

Ten tips from VoIP News to help you and your organization stay safe.

Owen Linderholm on **July 11th, 2006**

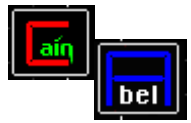
First off, what exactly is phishing? The short answer is that it is a highly successful form of scam where the crooks pretend to be a business or organization that you often interact with and then dupe you into providing real personal and financial information. They then use that information to steal identity or money from you. For more on phishing, see the VoIP News wiki and also the VoIP News VoIP Security FAQ.

Phishing scams started out with the infamous Nigerian scam emails and then evolved

VOIPSA

© 2007 VOIPSA and Owners as Marked

The security tools are out there...



Intelligent Wardialer [IWar]

PROTOS - Security Testing of Protocol Implementations

SiVuS

SIPv6 Analyzer
An Analyzer for SIP and IPv6

sipsak

SIPp

Scapy

SIPcrack - SIP login dumper/cracker

CODENOMICON

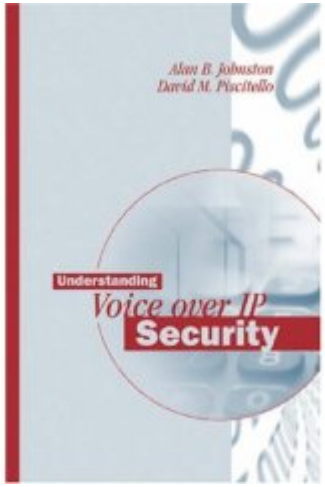
vomit - voice over misconfigured[1] internet telephones

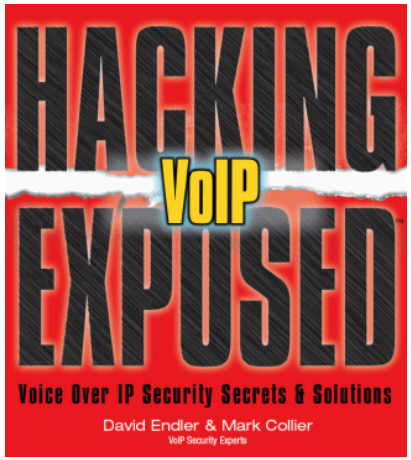
ASTEROID SIP Denial of Service Tool

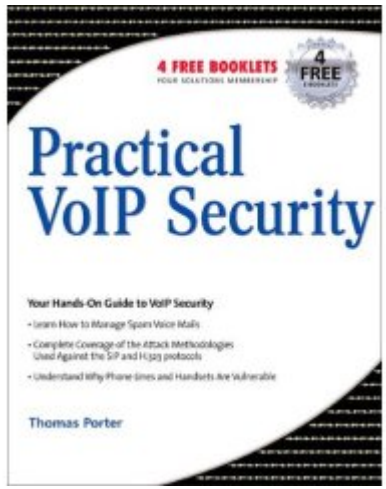
© 2007 VOIPSA and Owners as Marked

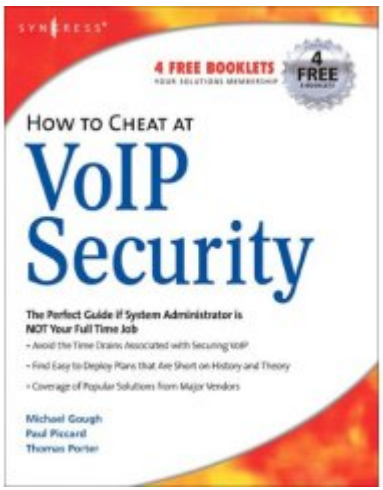
VOIPSA

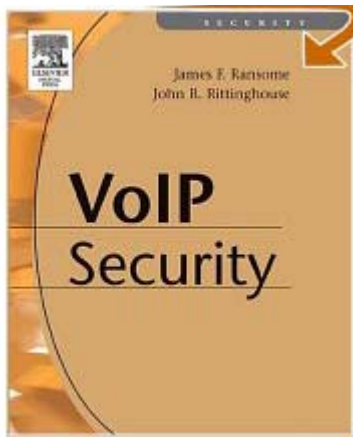
The books are now out there...







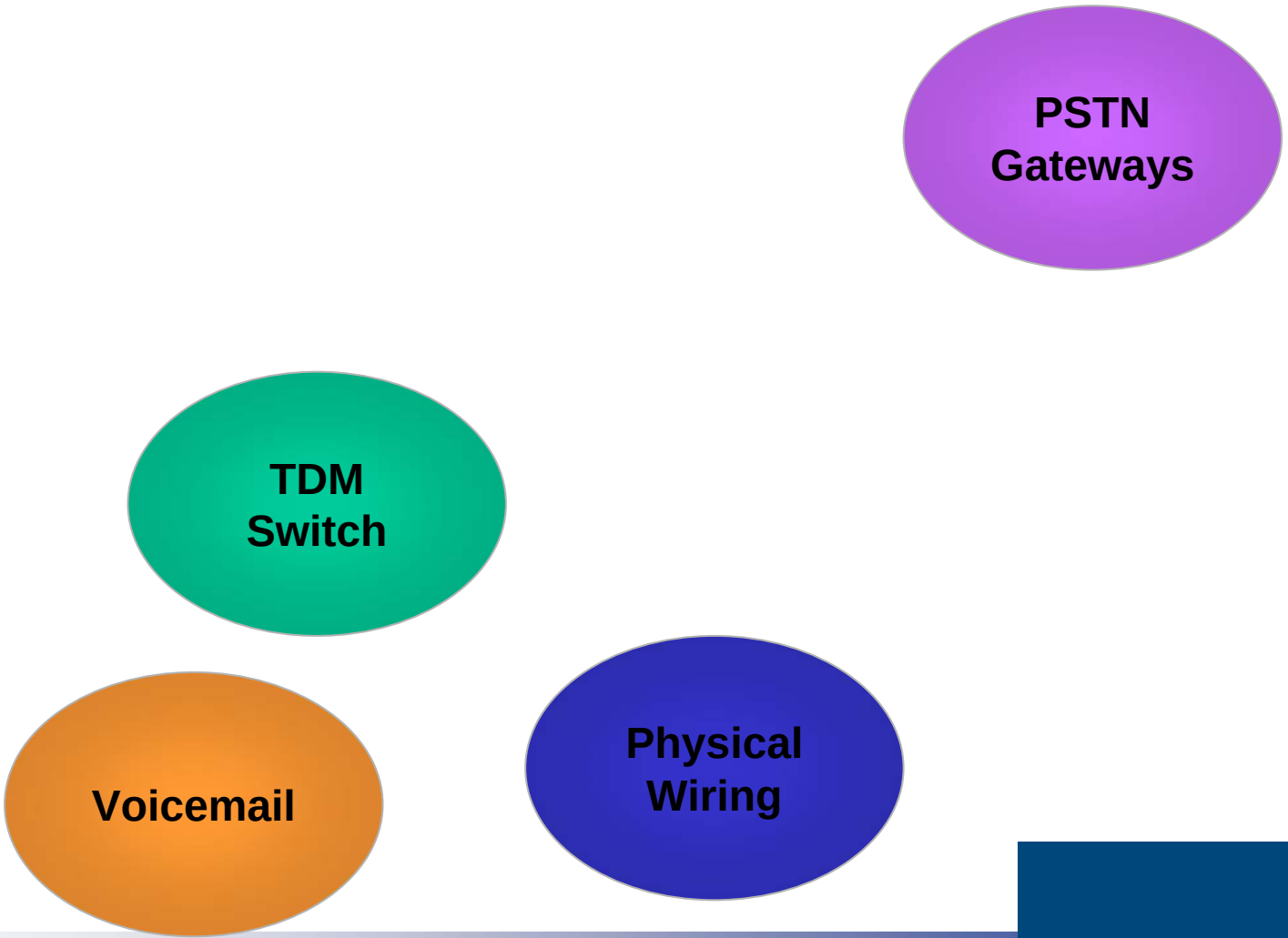




© 2007 VOIPSA and Owners as Marked

VOIPSA

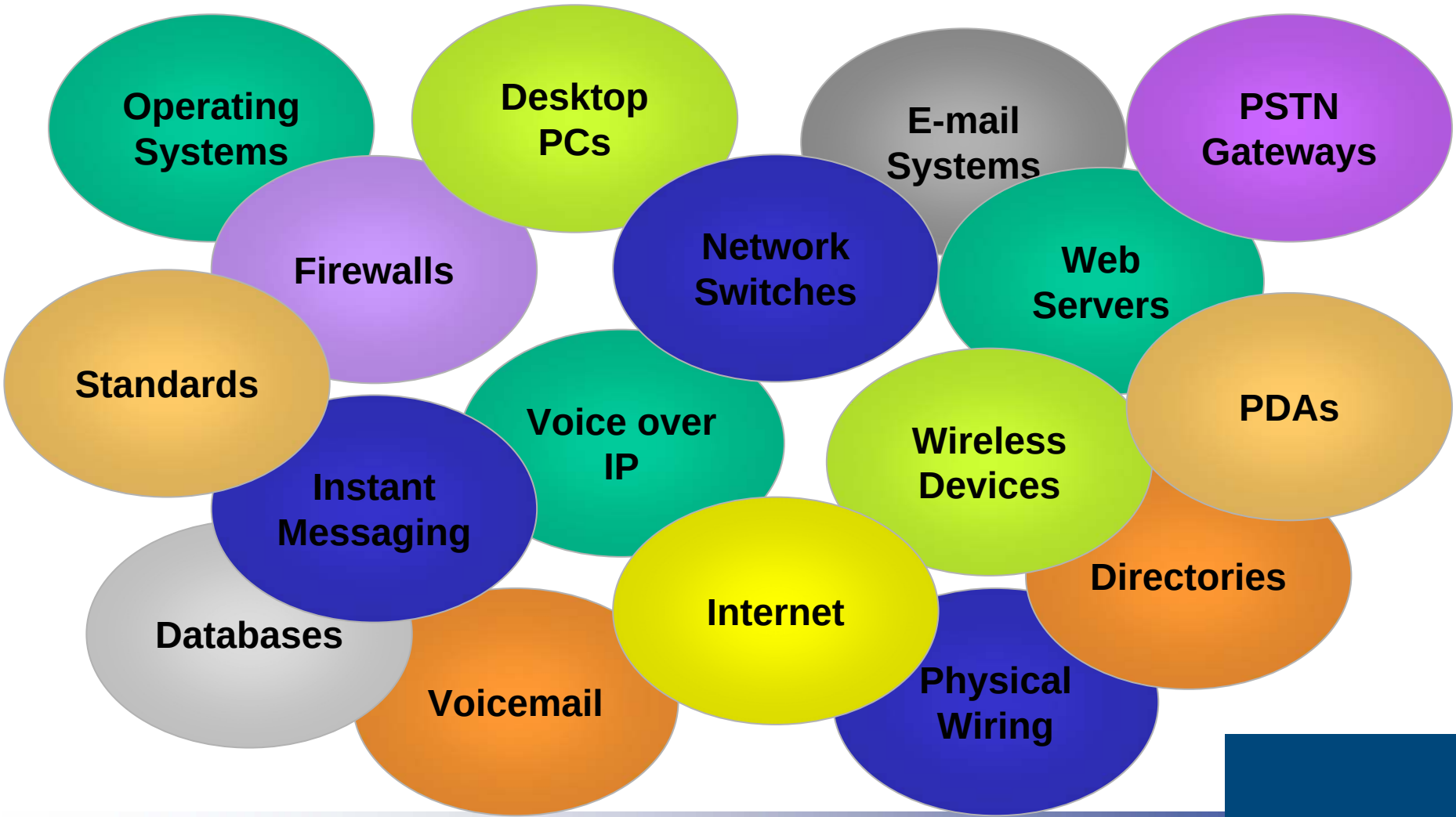
TDM security is relatively simple...



© 2007 VOIPSA and Owners as Marked

VOIPSA

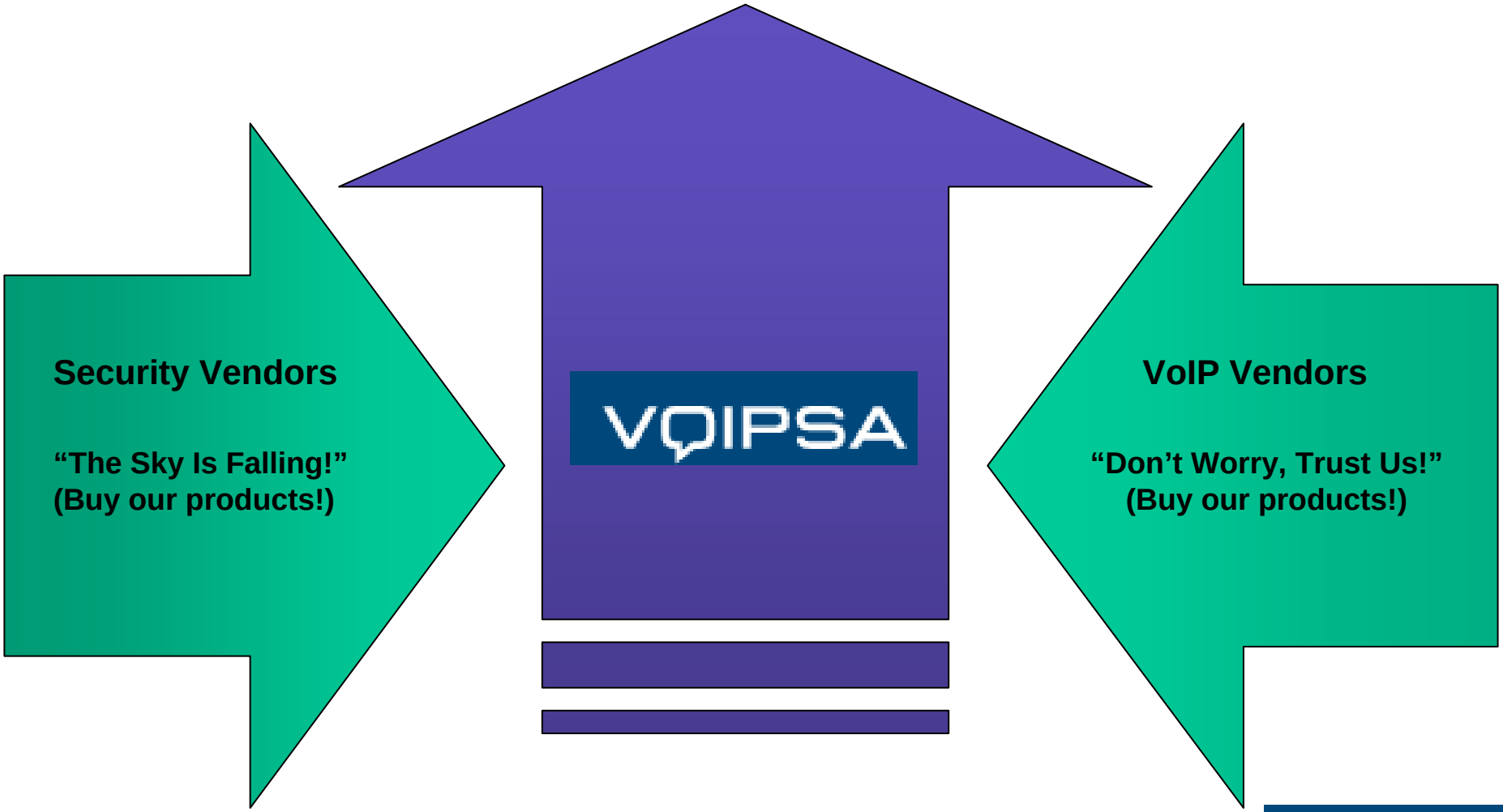
VoIP security is more complex



© 2007 VOIPSA and Owners as Marked

VOIPSA

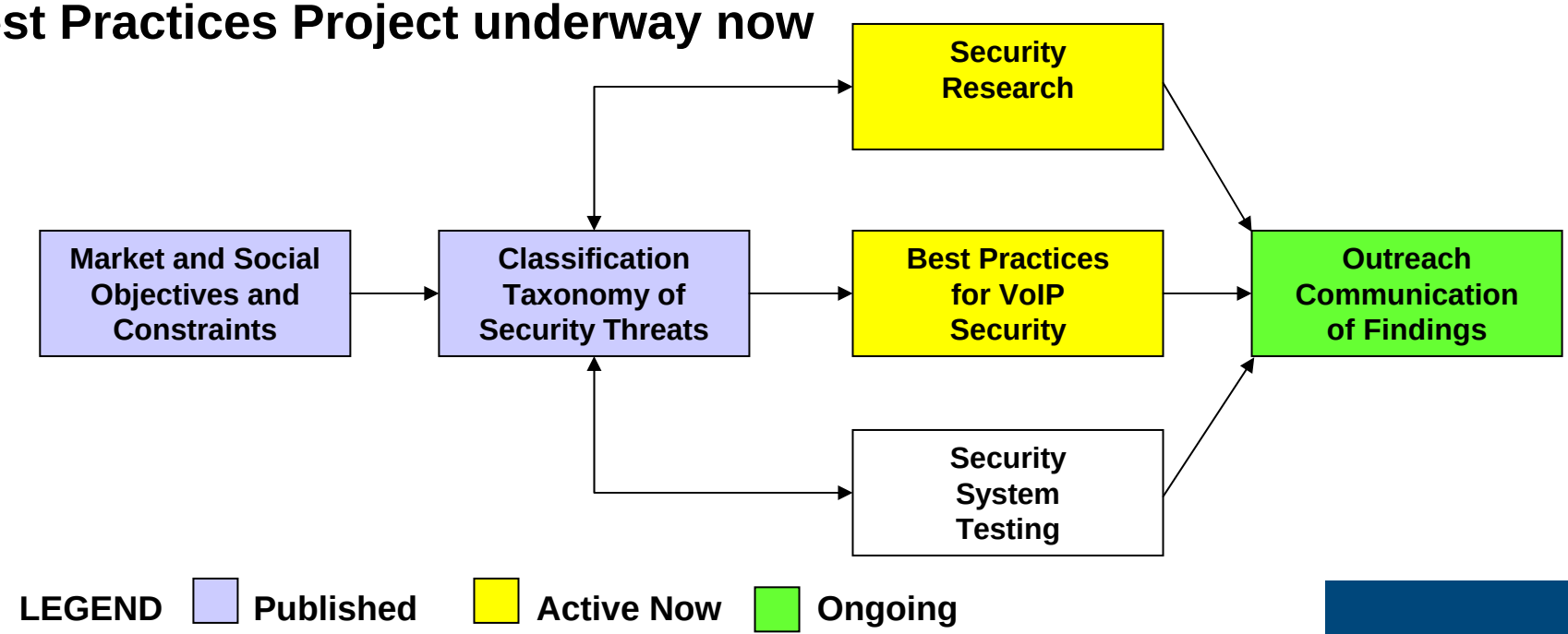
What is the Industry Doing to Help?



© 2007 VOIPSA and Owners as Marked

Voice Over IP Security Alliance (VOIPSA)

- www.voipsa.org – 100 members from VoIP and security industries
- VOIPSEC mailing list – www.voipsa.org/VOIPSEC/
- "Voice of VOIPSA" Blog – www.voipsa.org/blog
- Blue Box: The VoIP Security Podcast – www.blueboxpodcast.com
- VoIP Security Threat Taxonomy
- Best Practices Project underway now



© 2007 VOIPSA and Owners as Marked

VOIPSA

VoIP Security & Privacy

VQIPSA

Security concerns in telephony are not new…

Image courtesy of the Computer History Museum

Nor are our attempts to protect against threats…

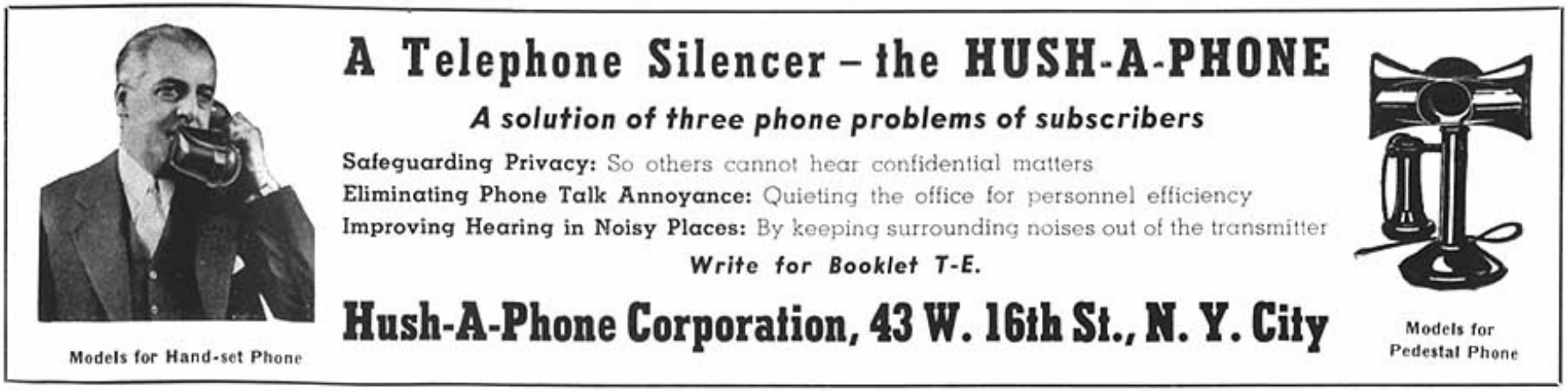


Image courtesy of Mike Sandman – http://www.sandman.com/

© 2007 VOIPSA and Owners as Marked

VOIPSA

First objective is to employ best practices and plug the obvious holes...

© 2007 VOIPSA and Owners as Marked

VOIPSA

Security Challenges … CIA

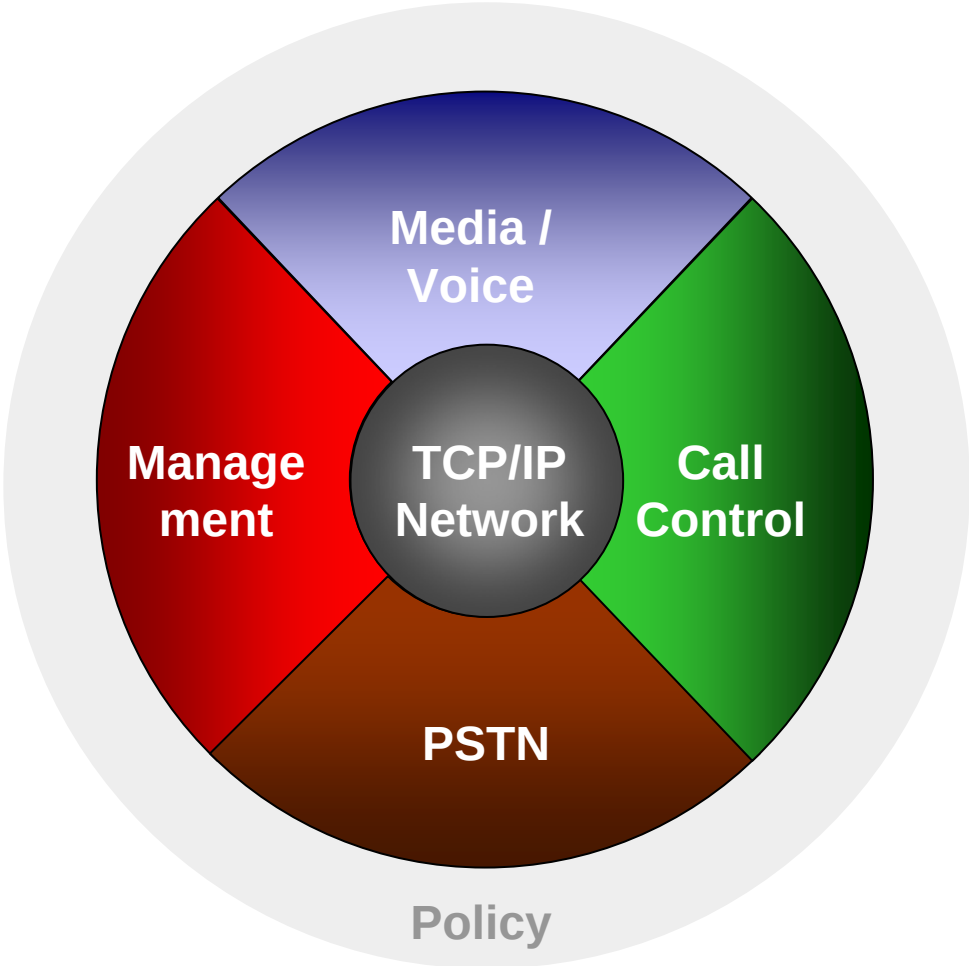
Confidentiality
Integrity
Availability

- **Confidentiality**
  - Protect the voice and data stream including call control signaling
  - Prevent eavesdropping on conversations, toll fraud, impersonation
- **Integrity**
  - Ensure that information is protected from unauthorized modification
  - Prevent discovery of a user, system or application password
- **Availability**
  - Ensure that communication services are available to users
  - Avoid any adverse effects resulting from a denial of service (DoS) attack or computer worm
- **Others**
  - Authentication
  - Authorization
  - Accounting / Audit Trail
  - Nonrepudiation

© 2007 VOIPSA and Owners as Marked

VOIPSA

Security Aspects of IP Telephony



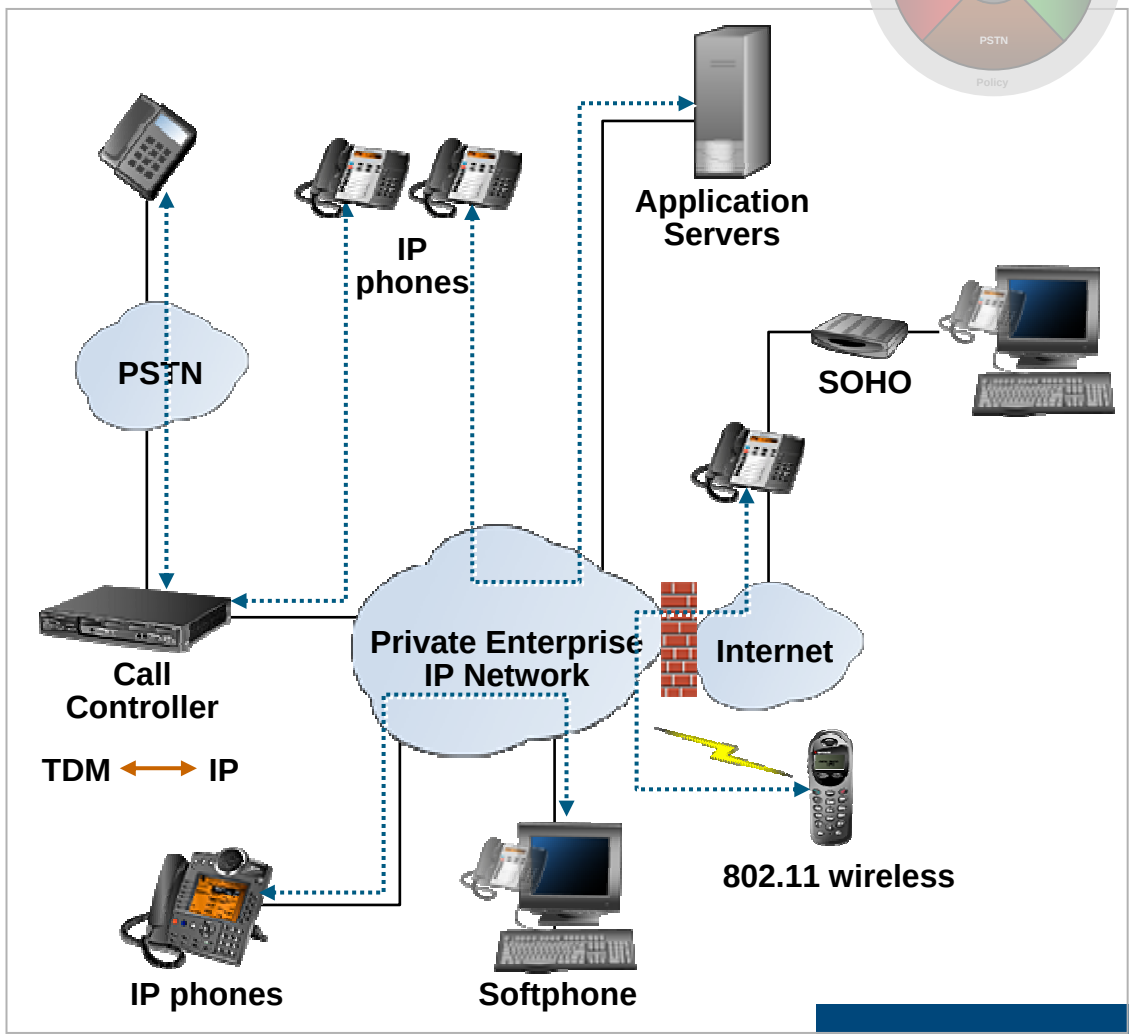
© 2007 VOIPSA and Owners as Marked

VOIPSA

The Media Path

- **Threats:**
  - Eavesdropping – particularly if over wireless or open Internet (sniffing)
  - Degraded voice quality through Denial of Service (DoS) attack

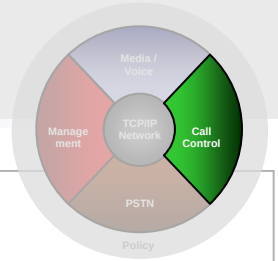
- **Defense Strategies:**
  - Encryption of voice path
  - WPA, WPA2 for wireless
  - VLANs
  - Packet filtering



© 2007 VOIPSA and Owners as Marked

VOIPSA

The Signalling Path



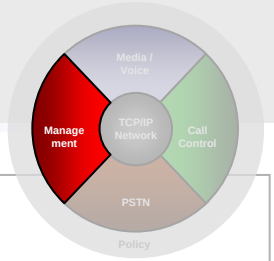
- **Threats:**
  - Denial of Service
  - Impersonation
  - Snooping account codes
  - Toll fraud

- **Defense Strategies:**
  - Signalling path encryption
  - Encrypted phone software loads
  - Proper system programming

© 2007 VOIPSA and Owners as Marked

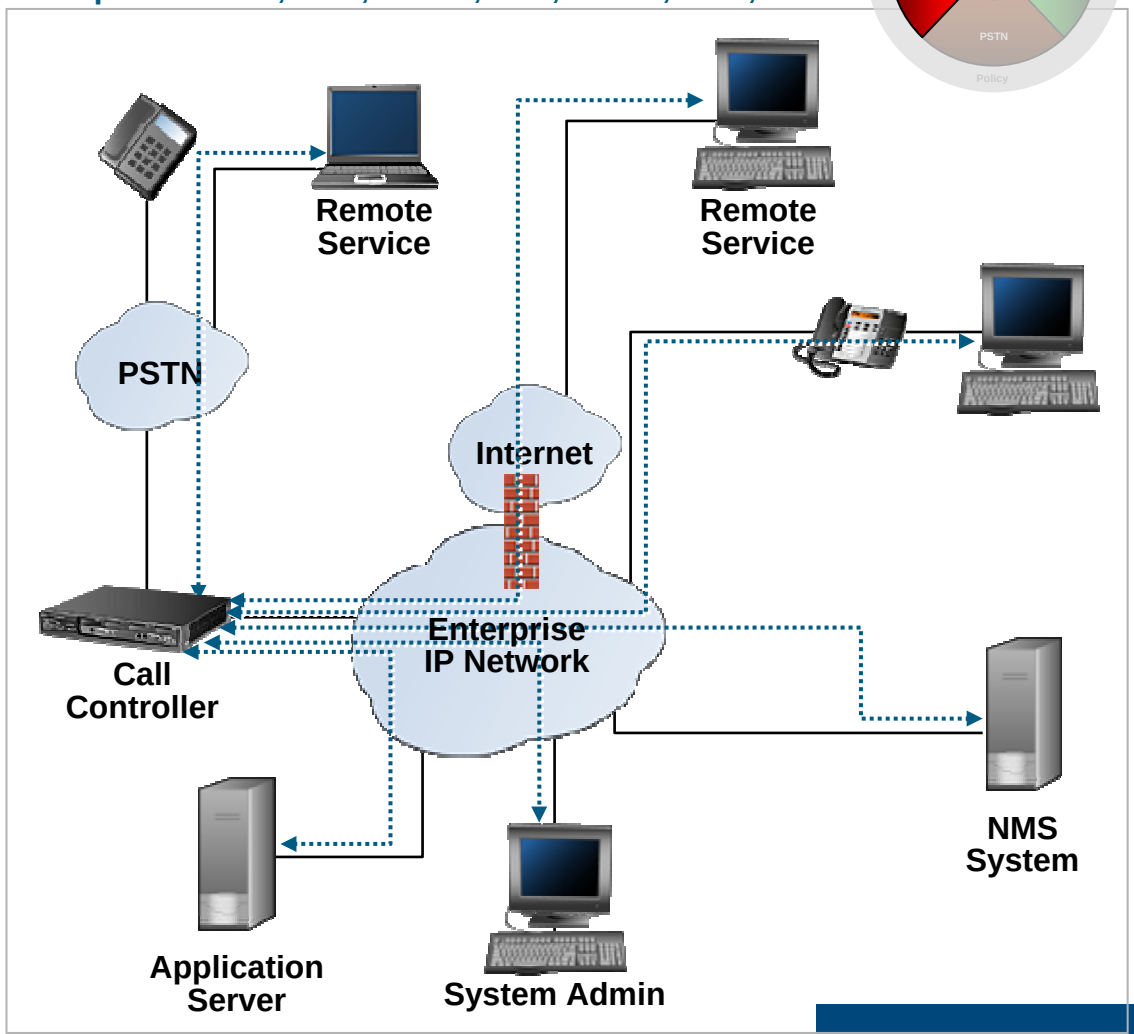
VOIPSA

The Management Path



- **Threats:**
  - Snooping passwords
  - Denial of service
  - Application Impersonation
  - Monitoring call patterns
  - Malicious system modifications

- **Defense Strategies:**
  - DoS defenses in network infrastructure
  - Changing default passwords
  - Strong password management
  - Ensure physical security
  - Authentication – secure port access
  - Secure Socket Layer (SSL)
  - Audit logs



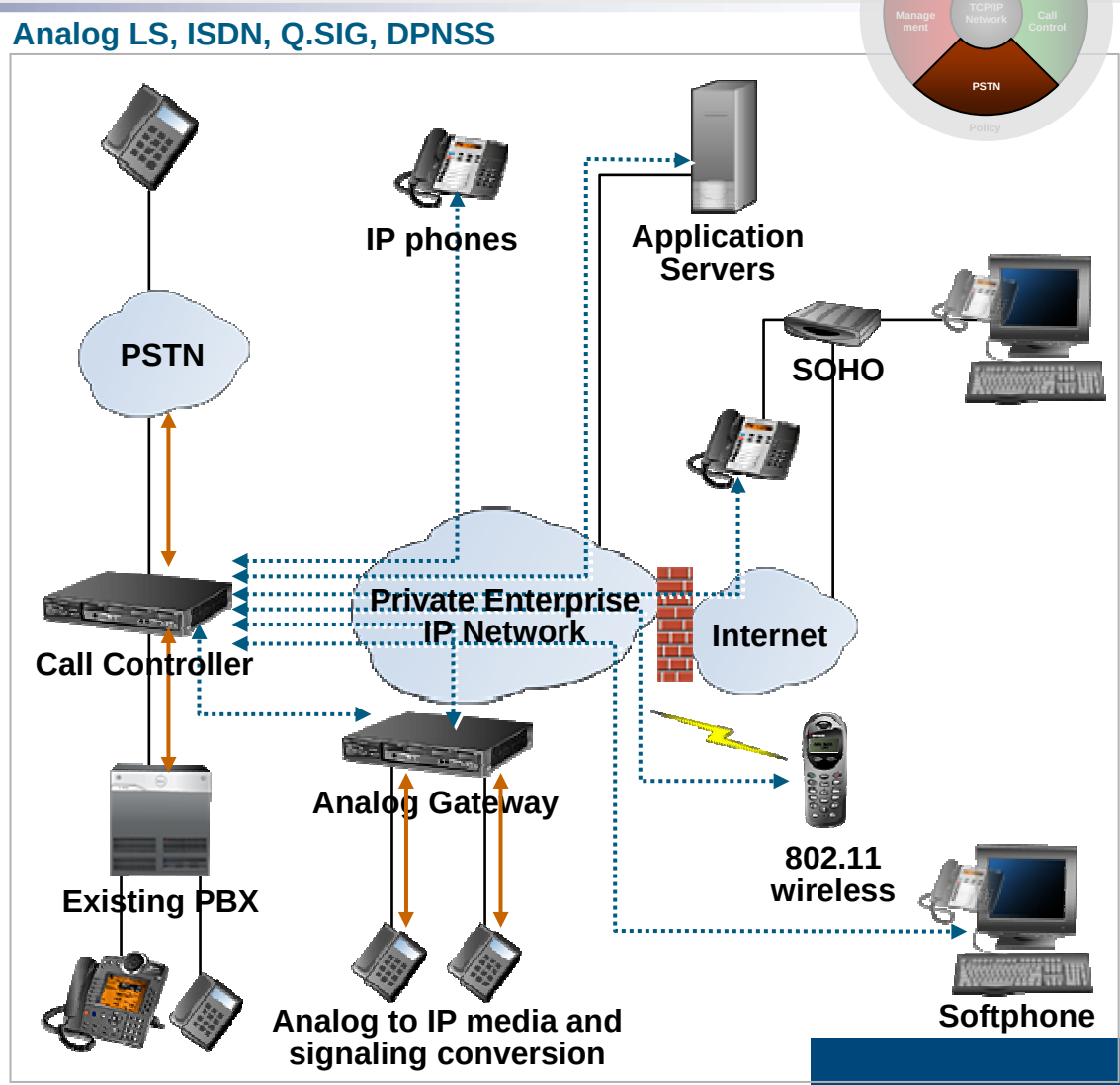
© 2007 VOIPSA and Owners as Marked

VOIPSA

PSTN and Legacy Devices

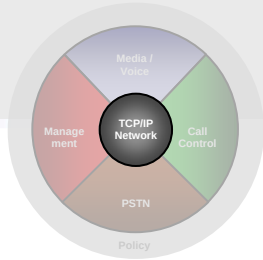
- **Threats:**
  - Toll fraud via public network attack
  - Impersonation
  - Feature access

- **Defense Strategies:**
  - Class of Restriction (COR)
  - Class of Service (COS)
  - Account Codes
  - Trunk Restrictions
  - Interconnect Restrictions



© 2007 VOIPSA and Owners as Marked

Other Best Practices



- **Network**
  - Networks should be evaluated for readiness to carry VoIP traffic.
  - Secure mechanisms should be used for traversal of firewalls.
- **Phone Sets**
  - Set software loads should be encrypted and tamper-proof.
  - Sets should run the minimum of services required.
  - Connection of a set to the system must require an initial authentication and authorization.
- **Servers**
  - Servers should be incorporated into appropriate patch management and anti-virus systems.
  - Sufficient backup power should be available to maintain operation of telephony devices (and necessary network infrastructure) in the event of a power failure.
- **Wireless**
  - All wireless devices should implement WPA and/or WPA2 versus WEP.

© 2007 VOIPSA and Owners as Marked

VOIPSA

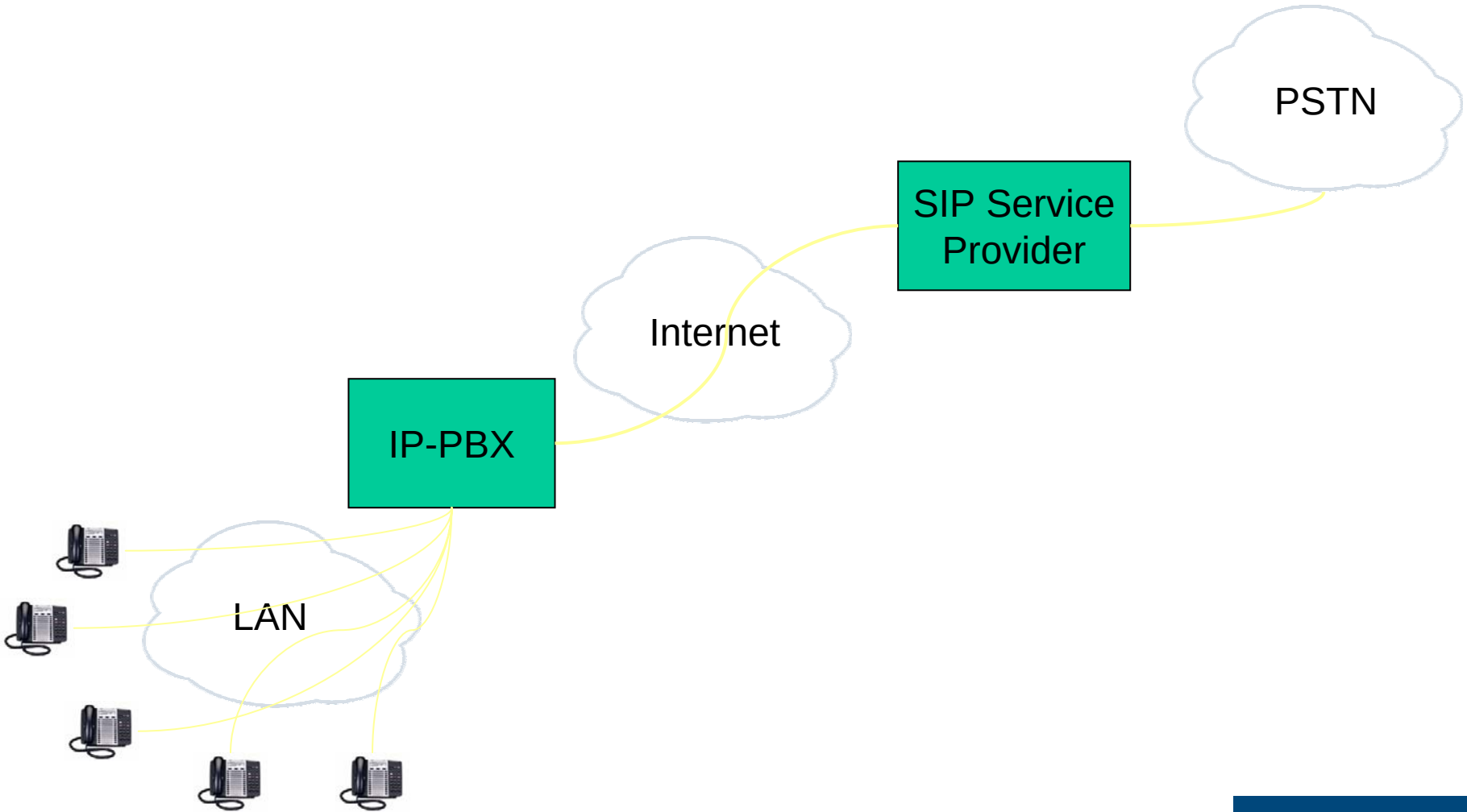
What about SPIT? ("SPam over Internet Telephony")

- **Makes for great headlines, but not *yet* a significant threat**
  Fear is script/tool that:
  1. Iterates through calling SIP addresses:
     111@sip.company.com, 112@sip.company.com, …
     Opens an audio stream if call is answered (by person or voicemail)
  2. Steals VoIP credentials and uses account to make calls
- **Reality is that today such direct connections are generally not allowed**
- **This will change as companies make greater use of SIP trunking and/or directly connect IP-PBX systems to the Internet (and allow incoming calls from any other IP endpoint)**
- **Until that time, Telemarketers have to initiate unsolicited calls through the PSTN to reach their primary market: slows them down and adds cost**

© 2007 VOIPSA and Owners as Marked

VOIPSA

The Challenge of SIP Trunking



© 2007 VOIPSA and Owners as Marked

VOIPSA

Resources

VQIPSA

Security Links

- **VoIP Security Alliance - http://www.voipsa.org**
  - Threat Taxonomy - http://www.voipsa.org/Activities/taxonomy.php
  - VOIPSEC email list - http://www.voipsa.org/VOIPSEC/
  - Weblog - http://www.voipsa.org/blog/
  - Security Tools list - http://www.voipsa.org/Resources/tools.php
  - Blue Box: The VoIP Security Podcast - http://www.blueboxpodcast.com/

- **NIST "Security Considerations for VoIP Systems"**
  - http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf
- **Network Security Tools**
  - http://www.sectools.org/
- **Hacking Exposed VoIP site and tools**
  - http://www.hackingvoip.com/

© 2007 VOIPSA and Owners as Marked

VOIPSA

Q&A

www.voipsa.org

VOIPSA

Speaker Introduction – Dan York

Dan York, CISSP, is Director of IP Technology reporting to the CTO of Mitel Corporation and focused on emerging VoIP technology and VoIP security. As chair of Mitel's Product Security Team, he coordinates the efforts of a cross-functional group to communicate both externally and internally on VoIP security issues, respond to customer inquiries related to security, investigate security vulnerability reports, and monitor security standards and trends. Previously, York served in Mitel Product Management bringing multiple products to market including Mitel's secure VoIP Teleworker Solution in 2003.

As Best Practices Chair for the VOIP Security Alliance, York leads the project to develop and document a concise set of industry-wide best practices for security VoIP systems. He is also heading up VOIPSA's move into "social media" with the launch of the Voice of VOIPSA group weblog. Additionally, York is the producer of Blue Box: The VoIP Security Podcast where each week he and co-host Jonathan Zar discuss VoIP security news and interview people involved in the field.

His writing can also be found online at his weblog, Disruptive Telephony.

© 2007 VOIPSA and Owners as Marked