netspi

RISK
COMPLIANCE
SECURITY

Reducing the risks to VoIP

- Intro
- Technologies
- Business Case
- Tools
- Threats
- Risks
- Demo
- Counter Measures
- Conclusion

Reducing the risks to VoIP Intro

- Who am I
  - David Bryan – Aka VideoMan
    - Hacker, technology enthusiast, security consultant, CISSP
      - Involved in DEFCON since 6
        - Firewall and network design as of DC10 to present
    - Brews beer
    - Bikes
    - Plays with electronics
    - Works for a Minnesota based security consulting company, NetSPI
    - dave@drstrangelove.net or david.bryan@netspi.com

Reducing the risks to VoIP Technologies

- Common Open Standards
  - SIP (Session Initiation Protocol)
  - IAX (Inter-Asterisk eXchange)
- Proprietary
  - Nortel
    - UNIstim (Unified Networks IP Stimulus)
  - Cisco
    - MGCP (Media Gateway Control Protocol)
    - SCCP (Skinny Client Control Protocol)
  - 3Com

Reducing the risks to VoIP Business Case

- Can share or use common infrastructure
- Reduces the cost of phone system deployments
  - 25 person office ~ $6-12K for full PBX deployments
  - Large enterprises
    - Trunks, MAN, WAN
- Offers additional features for little cost
  - Soft phones
  - Easier management
  - Voicemail, conference bridges, etc.
- Rapid deployment for new environments
- Overall reduced cost & ease of management

Reducing the risks to VOIP Threats

- Lack of Confidentiality
  - Allows for Eavesdropping
  - Allows for Interception
- Lack of Integrity
  - Session hi-jacking
  - Session replay attacks
- Lack of Availability
  - Prone to denial of service conditions
  - Weak protocol stacks
  - 911

Reducing the risks to VoIP Tools

- Unistimpy
- Vomit
- Cain and Abel
- Sipvicious
- VoIP Hopper
- Sipsak
- SIPp
- RTP Inject
- Etc, etc, etc.

Reducing the risks to VoIP Risks

- Phone calls getting dropped
- Endpoints being attacked, rebooted
- Bogus voice data
- Forged or intercepted calls
- Loss of confidentiality

Reducing the risks to VoIP Main reason?

- Lack of secure transport methods
- Lack of good authentication methods
- Lack of nonrepudation

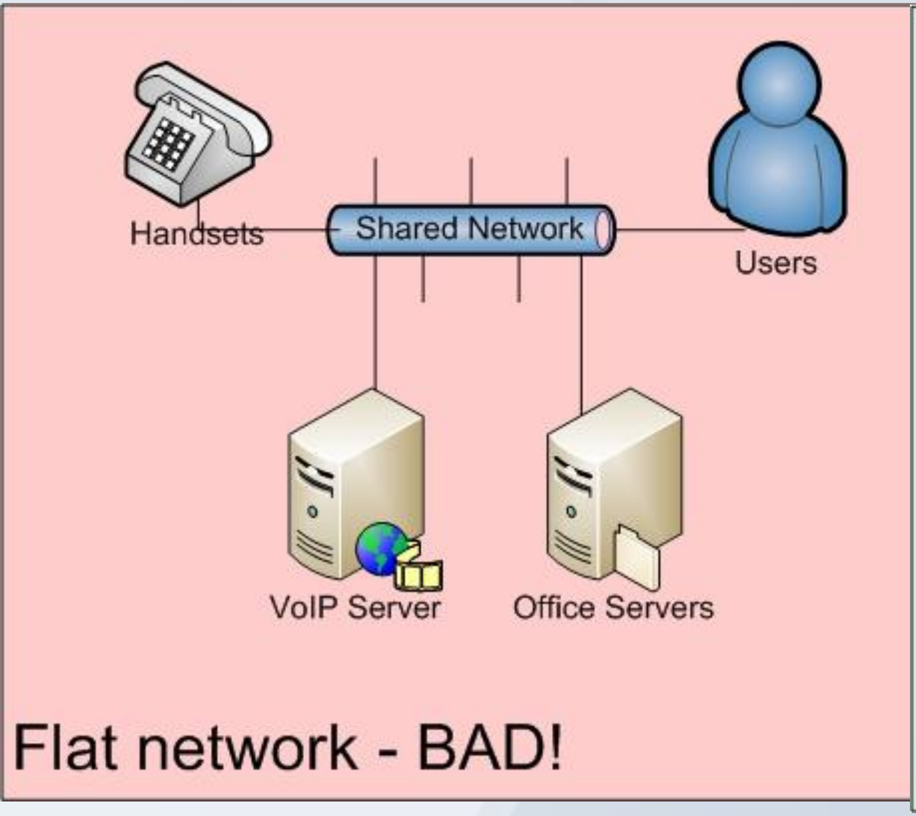
Reducing the risks to VoIP Demo

- Demo
  - Inject
  - Reboot
  - ?

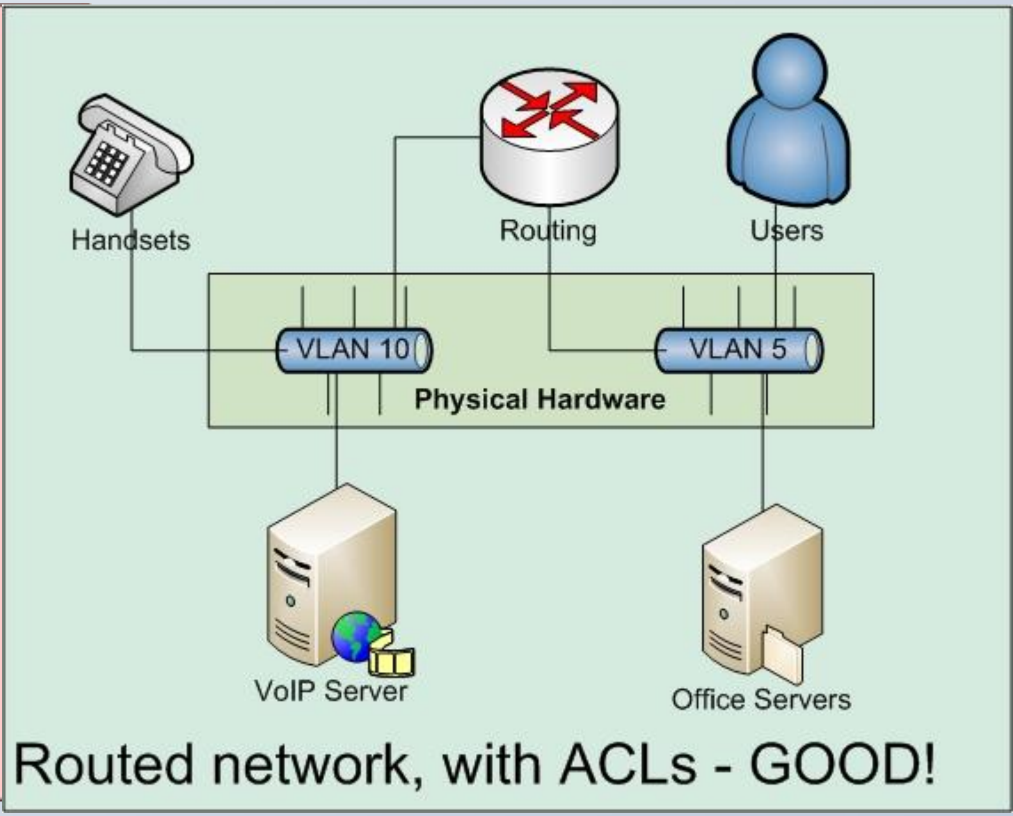
Reducing the risks to VoIP Counter Measures

- VLANs and Router ACLs
- Quality Of Service (QOS)
- Network Access Control (NAC)
- Secure SIP (TLS) and Secure Real Time Protocol (SRTP)
- Zfone and ZRTP
- Skype – Just kidding! Proprietary.

Reducing the risks to VoIP Topologies

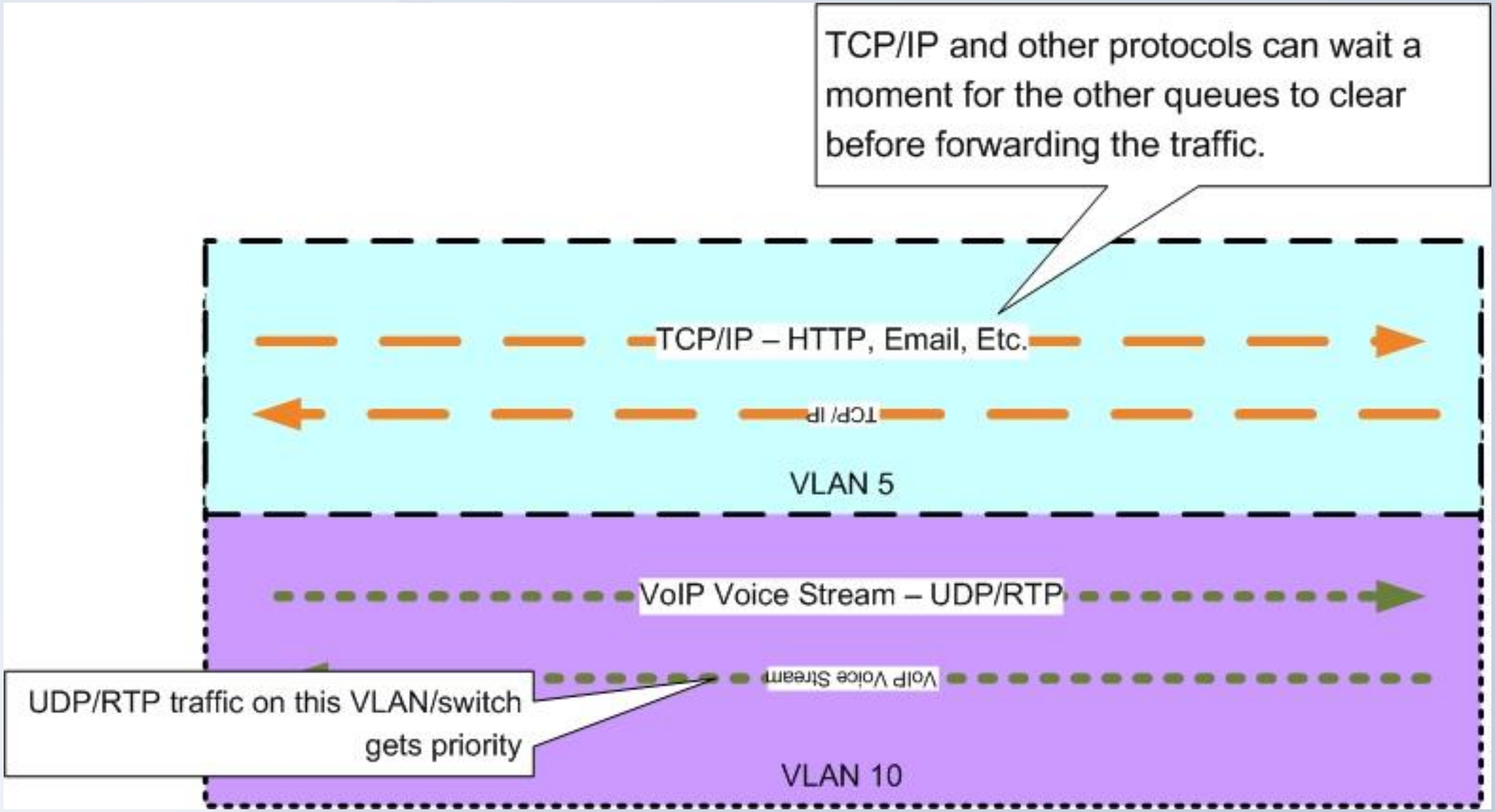


Flat network - BAD!



Routed network, with ACLs - GOOD!

Reducing the risks to VoIP 802.1q and QOS



TCP/IP and other protocols can wait a moment for the other queues to clear before forwarding the traffic.

UDP/RTP traffic on this VLAN/switch gets priority

Reducing the risks to VoIP Conclusion

- VoIP - Little to no security!
  - Great for reducing the costs to business.
  - No so good for privacy, availability, or integrity
  - Requires compensating controls for deployment.

Reducing the risks to VoIP Thanks to…

- LayerOne, Noid, Evil.
- NetSPI
- HBIC - aka Heather my wife.

Reducing the risks to VoIP Image References

http://www.pbase.com/benjiu/20050625_japan

http://tokyo.dualisanoob.com/images/first_fone.jpg

http://birdhouse.org/blog/wp-content/uploads/2006/04/tapped.jpg

http://www.crookedtimbre.net/static/telstra%20kiosk.jpg