RSA CONFERENCE 2006

Defending Voice over IP Networks

Rodney Thayer,
Canola & Jones,
02/13/06 - Session Code: TUT-031

Introduction

What this Tutorial is about

- VoIP (Voice over IP)
- Telephony
- Network Defense
- Studying attacks
- No exploits released

Contents

- Three “blocks” – 0900-1045, 1100-1245, 1400-1545

1. Intro; modern telephone networks; data network integration
2. Voice network threats
3. Defending voice networks
4. Impact of policy enforcement
5. Impact of voice/data convergence
6. Future threats

Administrivia

- Registration
- Use of cell phones, net, etc,
- Facilities, coat check, etc.
- Feedback forms

Introductions

Who's Rodney?

Introductions

Who are you?

Telephony in the Modern Era

circa 2006

How it was in the old days

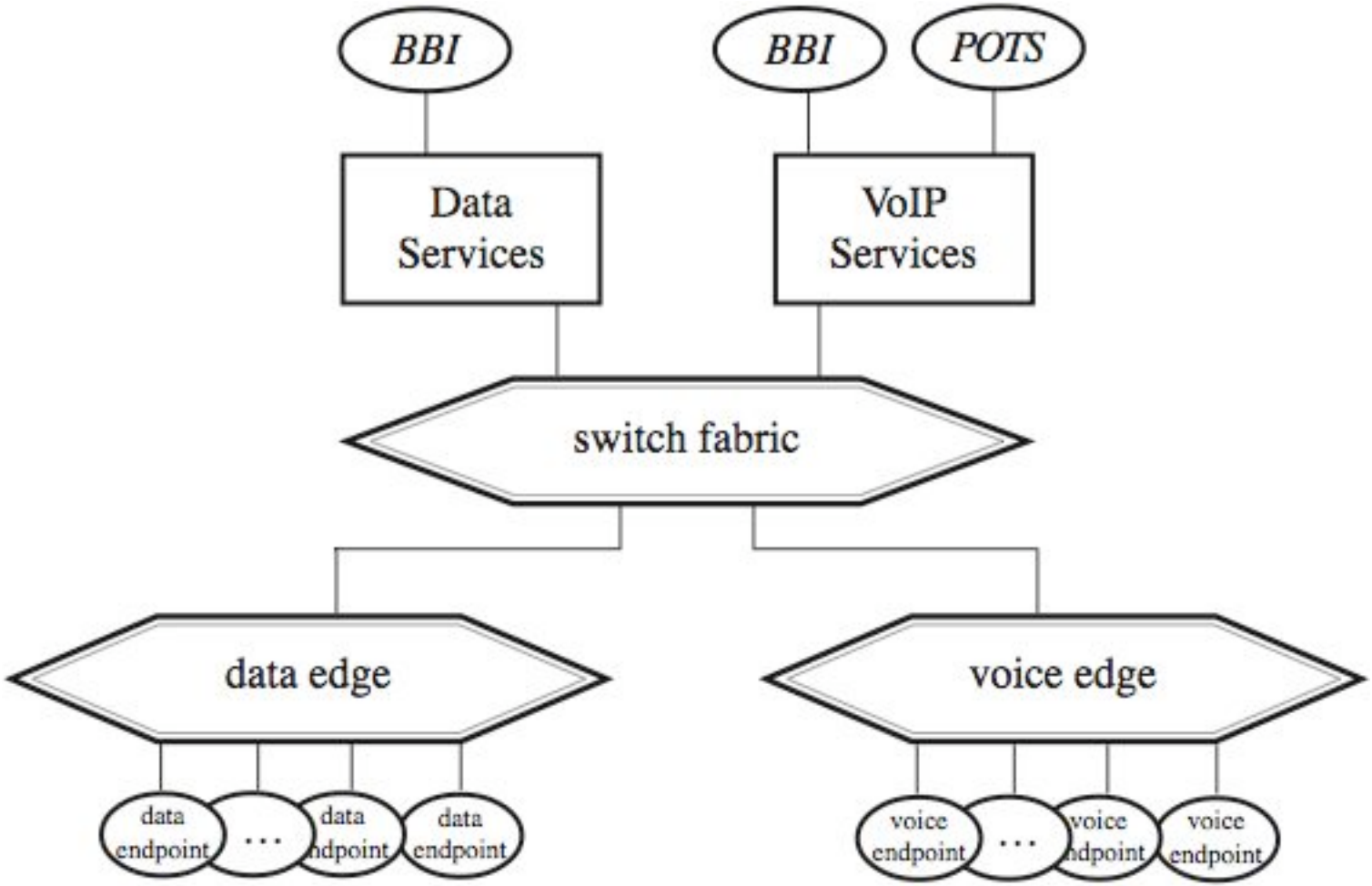
- Old school telco gear: analog phones, analog infrastructure
- Legacy (formerly hot, now old and crufty) digital telco gear
- Voice was really data (since 1957)
- Proprietary protocols
- Closed networks (operated by closed minds)
- Security by obscurity
- Hub-and-spoke technology with central control

The way things are now

- Voice *IS* data
- The telephone network *IS* the Internet
- The streams have been crossed: voice in data, data in phone calls
- The tools have merged: computers are phones and phones are computers
- Phone hackers and computer hackers are the same thing

Crossing the streams: voice joins the networking world

- First we had data networks: email, web, chat, office automation, data processing
- Then we added more media traffic, including video and audio and telephone calls
- We added enterprise telephony services (not just phone calls)
- Now the worlds are intertwined: directories, voice mail with data attachments, merged network traffic, merged or equivalent infrastructure
- *The attack surfaces are now intertwined too.*


BBI
BBI
POTS
Data Services
VoIP Services
switch fabric
data edge
voice edge
data endpoint
data endpoint
data endpoint
voice endpoint
voice endpoint
voice endpoint

Voice Network Threats

"Shiny. Let's be bad guys."

An attacker's view of a phone system

- As a tool
- As a target
- As a vector

Attacker's view of a phone system: As a tool

- Mis-use of the system
- Theft of services
- Malicious use: illegal, pornography, threats
- Graffitti target: defacement
- SPAM target
- *No software or hardware compromise needed for it to be useful*

An attacker's view of a phone system: As a target

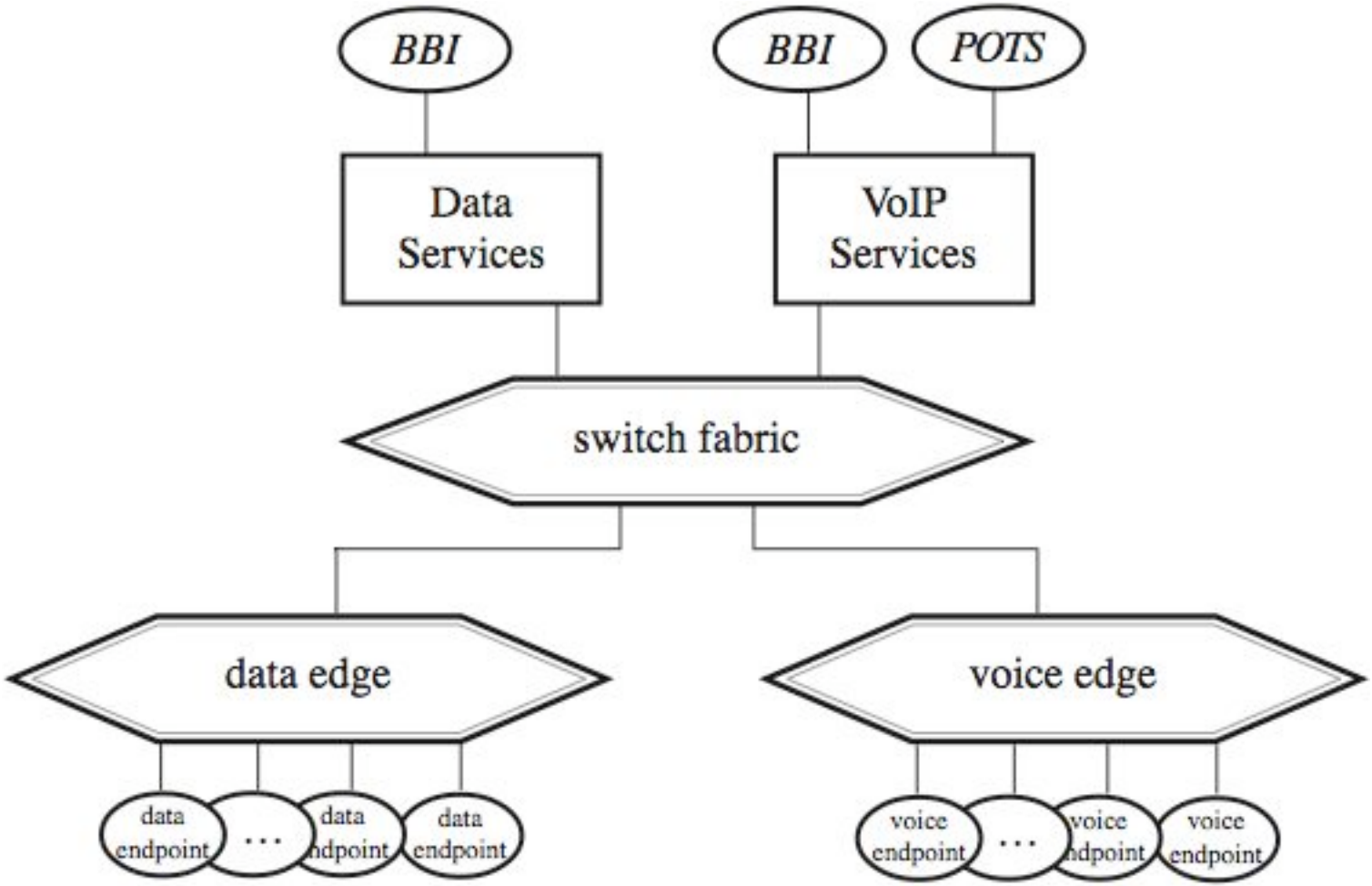
- Wire tapping
- Con games
- Physical Asset value
- Denial of Service attacks
- Business Process attacks

An attacker's view of a phone system: As a vector

- A vector: a path to attack something else
- Part of the enterprise network infrastructure
- Part of the public network infrastructure
- Target is interconnected so all nodes have value

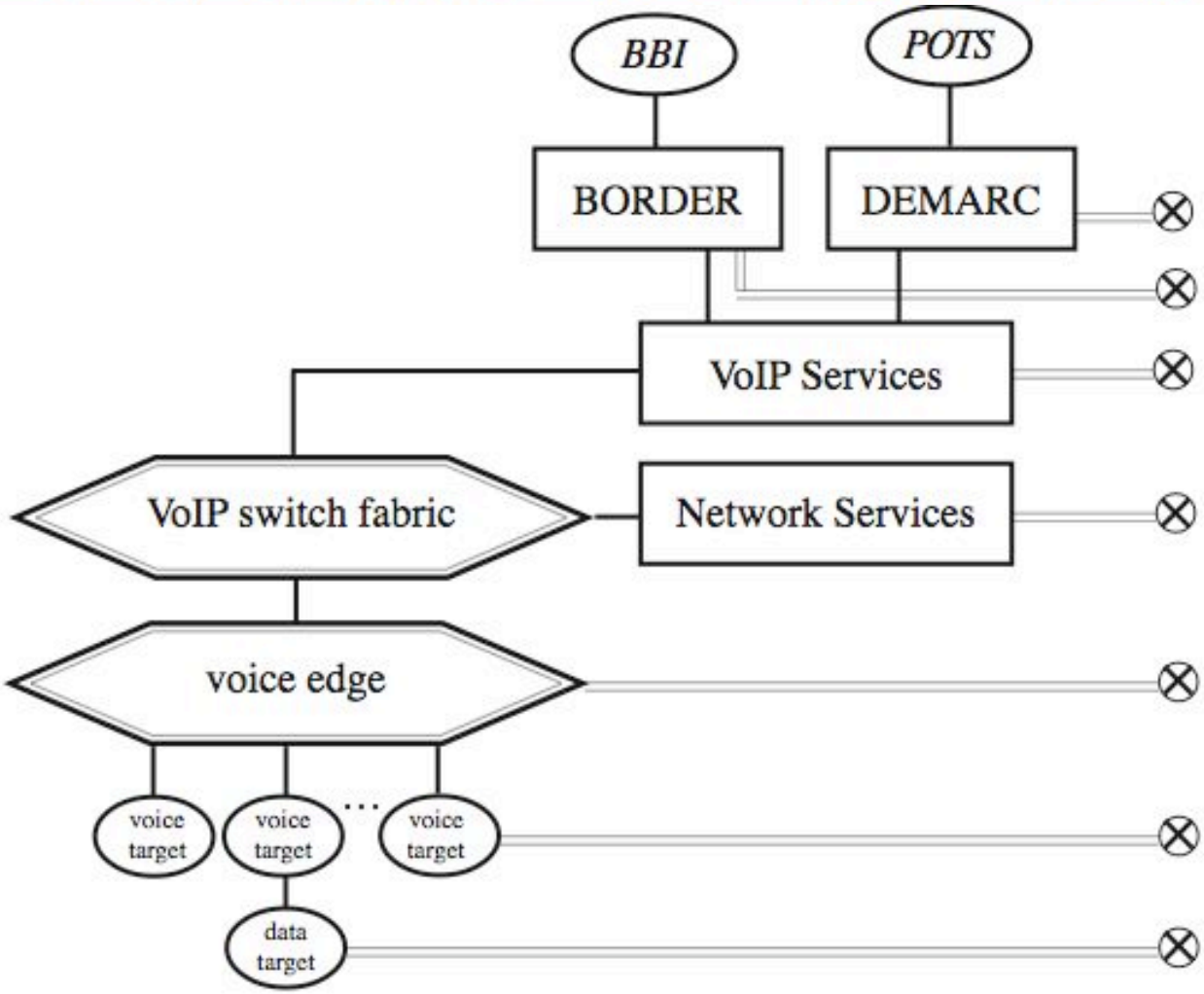
VoIP Network Targets

So many targets, so little time…


BBI
BBI
POTS
Data Services
VoIP Services
switch fabric
data edge
voice edge
data endpoint
data endpoint
data endpoint
voice endpoint
voice endpoint
voice endpoint

VoIP components as targets

- Management infrastructure
- Instruments
- Core services
- Dedicated infrastructure
- Shared infrastructure


BBI
POTS
BORDER
DEMARC
VoIP Services
VoIP switch fabric
Network Services
voice edge
voice target
voice target
voice target
data target

VoIP components as targets: Management Infrastructure

- Probably no logging
- Web UI flaws
- Management network segregation flaws
- Built for phone-heads, not network folk
- Security by obscurity as an implementation strategy

VoIP components as targets: Instruments

- It's a $30 box with a full IP protocol stack.
- Mis-optimized: fashion, cost per unit, physical reliability, minimal functionality
- Not resilience, management instrumentation
- Complete functionality
- Designed to leak information
- Not designed to be a secure endpoint
- Fully functional network peer
- Typically poorly monitored, as a network device

VoIP components as targets: Core services

- A “call manager” of some sort
- Gateway stuff, to get to POTS/outside world
- Bandwidth feed into network (core)
- Traditional telephony core services:
- Directory
- Call accounting
- Telephone usage policy enforcement

VoIP components as targets: Core services (more)

- Data interconnect to data network services
- Conventional servers, effectively stand-alone
- Strong telephony maintenance
- Weak network maintenance

VoIP components as targets: Dedicated infrastructure

- Switches
- Wiring
- VLANs
- Parallel data network
- “Parallel” management infrastructure
- Siloed staff

VoIP components as targets: Shared infrastructure

External:

- Shared data trunks
- Shared core/edge network gear
- Shared services infrastructure (hvac, power, physical)

VoIP components as targets: Shared infrastructure

Internal:

- Avoid better instrumentation, management
- Increased attack surface of data network
- More heterogeneous use of data network means easier to hide
- Soft phones: just another weakness in the desktop

VoIP components as targets: Conclusions

- Phones are likely to be weak.
- Phone software likely to be weak
- Infrastructure likely to be poorly defended
- Promising path into data network

Defending VoIP

"Trust but verify."

"Security is *hard*."

“First do no harm.”

Defending VoIP: Overview

- Voice system and staff
- New, different, complicated gear
- Different paths in and out
- Different suppliers and resources
- Voice vendor solutions
- Network vendor solutions
- Process solutions

Defending VoIP: Options

- Hardening
- Instrumentation
- Maintenance
- Passive defenses
- Active defenses

Defending VoIP: Hardening

- Fixed interconnect is safer than flexible interconnect.
- Tight binding of instruments to infrastructure
- Strict control of data flow
- Conventional core service defenses
- “Conventional” infrastructure defenses
- Treat phones as endpoints, apply endpoint security strategies.

Defending VoIP: Instrumentation

- It's a network. It needs logging.
- Integrated event management for all nodes
- 'Logging' means network logging, not call logging.
- Instrument core services too (especially directories)

Defending VoIP: Maintenance

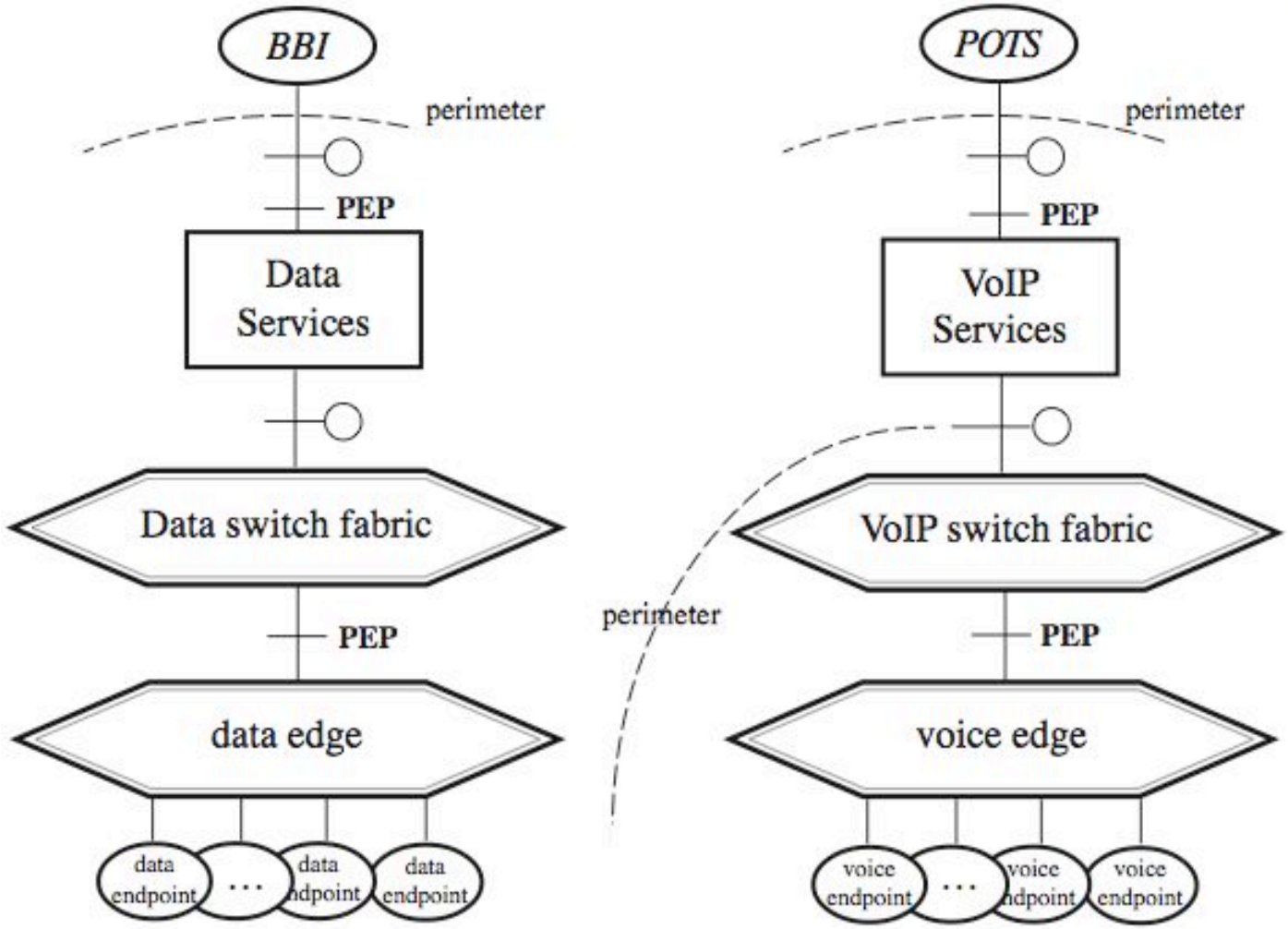
- All equipment should be maintained just like network gear.
- Ask for “windows update” for phones.
- Maintenance processes are now a superset of (voice, data) processes.
- Processes should reflect that voice is part of your data network.

Defending VoIP: Passive Defenses

- Firewalls (Data and VoIP)
- IDS (Data and VoIP)
- Event monitoring
- (Standard data network defenses)

Defending VoIP: Active Defenses

- Intrusion Prevention
- Access controls
- Segregated networks
- Standards
- (Standard data network defenses)
- Policies, e.g. endpoints are expendable
- Policy enforcement points


BBI
perimeter
PEP
Data Services
Data switch fabric
PEP
data edge
data endpoint
data endpoint
data endpoint
POTS
perimeter
PEP
VoIP Services
VoIP switch fabric
PEP
voice edge
voice endpoint
voice endpoint
voice endpoint
perimeter

VoIP Policy Enforcement

Policy Enforcement for VoIP

- Phones are computers.
- Phones are nodes on the network.
- Network policy enforcement should be balanced to work.
- Therefore, policy enforcement should be applied to phones.

Policy Enforcement for VoIP: Options

- 802.1X/etc. for soft phone PC's
- 'Thick' phones with security features
- NIST Opinions
- Update policies
- Integrated policy enforcement

Convergence

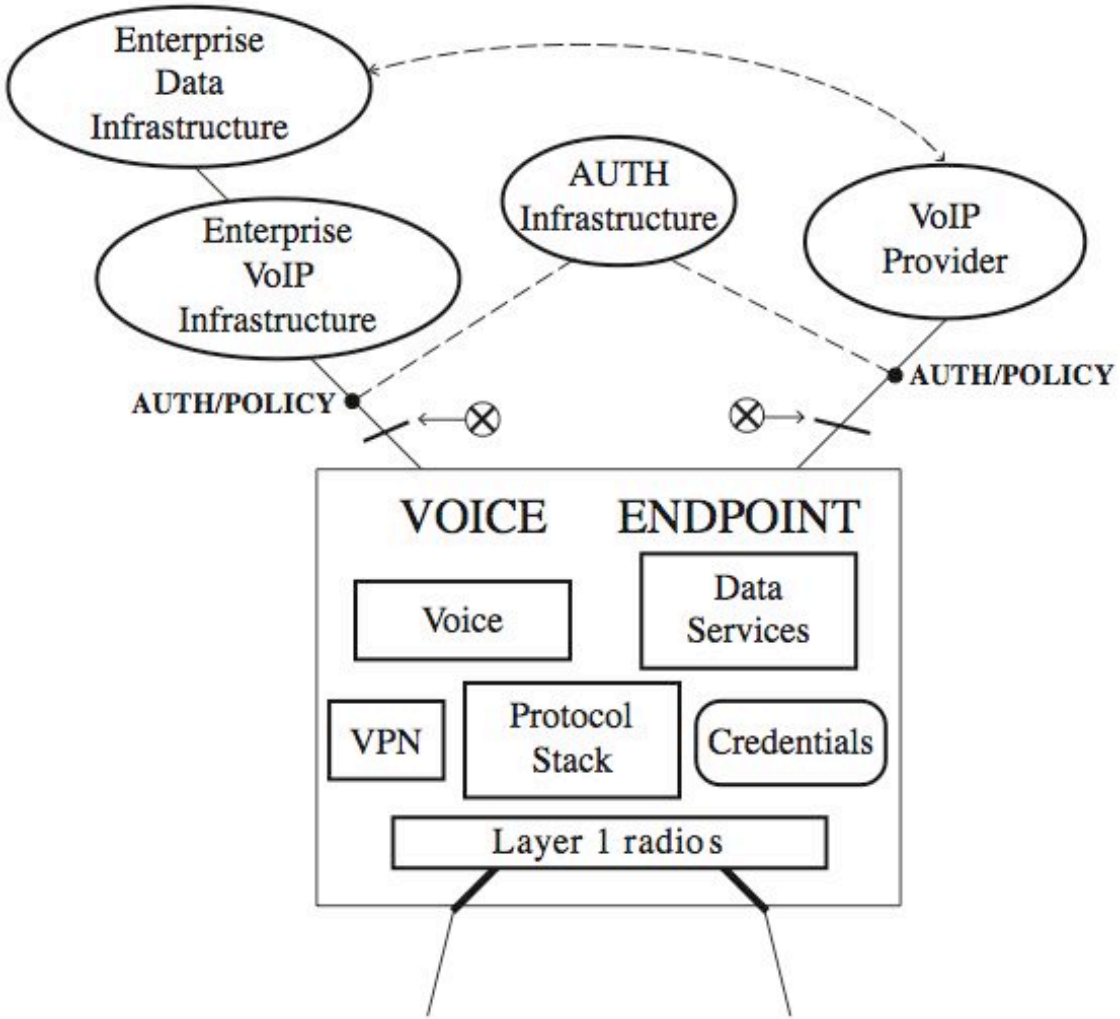
What happens when you cross the streams?

Convergence: Definition

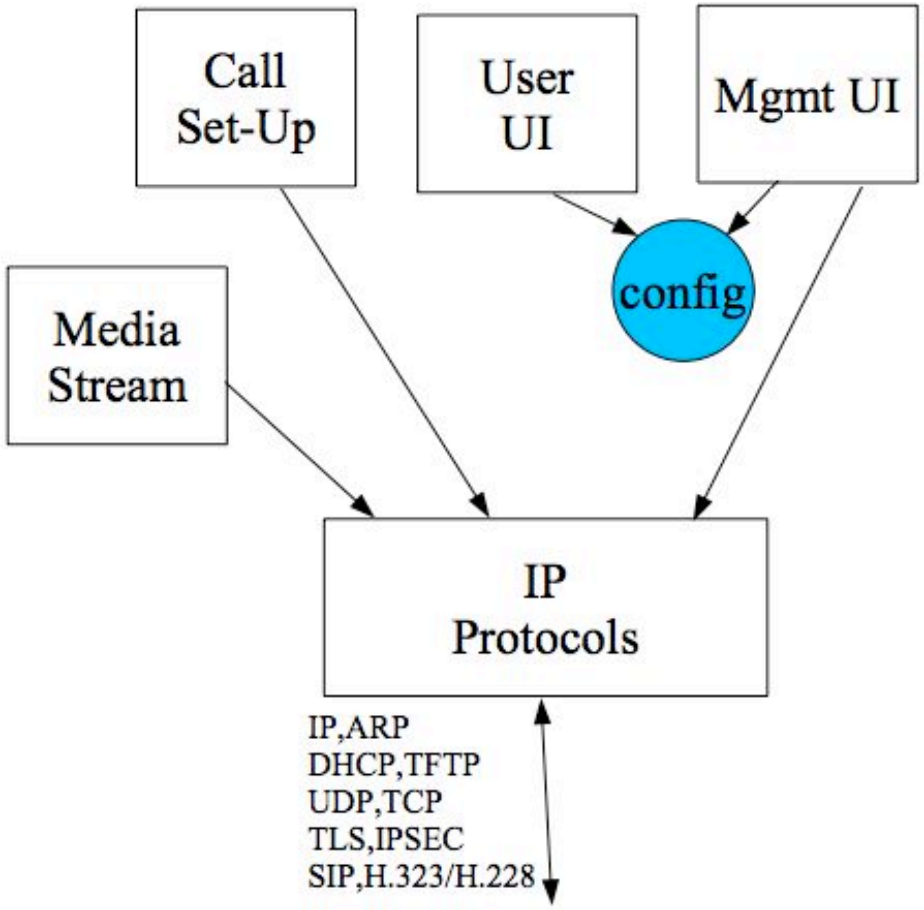
- Wireless everywhere
- 802.11 and GSM are just two kinds of radios.
- All phones are mobile phones.
- Phones are thick clients with rich services.
- *Some vendor is going to talk you into doing a forklift upgrade.*

Convergence: Issues

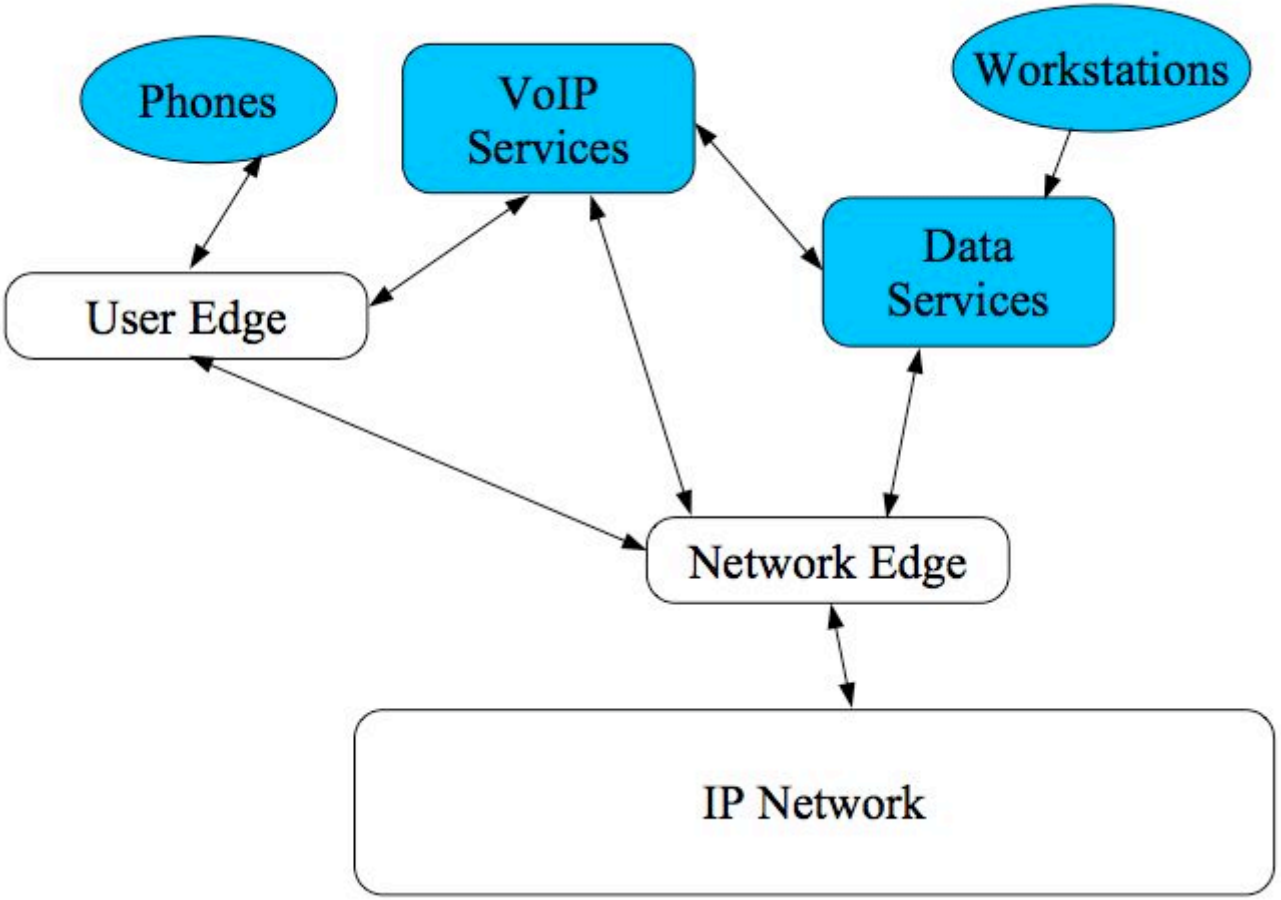
- How's all that authentication work?
- Do all those radios really work?
- Rich services means large attack surface.
- Phone vendor mentality does not yield reliable products.


Enterprise
Data
Infrastructure
AUTH
Infrastructure
VoIP
Provider
Enterprise
VoIP
Infrastructure
AUTH/POLICY
AUTH/POLICY
VOICE ENDPOINT
Voice
Data
Services
VPN
Protocol
Stack
Credentials
Layer 1 radios

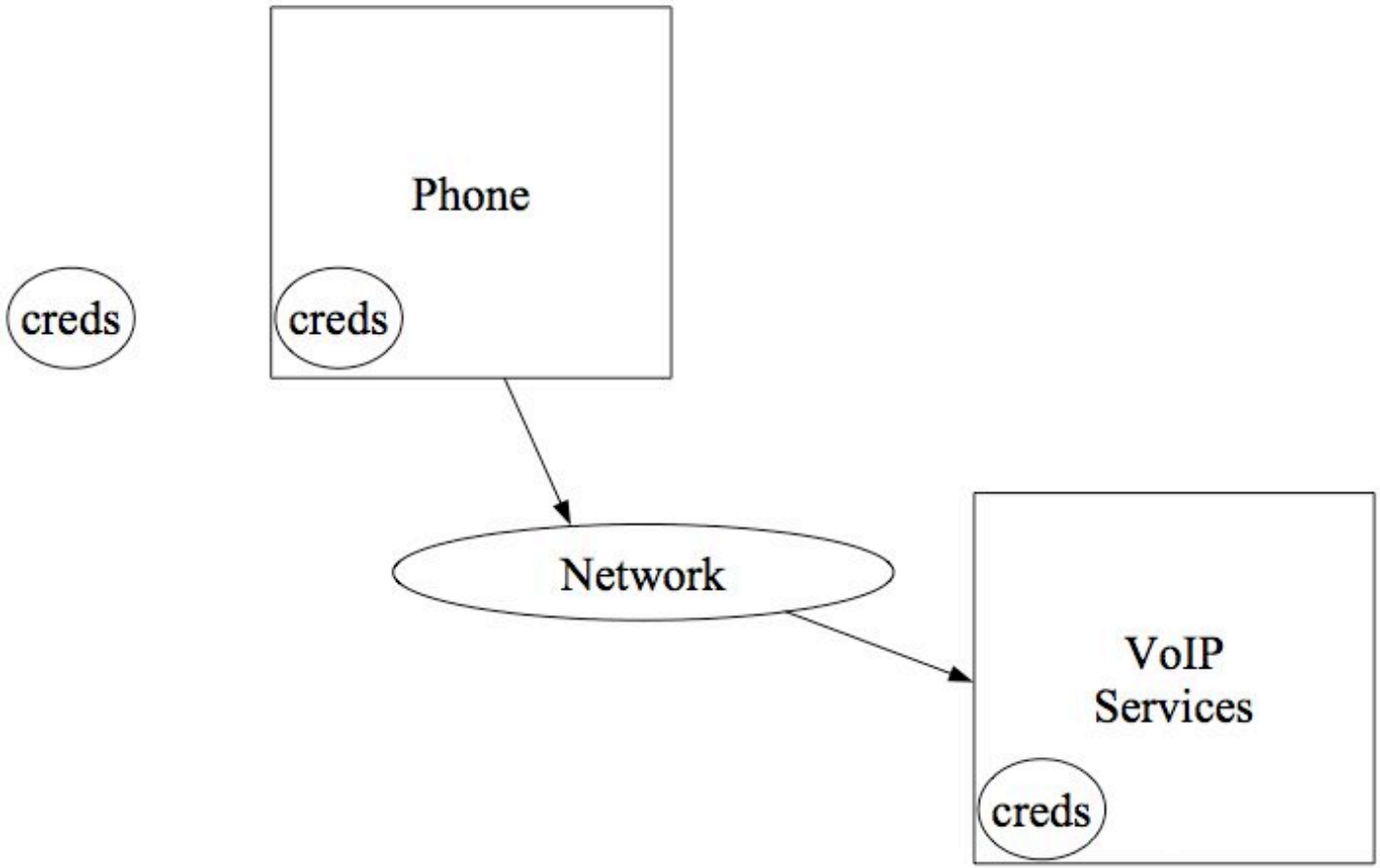
Phone Attack/Defense



Infrastructure Attack/Defense



Access Attack/Defense



Conclusions

Defending VoIP: Conclusions

- VoIP networks are viable targets. Be afraid.
- You can defend a VoIP network. Don't be cheap about it.
- Sexy features trump secure implementations in the marketplace.
- The current state of the art tends to produce vulnerable targets.
- Push your vendors for solutions: patch management, reliable phones, defendable voice systems.

RSA CONFERENCE 2006

Rodney Thayer

rodney@canola-jones.com

Canola & Jones

Internet Investigations