VoIP Vulnerability Futures

Rodney Thayer

TSC Labs

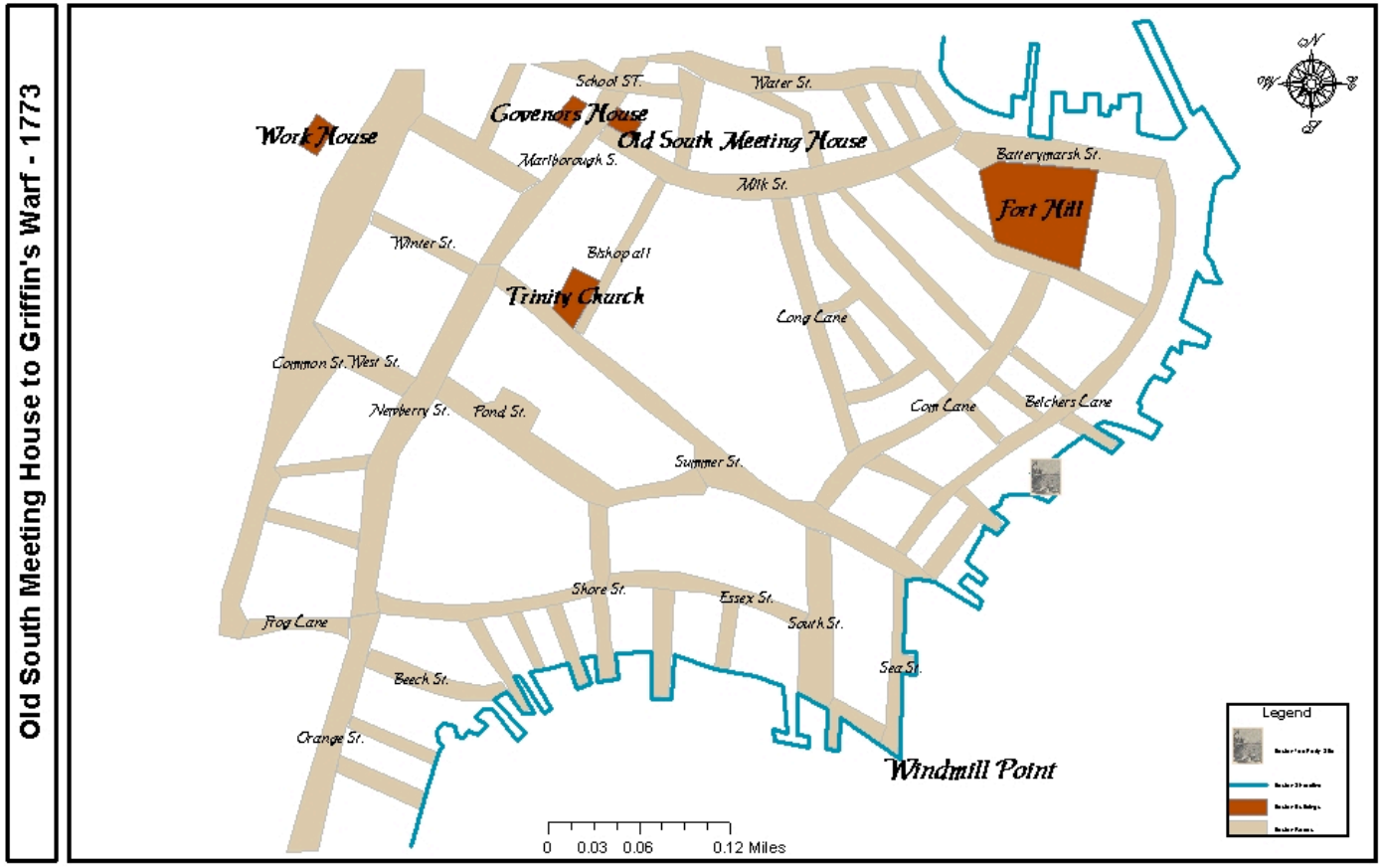
Introduction

- Why this is a reasonable topic
- VoIP Architecture Review
- VoIP Vulnerabilities
- Vendor behavior
- Vulnerability Predictions
- How to make things better

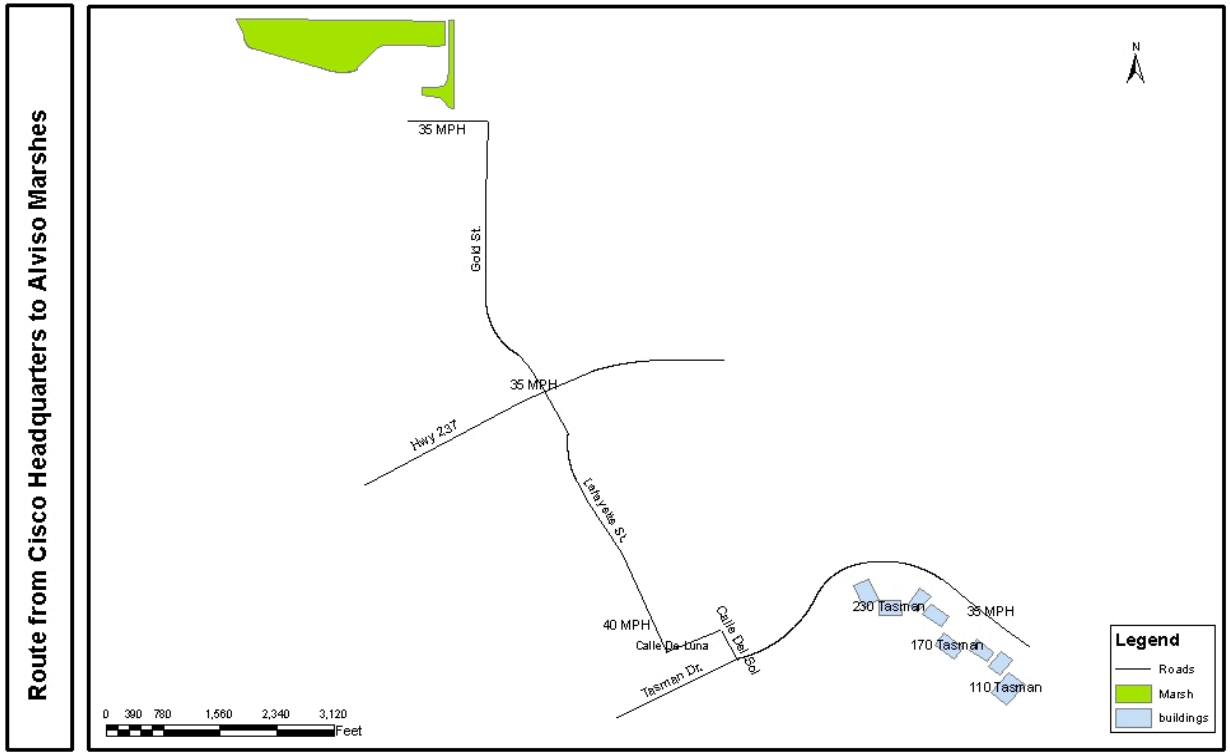
Disclaimer

- No zero-days were released in the production of this presentation.
- No NDA's were compromised in the production of this presentation.
- All snarky comments about vendors should be taken as examples – other vendors are just as bad.
- We describe many things as broken. We wouldn't be talking about this if we weren't trying to make things better.

Boston Tea Party 1773



Route from Cisco to Alviso



Why Talk About “Futures”?

- VoIP: not yet stable, already ‘legacy’
- New products are arriving vulnerable
- XP is no longer the ‘target celebre”
- Customers thought they were buying secure products
- Pointing out issues *should* improve the process going forward

VoIP Architecture Review

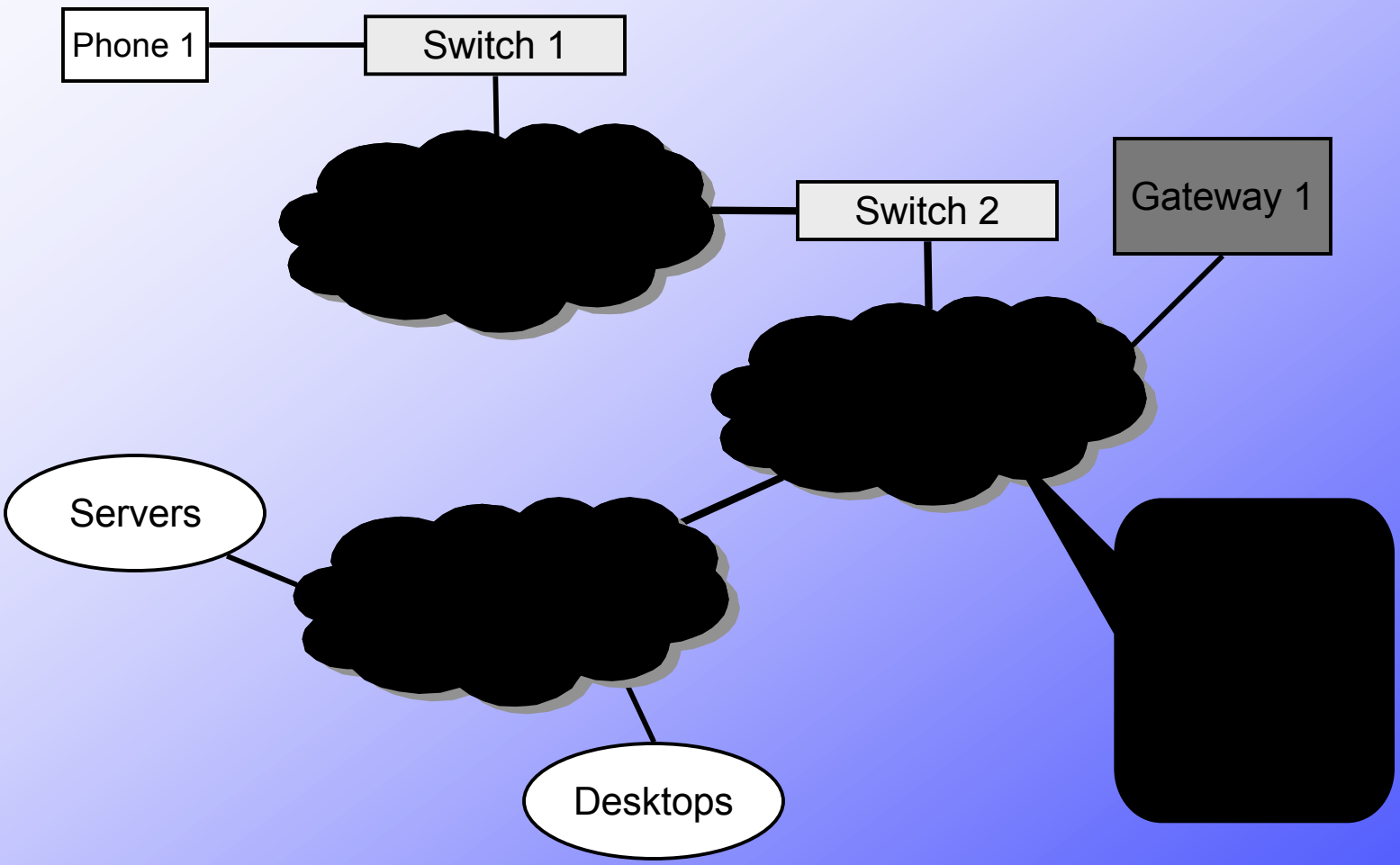
VoIP Components: Services

- PBX – Private Branch Exchange – full feature phone system
- Call manager
- SIP Proxies
- VoIP-POTS, VoIP-VoIP Gateways
- Directory Servers
- Voice Mail Servers

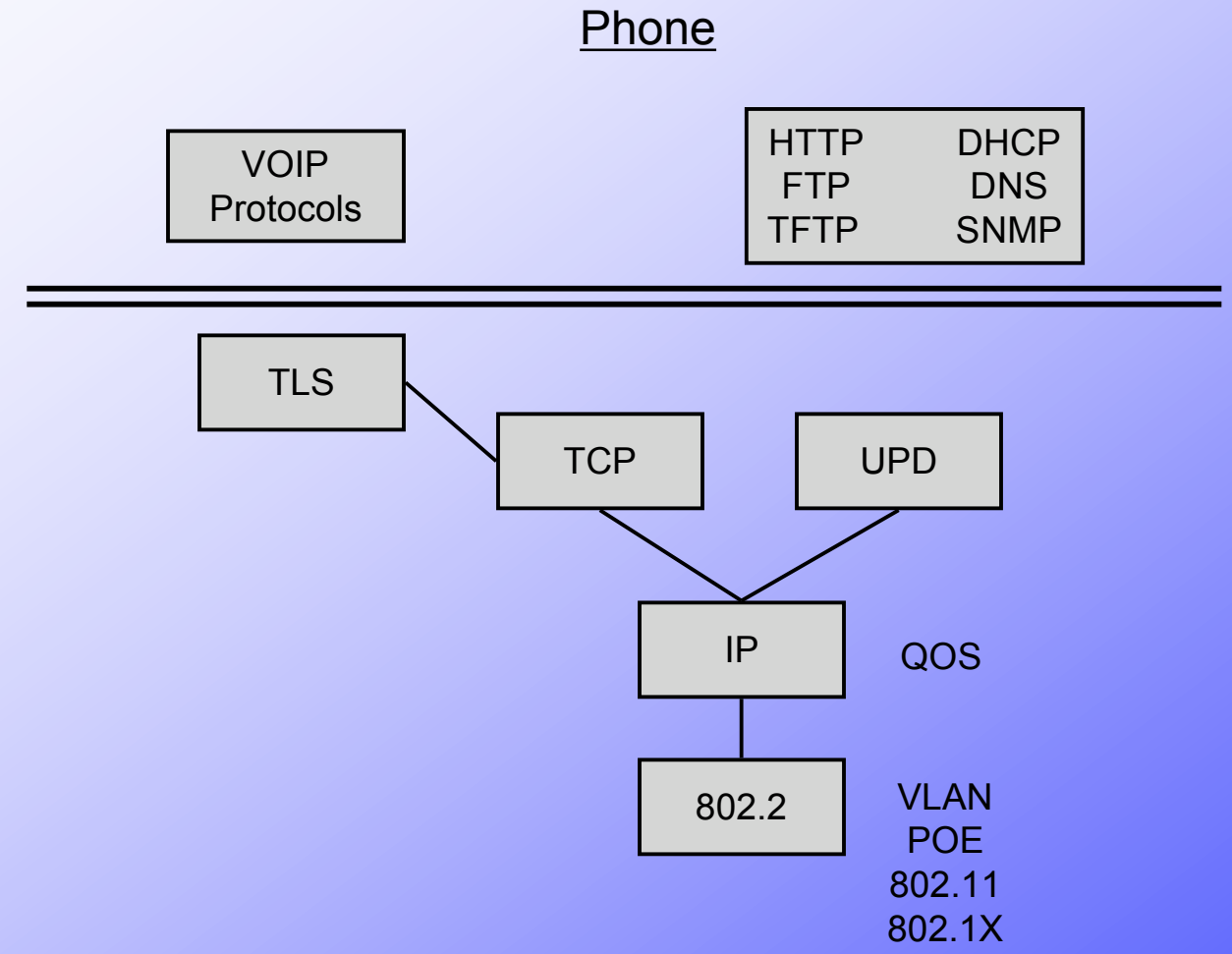
VoIP Components: Network Infrastructure

- Directory Servers (non-telephone specific)
- DHCP Server
- DNS Server
- Log Server
- Routers
- Switches

VoIP Network Elements



VoIP Phone: Protocol Elements



Past VoIP Vulnerabilities

Voice Protocols

- Standard VoIP
  - SIP
  - RTP
- CCITT Protocol flaws
  - H.323/H.228
  - ASN.1/DER

Phone Support Protocols

- HTTP (Web Server in phone)
- LDAP
- DNS
- DHCP

Server Support Protocols

- Call management
- LDAP
- DNS
- DHCP
- QoS

Infrastructure Protocols

- CDP
- (NAC)
- IP
- ARP

Vendor Behavior

Who are ‘the vendors’?

- Telco Hardware vendors: Avaya, Nortel
- Network Hardware vendors: Cisco, 3com
- Network operators: Cingular, Verizon, Orange
- Instrument vendors: (above plus) many random offshore manufacturers
- Protocol stack houses

Vendor Priorities

1. Stockholder value
2. Image
3. Market Share
4. Market position
5. Product Stability (optional)
6. Customer satisfaction (optional)
7. Security (very optional)

Stupid Vendor Tricks

- Resource-poor platform
- Partial protocol implementations
- Lack of testing
- Lack of security requirements
- Addiction to feature creep
- Ignorance of modern network requirements
- Proprietary protocols (with expected flaws)

Delivered Flaws

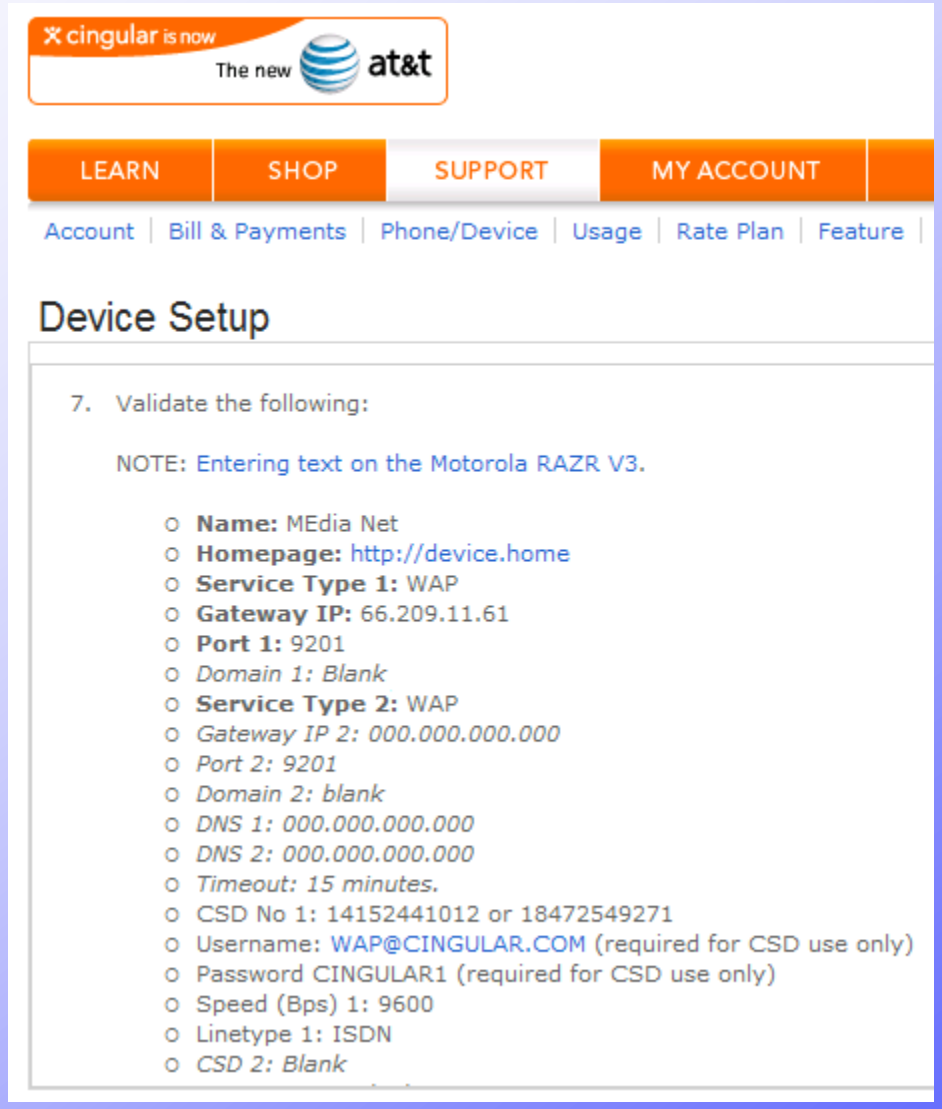
- SDLC deficiencies
- Security Illiteracy
- Testing deficiencies
- Prophylactic solutions to fundamental security flaws
- Mixed feelings about NAC
- Poor non-VoIP protocol implementations
- Immature VoIP protocol implementations
- Flawed proprietary VoIP protocols

Vulnerability Predictions

Legacy Telco

- Pre-DotComInternet telephone networks
- Possibly completely unsecured targets
- “Just across the aisle”
  - Possibly remotely accessible
  - Not well understood
  - “Pre-IPod” (i.e. can’t be high tech)

https://www.cingular.com/support/deviceConfig.do?content=KB39412.html



VoIP Instruments

- Vulnerable Platforms
  - Windows:
    - Is there a ‘windows update” for Mobile?
    - Lack of genetic diversity
  - iPod:
    - Multimedia attack vectors
    - ‘burning man’ custom protocol strategy
  - Embedded:
    - As underengineered as you can get away with

VoIP Instruments

- Protocol stack
  - Don’t assume the vendor can spell “IP”
  - All protocols fresh and vulnerable, all the time
- VoIP-specific protocols
  - Fast moving changes
  - Not stable
  - Features-based arms race
  - Time-to-market based vulnerabilities

VoIP Subsystems

- ‘Convergence’ Phones
  - Auth systems integration
  - Dual-stack platforms
  - Protocol edge cases due to handoff
  - New path into enterprise auth infrastructures
  - New path into resource-sharing environments
    - Attack your high end stereo
    - Attack your BMW
    - Attack your employer via the bootleg movie you just stuffed in your DVD player

VoIP Crypto

- Hardware can handle it
- Authorization should not be immortal
- All standard crypto rules apply
- Oh and the crypto should work:
  - Check the sigs
  - Roots
  - Key storage
  - Data format attacks…

Cool VoIP Targets

- Rich media
- Aggressively active content
- CODEC Attacks
- Games on phones
- Web 2.0 Fad Services e.g. Dodgeball

Enterprise VoIP Targets

- Email infrastructure
  - Exchange
  - Vmail/email exchanges
  - Blended spam/phish/voip platform active content attacks
- Gadget addict policy bypass
  - Is your Business Plan on your VoIP Phone?
  - Traffic analysis opportunities

Enterprise VoIP Infrastructure

- VoIP Deployment choices:
  1. Torture the Cisco-heads into deploying the phones
  2. Torture the Phone-heads into learning IOS
- VoIP Attack Choices:
  1. Bad vendor defaults not tuned
  2. Outdated IOS using long-in-the-tooth IOS sploits

How To Make Things Better

Customer Improvements

- Stop buying insecure junk
- Ask questions during the procurement process
- Make sure the product is sound before you buy it
- Sue the vendor if they screw up
- Connect your phones to a decent network

Vendor Improvements (1)

- Don’t forget it’s an IP node
- Gather security requirements from the real world
- Test products before they first ship
- Offer security upgrade paths
- Don’t go into denial about outside security research

Vendor Improvements (2)

- Stop dumping phones on newbie developers
- Spend some money on testing
- Implement FULL and SANE protocol stacks
- Don’t give priority to “look and feel” over “stable and secure”

Security Research Improvements

- Be vigilant about old vulnerabilities
- ‘Out’ insecure or vulnerable protocols
- (Politely) show how brittle telephones are
- Be vigilant about sloppy ‘new’ ideas

Credits

- Recon and mapping by *Operations*
- Cool conference venue by *Layer One 2007*
- Targetable VoIP products by *Cisco, Skype, Avaya*
- Exotic VoIP security research tools by *Fyodor* “and the usual suspects”
- Awesome student feedback from past VoIP training classes
- Cygnus and the folks sitting in the basement in Virginia

Rodney Thayer
rodney@thesecurityconsortium.net
www.thesecurityconsortium.net