

# **Voice over IP (VoIP) Vulnerabilities**

## **The Technical Presentation**

Diane Davidowicz  
NOAA Computer Incident Response Team  
N-CIRT  
[diane.davidowicz@noaa.gov](mailto:diane.davidowicz@noaa.gov)

"Security problems in state of the art IP-Telephony systems  
can be found in **every product**  
[and] **must** (not should)  
be solved **before** deploying“

Utz Roedig  
Darmstadt University of Technology

# Overview

- Traditional Telephony Systems
- VoIP Brings New Threats to IP Networks
- VoIP Security Threat Overview
- VoIP Threat Details
- VoIP Security Requirements and Security Solutions

# Traditional Telephony Systems

- Traditional telephone system is a mature technology
  - Public Switched Telephone Network(PSTN) and Private Branch Exchange (PBX)
  - Established, stabilized & highly evolved over the past decades
    - High level of quality of service
    - Security
      - Confidentiality
      - High availability
      - Integrity
    - High reliability - error free operation

# Traditional Telephony Systems

- Consists of dedicated equipment
  - Enjoyed complete separation from Internet hostilities
  - Typically not available to attackers with average or below average skills

# VoIP Overview

- Understanding the technology
  - Signaling plane
    - Call setup and tear down
      - gatekeepers and CCEs
  - Media transport plane
    - Carries the voice data
      - gateways and IP telephony endpoints
  - Management (administration) plane
    - Technically part of the signaling plane
    - Management interface can be attacked, thus its presented as a third plane for clarity
  - Assumption:
    - Both the Signaling plane and the Media transport plane traverse the same IP network

# New Threats to IP Data Networks

- Migration from traditional PBX system to VoIP
  - Weakens the security posture of well established data networks
- How?
  - Poorly implemented VoIP components
  - Deprecates traditional IP firewall

# New Threats to IP Data Networks

- Poorly implemented IP stacks in VoIP devices
  - May lead to access of IP data systems
    - By establishing an inroad of compromised VoIP devices that ultimately leads to the targeted computer
    - Exists mostly due to rush to market
      - Companies need to generate revenue for new technology
      - Code quality and security implementation suffer
        - not atypical of any new technology
        - E.g., wireless technology

# New Threats to IP Data Networks

- Deprecates Classical Firewall Technology
  - IP telephony protocols are very complex.
    - Traditional IP firewalls can not handle the protocols
      - H.323 dynamically allocates both TCP and UDP for call setup and voice transport
      - Implementation may require
        - both inbound and outbound call set up capabilities
    - Complex protocols weaken the security posture of the traditional IP firewall
      - Thereby raising the threat of exposure of the internal Local Area Network (LAN) to attacks

# New Threats to IP Data Networks

- Deprecates Classical Firewall Technology
  - Latency intolerance of voice data
    - Outmodes classical IP firewalls
  - Solutions
    - Subvert them for voice data (i.e., create route to bypass firewall)
      - Bad idea!
        - Violates security policy
        - Renders firewall ineffectual
        - Exposes previously protected LANs
        - Firewalls perform Network Address Translation (NAT) for private internal address

# New Threats to IP Data Networks

- Solutions
  - Upgrade/replace classical firewall with VoIP firewalls
    - May prove cost prohibitive
    - Limited number of vendors providing VoIP firewalls
    - Complicated by
      - Market flux as a result of proprietary solutions
      - Can cause interoperability issues

# VoIP Security Threat Overview

- Dispel Myth: This is not the comfy, cozy PBX
  - This is an IP network
  - IP networks, if not air gapped, are in some way are exposed to the Internet
    - A fully integrated VoIP network more than likely would not be implemented in an air gapped IP Network

# VoIP Security Threat Overview

- Remember: VoIP device is an IP device
  - Just like any other IP device, it is vulnerable to the same types of threats
- Quality and Security of VoIP is in its infancy
  - Especially when compared to traditional PSTN/PBX networks
  - Many security issues of VoIP stem from flaws in
    - The design, implementation and configuration of the equipment
    - And the policy faults

# VoIP Security Threat Overview

- Critical to understand security features and vulnerabilities of this new technology
  - Failure to do so and failure to take appropriate precautions can result in
    - Unavailability
      - Inability to dial, receive phone calls, or continue conversations already in progress
    - Lack of privacy
    - Lack of integrity
      - Both in audio message integrity and billing integrity
    - Lack of authentication
      - Leads to impersonation and toll fraud
    - Lack of access control
    - Lack of stability
    - Lack of quality of service

# VoIP Security Threat Overview

- Other vulnerabilities facing VoIP
  - Already established that Internet is big threat to VoIP
    - However, internal threat also increases dramatically
      - Most employees have access to local LAN ports that
        - allows them to plug IP sniffers into network
          - - IP sniffers = laptops with Ethereal
            - (<http://www.ethereal.com>)
    - This was not so easy to accomplish with PBX system

# Threats to VoIP Networks (Details)

- Signaling and media transport planes vulnerable to attacks against
  - Integrity
  - Confidentiality
  - Authentication
  - Non-repudiation

# Threats to VoIP Networks (Details)

- VoIP audio data & signaling are vulnerable to
  - Eavesdropping
  - Jamming
  - Active modification
    - How often have NOAA systems had system privilege level compromises?
  - Toll stealing

# Threats to VoIP Networks (Details)

- IP telephony components
  - Can be target of
    - DoS/DDoS Attacks
    - Attacks that lead to the compromise of the component
  - Compromised components
    - Reveal network infrastructure
    - Become a potential launch point for further attacks (e.g. source routing)
      - Into other IP Telephony components
      - Into IP data systems (computers, routers, etc.)
    - Viruses can disable OS hosting VoIP component

# Threats to VoIP Networks (Details)

- IP telephony components
  - Attacks carried out against VoIP end user systems
    - Current attack analysis show that most have classic security problems
    - Some vulnerabilities have been known for decades
      - yet new devices still deployed with them

# Threats to VoIP Networks (Details)

- Just to name a few:
  - Default administrator passwords
  - Weak Passwords (configured with maximum length of 6, 7, or 8 characters)
    - Vulnerable to dictionary attacks
    - Vulnerable to brute force attacks
    - Some implementations only allow numbers as password
      - Greatly reduces the key space
  - Worse, attacker can load new firmware with Trojan Horse backdoors
    - Not so trivial with traditional VoIP end systems
    - Java Phones and other Java telephony devices may make this trivial
  - PDA's VoIP over wireless may execute virus code too

# Threats to VoIP Networks (Details)

- Just to name a few.....
  - Other implementation faults: vulnerable to malformed strings
    - Little effort required to conduct this attack and the password attack
    - Common method to cause DoS
      - Poorly written VoIP end user applications & devices
      - DoS may be self-inflicted: ex - nmap, Harris Stat

# Threats to VoIP Networks (Details)

- Just to name a few.....
  - These attacks were SUCCESSFUL
    - Phones crashed
    - Phones rebooted
    - Phones hung and had to be rebooted

# Threats to VoIP Networks (Details)

- Just to name a few.....
  - Remote Administrative Interface
    - Passwords traverse network in clear text
      - Vulnerable to eavesdropping
    - Vulnerable to dictionary and brute force attacks from remote locations
    - If an HTTP interface, may have poorly written CGIs
  - Once the administrative interface compromised
    - Attacker can reset phone to factory specs
    - Can get user identities and E.164 numbers and change them, too
    - Can change the IP address for the H.323 Gatekeeper

# Threats to VoIP Networks (Details)

- Just to name a few.....
  - Media plane: Weakly implemented user privacy
    - Real-time Transport Protocol (RTP) used to transmit audio over UDP
      - Symmetric encryption designed into protocol
      - Unfortunately, not widely implemented into devices despite availability in protocol
    - UDP is easily spoofed
    - Unencrypted RTP can be intercepted
      - And because of UDP, can be modified and played back
      - Modification may go undetected by receiver

# Threats to VoIP Networks (Details)

- IP telephony components (continued)
  - Attacks carried out against: Gatekeeper
    - Man in the middle attack
      - Cryptographic protection in the extensions H.323 protocol would more securely thwart this
        - Commonly not implemented in the devices

# Threats to VoIP Networks (Details)

- IP telephony components (continued)
  - Attacks carried out against: Gatekeeper
    - Default Policy issue
      - End user devices need to be portable
      - Method for registration with gatekeeper supports this
      - End user device uses H.225 (RAS) to register a mapping of its
        - E.164 number
        - Voluntary number of additional symbolic names (aliases)
        - And IP address

# Threats to VoIP Networks (Details)

- IP telephony components (continued)
  - Attacks carried out against: Gatekeeper
    - Choice at gatekeeper is to
      - Allow any end user device to register
      - Or just allow pre-configured sets
    - Implementation flaw
      - Rather than be most restrictive and just allow pre-configured sets to register
      - Gatekeepers are typically configured to just allow any device to register
    - Faking user identity
      - Objective is to impersonate a user allowed to make international calls or toll calls
      - This is possible if gatekeepers aren't strictly configured to control this

# Threats to VoIP Networks (Details)

- IP telephony components (continued)
  - Attacks carried out against: Gatekeeper
  - Gatekeeper DoS attacks
    - One type of DoS attack unregisters users
    - Then attacker registers user with a new IP address
      - To maliciously redirect calls originally intended for the user
    - Another attack sent regular and irregular H.323 PDUs
      - which cycled through the registration and deregistration of terminals
      - Kept gatekeeper busy enough that it could not perform regular tasks
      - This is in the signaling plane and only a small amount of bandwidth was consumed in the successful attack

# VoIP Security Requirements and Security Solutions

## ● Security Requirements

- Defined in terms of
  - Protocols
  - Operating Systems and Components
  - Administration interfaces
  - Other Security Systems (Firewalls, VPNs, etc.)
  - People, Policies
  - A little more followup on cypto

# VoIP Security Requirements and Security Solutions

## ● Security Requirements

(extracted from "Security Analysis of IP-Telephony Scenarios" by Utz Roedig)

### ● Protocols

- What basic security services do they provide?
  - Enable them
  - Some protocols are currently being augmented to include security
    - ITU H.3xx/H.235 - Encrypted RTP with key exchange (using H.425)
    - IETF SIP - Encrypted RTP with key exchange (SIP message body)
- Can technology like IP Security (IPSec) be leveraged?
  - Some implementations may be proprietary, beware.

# VoIP Security Requirements and Security Solutions

## ● Security Requirements

(extracted from "Security Analysis of IP-Telephony Scenarios" by Utz Roedig)

- Operating Systems and Components
  - Must be kept patched up to date
    - Ex - Pingtel's VoIP SIP Phones, CISCO VoIP vulnerabilities
      - Cisco routers supporting VoIP were vulnerable
  - Systems and services must be secured
    - many vendors have neglected this step
    - e.g., invoke access and authentication controls where possible
    - enable only necessary services

# VoIP Security Requirements and Security Solutions

## ● Security Requirements

(extracted from "Security Analysis of IP-Telephony Scenarios" by Utz Roedig)

- Administration interfaces
  - Must be secured, is VPN or protocols like SSH or SSL/TLS available for interface?
  - Are access controls available and strong authentication?

# VoIP Security Requirements and Security Solutions

## ● Security Requirements

(extracted from "Security Analysis of IP-Telephony Scenarios" by Utz Roedig)

- Other Security Systems (Firewalls, VPNs, Radius)
  - IP Telephony must integrate into current security environment
  - Lack of VoIP Security solutions from most firewall vendors
    - exceptions: PIX, Checkpoint to name a few
  - Firewalls must be specifically designed with the hyper sensitive requirements of VoIP data
    - High reliability
    - High capacity
    - Low latency

# VoIP Security Requirements and Security Solutions

## ● Security Requirements

(extracted from "Security Analysis of IP-Telephony Scenarios" by Utz Roedig)

### ● People, Policies

- People must know how to operate/install/design and secure services

# VoIP Security Requirements and Security Solutions

## ● Solutions:

### ● Cryptography

- Seek implementations that leverage cryptography for
  - Signaling plane (H.323)
  - Media transport plane
- This is a start, but not a panacea
  - DoS and malformed string attacks still remain possible
    - This is an access issue
- IPSec/VPN VoIP enabled equipment goes a long way to preventing
  - Eavesdropping
  - Packet spoofing
  - Replay

# VoIP Security Requirements and Security Solutions

## ● Solutions:

### ● Cryptography

- Providing message integrity, authentication, and privacy via IPSec technology
  - Problem: not all VoIP devices are IPSec enabled.
  - This should be a consideration in purchasing VoIP equipment
  - Performance issue
    - VoIP IPSec enabled devices should support the following
      - latency
      - QoS
        - ToS byte must be in IP header, thus copied to IPSec header
      - Bandwidth restrictions to preserve call and video quality