IBM Research

Threat Assessment of IP Based Voice Systems

Threats to the Reliability and Security of IP Based Voice Systems

NOMS 2006 Conference

1st IEEE Workshop on VoIP Management and Security

Bill Rippon, IBM Research I/T

April 3, 2006

Contents

Purpose

- Analyze the potential threats to the reliability and security of IP based voice systems including; Voice over IP (VoIP) and IP Telephony (IPT)
- Identify the various threat categories
- Provide examples of potential attacks
- Provide mitigation approaches and recommendations

Mild Disclaimers and Clarifications

- I/T's favorite mantra "It Depends"
- The paper and this presentation do not provide an exhaustive list of all possible threats, attacks and mitigations
- As you will see there is quite a bit of overlap between different categories.
  - For example, lots of things can be considered a "Denial of Service"
- The fine print – Just for Fun
  - No animals were harmed during the creation of this presentation
    - At least not directly ☺
  - "Your mileage may vary". "Dealer sets actual price". "Not actual size". "Batteries are not included" ☺

Introduction

- Traditional or legacy voice services are rapidly giving way to IP based solutions
  - Voice over IP (VoIP) – Digitization, packetization and transport
  - IP Telephony - IP based phones and IP based voice infrastructure
- A variety of threats that existed in the legacy world will, of course, also exist in the IP based voice solutions. Although, IP based infrastructure could change the nature of the risk.
- IP based voice solutions and converged networks will also introduce new threats that need to be understood and managed

Industry Indicators

- According to TEQ Consult Group the shipment of IP lines surpassed that of TDM lines in 2005. (Source Business Communications Review Magazine)
- "Dell'Oro Group Predicts IP PBX Shipments will Surpass Traditional Time Division Multiplexing-Based Systems (TDM) Shipments in 2006" (Source http://www.delloro.com)
- "Infonetics Research estimates that overall TDM and IP PBX market will grow from $8.1 billion in 2005 to $11.6 billion 2009. Infonetics also estimates that IP PBX sales will increase 82% and TDM PBX revenue will drop by 88% worldwide over that same time period." (Source Network World Magazine)
- *"SCOTTSDALE, Ariz., January 31, 2006* - The global market for consumer VoIP services has arrived, with total VoIP subscribers worldwide at 16 million in 2005 and projected to grow to over 55 million in 2009, reports In-Stat (http://www.in-stat.com)."

Background

- Convergence
  - A common network infrastructure supporting multiple types of services
    - Typically this refers to the triad of voice, video and data
    - Motivation for converged networks
      - Desire for advanced applications and services
      - More responsive, flexible environment with reduced infrastructure
      - Demand for continuous cost reductions
  - The advancement of IP based voice standards and solutions is enabling the migration of voice to converged networks
- Architecture
  - There are substantial differences between traditional and IP based voice solutions
    - One such example is the potential for significant centralization, while simultaneously relying on a large number of loosely coupled layers (dependency on distributed data network). Centralized solutions could support tens of thousands, hundreds of thousands or even millions of endpoints.

Background

- Dependency on Other Parts of the Ecosystem
  - The reliability and security of IP based voice is heavily dependent on the reliability and security of the related components of the ecosystem
    - People, physical controls, environmental controls, device platforms, network, servers, etc.
  - Threats in any of the related components will inherently threaten the IP based voice services
  - This presentation/paper does not provide an analysis of all related areas. This observation is included merely for a more complete understanding of the overall environment

Threat Categories

- Denial of Service (DoS) – Voice or Network Infrastructure
  - Including degradation of service
- Non-DoS Data or Voice Service Outages
  - Including degradation of service
- Environmental Control Issues – Power and Cooling
- Vulnerability of Converged Networks
- Malicious Code (a.k.a. Malware)
- Identity, Privacy and Integrity Issues
- Unauthorized Access or Fraudulent Use
- Immaturity of the VoIP and IPT Systems

Threats and Attacks

Threats and Attacks - Denial of Service (*DoS*) – *Voice or Network Infrastructure*

- Malicious code
- System vulnerabilities
- Unauthorized access
- Packet or call floods
- Network or call routing/forwarding disruptions
- Priority queue exhaustion
- Invalid connection terminations
- Spam over Internet Telephony (SPIT)
- Account lockouts

Threats and Attacks
Non-Dos Data or Voice Service Outages

- Hardware or software failure
- Loss of power or cooling
- Cable cuts
- Improper configuration
- Insufficient change and problem management practices

Threats and Attacks
Environmental Control Issues – Power and Cooling

- Terrorism
- Utilities
- Accidental (i.e. the backhoe)
- Acts of nature
- Equipment failure

Threats and Attacks
Vulnerabilities of Converged Networks

- Attacks against the data network and services can indirectly or directly affect voice services
- The data network can provide communication paths that permit attacks directly against the voice environment
- One current area of concern is the use of IP softphones or other IP voice communications applications on the data network
  - Prevents the use of strong, conventional approaches to logical separation and protection
  - PCs have demonstrated continued susceptibility to malware and spyware

Note: The majority of the threat categories mentioned in this paper can apply to the vulnerabilities of converged networks. For additional attacks, please refer to the other threat category sections.

Threats and Attacks
Malicious Code (a.k.a. Malware)

- The data industry is very familiar with malware threats and attacks. IP voice services will naturally face similar issues.
- IP voice services must be concerned with both malware attacks in the data environment as well as attacks directed at the voice environment
- Malicious code can be introduced in a variety of ways
  - Exploit vulnerabilities in applications or operating system
  - E-mail attachments
  - Instant messaging programs
- Common attacks and infections
  - Trojan horse, worms, bots, key-loggers, root kits and spyware

Threats and Attacks
Identity, Privacy and Integrity Issues

- Session hi-jacking
- Compromised system accounts
- Active or passive eavesdropping
- Unauthorized call routing
- Unauthorized access to voice or network components
- Unauthorized data access
- Unwanted content exposure
- Malicious code and spyware
- Social Engineering
- Phishing schemes
- Network identity masquerading
- Voice identity masquerading
- Unauthorized network access
- Unauthorized access to voice services
- Caller-ID hacks
- Voice mailbox squatting or redirection

Threats and Attacks
Unauthorized Access or Fraudulent Use

- Elevation of privileges
  - Class of service
- Use of voice resources
  - Basic calling, voice mailboxes
- Access to data or voice infrastructure
  - Configuration
  - Tracing
- Modification of call flows
  - Forwarding

Note: For further issues please refer to the section on "Identity, Privacy and Integrity"

Threats and Attacks
Immaturity of the VoIP and IPT Systems

- Organizational differences and problem id, determination, resolution
- Sub-optimal architecture and implementations
- Inappropriate devices (not voice aware)

Note: This category is more general in nature. The vulnerabilities introduced by an immature technology or solution will typically enable some of the attacks that are detailed in other threat categories. While a few attacks will be listed here, please refer to other threat categories for additional attacks

Mitigation and Recommendations

Mitigation and Recommendations
Denial of Service (DoS) - Voice or Network Infrastructure

- Follow “Best Practices”
- Process and procedures for secure configuration, management and operation
- Harden voice and network infrastructure devices thru embedded or adjunct mechanisms
- Control network traffic to limit exposure to attacks and minimize damage
- Compartmentalize networks and services for voice and data
- Implement network access authentication where possible/practical
- Utilize emerging technologies for admission control
- Utilize verified software and firmware (such as IP phone firmware)

Mitigation and Recommendations
Non-Dos Data or Voice Service Outages

- Redundant networks, data services and voice services
  - Diverse paths and diverse providers where possible and appropriate
  - Provide redundant centralized services that are geographically dispersed
- Backup and emergency voice services
- Redundant and diverse power
  - Multiple feeds, circuits, UPS, generators, devices with dual power supplies
- Redundant and resilient cooling and/or provide for emergency procedures and equipment
- Develop disaster recovery plans and procedures (include backup equipment and backup sites)

Mitigation and Recommendations
Environmental Control Issues – Power and Cooling

- Multiple, diverse path, building power feeds
- Network and voice devices should use diverse building power
- Utilize Power-over-Ethernet (PoE)
- Utilize UPS power for infrastructure devices
- Utilize emergency generator backup power for critical components
- Provision portable A/C units for critical infrastructure components
- Develop standards, policies and procedures for dealing with environmental control issues

Mitigation and Recommendations
Vulnerabilities of Converged Networks

- Develop process and procedures for secure configuration, management and operation of network and voice infrastructure devices
- Access authentication, particularly in common areas
- Disable unused services or protocols on voice compartments
- Restrict access to services or protocols in the voice compartment that are used by management and support
- Disable embedded data switch ports on IP phones when not needed/desired (such as lobbies, cafeterias, etc.)

Note: A variety of other threat areas can exploit vulnerabilities that would impact a converged network. Please refer to the other threat category sections for additional recommendations.

Mitigation and Recommendations
Malicious Code (a.k.a. Malware)

- There are number of existing, typical, mitigation recommendations
  - Anti-Virus software for clients and servers
  - Patch management and vulnerability assessments
  - Host IPS, firewalls and ACLs
  - Network IPS, firewalls and ACs
- Other approaches
  - Session Border Controllers (SBCs)
    - more voice aware stateful firewalls
  - IPS style solutions targeted at IP voice attacks
  - Digitally signed software and firmware (such as for IP phones)
  - Utilize authentication and network admission control (pre-insertion checks)

Mitigation and Recommendations
Identity, Privacy and Integrity Issues

- Develop process and procedures for secure configuration, management and operation of network and voice infrastructure devices
- Define and enforce physical security control policies
- Implement available layer2 and layer3 security features
- Implement network identity management system
- Utilize network access authentication
- Utilize encryption for content, headers or entire packets as required
- Define and enforce policies for account management and credential selection (such as strong passwords)
- Utilize digital signature technology where available and appropriate

Mitigation and Recommendations
Unauthorized Access or Fraudulent Use

- Utilize network access authentication
- Authenticate phones to call control systems
- Control access to voice gateways (call setup)
- Excess capacity and, or on-demand provisioning
- Develop solutions for detection and blocking of SPIT
- Monitoring and alerting for call setup and voice traffic anomalies
- Disable auto-registration features or limit default class of service
- Disable unused voice mailboxes and control automatic registration of voice mailboxes

Note: For further mitigation and recommendations please refer to the section on "Identity, Privacy and Integrity"

Mitigation and Recommendations
Immaturity of the VoIP and IPT Systems

- Setup education programs and self-help resources for customers and support teams
- Subscribe to vendor and industry information sources to keep abreast of security and functional issues related to IP voice
- Merge data network and voice services groups into a single organization
- Limit the number of external providers that are responsible for voice and network services
- Iteratively review and update configuration management and operational practices within the organization
- Track changes in “best practices” recommendations from various sources
- Iteratively review and update standards, policies and procedures geared towards IP voice services
- Strive to select and migrate to, a single standards based solution for each function
- Continue to monitor the progress of emerging technologies and solutions, such as border control

Acknowledgement And References

Acknowledgement

I would like to thank my colleagues, from a variety of organizations within IBM, for assisting in the preparation of the white paper. Their input, comments and feedback were invaluable in the creation of the paper.

References

- D. Richard Kuhn, Thomas J. Walsh and Steffen Fries, “Security considerations for voice over IP systems”, NIST Special Publication 800-58, U.S., January 2005
- Greg S. Tucker, “Voice over Internet Protocol and security”, SANS Institute, October 2004 (available online http://www.sans.org/rr/whitepapers/voip/1513.php)
- A. Klein, “Security analysis: traditional telephony and IP telephony”, SANS Institute, 2003 (available online http://www.sans.org/rr/whitepapers/telephone/924.php)
- Anonymous, “IP telephony security in depth”, Cisco Systems Corporation, 2003 (available online http://www.cisco.com/go/safe)
- Anonymous, “SAFE enterprise layer2 addendum”, Cisco Systems Corporation, 2003 (available online http://www.cisco.com/go/safe)
- S. Convery and B. Trudel, “Cisco SAFE: A security blueprint for enterprise networks”, Cisco Systems Corporation, 2000 (available online http://www.cisco.com/go/safe)
- B. Munch, “IP telephony security: Deploying secure IP telephony in the enterprise network”, META Group, January 2005 (available online http://www.juniper.net/company/events/archive/metavoip.pdf)

References

- Anonymous, “Security in real-time IP communications”, Siemens AG, 2004 (available online at http://www.siemens.com/Daten/siecom/HQ/ICN/Internet/Enterprise_Networks/WORKAREA/en_ezine/templatedata/English/file/binary/0105_Security_in_Real-Time_IP_en_1297948.pdf)
- P. Brockmann, “IP telephony security – a double edged sword”, 3Com Corporation, 2005 (available online http://www.3com.com/voip/whitepapers.html)
- Anonymous, “Secure telephony solutions”, Nortel Networks, 2003 (available online http://www.nortel.com/solutions/security/collateral/nn104820-071403.pdf)
- Anonymous, “Secure telephony solution appendices”, Nortel Networks, 2003 (available online http://www.nortel.com/solutions/security/collateral/nn105080-071103.pdf)
- Anonymous, “Security for service provider VoIP networks”, Nortel Networks, 2004 (available online http://www.nortel.com/products/01/succession/cs/softswitch/collateral/nn109180-102904.pdf)
- Anonymous, “Solution architecture reference manual for IPT, IP communications systems test release 2.0”, Cisco Systems 2004 (available online at http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns268/networking_solutions_package.html)

References

- R. Droms, “Dynamic host configuration protocol”, Internet Engineering Task Force, RFC 2131, 1997
- P. Mockapetris, “Domain names – concepts and facilities”, Internet Engineering Task Force, STD 13, RFC 1034, 1987
- P. Mockapetris, “Domain names – implementation and specification”, Internet Engineering Task Force, STD 13, RFC 1035, 1987
- D. Mills, “Network time protocol (version 3) specifications, implementation and analysis”, Internet Engineering Task Force, RFC 1305, 1992
- Anonymous, “Information technology – Open Systems Interconnection – Basic reference model: The basic model”, International Organization of Standards, JTC1, IOS/IEC 7498-1:1994 2nd Edition
- J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, N. Handley, and E. Schooler, “SIP:Session initiation protocol”, Internet Engineering Task Force, RFC 3261, 2002.
- Anonymous, “802.3af IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks— Specific requirements, Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, Amendment: Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI)”, IEEE Standard 802.3af, 2003

References

- International Telecommunications Union, “Packet based multimedia communications systems,” ITU, Recommendation H.323, 2000.
- T. Ylonen and C. Lonvick (Editor), “The secure shell (SSH) protocol architecture”, Internet Engineering Task Force, RFC 4251, January 2006
- D. Harrington, R. Presuhn and B. Wijnen, “An architecture for describing SNMP management frameworks”, Internet Engineering Task Force, RFC 2261, January 1998
- Anonymous, “ 802.1X - IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control”, IEEE Standard 802.1x-2004
- Anonymous, “TCG trusted network connect, TNC architecture for interoperability, version 1.0 revision 4”, Trusted Computing Group, May 2005 (available online at https://www.trustedcomputinggroup.org/groups/network)
- Cisco Network Admission Control, Cisco Systems (available online at http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html)
- Microsoft Network Access Protection, Microsoft Corporation, (available online at http://www.microsoft.com/technet/itsolutions/network/nap/default.mspx)