Security in Converging Networks

Cross Network Attacks
Telecom Firewalls
And
Real-Time Mixed Media Firewalls

Lee Sutterfield
President
SecureLogix Corporation

13750 San Pedro
San Antonio, TX 78232
lsutt@securelogix.com
www.securelogix.com

TeleWall, TeleSweep Secure, TeleAudit, TeleVPN, ETM, TeleView, TeleBridge, TeleIDS, TelePort, SecureLogix Corporation and the SecureLogix Diamond Emblem are trademarks or registered trademarks of SecureLogix Corporation in the U.S.A. and other countries. All other trademarks mentioned herein are believed to be trademarks of their respective owners. © Copyright 2000-2002 SecureLogix Corporation. All Rights Reserved. U.S. Patent No. US 6,226,372 B1, US 6,249,575 B1 and US 6,230,980 B1 U.S. and Foreign Patents Pending.
Overview

- Pre-convergence Voice Vulnerabilities
- Telecom Firewall Solutions (circuit switched)
- Convergence Vulnerabilities
- Campus VoIP Security
- IP Trunk Vulnerabilities
- Real Time Mixed Media (RTMM) Firewalls (packet switched)
- Migration to Secure VoIP
Pre-Convergence Vulnerabilities between Voice and Data Networks
<table>
<thead>
<tr>
<th>RISKS</th>
<th>Legacy/TDM</th>
<th>Campus VoIP</th>
<th>IP-Trunking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Availability</td>
<td>LOW</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PBX Attack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Theft</td>
<td>MEDIUM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• DISA Abuse</td>
<td>• VM Toll Fraud</td>
<td></td>
</tr>
<tr>
<td>Eaves Dropping</td>
<td>LOW</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Wire Tapping</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cross Network Attacks</td>
<td>HIGH</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Modem Attacks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Voice Service Availability / Theft

Remote access to PBX for Toll Fraud or Disruption.
Eavesdropping Voice in TDM
Cross Network Attacks - Authorized Modems

Diagram showing network components including Internet, IP-Firewall, PSTN, ISP, PBX, Servers, Authorized Modem, and External Attack.
Cross Network Attacks - Unauthorized Modems

Employees use a modem to dial around the Firewall and IDS. Hacker “piggybacks” off ISP connection to access the Data Network.
Cross Network Attacks — WarDialing

After hours scanning — 2%-4% of phone lines have unauthorized modems.
Pre-Convergence
Voice Security
and
Telecom Firewalls
Circuit Switched VPNs
and
Telecom IDS
Telecom Firewall Deployment

Blocked!

External Attack

Internet

ISP

PSTN

IP-Firewall

Telecom Firewall

PBX

Servers

Workstations

TDM Telephones

External Attack
Telecom Firewall Core Functionality

◆ Log all Call Progress Information:
  ◆ Source, destination, time, duration, etc...
  ◆ Enterprise-wide, real-time, back to central server

◆ Characterize Call Type:
  ◆ Voice, fax, modem, VTC, STU-III (secure)
  ◆ Continuous monitoring of call for type changes

◆ Generic Security/Management Policy:
  ◆ Rule-based analysis of each call
  ◆ Autonomous execution
  ◆ Centrally managed push-down policy
Telecom Firewalls are the first Real-Time Media Firewalls for the enterprise.
Campus Level VoIP Deployments and Security
<table>
<thead>
<tr>
<th>RISKS</th>
<th>Legacy/TDM</th>
<th>Campus VoIP</th>
<th>IP-Trunking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Availability</td>
<td>LOW</td>
<td>MEDIUM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PBX Attack</td>
<td>• Viruses</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DoS Attacks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unauth. Access</td>
<td></td>
</tr>
<tr>
<td>Service Theft</td>
<td>MEDIUM</td>
<td>HIGH</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• DISA Abuse</td>
<td>• DISA &amp; VM...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• VM Toll Fraud</td>
<td>• VoIP Gateway</td>
<td></td>
</tr>
<tr>
<td>Eaves Dropping</td>
<td>LOW</td>
<td>MEDIUM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Wire Tapping</td>
<td>• Packet Sniffers</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Utilities - VOMIT</td>
<td></td>
</tr>
<tr>
<td>Cross Network Attacks</td>
<td>HIGH</td>
<td>HIGH</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Modem Attacks</td>
<td>• Cross VLAN Hack</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Modem Attacks</td>
<td></td>
</tr>
</tbody>
</table>
Inherited IP Vulnerabilities

“It may seem painfully obvious, but it’s important to remember that a VoIP network is an IP network. Any VoIP device is an IP device, and it’s therefore vulnerable to the same types of attacks as any other IP device. In addition, a VoIP network will almost always have non-VoIP devices attached to it and be connected to other mission-critical networks.”

- **Network Based**
  - Denial of Service
  - Packet Spoofing
  - Packet Sniffing
  - Packet Redirection
  - Packet Replay Attacks

- **Host Based**
  - Operating Systems
  - File Services
  - RPC Services
  - TCP/IP Stacks
  - Application(s)

Dr. Andrew Molitor, Aravox Technologies
VoIP Generic Vulnerabilities

- Basic Threats to IP Telephony
  - Data network access through VoIP ports (tunneling)
  - Free long distance calls over PSTN (spoofing)
  - Eavesdrop on conversations (packet sniffing)
  - Record conversations without authorization
  - Modify, delete, or replace fax/voice packets
  - Forward incoming phone calls to somewhere else
  - Denial-of-Service attack on business phone system
  - Denial-of-Service attack on business data network
  - Expose private conversations on Internet
  - Hijack conversations
  - Block calls of targeted individuals
  - Log all calls through an organization
VoIP Specific Vulnerabilities

- **New Applications and Protocols for Exploitation**
  - Softswitch, Call Agents, Proxy Servers, Presence Servers...
  - Signaling and Media

- **A Specific Example;**
  - VOMIT – Voice Over Mis-configured Internet Telephones
    
    A “utility” that converts Cisco IP phone conversations into a “.wav” file that can be played with ordinary sound players

- **VoIP Exploits Will Increase with Technology Deployment!!**  
  
  VoIP ...“the next interesting target”
Campus VoIP Server Security

Traditional TDM Voice Network

External Attacker

Internet

IP-Firewall

ISP

PSTN

Telecom Firewall

IPBX

PBX

IPBX gateway

TDM Phones

Call Server Cluster

IP Phones

Workstations

Servers

modem

SECURELOGIX CORPORATION

TeleWall, TeleSweep Secure, TeleAudit, TeleVPN, ETM, TeleView, TeleBridge, TeleIDS, TelePort, SecureLogix Corporation and the SecureLogix Diamond Emblem are trademarks or registered trademarks of SecureLogix Corporation in the U.S.A. and other countries. All other trademarks mentioned herein are believed to be trademarks of their respective owners. © Copyright 2000-2002 SecureLogix Corporation. All Rights Reserved. U.S. Patent No. US 6,226,372 B1, US 6,249,575 B1 and US 6,230,980 B1 U.S. and Foreign Patents Pending.
Campus VoIP Server Security

Enterprise-wide Real-time Reporting

Misuse & Toll Fraud Detection

Servers
Work stations
IP Phones
modem
Call Server Cluster
TDM Phones

External Attacker
ISP
PSTN
Internet
IP-Firewall
Telecom Firewall
PBX
IPBX gateway
CallServerCluster
External Attacker
ISP
PSTN
Internet
IP-Firewall
Telecom Firewall
PBX
IPBX gateway
CallServerCluster

TeleWall, TeleSweep Secure, TeleAudit, TeleVPN, ETM, TeleView, TeleBridge, TeleIDS, TelePort, SecureLogix Corporation and the SecureLogix Diamond Emblem are trademarks or registered trademarks of SecureLogix Corporation in the U.S.A. and other countries. All other trademarks mentioned herein are believed to be trademarks of their respective owners. © Copyright 2000-2002 SecureLogix Corporation. All Rights Reserved. U.S. Patent No. US 6,226,372 B1, US 6,249,575 B1 and US 6,230,980 B1 U.S. and Foreign Patents Pending.
IP Trunks and Secure IP Telphony
<table>
<thead>
<tr>
<th>RISKS</th>
<th>Legacy/TDM</th>
<th>Campus VoIP</th>
<th>IP-Trunking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Availability</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>VERY HIGH</td>
</tr>
<tr>
<td></td>
<td>• PBX Attack</td>
<td>• Viruses</td>
<td>• Viruses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DoS Attacks</td>
<td>• DoS Attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unauth. Access</td>
<td>• Unauth. Access</td>
</tr>
<tr>
<td>Service Theft</td>
<td>MEDIUM</td>
<td>HIGH</td>
<td>VERY HIGH</td>
</tr>
<tr>
<td></td>
<td>• DISA Abuse</td>
<td>• DISA &amp; VM...</td>
<td>• VoIP Gateway</td>
</tr>
<tr>
<td></td>
<td>• VM Toll Fraud</td>
<td>• VoIP Gateway</td>
<td></td>
</tr>
<tr>
<td>Eaves Dropping</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>HIGH</td>
</tr>
<tr>
<td></td>
<td>• Wire Tapping</td>
<td>• Packet Sniffers</td>
<td>• Packet Sniffers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Utilities - VOMIT</td>
<td>• Utilities - VOMIT</td>
</tr>
<tr>
<td>Cross Network Attacks</td>
<td>HIGH</td>
<td>HIGH</td>
<td>VERY HIGH</td>
</tr>
<tr>
<td></td>
<td>• Modem Attacks</td>
<td>• Cross VLAN Hack</td>
<td>• VoIP Trunk Hacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Modem Attacks</td>
<td>• Cross VLAN Hack</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Modem Attacks</td>
</tr>
</tbody>
</table>

SecureLogix Corporation and the SecureLogix Diamond Emblem are trademarks or registered trademarks of SecureLogix Corporation in the U.S.A. and other countries. All other trademarks mentioned herein are believed to be trademarks of their respective owners. © Copyright 2000-2002 SecureLogix Corporation. All Rights Reserved. U.S. Patent No. US 6,226,372 B1, US 6,249,575 B1 and US 6,230,980 B1 U.S. and Foreign Patents Pending.
IP Trunk Risk
External attack through IP Trunks against IP Voice and Data Network
External attack through IP Trunks against IP Voice and Data Network

Real-Time Mixed Media Firewall

Real-Time Mixed Media Firewall Policy Enforcement
<table>
<thead>
<tr>
<th>RISKS</th>
<th>Legacy/TDM</th>
<th>Campus VoIP</th>
<th>IP-Trunking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Availability</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>VERY HIGH</td>
</tr>
<tr>
<td></td>
<td>• PBX Attack</td>
<td>• Viruses</td>
<td>• Viruses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DoS Attacks</td>
<td>• DoS Attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unauth. Access</td>
<td>• Unauth. Access</td>
</tr>
<tr>
<td>Service Theft</td>
<td>MEDIUM</td>
<td>HIGH</td>
<td>VERY HIGH</td>
</tr>
<tr>
<td></td>
<td>• DISA Abuse</td>
<td>• DISA &amp; VM...</td>
<td>• VoIP Gateway</td>
</tr>
<tr>
<td></td>
<td>• VM Toll Fraud</td>
<td>• VoIP Gateway</td>
<td>• QoS Hijacking</td>
</tr>
<tr>
<td>Eaves Dropping</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>HIGH</td>
</tr>
<tr>
<td></td>
<td>• Wire Tapping</td>
<td>• Packet Sniffers</td>
<td>• Packet Sniffers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Utilities - VOMIT</td>
<td>• Utilities - VOMIT</td>
</tr>
<tr>
<td>Cross Network Attacks</td>
<td>HIGH</td>
<td>HIGH</td>
<td>VERY HIGH</td>
</tr>
<tr>
<td></td>
<td>• Modem Attacks</td>
<td>• Cross VLAN Hack</td>
<td>• VoIP Trunk Hacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Modem Attacks</td>
<td>• Cross VLAN Hack</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Modem Attacks</td>
</tr>
</tbody>
</table>
OK, so now what?
Technology Deployment Strategy for migration to secure enterprise voice services...
First Steps? Update legacy network.

- Secure legacy voice infrastructure, today.
- IP enable legacy infrastructure, today.
- Improve operations and save money on your phone bill, today.
- Characterize and Quantify real needs for IP telephony, today.
- Use data to plan for tomorrow’s move to IP telephony deployment.

*Telecom Firewalls automate all of the above.*
Next Steps? Deploy pilots, study and plan.

- Initiate your first green field deployment of campus level IP telephony infrastructure.
- Institute Voice Server Security...anti-virus, HIDS, Segmentation, etc.
- Institute VLAN security with RTM VLAN Firewall to secure, monitor and manage traffic
- Analyze data on effectiveness, QoS, cost...
- Test full IP Telephony deployment by implementing limited IP trunks at test sites.

*Telecom Firewalls support all of the above and will evolve with the network.*
Next Steps? Deploy pilots, study and plan.

- Integrate monitoring and policy of Call Server Security package, RTM VLAN Firewall and RTM IP Trunk Firewall.
- Analyze data on effectiveness, QoS, cost...
- Develop *real requirements* and complete plan for migration to full *Secure IP telephony*.
- Integrate monitoring and policy for VOICE NETWORK SECURITY and DATA NETWORK SECURITY.

*Telecom Firewalls support all of the above and will evolve with the network.*
Converging Apps - Unified Management

IP enable the old... move the old to the new.

Voice Network  Telecom FWL  Migrating Functionality
Audit
Infrastructure
Gateway etc.

IP Network

Migrating Functionality

TeleWall, TeleSweep Secure, TeleAudit, TeleVPN, ETM, TeleView, TeleBridge, TeleIDS, TelePort, SecureLogix Corporation and the SecureLogix Diamond Emblem are trademarks or registered trademarks of SecureLogix Corporation in the U.S.A. and other countries. All other trademarks mentioned herein are believed to be trademarks of their respective owners. © Copyright 2000-2002 SecureLogix Corporation. All Rights Reserved. U.S. Patent No. US 6,226,372 B1, US 6,249,575 B1 and US 6,230,980 B1 U.S. and Foreign Patents Pending.
Summary  Telecom Firewalls...

- ... solve the “last big back door” security problem for the data network security customer, today.

- ... cut costs and saves time and resources for the telecomm manager by IP-enabling his legacy infrastructure, today.

- ... positions both the data network manager and the voice network manager to proactively manage the migration to the new converged network of tomorrow.

- ... provide a centrally-managed, switch and media independent infrastructure which will support wholly new security and management capabilities in the future.