Speech & Security

Steve Chirokas
August 8, 2006
Security & Speech

- Know your Enemy (External & Internal)
- Know Yourself (Speech Vulnerabilities)
- Know Your Regulations?
- Protect Your Speech Assets
Who is Convergys?

– Largest Outsourcer of Agents in the World
  • $2.7B annual revenue, NYSE:CVG
  • Customer Service, Billing, Employee Care, Consulting Services
  • Solutions for web, chat, e-mail, phone and speech

– Convergys Speech Solutions
  • Hosted, Geographically redundant, massively scalable
  • Speech Science & VUI design
  • Convergys Labs

– Convergys Speech
  • Agents & Automation
  • Open Hosting
  • Security
Threats

- Stolen passwords
- Unauthorized Access
- Hacker
- Etc.

Common Defense
- Firewalls
- Network Address Translation (NAT)
- Proxy Servers
- DMZ’s
- VPN’s
- Encryption
- Mutual Authentication
- Secure Sockets
- Etc.
What makes Speech........

<table>
<thead>
<tr>
<th>Same as other Security Reqs.</th>
<th>Different from other Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Concern for Customer Info</td>
<td>• Audio + Data</td>
</tr>
<tr>
<td>• Need to Network (LAN/WAN)</td>
<td>• Concatenated, DTMF, TTS</td>
</tr>
<tr>
<td>• Balance Security &amp; Performance</td>
<td>• Recognition, Grammars, Dialogs</td>
</tr>
<tr>
<td>• Administrative Access</td>
<td>• Tuning (Logging/Reporting)</td>
</tr>
<tr>
<td>• Applicable Security Regulation</td>
<td>• Silence = Hang-up/ Zero-out</td>
</tr>
</tbody>
</table>
Audio Files

• Why more sensitivity to security issues with speech now?
  – More Transactions
  – “Back-end” System integration
  – Increasing Volume

• Caller Provided Examples:
  – Account Number
  – Social Security Number
  – Username
  – PIN/Password
  – Credit Card Number
  – System Provided: Any Account Information

• Speech Recognition – Data Persistence
  – Capture and Digitization
  – Match to a Grammar
Speech Not A Stovepipe

• Data Dips Drive Dynamic Dialogs
  – Caller info “shortcuts” what callers must say
  – Input keys access to additional
  – Dynamic Grammars

• You need to move information
  – Telephony Server/Media Gateway
  – VoiceXML Browser
  – Recognizer
  – VoiceXML Server
  – TTS Server
  – Prompt Server
  – Backend Systems
  – CTI System

• LAN & WAN
New to Many Security Managers

• Input
  – Speech – Results in recognizer and browser
  – Grammars
  – DTMF – Units tracked in logs

• Confirmations
  – Concatenated Audio - “I think you said your PIN was 562”
    <audio src="http://vmedia/en_us/prompts(chars/5.ulaw">5</audio>
    <audio src="http://vmedia/en_us/prompts(chars/2.ulaw">2</audio>

• Text To Speech
  – Browser Passes TTS Server Potentially Sensitive Data
  – TTS Server Sends Audio
Where is Data Exposed?

Network Transmission
- Vulnerable To Being “Sniffed”

- Log Files – Persisted Data
  - Application
  - Vendor
  - Tuning Files
  - Who’s tuning your Apps?

07/15/2005 17:27:26,02_CCNum, data, nomatches, 0
07/15/2005 17:27:26,02_CCNum, data, rawanswer, five six two five four three two five eight eight seven one
Security Regs. & Best Practices

• Regulations
  – Gramm-Leach-Bliley Act – Financial Institutions
  – Health Insurance Portability and Accountability Act (HIPAA)
  – Payment Card Industry Data Security Standard (Credit Card)
  – Title 21, Code of Federal Regulations, Part 11 (FDA)
  – Financial Breach Notification Act, California State Bill 1386
  – U.S. Government Information Security Reform Act (GISRA)
  – Sarbanes-Oxley

• ISO 17790
  – 1. Business continuity planning
  – 2. System access control
  – 3. System development and maintenance
  – 4. Physical and environmental security
  – …..10 broad areas
Security – 3 Layers

- Holistic Perspective
- LAN + WAN
- Data + Audio
- Proactive
- Automated
- Audit
- Maintain Speech Performance
- Dedicated Security Administrator

**People**
- Procedures
- Training
- Security Admin
- Personnel Security
- Physical Security
- Countermeasures

**Technology**
- Network Infrastructure
- Facilities Boundaries
- Computer Systems
- Mutual Authentication
- Encryption
- Log Suppression

**Operations**
- Security Policies
- Audit
- Key Management
- Access Control
- Sense, Warn, Respond
- Recover
People & Procedures

• People
  – Security Manager
  – Rigorous background checks
  – Separation of duties
  – Training
  – Experience

• Procedures
  – Identification of Sensitive Data
  – Key management
  – Audit
  – Intrusion Detection
Technology - Network

• Use HTTP/S (HTTP over SSL)
  – Web Servers Support HTTP/S
    • VoiceXML
    • Prompt Fetching
    • Some Backend Connectivity

• Redirect Through SSL Tunnels
  – “Transparent” To Existing Software
Network Encrypt - Challenges

• Speech Apps. Are Very Sensitive To Latency

• Encrypt Sensitive Data
  – Challenges include:
    • More Applications Impacting To Implement
    • Identification of Sensitive Data
    • Key Management
    • Not Always Point-to-Point
Application Log Files

• Easiest To Control
  – If It Is Sensitive, Don’t Log It!
  – Methods Include Suppression and Data Masking (Full or Partial)

• Identify What Is Sensitive During Requirements
  – Do Not Leave It To the Developers
  – Validate During Testing
  – Consider What Data Is Logged During Errors

• Includes VoiceXML App. and Browser logs
  – Includes Use of Log Tag
  – Ensure No Debugging Statements Are Left In Production Code
Vendor Log Files

• Hardest To Control, Easiest To Overlook
  – Includes: Application Frameworks, Browser, Reco, TTS, etc.
  – Example: May Log All DTMF Detection

• Know What Data Is Logged At Each Level/Configuration

Apache Access Log Example Logging Parameters Passed:


• Middleware Logs
  – Even If Network Is Encrypted, Messages May Be Logged
  – If Not Controllable, May Need To Additionally Encrypt the Data
Tuning Files

• Produces Event (Data) Logs and Utterances

• Prompts Played Could Be Logged During Tuning
  – Remember Confirmation!

• Build Tight Controls on Tuning of Sensitive Data
  – Requires Dialog Level Tuning Control
  – Require Additional Steps To Tune Sensitive Data
  – Some Data Should Never Be Tuned At the Same Time
  – Example: Account Number and PIN

• Always Encrypt Persisted Sensitive Data
Conclusion

- Know What Data Is Sensitive

- Secure Internally, Not Just Externally

- Know Where the Sensitive Data Is – Speech IS different!

- Know Where Sensitive Data Could Be Exposed

- Secure the Sensitive Data So It Is Not Exposed
Empowering Your customers and employees with speech technologies

SpeechTEKI 2006 Empower
The Voice Solutions Showcase

Thank You