Caller Authentication

Chuck Buffum
August 8, 2006
3 big questions

• How vulnerable (really) is my call center?

• What is available to strengthen my authentication?

• What are the obstacles for moving forward?
Vulnerability
Typical authentication tokens

IVR calls (DTMF or ASR)
- Account number
- PIN (4 digit)

Agent-handled calls
- Account number
- Two or three “content tokens”
  - Last 4 SSN
  - Date of birth
  - Zip code
  - Mother’s maiden name
Sources of compromise

Helpful customer service representatives
  • 5% of IVR calls roll over to agents for forgotten PIN
  • Myriad social engineering examples

Databases on the internet
  • Search by name & city (intended for private investigators)
    • Current address (zip code) & previous addresses
    • Full SSN
    • Date of birth
    • Drivers license
    • Marital status & family member/dependents names
  • Search by name & state (intended for genealogy research)
    • Mother’s maiden name

Stolen content
  • Account statements (dumpster diving)
  • Key logging and related forms of internet content theft
  • US Mail theft – entire blocks in a single day
Assessing your vulnerability

What authentication tokens do you require?
How vulnerable is each token?
Do “riskier” transactions require stronger authentication?
Can CSRs bypass authentication to “help” callers?
Are CSRs following security policy during peak hours?
Is there an auditable log of authentication tokens used?
Authentication Options

SpeechTEKI 2006
The Voice Solutions Showcase

Empower
Stronger authentication

Use multi-factor authentication

- What you know (traditional content)
- What you have (ANI/CLI)
- Who you are (voiceprint)
- What you do (behavioral pattern analysis)

Automate & log details of the authentication process

- Removes human error and gullibility
- Enables behavior analysis & fraud monitoring
- Enables remediation & audit ability (compliance)
Assessing possible tokens

All tokens can be compromised
Select tokens that complement one another’s strengths

Content tokens
  • Must be memorable for user and available in your database
  • Not too private (user will be saying out loud)
  • Not too easily compromised

Voiceprint tokens
  • Both text dependent and text independent are applicable
  • Longer enrollment with shorter token is better for consumers
  • Minimize cognitive load (random digits or use content token utterance)

Transparent tokens
  • ANI/CLI – assess calling patterns and quality of database
  • Behavior – presumes transaction logs and analytical engine
Security vs. Convenience

Strategic business concern
Consumer convenience cannot be compromised

Don’t extend the call duration
  • Replace a content token (or even 2) with a voiceprint
  • Use transparent tokens whenever appropriate

Don’t complicate the user experience
  • Minimize the change to the user experience
  • Sell the security and convenience benefits of the change

Expect opt-in enrollment vs. “passive” enrollment
Obstacles
Obstacles

Lack of reference deployments
   Many internal-facing references

Concern over consumer acceptance
   Several surveys show little or no consumer pushback

Admitting existing security is inadequate
   Can be turned into consumer protection benefit
Summary

Today’s call centers are vulnerable

Stronger authentication is available to be implemented

Careful design can strengthen security without compromising convenience

Security regulations (FFIEC) and privacy legislation are likely to drive stronger authentication in the coming years
Empowering Your customers and employees with speech technologies

SpeechTEKI 2006 Empower

The Voice Solutions Showcase

Thank You

Chuck Buffum
crack@buffumgroup.com