An approach to employing biometrics with no hardware, no software, no training

Presentation by: Peter Tapling, Authentify, Inc.

2003 Annual Computer Security Applications Conference
Las Vegas, Nevada
©2003 Authentify, Inc.
Abstract

» Biometrics is seen as a promising way to bind an individual to activities in the digital world. Many biometric solutions available today require some combination of specialized hardware, client-installed software, or significant user training in order for them to be successful. While applications for a controlled audience (such as employees) may find this acceptable, externally facing applications must overcome these problems. This session will present an approach to enabling Internet applications with integrated voice biometrics as piloted by one government agency.
Challenges of Any Registration Process

» Objective is to bind a carbon based persona to an electronic security credential
  • The **task** was performed user ID “dduck”, therefore the **person** who performed the task was [certainly] Donald Duck.

» Policies define process requirements
  • Policy will (should) reflect risk profile
  • [PKI has inherited some legal baggage (e.g. CPS)]

» Authentication for first time issuance is weak link
  • Shared secret only not near strong enough
  • “Personal presence” models prevalent, but operationally weak

» Delegation is often required to support broad communities

» Automation is desired to keep costs down
Additional Challenges Attributable to Biometrics

» “Answer” is no longer discreet
  • Biometrics are by their nature statistically based
  • Equal Error Rate becomes something to manage
» Biometric approach needs to be socialized
» New risks to consider
» Required software/hardware footprint, user training
» Capture device integrity
» Still have “first time” problem
Case Study Application

» US Social Security Administration
  • Registration for access to “Business Services Online” site

» Project was proof of concept to employ telephone authentication and voice biometrics to automate 3rd party authorization for access to the site
  • Goal to replace a paper-based, negative response process with a faster, higher quality process
  • Proof of concept was live during Q1/Q2 2003

» Application to eventually support:
  • Authentication for first time registration
  • Authentication for password reset
Basic Flow of Registration

1) User self-registers at site (name, SSN, FEIN, phone, email)
2) SSA checks that SSN works for FEIN
3) [Automated call placed to phone number, biometric captured]
4) User ID/Password issued to User
5) User identifies supervisor (name, phone, email)
6) Email delivered to supervisor
7) Supervisor follows link in email to approval site
8) Supervisor validates name/company name, enters SSN/FEIN
9) SSA checks that SSN also works for FEIN, FEIN matches
10) Supervisor validates/enters phone number
11) Automated call to supervisor, biometric captured, approval
12) If no approval, User’s ID cancelled
Business Services Online site enables businesses to self manage activities such as wage reporting.

BSO is a primary SSA initiative to address requirements of the Government Paperwork Elimination Act (GPEA).
During the proof of concept, users would complete the existing registration process, then self-select to participate in the test. This and following screen shots are from the proof of concept pages – they are *not* production SSA pages.

Welcome to this secure test site for receiving a PIN and Password from Social Security. Authentify Inc. is operating this website on behalf of Social Security.

Your participation and feedback are extremely valuable. Thank you for participating in the test of this potential new service.

Please Note: Since this is a test, Social Security will still mail a letter addressed to your employer to notify them that you applied for a PIN and password on their behalf. We will shortly mail your password directly to you.

The Paperwork Reduction Statement

This information collection meets the clearance requirements of 44 U.S.C. § 3507.
User identifies themselves and their company. This is a “light” version of the existing primary registration process.

Please complete the following information.

Fields marked with an asterisk (*) are required fields.

Information About You:

First Name*: Peter
Last Name*: Tapling
Social Security Number*: 000-00-0000
Phone Number: 773-243-0322
Phone Extension:

Information About Your Company:

Company Name*: Authentify, Inc.
BIN*: 000-000000
Are you Self Employed or head of your business? *
({Please select Yes or No})

Submit  Reset
Supervisor information is new information which would be collected. Note collection of phone number and email address as opposed to postal mailing address.
Supervisors are first introduced to the activity by an email which would, in production, from the SSA.

A primary benefit over the existing system is that a positive approval is sought from a named individual.
Supervisor is given an explanation of the process.

Welcome to the test site for enhanced Business Services Online. This site is operated on behalf of Social Security by Authentify Inc.

Thank you for responding to our email.

The purpose of this site is to evaluate the use of integrated Web, email, voice and automated telephony technologies for improving Social Security's Business Services Online while maintaining strong security. It will also measure the reaction of individuals such as yourself to the overall process.

Start The Process

The Paperwork Reduction Statement

This information collection meets the clearance requirements of 44 U.S.C. § 3507,
Supervisor enters/validates information.

Employee Peter Tapling has indicated that you are their supervisor.

If this is not correct please select the "No" button now.

No

Otherwise, please enter the following information about yourself and your company.

Fields marked with an asterisk (*) are required fields.

First Name*: James
Last Name*: Woodhill
Company Name*: Authentify, Inc
EIN*: 000-000000

Continue
Supervisor initiates an automated telephone call to their desk or current location.
Instructions on the process.

We will call you momentarily, however the following information is needed to complete the phone call. When you are ready for the phone select the "Call Me Now" button at the end of this page and we will call you then redisplay this page.

**Confirmation Number:** 412 073 6895
You will be prompted to say this number while interacting with the telephone.

You will also be prompted to say your telephone number twice during the call. This is the phone number you indicated on the previous page.

The final thing you will be prompted to say during the telephone call is either "I Authorize" or "I Deny". This will grant or reject access to Social Security’s site for your employee Peter Tapline.
Automated telephone call will:
- Validate intent
- Capture voice print
- Capture approve/deny recording

Use of phone provides “anchor” in the real world.
Summary Results

» Approval response from automated system improved 37%
» Audit trail from automated system deemed superior
» Survey results very positive

» Next Steps
  • Planned pilot during 2004

“I very much like the idea of voice identification. This process surpasses any other method of protecting my identity and SSN that I have seen. BRAVO!!

JoAnn W., Financial Advisory Firm
Rate the ease of the overall registration process, using Authentify.

Average Score 4.5

Rate the intrusiveness of the Authentify process:

Average Score 4.4

“I very much like the idea of voice identification. This process surpasses any other method of protecting my identity and SSN that I have seen. BRAVO!!

JoAnn W., Financial Advisory Firm
Lessons Learned

» This process will work
» Users broadly prefer the real time nature of a phone based process
» Use of the phone is very natural to users
» No need to “dumb down” the process – folks “get it”

» Biometric strategies
  • Manage EER towards successful enrollment
    – Phone offers true “multi-factor”
  • Balance risk of replay attacks against challenges of text independence
Benefits of Use of the Telephone

» Out-of-band trusted network
» Operates in true real-time
  • Can reduce exposure of temporary PINs to near-zero
» Uniquely engages a human in the process
» Requires no additional infrastructure or training
» Public Switched Telephone Network is highly auditable
» Phone is socialized as your “handle” for business
  • commercial or personal
» Can temporally bind digital transaction with authentication event
» Phone number is a “something you know”, controlling a phone acts as a “something you have”
Selected Authentify Customers

- Social Security Administration
- Associated Bank
- HP
- VeriSign
- PayPal
- Chicago Software Association
- IBM
- B2B Barter Bank
- Atrion
- GeoTrust
- AssureBuy
- Identrus
“On the Internet, nobody knows you’re a dog.”

... EXCEPT AUTHENTIFY!

Contact:
Peter Tapling
President & CEO
Phone: 773-243-0322
email: peter.tapling@authentify.com

©2003 Authentify, Inc.