opusresearch

Voice Biometrics Conference Takes on Growth and Challenges

A Conversational Access Technologies Advisory

May 7, 2007

Dan Miller
Senior Analyst

High-profile implementations, like VoicePay (in the UK) and Bell Canada's Voice Identification Service, signal a new era for voice biometrics technologies. Success in the near term is pegged on high levels of convenience and security for customer-facing applications. Long-term success will be linked to establishing spoken passwords as a highly trusted way to leverage existing infrastructure for securing Web-, mobile- and phone-based commerce.

"Big Mo" for Voice Biometrics

With several large-scale, customer-facing implementations in the works, voice biometric-based authentication is building momentum around the world. Opus Research's Voice Biometrics Conference 2007 became a place where vendors, practitioners and prospective implementers met to share experience and discuss issues giving shape to an emerging market.

The conference coincided with the rollout of two high-profile services: VoicePay and Bell Canada's Voice Identification Service.

In the case of VoicePay, a UK-based entrepreneur took an aggressive promotional stance for a new service that employs VoiceVault's Voice Sign technology as a certified "electronic signature" for credit card transactions. VoicePay founder, Paul Ogden, appeared on CNN on May Day and rode the ripple effect as local TV news stations picked up the story choosing to interview local "consumer advocates" – rather than techno-geeks or industry zealots – who described how spoken words provide a convenient way to secure credit card payments.

Later, from the podium at the Voice Biometrics Conference in Washington, DC, executives from Bell Canada and PerSay provided details surrounding the rollout of a service designed to make a spoken pass phrase into the universal identifier for a customer support line serving over 28 million customers across five services.

Building on Experience and Existing Infrastructure

While noteworthy in scope, size and visibility, recent announcements merely expand upon a base of longer-standing implementations of voice biometric-based applications. At the Voice Biometrics Conference, Oliver Geiseler from Volkswagen Financial Services AG, for instance, described how his firm went about deploying authentication solutions from VOICE.TRUST. In addition, Zsolt Kadar, from ABN AMRO, described how his company met the challenges of rolling out a voice biometric-based authentication service as an option for validating four million Dutch account holders. In this case, spoken codes provided less cumbersome alternatives to an existing authentication system that relies on smart cards nested in pocket sized keypads.

While noteworthy in scope, size and visibility, recent announcements merely expand upon a base of longer-standing implementations of voice biometric-based applications.

ABN AMRO's experience illustrates how voiceprints will co-exist with and extend the reach of existing user authentication systems. Likewise, Bell Canada's voice identification service is presented as a more convenient alternative to (but not a replacement for) an array of PIN-based services. In both cases, voice biometrics support each company's commitment to protecting privacy as they offer phone-based access to an increasingly complex and varied set of services.

Bell Canada is ahead of many of the diversified, incumbent telecommunications carriers. The simplicity of voice identification services parallel long-standing efforts to provide customer service through a single access number (310 BELL). Using speech recognition and call steering resources from Nuance, Bell Canada has had great success deploying 'Emily' – a single number and single voice offering customer service to wireline, wireless, high-speed Internet, digital TV and VoIP customers. Customers no longer have to remember or find toll-free numbers for each service as well as avoiding the headaches of navigating through multiple layers of IVR menus to get to the right agent or IVR system.

[At Bell Canada] using a spoken pass phrase for identification and authentication … was sold internally on the merits of cost savings and high levels of security and privacy.

Using a spoken pass phrase for identification and authentication helps customers avoid having to remember multiple PINs (for each service offered), while saving agent time associated with identifying and authenticating the customer. Bell Canada's service was sold internally on the merits of cost savings and high levels of security and privacy. At the same time, it solved a long-standing problem for telecommunications carriers who, until now, had no way of distinguishing between an "account holder" and a co-user.

Leveraging Existing Security Infrastructure

Both Bell Canada and ABN AMRO's approaches illustrate one of the recurrent themes that signal greater maturity and market potential for voice biometric solutions. They will augment existing security, speech processing, call processing and application processing infrastructures. Simply, these solutions provide cost savings for the company and convenience for customers.

At Bell Canada, for instance, the decision to move to a voice biometric identifier is left for the caller to make. When they call the customer service number, they are given the option to enroll in a simple, voice-based method for identification and authentication. At that point they initiate the enrollment process, which takes roughly two minutes, according to Bell spokespeople. If they choose to opt-out, they will stick with their existing PIN-based approach, or ask to be re-prompted in 60 days.

Bell Canada does not expect voice biometrics to replace the existing systems. The security infrastructure and workflows behind the voice biometric are "aware" of the caller's status and preferences. They enroll by repeating a passphrase three times. In subsequent calls, they are prompted to say the passphrase as a way to go straight into the voice response system or directly to an agent. Screen-pops let agents know whether a caller has enrolled in Voice ID and, if so, whether they have been authenticated.

The use of voiceprints presents a side-benefit of knowing whether the caller is identified as the "account holder" or as a co-user. This is something that a PIN-based system is incapable of determining. As of May 1st, more than 110,000 Bell Canada customers had registered at a rate of approximately 8,000 per month.

Voice biometrics has entered the next phase of maturity and self-realization.

Signs of Maturity and Self-Realization

Although it is often inaccurate to personify a technology, voice biometrics has entered the next phase of maturity and self-realization. Step one was to determine that voice biometrics (or voice prints) are best positioned as part of an overall security and access control application, rather than as a classic "voice processing application." The community crossed that threshold roughly two years ago.

Next comes the realization that voice can't do everything itself. In this day and age, few businesses or financial institutions believe that a single factor can suffice. Instead they use physical tokens, software tokens, PINs, passwords, challenge questions and other factors to build confidence in an authentication solution that suits the context of an application.

With maturity also comes recognition of the persistence of everyday things. This had not been an important lesson for the voice application crowd. In many cases, the case for building new voice or automated speech recognition systems involved a rip-and-replace tactic which relegated existing interactive voice response (IVR) infrastructure to the trash heap.

Next Up: A Security-Oriented Market Model

Melding voice biometrics with existing security infrastructure is the emerging deployment model. It is exemplified by the close relationship between long-standing security leader RSA (now a division of EMC) and voice processing's reigning giant, Nuance Communications. Opus Research has already discussed the implications of Adaptive Authentication for Phone (see "RSA Adapts Vocent Product Line," Nov. 3, 2006). As a platinum sponsor of the Voice Biometrics Conference, RSA shows ongoing commitment to expand its market share lead in strong authentication, encryption and access management over the telephone using voice biometrics.

In a 2006 report, Opus Research forecast annual spending of $400 million for voice biometrics solutions. That figure, pointedly, placed voice biometric security at more than twice that for automated speech processing (ASP) licenses. Such a comparison is inaccurate because voice biometric spending was largely accounted for by R&D and consulting projects, in addition to licensing and packaged solutions.

Spending on voice biometrics is set to resemble security sales at-large, where the unit of measure is a "credential," such as a token.

But at Voice Biometrics Conference, it became clear that the bespoke model is about to become passé. Spending on voice biometrics is set to resemble security sales at-large, where the unit of measure is a "credential," such as a token. Historically, voice processing software was licensed based on the number of active "ports" in IVR systems and, more recently, with the advent of IP-telephony, based on simultaneous users or "servers."

The move to credential-based pricing makes much more sense, given the problem that voice biometrics is positioned to solve. Yet, its adoption will not preclude pricing schemes that are based on transaction volumes, such as authentications or approval of online or phone based services. Nor will it preempt the idea of offering voice-based authentication as a service (software as a service) by a voice application service provider (VASP).

This report shall be used solely for internal information purposes. Reproduction of this report without prior written permission is forbidden. Access to this report is limited to the license terms agreed to originally and any changes must be agreed upon in writing. The information contained herein has been obtained from sources believe to be reliable. However, Opus Research, Inc. accepts no responsibility whatsoever for the content or legality of the report. Opus Research, Inc. disclaims all warranties as to the accuracy, completeness or adequacy of such information. Further, Opus Research, Inc. shall have no liability for errors, omissions or inadequacies in the information contained herein or interpretations thereof. The opinions expressed herein may not necessarily coincide with the opinions and viewpoints of Opus Research, Inc. and are subject to change without notice.