Monitoring Report – February, 2007

J. Markowitz, Consultants
Program A: Competitive Landscape and Standards Activities

This report is confidential and intended for registered JMC clients only

Competitive Landscape - SIV

Persay Achieves Profitability and Other Announcements

Israeli-based, SIV engine developer Persay made three announcements: it achieved profitability in 2006, it received additional venture funding, and that it is opening a US office.

POTENTIAL IMPACT: The most significant of these announcements is that Persay has become profitable. This is clear evidence that the market is growing. Having more than one profitable company in SIV is a very good sign because it indicates that the market is not ruled by a single vendor. The additional venture funds will enable Persay to solidify its profitability and enable it to open its US office in mid-2007.

DETAILS: In 2006, six years after being spun off from Comverse, Persay achieved profitability. Since it is a private company it was not possible to obtain details or a profit-loss statement of any type. The company does operate globally and has more than sixty deployments in Israel, North and South America, Europe,, Africa, and Australia. It also is the SIV supplier to British Telecom's URU online identity verification service and its technology is certified on the Microsoft Speech Server and Genesys Telecommunications Laboratories' GVP platform.

The company announced it had received funding from Israeli venture-capital company Athlone Global Security (AGS) made a $1 million investment. AGS is a private venture company that invests in emerging growth companies providing technology for homeland security. Last September, Shrem, Fudim, Kelner & Company (SFK), a leading Israeli financial-services and investment company, gave Persay $1.3 million in funding.

In May, 2007 Persay will open an office in New York City that will be the company's US Center for North American Operations The office will be headed by Ariel Freidenberg, Persay's VP of sales and business development, with the support of two US security executives, Steve Katz and Bill Marlow. Steve Katz is President of Security Risk Solutions and former Chief Information Security Officer for Citigroup. He will provide strategic development assistance in the financial services industry. Bill Marlow is an expert in security and risk management and former Senior Vice President for SAIC. He will help guide the company's commercial and government development programs.

CellMax Systems Partners with PCS Revenue Control Systems

Israeli SIV engine developer CellMax Systems Ltd. and point-of-sale system producer PCS Revenue Control Systems, Inc., announced the joint development of a payment system for school cafeterias that uses SIV.

POTENTIAL IMPACT: The use of biometrics in school cafeterias and other school activities is growing. The use of SIV remains fairly rare. This partnership could change that because of PCS's penetration of the academic market. Once the system has been developed we will be watching to see the kind of reception it gets from PCS's customers. The system will also need to overcome challenges that are unique to SIV, notably loud background noise and variable voice characteristics.

DETAILS: PCS Revenue Control Systems is a major supplier of point–of-sale and other systems for academic food service in the United States. PCS designs, manufactures and markets systems

for school meal programs and is one of only eight software programs available for state agencies school food authorities and local schools that are approved by the US Department of Agriculture to implement Nutrient Standard Menu Planning (NSMP).

The proposed system will authenticate each student as she/he purchases a meal in the school cafeteria. When the student says her/his name and student number that student's account data and photo come up on the food server's screen, the right lunch is placed before that student, and the student's account is charged automatically for the meal,. The goals of the system are to increase cafeteria line speed and to ensure that each child gets the meal she/he is supposed to receive. The project adds CellMax's SIV to PCS's line of cardless ID products. When it is deployed it will be the first time that SIV will be deployed in PCS-licensed lunchrooms.

Standard Life Adopts SIV from VeCommerce

UK financial-services provider Standard Life is deploying an SIV system in its IVR that was developed by Australian speech-processing solutions provider VeCommerce Ltd.

POTENTIAL IMPACT: This is another example of a financial-services institution that is strengthening security on its phone-banking services. This has become and continues to be a strong trend because financial services institutions, consortia, and regulators have been moving strongly to combat fraud and identity theft with strong authentication, including SIV.

DETAILS: SIV and speech recognition replace a pre-existing menu-based IVR systems that has a reputation for being inflexible and alienating customers. The new Standard Life system greets customers calling into the company with a human-like automated voice that asks the caller how it can help them. Customers can respond by speaking normal sentences such as 'I have a question about my pension'. The intention was to mirror the type of interaction a caller would have with a human agent. The use of automation is designed to maintain customer satisfaction while simultaneously driving down costs through self service.

A key component in the VeCommerce system is the VeConnect software which interprets the request, based on context and syntax rather than just key words and determines the most appropriate destination or specific agent for the call. In addition, VeSecure has also been deployed, which automates customer identification and verification over the phone prior to transferring the call to an agent, as well as VeQuery which allows customers to get the latest information on their policy values without having to speak to an agent. The underlying SIV and speech recognition technologies are provided by Nuance Communications.

Since the new system was deployed Standard Life has increased its call handling capacity by 25% and seen a 66% reduction in misrouted calls due to better first-time routing to the right advisor, resulting in higher levels of first-call resolution.

VxV Solutions Integrates vAuth with Ping Identity

US-based SIV integrator VxV completed an integration of its SIV-based authentication platform, vAuth and the Ping Identity PingLogin authentication and single sign-on framework for consumer authentication.

POTENTIAL IMPACT: VxV is new integration company that was founded by analysts from Opus Research. Their SIV platform was constructed from their experience working with and analyzing existing SIV technologies and solutions. The integration is one that other SIV solutions providers and engine developers have completed. The openness of Ping Identity Corp.'s platform and the popularity of single sign-on all make this an easy and attractive integration.

DETAILS: This is the starting point of a long-term strategic partnership between Ping Identity and VxV Solutions, which will include integration of vAuth with PingFederate for large corporate and government organizations.

The integration allows vAuth platform implementers to use their existing vAuth ID to log into PingLogin secured applications without the need for a password, token or other strong authentication mechanism. The integration will be available to all vAuth platform customers.
The integration was simplified due to VxV Solutions' support of the OpenID User-Centric Identity architecture. By leveraging the OpenID integration already available on the vAuth platform, VxV Solutions quickly created an application that acts as a bridge between a user's vAuth ID and a PingLogin authenticated single sign-on session. Using this method, no changes are required to an existing vAuth platform implementation.

Authentify and Purdue University Report on Study on SIV for Online Identity Authentication

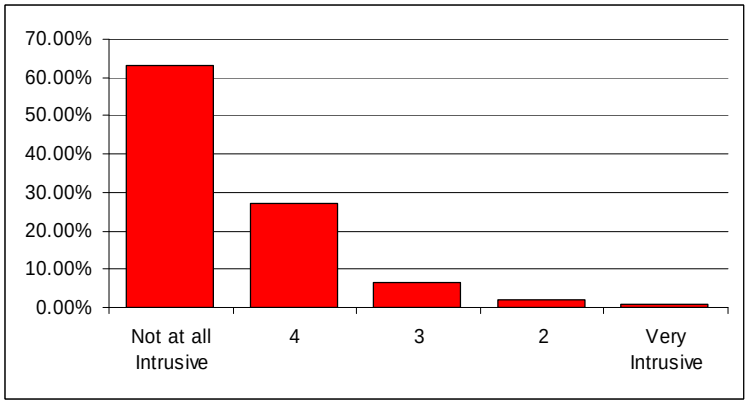
Authentify, a US supplier of SIV solutions, and the Biometric Standards, Performance, and Assurance Laboratory at Purdue University jointly presented the findings of a two-year study on SIV for online identity authentication in a talk, entitled *Case Study Phone-based Voice Biometrics for Remote Authentication*.

POTENTIAL IMPACT: This is the kind of usability and accuracy performance study that is sorely needed in SIV. This is a report on the first phase of the study which is going to look at other performance and usability factors.

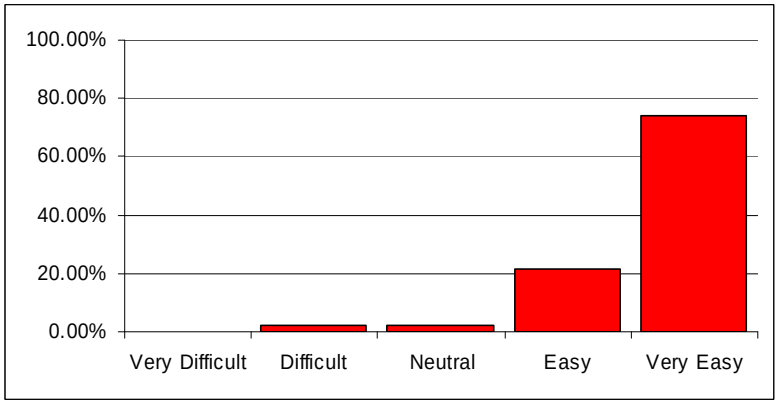
DETAILS: The talk was presented at RSA's annual user's conference. It describes the first phase of a study examining user acceptance, effectiveness, and reliability of phone-based voice biometrics for web-based applications and transactions. It was conducted at the Purdue laboratory Q4 2004 to Q2 2006. It addresses the questions: How does a voice biometric system perform for a typical remote authentication business scenario, and what conclusions can we make about the use of such a system?

To replicate voice biometric authentication in real world scenarios, the Lab conducted the study using the same system currently used by customers of Authentify. The process synchronizes an online user's web session with an automated, outbound phone call. The Purdue Lab recruited study subjects and oversaw field testing conditions for evaluating the use of land-based, mobile, and VoIP phones for remote voice biometric enrollment and authentication. Here are some of the findings.

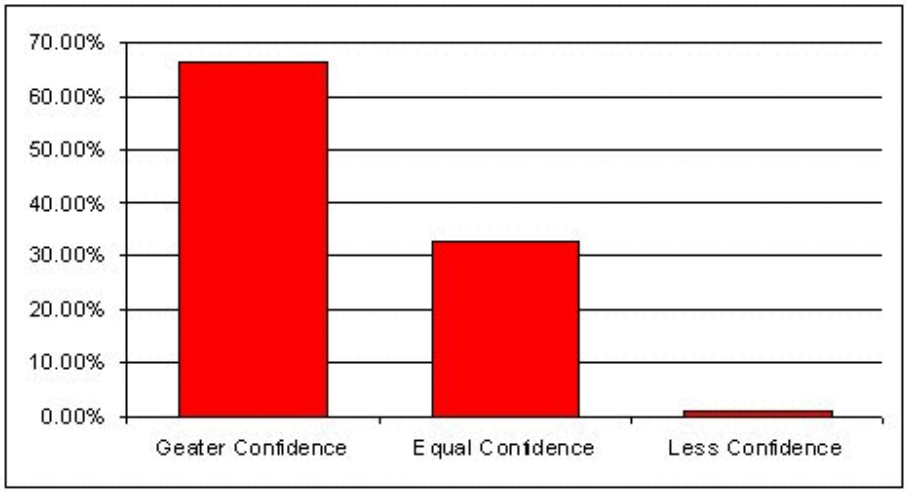
Question: How intrusive was the process?



Question: How easy or difficult was the system to use?



Question: When using this system do you feel more, less or the same amount of confidence
In the authentication security provided?



Authentify Named Codie Award Finalist

Chicago- based Authentify, a supplier of telephone-based, out-of-band authentication solutions using SIV was named a finalist in the Software & Information Industry Association's (SIIA) "Best Identity Management Solution" category of the 2007 Codie Awards.

POTENTIAL IMPACT: The fact that an SIV solutions provider was seriously considered for this aware is an sign that SIV is being taken seriously. Having an SIV solutions provider be a finalist enhances the visibility of SIV and the validity accorded to SIV solutions and products.

DETAILS: SIIA is the principal trade association for the software and digital content industry. The SIIA annual Codie Awards recognize the most innovative products and services in the software industry. Award winners in 72 categories are chosen from among finalist by votes cast by SIIA voting members. SIIA has more than 750 members who include well-known organizations, such as Bloomberg, Chemical Abstracts Service, Congressional Quarterly, Dow Jones, Factiva, McGraw Hill, Ovid, Proquest, Reed Elsevier, Thomson and Time Warner as well as software companies such as Apple, Oracle, Sun Microsystems, Novell, Symantec and Veritas.

This year is the 22nd year that Codie awards have been given out. There were a record number of nominations submitted: over 1,200 nominations by more than 600 companies.
The awards will be presented at the 2007 Codie Awards Gala held at the Palace Hotel in San Francisco on April 17, 2007.

TOPIC: Acquisitions by SIV Companies

Consolidation has not yet become as widespread in SIV as it is in biometrics and in the general speech-processing industry. The acquisitions that occurred this month reveal that those activities involve SIV companies acquiring technologies that are expanding their overall technology portfolios and do not represent industry consolidation.

Nuance Communications Acquires BeVocal

Nuance Communications, a US speech-processing and SIV engine and solutions provider, announced it signed an agreement to acquired BeVocal, a US provider of speech self-service solutions for the mobile marketplace.

POTENTIAL IMPACT: This is yet the newest Nuance acquisition, a company that grows by acquisition. The announcement took the speech-processing industry by surprise because Nuance (formerly Scansoft) is still digesting its latest acquisitions which include the original Nuance Communications and portions of Dictaphone. The acquisition of BeVocal is a part of Nuance's thrust into the mobile marketplace and makes it a far more viable competitor in that space. It is unlikely that SIV will be involved in deployments that result from this acquisition but it sets the stage for such developments.

DETAILS: BeVocal brings to Nuance a portfolio of highly repeatable applications; an established track record; and a predictable, recurring revenue stream derived from software-as-a-service and subscription-based offerings. BeVocal's customers include Cingular, Liberty Wireless, Metro PCS and Virgin Mobile. Nuance expects the acquisition to add between $21 million and $23 million in revenue in fiscal year 2007 and between $65 million and $70 million in fiscal year 2008. The acquisition is expected to be approximately neutral to earnings on a GAAP basis in fiscal year 2007 and $0.01 accretive per share in fiscal year 2008. On a non-GAAP basis, the acquisition is expected to be accretive to earnings, excluding amortization, stock-based compensation and non-cash taxes, by approximately $0.00 to $0.01 per share in fiscal year 2007 and $0.05 to $0.06 cents per share in fiscal year 2008.

Under the terms of the agreement, total consideration is approximately $140 million, net of BeVocal's cash and using yesterday's closing price of Nuance stock at $14.98 per share. The consideration comprises approximately 8.3 million shares of Nuance common stock and a net cash payment of approximately $15 million, due at closing. Terms also include the potential for additional cash consideration of up to $60 million in the form of an earn-out, payable 18-months after closing and based on the business achieving performance targets. The acquisition has been approved by both companies' Boards of Directors and is currently expected to close before the end of March 2007, subject to regulatory approvals and customary conditions.

Edentify Acquires Zelcom Group and Expands Board of Advisors

US identity-management company Edentify Inc. completed the acquisition of Zelcom Group, a privately-held provider of data analytics solutions. The company also added three security experts to its Board of Advisors.

POTENTIAL IMPACT: Although it claims to offer SIV, Edentify is a peripheral player in the SIV industry because it is focused primarily on general identity-management solutions. The announcements made this month reflect that orientation. Edentify and others that claim to offer SIV as part of a battery of identity-management technologies, represent acknowledgement of market interest in SIV. The activities of these companies are a good indicator of the potential directions that more pure-play SIV might take.

DETAILS: Zelcom brings advanced data-analysis services to Edentify that make Edentify's existing risk scoring technology more robust and expands the company's product line in that direction. The acquisition also enables Edentify to target Zelcom's customers, which includes a number of mortgage firms such as Aegis Mortgage of Houston, TX. Zelcom will operate as a wholly owned subsidiary of Edentify. Financial terms of the deal were not disclosed.

Edentify also added three security experts to its board of advisors, expanding the board to eight members. Samuel C. Lisker, Chief Information and Security Officer for America's Community Bankers Quinn E. Thomas, Vice President of ChoicePoint Inc.'s Public Record Business Unit, and Chuck Whitlock, investigative correspondent, author, speaker, and creator of the Crimeline program. The company expects these new board members to enhance Edentify's understanding of banking, credit bureau, government, and consumer markets.

Sentex Sensing Signs MoU to Acquire Vitelcom Mobile Technology

Sentex Sensing, a US supplier of SIV and other biometric solutions, announced that it signed a Memorandum of Understanding to acquire Spanish mobile phone manufacturer, Vitelcom Mobile Technology, its French subsidiary Purple Labs and Mexican subsidiary Vtech Holding.

POTENTIAL IMPACT: This acquisition moves Sentex solidly into the mobile phone handset arena and provides an outlet for its own prototype handset. The company has been pushing in that direction and has been trying to acquire BenQ, a former Siemens mobile division and another mobile-industry company in financial trouble. The acquisition of Vitelcom could provide Sentex with the entry into mobile products and services that it has been seeking.

DETAILS: Vitelcom's product line includes 3G, i-mode and Linux-based technologies and has manufacturing facilities capable of producing over 5 million phones a year. The company's sales are distributed amongst Spain and Latin America mainly for the Telefonica Moviles group. Vitelcom produced cumulative revenues in excess of $1.1 billion dollars over the past four years but was experiencing financial difficulties. Carlos Carrero, the sole shareholder of Vitelcom agreed in a "firm and binding" MOU to exchange shares of SNTX.OB for 100% of Vitelcom's common shares. The deal is worth around 60 million Euros. The binding Letter of Intent, engineered by Balmoral Capital Holdings and Miramar Capital, makes Vitelcom a Sentex subsidiary.

Competitive Landscape – Biometrics

TRUSTe Study: A Majority of Americans Surveyed Want Biometrics on Credit and Debit Cards

TRUSTe found that 82% percent of American consumers support the use of biometric identification on passports,

POTENTIAL IMPACT: The results are positive but I have a great deal of trouble with this survey. Despite the claim to represent the viewpoint of American consumers this study only interviewed little over 1,000 people. That is far too small a sample to even begin to be representative. Furthermore, the invitations were sent by email. I don't know how the invitees were selected but I do know that people who use email and who would take a survey via email are necessarily representative of those who don't use email. That's why I have far greater confidence in the results of the Javelin studies (see "Other Market News" below). That's also why I either qualified TRUSTe's use of "Americans" or changed the word to "respondents" and other comparable terms.

DETAILS: TRUSTe, an online privacy certification and seal program, and market information group TNS surveyed 1,025 U.S. consumers between September 25 and September 29, 2006. Three-quarters of those surveyed reported that they support the addition of biometric information to driver's licenses. Nearly as many (72.6%) support adding biometrics to Social Security cards. More than half (52%) of respondents agreed with the statement that "it will make it much harder

for terrorists to operate within the U.S. with the use of biometrics to establish the identity of Americans."

Seventy percent of respondents had heard of biometrics but the group as a whole seemed unsure about how effective biometrics are in combating identity theft. More than two-thirds of respondents (68%) believe that adding biometric identifiers to ID documents will make it much more difficult for thieves to steal their identities but a nearly identical proportion (67%) think that "criminals will find a way around the technology."

The survey also indicates that the subjects are willing to forego some personal privacy and anticipate misuse of the information in exchange for security.

- 53% of respondents agreed with the statement that the use of biometrics "will greatly reduce personal privacy because the government will be able to track your movements."
- 60% of respondents agreed that "there is a high potential for the government to misuse the information."

These results seem to indicate that in dealing with government use of biometric data, most people will tolerate a decrease in personal privacy to gain increased security in the form of physical safety. That didn't appear to translate to the retail sector because the survey found consumers to be more cautious about giving away their personally identifiable information. Three out of five people surveyed support adding biometric data to credit cards (64%) and debit cards (62%), but are much less likely to want that information on a retail store loyalty card (27%). This corresponds to other findings in the survey that 76% of respondents trusted banks and financial institutions "always" or "most of the time" as compared to 41% of respondents trusting retail stores "always" or "most of the time."

The survey revealed that consumers don't trust systems that use biometric identification as a payment method. Less than two percent of respondents have used a fingerprint payment system and 32% say that they "do not trust retail stores with this information." Only 23% of respondents expressed a desire to use this kind of payment system.

Methodology: The survey was commissioned by TRUSTe and conducted by market research group TNS. It polled 1,025 U.S. consumers between September 25 and September 29, 2006. Email invitations were sent to a nationally representative sample of the U.S. adult online population derived from the TNS NFO Internet Access Panel, which comprises more than one million U.S. households that have agreed to participate in survey research from time to time. In total, 1,025 online interviews were completed and the survey results are considered accurate to within three percentage points, 19 times out of 20.

TOPIC: Customers And Deployments

The following is a subset of the customer announcements in biometrics. These announcements were selected because they reveal the growing acceptance of biometrics as a whole in the private sector and among consumers.

BT Group PLC to Deploy Biometrics in Its Data Center

British telecom's BT Group PLC will spend 14 million euros ($27 million U.S.) over the next seven years on a new South London data center to strengthen its hosting and management services. The 10,010-square-foot facility, which will have biometric security features, should be complete by September and has additional room for expansion. The type(s) of biometric security to be used was/were not specified.

Dunkin' Donuts Switches to Biometrics

Ingersoll Rand Security Technologies announced that New Jersey Dunkin' Donuts franchise Alliance Management is using HandPunch biometric readers in 27 of the stores, with three more pending, to record time and attendance information from their over 300 employees. Alliance Management was using timecards but had numerous problems with them, including employees losing their cards. Furthermore, their time clocks were old and had to be replaced. Instead of

replacing the existing system with another time card system they opted to use biometric hand geometry. The new HandPunch readers have made payroll much easier. Now, instead of filling out or punching timecards, employees simply place their hands on the HandPunch. It automatically verifies the user's identity in less than one second. Employees use the units twice a day, to punch in and out. Store managers edit the punches and forward pay files to the company's in-house payroll department, which uses QuickBooks. Payroll is done bi-weekly. The results, according to Alliance Management, is greater accuracy, less cost, and better management of time and attendance.

ING Group Deploys Dealing Room with Biometric Solution From BIO-key International and Zvetco Biometrics

Biometric fingerprint identity management vendors BIO-key International Inc. and Zvetco Biometrics announced that ING Group implemented a biometric identity management system using their fingerprint and identity-management technologies. The system employs BIO-key's VST biometric matching software and Zvetco's Verifi fingerprint readers. Dutch biometric consultant BioXS integrated the two systems

ING Group is a global financial institution offering banking, insurance and asset management to over 60 million private, corporate and institutional clients in more than 50 countries. With a diverse workforce of over 114,000 people, ING comprises a broad spectrum of prominent companies that increasingly serve their clients under the ING brand. According to an ING representative "The real value of this added security measure is that in addition to improved security and Sarbanes-Oxley compliance, the biometric identity management improves dealer productivity. In the past, complex passwords were required for ING dealers to access secure trading room workstations, which were easy to forget or lose, and had to be changed often to maintain optimum security. Now, access to ING's dealer room computers is always at the user's fingertip."

TOPIC: Products and Partners

The number of products and partnerships in biometrics is growing rapidly. Although many vendors talk about the importance of financial services the partnerships that are being forged often involve other industries and the products still tend to be more general in terms of vertical.

NAFCU Services Signs Deal with BioPassword for Online Identification Solution

National Association of Federal Credit Unions Services Corp (NAFCU) signed an agreement making keystroke dynamics vendor BioPassword a preferred partner for multifactor authentication

As of December 31, 2006, multifactor authentication is now required for high-risk online/electronic financial transactions. It will soon be extended to self-service telephone transactions. The selection of BioPassword rather than a fingerprint, iris, or face recognition vendor is an indication that financial services are serious about looking at all biometric options. This is significant for acceptance of SIV, signature/sign recognition, and other forms of biometrics that are not part of the most visible government deployments.

BioPassword is one of the few companies providing keystroke dynamics technology for preventing fraud. Like SIV, authentication with keystroke dynamics is often tied to a password but may extend to more general keystroke patterns and it does not require the use of a special input device (keyboard). Keystroke dynamics examines speed, pressure, and other typing cadence patterns.

Sarnoff Labs Developing Covert Iris Scan Technology

US-based Sarnoff Labs has applied for a patent for a scanning method that scans irises as a pedestrian approaches a checkpoint - without the person being aware of it. The system uses an array of compact, high resolution cameras pointed in slightly different directions and each focusing on slightly different distances. When the subject comes into range (around nine feet/three meters away from the sensor) an infrared strobe light begins to flash in synchronicity with the camera exposures. This produces a bank of images, one of which should provide a view of the iris that is good enough for iris scanning biometrics to analyze.

The lab has filed for a patent that contains the following description of the technology: “A method and apparatus for obtaining iris biometric information that provides increased standoff distance and capture volume is provided herein. In one embodiment, a system for obtaining iris biometric information includes an array of cameras defining an image capture volume for capturing an image of an iris; and an image processor, coupled to the array of cameras, for determining at least one suitable iris image for processing from the images generated for the image capture volume. The image capture volume may include a plurality of cells, wherein each cell corresponds to at least one of the cameras in the array of iris image capture cameras.”

It is not clear how long development of the technology will take.

Instantaneous Age-Recognition System Created

Omron Corp. in Kyoto has developed the world's first system to instantly analyze a human face to determine whether the person is an adult or minor. The firm expects the system will be installed in video game arcades that have minimum age requirements and in alcohol vending machines. According to Omron, the system analyzes creases and sags, which appear on a face as the subject grows older, by matching them with a pictures of a million people of a variety of ages. The photos in the picture database are mainly of Asians, including Japanese, ranging in age from 3 to 80. The firm shot the pictures simultaneously using 80 cameras to capture the faces from various angles and researched skull shape and facial features. By collecting the pictures, the firm found that children's eyes are relatively larger in proportion to the face than those of adults and tend to be located lower on the face. Their eyes and eyebrows are also relatively further apart, and their lips are thinner and their chins are rounded. On the other hand, adults tend to have lines and sagging around their eyes and creases on their lips. Adults' faces also tend to be leaner, Omron said. Although the system is not as accurate if the subjects are wearing makeup or are baby-faced, the system can analyze pictures in 0.2 seconds to determine the subject's sex and age with, according to the company, 90.6% accuracy.

Standards Activities

MRCP Version 2 to Undergo More Changes

The Internet Engineering Technology Form’s (IETF) Media Resources Control Protocol (MRCP) is a low-level resource control standard for media resources, notably speech technologies. It facilitates communication between speech engines and the applications that need to use speech technologies in a standardized fashion that conceals the details of communication from application and system developers.

Many speech recognition and text-to-speech synthesis engine providers are MRCP compliant and MRCP has been incorporated into the VoiceXML language which extends standards-based development for the fast-growing body of application developers, system integrators, and platform developers.

Version 2 of MRCP adds support for SIV, SIP, and generally moves the standard more strongly in the direction of Web services. A few months ago, we announced the release of MRCP V2 Draft 11 for comment. Draft 11 was expected to be the final draft. Because of this, the IETF’s Internet Engineering Steering Group (IESG) examined the draft with regard to language and format. The IESG found quite a few typographical errors, many of which had protocol implications, and misuse and/or confusing use of core terms, such as SHOULD and MUST. The determined that there were enough of those errors that the document would never pass IESG muster. They announced that the editors have begun a final scrubbing of the document and will be producing a new draft and that there will be another Work Group Last Call (WGLC) on that draft before redoing the IESG Shepherd document and passing it to the IESG. The editors are restricting their work to scrubbing the document and will not entertain comments that will extend the protocol.

ISO 19092 (Part 1) Biometric Security Management

This standard replaces ANSI X9.84 and is an extension to ISO/IEC 17799-2005 *Code of Practice for Information Security Management*. Although this standard was developed through the financial

services group within ISO (for political reasons) it is designed to apply to any industry that uses policy-based biometric authentication. It specifies the requirements for securing and managing biometric information for all biometric applications and environments; this includes transmission and storage of biometrics information.

Key aspects of ISO 19092 are:

- Biometric system validation depends on maintenance of a secure **biometric event journal** that can be used for legal and regulatory compliance and ISMS audit.
- Control objectives and security controls can be tailored to meet the needs of an organization; **the binding of biometric security policy and practices to the biometric reference template (voice model)** enables biometric applications to 'transform biometric information into policy-based management action'.
- A Biometric Policy (BP) specifies a set of rules tied to a biometric reference template used by a set of application with common security requirements.
- A Biometric Practices Statement (BPS) defines the security practices followed by an organization during the biometric reference template lifecycle.

ISO 19092 extends and internationalizes X9.84 with new features requested globally by financial services. The new features include auditing, template management, Biometric Practice Statement, etc. There are two parts to ISO 19092 whereby Part 1 (above) is approved and Part 2 CD3 is going to DIS ballot. Part 2 specifies schema for secure biometric data, standard messaging formats and standard audit formats. It is stated to be CBEFF compliant though that is not formalized.

Other Market-related News

***Government Security News* Releases List of Top 100 DHS Contractors for 2006**

Government Security News (GSN), a publication for IT defense contractors and government agencies, published its annual "top ten DHS Contractors" for 2006. The list contains 100 companies who received the largest value of total contracts awarded by DHS between Oct. 1, 2005 and Sept. 30, 2006.

Only one biometrics contractor was on the list: Northrop Grumman Information Technology (#19) has a multi-year $357 million contract from the U.S. Citizenship and Immigration Services to provide biometric capture services. The lack of biometric suppliers is actually an opportunity for SIV and other biometric technology and solutions providers because the real value of this list is to provide names of companies tied into DHS that could become partners.

The list was compiled by *GSN* during the first week of December 2006, based on data made available by the Federal Procurement Data Center, a unit of the General Services Administration (GSA). About one-third of the companies that appear on the list are doing clean-up and other work related to Hurricane Katrina. This is one reason why giant construction and engineering firms (e.g., Fluor, Shaw Environmental and Bechtel) topped the list, rather than the systems integrators, technology companies and consulting firms more commonly associated with homeland security programs. In addition to well-known security contractors, the list includes a number of low-profile companies and organizations that have not received much attention in recent years, such as J.H.M. Research and Development, of Silver Spring, MD (#10) and Cooperative Personnel Services, of Sacramento, CA (#18). [for more information see *JMC Monitoring February, 2007 Report for Program C: Government Projects and Biometrics Initiatives*]

Javelin Study Finds Decline in Identity Theft

Javelin Strategy & Research, which does frequent surveys of the cost and occurrence of identity theft reported on its most recent survey. Despite the recent reports of hacking in Vermont, TJMAXX, and elsewhere combined with stolen FBI laptops and a missing hard drive at the US the Veterans Administration, Javelin saw a 12% decline in the overall cost of identity theft (from

$50 billion to $45 billion). In addition, Javelin observed that there were 500,000 fewer victims from one year to the next.

They attribute the decline to improved antifraud practices. In particular, improvements by credit-card providers, such as instituting better security practices related to mailed credit cards. Mail theft of credit cards accounts for 9 % of all identity thefts because they are easily stolen in transit and used on the Internet. Consumers have also contributed to the decline of identity theft. Unfortunately, young adults remain the most likely group to suffer ID theft because they take security risks, such as downloading music from illegal sites and not protecting their systems with anti-spy and anti-virus software.

Javelin also explained the discrepancy between their findings and a Gartner Group study that found ID theft to be on the rise. According to Javelin, Gartner's survey did not include groups that Javelin includes in its surveys, such as the 30% of Americans who do not use the Internet. This different indicates that the Internet remains a major source of identity theft. The Javelin research was sponsored by CheckFree, Visa USA and Wells Fargo & Co.

EQUS Group Study Finds Mobility and Security Biggest IT Concerns for 2007

Technology market research firm EQUS Group released its latest industry report, "Corporate Outlook for 2007: Security & Privacy," which identifies mobility and security as the two most pressing issues facing IT executive in 2007. The study report details the concerns of 83 IT executives and found that the majority of respondents ranked protection from attack as their highest concern, with 77% ranking its importance as 'high' or 'very high.' Proprietary data protection ranked second in importance, with 71% of respondents identifying this issue as high or very high importance. The majority of respondents also cited customer and client privacy and regulatory compliance as areas of continued importance for 2007.

An area of special concern is data theft from mobile devices, including thumb drives. According to EQUS “These devices have become indispensable business tools, and, as a result, companies are walking a fine line between trying to protect their networks and allowing employees the tools they need to do business.”

The study also examined whether smartcards and biometrics would be widely implemented this year. Only 13% of companies plan to implement smartcards in 2007. Just 9% of companies have plans to implement Biometrics this year.

Microsoft VISTA Speech Commander Function Poses a Potential Security Threat

Vista users can use the operating system’s Speech Command tool to instruct their computers to perform many operations. Security researcher George Ou tested whether Speech Command could be used by a malicious website feeding a wav file which would speak commands to download malware. This is an example of how friendly and security unaware speech recognition can be. In the 1990s, a similar problem was discovered with the speech command on MacOS. People would stand behind someone using a Mac and shout “shutdown” which caused the computer to shut down. There is no way to prevent something like this from happening except to disable Speech Command until Microsoft creates a patch that prevents it from listening to its own speakers or speakers of neighboring computers.

The wav file could be played through the speakers and be picked up by microphone. Once that happens the Speech Command would execute those commands. Mr. Ou reported the results of his findings to an online security discussion group that had been discussing Vista security. "I recorded a sound file that would engage speech command on Vista, then engaged the start button, and then I asked for the command prompt. When I played back the sound file with the speakers turned up loud, it actually engaged the speech command system and fired up the start menu. I had to try a few more times to get the audio recording quality high enough to get the exact commands I wanted but the shocking thing is that it worked!" This included being able to replace long URLs with voice macros so that he didn’t have to spell out the URLs. He also found that the system would respond to instructions from voices that had not been enrolled/trained. One of the other list participants pointed out that this kind of technique could be used to attack multiple computers at once. The scenario was a large stock-trading room. In the middle of the night one computer shouts the following sequence: "start listening", "start", "internet explorer", "download <some malware>.”

Technology for Monitoring Airplane Passengers

Scientists working on the Paris-based Security of Aircraft in the Future European Environment project are spending £25 million to develop an onboard threat detection system that will dramatically reduce the possibility an airplane will be hijacked. The system employs tiny and microphones that monitor the behavior of aircraft passengers during a flight. The cameras the size of a fingernail and would be fitted into the back of each seat. The location of the microphones was not specified but would likely be near the cameras.

The approach links video and audio analytics technology to the profiles of individual passengers and has the goal of preempting terrorist activity. The system will sound an alert in response to suspicious behaviors that indicate nervousness (notably, rapid eye movements, blinking excessively, or licking lips) the microphone could pick up suspicious chatter as well (e.g., recitations of the Koran or other Muslim prayers).

Although the system could probably not be deployed for at least ten years it has already attracted criticism from civil libertarians. In contrast, the airline industry has expressed cautious interest in the plan and hopes the cost of such a system could remain manageable. The industry is also looking at a variety of more near-term technology solutions.