InformationWeek :: reports

Next

Reports.InformationWeek.com October 2011

Get the Best of Biometrics

As data volume and sensitivity grow, companies cannot rely on password- and token-based authentication. Biometrics can be used to provide strong access control, but you must weigh added complexity and costs against assurance that users are who they say they are.

By Michael Cobb

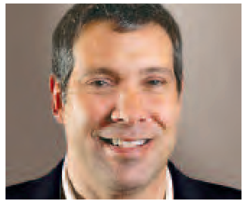
Presented in conjunction with

SECURITY dark READING
Protect The Business Enable Access

Report ID: S3731011

TABLE OF CONTENTS

Figures



ABOUT US

InformationWeek Reports' analysts arm business technology decision-makers with real-world perspective based on qualitative and quantitative research, business and technology assessment and planning tools, and adoption best practices gleaned from experience. To contact us, write to managing director **Art Wittmann** at *awittmann@techweb.com,* content director **Lorna Garey** at *lgarey@techweb.com,* editor-at-large **Andrew Conry-Murray** at *acmurray@techweb.com,* and research managing editor **Heather Vallis** at *hvallis@techweb.com.* Find all of our reports at *reports.informationweek.com*

Michael Cobb

InformationWeek Reports

Michael Cobb, CISSP-ISSAP, is a renowned security author with more than 15 years of experience in the IT industry. He is the founder and managing director of Cobweb Applications, a consultancy that helps companies secure their IT infrastructures and achieve ISO 27001 certification.

Michael co-authored the book *IIS Security* and has written numerous technical articles for leading IT publications.

EXECUTIVE SUMMARY

Use of biometrics has long been touted as the best way to overcome the vulnerabilities associated with password- and token-based authentication. With nonbiometric authentication, as long as people enter the correct combination of user name and password, either memorized or generated, they are granted access, regardless of who they actually are—users are authenticated but not positively identified. The system can verify only that users are in possession of the correct information, not that they originally enrolled with this information.

This inherent weakness is forcing companies with valuable information assets to seek better ways to control access. In this report, we examine the benefits and drawbacks of biometrics as a means of authentication, provide a snapshot of available biometric authentication technology and consider what the future may hold when it comes to this intriguing technology.

Previous Next
Table of Contents

Measuring Life

The basic premise of biometric authentication is that every individual is unique and anyone can be identified by his or her intrinsic physical or behavioral traits. (The term "biometrics" is derived from the Greek terms “bio,” meaning life, and “metric,” meaning to measure.)

There are two primary types of biometric measurement:

- *Physiological:* the shape of the body
- *Behavioral:* the behavior of a person

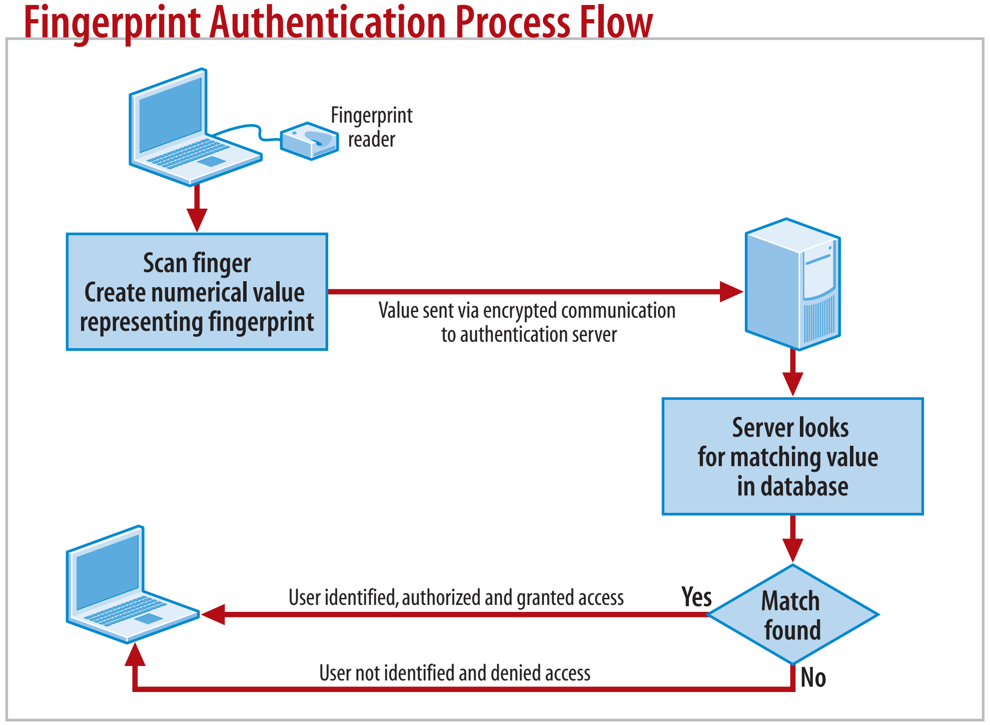
Most people are familiar with biometric techniques such as fingerprint and face recognition, which leverage physiological characteristics, but certain behavioral characteristics, such as typing rhythm, gait and voice, also can be used.

How It Works

Many people are under the misconception that biometric authentication involves the direct comparison of the biometric trait—an actual image of a fingerprint or face compared with fingerprints or face images stored on the authentication server. What actually happens is that the device capturing the image creates a numerical value to represent the fingerprint or face, and it is this value—a digital hash of distinct characteristics—that is sent to the authentication server for comparison with other stored values (see Figure 1).

Figure 1

Fingerprint Authentication Process Flow


Fingerprint reader
Scan finger
Create numerical value representing fingerprint
Value sent via encrypted communication to authentication server
Server looks for matching value in database
Match found
Yes
No
User identified, authorized and granted access
User not identified and denied access

Data: *InformationWeek Reports*

In facial recognition, for example, the camera first captures an image of the face, cleans it of unnecessary artifacts such as background noise, and then extracts relevant characteristics such as the distance between the eyes, width of the nose, shape of the cheekbones and length of the jawline. These values are then used to create a template. By discarding information that isn’t used for biometric measurements, the size of the template is reduced. If identification is the goal, this template is compared with all templates in the database. If a user name is also entered, the template is compared directly with the one associated with that user name. All authentication credentials passed between the user and server must be encrypted to prevent an eavesdropping attack.

The Downsides of Biometrics

Given that biometric technology has been around for quite a while, it may seem odd that its use is not more widespread. The primary system of criminal identification used during the late 1800s was devised by French criminologist Alphonse Bertillon. It involved taking numerous and precise measurements of the body and recording shapes of the body in relation to movements, along with markings such as scars, birthmarks and tattoos. Fourteen measurements were deemed necessary to avoid duplicate identities.

Bertillon's system relied on precise measurements, yet different people recorded different measurements for the same person. The amount of time and effort it took to collect the measurements, and the overall inaccuracies inherent in the process, led to its being quickly replaced when fingerprinting emerged as a more efficient and accurate means of identification. Further, the problems of accuracy and efficiency Bertillon faced in ensuring correct identification are still a challenge with today's biometric technology.

Other factors also have slowed the adoption of biometrics, and many of them have to do with cost.

The price point of technology required to implement a biometrics system fast and accurate enough to deliver an acceptable identification process has only recently dropped to levels that make it a viable option not just for government and military systems. The costs of readers and authentication servers that process biometric data are still more expensive than alternative authentication systems such as challenge-response or one-time password (OTP) tokens.

There is also the cost of enrollment, the process of adding users to the system, which is a prerequisite for any kind of authentication. With a biometric system, enrollment involves capturing and storing users' biometric information. Even at a one-site location, the logistics of successful enrollment require careful planning, with time allocated for each individual, including remote workers, to complete the process. Enrollment does in fact rule out biometrics as a means of authentication in many scenarios. Remote enrollment can't be trusted, and in, say, a business-to-consumer scenario, people are unlikely to agree to line up at the bank to have their retinas scanned and install infrared cameras on their PCs to log in to their online accounts.

Indeed, user resistance due to privacy concerns has been and still can be a barrier to adoption. The most accurate biometrics are those that can't be seen externally, which require some form of physical intrusion. And, from the company's side, biometric data is of course personally identifiable information (PII), which must be afforded the same protection as other PII data. Unlike passwords, the security of biometric data is a legal requirement under laws such as the Health Insurance Portability and Accountability Act and Federal Information Security Management Act, with severe penalties for data breaches. Additional

Related Report

Just 27% of the 438 business tech pros responding to our 2011 identity management survey say their firms have comprehensive IdM deployments. Will the consumerization of IT and the adoption of SaaS-based apps spur an IdM renaissance? Get our research and analysis.

Download

FAST FACT

74%

of companies using IdM for their employees require more than one authentication factor, our research shows.

steps must be taken to restrict access and usage to predefined purposes, all of which have cost implications. Although it would be difficult for attackers to automate the abuse of stolen biometrics in the same way they can passwords (they still have to fool the biometric reader), the implications for the victims are significant, as biometric characteristics can't be readily replaced.

Finally, there is still room for improvement when it comes to the ability of biometric systems to correctly match submitted biometric data with the person. With a password-based model, it is easy for a computer system to check whether the password submitted equals the password stored in its database. With biometrics, there is an element of interpretation, so the comparison is more "like" than "equal to." This means authentication is subject to false negatives, which prevent valid users from authenticating successfully, and false positives, which allow unauthorized users to authenticate successfully—the last thing you want in an authentication system.

The matching algorithm has to make a decision based on an acceptance threshold. This determines how close to a template the input must be for it to be considered a match. Users won't tolerate frequent false negatives, so the threshold has to be set below the ideal—where nobody would be granted access incorrectly—to reduce the number of false negatives, but this in turn increases the number of false positives.

The following performance metrics, therefore, must be considered when assessing a biometric system:

- *FAR (false acceptance rate):* percentage of users incorrectly granted access
- *FRR (false rejection rate):* percentage of valid uses incorrectly denied access
- *FER (failure to enroll rate):* rate at which attempts to create a template fail
- *FTC (failure to capture rate):* probability that the system fails to detect a biometric input when presented correctly
- *EER (equal error rate):* rate at which accept and reject errors are equal, with a lower EER being more accurate

Why Use Biometrics

Given all of biometrics' drawbacks, why do governments and large enterprises rely on the technology to control access to sensitive data and restricted areas, and why are smaller companies also starting to deploy biometrics?

With rising threat levels, increasing systems interconnectivity, and the mounting volume and value of data being held and shared by computers connected to the public Internet, data owners are reevaluating their access control methods. There is a growing need to go from checking that someone has the correct login information to ensuring that the person using the information is also the rightful owner of the information. The only way to achieve this is by using biometrics.

The ubiquitous user name and password combination can be too easily guessed or obtained by an adversary. Tokens such as OTP generators have an inherent weakness—they can be stolen. But criminals can't guess fingerprints the way they can guess passwords, and users can't forget their fingerprints the way they can forget their passwords, or misplace their fingerprints the way they can lose their tokens. Physical attributes can't be faked the way ID cards can. Any individuals who have uniquely authenticated themselves using biometrics can be tied directly to any actions they then perform. This is not the case with other forms of authentication.

Biometric systems also have lower administrative overheads: no more password resets; lost tokens; distributing, renewing and replacing tokens: or revocation procedures for lost and stolen tokens. Most mainstream network operating systems now allow the easy integration of biometric authentication to replace or supplement passwords. Depending on the nature of the assets being safeguarded, the false negatives threshold can be set to ensure the correct level of protection. Some systems allow you to set different thresholds for individual users. This is important, as the quality of each user's biometrics will vary—for example, as we age, our fingerprints fade. All these benefits make biometrics extremely attractive.

> "As more devices get built-in cameras, face recognition could surpass fingerprints as the biometric of choice."

Biometrics: Today's Choices

Let's take a look at the kinds of biometrics currently available:

DNA Profiling: DNA, the nucleic acid in nearly all living organisms that carries genetic information, is considered the ultimate biometric measurement, as it can produce proof-positive identification of a person, except in the case of identical twins. However, unlike other biometrics, it compares actual samples rather than templates generated from samples. Its main drawback is that comparisons can't be made in real time, so for now its use is limited to forensic applications. Although there will no doubt be advances in DNA capture and analysis, the technology is unlikely to be suitable for anything other than highly secure government environments.

Ear Recognition: Human ears are unique in size, shape and structure. The process of enrollment and authentication for ears is very similar to that for faces, though far less common or established. It is based on the distinctive shape of each person's outer ears. This form of biometrics will probably never gain too much steam, as face recognition will always be more palatable and intuitive for the user.

Face Recognition: Development in facial recognition currently focuses on image capture and pose correction. Improved processing times will allow real-time recognition even if the face is visible for just a fraction of a second. Pose correction aims to correct a nonfrontal image by fitting a 3-D morphable model onto a 2-D image, then rotating the model into a frontal 2-D image suitable for use. Skin biometric technology, based on the uniqueness of skin texture, is also being used to provide greater accuracy in recognition. A picture is taken of a patch of skin, called a skinprint. Using algorithms to turn the patch into a mathematical, measurable space, the system then distinguishes any lines, pores and skin texture.

The proliferation of devices with built-in

Previous Next

Table of Contents

cameras means face recognition authentication is likely to gain traction. It passes the acceptability test and requires no physical contact. As more and more devices get built-in cameras, face recognition could surpass fingerprints as the biometric of choice. It is a natural extension to the ubiquitous employee ID badge and closed-circuit television cameras. Interestingly, there is often a natural point at which to enroll users, whether they're employees or consumers—an employee's first day, queuing at a control point such as a check-in desk at an airport or hotel, or the company reception desk. You also can use face recognition to identify people in a crowd or to check that people in a controlled area are authorized to be there.

Figure 2

Biometric Types and Usage

Biometric	Type	Access Control
Body	Physical	Physical
DNA	Physical	Physical
Ear lobe	Physical	Logical/physical/remote
Face	Physical	Logical/physical/remote
Fingerprint	Physical	Logical/physical/remote
Gait	Behavioral	Physical/continuous
Iris/retina	Physical	Logical/physical/remote
Keyboard/mouse	Behavioral	Continuous
Palm	Physical	Logical/physical/remote
Signature	Behavioral	Physical
Voice	Behavioral	Logical/physical/remote

Data: *InformationWeek Reports*

Fingerprint Scanning: Fingerprints are by far the most common biometric used. Fingerprints are a safe and inexpensive method of verifying a person. Many laptops and keyboards now come with built-in fingerprint readers, and mobile phones also are coming on the market with built-in fingerprint authentication to control access to the phone's features. Fingerprint authentication is popular in areas where users need rapid access to information, such as in medical environments, because a simple swipe of a finger authenticates the user. There is a wide range of choices when it comes to fingerprint scanning, and in places where you have a variety of users with a variety of devices, it's probably the easiest biometric to roll out.

There are two types of fingerprint scanners: optical and capacitance. Optical scanners are more widely used mainly because they are less expensive. Capacitance scanners are more compact, and can check blood flow and temperature. The accuracy of optical entry-level readers can be affected by substances on the finger, such as sweat and oils, so these readers are not a great choice for use in areas where there's a lot of dirt, such as building sites or industrial plants.

Iris and Retina Scanning: The irises of the eye have more than 200 unique identifying characteristics—about six times as many as fingerprints. Iris identification takes only a few seconds, and when used for PC access, the camera that captures the iris image can double as a webcam. Retina scans, which examine the pattern of blood vessels inside of the eye, take longer and require the person to hold his or her eye close to the scanning device for 10 to 15 seconds.

Retina scans are the most precise and reliable biometric that can be viably used by businesses today, with advocates estimating the error rate is only one in a million. Retina scans are used in very high-security environments; they are currently too expensive to be practical for widespread use. Also, many consider retina scanning too invasive, because it involves examining inside the body.

Research in this area focuses on improving image acquisition and quality, including the ability to capture usable iris images from people moving in a crowd. Like all image-capture biometric systems, research is being done to improve segmentation algorithms, as more efficient algorithms can reduce the amount of time it takes for a scanning device to create a quality template.

Gesture Recognition: Every individual has unique mannerisms and body language traits. Analysis of body movements such as gait can be used to identify people from a distance. Gait is hard to disguise because a person's musculature essentially limits the variation of motion, and measuring it does not necessitate any contact with the person. A walking person does generate a large volume of data to be analyzed, however, requiring additional resources to store and analyze it in real time. In addition, surveillance cameras must be resighted to capture more than just faces. This field of biometrics can provide continuous authentication, ensuring that only authorized people are in restricted areas, but it is suitable only for organizations that need to be kept highly secure on a 24x7 basis.

Figure 3

Biometric Usability

Biometric	Ease of Enrolment	Ease of Use	Accuracy
DNA	1	1	4
Ear lobe	2	3	2
Face	3	4	3
Fingerprint	4	4	3
Gait	2	2	1
Iris/retina	3	3	4
Keyboard/mouse	3	4	1
Palm	3	4	3
Signature	4	4	2
Voice	3	4	2

Ease of enrolment/ease of use: 1 difficult to 4 easy; accuracy: 1 low to 4 high
Data: *InformationWeek Reports*

Handwriting Analysis: Although the shape of a signature can be copied, subtle details within a signature are difficult to replicate. This is because of the muscle memory required to write a signature that results from many years of repetition. Signatures can be used for face-to-face authentication and for systems in which users have devices that can capture pen input. However, other technologies are more accurate, limiting handwriting analysis's appeal.

Palm Scanning: Palm scanning uses vascular pattern measurements and offers a big advantage over fingerprints because it doesn't require any contact with the reader. For example, Fujitsu's PalmEntry access control system uses infrared light to capture vein patterns and generate a biometric template. This means factors such as lotions, abrasions and skin conditions that can interfere with the accuracy of contact readers aren't a problem. It can be used for logical or physical access control in most environments. Blood must be be actively flowing for the reader to give a positive identification, so it's not useful in forensics. But given the contactless nature of palm scanning, the technology has a lot of potential for use in public areas. However, the larger footprint of the scanner means it is less likely to replace fingerprint readers for desktop authentication.

Typing and Mouse Recognition: Keystroke length, typing speed, error patterns and mouse movements all can be used to create a unique template that distinguishes one person's typing from another's. Authenticating users in real time based on their mouse movements and keystrokes can combat the danger of stolen user names and password as they are continuously validated against a stored template. Infrastructures supporting large numbers of users, such as customer support desks that regularly access sensitive data, will find this additional form of authentication likely to become the norm, just as large enterprises run both gateway and desktop antivirus protection.

> "When planning for biometric authentication, be sure the system you choose will meet both short- and long-term needs."

Voice Recognition: Your voice is actually a physiological trait, but voice recognition also analyses the *way* a person speaks, so it's considered a behavioral trait. It works by taking a phrase spoken into a microphone and comparing frequency, intensity and other measurements with a prerecorded version. This method isn't as definitive or enduring as fingerprints, as voice changes with age and cultural immersion. However, voice authentication doesn't usually require additional hardware, as most computers now come with built-in microphones. It also can be used as a form of out-of-band authentication, with users calling in to authenticate themselves, thus avoiding man-in-the-middle or keylogger attacks. These calls can also be crossreferenced with authorized numbers when used for remote access. Voice recognition technology is the obvious biometric choice for any services that involve automated voice prompts.

Planning for Biometric Authentication

It is important that your choice of biometric authentication system meet both short- and long-term needs. When assessing the suitability of a biometric trait for use in an authentication system, consider the following factors:

- *Universality:* Every person using the system should possess the trait
- *Uniqueness:* The trait should provide sufficient differences to distinguish users
- *Permanence:* How rapidly a trait may vary over time
- *Measurability:* Ease of acquisition or measurement of the trait
- *Performance:* Accuracy, speed and robustness of the technology
- *Acceptability:* How willing users are to have this biometric trait captured and assessed
- *Circumvention:* How easy it is to imitate the trait using a substitute

Fingerprints have become popular because they exhibit all these traits except circumvention, but no one biometric will be a perfect option. To ensure you make the right choice for your organization, gather input from IT, security, business process owners and your users with consideration to the following:

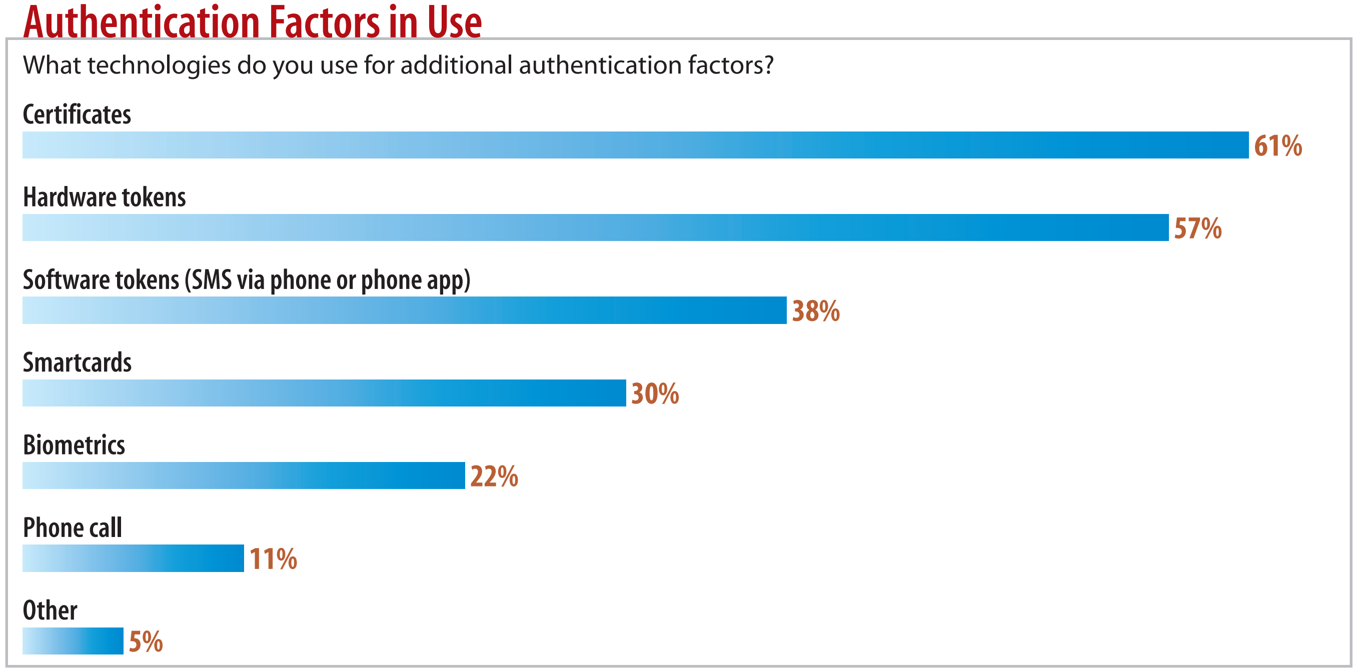
Deployment and Configuration: Your risk environment must justify the overall price of a biometric authentication system, factoring in setup, integration and user training costs. The best products come with all drivers and software preloaded on the scanning device. Avoid products that require anything beyond basic user interaction.

Suitability and Ease of Use: Security and usability should be the two biggest influences on your choice of technology. Spend time testing and choosing a product that suits you and your users. Where do they work and how do they work? For example, do they need rapid access to a variety of computers, or do you need to support the latest mobile devices, with employees accessing the network from a variety of locations?

Enrollment and Training: Plan how you intend to enroll all your users, as this process must take place in a trusted environment. Users will need training and, in some instances, assurance about the use of their biometric information. If possible, go for a gradual rollout, getting your initial users up to speed and ironing out any wrinkles before proceeding with mass deployment.

Figure 4

Authentication Factors in Use



Note: Multiple responses allowed R3020711/7
Base: 175 respondents at organizations using internal identity management for employees and requiring more than one factor of authentication
Data: *InformationWeek Analytics* 2011 Identity Management Survey of 438 business technology professionals, June 2011

Cost and Maintenance: Guided by your risk assessment, minimize cost and support by enrolling only those employees who need access to sensitive data or areas. If you're issuing scanners to everyone, the additional support and replacement costs add up quickly. In addition, a smaller user group is easier to train and manage.

Vendor lock-in is a potential risk. Be wary if you have to buy an entire suite of products—client-side applications, middleware and back-end authentication systems—from a single vendor. Wherever possible, choose a system that supports standards-based authentication protocols, such as the initiative for open authentication.

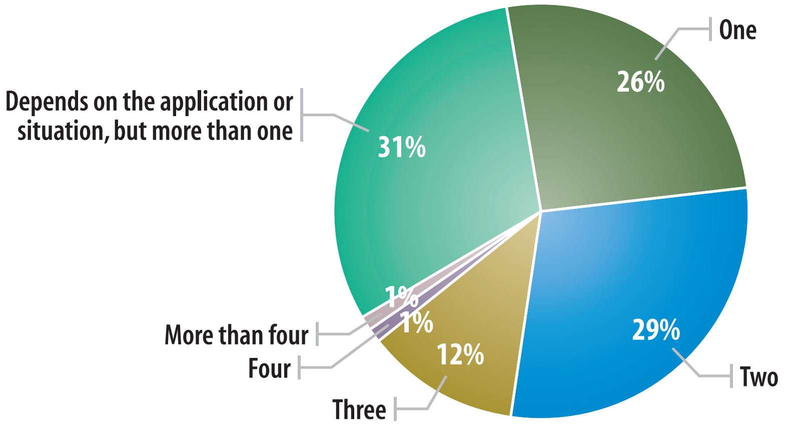
Scalability and Flexibility: To achieve an acceptable return on investment, it is important that your choice of biometric technology and products will meet future needs. To avoid unwanted surprises, you should know at what point an increase in the user base will require a change in your license or an upgrade to your authentication server.

Avoid any products that aren't installed and successfully running at a similar-sized organization. Take time to find out what other agencies or enterprises are doing. For example, PerSay's voice biometric technology is used in companies such as British Telecom and Bell Canada, which has more than 2.5 million voluntary enrollments in a system that uses the customer's voice as the password. NEXUS, operated by U.S. and Canadian border services, uses iris recognition in self-serve kiosks and reserved lanes at land crossings.

Figure 5

Number of Authentication Factors

How many factors of authentication are required to verify identity? For example, something you have, something you are, something you know, time-based authentication, biometrics.



Base: 235 respondents at organizations using internal identity management for employees R3020711/6
Data: *InformationWeek* Ö[ÍĜĊsâ2011 Identity Management Survey of 438 business technology professionals, June 2011

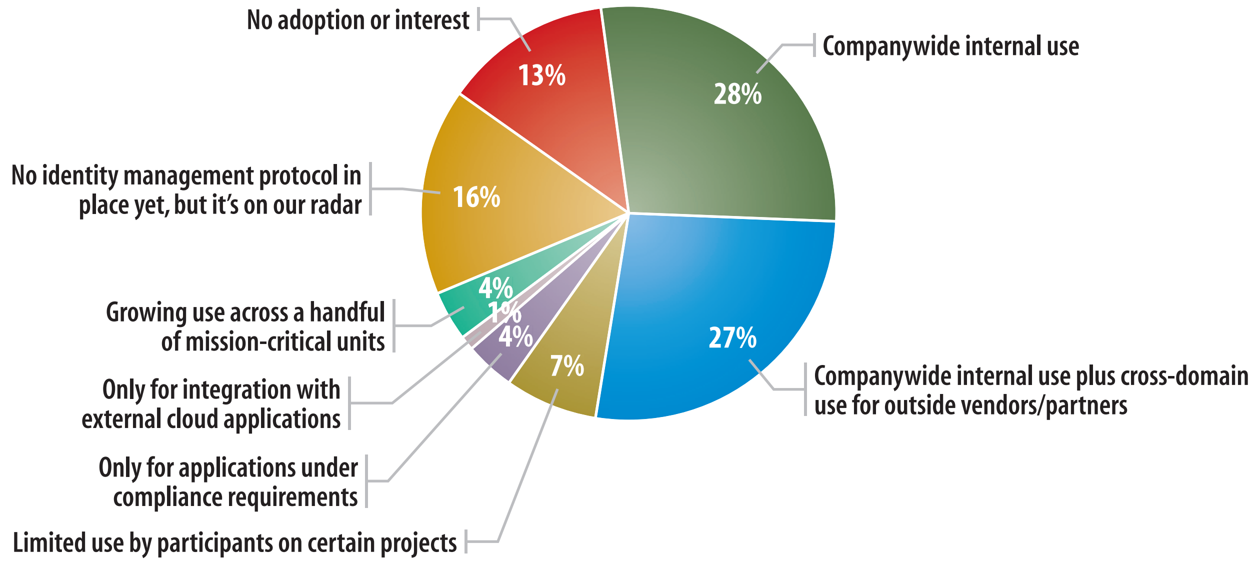
Security: Any form of hardware-based authentication will improve your overall level of security, but how far you need to raise the bar will be dictated by the results of your risk assessment. You may need the additional protection of out-of-band or bidirectional authentication. Once you have a shortlist, run extensive trials with a variety of users to see how the authentication process works in everyday use.

You'll need to include your authentication infrastructure in your security audits, particularly those used for physical access control. Many readers and scanners have built-in

Figure 6

Scope of Identity Management Use

Which of the following best characterizes the use of identity management within your organization?



Data: *InformationWeekĈ Ö[ÍĜĊÆsā* 2011 Identity Management Survey of 438 business technology professionals, June 2011 R3020711/1

storage for user information and fingerprint data, often with a USB port for uploading fingerprints and accessing log data. Unlike authentication servers, which reside in protected areas, these devices are positioned at building entry points or other generally accessible locations.

Looking Ahead

Science is continually finding and devising new ways to distinguish one person from another, but for any technology to gain widespread acceptance, there must be a set of standards to ensure quality and interoperability. The new ISO/IEC 24745 standard provides guidance for the protection of biometric information during storage and transfer. It also aims to address the risks of biometric information being compromised.

Unlike a password or security token, biometric identifiers can't be reissued. Your fingerprint is difficult to keep secret because a print is left on most things you touch and, once stolen, cannot be reset to a new value. This dilemma is being resolved using cancelable biometrics that work by distorting the biometric image or features before matching. The distortion characteristics can be changed easily and the same biometrics mapped to a new template. Biometric technology is improving all the time, with each new advance increasing accuracy, efficiency or ease of use. Biometric technology also has strong support from government.

New ways of measuring the body also are being developed. Facial thermography detects highly distinctive heat patterns emitted by the skin. It works much like facial recognition, but an infrared camera is used to capture the images so it works even in poor light or total darkness. Researchers also are looking at measuring skin composition, nailbed structure and body odor. The last is quite challenging, as deodorants and perfumes, diet and medication all can influence human body odor. Given that scientists have recently developed fluorescent bacteria that create a living invisible ink, we will likely see new weird and wonderful ways of measuring life in the not-too-distant future.

Certainly, as biometric systems become more commonplace, setup costs will fall, making the technology an option for an even wider range of situations. Still, the issue of privacy must be resolved. What we see now as outlandish or unacceptable may well change in the years ahead—who would have thought 15 years ago that laptops would come with built-in fingerprint readers? Given the ever-increasing number of threats to our personal and corporate data, people may become more accepting of new and better ways of controlling access to it.

FAST FACT

22%

of firms that require more than one authentication factor for employees use biometrics, according to our IdM poll.

Previous

Table of Contents

MORE LIKE THIS

Want More Like This?

Making the right technology choices is a challenge for IT teams everywhere. Whether it's sorting through vendor claims, justifying IT projects or implementing new systems, there's no substitute for experience. And that's what *InformationWeek* provides—analysis and advice from IT professionals. Our Reports site houses more than 900 reports and briefs, and more than 100 new reports are slated for release in 2012. Right now, you'll find:

Research: 2011 Strategic Security Survey: The 1,084 security pros responding to our 14th annual strategic security poll say CEOs are finally making risk management a priority. They also weigh in on the emerging risk areas of mobile devices and social media, as well as security budgets, software development, compliance and the cloud.

Strategy: How to Choose Multifactor Authentication: With so much business dependent on the Internet, security requirements and regulatory mandates are increasing pressure on business to adopt strong, multifactor authentication methods—user names and passwords are no longer sufficient. In this report, we show you how to weigh cost vs. risk in selecting the Web authentication method for your high-risk applications.

Strategy: Hardware-Based Authentication: Ready to consider replacing your password systems with hardware authentication products, which are becoming easier to deploy and manage? Factor in these six decision points.

PLUS: Find signature reports, such as the *InformationWeek* Salary Survey, *InformationWeek* 500 and the annual State of Security report; full issues; and much more.

Newsletter

Want to stay current on all new *InformationWeek Reports*? Subscribe to our weekly newsletter and never miss a beat.

Subscribe