Keystroke Dynamics:
Low Impact Biometric Verification

Tom Olzak
September 2006

Biometrics has long been one of the solutions touted by security vendors to meet multi-factor authentication objectives. However, user acceptance and cost issues often prevent organizations from adopting biometrics as a solution. This isn't to say that other multi-factor solutions are any less cost prohibitive. The capital expenditure and on-going maintenance costs of token-based systems are often higher than those for biometrics. Solutions based on keystroke dynamics might help meet these business challenges.

In this paper, I look at biometrics in general. This includes success factors for implementation and user acceptance. I also look at how the effectiveness of biometric solutions is measured. This is followed by an examination of keystroke dynamics technology, including its history, how it works, and why it may be the answer for organizations with people or cost issues.

Biometrics

Biometrics—when used with a PIN or password—is the use of unique human physical characteristics to identify and authenticate authorized personnel. You can use these devices to control doors, gates, etc. Biometric access control solutions can be applied to a wide variety of challenges, including room or building access as well as network or device identification and authentication.

Human traits used for biometrics are divided into physical and behavioral. There are several human physical characteristics that can be used to uniquely identify a person. They include:

1. The retina, specifically the blood vessel pattern inside the eye
2. Voice patterns
3. Finger or hand geometry, including fingerprints, finger or hand height and width, etc.
4. The features of the iris, the colored area of the eye surrounding the pupil

Behavioral traits identify a person through how she performs some measurable activity. Two examples include how she types—keystroke dynamics—and how she moves her mouse.

Success Factors for Biometrics

When considering the purchase and implementation of a biometrics identification system, An organization should address the following eight critical success factors:

1. Accuracy
2. Speed
3. Resistance to counterfeiting
4. Reliability
5. Data storage requirements
6. Enrollment time
7. Perceived intrusiveness
8. User acceptance

Accuracy

Biometric devices have improved significantly over the past several years. However, there are still no guarantees of 100% accuracy. It's your responsibility to select the level of inaccuracy that you and your employees can tolerate. When judging error rates, consider the principle
types of errors—Type I and Type II. Type I errors include all instances in which a biometric system denies access to an authorized user. The identification of an unauthorized user as an authorized user is an example of a Type II error. By adjusting the sensitivity of the biometric sensor, you can increase or decrease the occurrence of each error type. However, as you decrease Type I errors, you increase Type II errors. The opposite is also true.

The key objective in implementing a biometric system is the proper balance between these two error types. The most common method is to focus on the Cross-over Error Rate (CER). This is the point at which the frequency of Type I errors (False Rejection Rate or FRR) and the frequency of Type II errors (False Acceptance Rate or FRR) are equal. When shopping for the right system for your business, the CER is the best indicator of overall accuracy.

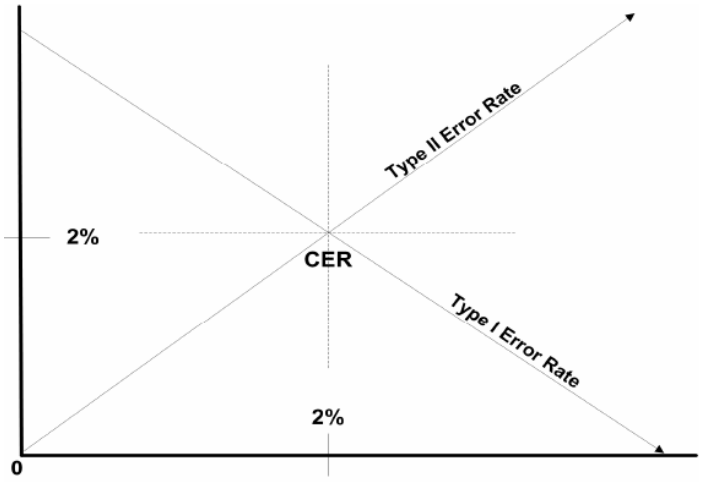

Figure 1: CER and Error Rate Relationship

CER is expressed as a percentage. Lower values are better. Values of two to five percent are generally considered acceptable.

Speed

When considering the probability that your users will accept the use of biometrics, the speed at which a sensor and its controlling software accept or reject authentication attempts is the most important factor. The effective throughput, or how many users a biometric sensor can
process in a given period, is a function of the entire authentication process. Figure 2 depicts the several stages involved. Acceptable throughput is typically five seconds per person or six to ten people per minute. User frustration begins to set in at lower throughput rates.

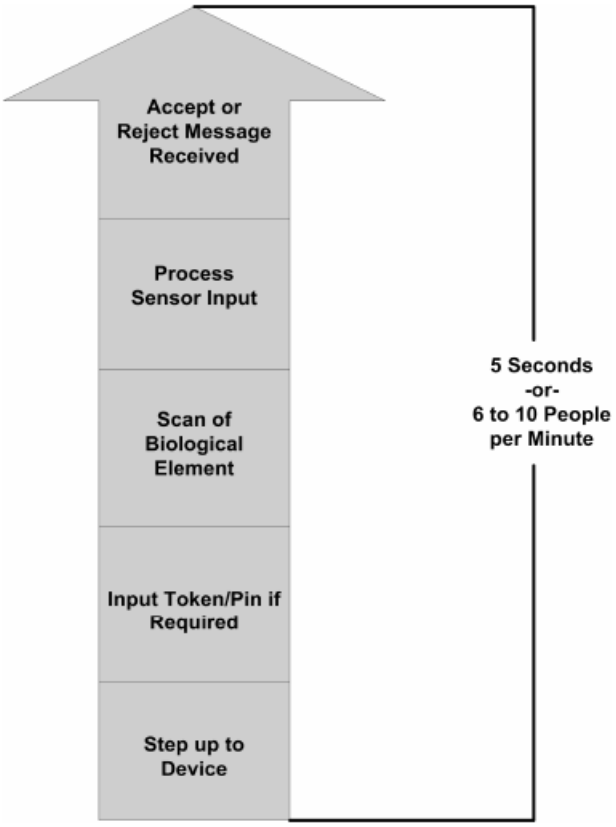

Figure 2: Biometric Authentication Process

Resistance to counterfeiting

Some biometric solutions might be susceptible to counterfeiting. For example, some early systems allowed an intruder to use lifted finger or hand prints to gain entry. Today's systems are, in general, more sophisticated; they use the entire geometry of a finger or hand instead of just the line patterns that make up prints. Make sure to ask the right questions if you consider using a biometric access control system. When possible, request a demonstration of the system's resistance to counterfeiting.

Reliability
Sensors must continue to operate at a low CER between failures. A gradual degradation in throughput affects user acceptability and organizational productivity.

Data storage requirements
The amount of storage necessary to support a biometric system depends on what data is actually stored. Voice recognition systems might use a great deal of storage; voice files are usually large. Current finger architecture recognition technology, however, simply stores a relatively small hash value created when a user is enrolled. Whenever a sensor scans the finger again, it re-computes the hash value and compares it to the stored value. Whatever biometric solution you choose, make sure you understand the impact on your storage environment.

Enrollment time
Another factor influencing user acceptance is the time required to enroll a new user into the biometric system. An acceptable enrollment duration is usually two minutes or less per person. This enrollment rate not only reduces employee frustration but it also helps reduce
administrative costs associated with system management.

Perceived intrusiveness
Second only to throughput, the amount of personal intrusiveness a sensor presents to your employees is a major determinant when assessing user acceptance. The following is a list of common fears that grow out of biometric implementations.

1. Fear that the company stores unique personal information
2. Fear that the company is collecting personal health information (retinal scans look at patterns that are also used to determine certain health conditions) for insurance purposes
3. Fear that the red light in retinal scanning sensors is physically harmful
4. Fear of contracting diseases through contact with publicly used sensors

One way to deal with these issues is to hold open and honest discussions about how the systems work, the health risks involved, and how the organization plans to use the information. Remember, user acceptance doesn't depend on how *you* perceive biometric authentication. Rather, it depends on how your employees perceive it.

Another way to address the issues surrounding intrusiveness is to deploy a solution that is not only non-intrusive, but it also adds no additional effort to authentication or authorization activities.

Keystroke Dynamics

Keystroke dynamics (KD) is a behavioral biometric. KD solutions usually measure both of the following:

- Dwell time – how long a key is pressed
- Flight time – how long it takes to move from one key to another

The way a person types can verify his identity with a FAR of approximately .01% and a FRR of approximately 3.0% (Checco, 2006). Table 1 shows how this compares with these same metrics for other types of biometrics.

Biometrics	FAR*	FRR*
Fingerprint	~0%	~1%
Voiceprint	~1.6%	~1.8%
Typeprint	~0.01%	~3.0%

*FAR—False Acceptance Rate
*FRR— False Rejection Rate

Table 1: Error Rate Comparisons
(DeepNet, 2006)

The slightly higher error rates might prevent KD from being used as an identification mechanism. However, it can easily fulfill a verification role for what most organizations will consider reasonable and appropriate multi-factor authentication.

History

The use of KD as a method of identification is not new. During the early days of the telegraph, operators were able to identify each other by the way they tapped out Morse code. This identification method, known as the "fist of the sender", was also valuable as a verification/identification method during World War II. Figure 3 depicts a timeline that shows how the technology has evolved.

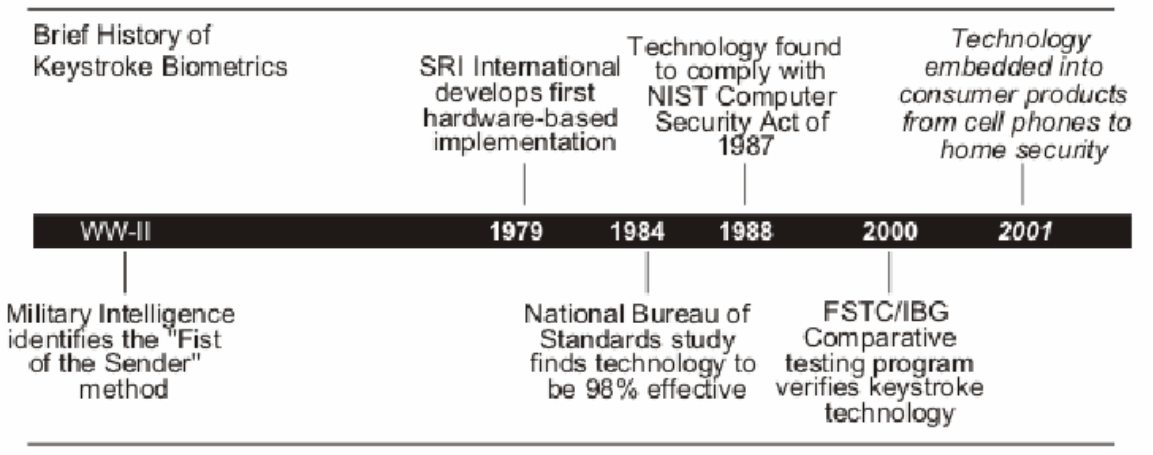

Figure 3: Keystroke Dynamics Timeline
(Checco, 2006)

How KD Works

To demonstrate how KD works, I'll walk through the basic functionality of the solution developed by BioPassword. This should in no way imply that I endorse the BioPassword product. Other companies, such as iMagic Software and DeepNet Technologies, also provide low impact KD biometric solutions.

As we've already seen, there are two metrics used to verify the identity of a user—dwell time and flight time (see Figure 4). As a person types, the KD application collects the time each key is pressed down and the cycle time between one key-down and the next. For verification purposes a known verification string is typically typed (i.e. account ID and password).

Figure 4: Keystroke Dwell Time and Flight Time
(BioPassword, 2006)

Once the verification string is entered, it's processed through an algorithm that compares the person's typing behavior to a sample collected in a previous session. The output of the comparison is a score. If this is the first time the KD system has seen this user, the algorithm is used to enroll her instead of verifying her identity.

If the score falls within a range defined by the organization as acceptable, and the password entered is correct, the user is authenticated and verified—access to the network is granted. If the score is not acceptable, business rules can be defined to determine how to proceed. Figure 5 depicts this process.

As you can see from the graphic, an organization can apply business rules to determine how the collected information and the comparison results are used. For example, an

employer who intends to roll out KD technology might choose to collect typing behavior samples without any interaction with the employees. This allows the silent and non-intrusive enrollment of all network users. Further, the KD system improves over time. This means that the more samples collected for a specific user, the lower the CER when verification is actually turned on.

Business rules can also be used to support the verification process. The error rate of biometric technology can be frustrating to both the users and the business. With KD technology, a business rule can be written to prompt the user for a cognitive password when the score is close but not quite close enough.

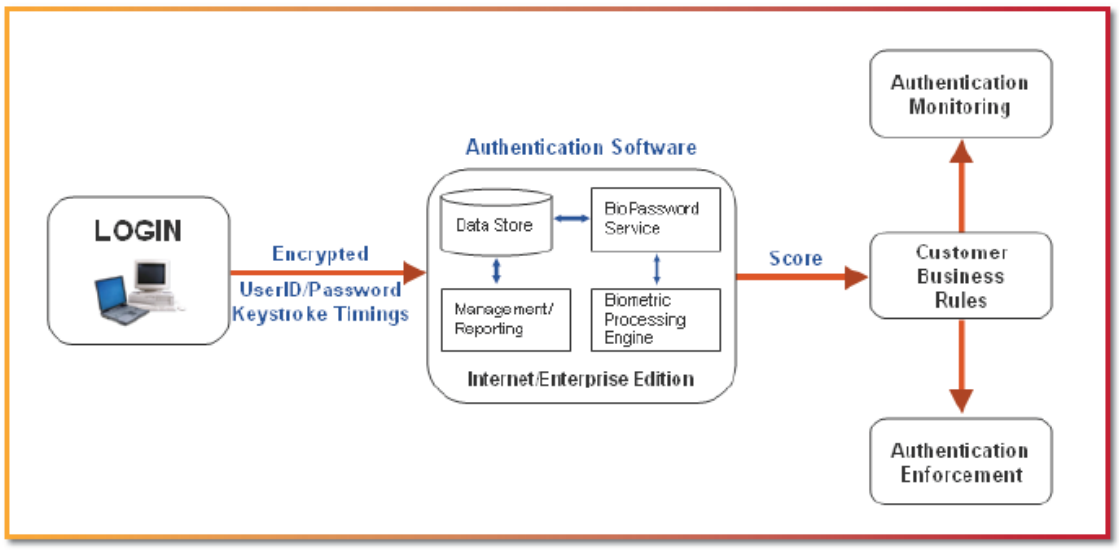

Figure 5: Authentication Monitoring and Enforcement
(BioPassword, 2006)

Low Impact Deployment

Earlier in this paper we examined the eight success factors for a biometrics solution. Several of these challenges are addressed or eliminated when considering a KD implementation.

Accuracy

The accuracy of KD solutions today is a little higher than other biometric technologies like fingerprint scanning. However, the ability to use business rules to react quickly to resolve errors potentially mitigates employee or management frustration. The use of business rules provides the tools necessary to significantly reduce the frequency of Type II errors without causing the usual productivity issues related to a corresponding increase in Type I errors.

One downside is the possible requirement to build an effective set of rules to ensure effective user verification.

Speed
Unlike fingerprint scanning or smart card authentication methods, the user isn't required to do anything other than log into his system. This is a daily routine that results in a transparent verification process. In such cases, speed is not an issue. There is one issue, however, that KD can introduce into an organization due to speed constraints—the inability to merge physical security and logical security multi-factor authentication methods.

Many organizations are combining physical access controls with computer network authentication controls. This results in a single control mechanism that's easy to manage by both the employees and the business. However, KD solutions don't necessarily work efficiently for physical access control if speed is an issue. In my opinion, it's faster to place a finger or a hand on a biometric sensor than it is to walk up to a keyboard and enter a verification string.

If the use of KD unacceptably slows physical entry, but it's the computer network verification control of choice, physical and logical access methods might have to remain separate.

Resistance to Counterfeiting
The use of biometrics without the use of a password or PIN is not without serious vulnerabilities. KD is no different. But like other biometric technologies, KD solutions require the use of a PIN or password for authentication; KD should be used to verify identity only. When used in this way, KD is very resistant to counterfeiting.

Reliability
As fingerprint scanners age, error rates can increase. This is not a problem with KD technology. The only entry device used is the keyboard—any keyboard.

Data Storage Requirements
I was unable to identify any storage advantages when using KD. This is the one success factor I believe is the same for all types of biometric solutions; make sure you have enough disk space.

Enrollment Time
Theoretically, there is no enrollment time with KD. The user simply starts typing and enrollment can be made absolutely transparent to her. She doesn't have to travel to a specific location nor does an organization have to designate a person at each location as an enrollment administrator. Enrollment is non-intrusive, low cost, and has little or no effect on productivity.

Perceived Intrusiveness and User Acceptance
Unlike fingerprint and retina scanners, the user doesn't have to touch or be touched by any special device. Further, no information about the user (fingerprint, retinal print, voice print, etc.) is kept by the employer. Issues affecting user acceptance are absent for KD solutions.

The final factor not included in the original list of eight is cost. In a traditional rollout of biometric technology, special sensors and software must be purchased, installed, and maintained. For organizations with hundreds or thousands of workstations spread across multiple locations, this can be cost prohibitive. KD solutions meet much of the cost challenge by not requiring the installation of any special equipment. Any keyboard can be used to collect typing behavior data for analysis. Further, no employee training is required to ensure proper use of the technology. Finally, enrollment time is virtually eliminated resulting in no loss of employee or management productivity.

Conclusion

Keystroke Dynamics as an identity verification solution is quickly emerging as a viable, low cost, non-intrusive alternative to traditional biometric technologies. As with all technology, KD is not without its challenges. Higher error rates and potential problems with physical and logical access control convergence require a review of how KD fits into the overall enterprise security strategy. For many organizations, however, KD technology is a low impact answer for multi-factor authentication business requirements.

 Tom Olzak, MBA, CISSP, MCSE, is President and CEO of Erudio Security, LLC. He can be reached at tom.olzak@erudiosecurity.com.

Check out Tom's book, Just Enough Security

Additional security management resources are available at http://adventuresinsecurity.com

Listen to Tom's podcasts at http://blastpodcast.com/viewpodcast.html?id=441

Free security training available at http://adventuresinsecurity.com/SCourses

---

Works Cited

BioPassword (2006). *Authentication solutions through keystroke dynamics.* Retrieved September 23, 2006 from http://www.biopassword.com/resources/BioPassword_Authentication_Technology_Whitepaper.pdf#search=%22authentication%20solutions%20through%20keystroke%20dynamics%22

Checco, J. C. (2006). *Keystroke dynamics & corporate security.* Retrieved August 21, 2006 from http://www.wsta.org/publications/articles/1003_article06.html

DeepNet (2006). *Keystroke biometric signature.* Retrieved August 21, 2006 from http://www.deepnettechnologies.com/products/pdf/deepnet%20typesense.pdf#search=%22%22keystroke%20biometric%20signature%22%22