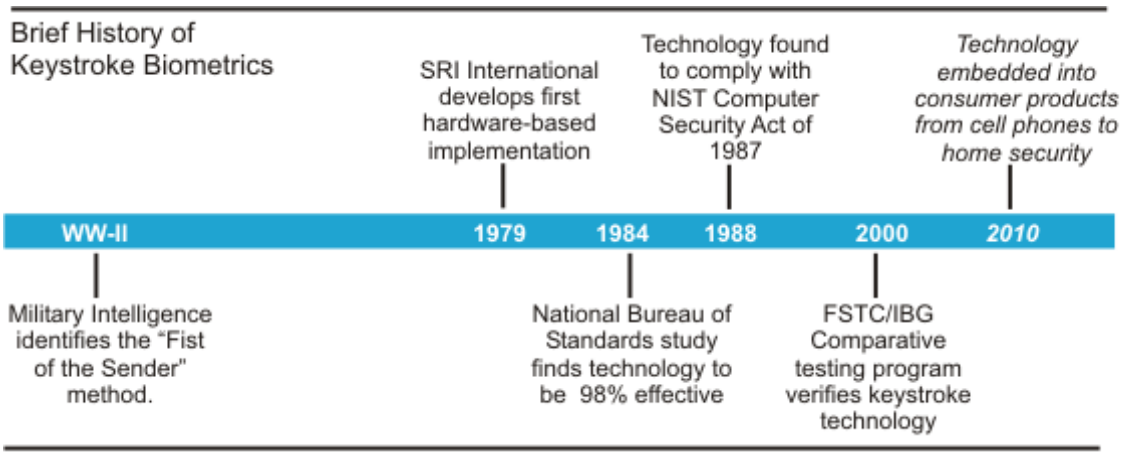
Keystroke Dynamics
And Corporate Security

John C. Checco

A Technological Breakthrough… from World War II?

The idea behind Keystroke Dynamics has been around since World War II. It was well documented during the war that telegraph operators on many U.S. ships could recognize the sending operator. Known as the "Fist of the Sender," the uniqueness in the keying rhythm (even of Morse-code), could distinguish one operator from another.

Since then, many adaptations of this phenomenon have been studied. Currently, several patents exist in the field of Keystroke Dynamics: 4621344, 5557686, 4805222, 4962530, 4998279, and 5056141.



What is Keystroke Dynamics

Biometrics is the *statistical analysis of biological observations and phenomena.* Biometric measurements can be classified as physical and behavioral.

> **Physical Biometrics** defines biological aspects of a person that determine identity. Measurement data is considered static which generates an absolute match. (Partial matches are mostly due to variability in the capture process, such as placing only part of a finger on a fingerprint device.) Examples of physical biometrics are: DNA, Iris, Retina, Fingerprint, Hand Geometry and Vein Structure.
>
> **Behavioral Biometrics** defines characteristic traits exhibited by a person that can determine identity. Measurements are considered dynamic which results in a "*confidence match.*" The quality of this measurement varies by behavioral as well as external factors of the subject being measured. Examples of behavioral biometrics are: Handwriting, Voice, Speech, Language Removal, Gait, Gesture and Typing patterns.

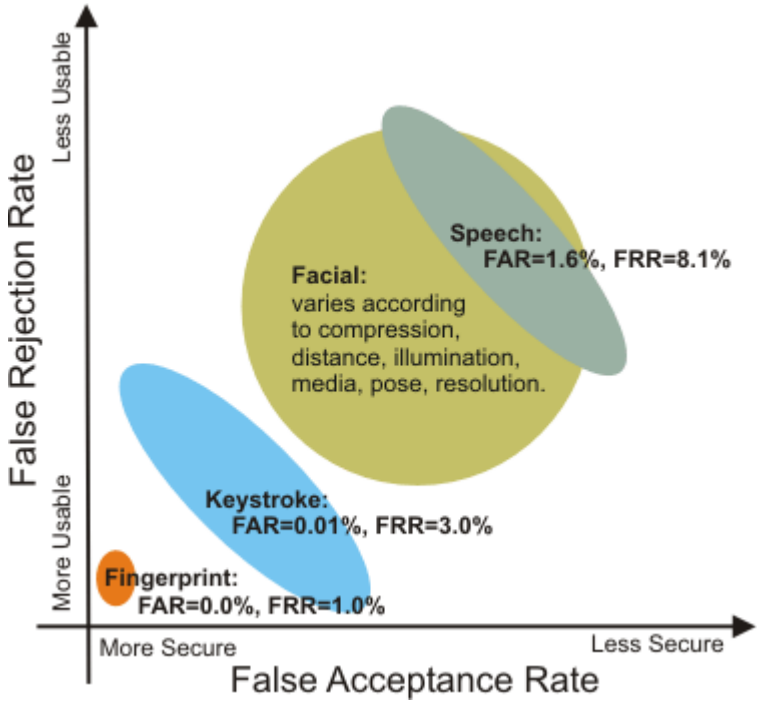
Keystroke Dynamics, being a behavioral measurement, is a pattern exhibited by an individual using an input device in a consistent manner. Raw measurements already available by the standard keyboard can be manipulated to determine *Dwell* time (the time one keeps a key pressed) and *Flight* time (the time it takes a person to jump from one key to another). Variations of algorithms differentiate between absolute versus relative timing. The captured data is analyzed to determine aggregate factors such as: Cadence, Content, Spatial Corrections, and Consistency. This is then fed through a *signature processing* routine, which deduces the primary (and supplementary) patterns for later verification. Signature processing is not unique to biometrics; in fact many of these algorithms are present in actuarial sciences from economic trending to quantum mechanics.

How Effective is Keystroke Dynamics

It is a widely-held belief that physical biometrics is more effective than its behavioral counterpart. But how does Keystroke Dynamics fair in the realm of behavioral sciences? All biometrics are validated by several important criteria:

> **False Acceptance Rate**: This determines how often an intruder can successfully bypass the biometric authentication. A lower rate is more secure; for example, an FAR of 0.01% states that the chance of fooling the system is 1:10000.
>
> **False Rejection Rate**: This signifies how often a real user will not be verified successfully. A high rate translates into more user retries; hence usability suffers.
>
> **Crossover**: The relationship between FAR and FRR is converse -- although not always linearly in behavioral biometrics. Crossover is where the FAR and FRR would be equals. The best technologies have the lowest crossover rate.

The diagram below shows where Keystroke Dynamics falls with respect to physical biometrics -- such as fingerprint -- and other behavioral biometrics.



One critical point to note is that all behavioral biometrics, because they are confidence based measurements, have the capability to be "tweaked" for specific applications. This allows the implementer to explicitly trade usability for security (or vice-versa) – whereas, physical biometrics do not have this capability. As a consequence, the FAR and FRR for all behavioral biometrics are dynamic and crossover can vary between implementations of the same biometric method.

Keystroke Dynamics in Corporate Use

The advantages to using Keystroke Dynamics versus other enhanced security mechanisms are twofold: with the end-user as well as the implementer.

Usage / Acceptance:

Biometric verification is a time-consuming operation in the computer world. Many applications for biometrics need to identify the user prior to obtaining the biometric sample, to simply limit the number of biometric templates it needs to verify against. With Keystroke Dynamics, the identification can be in the captured sample, so verification is limited to a single template.

Every workstation has a Keystroke Dynamics input device (a.k.a. keyboard); thus, the technology can really be seen as software-only. With a software-only biometric solution, users are not limited to individual or specific workstations.

As stated previously, behavioral measurements have more flexibilities than conventional physical biometrics:

- Behavioral measurements accommodate different thresholds for acceptance – risk versus reward.
- Behavioral biometrics can adapt to changing behavior, for example, by merging each successful verification into the master template; thus, constantly refining the accuracy of the user over time.
- Keystroke Dynamics, by design, has a non-invasive user interface. It can be implemented to silently capture user typing during normal operation; thus making enrollment "invisible."

Implementation / Deployment:

The comparison between Keystroke Dynamics and other biometric solutions -- software-only versus hardware-based -- really emerges as an advantage when translated into real savings from an implementation and deployment perspective.

As a software-only solution,

- This technology requires no physical hardware to install and no manpower needed for client-side installations or upgrades.
- The technology can be embedded in any in-house software application to augment entitlement-based access.
- The implementation provides a seamless method to harden remote-access security.
- It can be wrapped into your corporation existing single-signon solution as a secondary authentication mechanism.
- Simplified templates can be embedded into documents as a biometric signature (different from digital signature), and then verified from anywhere.

As a biometric solution,

- This technology does not require changes to existing network access policies; it more effectively enforces these policies.

- This technology provides better audit control and promotes proper use of application licensing.

- Logging of biometric access creates better forensic evidence; and can deter many internal threats to network security.

Markets for Keystroke Dynamics

Keystroke Dynamics has already found its way into many areas in the past 2 years. For corporations, this technology has found uses in **Network Security** (single sign-on, multi-password management, RADIUS, application access and document control management) as well as **Asset Identification** (online training, document signing, software licensing and PKI).

The consumer market has seen some integration of this technology in **Personal Information Security** (individual document encryption, online purchase verification, and secure laptop access).

The future of this technology in the corporation will hardly be seen by the end users. It will be embedded into many aspects of network infrastructure, and invisibly so.

The greatest growth for this technology will be seen in the consumer market. As refinements in this technology allow verification with less input and alternative forms of input (stylus, for example), it will find its way into PDAs, Tablet PCs, RIM, ATMs, Cell phones, and Home Security Access Pads.

Summary

The most useful inventions in history have one of two qualities. Some create an undeniable impression on its audience. It is easy to remember the beginning of the computer age and all its media attention. Others simply create no attention at all, because they extend what its audience has perceived to be there all along. How many of us can remember the exact year when video tape players also became recorders?

Keystroke Dynamics is one of those subtle technologies that will raise the bar on access security without users ever knowing it.

About the Author

John C. Checco (John.Checco@Checco.com) is a member of ASIS and founder of bioChec™ (http://www.bioChec.com), an implementer of keystroke biometric solutions.