The key to biometrics success

IWA speaks to **John Checco** about the potential for keystroke biometrics.

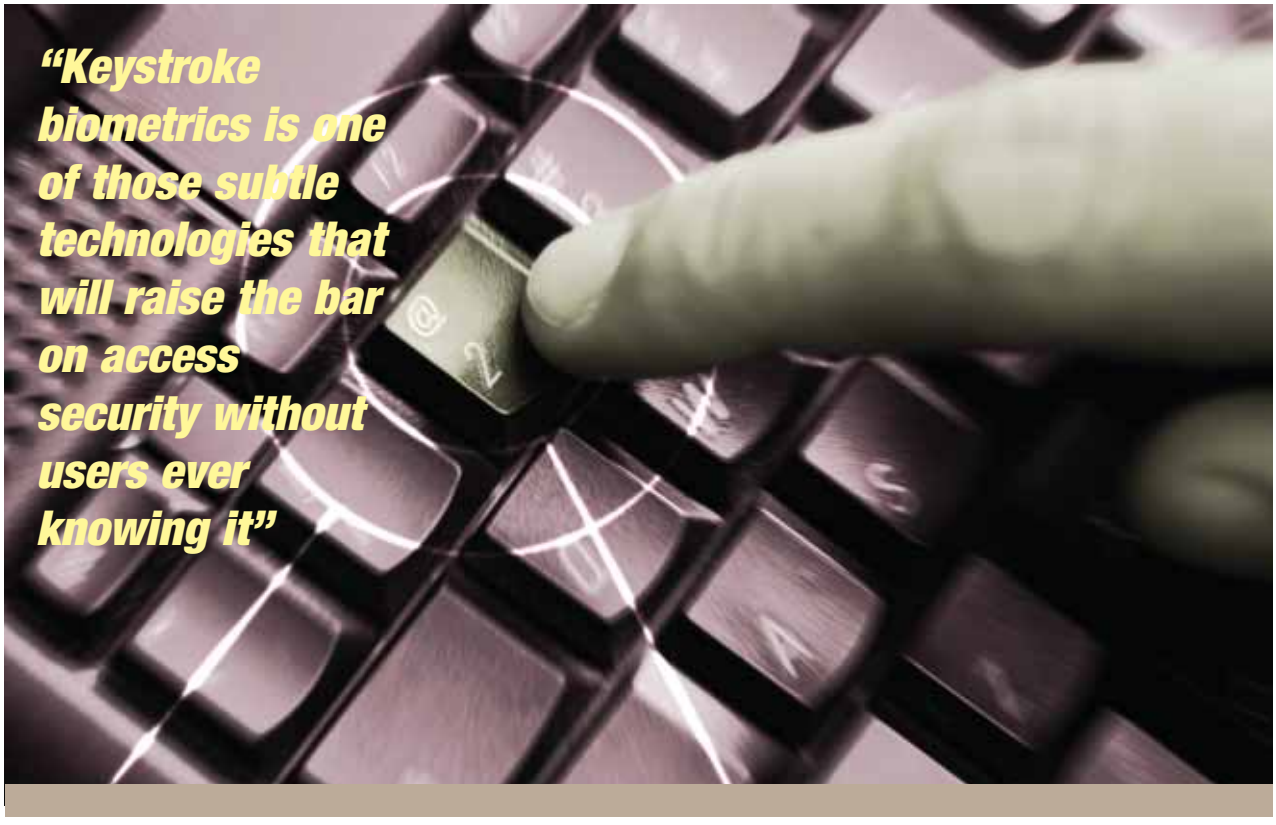
John Checco is President and CEO of Checco Services, Inc., which develops and sells bioChec keystroke biometric solutions. He is currently an active member of Infragard NYC Chapter, the American Society for Industrial Security (ASIS) and holds a Certified Information Systems Security Professional (CISSP) certification from (ISC)2. Among his many achievements is a patent for an implementation of what is now known as 'unified messaging', as well as a pending patent for his unique algorithm in keystroke biometrics. Mr Checco's experience encompasses research and development of cutting edge technologies from the IBM Watson Research Center, NYNEX Science and Technology Center, Advanced Technology Labs and Kodak Health Imaging.

IWA. What exactly is keystroke biometrics?

JC. The idea behind keystroke biometrics has been around since World War II. It was well documented during the war that telegraph operators on many US 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.

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 the 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 biometrics, 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



KEYSTROKE BIOMETRICS: TECHNOLOGICAL ADVANTAGES

PERFORMANCE

Keystroke biometrics inherently narrows the identification pool to achieve better false acceptance/rejection rates (FAR/FRR). To identify a fingerprint against a pool of users, one must either supply the identity of the user they are trying to match against (secondary input), or check the entire set of user templates against the sample input. Because most keystroke biometric implementations include the user ID as well as the passphrase, the identity of the user being matched against is supplied automatically.

PORTABILITY

Users are not limited to individual or specific workstations. Keystroke biometrics signatures have been consistent from laptop keyboards to desktop keyboards.

FLEXIBILITY

Dynamically managed threshold for acceptance. Physical biometrics are simply pass/fail measurements, whereas behavioral biometrics are confidence measurements. This means that in the keystroke biometrics realm, the FAR/FRR measurements will vary across different confidence levels. This translates into an efficiency of entitlement – a policy of mitigated risk where an administrator's threshold is set to a very low FAR, whereas an assistant can have a lower FRR for usability. Of course, these controls are useless unless they are complemented by a well-defined information security and auditing policy.

SECURITY

Constant behavioral refinement of templates over time. One of the unique traits of keystroke biometrics over all other biometrics is the ability to refine a user's template over time and adjust to small consistent changes in behavior. Adaptive template technology allows the keystroke biometric algorithms to create lower crossover rates as its use increases. No other biometrics system has been able to accomplish this to date.

USER ACCEPTANCE

Seamless, non-invasive signature capture and support for invisible (dynamic) enrollment. The key to any biometric is end-user acceptance. The perception of biometric authentication being an intrusive process has limited its marketability. Keystroke biometrics does not exhibit this problem, and most people are fascinated it can recognize them in such a short period of time. Another part of end-user acceptance is transparency in enrollment. When initially deploying a keystroke biometric solution, we have made use of everyday logins contributing to the template creation over a period of two weeks to a month. The user has no idea they were even enrolling.

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.

IWA. Many commentators believe it is probably the easiest biometric technology to implement and administer. Why then is it only now coming to the fore?

JC. In general, biometric technology implementations have been slow to meet a critical point in the market. Added to this market latency is the dichotomy of perceptions:

- Biometric data is considered private and not something the general public is likely to give willingly for the sake of protection. As an example, most people associate fingerprint readers with the government's AFIS database – even though most fingerprint manufacturers create proprietary data formats.
- Behavioral biometrics is not seen as a true biometric. This perception is compounded even more when one tries to explain the concept of keystroke biometrics as a software-only biometric. The public has been led to believe that biometric implementations are large intrusive machines that poke and prod.

With these perceptions, it has been difficult to get keystroke biometrics embedded into commercial implementations. In fact, with over nine US patents on different keystroke biometric algorithms, only a few have been made into commercial products.

The truth of the matter is that when it comes to identifying theft, behavioral biometrics is safer than physical biometrics. If someone steals your fingerprint (refer to the Japanese gummy bear experiments in the sidebar over the page) you cannot just go and get another; keystroke biometrics, on the other hand, measures typing behavior over a subset of a user's entire typing vocabulary. If that specific data were to be stolen, the user simply creates a new behavioral template using another phrase from their typing vocabulary.

IWA. How then does it compare to other forms of biometric identification – what are its strengths and weaknesses?

JC. There are two keys areas of consideration for keystroke biometrics over other physical and behavioral biometrics: technological advantages and those related to implementation. Both the technological advantages and the implementation advantages are highlighted in the adjacent sidebars.

IWA. Isn't it the case that physical biometrics are a more effective security measure than the behavioral equivalent?

JC. From a pure FAR/FRR measurement, physical biometrics will always outweigh behavioral biometrics. However, measuring the FAR/FRR from a physical biometric is creating a statistic from a known limited set of absolute values.

There is no equivalent parallel measurement in the behavioral biometric arena. The FAR/FRR statistics given for any voice recognition, keystroke or other behavioral biometric has with it a very detailed set of control variables used to limit the variability. Behavioral biometrics are dynamic and fluid systems; they rarely exhibit a consistent or even linear FAR/FRR under normal use.

Which brings up another vendor secret: the success of any behavioral biometric implementation relies heavily on properly tweaking the confidence thresholds to achieve the desired FAR/FRR, balancing the end-user expectations with the security policies that need to be enforced. Too many

times we have seen projects stall at the requirements stage because this balance could not be found. Part of our job is to objectively assess the information and systems protection policies before suggesting whether keystroke biometrics is the correct solution in the correct place.

IWA. What has been the uptake of keystroke biometrics to date; and with this in mind, what do you think the future holds?

JC. Keystroke biometrics is a niche solution. It works well for people who use computers as part of their daily lives. It is not a solution that would be used on an electronic passport or national ID card.

But there has been much excitement in the keystroke biometric commercial market with new regulations (GLBA, SOX, HIPAA, et al) coming to pass. Many financial institutions are looking for an economical and maintainable secondary web authentication for their small business and consumer users. The need for economical internet-based secondary authentication will only increase as financial firms realize the cost savings of reducing internet-based credit card fraud using this system.

Government agencies have also seen the need to use keystroke biometrics to round out mobile data protection.

Document control has been a big opportunity here. For documents that are considered confidential, companies need to institute a central document repository. Companies that are ISO-9001 compliant should already have this in place. But keystroke biometrics has some value-added features; not only can it be used to restrict access to documents, forensically audit all document actions, but the templates can be used to digitally sign the document when it is retrieved – so it can be traced if ever found in a rogue form.

The most useful inventions in history have one of two qualities. Some create an undeniable impression on its audience. Others simply create no attention at all, because they extend what their users have perceived to be there all along. How many of us can remember the exact year when video tape players also became video tape recorders? Keystroke biometrics is one of those subtle technologies that will raise the bar on access security without users ever knowing it.

FOOLPROOF FINGERPRINTS?

TSUTOMU MATSUMOTO, a Japanese cryptographer, recently showed that biometric fingerprint devices can be reliably fooled with a little ingenuity and US$10 worth of household supplies.

First he took a live finger and made a plastic mold using a free-molding plastic commonly available at hobby shops. He next poured liquid gelatin (the material used to make Gummi Bears) into the mold and let it harden. Matsumoto then took his experiments a step further. Enhancing a fingerprint left on a piece of glass with a cyanoacrylate adhesive, he photographed it with a digital camera and, using PhotoShop, improved the contrast and printed the fingerprint onto a transparency sheet. Using this fingerprint transparency to etch the fingerprint into the copper of a photo-sensitive printed-circuit board (thus making it three-dimensional), Matsumoto was able to make a gelatin finger, complete with fingerprint, that was able to fool fingerprint detectors about 80 percent of the time.

He tried these attacks against eleven commercially available fingerprint biometric systems, and was able to reliably fool all of them.

KEYSTROKE BIOMETRICS: IMPLEMENTATION ADVANTAGES

DEPLOYMENT/MAINTENANCE

With a software-only keystroke biometric solution, there is no physical hardware to install or maintain, which translate into very little manpower needed on client-side deployment for installations or upgrades.

COVERAGE

A software-only keystroke biometric solution can support remote access and telecommuting.

POLICY MANAGEMENT

In general, any secondary authorization should not change current policies. Keystroke biometrics is no exception. We have generally seen companies that have successfully deployed this solution to relax the time for password regeneration, because the adaptive template technology can maintain password strength for a longer period of time.

AUDIT CONTROL

Logging of any secondary authentication, especially biometric access, creates better auditing and forensic evidence.

SOLUTION MANAGEABILITY

A software-only solution always enjoys a minimal effort to deploy compared to other secondary authentication mechanisms. And although most vendors do not like to talk about this, software-only secondary authentication has a much easier exit strategy. Since you have not changed the way the user logs in, the secondary authentication can be suspended or removed by simply turning off the server-side processing of the keystroke signature.

IWA. What role does bioChec play? What makes your products standout and how do you differentiate yourself in your approach?

JC. bioChec, as a business, tries to enhance the customer experience through technology and education. bioChec enhances keystroke biometric technology in several ways:

- Adaptive template technology, which adjusts to subtle changes in user behavior over time.
- Dynamic enrollment implementation, which takes advantage of the adaptive template technology to build a user template from normal user interaction over time, rather than have an explicit enrollment.

bioChec also provides supporting services to ensure a successful deployment. We assess any implementation from the requirements to maintenance. bioChec will not suggest its solution before other, more critical, security holes get the attention needed. In some cases, we have educated customers in areas of information security policy and infrastructure security. This may have cost us few immediate product sales, but has never cost us a customer. ■