

# Keystroke recognition

Lots of potential, but - as yet - little practical use

by Ravi Das

In KJDI 24 we reviewed the technology behind signature recognition. The article explained how signature recognition works, the strengths and weaknesses of the underlying technology and the application options. This article examines another biometric technology: keystroke recognition.

In addition to unique physiological biometrics, we also possess unique behavioural biometrics. Think of the way we sign our name, for example. The way we use a computer keyboard also varies from one individual to the next. In fact, it's so unique that keystroke recognition is considered a behavioural biometric in its own right. This article is divided into two sections. The first explains how keystroke recognition works while the second reviews the strengths and weaknesses of keystroke recognition as a biometric solution.

## How keystroke recognition works

Compared with other biometric technologies, keystroke recognition is probably the easiest to implement and administer. At this stage, keystroke recognition solutions are entirely software-based - there is no need to install any hardware (figure 1). All you need is a computer and a keyboard.

To start the enrolment process, an individual is required to type a specific word or group of words (text or phrases). In most cases, the individual's user name and password are used. It is very important that the same words or phrases are used during both the enrolment and verification processes. If not, the behavioural typing characteristics will be significantly different, and, as a result, a mismatch will arise between the enrolment and verification templates.

To create the enrolment template, the individual must type his or her user name and password (or text/phrase) about 15 times (figure 2). Ideally, the enrolment process covers a period of time, rather than taking place all at once. This way, the capture of behavioural characteristics will be more consistent. With keystroke recognition, the individual being enrolled should type

without making any corrections (for example, using the backspace or delete key to correct any mistakes). If the individual does make corrections, the keystroke recognition system will prompt the individual to start again from scratch. The distinctive, behavioural characteristics measured by keystroke recognition include:

- the cumulative typing speed;
- the time that elapses between consecutive keystrokes;
- the time that each key is held down;
- the frequency with which other keys, such as the number pad or function keys, are used;
- the sequence used to type a capital letter (whether the shift or letter key is released first, for example).

These behavioural characteristics are subsequently used to create statistical profiles, which essentially serve as enrolment and verification templates. The templates also store the actual user name and password. The statistical profiles can either be 'global' or 'local'. Whereas a 'global' profile combines all behavioural characteristics, a local profile measures the behavioural characteristics for each keystroke.

The statistical correlation between the enrolment and verification templates can subsequently be modified, depending on the desired security level. An application which requires a lower level of security will permit some differences in typing behaviour. However, an application which requires a higher level of security will not permit any behavioural differences.

It is important at this point to make a distinction between static and dynamic keystroke verification. In case of the former, verification takes place only at



*Ravi Das is a Consultant for HTG Solutions. He has been involved in the IT industry for 10 years and launched HTG's security solutions division in January 2003. This division offers a complete security solutions package and uses biometric technology as its main product offering. Ravi holds a Master of Science Degree in Agribusiness Economics from Southern Illinois University and a Master of Business Administration (specialising in Management Information Systems) from Bowling Green State University.*



**Figure 1**  
Keystroke recognition solutions are entirely software based.

certain times - when the individual logs in to his or her computer, for example. With the latter, the individual's keystroke and typing patterns are recorded for the duration of a given session.

### The strengths and weaknesses of keystroke recognition

Keystroke recognition has several strengths and weaknesses. Arguably its biggest strength is that it doesn't require any additional, specialized hardware. As previously indicated, keystroke recognition is purely software-based, allowing the system to be set up very quickly. Second, keystroke recognition can be easily integrated with other, existing authentication processes. The adoption of other biometric technologies requires the implementation of a new process within an existing process. This calls for individuals who are properly trained in the use of contemporary biometric devices, which can greatly increase costs. Third, everybody is familiar with typing their user name and password. As a result, there is very little training required for an individual to use a keystroke recognition system properly. Fourth, the templates that are generated by the system are specific only to the user name and password used. Should this user name and/or password be tampered with, the individual only needs to select a new user name and password to create a new set of enrolment and verification templates.

The weaknesses of a keystroke recognition system are the same as those suffered by other systems that rely on a user name/password combination. For example,

passwords can be forgotten or compromised while users will have to remember multiple passwords in order to gain access to, for example, a corporate network. It should be noted that keystroke recognition still requires users to remember multiple passwords (the administrative costs of having to reset passwords will also continue to be incurred). As such, it only enhances the security of an existing user name/password-based system. Second, keystroke recognition is not yet a proven technology. As a result, it has not been widely tested. And finally, keystroke recognition is not necessarily a convenient system to use.

### In conclusion

Keystroke recognition is included in very few commercial applications at this point. Compared with other biometric technologies, it probably ranks last in terms of use. Having said that, behavioural biometrics are not particularly popular on the whole. Although it's quite possible that keystroke recognition will establish itself as a dominant technology, there are, at this stage, not enough vendors to propel the technology forward (unlike, for example, fingerprint recognition).

Compared with other physical biometrics, keystroke recognition is easier and cheaper to implement. However, it is unlikely to be used for applications such as physical access control, document verification, passport verification, etc. Instead, it will be used for computer security (where fingerprint and iris recognition solutions are already used as a substitute for user names and passwords). Keystroke recognition is also well suited to e-commerce applications. Here,

**Figure 2**

To start the enrolment process an individual must type a series of phrases, such as their user name and password, about 10-15 times over a period of time.



a user would be able to access an internet banking or e-commerce site by typing in the same text or phrase several times (rather than having to remember different user names and passwords). Moreover, the same text or phrase can be used to log into multiple e-commerce sites. Keystroke recognition could additionally be the security tool of choice for Multi Modal Security applications, where it can be used to provide 3rd, 4th, or even 5th tier security.

While small to medium-sized enterprises (SMEs) will probably not adopt keystroke recognition, it is well suited to large businesses and organisations, including major banks and financial institutions. It's also quite conceivable that keystroke recognition will be adopted by governments around the world.