

>> Home >> Technology

23.02.2004 / Biometric security solutions for SAP applications:

Fingerprint Access Control

Whether it's financial or customer data, staff records or accounting and procurement workflows, many companies manage critical information in SAP applications. The solutions must therefore be reliably protected against misuse. A new biometric access and function control system recognizes authorized users' fingerprints and keeps unauthorized users away from sensitive data.

Disgruntled former employees can hit companies where it hurts – and company networks are a particularly sensitive spot. In one example, an ex-employee of clothing company American Eagle published staff passwords and user names and a guide to infiltrating the company network on a hacker website. The 38-year-old wanted to unleash a denial-of-service attack on his former employer, shutting down the IT systems of clothes shops in the USA and Canada in the run-up to Christmas. The company was at least able to discover the attacks quickly and minimize the damage caused. At the end of last year a federal court sentenced the man to 18 months in prison.

This case is only one example highlighting the fact that companies cannot value the security of their mission-critical applications too highly. Passwords do not provide sufficient protection, given Gartner's findings that most cases of data misuse in companies can be put down to staff. It is usually not too difficult to get hold of a co-worker's access code. Surveys have shown that around 80 percent of users store their passwords in the vicinity of their computer, noting number combinations in diaries or on post-its affixed prominently to monitors. Memory aids like this make it easy for third-parties to manipulate or steal sensitive data. Gaining access is even easier if a user leaves his or her desk for a short time without logging out of the system.

Administering passwords is labor-intensive and therefore expensive. realtime calculates that every time a user forgets one of their passwords and calls the hotline, an internal cost of US \$ 50 is incurred. For 1,000 users each making two calls a year, this amounts to \$100,000. In addition to this, the cost of valuable working time wasted as a result of incorrect entries and blocked accounts must also be considered.

Expensive password administration

Security systems based on biometric recognition techniques bar the way for misuse of data by unauthorized persons. They authenticate users at logon using unmistakable personal characteristics like fingerprint, iris or voice. In contrast to passwords or smart cards, these characteristics cannot be stolen, forgotten or lost. Logging on is easy. To perform a dactyloscopy – a comparison of fingerprints – the users only need to place their fingertip on a biometric sensor on the keyboard or mouse. Apart from being very easy to use, biometric systems also provide economic benefits, for example making password administration unnecessary.

bioLock protects SAP solutions

SAP partner realtime AG has developed a biometric security solution for protecting SAP systems. bioLock is the first, and up to now the only, software to enable fingerprint verification of SAP solution users. The software does not replace a company's authorization concept, it instead makes sure that functions are actually carried out by authorized staff.

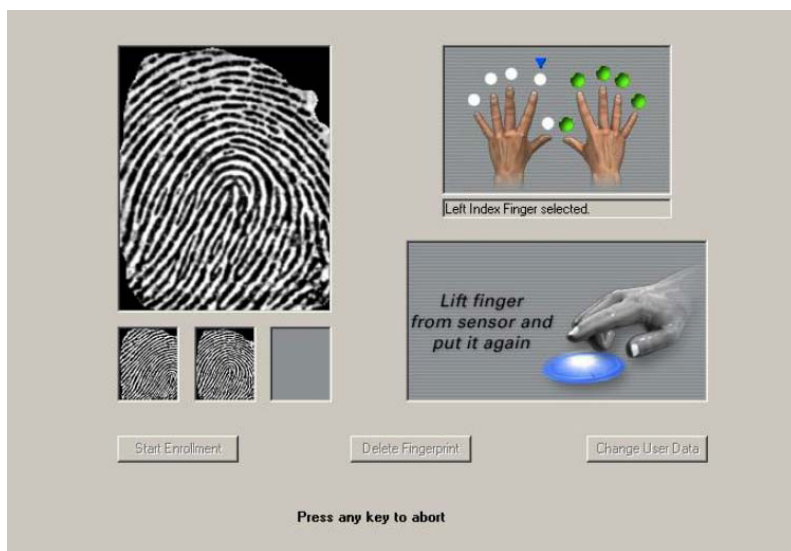
Highest security level at Brevard County

The county administration of Brevard County, Florida, USA has an award-winning bioLock installation. American media group InfoWorld last year praised the solution's outstanding innovation. Brevard County is home to the NASA facilities at Cape Canaveral and Cape Kennedy and is therefore subject to strict security guidelines. The county administration uses bioLock to protect individual transactions and infotypes in the HR system in order to prevent misuse of sensitive data. The authority's staff log on to SAP applications using fingerprint authentication. Kenneth D. Gunn, Director, Safety & Security, Homeland Security Coordinator, Florida Space Authority, says: "When Thomas Neudenberger, COO of realtime North America Inc. introduced me to this innovative technology, I thought: This is something we absolutely need here in the State of Florida to improve our Homeland Security. I personally introduced realtime to Brevard County Government and I hope, that the successful installation at Brevard will inspire more Government and private organizations across the nation to protect their vulnerable IT systems with innovative biometric technology.

bioLock compares the fingerprint on the keyboard or mouse with reference data for the registered users. These are then stored in encrypted form as templates in an SAP table in the database. The 128-bit encryption using CSP (cryptographic service provider) technology enables the program to immediately spot any attempt to manipulate the data record and abort the authentication.

A sensor instead of an ink pad

The templates contain all the relevant minutiae for each user – micro-characteristics of fingerprints such as bifurcations or ridge endings. Like constellations, minutiae images are unique and can be recognized regardless of position, angle or absolute size. bioLock grants a user access to the protected SAP application if his or her fingerprint matches the data in the template. The recognition process only takes a fraction of a second.



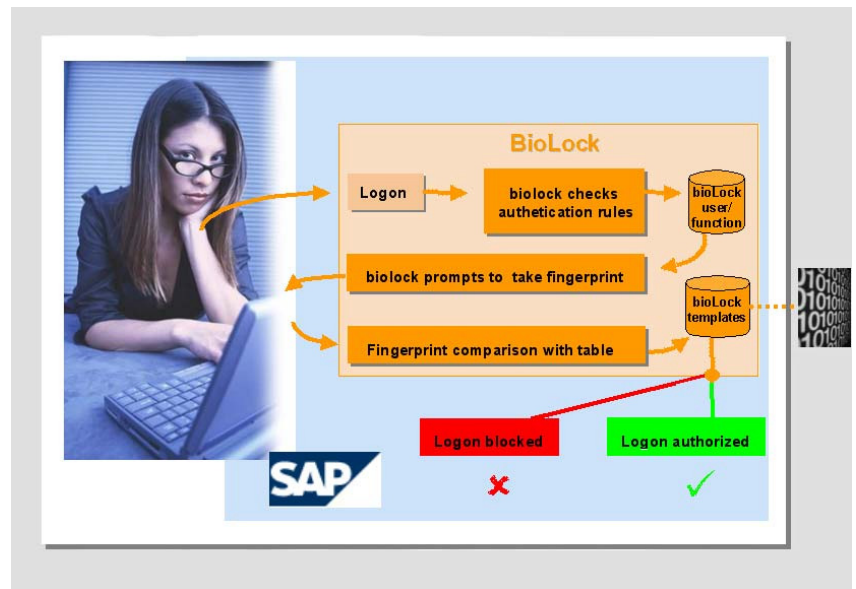
User registration

The program stores the user's minutiae when he or she registers or enrolls. Using the customizing function, the system administrator creates a bioLock user for all affected staff, taking fingerprints of as many of the user's fingers as possible. A user who, for example, has a plaster on their finger following an injury can then use another finger to log on. At registration, the biometric sensor on the keyboard of a bioLock workstation assumes the function of an ink pad. The user places each fingertip on the sensor three times, the program creates an average from the three prints and saves the minutiae in a template. Data about which applications, transactions or fields require the user to authenticate him or herself are stored there.

Multiple security levels

The security level can be scaled according to requirements. bioLock protects individual fields and complete system landscapes. It is often appropriate to biometrically secure single, critical functions such as displaying balance sheets, changing parts lists or approving batches of medicines. The program displays a dialog box prompting any user performing the transaction to authenticate him or herself. By default, bioLock records every authentication in log files.

SAP Logon with bioLock



Fingerprint authentication can be configured as the sole form of access control, or combined with password logon. Companies wanting to dispense with passwords completely have the option of single sign-on using the bioPortal solution. It combines bioLock with Software ID Center from Siemens. ID Center stores all staff's biometric data on a separate security server. bioPortal provides all users with direct access to the applications their fingerprints authorize them for. They click on the desired application and the program checks if their fingerprint is stored. If it is, they are automatically logged in. In addition to SAP solutions, bioPortal also protects databases and other applications against unauthorized access. The solution can be implemented in conjunction with SAP Enterprise Portal.

Biometric authorizations by fingerprint can also be used as electronic signatures. This allows business processes to be implemented from start to finish in the SAP solution. Healthcare is just one of the areas where this can be useful. Instead of requisitions for medications having to be printed out for doctors to sign, they can approve them with their fingerprint, saving on consumables. bioLock attaches the fingerprint data to the SAP documents or log records, thereby documenting the approval.

Installed in a few hours

bioLock protects SAP [R/3](#) 4.x and later solutions. The software has been developed in a reserved SAP name space, meaning there are no applications with similar names that could overwrite bioLock when importing transactions. This makes installation far easier, since existing SAP solutions do not have to be adapted.

Customization is also quick and easy. realtime supplies a customization toolkit containing various modules for configuring the solution. Application examples include a demonstration of how the modules can be used to configure user exits in order to perform the required settings. Among configuration options are how many additional logon attempts bioLock allows users after a failed logon attempt. Customers can also specify that users authenticate themselves several times to access individual applications, or that an additional person must be present for authorization.

Further information at www.bioLock.us , www.realtimenorthamerica.com or 1-877-bioLock