

# SAP INFO

THE SAP MAGAZINE • WWW.SAP.INFO

Biometrics:

## Beyond Sarbanes-Oxley Compliance

The information security issues of Sarbanes-Oxley Act (SOA) ask companies to be able to document which users attempted to modify data. Biometric systems help to overcome some weaknesses of password protection.

Lately, there have been many stories of companies filing annual reports late or attempting to budget projects to comply with the Sarbanes-Oxley Act. Such publicity will not help corporations regain the trust of investors. Instead, companies should be disclosing the innovative ways of improving internal controls and corporate governance in an ever-changing environment of Web services, intranets, and of extranets.

SOA requires systems to document answers to: What did the CEO and the CFO know and when did they know it? Evidence in legal cases has included even emails and voicemails. SAP responded quickly to SOA to develop additional functions for its customers in more than 18,000 companies. SAP Compliance Management for SOA provides even tighter integration for SAP R/3. Many executives have chosen to use one, common set of processes throughout their companies. While this step alone improves processes and reduces maintenance of systems, much more must be done to improve information security.

Researchers at California State University, Fullerton (CSUF) have launched biometrics research projects using real-time's bioLock system for SAP R/3. The biometrics research program is part of the Forum for Advanced Security Technologies (FAST). On March 6, 2005, Vijay Karan and Curtis Williams (CSUF) joined Thomas Neudenberger of realtime North America in a biometrics presentation at the SAP Cur-

riculum Congress 2005 in Atlanta, Georgia. Professors Malini Krishnamurthi and Paul Sheldon Foote (CSUF) co-authored the presentation with the presenters. Professors from some other universities in SAP's University Alliance Program have expressed an interest in providing hands-on biometrics education for students and in working on academic research projects.

The researchers have found that SOA is being implemented in phases. SOA sections 301, 302, 401, 404, and 409 have implications for current and future added functions for SAP R/3. SAP's Whistle Blower enables anonymous emails to public company audit committees (301). SAP supports CEOs and CFOs with the accuracies of financial disclosures and with the evaluations of reporting controls and processes (302) with: Management of Internal Controls (MIC), Audit Information System (AIS), SAP Business Information Warehouse (SAP BW), and SAP Strategic Enterprise Management (SAP SEM) Cockpit. Disclosures of all auditor adjustments are possible (401). External auditors have traditionally provided management letters discussing internal control system weaknesses. Under section 404, external auditors will need to evaluate more complex internal control systems. In the future, there will be a need to provide real-time (perhaps within 48 hours) Form 8-K disclosures of events having material effects on financial performance.

## 20 ways to bypass passwords

The realtime bioLock system provides SOA solutions for SAP R/3 systems, a major opportunity for current SAP R/3 users. Biometrics can be used for much more than augmenting or replacing passwords. It is possible to document when the CEO and CFO saw and when they saw it in an SAP R/3 system using bioLock.

But bioLock does not stop at the CEO and CFO level. Companies should register all critical users (such as: HR, Finance, Development, Purchasing, and Administration). Auditors will always know exactly, who did what and when in the entire SAP system. All activities down to the field level will be recorded and saved in the internal bioLock log file. This log file can be sorted or filtered by users, activities or rejections and exported in different formats.

While the focus of firewalls was keeping unauthorized users from destroying or stealing data, the information security issues of SOA are very different. Companies and external auditors need to be able to document which authorized users of portions of a system attempted to aggregate or modify data.

Researchers have found more than 20 different ways to obtain a password to an SAP User profile, including: looking under the keyboard, calling for a password reset, using password sniffers and crackers, and looking over an employee's shoulder (Shoulder Surfing). CEOs and CFOs who must certify financial statements must be sure that no one has been able to make improper changes.

### Case: Brevard County, Florida

By obtaining someone else's password, a disgruntled Brevard County, Florida employee was able to use another SAP user profile with extended authorization to disseminate confidential information in the organization. A lawsuit and bad publicity followed. In November 2003, the county government won the prestigious InfoWorld 100 Award for protecting and auditing access of critical HR infotypes in SAP R/3 using a fingerprint identification system.

### Case: American Eagle Outfitters

A former, disgruntled employee of American Eagle Outfitters spread multiple logon information in 'hacker' chat rooms with clear instructions, how to cause damages to his former employer. The attacks resulted in financial damages during the Christmas shopping season. Since the employee could be identified he was charged with 'password trafficking' and 'computer damages' and sentenced to 18 months of prison.

A lesson to be taken from these cases is that current and former disgruntled employees can be responsible for billions

of dollars per year of losses. New concerns about terrorism are simply accentuating prior failures to invest in the information security technology.

Special keyboards with smart cards from Cherry Electrical Products provide two-factor authentication. Identity management is even stronger using both biometrics and smart cards. All functions in bioLock can be protected either with biometrics or smart card or both. For very critical functions such as wire transfers or the bioLock administration the system could even request the identification of 2 individual people (comparable to requiring two signatures on a check).

The combination of biometrics and smart cards has implications also for homeland security, crime detection, and law enforcement. Crude information security systems focus upon only keeping out unauthorized users. Future research will result in sophisticated information security systems capable of monitoring improper patterns of data usage. Whether disgruntled and clueless employees or external terrorists are attempting to modify or destroy data, sophisticated information security systems will be needed.

Some of the most promising ways to improve information security are biometrics, virtual (or intelligent) agents, and radio frequency identification (RFID). SAP Research is providing the infrastructures for future technologies. Biometrics could fit well within SAP Auto-ID Infrastructure. California State University, Fullerton researchers will focus upon the new technologies. Current and future CEOs, CFOs, CIOs, CSOs, legislators, and many others must learn how to use the new technologies to cope with information security threats, internal and external.

Paul Sheldon Foote ■

Find this article at  
[www.sap.info/en/go/26900/](http://www.sap.info/en/go/26900/)



**Paul Sheldon Foote**, is Professor of Accounting, California State University, Fullerton, USA. He teaches courses using SAP R/3 and is researching a role for biometrics in SAP's auto-ID infrastructure.