

Biometric Technology: ThinkPad and Beyond

By Brian R. Hook
TechNewsWorld
11/02/04 5:00 AM PT

"Everything is a trade-off, and the techniques used to find the bad guys will be balanced by our democracy and drive for rights of privacy," said security expert Evan Scott. "In the end, I think we will have non-evasive forms of security that will confirm identities and not infringe on our rights."

Biometric identification is no longer something found only in science fiction. The technology, such as fingerprint identification and face recognition, is starting to be used on a regular basis on everything from personal computers to airport security systems.

Clain Anderson -- program director for security and wireless at the PC division of IBM (NYSE: IBM) in Research Triangle, North Carolina -- led the team that recently implemented an integrated fingerprint reader on the new IBM ThinkPad T42. The fingerprint reader allows one-touch authentication for users, taking the place of power-on password, the hard-drive password and Microsoft's (Nasdaq: MSFT) Windows operating system password.

IBM ThinkPad Leads Way

Each system with the fingerprint reader also features a security chip called the IBM Embedded Security Subsystem, allowing the fingerprint to be added to other authentication tools. This provides a broad range of security functions, including instant log-on to most applications through a password manager and file encryption.

"IBM's ThinkVantage Technologies have helped to move the PC industry beyond being a commodity business... to sell PCs based on differentiated features," said Anderson. "PC buyers are the winners from these developments."

Anderson said that IBM tests all of its products for privacy-related risks. Fingerprint templates are captured on the sensor and matching is accomplished on the sensor. The templates cannot be copied or sent to another system. "You haven't exposed your fingerprint to the world by using a ThinkPad with a fingerprint reader."

Privacy and Security

Evan Scott, president of the Evan Scott Group International -- a managerial consultation and executive search firm based in Philadelphia that specializes in homeland and physical security technologies, such as biometrics and business intelligence software -- said that although privacy is an issue, it must be weighed against security concerns.

"Everything is a trade-off, and the techniques used to find the bad guys will be balanced by our democracy and drive for rights of privacy," Scott said. "In the end, I think we will have non-evasive forms of security that will confirm identities and not infringe on our rights." He eventually expects the use of biometrics, including iris recognition and digital surveillance technology, to be used on a more regular basis.

Judith Katz, president and chief executive officer of Count Me In, said that the increasing popularity of biometrics is driving the technology into the mainstream. Count Me In, based in the Chicago suburb of Mt. Prospect, develops small business software that integrates fingerprint recognition technology.

"The best of these automated systems integrate with other computer programs, enabling companies to streamline their business functions while eliminating many costly, time-consuming and error-prone administrative tasks," said Katz. The technology behind Count Me In's biometric identification system does not retain the actual fingerprint of an individual, but rather a composite of the fingerprint -- relying on dimensions and other unique distinguishing patterns, Katz explained.

InteliTrac

InteliTrac, based in Rockville, Maryland, has created a high-speed, biometrics security system called IdentiPort. The system provides real-time document authentication, fingerprint verification and face recognition functions.

According to Robert Oertel, vice president of business development, InteliTrac's biometric database targets for real-time or near-real-time matching and searching from a large biometric data set. The system, currently in use at the Santiago Airport in Chile, verifies identification documents such as passports, visas and drivers' licenses.

Dave Bixler, information security officer at [Siemens Business Services](#) (NYSE: SI), said that development of biometrics opportunities are endless. Bixler said that virtually anything from ATMs to safes can make use of biometric technology.

"Assuming the technology proves cost-effective and secure, this technology has the potential to dramatically improve information and physical security at almost all levels. It could also prove to be a boon to the single sign-on vendors," said Bixler.

"Imagine putting a finger on a sensor and authenticating your VPN to connect to your network remotely, logging into your e-mail using the same credential, and ... encrypting and digitally signing the e-mail you're sending."

But Bixler said that until security and privacy issues are completely addressed, biometrics will probably remain a limited-use technology. "Any personal information that is stored centrally is a concern. It only takes one leak ... to irreparably damage your privacy -- that is one genie that can never be put back in the bottle," said Bixler.