

YOU TELL US



INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

THE INFORMATION TECHNOLOGY FOR European Advancement program was formed in 1999 to help European companies compete with U.S. firms in the software realm. So what is Europe getting for the hundreds of millions of euros pouring into the program?

We posed that question to more than a dozen R&D funding experts. Few had

even heard of ITEA, let alone had any opinion about its success.

When the current ITEA program ends in 2008, €1.2 billion (about US \$1.4 billion) and 9500 person-years of R&D will have been invested in 85 projects, involving more than 450 partners from large and small companies, government research centers, and academia, in 23 countries. Funding levels

differ from country to country, but in general, local governments provide 35 percent to 40 percent, with the rest coming from Alcatel, Barco, Bosch, Bull, DaimlerChrysler, Italtel, Nokia, Philips, Siemens, Thales, Thomson, and other companies.

The second incarnation of the program, ITEA 2, which will issue a call for projects that are slated to begin next year, probably will cost €3 billion over eight years. The program aims to fund projects that focus on precompetitive applied research into software to help applications inside a cellphone, PDA, or automobile operate with each other. If successful, such software could give key European industries that make such products a leg up on their international rivals.

It remains to be seen how Europeans will gauge whether ITEA is successful, given that there is no funding for research to assess the return on investment, according to Ed Steinmueller, Science and Technology Policy Research Professorial Fellow at the University of Sussex, in Brighton, England.

He thinks that ITEA managers might not be able to distinguish between projects that explore truly novel technologies and those that could result in merely incremental improvements. But Steinmueller says that this is just speculation on his part. "It is not

THE 8-HOUR LAPTOP

A LAPTOP PC that runs on a single battery charge throughout a long flight would seem to be good news for road warriors, and the prize might soon be at hand. Matsushita Electric Industrial Co. and Intel Corp. announced in August that they would join together to create one.

Matsushita, of Osaka, Japan, is leveraging its technology for lithium-ion batteries, which are not only capacious but fast on the draw, going from dead to three-quarters charged in a minute or so. Intel, of Santa Clara, Calif., plans to add electronic tricks akin to those in its Centrino mobile technology to make more economical use of battery output. It has reported running a PC on a Matsushita Panasonic battery for up to 12 hours in the lab, although right now the two companies are shooting for just 8 hours on the road.

To every silver lining there is a black cloud. "If they want to run all day, they'll probably take away things—the infrared port, the CD-ROM," says IEEE Fellow Nick Tredennick, the editor of *Gilder Technology Report*. "Also, it's not clear there's a market for an all-day laptop now that everybody's moving to PDAs."

And, of course, the guys who get to fly the farthest nonstop are precisely the ones who rate a first-class seat with an electric outlet. And for them, a PDA may be more than enough: they never type anything longer than what they can manage with their thumbs.

More information at <http://intel-news.notlong.com>.

—Philip E. Ross



possible to provide reliable or defensible evidence for such a conclusion without systematic program-level assessment." He adds that the United States and Japan have similar difficulties in assessing the return on investment of R&D funds.

Most ITEA projects have Web sites, but many of them are devoid of useful information. For instance, about all we learn from the AMEC (Ambient Ecologies) site, <http://www.amecproject.com>, is that the project defines the architectural framework and develops the methodologies, tools, and design methods "for people involvement, which will facilitate a user-centred evolution to this new Ambient Intelligent environment."

Other projects, such as ObjectWeb (<http://www.objectweb.org>), an open-source software community that is developing middleware—software that sits between operating systems and applications and helps the nodes communicate efficiently—have active Web sites and are clearly thriving well beyond the termination of ITEA funding.

More information at <http://www.itea-office.org>. Also check out a Philips Research—sponsored list of links to European R&D projects at <http://www.hitech-projects.com/euprojects>.

—Harry Goldstein

FINGERPRINT ID FOR WIRELESS KEYS

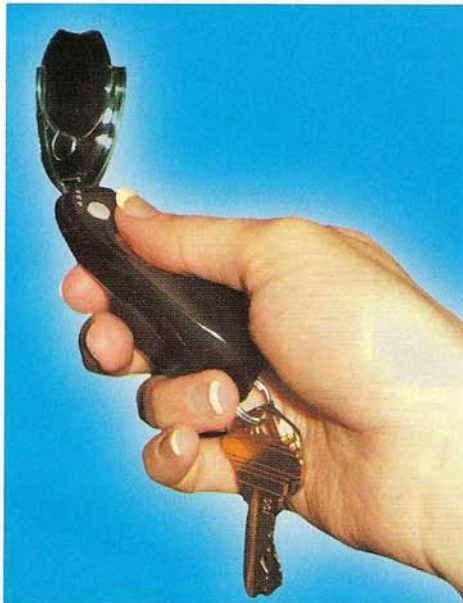
THE TYPICAL FINGERPRINT

ID unit is either affixed to the thing it guards—such as an entryway or a computer—or draws its power and communications link through a USB port. But Fairfax, Va., start-up Privaris Inc. wants to move the fingerprint guardian away from the gate and put it into your pocket. The ID unit consists of a small fingerprint scanner placed in a battery-powered device that fits like a fob on a key chain. Best of all, it can communicate wirelessly with either RFID readers or Bluetooth radios.

A typical use for the Privaris device is as an RFID key to control access to a building. You put your finger onto the fob's sensor, and software determines whether it really is your finger. If the sensor recognizes your finger, an LED lights and the device emits its "Open Sesame" signal. Place the fob within a few centimeters of the RFID reader and the door will unlock. The advantage of the biometric sensor in this scenario, in case you missed it, is that someone who steals your key still can't get into the building. The advantages of putting the sensor in a wireless device are its convenience and its compatibility with existing RFID readers.

Privaris's innovation is not in the sensor itself, which is made by a leading fingerprint sensor company, AuthenTec Inc., of Melbourne, Fla. Instead the smarts lie in fitting all the processing power needed to interpret the fingerprint sensor's data into something the size of a key-chain fob, according to Michael M. Kohnoski, Privaris's chief operating officer.

Privaris has also thought through a number of potential vulnerabilities. Because all the fingerprint recognition happens inside the device itself, no data describing your fingerprint, which would be a nice prize for an identity thief, will ever be transmitted through the air or over a network. Sniffing the wireless signal won't get a thief anywhere either, because the Bluetooth signal is encrypted, and the RFID signal has such a short range that a person would have



to be indecently close to pick it up. A thief also can't steal a Privaris fob and reprogram it, because the fob can be reprogrammed only by the machine that originally set it up, Kohnoski explains. And that would be safely behind the door the thief is trying to breach.

Fingerprint recognition systems can err in two ways. There are false positives, as in: "I'm not Joe, but thanks for letting me into his office," and false negatives, as in: "I'm Joe. Why won't you let me in my office?!"

The rate of false positives for the Privaris unit can be set from 1 in 1000 to 1 in 100 000, depending on the application or your level of paranoia. But increasing security comes at the cost of a slightly longer delay between when you put your finger on the sensor and when the device recognizes you—going from less than a second to about 1.5 seconds.

It's the false negatives that bother the average user, because they can cause long queues at entryways as people repeatedly try and fail to get ID systems to recognize them. Privaris doesn't track false negatives but says they shouldn't happen if there was a good "enrollment," when the separate set-up machine read your fingerprint scan and downloaded the data into your wireless device.

More information at <http://www.privaris.com>.

—Samuel K. Moore

FROM LEFT: CUT AND DEAL/INDEXOPEN & RIM; PETER BEAVIS/GETTY IMAGES; PRIVARIS