

# MIT technology insider

FROM THE EDITORS OF TECHNOLOGY REVIEW

CONTENTS

12.03

**1 Spinoff Spotlight**  
CoreStreet finds a new way to lock the door

**3 Lab News**  
What to do with wireless/Visualizing the genome/Pebble-bed fellows/Bacteria clustering solved

**4 In the Lab**  
Hatsopoulous  
Microfluids Laboratory

**5 Technology Transfer Report**  
License to strain/Money for genes/Cash for conferencing/Mapping mutations

**6 MIT Insight**  
Productivity's technology iceberg

**7 The List**  
MIT's most frequently cited patents

## KEY

### FUNDING

\$	UNDER \$2 MILLION
\$\$	\$2 MIL.-\$10 MIL.
\$\$\$	\$10 MILLION PLUS

### PATENT STRENGTH

☐	NO CORE PATENTS
☐☐	CORE PROTECTION
☐☐☐	DOMINANT POSITION

### TIME TO MARKET

🕒	LESS THAN 1 YEAR
🕒🕒	1-3 YEARS
🕒🕒🕒	MORE THAN 3 YEARS

## SPINOFF SPOTLIGHT

# Securities Exchange

CORESTREET USES CRYPTOGRAPHIC TECHNOLOGY TO CREATE A SECURITY SYSTEM THAT PERMITS CONTROL OF ACCESS TO DOORS AND DATABASES

On October 11, 2001—exactly one month after the terrorist attacks—a group of Java programmers founded CoreStreet. The group had sold its previous venture, Engine 5, which developed e-commerce systems for companies such as Nokia, Barnes & Noble, and Yahoo! Their original, vague intention had been to launch a software company and then come up with an idea for a product. But the rush of events gave shape to their amorphous mission. The dot-com bubble had burst, and the country was consumed with anxiety about the threat of terrorism, so they decided to focus on security. “We wanted to do something more meaningful,” says CoreStreet president Phil Libin.

The programmers started operations with \$1.5 million of their own money, and by January 2002 they had recruited Silvio Micali, a professor in the Cryptography and Information Security Group of the MIT Laboratory for Computer Science. Micali had recently founded his own firm, NovoModo, based on a dozen patents for a secure identification system. The two startups merged in August 2002, and the new entity, operating under the CoreStreet name, sells a system that can validate—in real time—individuals’ authorization to access secure areas. So far, the CoreStreet system manages access only to computers, but the company aims to create a key that could govern access to both computer files and locked rooms.

Micali—who is now CoreStreet’s chief scientist and was also founder of Peppercoin, a company that handles micropayments over the Web—explains that a secure-access solution must address two separate problems. One is authentication: proving that a person is who he says he is. There are plenty of mechanisms for doing this, including personal identification numbers (PIN), identification cards, and retinal scanning. The

much tougher problem, which CoreStreet addresses, is validation: showing that a particular person is allowed to access a specific area at the time he chooses and also to engage in the activities he wants to engage in.

There are ways to perform validation. If a secure door is wired into a network, a central database can provide up-to-the-minute access information. But the process takes time and bandwidth, and requires the database to be online. Moreover, it would be too expensive to wire together, all the PIN-controlled locks on secure doors at airports.

Some locations—such as cargo containers at sea or doors to airplane cockpits—simply cannot be connected by wire. And wireless connections can be both insecure and slow.

Imagine you are running a military base. Thousands of new recruits might pass through each month, each staying for only 30 days. You could give them

temporary access to a restricted area for a particular project, but what if they are not allowed in once the project is over? A daily master list could specify whose authorizations have been revoked—but with more than, say, 100,000 users, such a system would be impractical.

CoreStreet provides what the company calls proofs: strings of data, each about 20 bytes long, created through cryptography. The data strings grant particular access privileges at particular times. These proofs are similar to the public keys in e-mail security systems, but they are much more compact. Only the person with the cryptographic key can produce the proofs.

A proof is an algorithm that performs a mathematical test on each person’s information: his identity, the identity of the computer or door he wants to access, and the time period for which access is allowed. If all those factors are valid, the



CONTINUED ON PAGE 2

**AT A GLANCE**

## NAME

CoreStreet

## CONTACT

Phone: 617-661-3554

www.corestreet.com

## PRODUCTS

&gt; Secure access-validation system

algorithm produces a yes. But if, say, access was good only yesterday, then today the numbers will add up wrong—and the request will be rejected.

The proofs themselves contain no secrets, and thus they may be distributed publicly for matching against any identification system that is used. (Micali says CoreStreet considers itself “agnostic” on the question of identification.) Because the proofs are so small, they can sit on distributed servers until they’re needed, or they can be sent over a pager or cell phone to a person who is seeking instant access in a remote location—such as that seafaring cargo hold. Because proofs are generated by a cryptographic key, any attempt to alter one would be evident. And since they’re good for only a set period of time, people could carry their proofs with them on ID badges or key cards.

The first customers for the technology, Libin says, were the federal government and financial institutions—organizations already familiar with the need for and the difficulty of performing validation. In January 2003 the company signed an agreement with Akamai Technologies in Cambridge, MA. Akamai, which sets up servers around the Internet to cache content, stores the proofs at various sites for easy access when they’re needed.

But why not combine a security system that allows the right people to get into, say, a pharmaceutical company’s database with one that allows them to get into its building? Last September CoreStreet formed a partnership with Assa Abloy, the world’s largest lock manufacturer, to start making locks compatible with the CoreStreet proof system. Again, the first customers are those with advanced security needs—including military bases and banks. But Libin says the technology could eventually be incorporated into locks for

less demanding applications, such as hotels. Micali imagines proofs becoming part of vehicle ignition systems, so that, for example, only an authorized driver would be allowed to drive a truck full of hazardous cargo.

The company is also pursuing the growing market for high-tech ID cards. Already, the U.S. Department of Defense has issued three million Common Access Cards, with a total of five million due by the end of next year, Libin says. These cards are designed to provide access to buildings and computer networks; they also allow cardholders to sign e-mail digitally, verifying the source of messages they send. The government is starting to issue Transportation Workers Identity Credentials to people who drive trucks and work in airports and railroad stations. About 12 million people may eventually be credentialed. And several European countries are working on national ID cards. “Just staying in military- and national-ID-style programs, it’s very big business, and brand new,” says Libin. “Two years ago it didn’t exist.”

Victor Wheatman, an analyst who covers security for Gartner Research, agrees that groups that need high security—the intelligence community and operators of nuclear power plants, for instance—would find products like those from CoreStreet useful. But he wonders whether other applications will require that level of security. “Passwords and user IDs are good enough” for most corporate access-control purposes, Wheatman says.

Based in Cambridge, MA, CoreStreet has grown from its original group of about half a dozen to 33 employees. The company raised \$4 million in an original financing round led by POD Holding of Stockholm, Sweden, and Boston. Libin expects a second fund-raising round, now in the works, to see the company through to profitability.

**SUBSCRIPTION ORDER FORM**

**YES!** I’d like to subscribe and receive the charter subscription rate of \$125 for 12 electronic issues. And with my paid subscription I’ll receive the **MIT Spinoff Directory**, a comprehensive five-year listing of all MIT spinoff companies. Plus, every three months, I will also receive an exclusive report tallying MIT’s most important deals—the **MIT Quarterly Licensing Report**.

NAME \_\_\_\_\_

ADDRESS \_\_\_\_\_

CITY \_\_\_\_\_ STATE \_\_\_\_\_ ZIP \_\_\_\_\_ COUNTRY \_\_\_\_\_

E-MAIL (required) \_\_\_\_\_

Fill out this form or click here to subscribe

 **GO TO WWW.TECHNOLOGYINSIDER.COM****MIT**technologyinsider

FROM THE EDITORS OF TECHNOLOGY REVIEW

**PUBLISHER & CEO**

R. Bruce Journey

**EDITOR IN CHIEF**

Robert Buder

**V.P. GENERAL MANAGER**

Martha Connors

**MANAGING EDITOR**

Herb Brody

**CONTRIBUTORS**

Sally Atwood, Neil Savage, Lisa Scanlon, Tracy Staedter, Davin Wilfrid

**COPY EDITOR**

Elyse Friedman

**GRAPHIC DESIGNER**

Matthew Bouchard

**EDITORIAL INDEPENDENCE**

Technology Review, Inc. is a wholly owned and separately incorporated subsidiary of MIT that is editorially independent from the university and its administration, faculty, and community. All content of the *MIT Technology Insider* is the sole responsibility of the editors. Sponsors have no influence over editorial content, and no employee or contractor is permitted to have any financial positions in companies covered.

MIT Technology Insider

Technology Review, Inc.

One Main Street, 7th Floor, Cambridge, MA 02142

tel 617-475-8000 fax 617-475-8043

www.technologyinsider.com