



You can thank George Davida for Internet security.

Secrets and Lies? *An outspoken professor laments the unraveling of UWM's cryptography program.*

BY ROBERT MCGUIRE

Nobody calls professor George Davida a wallflower. You can find him most mornings at the counter at Beans & Barley, having his regular breakfast of coffee and whole-wheat toast, holding forth indignantly on just about any topic the morning news provides.

But in the world of cryptography (the study of codes and ciphers), his specialty as a professor of computer science at the University of Wisconsin-Milwaukee, Davida is best known for a tense standoff he had in the late '70s with the National Security Agency, which for several months was threatening to jail him for his work. They said his research would make it easier for the bad guys to keep secrets from the good guys. They issued a secrecy order demanding that he stop and never talk

about it to anyone. He confesses now that he was frightened. But at the time, he was all over the national media insisting that academic freedom trumps national security, and the government eventually backed off.

That was the first of many battles in defense of academic freedom that in the area of cryptography, according to others in the field, have made possible the secure electronic commerce many of us take for granted today. If the NSA had had its way, doing business with *eBay* and *Amazon.com* would be either less secure or more expensive. And, they say, the NSA didn't get its way because of Davida.

"There were only a few people with the guts and vision early enough to make this fight. I think the country as a whole owes him quite a bit," says Rene

Peralta, a former UWM professor who worked with Davida.

"He's one of those people who is a pioneer, and because he was controversial, he's not been given the credit," adds Gene Spafford, a computer science professor at Purdue University. "Some people were saying, 'Don't rock the boat. You'll jeopardize funding.' But he stood up for principle."

Davida isn't shy about rocking boats. He says too many faculty members resent and undermine the success of others and too few administrators know enough about cryptography to support it. In his version of events, UWM's three cryptographers had the market cornered on cutting-edge research and had excellent reputations in the rest of academia and the industry. But those resources were squandered and the two other professors driven away.

"UWM and the UW System doesn't seek to enhance areas of excellence in which they are known," says Davida. "It's basically a matter of jealousy and holding grudges."

Spafford and G.R. Blakley at Texas A&M both say UWM had one of the best-known cryptography programs in the country but that its star has fallen, citing the renown of faculty who have left.

Peralta, now at Yale, says he

came to the United States specifically to work with Davida but was finally driven unwillingly from Milwaukee: "It's a classic story of an institution that ought to be striving to be better, but to be better wasn't in the interests of some of the people there. We had everything from benign neglect to outright hostility from the university."

When it comes to Davida's own reputation, other cryptographers mention his leadership more than his research. His most famous research paper exposed the flaws in someone else's work. He found the vulnerability in a technology invented at the Massachusetts Institute of Technology, which forced them back to the drawing board to develop the electronic signatures essential for electronic commerce today.

Davida works in one of those monkish fields that bewilders the uninitiated. And like many professors, he's not as good as he could be at translating that work to the rest of us. He and his graduate students are now working in biometrics – how to turn an image of the body into a digitally encrypted signature. Is that like the retinal scans you see in the movies? he's asked.

"No, no," he says impatiently. "Retinas are a dead end. The iris is much better."

Who Wants to Be a Millionaire?

To afford the Kohler Co.'s new exclusive Riverbend club, you'll have to be one. That, and be willing to part with a \$55,000 deposit (refundable upon termination after 10 years of membership) and \$2,700 a year for the privilege of gracing the estate of former Gov. Walter Kohler. Or go for broke with a \$6,200-a-year golf membership. But count yourself lucky, if you've got the dough. According to Alice Hubbard, Kohler's group vice president of hospitality and real estate, the membership costs are reasonable, when compared with other similar clubs across the country, which she says require deposits of between \$75,000 and \$125,000: "We wanted to be a little more conservative in pricing."