Oblivious RAM

If encryption isn't going to cut it, how else will businesses secure data?

BY CHRISTINE CIGNOLI

LACK OF SECURITY is often cited as a stumbling block by those businesses hesitant to move data and services to the cloud. That hasn't stopped plenty of enterprises, though.

But current methods of security—namely encryption—may not be cutting it. (See last summer's NSA PRISM surveillance program debacle for a prime example.) In general, software-based security isn't to be trusted, according to one MIT researcher, who's been working on designing a hardware component to better secure servers.

"Think of software security as just trusting millions of lines of code," said Srini Devadas, the Edwin Sibley Webster Professor of Electrical Engineering and Computer Science at MIT. "You don't know who wrote it, but it's really convenient to trust the code."

Security in the cloud is largely based on various methods of encryption. Encryption can hide the exact data that's accessed or downloaded through websites or cloud-based software or services, but it can't hide that the access is happening, or the fact that a certain site is being accessed. That information—those memory access patterns—make it possible to see which sites a user is accessing, and when, regardless of whether encryption is being used. And those patterns can give away important information.

The work Devadas and some of his graduate students are doing (along with researchers from several other universities) focuses on hiding those memory access, or memory at rest, patterns.

The crux of the research project is Oblivious RAM, or O-RAM. In the past, there's been too much overhead associated with O-RAM to consider it for practical use.

"We invented a new kind of O-RAM," Devadas said. "We got the overhead down, and that is the academic contribution. To make this whole thing viable, you can't hide access patterns if every access turns into a million accesses. It would take forever to do any real work."

FROM THE LAB TO THE DATA CENTER

Existing methods of security aren't enough, Devadas said. "People are not going to the level of doing encryption that they should to protect themselves." But the challenge with hardware security is that development and deployment take much longer than for software counterparts, he said.

And the road from academia to available product is paved with discarded ideas.

"The academic to commercial deployment gap is a really big gap," Devadas said. Some of his projects have simply stayed in the lab, though one started 10 years ago is just now being deployed. In the next year or so, Devadas and his team will focus on building their concept into a real silicon processor.

The MIT research announcement certainly comes at a good time—or a bad one, from the perspective of software makers. Last summer's NSA debacle shed light on the limits of encryption used for cloud security—and sometimes, timing is everything for a concept to become reality.

"With security, things change quickly," Devadas said. "You never know. It suddenly becomes a problem." ■

CHRISTINE CIGNOLI *is managing editor of* Modern Infrastructure. *Contact her at ccignoli@techtarget.com.*