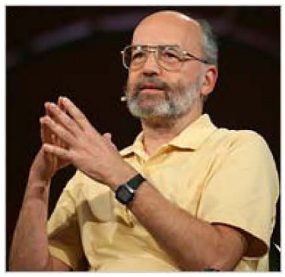
The New York Times

Technology

Adding Math to List of Security Threats

By JOHN MARKOFF
Published: November 17, 2007

SAN FRANCISCO, Nov. 16 — One of the world's most prominent cryptographers issued a warning on Friday about a hypothetical incident in which a math error in a widely used computing chip places the security of the global electronic commerce system at risk.



Gabriel Bouys/Agence France-Presse — Getty Images

Adi Shamir, a cryptographer and professor in Israel.

Adi Shamir, a professor at the Weizmann Institute of Science in Israel, circulated a research note about the problem to a small group of colleagues. He wrote that the increasing complexity of modern microprocessor chips is almost certain to lead to undetected errors.

Historically, the risk has been demonstrated in incidents like the discovery of an obscure division bug in Intel's Pentium microprocessor in 1994 and, more recently, in a multiplication bug in Microsoft's Excel spreadsheet program, he wrote.

A subtle math error would make it possible for an attacker to break the protection afforde to some electronic messages by a popular technique known as public key cryptography.

Using this approach, a message can be scrambled using a publicly known number and then unscrambled with a secret, privately held number.

The technology makes it possible for two people who have never met to exchange information securely, and it is the basis for all kinds of electronic transactions.

Mr. Shamir wrote that if an intelligence organization discovered a math error in a widely used chip, then security software on a PC with that chip could be "trivially broken with a single chosen message."

Executing the attack would require only knowledge of the math flaw and the ability to sen a "poisoned" encrypted message to a protected computer, he wrote. It would then be possible to compute the value of the secret key used by the targeted system.

With this approach, "millions of PC's can be attacked simultaneously, without having to manipulate the operating environment of each one of them individually," Mr. Shamir wrote.

The research note is significant, cryptographers said, in part because of Mr. Shamir's role in designing the RSA public key algorithm, software that is widely used to protect e-commerce transactions from hackers.

"The remarkable thing about this note is that Adi Shamir is saying that RSA is potentially vulnerable," said Jean-Jacques Quisquater, a professor and cryptographic researcher at the Université Catholique de Louvain in Belgium.

Mr. Shamir is the S in RSA; he, Ronald Rivest and Leonard Adleman developed it in 1977.

Because the exact workings of microprocessor chips are protected by laws governing trade secrets, it is difficult, if not impossible, to verify that they have been correctly designed, Mr. Shamir wrote.

"Even if we assume that Intel had learned its lesson and meticulously verified the correctness of its multipliers," he said, "there are many smaller manufacturers of microprocessors who may be less careful with their design."

The class of problem that Mr. Shamir described has been deeply explored by cryptography experts, said Paul Kocher, who is president of Cryptography Research, a consulting and design firm in San Francisco. However, he added that it illustrated how small flaws could subvert even the strongest security.

An Intel spokesman noted that the flaw was a theoretical one and something that required a lot of contingencies.

"We appreciate these and we look at everything," said George Alfs, an Intel spokesman.

In e-mail correspondence after he sent the note, Mr. Shamir said he had no evidence that anyone is using an attack like the one he described.