Dutch Court: NXP's smart card code can be released

July 21, 2008 5:11 PM ET

AMSTERDAM, Netherlands (AP) - A Dutch company warned corporate customers Monday to upgrade the security of a smart-card chip widely used to enter buildings and for public transportation after scientists won the right to publish its arithmetic code.

A spokesman for NXP Semiconductors said the compromised code of the smart cards may require "complex system modifications" of hardware, software and infrastructure, and could take years for customers to secure their systems.

A district court in Arnhem on Friday rejected NXP's request to block a research group from Radboud University Nijmegen from publishing the algorithm of the Mifare Classic chip that the scientists had decoded.

The research group, headed by Bart Jacobs, said it told NXP in March it would release its findings at a Spanish conference in October 2008, giving the chip-maker six months to react. NXP said publication of the algorithm would be irresponsible.

"Damage to NXP does not result from the publication of this article but from the production and marketing of a defective chip, which is NXP's responsibility," the court said.

NXP spokesman Pieter van Nuenen said the Mifare Classic is one of several chips the company makes and is about 10 years old, making it "not the most modern and secure one."

The Mifare Classic is used in more than 1 billion cards, roughly 70 percent of "contactless" smart cards worldwide, NXP says on its Web site. It said the London subway and bus system invested $400 million in a system based on the chip.

Van Nuenen said it was "very unlikely" the company will appeal.

A company statement urged customers to take "the appropriate measures to upgrade the security" of their systems, whether by switching to a higher level security chip or to another system altogether.

"Different installations have different security requirements," it said, and it was impossible to protect all users before the scheduled publication date. "These upgrades will take up to a number of years," the statement said.

But hacking into the system, even with the code, is not simple, said Jacobs, a professor of software security.

Jacobs told The Associated Press that even with the information released in the scientific paper, malicious hackers would still need to buy hardware and write software to manipulate the chips, which could take months.

His academic group spent more than a year researching the Mifare Classic, analyzing what went in and out of it to uncover the mathematics behind it. He said the majority of time was spent figuring out how to "talk" to the chip, while the cryptology only took about a month to crack.

Jacobs said his group intended to strengthen security, not to create chaos. Another group in the United States also cracked the chip but used a different approach, physically dismantling the chip to figure out how it worked, he said.

"We are the messengers," Jacobs said about the case. "Killing the messenger doesn't solve the problem."