Unique locks on microchips could reduce hardware piracy

March 5 2008

Hardware piracy, or making knock-off microchips based on stolen blueprints, is a burgeoning problem in the electronics industry.

Computer engineers at the University of Michigan and Rice University have devised a comprehensive way to head off this costly infringement: Each chip would have its own unique lock and key. The patent holder would hold the keys. The chip would securely communicate with the patent-holder to unlock itself, and it could operate only after being unlocked.

The technique is called EPIC, short for Ending Piracy of Integrated Circuits. It relies on established cryptography methods and introduces subtle changes into the chip design process. But it does not affect the chips' performance or power consumption.

Michigan computer engineering doctoral student Jarrod Roy will present a paper on EPIC at the Design Automation and Test in Europe conference in Germany on March 13.

Integrated circuit piracy has risen in recent years as U.S. companies started outsourcing production of newer chips with ultra-fine features. Transferring chip blueprints to overseas locations opened new doors for bootleggers who have used the chips to make counterfeit MP3 players, cell phones and computers, among other devices.

This is a very new problem, said Igor Markov, associate professor in the

Department of Electrical Engineering and Computer Science at U-M and a co-author of the paper.

"Pirated chips are sometimes being sold for pennies, but they are exactly the same as normal chips," Markov said. "They were designed in the United States and usually manufactured overseas, where intellectual property law is more lax. Someone copies the blueprints or manufactures the chips without authorization."

A cutting-edge fabrication facility costs between $3 billion and $4 billion to build in the United States., said Farinaz Koushanfar, assistant professor in the Department of Electrical and Computer Engineering at Rice University and a co-author on the paper.

"Therefore, a growing number of semiconductor companies, including Texas Instruments and Freescale (a former division of Motorola), has recently announced that they would cease manufacturing chips with finer features, and outsource production to East Asia. However, even in U.S. facilities, working chips are sometimes reported defective by individual employees and later sold in gray markets," Koushanfar said.

With EPIC protection enabled, each integrated circuit would be manufactured with a few extra switches that behave like a combination lock. Each would also have the ability to produce its own at least 64-bit random identification number that could not be changed. The chips would not be manufactured with an ID number, but instead with the tools needed to produce the number during activation.

In the EPIC framework, chips wouldn't work correctly until they were activated. To activate a chip, the manufacturer would plug it in and let it contact the patent owner over an ordinary phone line or Internet connection.

"All chips are produced from the same blueprint, but differentiate themselves when they are turned on for the first time and generate their ID," Roy said. "Nothing is known about this number before activation."

The chip would transmit its ID securely to the patent owner. The patent owner would record the number, figure out the combination to unlock that particular chip, and respond securely with the key.

The uniqueness of the activation key rules out the possibility that someone could observe it and reuse it without cracking it. Because the key is generated on the fly, it wouldn't make sense to copy it like you could copy software activation keys, which are printed on CD envelopes.

Theoretically, there are ways to illegally copy chips protected by EPIC, Markov said. But EPIC makes this very difficult.

"If someone was really bent on forging and had a hundred million dollars to spend, they could reverse-engineer the entire chip by taking it apart. But the point of piracy is to avoid such costs," he said. "The goal of a practical system like ours is not to make something impossible, but to ensure that buying a license and producing the chip legally is cheaper than forgery."

Ending Piracy of Integrated Circuits (.pdf):
www.eecs.umich.edu/~imarkov/pu … conf/date08-epic.pdf

Source: University of Michigan