Graduate Cryptographers Unlock Code of 'Thief Proof' Car Key

By JOHN SCHWARTZ

Published: January 29, 2005 in New York Times

All that would be required to steal a car, the researchers said, is a moment next to the car owner to extract data from the key, less than an hour of computing, and a few minutes to break in, feed the key code to the car and hot-wire it.

An executive with the Texas Instruments division that makes the systems did not dispute that the Hopkins team had cracked its code, but said there was much more to stealing a car than that. The devices, said the executive, Tony Sabetti, "have been fraud-free and are likely to remain fraud-free."

The implications of the Hopkins finding go beyond stealing cars.

Variations on the technology used in the chips, known as RFID for radio frequency identification, are widely used. Similar systems deduct highway tolls from drivers' accounts and restrict access to workplaces.

Wal-Mart is using the technology to track inventory, the Food and Drug Administration is considering it to foil drug counterfeiting, and the medical school at the University of California, Los Angeles, plans to implant chips in cadavers to curtail unauthorized sale of body parts.

The Johns Hopkins researchers say that if other radio frequency ID systems are vulnerable, the new field could offer far less security than its proponents promise.

The computer scientists are not doing R.&D. for the Mafia. Aviel D. Rubin, a professor of computer science who led the team, said his three graduate students did what security experts often do: showed the lack of robust security in important devices that people use every day.

"What we find time and time again is the security is overlooked and not done right," said Dr. Rubin, who has exposed flaws in electronic voting systems and wireless computer networks.

David Wagner, an assistant professor of computer science at the University of California, Berkeley, who reviewed a draft of a paper by the Hopkins team, called it "great research," adding, "I see it as an early warning" for all radio frequency ID systems.

The "immobilizer" technology used in the keys has been an enormous success. Texas Instruments alone has its chips in an estimated 150 million keys. Replacing the key on newer cars can cost hundreds of dollars, but the technology is credited with greatly reducing auto theft. - Early versions of in-key chips were relatively easy to clone, but the Texas Instruments chips are considered to be among the best. Still, the amount of computing the chip can do is restricted by the fact that it has no power of its own; it builds a slight charge from an electromagnetic field from the car's transmitter.

Cracking the system took the graduate students three months, Dr. Rubin said. "There was a lot of trial and error work with, every once in a while, a little 'Aha!' "

The Hopkins researchers got unexpected help from Texas Instruments itself. They were able to buy a tag reader directly from the company, which sells kits for $280 on its Web site. They also found a general diagram on the Internet, from a technical presentation by the company's German division. The researchers wrote in the paper describing their work that the diagram provided "a useful foothold" into the system. (The Hopkins paper, which is online at **www.rfidanalysis.org,** does not provide information that might allow its work to be duplicated.

The researchers discovered a critically important fact: the encryption algorithm used by the chip to scramble the challenge uses a relatively short code, known as a key. The longer the code key, which is measured in bits, the harder it is to crack any encryption system.

"If you were to tell a cryptographer that this system uses 40-bit keys, you'd immediately conclude that the system is weak and that you'd be able to break it," said Ari Juels, a scientist with the research arm of RSA Security, which financed the team and collaborated with it.

Graduate Cryptographers Unlock Code of 'Thiefproof' Car Key

Published: January 29, 2005 by New York Times

(Page 2 of 2)

The team wrote software that mimics the system, which works through a pattern of challenge and response. The researchers took each chip they were trying to clone and fed it challenges, and then tried to duplicate the response by testing all 1,099,511,627,776 possible encryption keys. Once they had the right key, they could answer future challenges correctly.

Mr. Sabetti of Texas Instruments argues that grabbing the code from a key would be very difficult, because the chips have a very short broadcast range. The greatest distance that his company's engineers have managed in the laboratory is 12 inches, and then only with large antennas that require a power source.

Dr. Rubin acknowledged that his team had been able to read the keys just a few inches from a reader, but said many situations could put an attacker and a target in close proximity, including crowded elevators.

The researchers used several thousand dollars of off-the-shelf computer equipment to crack the code, and had to fill a back seat of Mr. Green's S.U.V. with computers and other equipment to successfully imitate a key. But the cost of equipment could be brought down to several hundred dollars, Dr. Rubin said, and Adam Stubblefield, one of the Hopkins graduate students, said, "We think the entire attack could be done with a device the size of an iPod."

The Texas Instruments chips are also used in millions of the Speedpass tags that drivers use to buy gasoline at ExxonMobil stations without pulling out a credit card, and the researchers have shown that they can buy gas with a cracked code. A spokeswoman for ExxonMobil, Prem Nair, said the company used additional antifraud measures, including restrictions that only allow two gas purchases per day.

"We strongly believe that the Speedpass devices and the checks that we have in place are much more secure than those using credit cards with magnetic stripes," she said.

The team discussed its research with Texas Instruments before making the paper public.

Matthew_Buckley, a spokesman for RSA Security, said his company, which offers security consulting services and is developing radio frequency ID tags that resist unauthorized eavesdropping, had offered to work with Texas Instruments free of charge to address the security issues.

Dr. Wagner said that what graduate students could do, organized crime could also do. "The white hats don't have a monopoly on cryptographic expertise," he said.

Dr. Rubin said that if criminals did eventually duplicate his students' work, people could block eavesdroppers by keeping the key or Speedpass token in a tinfoil sheath when not in use. But Mr. Sabetti, the Texas Instruments executive, said such precautions were unnecessary. "It's a solution to a problem that doesn't exist," he said.

Dan Bedore, a spokesman for Ford, said the company had confidence in the technology. "No security device is foolproof," he said, but "it's a very, very effective deterrent" to drive-away theft. "Flatbed trucks are a bigger threat," he said, "and a lot lower tech."