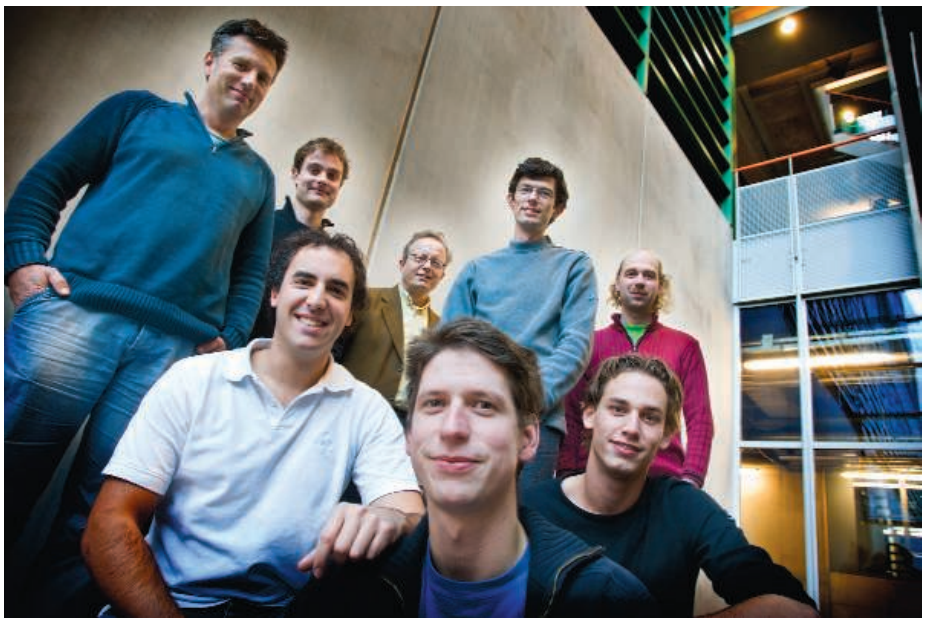


The Radboud gang. Clockwise from the left: Ronny Wichers Schreur, Gerhard de Koning Gans, Bart Jacobs, Wouter Teepe, Peter van Rossum, Ruben Muijers, Roel Verdult, and Flavio Garcia.

CREDIT: DICK VAN AALST, RADBOUD UNIVERSITY NIJMEGEN

CRYPTOGRAPHY

University Hackers Test the Right To Expose Security Concerns

When students in the Netherlands picked apart the world's most common smart card system, were they torpedoing its manufacturer or protecting the public's right to know?

NIJMEGEN, THE NETHERLANDS—In winter 2006, Roel Verdult was looking for a project for his master's thesis in computer science here at Radboud University Nijmegen. Flavio Garcia, then a doctoral student, laid down an unusual challenge. "He said, 'Well, for a goal, let's start with free parking,' " Verdult recalls. Garcia wanted Verdult to intercept and commandeer the communications between a gate controller at a parking lot and the "radio-frequency identification" (RFID) cards people wave in front of it to activate it.

Thus began an adventure that in March would lead Verdult, Garcia, and colleagues in Radboud's software security and correctness program to crack the secret messages exchanged in the world's most widely used RFID system, the MIFARE Classic. The card system opens parking gates, but it also tallies fares in the London Underground, the Netherlands' OV-Chipkaart transit system, and dozens of other transportation systems around the world. It also controls access to military bases, nuclear power plants, and myriad other buildings, the researchers say.

The team's "hack" would bring the Dutch secret service to the Radboud lab, force the country to consider replacing more than 600,000 transit fare cards, and prompt a lawsuit from the system's manufacturer, NXP Semiconductors, which sought to suppress the researchers' work. The episode has thrown a spotlight on the tension between an academic's desire to publish and the potential damage that could result. In this case, a judge ruled that the Radboud group had a right to publish their findings, as they did last month.

The company is not happy: "Broadly publishing detailed information … is, in our understanding, not responsible disclosure of sensitive information," says NXP spokesperson Alexander Tarzi. Garcia counters that, with a billion MIFARE Classic cards in circulation, the public should know they do not provide real security: "I believe the world is better off with this information out there."

A peek inside

If a hacker is supposed to be a geeky loner holed up in his cluttered bedroom, the Radboud guys don't fit the stereotype. Garcia, 30, drives a 2001 Alfa Romeo GTV sports car, used to race motocross, and says he enjoys the nightlife. Verdult, 26, practices karate and has a vicelike handshake and an easy smile. But both have been fiddling with computers since they were children. Growing up in Argentina, Garcia started programming simple video games at age 7. As an undergraduate intern at a software company, Verdult figured out how to run the company's software on computers lacking a special license chip—and alerted his boss.

To tackle the MIFARE Classic system, Verdult and Garcia built a €40 gadget to listen to the conversations between its RFID cards and readers. They joined forces with master's student Gerhard de Koning Gans, who built a similar device that talked to a reader as well. "Security evaluations are an intrinsic part of this field," says Bart Jacobs, director of Radboud's software security and correctness program. "We regularly ask our students to do them."

The Radboud team had to figure out how the MIFARE Classic reader and card scramble their messages. The messages are binary numbers—strings of 0s and 1s—that spell out commands, such as "Deduct €1.60 from the amount recorded on the card." As in many cryptographic schemes, the messages are scrambled using another sequence of 0s and 1s called a "key stream." In a conversation, each bit of each message is combined with a bit of the key stream through an "exclusive or" (XOR), a maneuver just like adding the two bits, except that the sum of 1 and 1 is set to zero. (If a command is 1100 and the key stream 0101, the XOR-scrambled message is 1001.)

Ideally, the key stream should be random, but being a machine, a MIFARE Classic reader cannot generate a truly random string of 0s and 1s. Instead, it relies on a complex but predictable recipe. (The card has the same system, which it synchronizes to the reader's.) The challenge was to figure out this secret recipe. If they could do that, the researchers could calculate the key stream to decipher any conversation or even send commands to rewrite or clone cards.

The Radboud students weren't the only ones prying into the system. Karsten Nöhl, a grad student at the University of Virginia, Charlottesville, and Henryk Plötz, a grad student at Humboldt University in Berlin, literally hacked open chips from MIFARE Classic readers and cards to see the wiring inside, as they reported at the Chaos Communication Congress in Berlin in December 2007.

At the system's heart lay a digital circuit called a linear feedback shift register (LFSR). It takes 48 0s and 1s jumbled in a row and, with each tick of the chip's clock, shifts them all one space to the left, spitting out the left-

Published by AAAS

most bit and using a feedback circuit to inject a 0 or 1 into the empty spot at the right (see diagram). A hugely long string of seemingly random bits emerges from the LFSR's left end. That output is too predictable to make a key stream, however. So, in the MIFARE Classic, certain bits of the LFSR feed into a filter function—which Nöhl and Plötz didn't reveal—for more scrambling. With each clock tick, the filter uses the current settings of those bits to calculate one bit of key stream.

Nöhl and Plötz showed parts of how the system works. But knowing how a thing works doesn't guarantee you can break into it, says Wouter Teepe, a postdoc at Radboud. "I can take apart the lock in my door to see how it works," he says. "But even if my neighbor has the same [type of] lock, knowing how it works doesn't mean I can get into his house" without the key.

Tell me your secrets

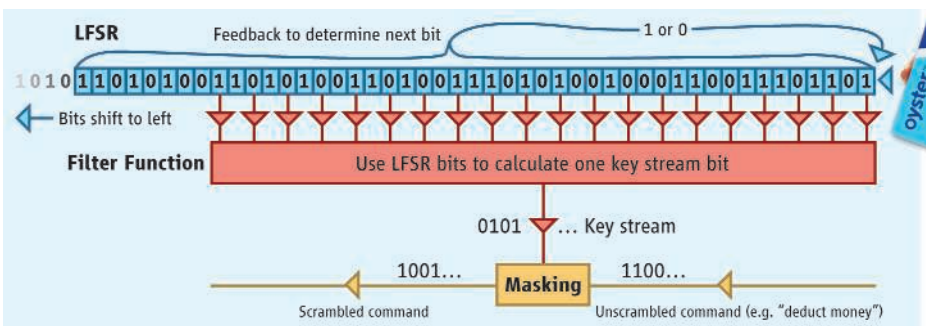
To pick that digital lock, the Radboud researchers still needed two things: the precise form of the filter function and the very first settings of the bits in the LFSR—the so-called "key" which serves as a seed for generating the key stream. The MIFARE Classic reader would soon tell them enough to deduce both. Whenever a MIFARE Classic card comes within range of a reader, the card sends its 32-bit ID number. Using that ID, the reader looks up the card's individualized key and loads it in the LFSR. To make sure the reader is legit, the card also sends a 32-bit random number called a challenge nonce that the reader must respond to correctly. The reader sends a challenge nonce of its own and then replies to the card's challenge—although now that the key has been set, these two messages and all that follow are scrambled with the key stream. Finally, the card answers the reader's nonce, ending the "initialization."

De Koning Gans and Verdult quickly found oddities in this exchange of hellos. Every time the reader was switched off and on again, it issued the same challenge nonce. For certain combinations of a card's ID and nonce, even the scrambling of the reader's nonce remained the same. That suggested that the ID number and nonce, XORed together, fed into the LFSR, marching in from the right like jurors into a box, presumably to scramble things even more.

Oddly, instead of 32-bit IDs and nonces, the reader would also accept ones 48 bits long. That flaw meant that researchers could set all the bits in the LFSR. It also meant that they could feel out the filter function by changing the bits one by one while keeping everything else the same. "Basically, we could choose the input of the filter function and also tell what comes out," says Peter van Rossum, an assistant professor at Radboud. "If you stare at it long enough, you can figure out what [the function] is."

Knowing the filter, the researchers needed only the initial 48-bit setting of the LFSR—the key—to calculating the appropriate key stream. Verdult found that if a card didn't reply to a reader's challenge, then the reader sent a 32-bit "halt" command, but it would scramble it. That was a blunder because hackers could strip out the easily guessed message to get the 32-bit stretch of key stream that scrambles it. The team found a way to snare 32 more bits as well.

In principle, the Radboud hackers were done. If they fed a reader a valid ID and any old nonce, it would reveal 64 bits of key stream. From those bits they could work backward to find the 48-bit key and then generate the entire key stream. In practice, that calculation would take months. Then Ronny Wichers Schreur, a 42-year-old doctoral student at Radboud, noticed that only every other bit of the LFSR feeds into the filter function. That meant the odd and even bits of the key stream could be treated separately, slicing one huge problem into two far smaller ones that could be solved within a second.



Scramble. As bits step through the LFSR, some feed the filter function, which makes the key stream used to scramble messages. A card's ID feeds into the LFSR, but that lets hackers control its bits.

To prove the system had been broken, three members of the team went to London to take a free subway ride. Using de Koning Gans's device, they sensed the ID number of an Oyster Card and fed it into a turnstile to get the card's key. Back in their hotel room, they loaded the key into a reader they'd bought for a few hundred euros and then recharged the card at will. At Radboud, they filmed themselves using a similar approach to clone a passerby's building-access card.

An unscrambled "Halt!" message

Group-leader Jacobs knew that cracking the system was "immediately a matter of national security." On Friday, 7 March, he told university officials, who immediately informed the Dutch government. The next day, two agents from AIVD, the Dutch secret service, showed up. On Sunday, the researchers alerted NXP. They planned to keep quiet until they could publish, giving NXP time to address the problem. But on 12 March, the Netherlands' Minister of the Interior, Guusje ter Horst, announced that the system had been compromised. In a press conference that day, the researchers promised not to divulge the hack's details until autumn.

NXP wanted them hushed for far longer. In June, it sued to stop publication, arguing that it would violate the company's copyrights and damage the company and its clients. The university had to fight back, says Roelof de Wijkerslooth de Weerdesteyn, president of the executive board of Radboud: "It is the responsibility of scientists to go for the truth and to publish the truth."

The Dutch court agreed. On 18 July in the district court of Arnhem, Judge R.J.B. Boonekamp found that NXP couldn't claim copyright to a design it had kept secret and that the company hadn't shown that publication would cause enough damage to warrant limiting the scientists' freedom of expression.

On 6 October, at the European Symposium on Research in Computer Security in Málaga, Spain, Garcia presented the team's work, delivering a paper rich in conceptual detail but short on how-to pointers for hackers. Nevertheless, by month's end, anonymous hackers had posted on the Web a computer program for attacking MIFARE Classic readers.

Bruce Schneier, a security technologist in Minneapolis, Minnesota, says that NXP created its own problems by ignoring a key principle of cryptography: Good systems use designs that are so hard to crack that the details can be made public. "Only very bad systems rely on secrecy," Schneier says. NXP has apparently taken that lesson begrudgingly to heart: While continuing to market the MIFARE Classic, it has introduced a new RFID card system that uses a public design. **–ADRIAN CHO**

CREDIT: TRANSPORT FOR LONDON 2005

Published by AAAS