

NXP Announces New, More Secure Chip for Transport, Access Cards

According to the company, the chip is backward-compatible with the less-secure Mifare Classic chip, recently hacked by two research groups.

By Mary Catherine O'Connor

March 14, 2008—[NXP Semiconductors](#), a Philips spin-off, announced on Monday the completion of a new RFID chip designed for access control and payment applications. The chip, known as Mifare Plus, can support a number of data security protocols, including those employing advanced encryption standard (AES) encryption.

The new chip is backward-compatible with the Mifare Classic chip, introduced in 1994. The Classic chip uses proprietary cryptography that was recently hacked by two separate research teams by reverse-engineering the chip and uncovering the security algorithm it uses. A party who knows the Classic chips' security algorithm could use this information to clone RFID tags containing the chip—a weakness that could be exploited to make fake transit passes or unauthorized copies of key cards, in order to enter buildings. London's transit system uses the Classic Chip in its RFID-based Oyster transit cards (see [RFID Payment Platforms Gaining Momentum](#)), and Boston also sells transit cards carrying the Classic chip for riding its transit system, the T (see [Smart Cards for Smart Commuters](#)).

According to NXP, the Mifare Plus chip's backward-compatibility means issuers of transit cards, key cards and other products that use the Classic chip can introduce similar offerings containing the Mifare Plus chip without having to revoke or reissue cards that carry the Classic chip and are already in users' hands. To read the embedded RFID tags made with the Mifare Plus chip, however, users will need to upgrade their reader software.

An RFID interrogator can employ the AES encryption deployed on the Mifare Plus chip to authenticate that chip before accepting its data and triggering a function, such as opening a locked door or allowing a commuter to pass through a transit turnstile. A number of additional security features, through the support of secure random identifiers, can prevent individuals from being identified and tracked by nefarious parties with RFID readers, NXP reports.

The chip's encryption scheme uses a 128-bit key, whereas the Mifare Classic's security algorithm employs a 48-bit key. The larger an encryption key, the longer it will take hackers to determine the key through reverse engineering.

NXP declines to reveal pricing for the Mifare Plus chip, but a chip's price generally increases in step with its security features, so it will most likely cost more than the Classic chip. NXP says it will continue to manufacture and sell the Mifare Classic chip. Compared with other chips in the Mifare product family, the Classic supports the fewest security features. According to Manuel Albers, NXP's director of regional marketing in the Americas, the Plus is more secure than the Classic but less secure than the Mifare DESfire

chip, which uses a very robust data protection scheme called triple-DES. All chips in the Mifare line are made for passive 13.56 MHz applications, compliant with the ISO 14443 air interface protocol.

Karsten Nohl, a graduate student at the [University of Virginia's](#) Department of Computer Science, was on a team of experts that cracked the Mifare Classic encryption method. Nohl presented the team's findings at a security conference in December, and told in February that he expected NXP would soon announce a new chip with more robust security than the Classic, but less robust than the DESfire chip, thus making it still affordable for NXP customers who currently deploy millions of cards for transit and access applications that utilize the Classic chip.

Nohl and his team initiated the project to test the security used on the Classic chip because the researchers believed the cryptography was weak—but just how weak the cryptography turned out to be a surprise, he said. Nohl added that in reaction to the successful break of the Classic chip's cryptography, a Dutch transit organization has delayed its plans to issue transit cards with the chip as part of a new \$3 billion national transit fare system for its subways and buses.

The second team of researchers to illustrate that the Classic chip can be cloned is from [Radboud University](#) in Nijmegen, the Netherlands. This group released a [video demonstration](#) in which a key card containing a Mifare chip was repeatedly cloned. This video shows an unauthorized party using the cloned chip to grant access to a building. The Associated Press reported that in reaction to the researcher's findings, Guusje ter Horst, the Dutch interior affairs minister, wrote a letter to the country's parliament stating she was preparing supplemental security measures for some government buildings. In addition, according to a [Computerworld news article](#), data-security analyst Ken van Wyk, principal at [KRvW Associates](#), says one European country, which he would not identify, has dispatched security guards to provide supplemental security at some of its government facilities that use access control cards containing the MiFare Classic chip.

NXP issued a statement on March 6 to address initial news reports of the successful hacks. In it, the company said it had begun discussions with the researchers and was working to determine countermeasures that implementers of access or fare systems that use the Classic chip could take to stem the likelihood of abuse of the chip's security. The statement also noted that the Mifare Classic chip is not used in RFID tags incorporated in e-passports or banking cards.

The company made a second statement on March 12, in which it referenced ter Horst's letter and confirmed that in addition to its adoption in transit applications, the Class chip is also used in a "considerable number" of access-control applications. (The Classic chip, ter Horst said, is used in 2 million access passes for Dutch buildings—some of them government offices.)

RELATED ARTICLES On its [Mifare.net Web site](#), NXP posted open letters to both [end users](#) of the chips (such as transit or building security operators) and the [systems integrators](#) who install fare-collection or access-control systems. In the letters, the company called on end users and systems integrators to work together in determining how users might add additional security measures to their back-end systems to thwart attacks.

NXP also noted, in the letters, that it is not in the business of dictating or directing the security measures end users may build around its products: "NXP's expertise is the design and manufacturing of chips," the company indicated. "We do not design end-to-end security systems, as this is typically the responsibility of the system integrator."