guardian.co.uk

Why being open about security makes us all safer in the long run

Bruce Schneier
The Guardian, Thursday August 7 2008

London's Oyster card has been cracked, and the final details will become public in October. NXP Semiconductors, the Philips spin-off that makes the system, lost a court battle to prevent the researchers from publishing. People might be able to use this information to ride for free, but the sky won't be falling. And the publication of this serious vulnerability actually makes us all safer in the long run.

Here's the story. Every Oyster card has a radio-frequency identification chip that communicates with readers mounted on the ticket barrier. That chip, the "Mifare Classic" chip, is used in hundreds of other transport systems as well — Boston, Los Angeles, Brisbane, Oslo, Amsterdam, Taipei, Shanghai, Rio de Janeiro — and as an access pass in thousands of companies, schools, hospitals, and government buildings around Britain and the rest of the world.

The security of Mifare Classic is terrible. This is not an exaggeration; it's kindergarten cryptography. Anyone with any security experience would be embarrassed to put his name to the design. NXP attempted to deal with this embarrassment by keeping the design secret.

The group that broke Mifare Classic is from Radboud University Nijmegen in the Netherlands. They demonstrated the attack by riding the Underground for free, and by breaking into a building. Their two papers (one is already online) will be published at two conferences this autumn.

The second paper is the one that NXP sued over. They called disclosure of the attack "irresponsible," warned that it will cause "immense damages," and claimed that it "will jeopardize the security of assets protected with systems incorporating the Mifare IC." The Dutch court would have none of it: "Damage to NXP is not the result of the publication of the article but of the production and sale of a chip that appears to have shortcomings."

Exactly right. More generally, the notion that secrecy supports security is inherently flawed. Whenever you see an organization claiming that design secrecy is necessary for security — in ID cards, in voting machines, in airport security — it invariably means that its security is lousy and it has no choice but to hide it. Any competent cryptographer would have designed Mifare's security with an open and public design.

Secrecy is fragile. Mifare's security was based on the belief that no one would discover how it worked; that's why NXP had to muzzle the Dutch

researchers. But that's just wrong. Reverse-engineering isn't hard. Other researchers had already exposed Mifare's lousy security. A Chinese company even sells a compatible chip. Is there any doubt that the bad guys already know about this, or will soon enough?

Publication of this attack might be expensive for NXP and its customers, but it's good for security overall. Companies will only design security as good as their customers know to ask for. NXP's security was so bad because customers didn't know how to evaluate security: either they don't know what questions to ask, or didn't know enough to distrust the marketing answers they were given. This court ruling encourages companies to build security properly rather than relying on shoddy design and secrecy, and discourages them from promising security based on their ability to threaten researchers.

It's unclear how this break will affect Transport for London. Cloning takes only a few seconds, and the thief only has to brush up against someone carrying a legitimate Oyster card. But it requires an RFID reader and a small piece of software which, while feasible for a techie, are too complicated for the average fare dodger. The police are likely to quickly arrest anyone who tries to sell cloned cards on any scale. TfL promises to turn off any cloned cards within 24 hours, but that will hurt the innocent victim who had his card cloned more than the thief.

The vulnerability is far more serious to the companies that use Mifare Classic as an access pass. It would be very interesting to know how NXP presented the system's security to them.

And while these attacks only pertain to the Mifare Classic chip, it makes me suspicious of the entire product line. NXP sells a more secure chip and has another on the way, but given the number of basic cryptography mistakes NXP made with Mifare Classic, one has to wonder whether the "more secure" versions will be sufficiently so.

• *Bruce Schneier is a security technologist and author: schneier.com/blog*