Cambridge team exposes EMV card vulnerabilities

September 13 2012, by Nancy Owano

(Phys.org)—At a cryptography gathering in Leuven, Belgium, on Tuesday, Cambridge University researchers made it known that they do not like what they see in chip and pin systems. Banks rely on customer confidence in their word that chip and pin systems are safe, but the researchers tell quite a different story. Part of the problem has to do with the number generators, which the researchers give a failing grade. Each time a customer is involved in a chip and pin transaction, withdrawing cash or buying goods, a unique unpredictable number is created to authenticate the transaction. The unpredictable number, generated by software, is supposed to be chosen at random. But researchers say the number is highly predictable, because dates or timestamps had been used.

Their paper, "Chip and Skim: Cloning EMV Cards with the Pre-play Attack" presents the troubling details of weaknesses in protocol and random number generation which leave customers in the cold as fraud victims. "EMV" is the name given to the system from its original developers Europay, MasterCard and Visa. The system is also known as chip and pin, and is the leading system for card payments, in Europe, much of Asia, and starting to be used in North America.

Payment cards contain a chip so they can execute an authentication protocol. POS terminals or ATMs generate the unpredictable number, for each transaction to ensure it is fresh.

Some EMV implementers have merely used counters, timestamps or home-grown algorithms to supply this number. This exposes them to a pre-play attack, say the Cambridge team. The researchers find it shocking that many ATMs and point-of-sale terminals have "seriously defective" random number generators, often "just counters."

The study authors also point to a key shortcoming at the protocol level where "the party depending upon freshness in the protocol is not the party responsible for generating it." Although the issuing bank is depending on the merchant for transaction freshness, they said, the merchant "may not be incentivised to provide it, may not be able to deliver it correctly due to lack of end-to-end authentication with the issuer, and might even be collusive (directly or indirectly)."

The study team's harshest words are for those banks that "suppress information about known vulnerabilities, with the result that fraud victims continue to be denied refunds." The researchers argue the lack of fairness when any customer who complains of fraud may be told by the bank that since EMVs are secure, the victim is mistaken "or lying when they dispute card transactions." And yet, said the study, "again and again, the banks have turned out to be wrong."

One vulnerability after another has been discovered and exploited by criminals. They said it has mostly been left to independent security researchers to identify what is happening and to spread the word.

The researchers said that, in looking for solutions, it would not be practical to turn to what is a slow and complex negotiation process between merchants, banks and vendors. "It is time for bank regulators to take an interest," they said. "It's welcome that the US Federal Reserve is now paying attention, and time for European regulators to follow suit."

More information:
www.lightbluetouchpaper.org/20 … the-pre-play-attack/
www.cl.cam.ac.uk/~rja14/Papers/unattack.pdf