

Cambridge researchers show Chip and PIN system vulnerable to fraud

February 11 2010



(PhysOrg.com) -- Researchers at the University of Cambridge Computer Laboratory have uncovered flaws in the Chip and PIN system that allow criminals to use stolen credit and debit cards without knowing the correct PIN.

Fraudsters can easily insert a "wedge" between the stolen card and terminal, which tricks the terminal into believing that the PIN was correctly verified. In fact, the fraudster can enter any PIN, and the transaction will be accepted, Steven Murdoch, Saar Drimer, Ross Anderson and Mike Bond have found.

According to Dr Murdoch: "We have tested this attack against cards

issued by most major UK banks. All have been found to be vulnerable."

Victims of this attack may have a difficult time being refunded by their bank. The receipt produced will state "Verified by PIN", and bank records will show that the correct PIN was used. Banks may then argue that the customer must have been negligent and had allowed the criminal to know their PIN.

Dr Drimer says: "The technical sophistication for carrying out this attack is low, and the compact equipment will not be noticed by shop staff. A single criminal can develop and industrialise a kit to be used by others who do not need to understand how the attack works."

The Cambridge attacks - being broadcast on BBC Two's Newsnight - call into question both the design of the Chip and PIN system, and the security of card payments. Victims of fraud are commonly told that bank systems can be relied upon. However, this attack shows that criminals are able to not only defraud customers, but cause bank systems to make the false assertion that the PIN was verified correctly.

Professor Anderson says: "Over the past five years, thousands of cardholders have had stolen chip and PIN cards used by criminals. The banks often tell customers that their PIN was used and so it's their fault. Yet we've shown that it's easy to use a card without knowing the PIN - and the receipt will say the transaction was 'verified by PIN' even though it wasn't."

"This is not just a failure of bank technology. It's a failure of bank regulation. The ombudsman supported the banks and the regulators have refused to do anything. They were just too eager to believe the banks."

The attack - including a demonstration of it being deployed in practice - will be featured BBC Two's Newsnight at 10:30pm on Thursday 11

February 2010.

The Cambridge team's results are also to be presented at the academic conference "IEEE Symposium on Security and Privacy", Oakland, CA, US, in May 2010.

Provided by University of Cambridge

Citation: Cambridge researchers show Chip and PIN system vulnerable to fraud (2010, February 11) retrieved 1 April 2023 from

<https://phys.org/news/2010-02-cambridge-chip-pin-vulnerable-fraud.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.