Not so smart after all

Chips used in the Mondex electronic cash card system can be cracked, a leaked bank report reveals.

By Duncan Campbell

***Guardian*, 24 September 1997**

Technical weaknesses in the Japanese-made chip have privately been known to participants in the Mondex system for more than a year, and can allow secret data on the card to be read. This could give dishonest merchants or users a licence to print electronic money.

“Our assertion is not that the tamper resistance on the cards is perfect because [it’s] not”, says John Beric, security manager of Mondex International. “We try to make them so hard that they are not economically viable to attack.” Current Mondex cards are “fit for purpose”, he adds, even if they are not invulnerable to electronic forgery. The cards, which have been in use for 2 years at a digicash trial in Swindon, can store a cash value up to £500.

Embedded into each card is a Hitachi H8/3101 chip, containing cryptographic programs and keys allowing monetary value to be loaded in and out. But the 3101 chip can be made to hand out its complete programming and secret keys, it appears from a leaked report describing investigations by a Dutch research team. In 1996, the team from the Netherlands Organisation for Applied Scientific Research, TNO, identified “weakness in 3101 chip . . . through technical attacks” such as microprobing. In particular, they made a “successful attack” by activating a test mode in which the chip dumps its contents to a serial port on the chip through which the information can be readily accessed electronically.

From this information, hackers or crooks could derive keys enabling them to transfer forged value into customers' cards. This value could then be spent in the ordinary way. A more sophisticated attack, according to Cambridge University security specialist Ross Anderson, would be to use the secret keys to validate new customer cards loaded with value.

The Dutch group found that, when manufactured, the Mondex chip has a link used for test purposes. If the chip tests OK, the link is burnt out, or fused. But, using microprobe technology, the link can be reconnected. The chip can then be put into a "memory access test mode", and disgorge its contents.

This and other high-tech methods of attacking chips like Mondex were publicly described by TNO researcher Ernst Bovelander at the Eurocrypt 97 conference at Konstanz in Germany, 4 months ago. He said that students at Delft University were now routinely asked to crack smart cards as part of their course work.

Until this month, details about the targets of Bovelander's team were a strictly guarded secret. But a memorandum written in May 1996 by the National Bank of New Zealand (NBNZ) and leaked last month, revealed that TNO had been hired to review the security of Mondex cards. Mondex will not confirm that it hired TNO. Officials of NBNZ then threatened legal action against the Canadian Electronic Frontier Foundation after they put a copy of the memorandum on the Net. The memorandum is now available at another site, http://jya.com/mondex-hack.htm

Mondex insists that simply reconnecting the fused link will not suffice to read out the chip's memory. "I have never seen a report by TNO saying they have broken Mondex", says Beric. "You can't re-enable test mode with that attack. The conclusion is erroneous". The summary in the NBNZ memo was "garbled", he claims. But he does not deny that the contents of the 3101 chip could be read. "It's on the list of vulnerabilities. Test modes are always going to be a vulnerability."

Since it was leaked, the NBNZ memo has been widely circulated among security experts, who believe that Bovelander's recent revelations about smart card security concerned Mondex's 3101 chip. Mondex say that Bovelander was talking about an earlier chip — but that in any case their next generation chip, the H8/3109, will not be vulnerable to such attacks.

The 3109 chip will go into use in a new trial due to start next month in Manhattan. But TNO has already identified how to attack the new 3109 chip. "We're just like cash", says Beric. "Every central bank has to roll over its security technology" as forgers catch up with new banknote systems.

[Duncan Campbell is a freelance writer and broadcaster, and not the Guardian's crime correspondent of the same name]

24 September 1997