

Computer Science Strikes Back Against Fraud
Graham Steel
EPSRC Computer Science Writing Competition 2007

Billed as a major advance in fraud prevention, 'Chip and PIN' ostensibly makes a stolen credit card much harder to use: a thief only has three chances to guess a four digit PIN before the card becomes locked. But in May 2006, Shell ordered its petrol stations across the UK to stop accepting all payments by 'Chip and PIN'. A £1m fraud had been perpetrated against Shell customers who had paid under the scheme. How was this new system broken so quickly?

Details of the fraud are still emerging, but it is known that PIN keypad devices were tampered with in order to capture both customers' magnetic stripe details, and their PINs. A spokesman for the card providers' payments association, APACS, said the fraud had involved a “conspiring” or “coerced” member of staff. Shell have now taken steps to secure their PIN pads. However, attempted fraud by organised, tech-savvy criminals with access to insiders is a growing phenomenon. In March 2005, a gang of fraudsters attempted a high-tech heist at the London branch of the Japanese Sumitomo Bank: members of the gang obtained jobs as cleaners in the building, and used their inside access to tamper with computers in order to learn user names and passwords. The fraud was detected only when the gang attempted to transfer £13.9m to an account in Israel. In this increasingly hostile environment, where the would-be hackers are no longer bored teenagers, but highly organised criminals with insider access, can Computer Science provide a way of fighting back?

At the University of Edinburgh, an EPSRC-funded project aims to explore ways that technologies originally developed to reduce the number of bugs in computer programs can help to improve the design of security critical systems, such as cash machines and payment devices. The focus of the project is on the electronic modules used for securing sensitive data in potentially hostile environments like the cash machine network. Dr Graham Steel, lead researcher on the project, explains:

“These electronic security modules are sealed, tamper-proof boxes, containing a small amount of memory and a chip designed to encrypt and decrypt data. A PIN should never appear in the clear inside a security module. Everywhere else, even inside banks, they are kept secret by encrypting them.”

When you type in your PIN at a cash machine, a security module attached to the keypad immediately encrypts it. Your encrypted PIN is passed around the cash machine network, perhaps being decrypted and re-encrypted several times, each time inside a security module. Eventually, it arrives at your bank, where the PIN you typed is verified against the correct value, again inside a security module. So what can go wrong? Dr Steel again:

“Banks have to secure themselves against insider attacks. That means the security modules have to be designed so that no matter what code might be running on the bank's computers, there's no way that the security module will ever give away a PIN.”

Designing a module that stays secure even when an intruder is sending it commands is not easy, so perhaps it's not surprising that vulnerabilities in these security modules have been found as a result of pain-staking analysis by experts. According to Dr Steel, the aim of the Edinburgh approach is to make this analysis systematic and automated:

“The idea is to model all the operations we expect an intruder to be able to perform, like building up input, calling a command, and breaking down the output, and then to explore all the possible ways this could be done to see if any of them lead to a breach of security. This sounds simple, but the number of possibilities is so large that trying them all out, even with the fastest computer on the planet, is a non-starter. Our research looks at ways mathematical and logical techniques can be used to cut this search space down and make the problem tractable.”

The Edinburgh model even allows the intruder to send incorrect inputs to the security module to see if an error is signalled. Sometimes, that can 'leak' information about the value of a PIN. Dr Steel says his team's research is trying to introduce some science into what had previously been something of a black art:

“Preventing these kinds of attacks is a real concern for the secure hardware industry. We're realistic: our formal analysis alone won't prevent insider fraud, but we're pleased to be making a material contribution to securing critical systems against organised crime.”

--

The project is funded by [EPSRC](#) grant number [GR/S98139/01](#). See <http://dream.inf.ed.ac.uk/projects/aascs/> for more details.