Layer upon layer of security

Turning a point-of-sale terminal into a video game shows that there are many ways for fraudsters to compromise security

BY STEPHEN WILSON

Cambridge University security researchers revealed recently that certain EMV terminals could be tampered with and taken over by determined criminals.

To prove their point they re-configured an EMV POS terminal to play the video game Tetris (see www.cl.cam.ac.uk/research/security/projects/banking/tamper).

The serious side of this work is that a compromised terminal might possibly be used to skim card details, and that it's difficult for cardholders to detect this type of fraud.

As with almost all security matters, we will see that the best response to such threats will be multi-layered. The principle of "defence in depth" carries over into all aspects of smartcard design. In this issue of *Online Banking Review*, we'll look at the multi-layered security of card systems, and see that smartcard platforms offer so many more options for staying ahead in the cybercrime arms race.

To make an EMV terminal play Tetris, the Cambridge team bought a device on eBay, and took it apart in their lab. Importantly, the model was not one approved by the UK banking regulator.

The researchers' website shows that most if not all of the terminal's electronics were replaced by custom-built circuitry, which placed the card reader, the LCD display and the keypad under the control of the attackers. This means that the card reader can record information from the chip and display it on the screen, and that data from the keypad, including PINs, can also be recorded by the attacker.

The implications for smartcards in general and EMV in particular should not be exaggerated.

The whole history of banking security – hundreds of years of it – has been an arms race. We all know that banking systems will continue to be attacked, and all we know there is no such thing as perfect security. The real question is, which technology platforms are likely to equip banks with a stronger, more flexible set of defences and responses to new threats as they arise?

The EMV platform should not be dismissed simply because someone discovered a way to attack a non-standard terminal. Interesting and novel attacks always deserve the attention of security professionals as they can be abstracted to reveal deeper weaknesses. But the Tetris demonstration is not in the "interesting" category. If it has any lessons at all, it merely underscores the necessity for the sorts of terminal security already widespread in Australia.

We almost take tamper resistance for granted in this country, thanks to Australian Standard AS 2805 which led the way internationally in terminal security. All EFTPOS terminals need to have their mechanical designs certified, in respect of being tamper resistant and tamper evident.

> **We should remember what makes smartcards smart ... a smartcard can tell what's going on around it**

It's worth remembering that the terminal re-programmed to play Tetris was not one approved by the banks.

To mount a successful attack on an EFTPOS terminal requires access to the environment in which it is located, and possibly the ongoing collusion of the merchant. If a terminal has been modified to simply intercept PIN numbers from the keyboard, and doesn't function as an EFTPOS device anymore, then it will soon be spotted by customers who would raise the alarm. Remember that modifying ATMs and POS terminals to simply skim magnetic strips as the cards slide by is much simpler, and can be done unobtrusively, without much alteration to the appearance of the hardware.

While the Cambridge researchers claimed a compromised terminal could steal account details, the access controls of the Card Operating System place strict limits on the types of data available to unauthorised readers and applications. Critical data is usually only accessible once a PIN has been presented to the chip and verified. While an altered EFTPOS terminal might pass through the PIN, most sophisticated smartcards will only communicate with mutually authenticated readers, regardless of the PIN.

Mutual authentication between smartcard and reader is becoming increasingly familiar to ordinary consumers through the mobile phone function of SIM Lock, which restricts how a SIM can be moved between handsets. That is, a SIM and a handset can reach agreement on whether or not they are compatible with one another. The usefulness of this extra layer of security in banking will be readily appreciated by most customers (and will become a must-have in Internet banking, to combat phishing and pharming).

At the deepest levels of access control there lies certain control data which is never released from the chip, but without which the smartcard cannot function. These include cardholder private keys which typically are generated inside the chip. The uniqueness and copy-protection of these keys makes it essentially impossible to clone or counterfeit smartcards. This functionality limits the damage that can be done, in the event of a single smartcard being compromised, to abuse of the one cardholder's account.

As smartcards grow in popularity, we will see more and more reports of security breaches. The arms race will continue as it always has.

To make sense of the deeper issues, and to make robust security decisions that will carry us through frequent scares, we should remember what makes smartcards smart. It's simply this: unlike magnetic stripe cards or the vast majority of personal security devices today, a smartcard can tell what's going on around it, and can thereby combat a whole range of attacks today and into the future.

Stephen Wilson is a leading international authority on identity management and information security. In early 2004, Stephen established Lockstep Consulting to provide independent security advice and to develop new smartcard solutions to identity theft.

swilson@lockstep.com.au