TAMPER-PROOFING COMPUTER CHIPS

Philip Paul, a beneficiary of the Academy's Engineering Leadership Award, used his grant to gain a valuable summer-long internship at IBM Research in Zurich. His subsequent PhD work has resulted in two patent applications that will help protect encryption systems for printer cartridges. He writes about what his research has discovered about the ways that hackers penetrate card security systems and how to protect against these threats.

After my third year of engineering undergraduate studies at Cambridge I spent a whole summer as an intern at IBM Research in Switzerland in 2004, working on a project with the help of my Engineering Leadership Award from the Academy. It was here that I discovered how much I enjoy research as part of a product development process.

Afterwards I chose a PhD project sponsored by Seiko Epson which focuses on developing new techniques for increasing the security of microelectronic security devices – the sort of devices embedded within the every-day chip-and-pin bank cards or payment cards for transport networks most of us carry.

I guess I could have been a hacker rather than a defender. But an attacker has only to find one glitch in the system whereas a defender has to protect against a multitude of attacks. While hackers, of course, contribute by finding weaknesses, at some point someone needs to address them and close the security loopholes. So I found it more interesting and challenging to construct a defence against tampering with computer chips.

ON THE SURFACE

Identification and security systems have come a long way since the days when credit cards were embossed and copied onto a transaction slip by a mechanical reader. Similarly, magnetic strips are nothing new; they are merely a fancier and machine-readable way to write details onto a card, much like pen and paper. They offer no protection from copying as the entire data stored on such cards can be easily read and transferred to a blank card.

Today microchips have become cheap to the point of being disposable so the natural next step for such systems is to incorporate a microchip as the means of identification. This means cards can contain authentication data, but do not actually need to reveal all or any of it to third parties while using the device. This is achieved by implementing sophisticated authentication protocols in the chip itself.

FALSE CONFIDENCE

This comparative security of microchips means we place more trust in such devices – and the more we trust them, the more attractive a target they become for criminals. The balance on early phone cards for example was updated by raising the supply voltage for the card, which could be filtered out in a very simple way. This prevents the credit balance being updated, hence phone calls could be made for free.

ENGINEERING LEADERSHIP ADVANCED AWARDS

This scheme is open to second year MEng undergraduates, all of whom are in the top 20% in their universities. Participants on the scheme have clear leadership potential and are provided with the funding and opportunities to undertake an accelerated personal development programme. Each year around 30 Engineering Leadership Advanced Awards are made to students. Each will benefit from a mentor – who will be a Sainsbury Management fellow – and training and networking event organised by The Royal Academy of Engineering. They will receive funds of £5,000 each to be used over the next three years to improve foreign language skills, attend work placements (especially overseas), visit conferences in the UK and abroad, conduct studies of engineering in specific sectors, and prepare for fast-track careers in UK industry.

A more recent example of flawed security devices is the Mifare chip card, widely used as access and payment cards in public transport networks. Researchers discovered the cipher used in the card is weak, thus allowing the secret key to be extracted from Mifare cards.

So how do criminals attack security devices – and what can we do to prevent their efforts from succeeding?

MICROCHIP WEAKNESSES

All security devices have one thing in common: they perform a cryptographic operation, such as a signature, protected by a secret key. An attacker has to find the secret key stored on the security device. While plenty of secure ciphers and protocols have been designed to prevent this, their implementation on a microchip might actually allow an attacker to extract the key without having to break the cipher.

A protection grid on a ST microelectronics smart card. The grid is implemented in the topmost metal layer of the grid itself, and covered by the chip passivation (typically silicon nitride and silicon oxide, which are robust to chemicals. Silicon oxide is essentially glass)

The attacker can do this in two ways. First is the non-invasive type of attack, in which the security device is closely monitored during normal operation. The timings of cryptographic operations, levels of power consumption and electro-magnetic emissions may be monitored and analysed to reveal hidden information. Or the inputs to the security device may be manipulated deliberately to cause it to malfunction and leak its secrets.

In spite of major efforts by research groups around the world, it has proved impossible so far to completely eliminate the data dependency of the power consumption traces. Until that is achieved, non-invasive attacks will remain a problem.

INVASIVE ATTACKS

The second method of attack is more threatening; invasive attacks. This is the danger on which my recent work has focused and for which I developed patents for Epson.

Invasive attacks all begin by removing the packaging of the security device. Some attacks then aim to analyse the microchip circuitry without running the chip. Most attacks attempt to read out signals from the chip while it is operating. By removing the packaging and making holes in the passivation of a chip, the criminal can directly probe data wires and read data being transferred between different parts of the chip.

A laser beam can be aimed at individual transistors – for example in the memory of the chip – which can induce faults in the running chip and reveal secret data by analysing the failed computation.

DETECTING BREAK-INS

Surprisingly little work has been published that shows how to defend against these attacks. My PhD research has focused on this defence and I maintain that an effective tamper protection grid should allow a security device to detect the removal of its packaging and warn the chip of an attack.

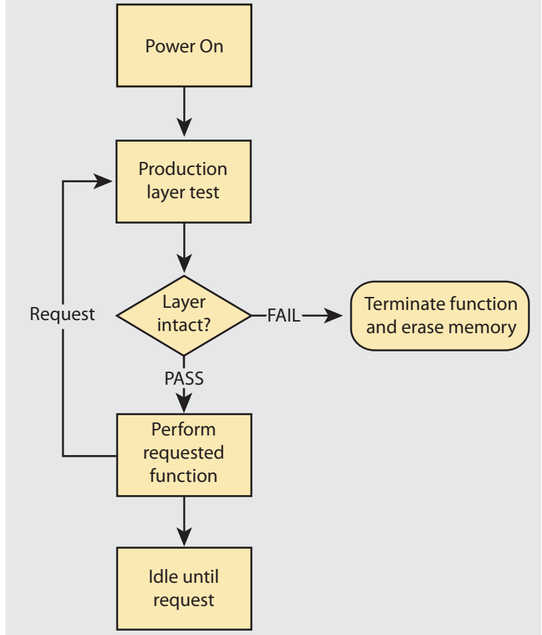
That way, a security device that has been tampered with will refuse to undertake sensitive operations and so no keys can be extracted from the running device.

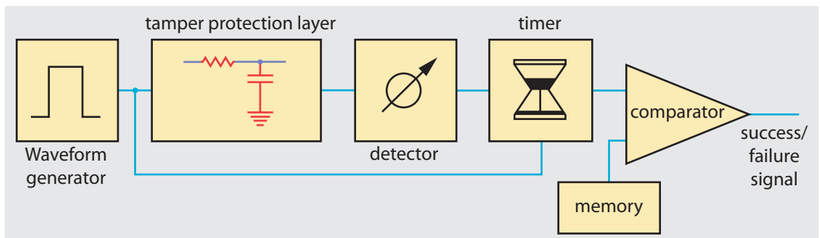
My research has revealed that a suitable technology for tamper protection grids is the use of organic electronics, polymer electronic materials that are very cheap to fabricate because they can be solution-processed and simply printed in the appropriate pattern.

SLOW IS NOT A PROBLEM

Organic electronics are becoming stable enough for commercial operation. However, they are currently quite slow compared with silicon. These properties actually make them ideal for protection grids. High device performance is not a requirement if the protection grid is only monitored for consistent characteristics. Its comparative vulnerability allows rapid detection of damage to the packaging, while the low cost of fabrication has a minimal effect on the cost of the device.

In its simplest form, such protection could comprise a network of printed conductor lines, which is the subject of the first patent application. The conductors can easily be printed between standard contact pads of the chip. Using inkjet technology, it is relatively simple to change the pattern from device to





RC-delay-diagram: a flow chart for a simple delay line-style protection scheme. On the left is a pulse generator (which is part of the smart card), which sends a pulse to the protection grid (the second box from the left) and the timer (for reference). The detector (third from left) is part of the chip again, and detects the pulse reaching the other end of the grid. The timer measures how long the pulse took to reach the other end, the value of which is compared to the reference value.

device, creating a characteristic and unique fingerprint for each device. In turn, the time delay along the protection grid line or its resistance value can be measured by the chip and compared to a reference value, as shown in the flow chart. Or one could derive the cryptographic key from the protection grid characteristics so that each device has an individual key that is automatically destroyed when the packaging is removed.

A stable organic conductor suitable for inkjet printing is already widely used and readily available. It serves as an anti-static coating in films and also more recently in organic LEDs. Experimental evaluation of these simple devices has so far shown promising results. The devices are easily altered or broken when subjected to chemicals used for depackaging, such as acids. At the same time the material is stable in an ambient environment.

Attempts to depackage mechanically can be detected by creating a package similar to a seal sticker. If the grid is printed on a brittle layer sandwiched between softer epoxy layers, any strong force applied to the chip will lead to the brittle layer cracking and breaking the protection grid, safeguarding the device. Further, if the criminal tries to pick off the resin coating around the chip, the grid that sits within the plastic is physically broken, rendering the device secure.

Organic protection layers are not just limited to simple resistor lines. As laid out in my second patent application, a more advanced approach is to implement transistor circuits, which offer a much greater range of possibilities. Currently, organic transistors are quite large compared with their silicon counterparts and their performance is still relatively low, which limits the complexity of circuits. For monitoring purposes, however, a bridge-like configuration or a simple ring-oscillator circuit should suffice, as these circuits can be used to compare transistor characteristics sensitively. In the longer term, as organic transistor technology develops, it will be possible to implement more complex circuits such as memories, or logic circuits.

An example of the proposed protection grid printed on a glass slide with an inkjet printer for testing. The final devices will be printed on top of the secured microchip. The pattern itself is flexible, and not limited to the meander shown here. Using inkjet technology, the pattern may even be varied from device to device

THE NEXT STEPS

My research has shown how the concept of organic electronic materials as protection grids is superior to current metal protection grids, as attacks can be detected instead of simply relying on the grid as a physical barrier. As my scheme is quite similar to ones already implemented on commercial chips, I believe the scheme will also conquer one of the toughest of challenges – cost.

The crucial element, however, is always to approach device security in a holistic way because flaws in other parts of the overall system might be enough to compromise the device's encryption key. Hackers always consider it a challenge when one particular line of defence has been created. It's rather like a security arms race. A protection scheme that may be secure now might be proven vulnerable in the future and must be constantly developed.

So in the future we will certainly have more challenges to face, but eventually security devices will have fewer and fewer flaws. If the items they are protecting are not of great value then the protection grids will prove much too time consuming for criminals to attack and crack.

RESEARCHERS CLONE TRANSPORT CARDS

The worldwide problem of keeping one step ahead of criminal hackers in the war against theft through security devices is highlighted by claims that millions of 'Mifare' cards used in various access systems and transport networks could be susceptible to cloning. The *Metro* newspaper reported that researchers at Radboud University in the Netherlands had recently found a way to hack past the security systems protecting the microchip at the heart of the card, which is widely used in several countries.

Researchers copied the encryption key from smart-card readers and created clone cards. They then told the Dutch government and chip manufacturer NXP about their work, to give them time to harden the systems against attack. Efforts by the manufacturer to gain an injunction to prevent the research group from publishing their findings failed in court, the judge quoting the declaration of human rights and freedom of speech as reasons for rejecting the case.

When it comes to security systems Philip Paul feels that flaws should be fixed, not hushed up.

BIOGRAPHY – Philip Paul

Philip Paul grew up close to Frankfurt, Germany. He was a self-employed IT consultant before leaving Germany to read engineering at Cambridge University, where he stayed to carry out research towards a PhD. On finishing his doctorate he will be looking for research work in industry.