# What the silicon manufacturer has put together let no man put asunder


But of course the argument probably goes the other way; if man can put it together then man can take it apart. This has been an argument in the security of the smart card chip world for as long as I can remember with just as many people saying ah yes but it's not really practical. Now we have an account with video by Christopher Tarnovsky of Flylogic Engineering LLC taking apart an Infineon SLE66 at the Black Hat 2010 conference in Washington DC in February.

This is one of the core chips used in the GSM and EMV worlds. So do we need to be worried, is the marriage (of smart card chip and security) over?

As one that has been actively involved in the security of smart card chips for the last 20 years or more I feel adequately qualified to opine in this area and more to the point I can boast of being trained in both the techniques of micro probing chips (thank you TNO/EIB now Brightsight) and of microsurgery (thank you John Walker) with an FIB (Focussed Ion Beam) machine. I should hasten to add that I wouldn't have passed an examination in either technique but at least I can appreciate the practical problems.

So who is Christopher Tarnovsky and what has he managed to do? Well first of all we should realise that Christopher is a professional integrated circuit reverse engineering specialist. He worked for NDS (providers of the SKY satellite TV conditional access system) from 1997 until 2007 engaged as he puts it on reverse engineering of many smart card chips including the Infineon SLE66. Since that time he has been the key engineer behind Flylogic Engineering which according to their web site is a professional chip evaluation/reverse engineering house. I understand they have their own FIB machine which at $1 million per pop is not the normal back bedroom toolkit. So let there be no doubt that Christopher is a highly skilled chip reverse engineer with access to the best equipment.

The target for Tarnovsky's attack was the SLE66 family of secure microprocessors from Infineon. This is a 10 year old design (maybe more) but is none the less the mainstay of the Infineon product line for smart cards and similar products including TPM (Trusted Platform Module) chips as used in the Xbox360 for example. For the avoidance of doubt the SLE66 would be considered a secure microprocessor chip and has been evaluated under Common Criteria to EAL 5+.

What Tarnovsky has managed to do and demonstrate is that over a six month period he has painstakingly analysed the chip and using a FIB machine has managed to bypass the shield protecting the core logic and probe the data bus of the CPU at a point at which it is not enciphered. Although he only probed one data line at a time he managed to disable the dummy cycle generator that would throw the synchronisation necessary to recover the complete 8 bit data bus (effectively you need to repeat a fixed cycle probing one data line at a time, the insertion of random dummy CPU cycles would break the necessary synchronisation). Of course it wasn't really six months because Tarnovsky was working on this chip before his last Black Hat presentation in 2008. In his work he also claims the cost of this attack to be about $200,000 on a commercial basis (just for me – who is paying this bill, I know it's not Infineon?).

Now here is the real story, what Tarnovsky has done is a fantastic achievement in reverse engineering of a security microprocessor. Nobody would have said it impossible but most (me included) would have argued that nobody with the necessary skills and resources is likely to sit down and do this. I confess to being quite surprised because

the real cost in terms of skilled people and equipment is really much higher than the claimed $200K. Again I can speak from experience because in the 90's I set up a laboratory to do just these sorts of exercises and we couldn't afford to have our own FIB machine.

So now to the interesting bit, how worried should we be? By Tarnovsky's own admission the SLE66 was a difficult chip to beat and as he pointed out the active shield required extensive analysis and testing to circumvent. The flaw in the design of the chip in his view was the availability of the unencrypted data bus in the CPU which Infineon have already corrected in their newer chip the SLE78.

Will we see lots of hackers decoding the SLE66? No, it really is beyond the scope of anything but a commercial (government) reverse engineering laboratory. In my view it is beyond the scope of even a well resourced university department, this chip is a different ball game to the NXP Mifare chip which has been successfully hacked over the last few years.

So how about all those EMV cards out there or the GSM SIM cards, should the Financial Institutions (FIs) or the Mobile Network Operators (MNOs) be concerned? Frankly no, they all operate with unique chip keys and in both cases individual cards can easily be identified and processed accordingly. How about cards with global keys? Well that would be a concern but does anybody still do that? Then there are those TPM chips as used perhaps in the electronic games market, Mmmm now here is a target like PayTV that hackers feel is open house, there is also a history of commercial resources being brought into play. I think I would be (already) using a newer chip here but also notice that these guys usually build a lot more into their systems than can be destroyed by the vulnerability of a single chip.

Then last of all (for the moment) how do we look on the Common Criteria process? Should the SLE66 have an EAL5+ rating? Does it need to be re-rated? This is more difficult to answer but let us not forget that a CC rating is a measure of how well a Target of Evaluation (TOE) meets its specification, it's like a security quality measure not necessarily a statement of how secure a device actually is, although the chip's resistance to attack is part of that measure. Of course you wouldn't normally evaluate a low security functionality device to a high CC level but conceptually you could. So has the reverse engineering exercise by Christopher Tarnovsky changed the perception of how difficult the work function really is? Well it has moved my goal post but just a bit and I shall happily carry on using EMV cards and my mobile phone with little fear of being compromised because of chip hacking.

And just as an afterthought lots of FIs and MNOs use chips far less secure than the SLE66. In America they are still using magnetic stripes for financial payment cards.

Dr. David Everett - March 2010