Smart Card Tutorial

First Published in June 1998

Smart Cards and Information Leakage

The media has been full of discussions on Differential Power Analysis (DPA) this month for which claims have varied from it doesn't matter through to predictions of the end for Smart Cards. The truth, of course, always lies somewhere in between these extreme views and so this month we will explore the subject and attempt to balance these views.

The story starts with TEMPEST (Transient Electromagnetic Pulse Emanation Standard) a U.S government code word that defines a classified set of standards for limiting electric or electromagnetic radiation emanations from electronic equipment. Microprocessors, computers, VDU's in fact all electronic devices emanate radiation through the ether or through electrical conductors. In the early 50's the U.S government became concerned that such radiation patterns may be collected and analysed by an enemy. The use of cryptography could effectively be thwarted if the appropriate information could be successfully reconstructed. Research in the laboratory showed that such signals could be collected at some considerable distance from the source of the emanations and accordingly the Tempest program was started.

Although the subject of Tempest was well known in the defence world it entered the wider public domain with the publication of a land mark paper in 1985 entitled "Electronic Radiation from Video Display Units: An eavesdropping Risk" by Win van Eck of the Netherland's PTT Research Laboratories. His paper showed the successful reconstruction of the image displayed on the target VDU captured at some distance away, even outside the building. It is the use of square wave signals and high switching frequencies in digital equipment that leads to the radiation of electromagnetic fields with frequency components extending into hundreds of megahertz. It is important to note here that although the spectral power of these signals decreases with increasing frequency, that the radiation effectiveness increases with increasing frequency.

The solution to this problem is equally well known and relates to the screening of the equipment by creating an effective Faraday Cage and the filtering of the signal and power cables to reduce their radiating capability. The levels required for such screening and filtering are part of the classified Tempest standard. In this particular case the designer of equipment receives expert advice on the level of protection required. The designer of cryptographic equipment needs similar advice from experts on the appropriate algorithms and the necessary key lengths.

In the world of cryptographic security another seminal paper was published in 1996 by Paul Kocher entitled "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and other Systems". In this paper he was able to show that by measuring the amount of time required to perform private key operations, that attackers could, in principle, find the key exponents and thereby potentially break the cryptographic system. Although such attacks are in practice somewhat difficult and adequate defences fairly straightforward, the issues raised have none the less much wider implications.

Two years ago Dan Boneh and colleagues from Bellcore highlighted the vulnerability of Smart Card cryptographic implementations to Differential Fault Analysis (DFA). They showed in their paper ("On the Importance of Checking Calculations") how you could take advantage of induced random hardware faults. In particular they showed how you could theoretically break the Chinese Reminder Theorem by such techniques. Again the ideas were not new and in practice are not only difficult to create but are also relatively easy to protect against.

The main point about all these attacks is that the principles are well known. The difficulty for the designer is to ensure that adequate controls are applied to the particular implementation, to ensure that his system is not vulnerable to a low work function attack. Protection controls by their very nature are an overhead and perfect security can never be achieved. Security is an all pervasive subject

where one is not only concerned about the strengths of the front door but also whether there is an unattended back door, and in particular, has some new tool been invented that can effortlessly bore a hole in the door.

And now we come to the new paper “Introduction to Differential Power Analysis and Related Attacks” by Paul Kocher, Joshua Jaffe and Benjamin Jun from the U.S consultancy company Cryptography Research. This paper describes a class of attacks against Smart Cards and secure cryptographic tokens based on the analysis of the device’s power signal. This involves the use of advanced statistical techniques to reconstruct the processor tasks thereby determining the secret information such as cryptographic keys and PINs stored in the card.

As we have already discussed, the concept of information leakage is not new, it is the success that Paul Kocher and his colleagues have demonstrated in applying their new tools to break existing Smart Card implementation that has raised concern.

The monitoring of power consumption to identify cryptographic operation in Smart Cards was first reported by Ernst Bovenlander of TNO at the 1997 Eurocrypt Conference, where he was able to identify the regular structure of the DES cryptographic algorithm. The work of Kocher, Jaffe and Jun takes this much further by being able to determine the actual keys used in the cryptographic algorithms. They show that the operation of the transistors within the Smart Card chip produces observable electronic behaviour. Because the operation of the logic is regularly being synchronised to a deterministic clock pattern, it is possible to identify macro characteristics of the microprocessor operation just by simple monitoring of the power consumption.

So just how practical are these attacks? In their paper Kocher et al first define the concept of simple power analysis (SPA). Here they discuss the monitoring of the power signal using, say an oscilloscope, where they point out that it may be possible, for instance, to visually observe the difference between the squaring and multiply operations commonly used in the implementation of the RSA (or other public key) algorithm. As they point out it is not particularly difficult to protect against this type of attack.

The thrust of their paper is aimed at Differential Power Analysis (DPA) where they use statistical analysis and error correction techniques to extract information correlated to secret keys. The attack requires two phases, the collection of power signal data followed by the data analysis.

In their paper they give an example of a DPA attack on the DES algorithm. As they point out such techniques require a detailed knowledge of the target algorithm and its likely implementation. In the example quoted 1000 samples of the DES operation are stored for analysis where each sample consists of 100,000 data points. The attacker is also assumed to have the relevant 1000 ciphertexts.

A third analysis tool is described as High-Order Differential Power Analysis (HO-DPA). This is described as an extension of the DPA technique where sample data is collected from multiple cryptographic suboperations. Here it may be data from multiple sources (e.g. different Smart Cards doing the same operation), correlated signals stored using different measurement techniques (e.g. power signal and EMR signal) or signals with different temporal offsets. Clearly such analysis requires an even deeper understanding of the underlying mechanisms. As the authors point out they are not aware of any actual systems that are vulnerable to HO-DPA that are not also vulnerable to DPA.

Cryptography Research is currently licensing their technology to implementers that is resistant to these attacks. Whilst it is possible to modify the hardware of the processor to help mask these unwanted signals it is clear that the actual implementation of the cryptographic algorithms is fundamental to an adequate protection profile. The authors of the paper should be complimented for the success of their research and for bringing it into the public domain because it helps focus the designers of such systems to ensure that adequate protection mechanisms are employed. As history shows the battle will continue but there seems every reason to believe that the seesaw is tipped to the advantage of the designer. New attack methods will always appear but good security designs continuously employ change to ensure that the economics of an

attack remain with the defenders. Well implemented Smart Card devices present a formidable tamper resistant barrier, with what should we compare them ?

David B Everett

■ According to a Visa spokesperson, chip technology is the most secure technology available today. HO-DPA was discovered by Visa during due diligence which was being carried out by a third party security laboratory under contract to Visa. There is no economic case for breaking chip technology, no chip is 100% secure but Visa intends to stay several steps ahead of the attackers.

Visa believes the problem to be a security systems issue. Visa has 9 million chip cards in the market place and there has not been a case of any cards being compromised. Visa cash is fully accountable and has an audit trail.