How to Explain Side-channel Leakage to Your Kids?

[Published in Ç.K. Koç and C. Paar, Eds., *Cryptographic Hardware and Embedded Systems – CHES 2000*, vol. 1965 of *Lecture Notes in Computer Science*, pp. 229–230, Springer-Verlag, 2000.]

David Naccache and Michael Tunstall

[1] Gemplus Card International
34 rue Guynemer, Issy-les-Moulineaux, F-92447, France
david.naccache@gemplus.com
[2] Gemplus Card International, Card Security Group
B.P. 100, Gémenos, F-13881, France
michael.tunstall@gemplus.com

Abstract. This paper will attempt to explain some of the side-channel attack techniques in a fashion that is easily comprehensible by the layman.
What follows is a presentation of three different attacks (power, timing and fault attacks) that can be carried out on cryptographic devices such as smart-cards.
For each of the three attacks covered, a puzzle and it's solution will be given, which will act as an analogy to the attack.
How these attacks can be applied to real devices will also be discussed.

1 Timing Attacks

When an algorithm is executed on a device it will take a certain amount of time to complete. In some instances the amount of time the algorithm takes to execute will vary depending on the secret information that is normally not available to an external observer. An animated PowerPoint slide-show (game) and it's winning strategy give an example of how this technique can be used.

The story was originally told by Eli Biham at the dinner that followed the Ph.D. defenses of Helena Handschuh and Pascal Paillier.

2 Power attacks

A cryptographic device will consume a varying amount of current as it executes an algorithm. By making observations one can attempt to deduce information about what is occuring.

The following is a situation where this technique can be applied: A paparazzi is investigating the lives of a Royal couple. He follows then to a restaurant and

then to their home. He is under the impression that they have had an argument, but as the two are public figures they will not permit themselves to argue in public.

To simplify the situation we will make the assumption that their home (castle?) consists of two rooms each with one lightbulb and no other electronic equipment. There are not any windows or convenient keyholes either and the reporter wishes to find out whether or not the two are still talking to each other.

As suggested at the beginning of this section the solution revolves around the amount of current consumed by the two lightbulbs. The reporter needs to find access to the electricity meter (which in our scenario is outside the Royal property). By looking at the speed that the disk inside the meter is rotating the reporter is able to determine whether one or two lights are turned on.

3 Fault Generation

Finally, as an algorithm is being executed by a device it is possible to physically attack the device to change the output of the algorithm, a potentially strong attack against cryptographic devices. It is also possible to attack the device in a manner that will change its behavior, creating other opportunities to attack the device. This as well will be illustrated using an animated PowerPoint slide-show.