When Should a Side-Channel Attack or a Fault Attack be Considered as Successful?

Werner Schindler

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Federal Office for Information Security
Godesberger Allee 185–189
53175 Bonn, Germany
Werner.Schindler@bsi.bund.de

Security implementations shall be immune against side-channel attacks and fault attacks. In scientific papers the secret key is usually discovered completely, possibly after a (feasible) brute force search. There remains no doubt whether the attack is successful or not.

In real-world security evaluations the situation may be different: The evaluator might gain partial information on the targeted key (e.g. the Hamming weight of some key bytes) by a side-channel attack or a by fault attack. The fundamental question is whether this information is essentially useless or can be exploited efficiently. The evaluator finally has to decide whether the target of evaluation may yet be viewed as secure or whether it should be counted as broken.

The talk sketches three well-known examples where partial key information was successfully be exploited by non-obvious methods [1–3]. Moreover, general aspects of this topic are addressed.

References

1. D. Naccache, P.Q. Nguyen, M. Tunstall, C. Whelan: Experimenting with Faults, Lattices and the DSA. In: S. Vaudenay (ed.): Public Key Cryptography — PKC 2005, Springer, Lecture Notes in Computer Science 3386, Berlin 2005, 16–28.
2. W. Schindler, K. Itoh: Exponent Blinding Does not Automatically Lift (Partial) SPA Resistance to Higher-Level Security. In: J. Lopez, G. Tsudik (eds.): Applied Cryptography and Network Security — ACNS 2011, Springer, Lecture Notes in Computer Science 6715, Berlin 2011, 73–90.
3. X. Zhao, F. Zhang, S. Guo, T. Wang, Z. Shi, H. Liu, K. Ji: MDASCA: An Enhanced Algebraic Side-Channel Attack for Error Tolerance and New Leakage Model Exploitation. In: W. Schindler, S. Huss (eds.): Constructive Side-Channel Analysis and Secure Design — COSADE 2012, Springer, Lecture Notes in Computer Science 7275, Berlin 2012, 231–248.