Federal Office
for Information Security

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

Werner Schindler

Federal Office for Information Security (BSI),
Bonn, Germany

Fréjus, June 25, 2013

Outline

- Introduction and motivation
- Example 1: DSA: Fault attack on the generation of the ephemeral key
- Example 2: RSA: Power attack on RSA with exponent blinding
- Example 3: AES: Algebraic side-channel analysis
- Conclusion

Implementation attacks in literature

- In scientific papers side-channel attacks and fault attacks are usually either successful (maybe a feasible exhaustive search is necessary) or unsuccessful (due to effective countermeasures).
- Anyway, the success or the failure of the attack is obvious and need not be discussed.

Implementation attacks in security evaluations (I)

- In real-life security evaluations the situation may be quite different.
- An implementation attack may provide partial information. But: Does this information suffice for a successful attack?
- For instance:
  - AES: Hamming weights of some key bytes (reduces exhaustive search)
  - RSA: Hamming weight of some key bytes (exhaustive search is infeasible anyway; can the algebraic structure of RSA be exploited?)

Implementation attacks in security evaluations (II)

- Anyway, the evaluator of a security implementation has to decide whether he views an implementation as vulnerable or yet as secure.
- So far this topic has not considered in the scientific literature in a systematic way.
- In the following we present three well-known examples of successful attacks for which the exploitation of the gained information is not obvious.

Example 1: Fault Attack on DSA

- Fault attack on the generation of the ephemeral key in DSA
- Note: Each DSA signature (r,s) requires a 160 bit (= 20 byte) ephemeral key k.
- Reference [1]

Example 1 (II)

Scenario:

- For each signature (r_i,s_i) a procedure generates 20 random bytes (= ephemeral key k_i).
- The attacker tries to terminate this procedure by a power glitch before the last random byte has been generated.
- The attacker decides on basis of an SPA whether the fault injection has been successful (← shorter execution time).
- If less than 20 random bytes have been generated the least significant byte of the ephemeral key k equals zero.

Example 1 (III)

- Situation:

  The attacker has successfully disturbed the generation of N ephemeral keys.

  He knows N modular equations

  $k_i s_i \equiv h(m_i) + r_i x \pmod{q}$ for $i=1,\ldots,N$

  known: $r_i, s_i, h(m_i)$ unknown: x, k_i

Additionally, the attacker knows that the 8 least significant bits of each k_i are 0.

Example 1 (IV)

- Question: How should this situation be assessed?
- One might argue that each ephemeral key k_i still has 152 bits of entropy so that the attacker's knowledge is meaningless.
- One the other hand: The ephemeral keys $k_1,\ldots,k_N$ are related by an under-determined system of linear equations. In an information theoretical sense this information is clearly sufficient.
- Is it feasible to calculate the long-term key x?

Example 1 (V)

- The answer is yes!
- The knowledge of the least significant byte of all k_i allows to transform the search for x into a closest vector problem.
- The closest vector problem can be solved with less than 30 disturbed signatures [1].

- Note: This technique (reformulation as a closest vector problem) had already been developed for other cryptographic problems.

Example 2: Power Attack on RSA

Scenario:

- RSA with CRT, s&aM, exponent blinding
- The evaluator
  - applies SPAs or template attacks with sample size 1 to the particular power traces
  - is able to guess the exponent bits with error probability ε
- SPA or template attacks are not successful (too many false exponent bits)

Example 2 (II)

- Numerical example:
  - k - bit primes (here: k = 1024)
  - (unknown) R-bit blinding factors r_j (exponent blinding), here: R = 16
  - here: $\varepsilon = 0.10$
  - $\rightarrow$ 104 false bit guesses per power trace in average
- Possible (but wrong) conclusion:
  This obvious weakness of the implementation cannot be exploited.

Example 2 (III)

- **But:** The information from the particular power traces can be combined.
- Reference [2]

Example 2: Basic attack (I)

- Basic attack:
  - power trace j ($1 \leq j \leq N$): exponent: $v_j = d_p + r_j * \varphi(p)$
  - attacker guesses: $v_{j(g)} = v_j \oplus e_j$ (error vector)
  - consider $v_{i(g)} \oplus v_{j(g)}$ for $1 \leq i < j \leq N$
  - Two cases are possible:

    a) $r_i = r_j \rightarrow \text{ham}(v_{i(g)} \oplus v_{j(g)}) = \text{ham}(e_j \oplus e_i)$

    $E(\text{ham}(v_{i(g)} \oplus v_{j(g)})) \leq 2*1040*\varepsilon = 208$

    b) $r_i \neq r_j \rightarrow E(\text{ham}(v_{i(g)} \oplus v_{j(g)})) \approx 0.5* 1040 = 520$
  - $\rightarrow$ distinguisher whether the blinding factors r_i and r_j are identical or not

Example 2: Basic attack (II)

- Basic attack:
  - Divide the guessed exponents into classes with identical (but unknown) blinding factors
  - Bitwise majority decision between the guessed exponents in the blinding class, which at first contains t elements (‘t-birthday’, here: $t = 7$)
  - Exhaustive search for the remaining errors
    $\rightarrow d_p + s*\varphi(p)$ for some $s \rightarrow p,q$
  - For 1024 bit primes with small blinding factors the basic attack may tolerate error rates up to ≈ 25 %

Example 2: Basic attack (III)

- Bottleneck:
  - no. of traces (to find a t-birthday)
  - no. of computations (mutual comparisons)

  unless R is rather small
- Large R makes the basic attack infeasible.
- Just limiting the number of operations with the secret key d (clearly) below $2^{R/2}$ prevents the basic attack but ...

Example 2: Enhanced attack (I)

- Consider u-sums $S(i_1,..,i_u) := v_{i\_1(g)} + \ldots + v_{i\_u(g)}$ for u = 2, 3 or 4
- If $r_{i\_1} + \ldots + r_{i\_u} = r_{j\_1} + \ldots + r_{j\_u}$ then $ham(NAF(S(i_1,..,i_u) - S(j_1,..,j_u))) =$
  $ham(NAF(e_{i\_1} + \ldots + e_{i\_u} - e_{j\_1} - \ldots - e_{j\_u}))$ is "small"
- If $r_{i\_1} + \ldots + r_{i\_u} \neq r_{j\_1} + \ldots + r_{j\_u}$ then $E(ham(NAF(S(i_1,..,i_u) - S(j_1,..,j_u)))) \approx (k+R)/3$

Example 2: Enhanced attack (II)

- Step 1: This distinguisher allows to determine a system of linear equations in the blinding factors $r_1, \ldots, r_N$
  Numerical example: RSA with CRT, 1024 bit primes, 16 bit exponent blinding
  - $\varepsilon = 0.13$, $\approx$ 140 power traces, $\approx 2^{25}$ comparisons
  - $\varepsilon = 0.08$, $\approx$ 30 power traces, $\approx 2^{23}$ comparisons
- Step 2: Solve the system of linear equations
- Step 3: Determine d_p etc.

Large error probability ε or large blinding factors (e.g. R > 64) make the enhanced attack infeasible.

Example 3: Algebraic side channel attacks

- Scenario:
  - Side-channel attack (power attack, cache attack) on an (at least partially) unprotected AES implementation
  - The implementation leaks.
  - A ‘pure’ attack is infeasible e.g. since too few traces are available, at least in the attack phase.

- Conclusion? Any attack impossible?

Example 3 (II)

- The AES cipher can be described by a system of nonlinear equations over GF(2).
- To date it is infeasible to solve this system.
- A side-channel attack may provide additional (possibly uncertain) equations (e.g., on intermediate results).
- Idea: The extended system of equations might allow a solution (e.g. with Gröbner bases or SAT solvers).
- References: [3], [4], …

Open question

- In all three examples successful attacks are known.
- But what about the question from the beginning:
  - Does it suffice to know the Hamming weight of some / each RSA key byte?

    (I don't know.)

Conclusion

- Side channel attacks and fault attacks exist, which provide only partial information.
- It is not always clear whether (and, of course, how) this information can be used for a successful attack.
- However, the answer may be relevant for security evaluations.
- Such problems are worth being considered.

References

- [1] D. Naccache, P.Q. Nguyen, M. Tunstall, C. Whelan: Experimenting with Faults, Lattices and the DSA. PKC 2005, Springer, LNCS 3386,16-28.
- [2] W. Schindler, K. Itoh: Exponent Blinding Does not Automatically Lift (Partial) SPA Resistance to Higher-Level Security. ACNS 2011, Springer, LNCS 6715, 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. COSADE 2012, Springer, LNCS 7275, 231-248.

References

- [4] M.S.E. Mohamed, S. Bulygin, M. Zohner, A. Heuser, M. Walter, J. Buchmann: Improved Algebraic Side-Channel Attack on AES. HOST 2012, IEEE, 156 –161.

Contact

Federal Office for Information Security (BSI)

Werner Schindler
Godesberger Allee 185-189
53175 Bonn, Germany

Tel: +49 (0)228-9582-5652
Fax: +49 (0)228-10-9582-5652

Werner.Schindler@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de