DFA on WolfSSL Ed25519

Seminar 11, PB173

Łukasz Chmielewski

CRoCS,
Masaryk University,
chmiel@fi.muni.cz

Part of the content is reused with permission of Lejla Batina and Ileana Buhan, Radboud University Nijmegen, The Netherlands.

May 2nd, 2024

CRoCS
Centre for Research on Cryptography and Security

Outline

1. Introductions on Fault Attacks
2. Recall on Differential Fault Analysis (RSA)
3. Real-world example: fault attacks on WolfSSL

Attack categories

- Fault Injection was already partially covered on seminar 1.
- Even Differential Fault Analysis (DFA) was briefly mentioned, but I will recall it now.

Plan

Attack categories

- Side-channel attacks
  - use some physical (analog) characteristics
  - the target is running in normal conditions
- Faults: use abnormal conditions causing malfunctions in the system
- Micro-probing: accessing the chip surface directly in order to observe, learn and manipulate the device
- Reverse engineering

Types of implementation attacks

Active vs passive:

- Passive i.e. eavesdropping: the device operates within its specification
- Active i.e. tampering: the key is recovered by exploiting some abnormal behavior e.g. power glitches or laser pulses

Invasiveness:

- Non-invasive aka low-cost:
  - power/EM measurements
  - Coldboot attacks: data remanence in memories - cooling down is increasing the retention time
  - Rowhammer – is essentially a fault attack
- Semi-invasive: the device is de-packaged but no direct contact exists with the chip e.g. optical attacks
- Invasive aka expensive: the strongest type is bus probing

CROCS
Centre for Research on Cryptography and Security

Methods

- Variation in supply voltage i.e. glitching
  - Can cause a processor skip instruction
  - Actively investigated by smartcard industry
  - So-called unloopers were used to activate the infinity loop in PayTV smartcards
- Variation in the external clock: may cause data misread or an instruction miss
- Change in temperature
  - The temperature threshold is defined for which the chip will work properly
  - Can cause changes in RAM content
- White light: photons induce faults
- X-rays and ion beams

Goals

- Insert computational fault
  - Null key
  - Wrong crypto result (Differential Fault Analysis - DFA)
- Change software decisions
  - Force approval of false PIN
  - Reverse life cycle state – PayTV and old phone cards
  - Enforce access rights
  - Break secure boot

CROCS
Centre for Research on Cryptography and Security

Practical Fault Injection Aspects and what we concentrate on in this lecture

- Most common FI: voltage and EM (due to its price)
  - `https://github.com/newaetech/chipshouter-picoemp`
- Differential Fault Analysis (DFA)
  - We mention a few advanced recent methods that strongly relate to SCA
- Glitching decisions:
  - secure boot
  - obtaining memory dumps
  - enabling debug interfaces

CRОCS
Centre for Research on Cryptography and Security

DFA

- Bellcore attack in 1995
  - Differential faults on RSA-CRT signatures
  - Requires 1 correct and 1 wrong signature
- Attack on DES in 1997 by Biham and Shamir
- Special attacks on AES, ECC etc.
- Fault attacks on key transfer

CROCS
Centre for Research on Cryptography and Security

DFA on cryptosystems

- Basic DFA scenario:
  - adversary obtains a pair of ciphertexts that are derived by encrypting the same plaintext (one is correct value and the other is faulty)
  - two encryptions are identical up to the point where the fault occurred
  - $\rightarrow$ two ciphertexts can be regarded as the outputs of a reduced-round iterated block cipher where the inputs are unknown but show a small (and possibly known) differential
- DFA on DES
  - the original attack of Biham and Shamir exploits computational errors occurring in the final rounds of the cipher
  - assumes that one bit of the right half of the DES internal state is flipped at a random position

Recall from seminar 1: RSA with CRT

Optimization of computing a signature giving about 4-fold speedup:
$n = p \cdot q$ Signature: $s = m^d \mod n$

Pre-computed values $d_p := d \mod (p-1)$ $d_q := d \mod (q-1)$
$i_q := q^{-1} \mod p$

$s_p := m^{d_p} \mod p$ $s_q := m^{d_q} \mod q$

Garner's method (1965) to recombine s_p and s_q:
$s = s_q + q \cdot (i_q(s_p - s_q) \mod p)$

Where to glitch?

Almost anywhere :-) computations of s_p and s_q.

If error is in s_p then the adversary can recover q as follows: $q = \gcd(n, s - \hat{s})$.

CROCS
Centre for Research on Cryptography and Security

Plan

Ed25519

- Instance of EdDSA, which was proposed to “fix the unnecessary requirements on randomness” in ECDSA
- Does not depend on a “good” source of randomness, but instead derives a secret deterministically (hashing the msg and a long-term auxiliary key)
- Widely adopted by TLS1.3, Zcash, SSH, Tor, Signal, WolfSSL etc. (check “Things that use Ed25519”)
- Turns out to be easy to attacks in some real-world deployments i.e. WolfSSL

Niels Samwel, Lejla Batina, Guido Bertoni, Joan Daemen and Ruggero Susella: *Breaking Ed25519 in WolfSSL*, CTRSA2018.
Niels Samwel, Lejla Batina: *Practical Fault Injection on Deterministic Signatures: the Case of EdDSA*, Africacrypt 2018.

CROCS
Centre for Research on Cryptography and Security

Ed25519

Algorithm 1 Ed25519 key setup and signature generation

Key setup.

1: Hash k such that $H(k) = (h_0, h_1, \ldots, h_{2b-1}) = (a, b)$
2: $a = (h_0, \ldots, h_{b-1})$, Private scalar
3: $b = (h_b, \ldots, h_{2b-1})$, Auxiliary key
4: Compute public key: $A = aB$.

Signature generation.

5: Compute ephemeral private key: $r = H(b, M)$.
6: Compute ephemeral public key: $R = rB$.
7: Compute $h = H(R, A, M)$ and convert to integer.
8: Compute: $S = (r + ha) \mod l$.
9: Signature pair: (R, S).

CRoCS
Centre for Research on Cryptography and Security

The Attack

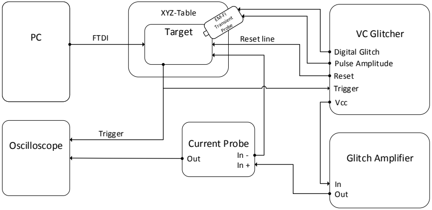
Two signatures, original (R, S) and faulty (R', S'):

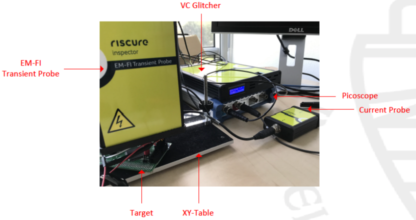
$$S = r + ha$$
$$S' = r + h'a$$

$$S - ha = S' - h'a$$

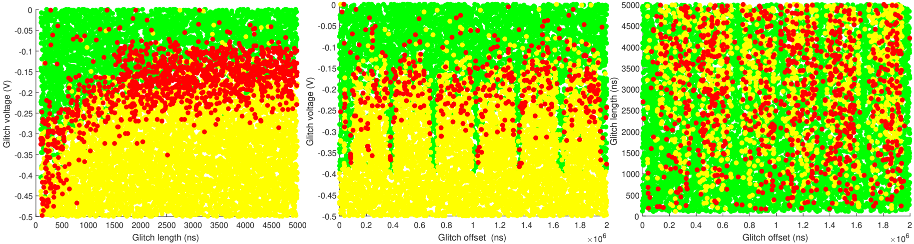
$$a = \frac{S - S'}{h - h'}$$

Setup


PC
FTDI
XYZ-Table
Target
EM-FI Transient Probe
Reset line
VC Glitcher
Digital Glitch
Pulse Amplitude
Reset
Trigger
Vcc
Oscilloscope
Trigger
Current Probe
Out
In -
In +
Glitch Amplifier
In
Out

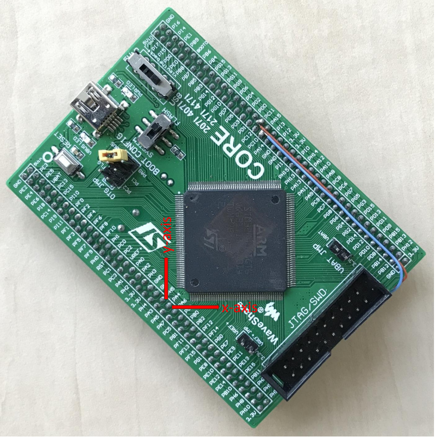

VC Glitcher
EM-FI
Transient Probe
riscure
inspector
EM-FI Transient Probe
DELL
Picoscope
Current Probe
Target
XY-Table

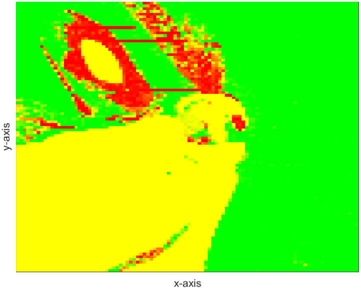
Results



Voltage fault injection results, Normal (green), Inconclusive (yellow), Successful (red).

Results





Conclusion

Two real physical side-channel attacks were actually performed against Ed25519

- Side-channel analysis of Ed25519 with 4 000 traces
- Fault injection on Ed25519 with 100% success rate for EM FI and 70% for voltage glitching out of 10 000 measurements
- For both attacks there exist inexpensive countermeasures

CROCS
Centre for Research on Cryptography and Security

Questions