Snake Oil Crypto:

How I stopped to worry and started to love crypto

Team CIRCL
https://www.d4-project.org/

2019/11/27

D4 project

Jean-Louis Huynen

Outline

- Cryptography 101,
- Cryptography and Network captures,
- D4 passiveSSL Collection,
- Leveraging OpenPGP metedata,
- Checking for weak crypto.

Cryptography 101

- **Plaintext** P: Text in clear,
- **Encryption** E: Process of disguising the plaintext to hide its content,
- **Ciphertext** C: Result of the Encryption process,
- **Decryption** D: Process of reverting encryption, transforming C into P,
- **Encryption Key** EK: Key to encrypt P into C,
- **Decryption Key** DK: Key to decrypt C into P,
- **Cryptanalysis**: Analysis of C to recover P without knowing K.

Cryptography Services

- **Confidentiality** : Ensure the secrecy of the message except for the **intended** recipient,
- **Authentication** : Proving a party's identity,
- **Integrity** : Verifying that data transmitted were not altered,
- **Non-repudiation** : Proving that the sender sent a given message.

Type of Encryption Applications

- **In-transit encryption**: protects data while it is transferred from one machine to another,
- **At-rest encryption**: protects data stored on one machine.

Kerckhoffs's Principle

It [cipher] should not require secrecy, and it should not be a problem if it falls into enemy hands.

There is no security in obscurity.

Attackers model I

Black Box - Attackers may only see inputs / outputs:

- **Ciphertext-Only Attackers (COA) :** see only the ciphertext,
- **Known-Plaintext Attackers (KPA):** see ciphertext and plaintext,
- **Chosen-Plaintext Attacker (CPA):** encrypt plaintext, and see ciphertext,
- **Chosen-Ciphertext Attakers (CCA):** encrypt plaintext, decrypt ciphertext.

Attackers model II

Grey Box - Attackers see cipher's implementation:

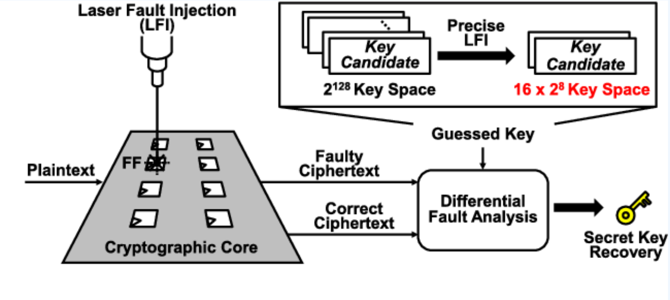
- **Side-Channel Attacks:** study the behavior of the implementation, eg. **timing attacks** [1]:
  - Osvik, Shamir, Tromer [OST06]: Recover AES-256 secret key of Linux's dmcrypt in just 65 ms
  - AlFardan, Paterson [AFP13]: "Lucky13" recovers plaintext of CBC-mode encryption in pretty much all TLS implementations
  - Yarom, Falkner [YF14]: Attack against RSA-2048 in GnuPG 1.4.13: "On average, the attack is able to recover 96.7% of the bits of the secret key by observing a single signature or decryption round."
  - Benger, van de Pol, Smart, Yarom [BvdPSY14]: "reasonable level of success in recovering the secret key" for OpenSSL ECDSA using secp256k1 "with as little as 200 signatures"

8

Most recent timing attack: **TPM-fail** [24420]

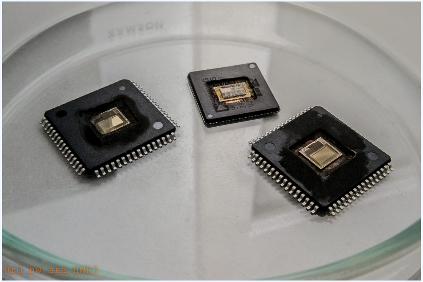
We discovered timing leakage on Intel firmware-based TPM (fTPM) as well as in STMicroelectronics' TPM chip. Both exhibit secret-dependent execution times during cryptographic signature generation. While the key should remain safely inside the TPM hardware, we show how this information allows an attacker to recover 256-bit private keys from digital signature schemes based on elliptic curves.

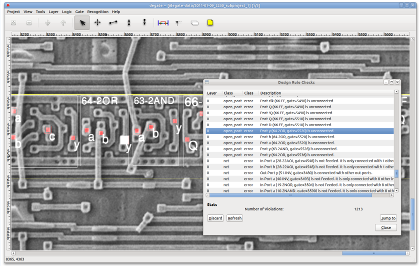
- **Invasive Attacks:**
  - injecting faults [MFS+18],



Attackers model V

- decapping chips [2], reverse engineering [3] [4], etc.





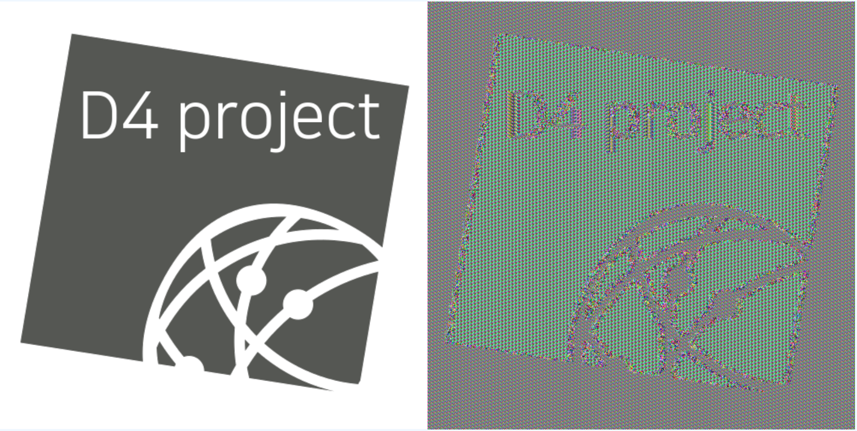
[1] https://cryptojedi.org/peter/data/croatia-20160610.pdf
[2] https://siliconpr0n.org/wiki/doku.php?id=decap:start
[3] http://siliconzoo.org
[4] http://degate.org

- **Indistinguishability (IND) :** Ciphertexts should be indistinguishable from random strings,
- **Non-Malleability (MD):** "Given a ciphertext $C_1 = E(K, P1)$, it should be impossible to create another ciphertext, C_2 , whose corresponding plaintext, P_2 , is related to P_1 in a meaningful way."

Semantic Security (IND-CPA) is the most important security feature:

- Ciphertexts should be different when encryption is performed twice on the same plaintext,
- To achieve this, randomness is introduced into encryption / decryption:
  - $C = E(P, K, R)$
  - $P = D(C, K, R)$

Semantic Security



For instance AES-ECB is not semantically secure - An attacker can build a codebook to crack it. No Semantic Security without randomness

-

For instance AES-ECB is not semantically secure - An attacker can build a codebook to crack it. No Semantic Security without randomness

-

Random Number Generator:

-

Pseudo Random Number Generator:

-

Entropy

Some attacks requires less than CCA / CPA:

- Side Channel attacks as for instance Padding Oracle (Vaudenay Attacks)

Cryptography and Network captures

D4 passiveSSL Collection

Leveraging OpenPGP metedata

Checking for weak crypto

Snake Oil Crypto[5] - Problem Statement

IoT devices **are often the weakest devices** on a network:

- Usually the result of cheap engineering,
- sloppy patching cycles,
- sometimes forgotten–not monitored,
- few hardening features enabled.

We feel a bit safer when they use TLS, but should we?

[5] https://github.com/d4-project/snake-oil-crypto

Keep a log of links between:

- x509 certificates,
- ports,
- IP address,
- client (ja3),
- server (ja3s),

  "JA3 is a method for creating SSL/TLS client fingerprints that should be easy to produce on any platform and can be easily shared for threat intelligence."[6]

Pivot on additional data points during Incident Response

[6] https://github.com/salesforce/ja3

Snake Oil Crypto - Objectives

Collect and **store** x509 certificates and TLS sessions:

- Public keys type and size,
- moduli and public exponents,
- curves parameters.

Detect anti patterns in crypto:

- Moduli that share one prime factor,
- Moduli that share both prime factors, or private exponents,
- Small factors,
- Nonces reuse / common preffix or suffix, etc.

Focus on low hanging fruits that appeal to attackers

Researchers have shown that several devices generated their keypairs at boot time without enough entropy[7]:

```
prng.seed(seed)
p = prng.generate_random_prime()
// prng.add_entropy()
q = prng.generate_random_prime()
n = p*q
```

Given n=pq and n’ = pq’ it is trivial to recover the shared p by computing their **Greatest Common Divisor (GCD)**, and therefore **both private keys**[8].

[7] Bernstein, Heninger, and Lange: `http://facthacks.cr.yp.to/`

[8] `http://www.loyalty.org/~schoen/rsa/`

Snake Oil Crypto - GCD

In Snake-Oil-Crypto we compute GCD[9] between:

- between certificates having the same issuer,
- between certificates having the same subject,
- on keys collected from various sources (PassiveSSL, Certificate Transparency, shodan, censys, etc.),

"Check all the keys that we know of for vendor X"

[9] using Bernstein's Batch GCD algorithm

Snake Oil Crypto - MISP feed

2019-11-08	**Name:** crypto-material **References:** 0 **Referenced by:** 6 **uses Object 13800 (network: x509)** **uses Object 13801 (network: x509)** **uses Object 13802 (network: x509)** **uses Object 13803 (network: x509)** **uses Object 13804 (network: x509)** **uses Object 13805 (network: x509)**			
2019-11-08	Other	**p:** text	12732045980491482532629620809854872609730718866846479950748763 99251101386987265586481573653124576541684265313376164608426942 4192867704218331356123978614869
2019-11-08	Other	**q:** text	None
2019-11-08	Other	**rsa-modulus-size:** text	1024
2019-11-08	Other	**type:** text	RSA

Snake Oil Crypto - MISP feed

The MISP feed:

- **Allows** for checking automatic checking by an IDS on hashed values,
- **contains** thousands on broken keys from a dozen of vendors,
- **will be accessible upon request (info@circl.lu).**

In the future:

- **Automatic** the vendor checks by performing TF-IDF on x509's subjects,
- **automatic** vendors notification.

First release

- ✓ sensor-d4-tls-fingerprinting [10]: **Extracts** and **fingerprints** certificates, and **computes** TLSH fuzzy hash.
- ✓ analyzer-d4-passivessl [11]: **Stores** Certificates / PK details in a PostgreSQL DB.
- snake-oil-crypto [12]: **Performs** crypto checks, push results in MISP for notification
- lookup-d4-passivessl [13]: **Exposes** the DB through a public REST API.

---

[10] `github.com/D4-project/sensor-d4-tls-fingerprinting`
[11] `github.com/D4-project/analyzer-d4-passivessl`
[12] `github.com/D4-project/snake-oil-crypto`
[13] `github.com/D4-project/lookup-d4-passivessl`

Get in touch if you want to join/support the project, host a passive SSL sensor or contribute

- Collaboration can include research partnership, sharing of collected streams or improving the software.
- Contact: info@circl.lu
- https://github.com/D4-Project - https://twitter.com/d4_project

References I

- *Tpm-fail: TPM meets timing and lattice attacks*, 29th USENIX Security Symposium (USENIX Security 20) (Boston, MA), USENIX Association, August 2020.
- Nadhem J. Al Fardan and Kenneth G. Paterson, *Lucky thirteen: Breaking the tls and dtls record protocols*, Proceedings of the 2013 IEEE Symposium on Security and Privacy (Washington, DC, USA), SP '13, IEEE Computer Society, 2013, pp. 526–540.
- Ross J. Anderson, *Security engineering: A guide to building dependable distributed systems*, 2 ed., Wiley Publishing, 2008.
- Jean-Philippe Aumasson, *Serious cryptography: A practical introduction to modern encryption*, no starch press, 2017.

References II

- Naomi Benger, Joop van de Pol, Nigel P. Smart, and Yuval Yarom, *"Ooh aah... just a little bit" : A small amount of side channel can go a long way*, Cryptographic Hardware and Embedded Systems – CHES 2014 (Berlin, Heidelberg) (Lejla Batina and Matthew Robshaw, eds.), Springer Berlin Heidelberg, 2014, pp. 75–92.
- Dieter Gollmann, *Computer security (3. ed.)*, Wiley, 2011.
- Kohei Matsuda, Tatsuya Fujii, Natsu Shoji, Takeshi Sugawara, Kazuo Sakiyama, Yu-Ichi Hayashi, Makoto Nagata, and Noriyuki Miura, *A 286 f2/cell distributed bulk-current sensor and secure flush code eraser against laser fault injection attack on cryptographic processor*, IEEE Journal of Solid-State Circuits **53** (2018), no. 11, 3174–3182.
- Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot, *Handbook of applied cryptography*, 1st ed., CRC Press, Inc., Boca Raton, FL, USA, 1996.

References III

Dag Arne Osvik, Adi Shamir, and Eran Tromer, *Cache attacks and countermeasures: The case of aes*, Topics in Cryptology – CT-RSA 2006 (Berlin, Heidelberg) (David Pointcheval, ed.), Springer Berlin Heidelberg, 2006, pp. 1–20.

Yuval Yarom and Katrina Falkner, *Flush+reload: A high resolution, low noise, l3 cache side-channel attack*, 23rd USENIX Security Symposium (USENIX Security 14) (San Diego, CA), USENIX Association, August 2014, pp. 719–732.