Snake Oil Crypto:

How I stopped to worry and started to love crypto

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

2019/11/27

Jean-Louis Huynen

Outline

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

Cryptography 101

Cryptography Concepts

- **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 in the process,
- **Non-repudiation** : Proving that the sender sent a given message.

Type of Encryption Applications

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

Attack Models

Kerckhoffs's Principle

Security Notions

Attack Models

Cryptography and Network captures

D4 passiveSSL Collection

Leveraging OpenPGP metedata

Checking for weak crypto

Snake Oil Crypto[1] - 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?

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

Snake Oil Crypto - TLS Fingerprinting

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."[2]
Pivot on additional data points during Incident Response

[2] 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

Snake Oil Crypto - RSA on IoT

Researchers have shown that several devices generated their keypairs at boot time without enough entropy[3]:

```
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**[4].

[3] Bernstein, Heninger, and Lange: http://facthacks.cr.yp.to/
[4] http://www.loyalty.org/~schoen/rsa/

Snake Oil Crypto - GCD

In Snake-Oil-Crypto we compute GCD[5] 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”

[5] 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 41928677042183313561239786148 69	
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 [6]: **Extracts** and **fingerprints** certificates, and **computes** TLSH fuzzy hash.
- ✓ analyzer-d4-passivessl [7]: **Stores** Certificates / PK details in a PostgreSQL DB.
- snake-oil-crypto [8]: **Performs** crypto checks, push results in MISP for notification
- lookup-d4-passivessl [9]: **Exposes** the DB through a public REST API.

[6] github.com/D4-project/sensor-d4-tls-fingerprinting
[7] github.com/D4-project/analyzer-d4-passivessl
[8] github.com/D4-project/snake-oil-crypto
[9] 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


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.


Dieter Gollmann, *Computer security (3. ed.)*, Wiley, 2011.


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.