Snake Oil Crypto: How I stopped to worry and started to love crypto

Team CIRCL

2019/12/06



Jean-Louis Huynen

- Use-Case: RSA,
- First Hands-on: Understanding RSA,
- Snake-Oil-Crypto: a primer,
- Second Hands-on: RSA in Snake-Oil-Crypto,
- D4 passiveSSL Collection,
- Interactions with MISP.

Understanding RSA

Ron Rivest, Adi Shamir, and Leonard Adleman in 1977:

- asymmetric crypto system,
- can encrypt and sign,
- messages are big numbers,
- encryption is basically multiplication of big numbers,
- creates a trapdoor permutation: turning x in y is easy, but finding x from y is hard.

~/hands-on/UsingRSA

- Decrypt message.bin
- generate a new private key,
- generate the corresponding public key,
- use this new key to encrypt a message,
- use this new key to decrypt a message.

run: sage rsa.sage at the folder's root:

```
PlainText is: 1234567890
p = random_prime(2^32) = 2312340619
q = random_prime(2^32) = 2031410981
n = p*q = 4697314125248937239
phi = (p-1)*(q-1) = 4697314120905185640
e = random_prime(phi) = 2588085603940229747
d = xgcd(e,phi)[1] = -2102894211931680277
Does d*e == 1?
mod(d*e, phi) = 1
CipherText y = power_mod(x, e, n) = 1454606910711062745
Decrypted CT is: 1234567890
```

Several potential weaknesses:

- Key size too small: keys up to 1024 bits are breakable given the right means,
- close p and q,
- unsafe primes, smooth primes,
- broken primes (FactorDB, Debian OpenSSL bug).
- signing with RSA-CRT (instead of RSA-PSS)

Several potential weaknesses:

- share moduli: if n1 = n2 then the keys share p and q,
- share p or q,

In both case, it is trivial to recover the private keys.

BREAKING SMALL KEYS¹

Hands-on:

~/hands—on/SmallKey

- what is the key size of smallkey?
- what is n?
- what is the public exponent?
- what is n in base10?
- what are p and q?

Let's generate the private key: using p, then using q.

¹https://www.sjoerdlangkemper.nl/2019/06/19/attacking-rsa/

```
~/hands-on/ClosePQ
```

use Fermat Algorithm² to find **both p and q**:

```
def fermatfactor(N):

if N <= 0: return [N]

if is_even(N): return [2,N/2]

a = ceil(sqrt(N))

while not is_square(a^2-N):

a = a + 1

b = sqrt(a^2-N)

return [a - b, a + b]
```

²http://facthacks.cr.yp.to/fermat.html

Researchers have shown that several devices generated their keypairs at boot time without enough entropy³:

```
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.

"They cracked cracked about 13000 of them"

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

~/hands-on/SharedPrimeFactor

Read README.txt, you have a challenge to solve :

- the answers folder should be left alone for now,
- scripts contains scripts that may be useful to solve the challenge,
- attempts may hold your attempt are generating private keys.
- bgcd-bd.sage contains Daniel J. Berstein's algorithm for computing RSA collisions in batches.

Hands-on: Exploiting Weaknesses in RSA – at bigger scale –

We reckon that IoT devices **are often the weakest devices** on a network:

- Usually the result of cheap engineering,
- sloppy patching cycles,
- sometimes forgotten-not monitored (remember the printer sending sysmon?),
- few hardening features enabled.

We feel a bit safer when they use TLS, but we what you now know about RSA, should we?

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

SNAKE OIL CRYPTO - GCD

In Snake-Oil-Crypto we compute GCD⁶ 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.),
- python + redis + postgresql⁷

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

⁶using Bernstein's Batch GCD algorithm ⁷https://github.com/D4-project/snake-oil-crypto/ Quick Demo:

- Let's check how strong are the RSA keys in our database...
- check some results on https://misp-eurolea.enforce.lan
- how bad can it be?
- do you find some vendors we should notify?

SNAKE OIL CRYPTO - MISP FEED

Selected

Attribute: 38881

lame:

Type: attribute

	event: GYZLI Shaka CLUVING	Real Property Present Control Processor	t 2	
	event: (2597) Snake-Other 2000 Database	new official and the second	illy output 2	
83630992148118304595605	event: (2076) 91866-0620 97613-061301-06130-20	ALLE FOR A REAL FRAME RAIL FRAME RAIL	v outrisp2	
/66018/01/9/05314944541	event: (1955). Soake-Discrete Disburger (1955)	in output, 2, rocas, contents (2845) 50	ake-Oil-Crypto Daily output 2	
	event: (2773) SnakeOil-Greato Datyonini0723) Shake-Oil-Cry	appenty Schwart 1997 1 15 No. append	Saker Hat Heb Dairy output 2	
	event: (1906) South Ril Grante Pail Sport Audio Contract Contract		A BAR BERRY Put Path youtput 2	
	1: (2892) Snalevent für Stadent i State 7 5577 State 1	oto Daily output 2	122281 Stake, Olis Britto Bally output 2	
	event (2584) Snake-Ol-Crypto Daily diffout USP event (2584) Snake-Ol-Crypto Daily diffout USP	this on avent bridger side to be	1 19727 Shaketous crypto Daily output 2	
	(507) evided Object and the evidence of the second state of the second s	BORN CELLS HER MELSER FREE	A CONTRACTOR OF CONTRACTOR Daily output 2.	
event?\2	194760205401 EOM & ONE OWN DISKED ON Disk of Daily over	(2352) SPENG ON GUILDEN STRATT	Solver Citrophile Anno Daily output	: 2
event: (4833	 Soake-Qij-CryptoeDaity Olifpat Spake, Qij-Crypto Daily Output 2 	event: (1914) Swore Oreg event: (2978) St	nake@ctrickleanershipshipshipshipshipshipshipshipshipship	ut 2
even	: e26/12/wester Bone of Possily on possily of population of the state	event 929950 2237 1995 4935 1995	Talicourse Dalls putter Daily detBut 2 webbiily sector at 5.0 ptc (2 ptg Detbue 2 put	2
eventev(2069)41 even	28k S G & C Opported & A Share & Share & Crypto Daily output 2	event: (4773) Sna	ke-Olusevate 20017 Statke Oil, Crypto Daily ou 278 Spake Oil Krypto Daily output 2	tput 2
attribute: 102403@980\$1245718	MISP MISP (1)	event: (2/82) Share of the company o	Average of the Averag	200 mar 101 47
event: (2786) Buen is the state of the second state of	event: (2468) Spake	212570) Shartesoni Civito Dally dutput 2	atput 2
event: (2639) Sn event: (273	Invertial Dyblacteries Output the Daily other 2	event: (2611) 2745 and aller fig	The Bane Sur expto Daily output 2	attribute: 1024
event: (2145) S	event: (2222) on Bits Out Copper Sally Copper Daily out put 2.	event: 121012/ SARVE Space Aleman	BH-Corpte Daily deeput 2.	
event: (2365	vertal analygenergy state onthebote daily output 2 I Snake-DISH-Typte dent state Soake OII Coupte Daily output 2	event (1903) Snalevent	to all would be the total and the service being of	tput Z attribute: RSA
	2017L Cooke Oil Constant of Street O	EVENC (2204) Shakeron-U.Sent 19923	Shine of the other of the second s	tout 2

MISP MICD

attribute: 13179552249776999 00028067701910107536192295135825 Rosess37956540760405711252116334343 event: (4879) Snal output 2... ally output 2... output 2... Jaily output 2

event: (2714) S oto Dally output 2. (1985) Snake Oil Crypto Daily output 2... event: (2275)(3 Daily output 2.

lui S event: (193 theogtput 2... event: (4872), Sna

Reub? Covpto Daily output 2. ly output 2... event: (285

Certific Grupte Daily output 2.. event: (2) Crypto Daily output 2...

unta Dally output 2...

Snake-Oil-Crypto Daily output 2 ... 2521FSRUKE OFFERALLY OFFICE OFFICE (1916) Snake-Off-Crypto Daily out event: (2579) Scale of the Crypto Daily Structure of the Structure of the

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.

~/hands-on/TLSinspection

- open stripped.pcap
- what is the admin password?
- bummer, it's encrypted,
- what is the admin password?

D4 - full chain demo.

- ✓ sensor-d4-tls-fingerprinting ⁸: Extracts and fingerprints certificates, and computes TLSH fuzzy hash.
- ✓ analyzer-d4-passivessl ⁹: Stores Certificates / PK details in a PostgreSQL DB.
- snake-oil-crypto ¹⁰: Performs crypto checks, push results in MISP for notification
- lookup-d4-passivessl¹¹: Exposes the DB through a public REST API.

⁸github.com/D4-project/sensor-d4-tls-fingerprinting ⁹github.com/D4-project/analyzer-d4-passivessl ¹⁰github.com/D4-project/snake-oil-crypto ¹¹github.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-Projecthttps://twitter.com/d4_project