CERTIFIED SIDE CHANNELS
29th USENIX Security Symposium

Cesar Pereida García, Sohaib ul Hassan, Nicola Tuveri, Iaroslav Gridin, Alejandro Cabrera Aldaya, Billy Bob Brumley,
{cesar.pereidagarcia, sohaibulhassan, nicola.tuveri, iaroslav.gridin, alejandro.cabreraaldaya, billy.brumley}@tuni.fi

Network and Information Security Group (NISEC), Tampere University, Tampere, Finland

Aug 12-14, 2020
“Cryptographic keys stored within a cryptographic module shall be stored in either plaintext form or encrypted form [...] Documentation shall specify the key storage methods employed by a cryptographic module” - FIPS 140-2
Key Parameters

ECC Private-Key: (256 bit)

priv:

pub:

Field Type: prime-field

Prime:
00:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
A:
00:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
B:
bc:65:1d:06:b0:cc:53:b0:...:3e:27:d2:60:4b

Generator (uncompressed):

Order:
00:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
63:25:51

Cofactor: 1 (0x1)

Seed:
b7:81:9f:7e:90

RSA Private-Key: (1024 bit, 2 primes)

modulus:

publicExponent:
65537 (0x10001)

privateExponent:

prime1:

prime2:
00:d7:c2:44:2d:ac:25:6c:0f:2a:2c:7e:8c:cd:56:
03:25:5b:07:4c:ac:89:3d:...:30:9e:70:d5:2f

exponent1:

exponent2:
00:b8:ff:86:19:3e:64:e2:1f:52:c9:ec:73:40:8c:
b4:a1:cf:ca:24:bc:8e:00:...:17:9d:a8:c7:e5

coefficient:

DSA Private-Key: (1024 bit)

priv:
00:e3:6c:c6:d1:d5:6d:e3:57:81:77:83:00:10:d7:
40:a6:86:f8:7d:ef

pub:
0b:53:17:91:46:09:c5:33:...:41:0a:38:be:2c:

P:
82:6f:2b:26:75:0b:8c:bb:...:29:8d:45:36:ac:
c3:3d:c8:ef:c1:d6:36:76:4d

Q:
9c:43:da:c1:9a:al

G:
97:92:a1:5f:af:09:c2:4a
Does the choice of key format impact security?

Does including or excluding key parameters impact security?
Hunting Side-Channel Leakage - Tooling

---

**TriggerFlow**

Program execution code path analysis.

```
openssl genpkey -algorithm RSA -out key.pem
```

```
pkey_rsa_keygen()
  rsa_pmeth.c:749
```

```
witness()
  bn_prime.c:356
```

```
BN_MONT_CTX_set()
  bn_mont.c:450
```

```
BN_mod_inverse()
  bn_gcd.c:241
```

```
BN_mod_exp_mont()
  bn_exp.c:422
```

```
BN_gcd()
  bn_gcd.c:125
```

---

1Available at https://gitlab.com/nisec/triggerflow
Hunting Side-Channel Leakage - Targets

CVE-2016-2178
CVE-2016-7056
CVE-2018-0734
CVE-2018-0737
CVE-2018-0737

OpenSSL
Cryptography and SSL/TLS Toolkit

arm
MBED
Vulnerabilities
Data-cache attack on Sliding Window Exponentiation

Precomputation

\[ y := g^x \mod p \]

\[ g^1 \mod m \quad g^3 \mod m \quad g^5 \mod m \quad \ldots \quad g^{15} \mod m \]

Exponentiation

\[ S M M M \ldots M S S M S S S S S S M \]
OpenSSL Cryptography and SSL/TLS Toolkit

RSA - Key Validation Bypass

`openssl rsa -in rsa.pem -check`

`RSA_check_key_ex()`

`bn_miller_rabin_is_prime()`

`BN_mod_exp_mont()`

`BN_gcd()`

`BN_mod_inverse()`

`BN_MONT_CTX_set()`

`BN_mod_inverse()`

`BN_mod_inverse()`

`BN_mod_inverse()`

\[ d \times e \equiv 1 \mod \text{lcm}(p-1, q-1) \]

\[ \text{lcm}(p-1, q-1) = (p-1) \times (q-1) \]

\[ \text{gcd}(p-1, q-1) \]

\[ iqmp = q^{-1} \mod p \]

\[ (2^w)^{-1} \mod p \]

\[ b^m \mod p \]
RSA Private-Key: (1024 bit, 2 primes)

modulus:

publicExponent: 65537 (0x10001)

privateExponent:

prime1:

prime2:
00: d7: c2: 44: 2d: ac: 25: 6c: 0f: 2a: 2c: 7e: f8: cd: 56: 

exponent1:

exponent2:

coefficient:

\[ d = e^{-1} \mod \text{lcm}(p-1, q-1) \]
\[ \text{lcm}(p-1, q-1) = (p-1) \times (q-1) \]
\[ \text{gcd}(p-1, q-1) \]

\[ iqmp = q^{-1} \mod p \]
ECDSA - Explicit Parameters Bypass

Private-Key: (256 bit)

priv:

```
54:35
```

pub:

```
99:c7:35:28:28
```

**ASN1 OID: prime256v1**

**NIST CURVE: P-256**

---

ECC Private-Key: (256 bit)

```
priv:


pub:


Field Type: prime-field

Prime:

```
00:ff:ff:ff:ff:00:00:00:01:00:00:00:00:00:00:
00:00:00:00:00:ff:ff:ff:ff:ff:ff:ff:ff:ff:
```

Order:

```
00:ff:ff:ff:00:00:00:00:ff:ff:ff:ff:ff:ff:
```

**Cofactor: 1 (0x1)**

---

ECC Private-Key: (256 bit)

```
priv:


pub:


Field Type: prime-field

Prime:

```
00:ff:ff:ff:ff:00:00:00:01:00:00:00:00:00:00:
00:00:00:00:00:ff:ff:ff:ff:ff:ff:ff:ff:ff:
```

Order:

```
00:ff:ff:ff:ff:00:00:00:00:ff:ff:ff:ff:ff:
```

**Cofactor: 0 (0x0)**

---

Diagram:

```
openssl dgst -sha256 -sign prime256v1.pem -out data.sig data
ecdsa_sign_setup() ecs_ossl.c:182 ecp_nistz256_points_mul() ecp_nistz256.c:961

openssl dgst -sha256 -sign explicit.pem -out data.sig data
ecdsa_sign_setup() ecs_ossl.c:182 ec_scalar_mul_ladder() ec_mult.c:149

openssl dgst -sha256 -sign nocofactor.pem -out data.sig data
ecdsa_sign_setup() ecs_ossl.c:182 ec_wNAF_mul() ec_mult.c:414
```
Protocol Level Attack

Timing Attack

EM Attack

Cumulative probability vs. Time (CPU cycles, millions)

Threshold

Cumulative probability

Time (CPU cycles, millions)

20.6 20.8 21.0 21.2 21.4 21.6 21.8

249
250
251
252
253
254
255
256
Responsible Disclosure and Countermeasures
We reported our findings to *OpenSSL* and *mbedTLS*, and they acknowledge the vulnerabilities. OpenSSL assigned **CVE-2019-1547** based on our work, and we made several contributions to the codebase.

- **Cofactor**: Manual computation from field cardinality and generator order.
- **Explicit parameters**: Match explicit parameters to internal table of named curves to use available specialized implementations.
- **Modular inverse**: Set the `BN_FLG_CONSTTIME` flag to use safer version against SCA.
- **Modular exponentiation**: Set the `BN_FLG_CONSTTIME` flag to use safer version against SCA.
- **GCD**: Replace for constant-time GCD by Bernstein and Yang [BY19].
- **Triggerflow**: Integrate new unit tests for continuous testing.
Conclusions

- Key formats and key parameters do have an impact on security.
- We demonstrated it with D-cache, LLC, timing, and EM attacks across different cryptosystems.
- We made several contributions to OpenSSL and mbedTLS.
- Future work: extend test coverage for more key formats, key parameter combinations, architectures, compilation options, and libraries.
Thank you for listening.

All questions welcomed!

For more research, follow us at:

🐦 @CesarPereidaG
🐦 @NISEC_TAU