Tampere University

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

Key Formats

“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:
    6b:76:cc:81:6d:ce:9a:8e:[...]:bc:f0:55:54:35
pub:
    04:39:6d:7a:e4:80:01:6d:[...]:99:c7:35:28:28
Field Type: prime-field
Prime:
    00:ff:ff:ff:ff:00:00:00:01:00:00:00:00:00:00:
    00:00:00:00:00:00:ff:ff:ff:ff:ff:ff:ff:ff:ff:
    ff:ff:ff
A:
    00:ff:ff:ff:ff:00:00:00:01:00:00:00:00:00:00:
    00:00:00:00:00:00:ff:ff:ff:ff:ff:ff:ff:ff:ff:
    ff:ff:fc
B:
    5a:c6:35:d8:aa:3a:93:e7:b3:eb:bd:55:76:98:86:
    bc:65:1d:06:b0:cc:53:b0:[...]:3e:27:d2:60:4b
Generator (uncompressed):
    04:6b:17:d1:f2:e1:2c:42:47:f8:bc:e6:e5:63:a4:
    40:f2:77:03:7d:81:2d:eb:[...]:68:37:bf:51:f5
Order:
    00:ff:ff:ff:ff:00:00:00:00:ff:ff:ff:ff:ff:ff:
    ff:ff:bc:e6:fa:ad:a7:17:9e:84:f3:b9:ca:c2:fc:
    63:25:51
Cofactor:  1 (0x1)
Seed:
    c4:9d:36:08:86:e7:04:93:6a:66:78:e1:13:9d:26:
    b7:81:9f:7e:90
```

```
RSA Private-Key: (1024 bit, 2 primes)
modulus:
    00:c2:ac:d4:1b:cf:51:d5:e6:92:fe:a0:99:10:a0:
    b3:25:0a:d3:ca:ac:d6:16:[...]:9d:f9:6a:14:61
publicExponent: 65537 (0x10001)
privateExponent:
    00:8a:70:37:22:53:ab:61:8e:67:a8:15:72:e4:25:
    33:60:3b:33:e3:a4:47:56:[...]:50:4f:92:18:f5
prime1:
    00:e6:fb:e3:13:c7:56:72:e3:f5:70:f4:e6:9b:4a:
    fa:a1:de:2c:73:81:86:37:[...]:a0:d6:0d:6b:6f
prime2:
    00:d7:c2:44:2d:ac:25:6c:0f:2a:2c:7e:f8:cd:56:
    03:25:5b:07:4c:ac:89:3d:[...]:30:9e:70:d5:2f
exponent1:
    27:39:54:f9:51:db:6b:4d:2c:ab:ce:da:ae:3a:50:
    4f:56:84:23:e5:35:de:79:[...]:13:2c:64:40:ff
exponent2:
    00:b2:8f: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:
    00:ab:e3:c8:24:f2:a6:51:6b:cc:35:da:6c:6b:f2:
    27:28:7f:87:e0:cc:be:01:[...]:1f:b2:a2:fe:25
```

```
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:
    02:a3:07:6e:da:2a:5a:6a:a0:72:aa:47:9d:cc:0b:
    da:00:d4:26:36:5f:fe:98:35:43:db:85:d4:31:79:
    0b:53:17:91:46:09:c5:33:[...]:41:0a:38:be:2c:
    be:d6:96:d7:79:8d:67:49
P:
    00:b2:9e:fe:64:e2:e5:85:60:de:d8:aa:f9:6b:8c:
    94:91:a9:9e:a6:2a:a8:84:cc:9f:47:6b:01:e1:7c:
    82:6d:fb:26:75:0b:8c:bb:[...]:29:8d:45:36:ac:
    c3:3d:c8:ef:c1:d6:36:76:4d
Q:
    00:fe:35:e4:84:b7:f6:b4:74:72:15:bb:cb:2e:45:
    9c:43:da:c1:9a:a1
G:
    52:c8:59:56:3f:3f:6f:ec:6d:16:da:62:45:e5:9d:
    60:ca:4d:66:c5:ee:c6:d2:60:dd:f5:e1:e8:4f:3e:
    a2:20:d4:1f:cf:d9:2f:d9:[...]:de:14:41:70:57:
    97:92:a1:5f:af:09:c2:4a
```

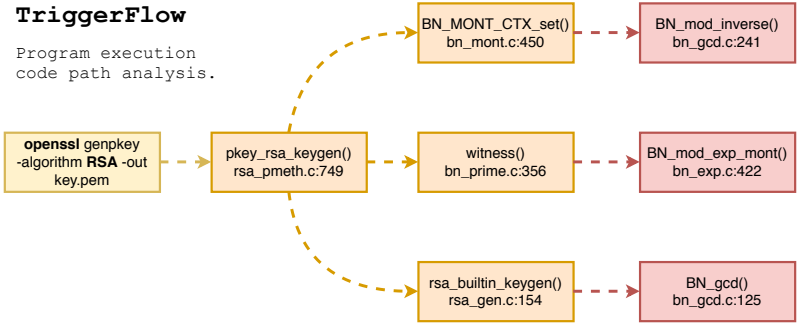
Does the choice of key format impact security?

Does including or excluding key parameters impact security?

Hunting Side-Channel Leakage - Tooling [1]

TriggerFlow

Program execution
code path analysis.



[1] Available at `https://gitlab.com/nisec/triggerflow`

Hunting Side-Channel Leakage - Targets

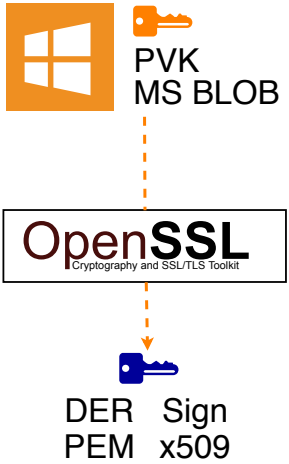
- CVE-2016-2178
- CVE-2016-7056
- CVE-2018-0734
- CVE-2018-0737
- CVE-2018-0737

OpenSSL
Cryptography and SSL/TLS Toolkit

arm MBED

Vulnerabilities

DSA - Key Formatting Bypass

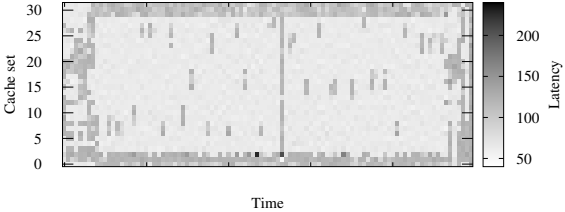


Data-cache attack on Sliding Window Exponentiation

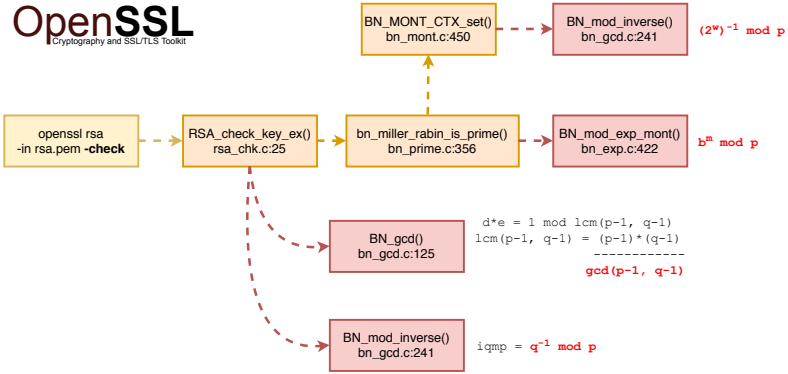
Precomputation

$y := g^x \bmod p$

Exponentiation



RSA - Key Validation Bypass



RSA - Missing Parameters Bypass

```
RSA Private-Key: (1024 bit, 2 primes)
modulus:
    00:c2:ac:d4:1b:cf:51:d5:e6:92:fe:a0:99:10:a0:
    b3:25:0a:d3:ca:ac:d6:16:[...]:9d:f9:6a:14:61
publicExponent: 65537 (0x10001)
privateExponent:
    00:8a:70:37:22:53:ab:61:8e:67:a8:15:72:e4:25:
    33:60:3b:33:e3:a4:47:56:[...]:50:4f:92:18:f5
prime1:
    00:e6:fb:e3:13:c7:56:72:e3:f5:70:f4:e6:9b:4a:
    fa:a1:de:2c:73:81:86:37:[...]:a0:d6:0d:6b:6f
prime2:
    00:d7:c2:44:2d:ac:25:6c:0f:2a:2c:7e:f8:cd:56:
    03:25:5b:07:4c:ac:89:3d:[...]:30:9e:70:d5:2f
exponent1:
    27:39:54:f9:51:db:6b:4d:2c:ab:ce:da:ae:3a:50:
    4f:56:84:23:e5:35:de:79:[...]:13:2c:64:40:ff
exponent2:
    00:b2:8f: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:
    00:ab:e3:c8:24:f2:a6:51:6b:cc:35:da:6c:6b:f2:
    27:28:7f:87:e0:cc:be:01:[...]:1f:b2:a2:fe:25
```

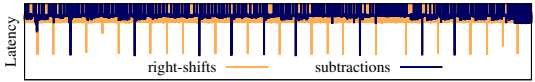
arm MBED

Group	# of keys
Invalid	216
Public	8
CRT vulnerability	16
CRT & d vulnerabilities	16

$$d = e^{-1} \bmod \mathrm{lcm}(p-1, q-1)$$

$$\mathrm{lcm}(p-1, q-1) = \frac{(p-1)*(q-1)}{\gcd(p-1, q-1)}$$

$$\mathrm{iqmp} = q^{-1} \bmod p$$

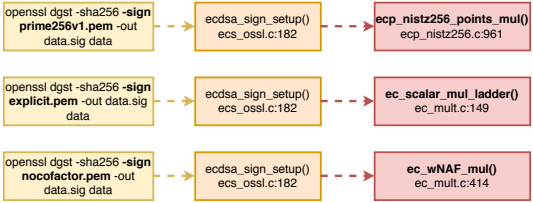


ECDSA - Explicit Parameters Bypass

```
Private-Key: (256 bit)
priv:
    6b:76:cc:81:6d:ce:9a:8e:bc:6f:f1:90:bc:f0:55:
    53:10:d1:fb:08:24:04:7f:70:3f:62:7f:33:8b:cf:
    54:35
pub:
    04:39:6d:7a:e4:80:01:6d:f3:1f:84:f8:04:39:e3:
    20:b0:63:8e:02:40:14:a5:d8:e1:49:23:ee:a7:69:
    48:af:b2:5a:32:1c:ca:da:bd:8a:42:95:a1:e8:82:
    38:79:b9:b6:53:69:bd:49:d3:37:08:68:50:b3:c7:
    99:c7:35:28:28
ASN1 OID: prime256v1
NIST CURVE: P-256
```

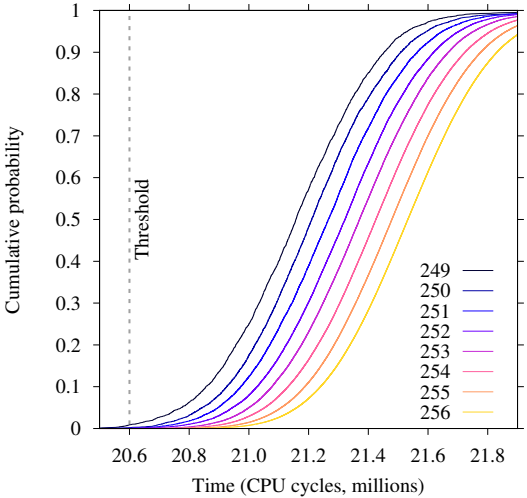
```
ECC Private-Key: (256 bit)
priv:
    6b:76:cc:81:6d:ce:9a:8e:[...]:bc:f0:55:54:35
pub:
    04:39:6d:7a:e4:80:01:6d:[...]:99:c7:35:28:28
Field Type: prime-field
Prime:
    00:ff:ff:ff:ff:00:00:00:01:00:00:00:00:00:00:
    00:00:00:00:00:00:ff:ff:ff:ff:ff:ff:ff:ff:ff:
    ff:ff:ff
[...]
Order:
    00:ff:ff:ff:ff:00:00:00:00:ff:ff:ff:ff:ff:ff:
    ff:ff:bc:e6:fa:ad:a7:17:9e:84:f3:b9:ca:c2:fc:
    63:25:51
Cofactor:  1 (0x1)
```

```
ECC Private-Key: (256 bit)
priv:
    6b:76:cc:81:6d:ce:9a:8e:[...]:bc:f0:55:54:35
pub:
    04:39:6d:7a:e4:80:01:6d:[...]:99:c7:35:28:28
Field Type: prime-field
Prime:
    00:ff:ff:ff:ff:00:00:00:01:00:00:00:00:00:00:
    00:00:00:00:00:00:ff:ff:ff:ff:ff:ff:ff:ff:ff:
    ff:ff:ff
[...]
Order:
    00:ff:ff:ff:ff:00:00:00:00:ff:ff:ff:ff:ff:ff:
    ff:ff:bc:e6:fa:ad:a7:17:9e:84:f3:b9:ca:c2:fc:
    63:25:51
Cofactor:  0 (0x0)
```

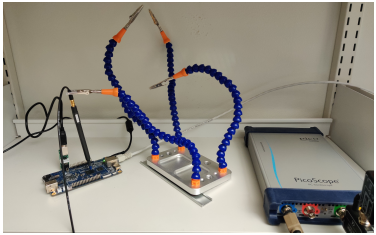


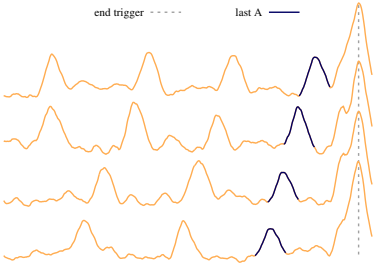
Protocol Level Attack

Timing Attack



EM Attack





Responsible Disclosure and Countermeasures

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 code base.

- **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