SYNACKTIV
DIGITAL SECURITY

Cache attack, ECC, FRP256v1, backdoor, NIST, fin du monde

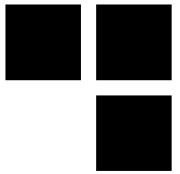
On ne nous dit pas tout...

Présenté 16/06/2016

Pour BeeRumP 2016

Par Eloi Vanderbeken

Contexte



- **Les cache attacks c'est cool**
  - Accès au cache CPU : rapide.
  - Accès à la RAM : lent.

  → **fuite d'information potentiellement exploitable**
  - Théorisé au milieu des années 90
  - Premières attaques au début des années 2000.
  - De nombreuses évolutions récentes (depuis le JavaScript, inter-VM, sur les proco mobile etc.).

- **Les courbes elliptiques c'est cool**
  - Very tiny keys, much powerful.

- **Un leak de 1 bit suffit pour attaquer ECDSA**
  - Arrivé plusieurs fois dans le passé
  - Notamment sur OpenSSL : CVE-2014-0076, CVE-2011-1945

CVE-2011-1945

- **Si les premiers bits du k random sont à 0 → temps de signature plus court.**
- **Patch pour éviter une timing attack :**

```
143         /*
144          * We do not want timing information to leak the length of k, so we
145          * compute G*k using an equivalent scalar of fixed bit-length.
146          */
147
148         if (!BN_add(k, k, order))
149             goto err;
150         if (BN_num_bits(k) <= BN_num_bits(order))
151             if (!BN_add(k, k, order))
152                 goto err;
```

problem?

BN_add exécuté ou non suivant la valeur de k !

```
/*
 * We do not want timing information to leak the
 * compute G*k using an equivalent scalar of fixe
 */

if (!BN_add(k, k, order))
    goto err;
if (BN_num_bits(k) <= BN_num_bits(order))
    if (!BN_add(k, k, order))
        goto err;
```

Explication…

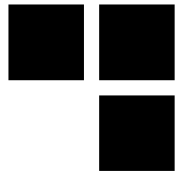
- Order = 1010b

- k = 0100b
- k + Order = 1100b < 10000b → deuxième add effectué

- k = 1001b
- k + Order = 10011b >= 10000b → deuxième add pas effectué

- Oracle pour savoir si k < à $2^{\log2(order)+1}$ - order
- **SI on arrive à savoir quand le 2eme add est effectué**

Hélas…



- **Le nombre d'additions dépend de k mais…**
  - Si l'ordre est de la forme 100000...000XXX ou 0xFFFFFF...FFFFFYYY
  - → pas exploitable en pratique
  - probabilité de tomber dans l'un des deux cas beaucoup trop faible.

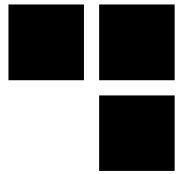
Hélas…

- **C'est le cas de la vaste majorité des courbes :**

NIST P-224	True ✔	True ✔	= 0xffffffffffffffffffffffffffff16a2e0b8f03e13dd29455c5c2a3d
Curve1174	True ✔	True ✔	= 0x1fffffffffffffffffffffffffffffff77965c4dfd307348944d45fd166c971
Curve25519	True ✔	True ✔	= 0x1000000000000000000000000000000014def9dea2f79cd65812631a5cf5d3ed
secp256k1	True ✔	True ✔	= 0xfffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd0364141
E-382	True ✔	True ✔	= 0xfffffffffffffffffffffffffffffffffffffffffffffffd5fb21f21e95eee17c5e69281b102d2773e27e13fd3c97
M-383	True ✔	True ✔	= 0x10000000000000000000000000000000000000000000000006c79673ac36ba6e7a32576f7b1b249e46bbc225be907

- **Src : https://safecurves.cr.yp.to/**

Mais…



- **Si l'ordre est de la forme 0111100...1b ...**
  - Typiquement si l'ordre est choisi de manière aléatoire...
  - Exploitable.

Et qui utilise des ordres aléatoires ?

brainpoolP256t1	True ✔	True ✔	= 0xa9fb57dba1eea9bc3e660a909d838d718c397aa3b561a6f7901e0e82974856a7
brainpoolP384t1	True ✔	True ✔	= 0x8cb91e82a3386d280f5d6f7e50e641df152f7109ed5456b31f166e6cac0425a7cf3ab6af6b7fc3103b883202e9046565

Et qui utilise des ordres aléatoires ?

brainpoolP256t1	True ✔	True ✔	= 0xa9fb57dba1eea9bc3e660a909d838d718c397aa3b561a6f7901e0e82974856a7
brainpoolP384t1	True ✔	True ✔	= 0x8cb91e82a3386d280f5d6f7e50e641df152f7109ed5456b31f166e6cac0425a7cf3ab6af6b7fc3103b883202e9046565
NIST P-256	True ✔	True ✔	= 0xffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551

Et qui utilise des ordres aléatoires ?

brainpoolP256t1	True ✔	True ✔	= 0xa9fb57dba1eea9bc3e660a909d838d718c397aa3b561a6f7901e0e82974856a7
brainpoolP384t1	True ✔	True ✔	= 0x8cb91e82a3386d280f5d6f7e50e641df152f7109ed5456b31f166e6cac0425a7cf3ab6af6b7fc3103b883202e9046565
NIST P-256	True ✔	True ✔	= 0xffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551
ANSSI FRP256v1	True ✔	True ✔	= 0xf1fd178c0b3ad58f10126de8ce42435b53dc67

AVEZ-VOUS DES QUESTIONS ?

MERCI DE VOTRE ATTENTION,

SYNACKTIV
DIGITAL SECURITY