Sweet32: Birthday attack

64-bit block ciphers in TLS

Alexandru Caciulescu
Radu Chiscariu
Razvan Cojocaru
Valentin Buza

Attack purpose

- Recover secret cookie from HTTPS with 3DES
- Capture large amounts of ciphertext
- Find a collision (2 blocks with the same value)
- Collisions happen often enough to be a problem!

HTTP header (the plaintext)

- Useful collision:

Block1 – known plaintext

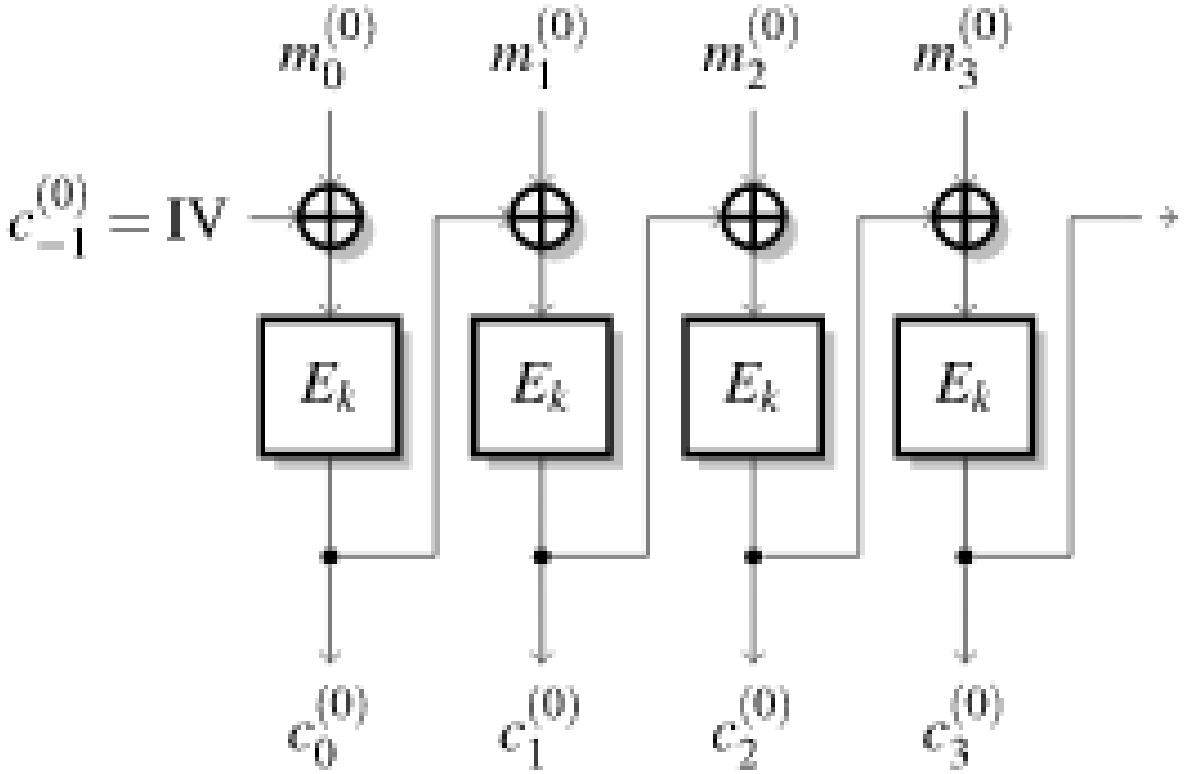
Block2 – secret cookie

```
GET / HTTP/1.1
Host: www.ab.ro
Cookie: secret=<cookie_here>
Accept: text/plain
```

Why obtain a collision

$c_i = E_k(m_i \oplus c_{i-1})$

$m_i \oplus m_j = c_{i-1} \oplus c_{j-1}$



How to…

1. Generate large amounts of ciphertext (about 35GB)
2. Sort the blocks
3. Search for collisions

Sorting and collision lookup

- C++11 header-only sorting library (disk sorting, multithread)
- Total sorting time for ciphertext blocks: around 1-2 hours
- Implemented C++ collision detection module
- Expected running time for collision detection on sorted data: around 30 mins

Collision detection module

On first run:

5 collisions

```
Found collision 735174213495964967
Found collision 1247948159810218381
Found collision 6810904725035589557
Found collision 7704228482905844942
Found collision 13709301323247256842
Nr collisions = 5
updated 735174213495964967 locations: 122347852 18446744073709551615
updated 13709301323247256842 locations: 122347853 18446744073709551615
updated 1247948159810218381 locations: 122347854 18446744073709551615
updated 7704228482905844942 locations: 122347855 18446744073709551615
updated 735174213495964967 locations: 122347852 893212236
updated 13709301323247256842 locations: 122347853 893212237
updated 1247948159810218381 locations: 122347854 893212238
updated 7704228482905844942 locations: 122347855 893212239
updated 6810904725035589557 locations: 1064792912 18446744073709551615
updated 6810904725035589557 locations: 1064792912 3260804768
Collision value: 735174213495964967 locations: 122347852 - 893212236
Collision value: 1247948159810218381 locations: 122347854 - 893212238
Collision value: 6810904725035589557 locations: 1064792912 - 3260804768
Collision value: 7704228482905844942 locations: 122347855 - 893212239
Collision value: 13709301323247256842 locations: 122347853 - 893212237
```

Solution

- Insert redundant headers
- Random shuffle the HTTP headers before encryption
- Different location for headers each time
- Impossible to find collisions as before

Source Code

- https://github.com/razvancojocaru/tema-SASC

Bibliography

- Sweet32 attack description: https://sweet32.info/
- Bhargavan et al. On the Practical (In-)Security of 64-bit Block Ciphers, ACM CCS 2016