BarbHack 2020

un HSM sans HSM

POGGI Jérôme
@EdGtslFcbngq6sk
EdGtslFcbngq6sk@itsnotmy.pw

Plan

- Qui suis-je ?
- Petite intro sur la crypto
- C’est quoi un HSM ?
- Pourquoi faire ?
- Le low tech …
- Conclusion

Qui suis-je ?

Qui suis-je ?

- Tombé dans l'informatique à 12 ans
- +22 ans d'XP dans la SSI
- Dev, Admin, Pentesteur, Auditeur, Architecte …
- Actuellement RSSI dans une grande collectivité
  - Où cette solution a été conçue et implémentée

Petite intro sur la crypto

Petite intro sur la crypto

- On ne dit pas « crypter » !

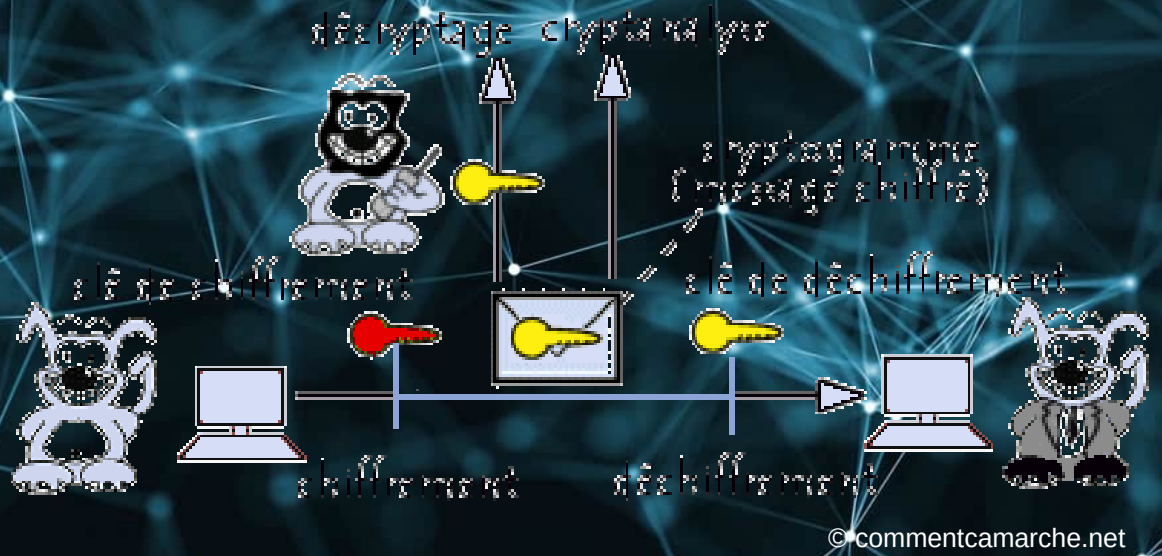
On dit « chiffrer » !

- Cryptographie : Protéger des messages avec des secrets ou des clés.
  - En assurant Confidentialité, Authenticité et Intégrité
- Chiffrement : Procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clef de (dé)chiffrement.
  - Chiffrer : L'action de procéder à un chiffrement.
  - Déchiffrer : Consiste à retrouver le texte original (aussi appelé clair) d'un message chiffré dont on possède la clé de (dé)chiffrement
- Cryptologie : Science comprenant la cryptographie, la cryptanalyse, et la stéganographie

On dit « chiffrer » !

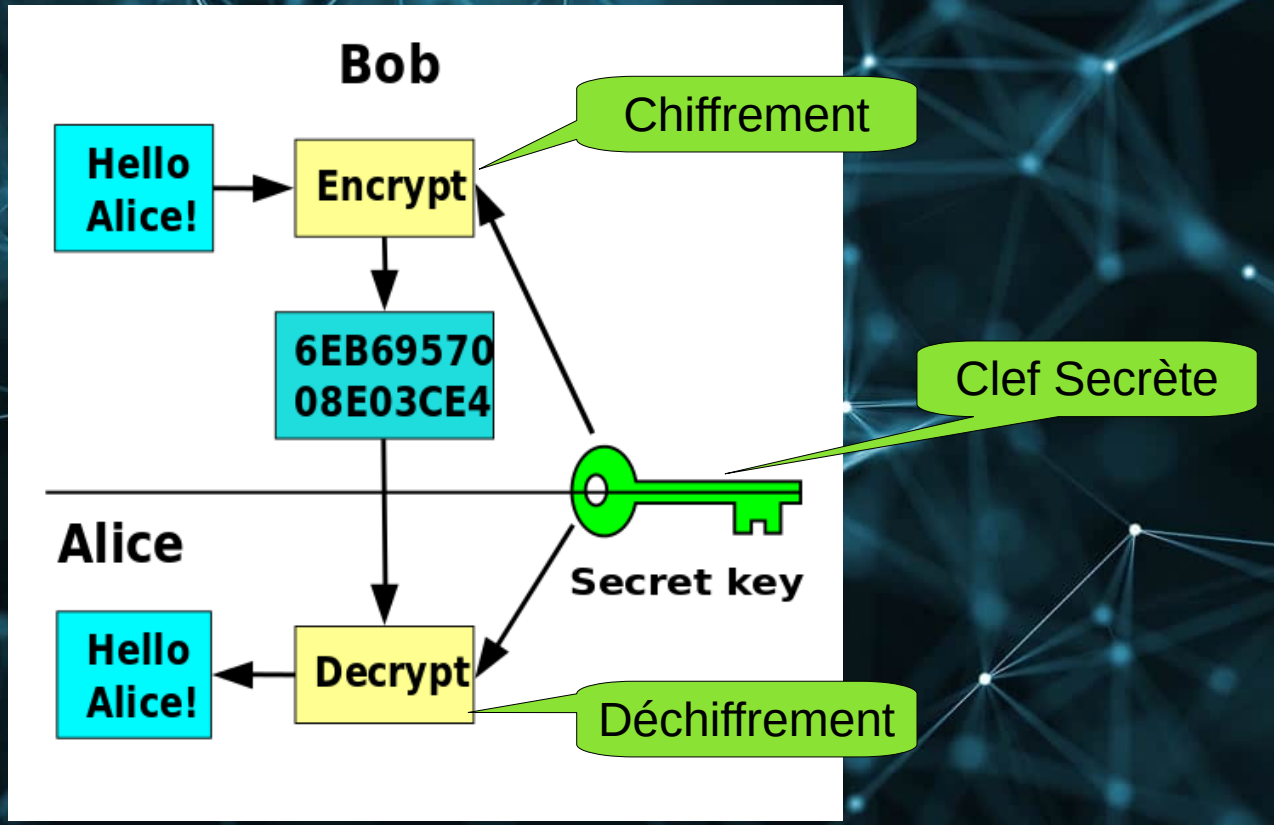
- Décrypter / Décryptage : Consiste à retrouver le texte original à partir d'un message chiffré sans posséder la clef de (dé)chiffrement et de la méthode.
- Crypter / Cryptage / Cryptation :
  - Le terme « cryptage » et ses dérivés viennent du grec ancien κρυπτός, kruptos, « caché, secret ».
  - Incorrecte : la terminologie de cryptage reviendrait à chiffrer un clair sans en connaître la clef et donc sans pouvoir le déchiffrer ensuite.
  - Autant faire un *dd if=/dev/urandom* …
- Chiffrage : pour une proposition commerciale oui …

En résumé ...

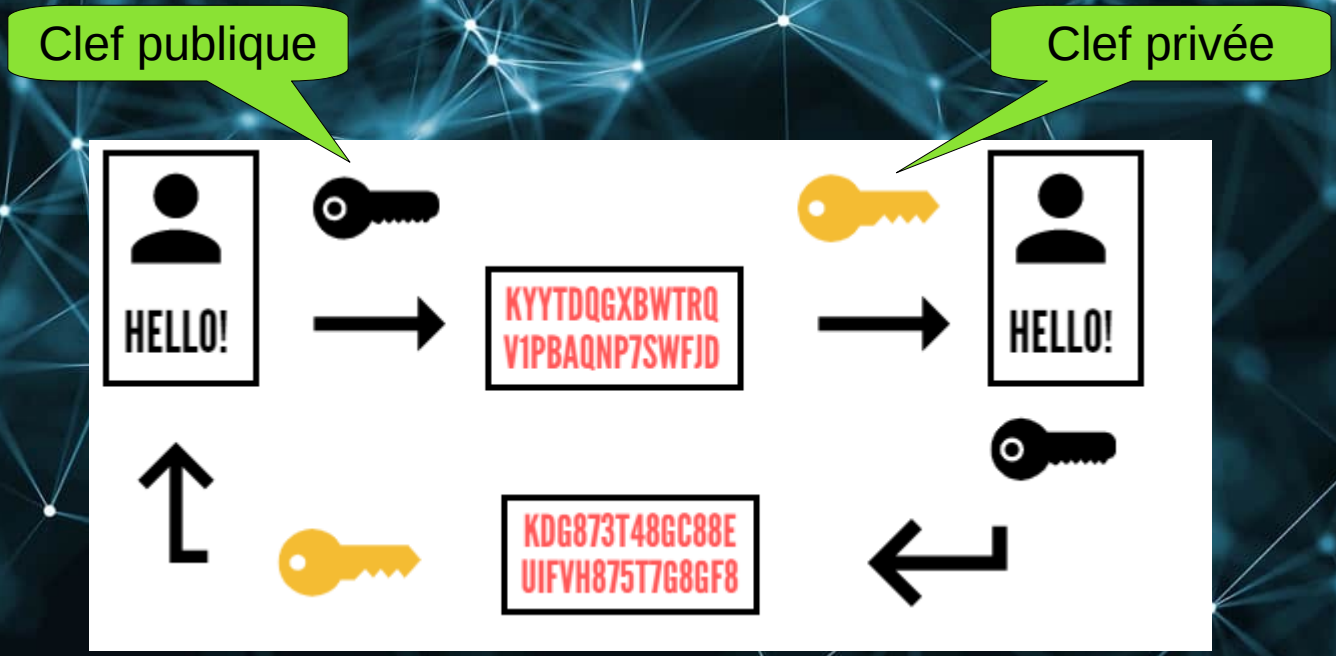


© commentcamarche.net

Crypto Symétrique

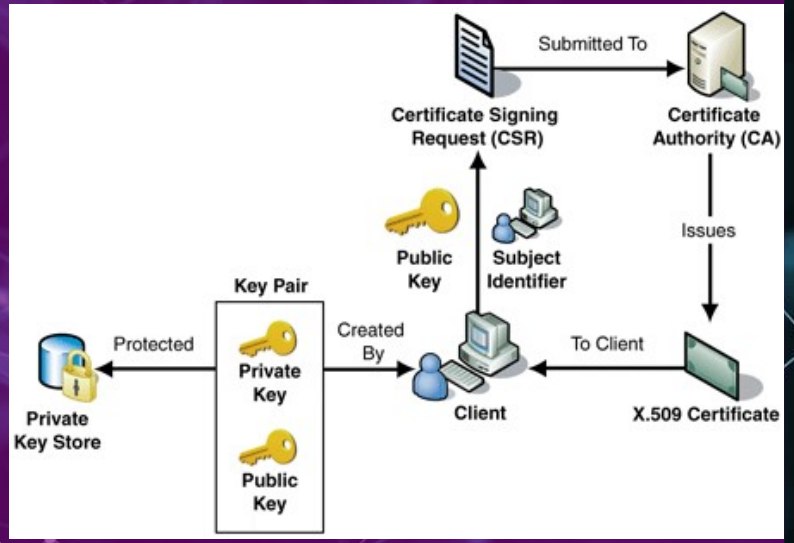


Crypto Asymétrique



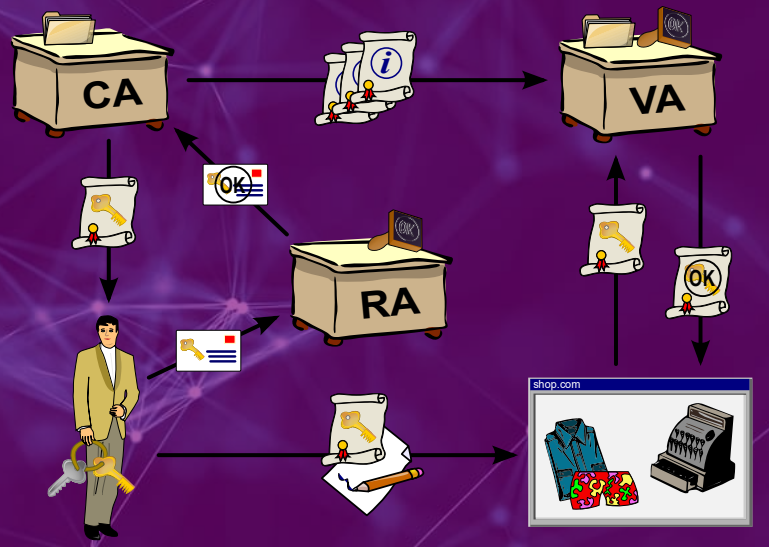
Certificats X509

- Couple de Clef publique / Clef privée
  - Avec des propriétés
    - Date de validité
    - Émetteur, Propriétaire
    - Usages
    - Propriétés diverses
  - Signé par une autorité de certification



PKI ou ICP

- C'est un gestionnaire de certificats
  - Autorités de Certifications (CA)
  - Autorités de Validations (VA)
  - Autorités d'Enregistrements (RA)
  - De manière sécurisée
    - Par du matériel et des procédures
  - Les AC sont
    - soit sur disque (Off-Line) –> Protection importante
    - soit en mémoire (On-Line) –> Utilisation fréquente

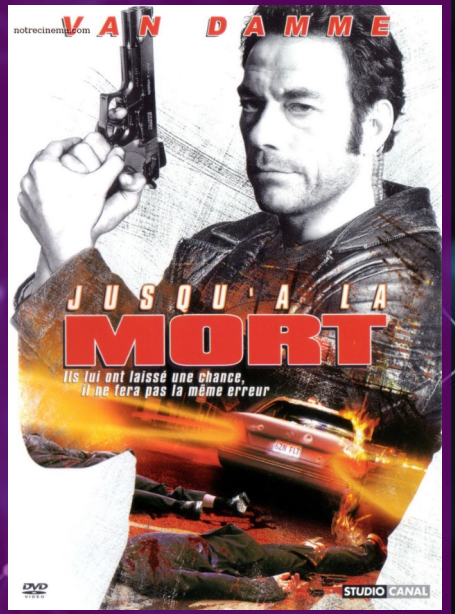


C’est quoi un HSM ?

- HSM = *Hardware Security Module*
  - Boîte Noire Transactionnelle
- Appareil considéré comme inviolable offrant des fonctions cryptographiques.
  - Matériel physique !
  - Carte PCI, Rack 1U,
    Gros lecteur de carte à puce …

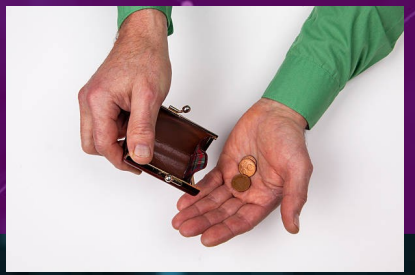
HSM pour faire quoi ?

- Créer des clefs secrètes (Symétrique et Asymétrique) non prédictibles
- Stocker de manière sécurisé des clefs secrètes
- Protéger les clefs secrètes jusqu'à la mort
  - Voir s'autodétruire !
- Être capable de les restaurer de manière sécurisée
  - Ex : avec plusieurs cartes à puce
- Utiliser un générateur réellement aléatoire
  - TRNG : *True Random Number Generator*
  - Très important pour que les clefs secrètes soient non prédictibles



Mon besoin

- Protéger les Certificats Autorité et sous Autorité de la PKI
  - Par un mot de passe très fort
- Chargement seulement en présence de 3 personnes
- Avoir une haute disponibilité des secrets
  - Plusieurs personnes capable de créer l'accès
  - Ne pas être dépendant des congés et de la « feature » dite du poisson dory …
    - En gros de la couche 8
- Ne jamais laisser traiter les secrets directement par l'humain
- Avec un budget proche de 0 €



La solution : des secrets protégés

- Jamais disponible en clair
- Manipulés uniquement par des scripts
  - Effacer la mémoire après chaque utilisation
  - N'utiliser la version en clair qu'au dernier moment, pendant le moins de temps possible
  - Auto-contrôlés en continu
  - Contrôlés systématiquement par l'opérateur
- Nécessité de 3 personnes pour utiliser les clefs
  - 2 personnes du directoire parmi 6 (6x5 = 30 combinaisons, dé-doublonée = 15 combinaisons)
  - 1 exploitant sécurité parmi 4 (4 combinaisons)
  - 60 (4x15) combinaisons possible d'utilisation des clefs secrètes
- Confidentialité, Responsabilité partagée, Haute disponibilité

Le low tech ... phase 1

- **Un HSM Papier !**
- Création de 8 secrets de 32 caractères parmi 69
  - Entropie = 195 bits =log(69^{32})/log(2)
    - 2^{195} = beaucoup d'années, même à 10^{12} tests secondes ... ($5x10^{58}$ cas possible)
- Chacun des 8 secrets est chiffré avec la concaténation de 3 mots de passe de au moins 8 caractères
  - 2 mots de passe de directeurs et 1 d'exploitant
  - Entropie la plus basse estimée à 112 bits = log(26^{24})/log(2)
    - 2^{112} = ouf ! encore beaucoup d'années ($5x10^{33}$)

Le low tech … phase 2

- **Le chiffrement**
- Ces 8 secrets sont chiffrés en AES-256-CBC et imprimés
  - Donc 60 combinaisons de 8 secret chiffrés à imprimer
    - En base64 pour la lisibilité
    - Suivi d'un petit MD5 pour contrôle
    - Le tout en double exemplaires
      - Chacun dans un coffre différent
    - Vu l'entropie des secrets : une clef USB peut même être utilisée pour sauver les 60 pages
- La minute est consigné dans un PV signé par tous

Le low tech ... phase utilisation

- A chaque ouverture d'enveloppe contenant les 60 pages
  - Vérification que l'enveloppe n'est pas altérée
  - Vérification des bonnes signatures en conformité avec le registre d'utilisation
  - Pas de feuille manquante
  - Enveloppe précédemment utilisée présente avec les bonnes signatures
  - Utilisation du bon secret pour chaque besoin
- RIEN au format électronique !
  - Difficulté à l'utilisation (90 caractères à la main ...)
  - Mais rupture de protocole complète entre la création et le stockage

Exemple d'une « page »

```
##########################################################################
#                          Fichier CONFIDENTIEL                          #
#                        Combinaison : D1 D5 E1                          #
##########################################################################

--- Début du secret 1 chiffré en aes-256-cbc et encodé en base64 ---
U2FsdGVkX18onf2oKX92i8YBrZjr/PC/paVvfO6If2uwl30hiFSFlPczR3Yz/K/K
UsfjPCk/1mVsTDOMbmvxPQ==
--- Fin du secret 1 ---
MD5 : 4831ca2ec4aff3c8af4fa8342d29ab92

--- Début du secret 2 chiffré en aes-256-cbc et encodé en base64 ---
U2FsdGVkX18w0v3aGqZTEAK5F6uGDZZ89GSfTAgbvCgOtxN1renQibRiN1yZhiPS
1XoFSJl0EyoLzvUXwcEwUw==
--- Fin du secret 2 ---
MD5 : 9c53fec22ac5ffc7b78cf607623b4e00
...
```

Remarque :
$ echo -n "Salted__" | openssl base64 -e
`U2FsdGVkX18=`

Procédure de création des clefs

- Boot sur un PC sans unité de stockage, sur une Live CD
- Copie du script de création des combinaisons depuis une clef USB
- Vérification de l'intégrité du script, analysé hors ligne et par une personne extérieure
- Saisie des mots de passe, Chiffrement puis Impression des 60 x 2 pages
- Destruction du support de boot (CD)
- Contemplation du PC éteint par l'assemblée pendant ...

Utilisation des clefs

- Choix aléatoire d'un secret parmi les 8 pour chaque besoin
  - A faire la première fois
- Consigné dans un document à part
- Choix d'une des 60 combinaisons suivant les personnes présentes
- Saisie des 3 mots de passe dans l'ordre
- Saisie, Vérification manuelle
- Déchiffrement du secret par le script

Les scripts

- 3 scripts
  - Un pour créer les 8 secrets chiffrés avec les 60 combinaisons
  - Un pour créer les Autorités de Certification
  - Un pour activer les Autorités de Certification
- Disponibles sur mon GitHub :
  - https://github.com/coh7eiqu8thaBu/Script_PKI

Conclusion

Conclusion

- Les avantages
  - Sécurité cryptographique assurée
  - Traçabilité, Intégrité, Disponibilité garanties
  - Le prix
  - La simplicité
  - L'auditabilité

Conclusion

- Les inconvénients
  - Si une des 10 personnes perd son mot de passe
    - Il faut déchiffrer les 8 secrets et refaire la procédure
  - Saisie lourde des secrets
    - Vu l'entropie une action d'OCR + sauvegarde sur clef USB est possible
  - L'intégrité dépend du binaire openssl
    - Intégrité originelle des binaires ???
  - Le RNG n'est pas 100 % fiable

Amélioration

- Procédure de changement de Quorum
- Éviter de devoir à retaper le « secret chiffré » si un mot de passe est faux
- Utiliser gpg pour la signature / vérification du code
- Utiliser un TRNG tel que « Infinite noise » - 13-37.org
- Créer un script de contrôle d'intégrité tournant pendant les opérations

Conclusion

- Pas besoin de dépenser beaucoup
- Il suffit de :
  - Un peu de math,
  - Un soupçon de crypto,
  - Une pincé de dev,
  - Une grosse cuillère de revues de code
  - Le tout arrosé d'un esprit critique

Merci
et
« Hack the Planet !!! »

Références

- Stéphane Bortzmeyer
  - http://www.bortzmeyer.org/cryptage-n-existe-pas.html
- Olivier Robert (déjà en 1999)
  - https://groups.google.com/forum/?fromgroups=#!msg/fr.misc.cryptologie/4VyZm35hrNg/7AMLfElxgjAJ