R4B10 - Cryptographie et Sécurité

Sécurité (introduction), Cryptographie (rappels)

Bruno BEAUFILS

2024/2025

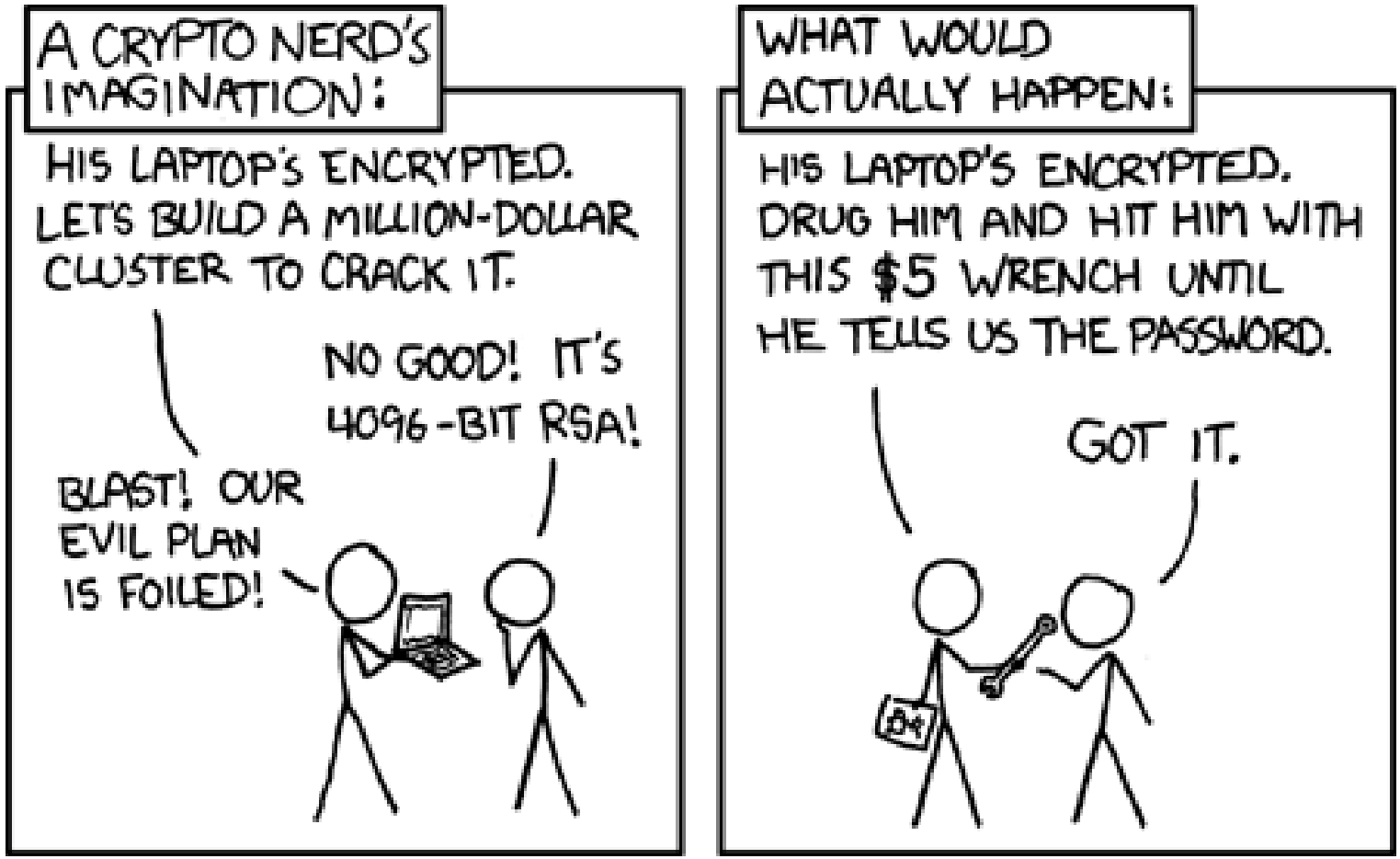
1. Sécurité (introduction)

2. Cryptographie (rappels)

Objectifs

- Assurer la **sécurité** des données, services et réseaux
  - garantir des propriétés d'un système
- Propriétés à garantir (**CAID** ou *CIA*)
  - **Confidentialité**
    - accès limité aux personnes autorisées
  - ***Authenticité***
    - preuve d'identification
  - **Intégrité**
    - données non altérées
  - **Disponibilité** (*Availability*)
    - accès possible sans faille (coupure)
- Une des missions principales des administrateurs système
  - par exemple métier de SRE (*Site **Reliability** Engineer*)
  - doit être à la base de la réflexion
    - dès le développement

La vraie vie



Outils

- **méthodes** (*PSSI*)
  1. définition du périmètre
     - lister ce qui doit être protégé
  2. évaluation des risques
     - identifications (actifs, responsables, vulnérabilités, menaces et modèle de menace)
  3. traiter les risques
     - accepter, éviter, transférer, réduire
  4. sélectionner des mesures
- **comportements**
- **documentation**
  - procédures
  - base de connaissances
  - historique de modifications (*changelog*) ou d'interventions, journalisation
  - bonnes pratiques
    - IETF : les *Best Current Practices* (BCP)
    - ANSSI : règles de base et les guides et bonnes pratiques
  - Common Vulnerabilities and Exposures (CVE)
- ***cryptographie***

Références

Quelques références pour aller plus loin

- **ANSSI**
  - Agence nationale de la sécurité des systèmes d'information
  - Guide d'élaboration de politiques de sécurité des systèmes d'information
- **CERT**
  - *Computer Emergency Response Team*
  - CERT-FR, CERT-EU, CERT/CC, CERT-RENATER, etc.
- **OWASP**
  - *Open Source Foundation for Application Security*
- **picoCTF**
  - outils de formation à la sécurité par la pratique

1. Sécurité (introduction)

2. Cryptographie (rappels)

Vocabulaire

Chiffrement (*encryption*)

Rendre un document illisible **avec une *clef* de chiffrement**, excepté pour son destinataire

Déchiffrement (*decryption*)

Rendre lisible un document chiffré **en connaissant** la *clef* de chiffrement

Décryptage (*cipher breaking*)

Rendre lisible un document chiffré **sans connaître** la *clef* de chiffrement

Cryptologie (*cryptology*)

Science du secret :

- **Cryptographie** (*cryptography*) : étude de la protection par le chiffrement
- **Cryptanalyse** (*cryptanalysis*) : analyse des méthodes de chiffrement pour les *casser*

https://chriffrer.info

Chiffrement symétrique

- Chiffrement **symétrique** (à *clé secrète*)
  - la même clé sert à chiffrer et déchiffrer
- Utilisations :
  - principale utilisation : assurer la **confidentialité**
  - exemple : protection d'informations sensibles
    - données sur disques (vol)
    - messages échangés (capture des messages)
  - difficulté
    - les 2 parties doivent connaître la clé **avant** la communication
- Exemples : DES, AES

Chiffrement asymétrique

- Chiffrement **asymétrique** (à *clé publique*) utilise 2 clés **différentes**
  - une sert généralement à chiffrer — clé **publique**
    - elle peut être diffusée largement et être de connaissance publique
  - une autre sert généralement à déchiffrer — clé **privée**
    - elle doit être protégée **strictement** et accessible qu'à son propriétaire
- Caractéristiques
  - chiffrer avec la clé publique ne peut être déchiffré qu'avec la clé privée
  - chiffrer avec la clé privée peut-être déchiffré avec la clé publique
  - calculs longs (beaucoup plus qu'en symétrique)
- Utilisations :
  - principale utilisation : permettre l'**authentification**
  - exemple : vérification de signature
  - difficultés :
    - la clé publique doit être **distribuée largement**
    - l'utilisateur doit être capable d'**authentifier le propriétaire** de la clé publique
- Exemples : RSA, El Gamal

Empreintes (*fingerprint*)

- Résultat d'une fonction de hachage
  - convertit un ensemble d'octets en une suite d'octets de **longueur fixe**
    - collision (2 suites avec le même haché) possible
  - **hachage cryptographique**
    - hachage *pratiquement* impossible à inverser
    - résiste aux collisions
  - sel (*salt*)
    - données ajoutées à la suite avant le calcul du haché
- Utilisations
  - principale utilisation : vérification d'**intégrité**
  - exemple : stockage de mots de passes, vérification de copies ou téléchargements
- Exemples : MD5, SHA256

Rôles

La cryptographie est utilisée pour assurer certaines propriétés

- **confidentialité**
  seule la personne autorisée à accéder à un contenu peut y accéder
- **intégrité**
  le contenu n'a pas été modifié entre sa production et son accès
- **non-répudiation**
  le producteur du contenu ne pas renier qu'il en est l'auteur
- **authentification**
  l'identité du producteur du contenu est celle annoncée
  - Facteurs d'authentification
    - **ce que l'on sait** *le plus courant (ex : mots de passe)*
    - ce que l'on possède
    - ce que l'on est
    - ce que l'on fait