Quoi: GnuPG Quand: Samedi le 16 février 2019 13:00-15:00 Où: Au Centre de Loisirs St-Louis de France
Qui: Sébastien Boisvert (mail: seb à boisvert point info)

Sujet

- Cryptologie
  - Cryptographie
    - Cryptographie asymétrique ⇐
  - Cryptanalyse

Bob, Alice, Eve, Mallory

- Alice et Bob
- 4 utilisateurs UNIX
  - Alice (agent A)
  - Bob (agent B)
  - Eve (agent E, écouteuse externe, qui écoute les messages)
  - Mallory (agent M, malicieux, modifie les messages)
- Le bureau de poste: /tmp

Concepts

- Agent
  - exemples: Alice, Bob, Eve, Mallory
- Message
  - exemple: un fichier message.txt
- Cryptographie asymétrique
  - chaque agent possède:
    - une clé privée
    - une clé publique
- Chiffrement
  - Alice: gpg –recipient Bob –encrypt message.txt –output message.txt.encrypt.gpg
  - Bob: gpg –decryptmessage.txt.encrypt.gpg –output message.txt
- Signature
- Authenticité (avec signature et vérification)
  - Alice: gpg –sign –default-key Alice message.txt –output message.txt.sign.gpg
  - Bob: gpg –verify message.txt.sign.gpg
- Intégrité
  - exemples: md5sum, sha1sum
- Confidentialité
  - Eve ne peut pas écouter les messages
  - Mallory ne peut pas modifier les messages

Scénario 1: Alice envoie un document non-chiffré non-signé à Bob

- Bob ne peut pas vérifier si le message provient d'Alice (pas de signature)
- Eve peut écouter le message (pas de chiffrement)
- Mallory peut modifier le message

Scénario 2: Alice envoie un document non-chiffré signé à Bob

- Bob peut vérifier si le message provient d'Alice (signature)
- Eve peut écouter le message (pas de chiffrement)
- Mallory ne peut pas modifier le message (car le message est signé par Alice)

Scénario 3: Alice envoie un document chiffré non-signé à Bob

- Bob ne peut pas vérifier si le message provient d'Alice (pas de signature)
- Eve ne peut pas lire message (chiffrement)
- Mallory peut modifier le message (la clé publique de Bob est connue, pour le chiffrement)

Scénario 4: Alice envoie un document chiffré signé à Bob

- Bob peut vérifier si le message provient d'Alice (signature)
- Eve ne peut pas lire message (chiffrement)
- Mallory ne peut pas modifier le message (car le message est signé par Alice)

Liens externes

- GPG (Wikibook)
- GNU Privacy Guard
- The GNU Privacy Guard (en anglais)
- OpenPGP
- RFC 4880 : OpenPGP Message Format
- Les fonctions de hachage cryptographiques (Wikibook)

From:
https://linuq.org/ - **LinuQ: Logiciels libres à Québec**

Permanent link:
https://linuq.org/logiciels/gnupg

Last update: **2019/02/14 09:08**