

# Administration des systèmes d'exploitation Sécurité

Etienne Papegnies

Université d'Avignon et des Pays de Vaucluse

*etienne.papegnies@univ-avignon.fr*

2017

# Plan

- 1 Surface d'Attaque
- 2 Hashing
- 3 Chiffrement Asymétrique
- 4 MITM & HTTPS
- 5 Vulnérabilités
- 6 Veille Technologique
- 7 VPN
- 8 Sauvegarde
- 9 Éducation des Utilisateurs
- 10 Post Mortem
- 11 Conclusion / Paranoïa

## Ordinateur sans connexion Internet: quelle est la surface d'attaque?

- La surface d'attaque est un concept permettant d'évaluer le risque auquel est exposé un système informatique.
- Un ordinateur sans connexion Internet est dit "Air-Gapped"



Ordinateur sans connexion Internet:  
quelle est la surface d'attaque?

- La surface d'attaque est un concept permettant d'évaluer le risque auquel est exposé un système informatique.
- Un ordinateur sans connexion Internet est dit "Air-Gapped"



Les ports USB.

L'USB c'est cool:

- On branche une clef USB -> ça marche !
- On branche un clavier USB -> ça marche !
- Est-ce que une clef USB peut prétendre être un clavier ?
  - Ouaiip.



**(TS//SI//REL)** COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

08/05/08



**(TS//SI//REL)** CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The

Serveur connecté à internet, sans services.

- Les ports Physiques (USB etc)
- Le driver réseau
- La fonction de routage du Kernel

+ serveur SSH.

- Les ports Physiques (USB etc)
- Le driver réseau
- La fonction de routage du Kernel
- Le serveur SSH

Station de travail sous Windows avec un antivirus connectée à internet, avec un employé qui consulte Facebook

- Les ports Physiques (USB etc)
- Le driver réseau
- La fonction de routage du Kernel
- L'antivirus
- Le navigateur web

Pour analyser la surface d'attaque, vous devez:

- Noter tous les flux de données extérieures dans votre SI
- Recenser tout le matériel soumis à ces flux de données
- Recenser toute la couche logicielle soumis à ces flux de données



# Plan

- 1 Surface d'Attaque
- 2 Hashing**
- 3 Chiffrement Asymétrique
- 4 MITM & HTTPS
- 5 Vulnérabilités
- 6 Veille Technologique
- 7 VPN
- 8 Sauvegarde
- 9 Éducation des Utilisateurs
- 10 Post Mortem
- 11 Conclusion / Paranoïa

# Plan

- 2 Hashing
  - Hash Function
  - Cryptographic Hash Function
  - Password Hash Function

Fonction qui:

- prends en entrée des données de taille arbitraire
- fait correspondre une sortie de taille fixe
- est déterministe

```
#!/usr/bin/python -u
```

```
def hash_function(text):
```

```
    out = 0
```

```
    for c in text:
```

```
        out += ord(c)
```

```
    return out % 100
```

```
print hash_function("hello")    # -> 32
```

```
print hash_function("world")    # -> 52
```

```
print hash_function("!")        # -> 33
```

# Plan

## 2 Hashing

- Hash Function
- Cryptographic Hash Function
- Password Hash Function

# Introduction

- Une fonction de hachage avec les propriétés:
  - Est rapide à calculer quelque soit la taille de l'entrée
  - A un espace de sortie suffisamment large
  - Un petit changement dans l'entrée provoque une cascade de changements en sortie
  - En utilisant la sortie, il est difficile de re-cr  er l'entr  e
  - Si on a l'entr  e et la sortie, il est difficile de trouver une autre entr  e avec la m  me sortie

A terminal window titled 'ouroumov@Bloc: ~/Desktop' showing three SHA256 hash calculations. The first command is 'echo "Hello" | sha256sum' resulting in '66a045b452102c59d840ec097d59d9467e13a3f34f6494e539ffd32c1bb35f18'. The second is 'echo "Hello man!" | sha256sum' resulting in '8d22ae98896b86010d7ed75881f430a1c7363d9664effae105a202f05c954e05'. The third is 'echo "Hello man." | sha256sum' resulting in 'c50dd0c10b39f3a1e87f9623a2dcc37bb4e808e3d719fb7849edad76562bd2d7'. Each line is followed by a hyphen and a space.

```
ouroumov@Bloc: ~/Desktop
ouroumov@Bloc:~/Desktop$ echo "Hello" | sha256sum -
66a045b452102c59d840ec097d59d9467e13a3f34f6494e539ffd32c1bb35f18 -
ouroumov@Bloc:~/Desktop$ echo "Hello man!" | sha256sum -
8d22ae98896b86010d7ed75881f430a1c7363d9664effae105a202f05c954e05 -
ouroumov@Bloc:~/Desktop$ echo "Hello man." | sha256sum -
c50dd0c10b39f3a1e87f9623a2dcc37bb4e808e3d719fb7849edad76562bd2d7 -
ouroumov@Bloc:~/Desktop$
```

# Plan

## 2 Hashing

- Hash Function
- Cryptographic Hash Function
- Password Hash Function

Une fonction de hachage pour mots de passe doit:

- Avoir les propriétés d'une fonction de hachage cryptographique
- Utiliser un Sel concaténé avec le mot de passe
- Être configurable pour pouvoir consommer:
  - Une quantité de mémoire arbitraire
  - Un nombre de cycles CPU arbitraire

## BCrypt Hash Function, cost level 10

Password	Salt	Hash
PasswOrd	Q/AzxLshsyaAqptlgni74u	\$2a\$10\$Q/AzxLshsyaAqptlgni74uN5WQrGCW176CPbPSVqrt/pUNS7HW9tu
lolwhat	7JYaQZA9w/PGfv4C0ab920	\$2a\$10\$7JYaQZA9w/PGfv4C0ab920qmH.YFrQmucp1wqRfUEd3KHI/ty6dHm
lolwhat	02h4313J6Qgs/3daZ/iaze	\$2a\$10\$02h4313J6Qgs/3daZ/iaze9RJr3EIb1B6HZRX8zAWuP3TNKSY1zDu

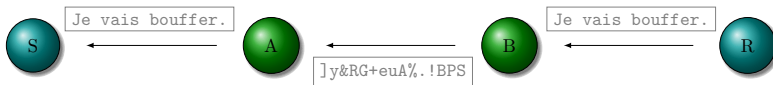
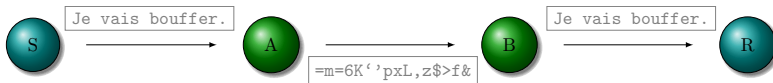
# Plan

- 1 Surface d'Attaque
- 2 Hashing
- 3 Chiffrement Asymétrique**
- 4 MITM & HTTPS
- 5 Vulnérabilités
- 6 Veille Technologique
- 7 VPN
- 8 Sauvegarde
- 9 Éducation des Utilisateurs
- 10 Post Mortem
- 11 Conclusion / Paranoïa

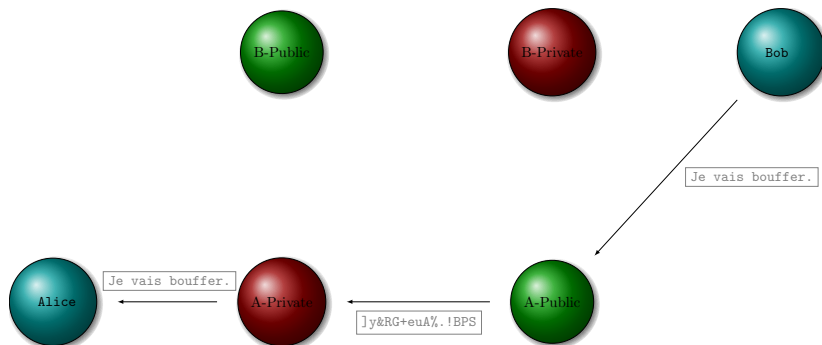


# Introduction

- Méthode de chiffrement a deux clefs
- Ce qui est chiffré avec une clef ne peut être déchiffré que par l'autre

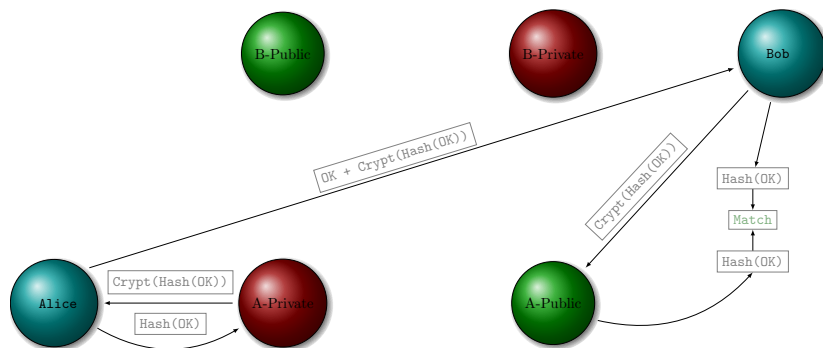


# Communication chiffrée de Bob vers Alice



- Bob est sûr que Alice est la seule à pouvoir lire le message
- Alice ne sait pas qui est l'auteur du message

# Réponse en clair de Alice avec Signature du message



- Alice envoie message en clair + hash chiffré par sa clef privée
- Bob déchiffre le hash de Alice, et calcule le hash de son côté

# Plan

- 1 Surface d'Attaque
- 2 Hashing
- 3 Chiffrement Asymétrique
- 4 MITM & HTTPS**
- 5 Vulnérabilités
- 6 Veille Technologique
- 7 VPN
- 8 Sauvegarde
- 9 Éducation des Utilisateurs
- 10 Post Mortem
- 11 Conclusion / Paranoïa

# Plan

- 4 MITM & HTTPS
  - MITM
  - HTTP
  - HTTPS

Le type au milieu.



Quelqu'un en position de MITM peut:

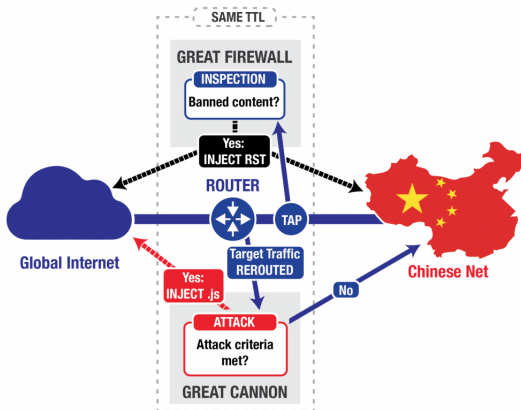
- Intercepter le trafic
- Modifier le trafic

# Plan

- 4 MITM & HTTPS
  - MITM
  - HTTP
  - HTTPS

# HTTP

- HTTP est ni authentifié, ni encrypté.
- Certains acteurs peu scrupuleux utilisent ça pour lancer des DDoS massifs





2017-05-03

# Administration des systèmes d'exploitation - Sécurité

└ MITM & HTTPS

└ HTTP

└ HTTP

## HTTP

- HTTP est ni authentifié, ni crypté.
- Ce défaut attire l'attention des cybercriminels et se pose le problème des DDoS massifs



► Ars Technica's article on China's "Great Cannon"

# Plan

- 4 MITM & HTTPS
  - MITM
  - HTTP
  - HTTPS

# HTTPS

- La version "sûre" de HTTP
- À la fois encrypté et authentifié
- Meilleur système actuel pour protéger le trafic, mais loin d'être idéal
- Depuis l'apparition de "Let's Encrypt", il n'y a plus d'excuse pour ne pas protéger le trafic de son site

# HTTPS: implémentation

- Crypto Asymétrique pour l'établissement de la connexion
- Utilisation de certificats contenant des clefs publiques
- Crypto symétrique pour le gros du trafic

## Administration des systèmes d'exploitation - Sécurité

└ MITM &amp; HTTPS

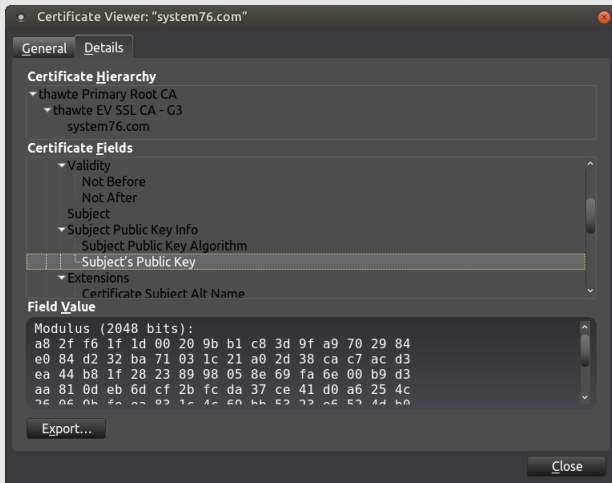
└ HTTPS

└ HTTPS: implémentation

HTTPS: implémentation

- Crypto Asymétrique pour l'établissement de la connexion
- Utilisation de certificats contenant des clés publiques
- Crypto symétrique pour le gros du trafic

► A nice technical analysis of what happens at the begining of an HTTPS connection



# HTTPS: Problèmes

- Basé sur une chaîne de confiance
  - Grand nombre de CAs "root"
  - Contrôle d'un CA 'root' permet de MITM le trafic
  - Certains CAs ne sont pas dignes de confiance
- Approche souvent trop tolérante car
  - Les entreprises ont de l'inertie
  - Sécurité moyenne > Pas de sécurité

# Plan

- 1 Surface d'Attaque
- 2 Hashing
- 3 Chiffrement Asymétrique
- 4 MITM & HTTPS
- 5 Vulnérabilités**
- 6 Veille Technologique
- 7 VPN
- 8 Sauvegarde
- 9 Éducation des Utilisateurs
- 10 Post Mortem
- 11 Conclusion / Paranoïa

# Types de vulnérabilités

Il existe de nombreux types de vulnérabilités, mais il est pratique de les lister par type d'impact possibles:

- Denial Of Service
- Information Leakage
- Man In The Middle
- Privilege Escalation
- Remote Code Execution

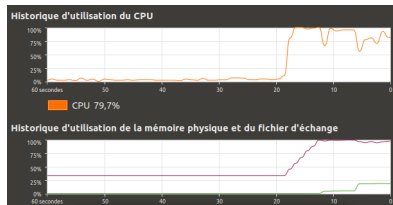


# Plan

## 5 Vulnérabilités

- Denial Of Service
- Information Leakage
- Man In The Middle
- Privilege Escalation
- Remote Code Execution

:( ) { : | : & } ; :



# Plan

## 5 Vulnérabilités

- Denial Of Service
- **Information Leakage**
- Man In The Middle
- Privilege Escalation
- Remote Code Execution

# Exemple: Heartbleed

## Heartbleed

SERVER, ARE YOU STILL THERE?  
IF SO, REPLY "HAT" (500 LETTERS).



...a connection. Jake requested pictures of deer.  
User Meg wants these 500 letters: HAT. Lucas  
requests the "missed connections" page. Eve  
(administrator) wants to set server's master  
key to "14835038534". Isabel wants pages about  
snakes but not too long". User Karen wants to  
change account password to "CoHoBaSt". User



HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User



...a connection. Jake requested pictures of deer.  
User Meg wants these 500 letters: HAT. Lucas  
requests the "missed connections" page. Eve  
(administrator) wants to set server's master  
key to "14835038534". Isabel wants pages about  
snakes but not too long". User Karen wants to  
change account password to "CoHoBaSt". User



2017-05-03

# Administration des systèmes d'exploitation - Sécurité

## └─ Vulnérabilités

### └─ Information Leakage

#### └─ Exemple: Heartbleed

Exemple: Heartbleed



► Heartbleed: Ars Technica Article

► Heartbleed: xkcd explanation

# Plan

## 5 Vulnérabilités

- Denial Of Service
- Information Leakage
- **Man In The Middle**
- Privilege Escalation
- Remote Code Execution

## Exemple: Superfish

Lenovo's Massive Fuckup



2017-05-03

# Administration des systèmes d'exploitation - Sécurité

- └ Vulnérabilités

- └ Man In The Middle

- └ Exemple: Superfish

Exemple: Superfish

Lenovo's Masske Facing



► Why I don't like Lenovo



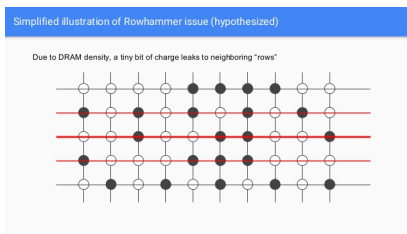
# Plan

## 5 Vulnérabilités

- Denial Of Service
- Information Leakage
- Man In The Middle
- Privilege Escalation
- Remote Code Execution

# Exemple: Rowhammer

## Physical attack on DRAM memory



- En changeant les valeurs d'une page de mémoire répétitivement, il est possible de faire changer la valeur de Bits dans la page d'à côté.
- Cela peut permettre à un programme tournant avec des privilèges utilisateurs d'obtenir les privilèges de root.

2017-05-03

# Administration des systèmes d'exploitation - Sécurité

└─ Vulnérabilités

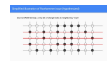
└─ Privilege Escalation

└─ Exemple: Rowhammer

► Project Zero writeup on Rowhammer

Exemple: Rowhammer

Physical attack on DRAM memory



- ◆ En changeant les valeurs d'une page de mémoire adjacente, il est possible de faire basculer le contenu de bits de la page d'origine.
- ◆ Cela peut permettre à un programmeur d'accéder avec des privilèges arbitraires d'une des pages de mémoire.

# Plan

## 5 Vulnérabilités

- Denial Of Service
- Information Leakage
- Man In The Middle
- Privilege Escalation
- Remote Code Execution

## Exemple: Shellshock

24 Septembre 2014

Une des pires vulnérabilités de tout les temps.



- Permet d'exécuter du code arbitraire sur des serveurs web
- Dans les jours suivant l'annonce, un scan automatique massif d'internet était en cours pour compromettre des serveurs

2017-05-03

# Administration des systèmes d'exploitation - Sécurité

└─ Vulnérabilités

└─ Remote Code Execution

└─ Exemple: Shellshock

Exemple: Shellshock

24 Septembre 2014

Une des plus vulnérabilités de tout les temps.



- Permet d'exécuter du code arbitraire sur des serveurs web
- Dans les jours suivant l'annonce, on a vu le monde se masser d'internet états en cours pour compromettre des serveurs

► [Ars Technica's article on Shellshock](#)

# Plan

- 1 Surface d'Attaque
- 2 Hashing
- 3 Chiffrement Asymétrique
- 4 MITM & HTTPS
- 5 Vulnérabilités
- 6 Veille Technologique
- 7 VPN
- 8 Sauvegarde
- 9 Éducation des Utilisateurs
- 10 Post Mortem
- 11 Conclusion / Paranoïa

# Veille Technologique

Si vous êtes responsable de la sécurité, il faut surveiller l'actualité.



## US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

- Surveillez les sources d'informations
  - CERT
  - Ars Technica
  - Slashdot
  - Podcasts de sécurité ( [twit.tv/sn](http://twit.tv/sn) )
- Utilisez l'analyse de votre surface d'attaque pour poser des alertes
  - Sur le matériel que vous utilisez
  - Sur les logiciels que vous utilisez



2017-05-03

# Administration des systèmes d'exploitation - Sécurité

## └ Veille Technologique

## └ Veille Technologique

### Veille Technologique

Si vous êtes responsable de la sécurité, il faut surveiller l'actualité.



**US-CERT**

UNITED STATES CYBERSECURITY PROGRAM

- Suivez les sources d'informations
  - » CERT
  - » Ars Technica
  - » Slashdot
  - » Podcasts de sécurité (mishka/ps)
- Utilisez l'analyse de votre surface d'attaque pour poser des alertes
  - » Sur le matériel que vous utilisez
  - » Sur les logiciels que vous utilisez

▶ US-CERT

▶ FR-CERT

▶ Slashdot

▶ Ars Technica

▶ Hackernews

▶ Weekly "Security Now" podcast by Steve Gibson

▶ Threatpost

▶ Brian Krebs's Website

▶ Google's "Project Zero" team

# Plan

- 1 Surface d'Attaque
- 2 Hashing
- 3 Chiffrement Asymétrique
- 4 MITM & HTTPS
- 5 Vulnérabilités
- 6 Veille Technologique
- 7 VPN**
- 8 Sauvegarde
- 9 Éducation des Utilisateurs
- 10 Post Mortem
- 11 Conclusion / Paranoïa

# Introduction

- Un VPN est un réseau "Logique" qui vient se superposer sur un réseau physique
- Permet
  - De traverser un NAT
  - De contourner le problème de l'adressage dynamique
  - De connecter multiples sites séparés de manière sécurisée



# Plan

- 1 Surface d'Attaque
- 2 Hashing
- 3 Chiffrement Asymétrique
- 4 MITM & HTTPS
- 5 Vulnérabilités
- 6 Veille Technologique
- 7 VPN
- 8 Sauvegarde**
- 9 Éducation des Utilisateurs
- 10 Post Mortem
- 11 Conclusion / Paranoïa

# Plan

- 8 Sauvegarde
  - Miroir Vs Sauvegarde
  - Règle 3-2-1

# Miroir Vs Sauvegarde

## Miroir

- Copies à l'identique d'un fichier / dossier
- Lorsqu'un fichier est modifié, chaque copie est modifiée

## Sauvegarde

- Ne permet pas la suppression de fichiers
- Définit un point de restauration dans le temps

# Plan

- 8 Sauvegarde
  - Miroir Vs Sauvegarde
  - Règle 3-2-1

# Règle 3-2-1

- 3 Copies
- 2 Supports différents
- 1 copie dans un endroit différent



# Plan

- 1 Surface d'Attaque
- 2 Hashing
- 3 Chiffrement Asymétrique
- 4 MITM & HTTPS
- 5 Vulnérabilités
- 6 Veille Technologique
- 7 VPN
- 8 Sauvegarde
- 9 Éducation des Utilisateurs**
- 10 Post Mortem
- 11 Conclusion / Paranoïa

Pour réduire les risques, éduquez les utilisateurs de vos systèmes:

- Politique de sécurité que les employés doivent signer
- Formation sur les concepts de base de la sécurité
- Renforcement négatif par retenue de salaire
- Exercices:
  - Saupoudrer le parking avec des clefs USBs
  - Organiser des fausses campagnes de Fishing

# Plan

- 1 Surface d'Attaque
- 2 Hashing
- 3 Chiffrement Asymétrique
- 4 MITM & HTTPS
- 5 Vulnérabilités
- 6 Veille Technologique
- 7 VPN
- 8 Sauvegarde
- 9 Éducation des Utilisateurs
- 10 Post Mortem**
- 11 Conclusion / Paranoïa

Si un incident de sécurité se produit, il est nécessaire d'y répondre.

- Évaluer l'impact de l'incident
- Arrêter les machines compromises
- Faire des images des machines compromises
- Réinstaller les machines compromises
- Si la source du problème est identifiée et qu'une mitigation existe, l'appliquer
- Restaurer les données depuis une sauvegarde
- Remettre en route les services
- Contacter la police
- Si des clients sont affectés, contacter les clients
- Si les données personnelles des clients sont affectés, contacter la CNIL

# Plan

- 1 Surface d'Attaque
- 2 Hashing
- 3 Chiffrement Asymétrique
- 4 MITM & HTTPS
- 5 Vulnérabilités
- 6 Veille Technologique
- 7 VPN
- 8 Sauvegarde
- 9 Éducation des Utilisateurs
- 10 Post Mortem
- 11 Conclusion / Paranoïa

# Même les paranos ont des ennemis

## Questions:

- Avez vous déjà téléchargé et exécuté un fichier .exe venant d'un site HTTP ?
- Si quelqu'un vole votre ordinateur portable là dessus, quelles infos il obtien ?
- Si quelqu'un a accès à votre ordinateur un jours ou vous êtes pas là, qu'est-ce qu'il peut faire ?

## Administration des systèmes d'exploitation - Sécurité

## └ Conclusion / Paranoïa

## └ Même les paranos ont des ennemis

Même les paranos ont des ennemis

Questions:

- Avez-vous déjà téléchargé et exécuté un fichier .exe venant d'un site HTTP ?
- Si quelqu'un vole votre ordinateur portable le dimanche, quelles infos il obtient ?
- Si quelqu'un a accès à votre ordinateur un jour ou deux êtes-vous là, qu'est-ce qu'il peut faire ?

- "Evil Maid" attack
- Disk Encryption is important