Administration des systèmes d'exploitation
Sécurité

Etienne Papegnies

Université d'Avignon et des Pays de Vaucluse

etienne.papegnies@univ-avignon.fr

2017

Plan

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 ?
  - Ouaip.

TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-I

ANT Product Data

(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

COTTONMOUTH - 1

(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

Plan

Fonction qui:

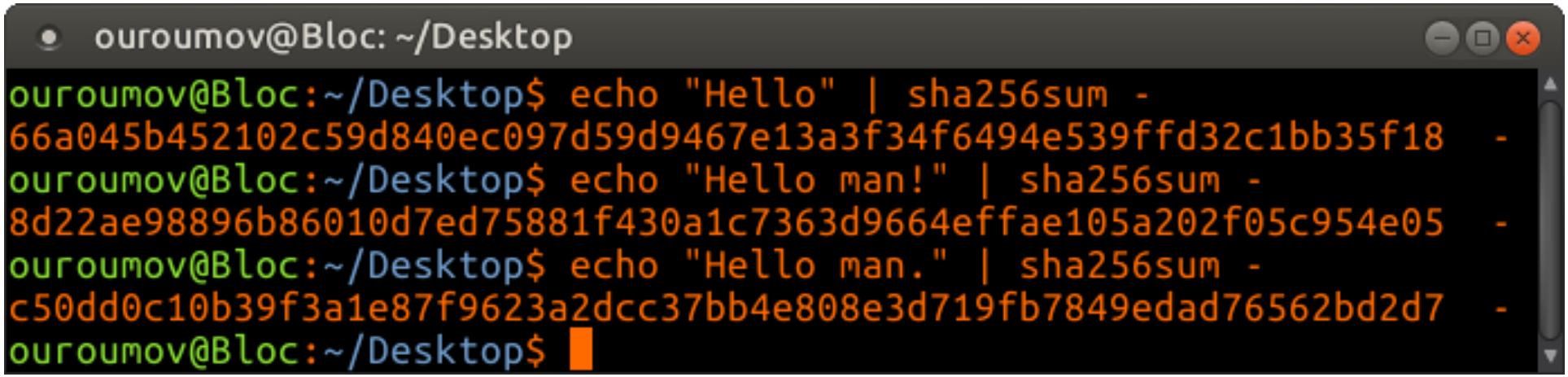
- prends en entrée des données de taille arbitraire
- fait correspondre une sortie de taille fixe
- est déterministe

```
#! /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

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-créer l'entrée
  - Si on a l'entrée et la sortie, il est difficile de trouver une autre entrée avec la même sortie



Plan

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

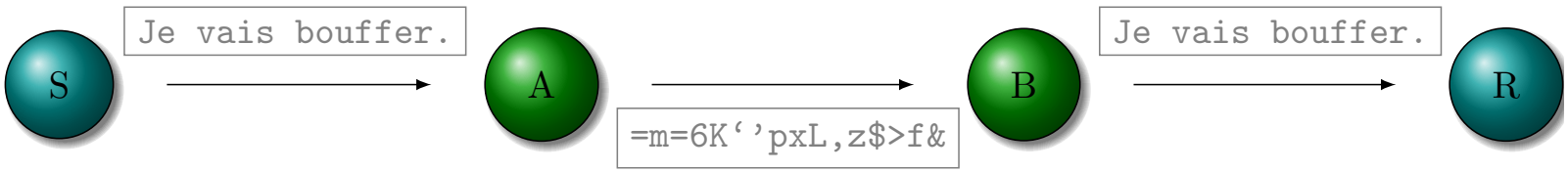
BCrypt Hash Function, cost level 10

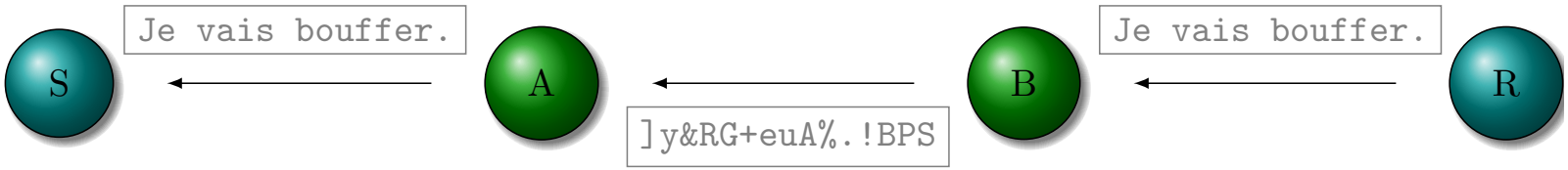
Password	Salt	Hash
Passw0rd	Q/AzxLshsyaAqptlgni74u	$2a$10$Q/AzxLshsyaAqptlgni74uN5WQrGCW176CPbPSVqrt/pUNS7HW9tu
lolwhat	7JYaQZA9w/PGfv4C0ab92O	$2a$10$7JYaQZA9w/PGfv4C0ab92OqmH.YFrQmucp1wqRfUEd3KHI/ty6dHm
lolwhat	02h4313J6Qgs/3daZ/iaze	$2a$10$02h4313J6Qgs/3daZ/iaze9RJR3EIblB6HZRX8zAWuP3TNKSY1zDu

Plan

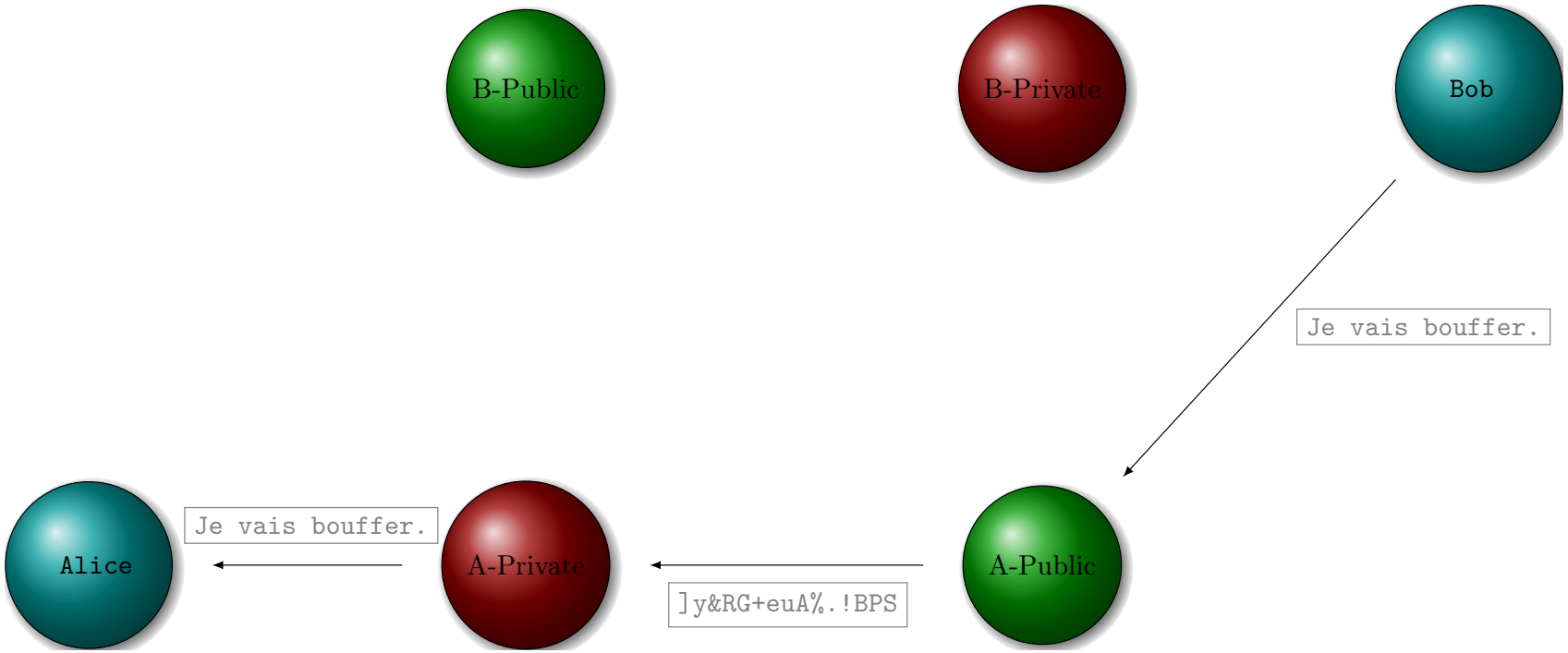
Introduction

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



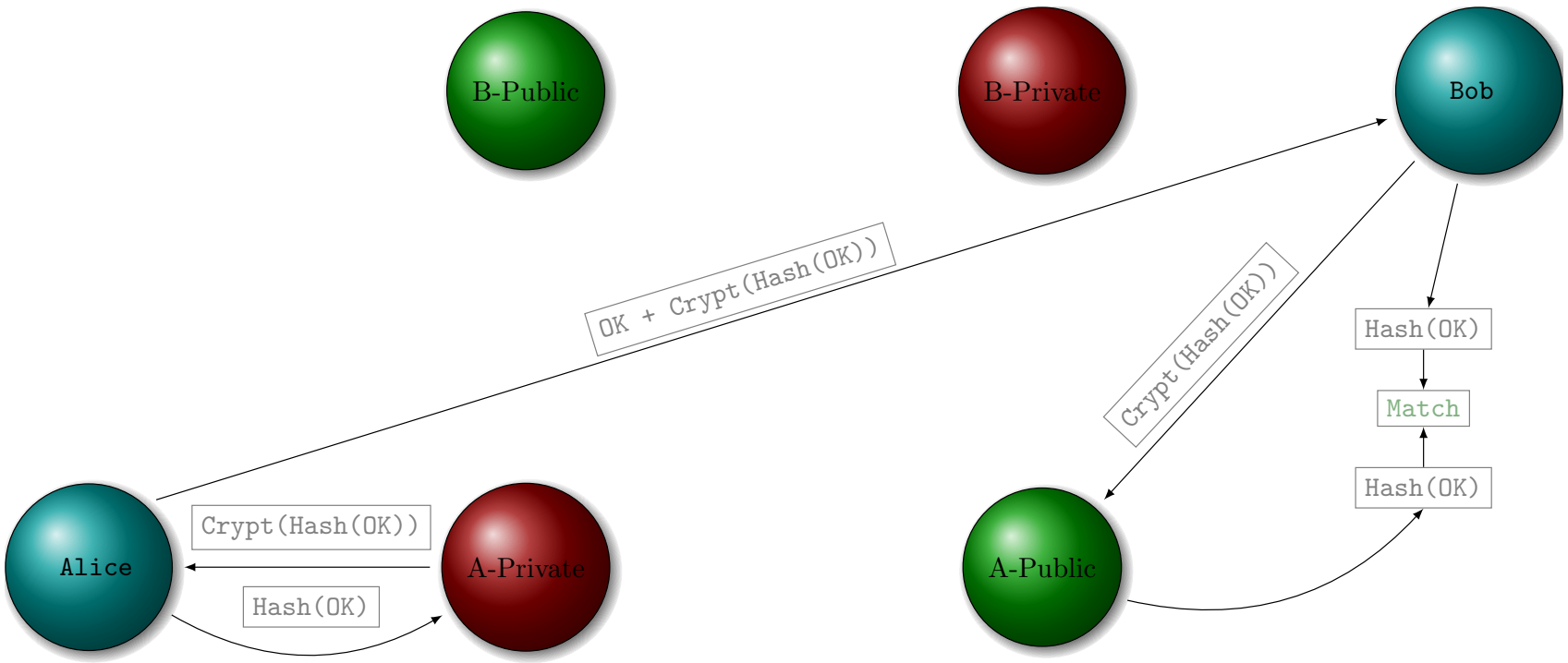


Communication chiffrée de Bob vers Alice



- 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

Plan

Le type au millieu.

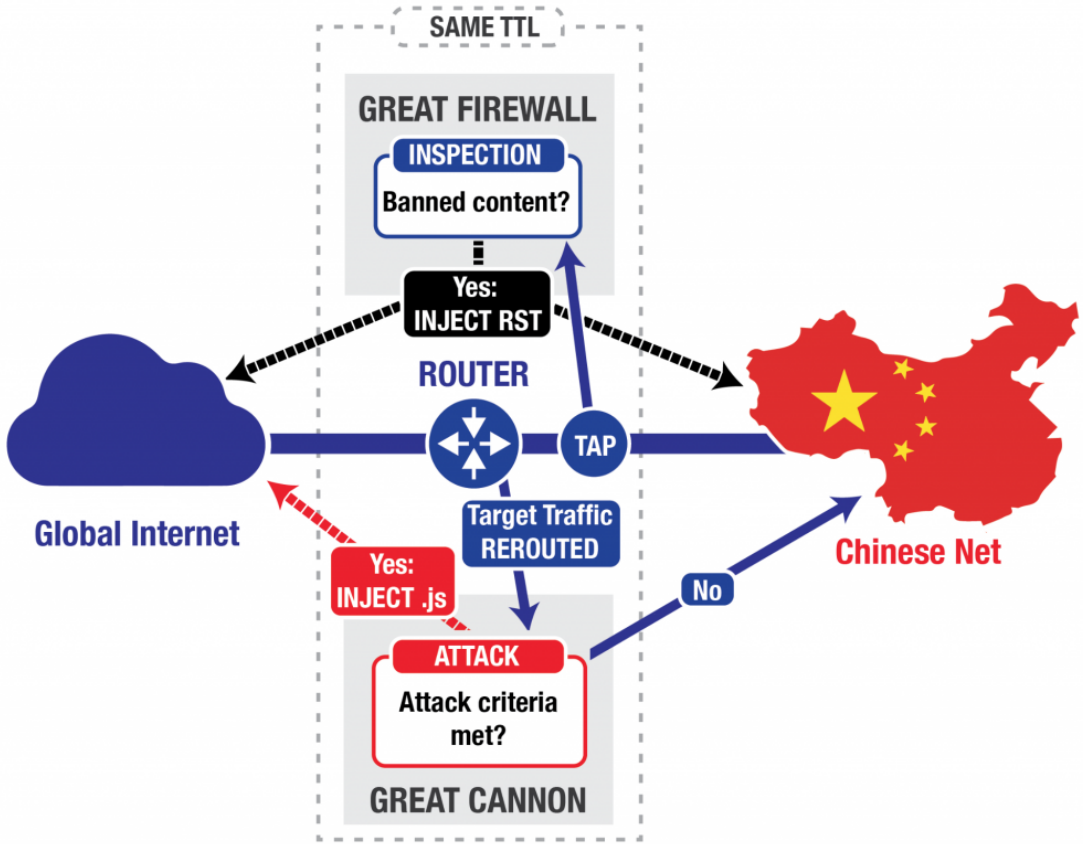
Quelqu'un en position de MITM peut:

- Intercepter le traffic
- Modifier le traffic

Plan

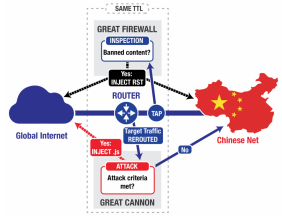
HTTP

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



HTTP

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



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

Plan

HTTPS

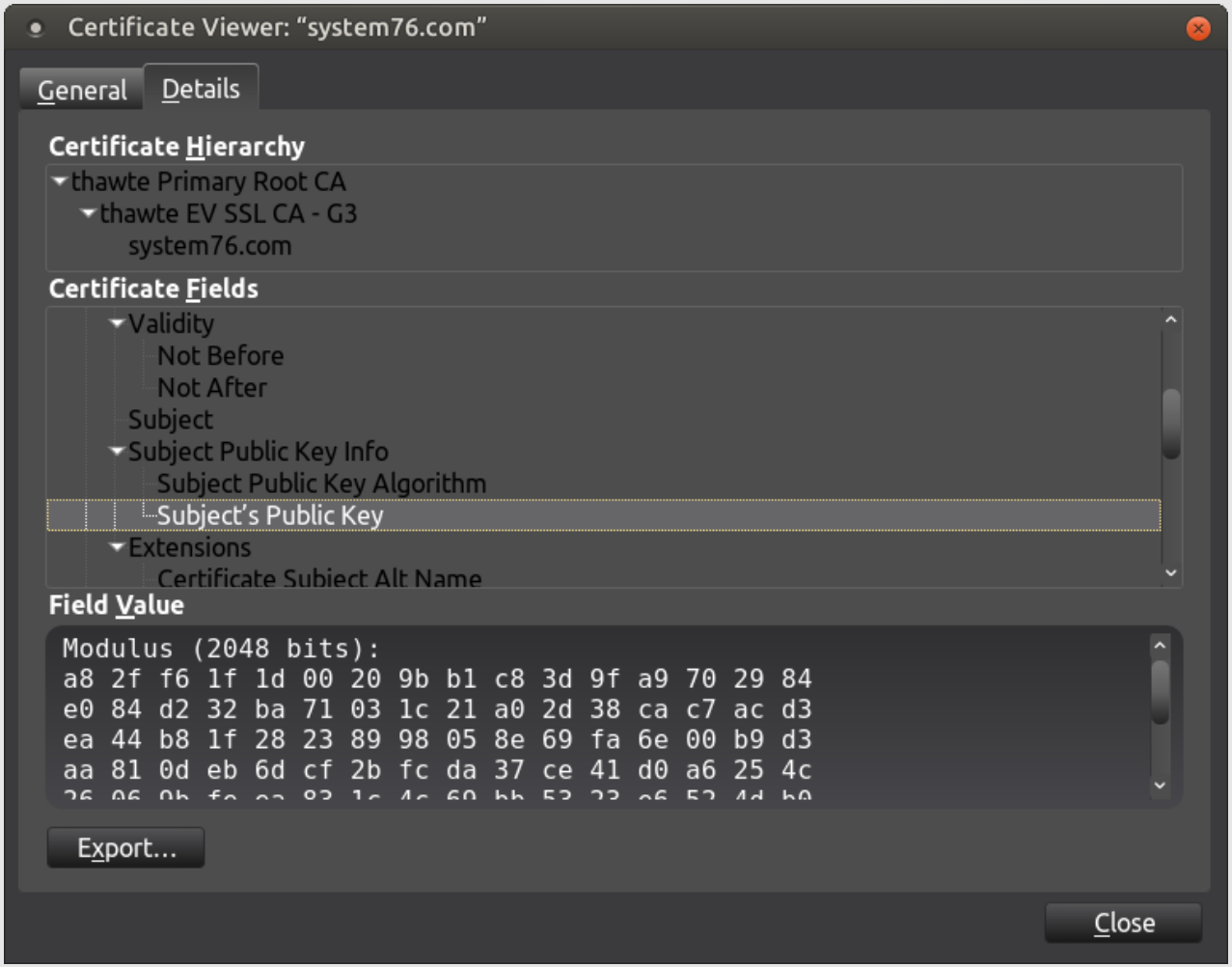
- La version "sûre" de HTTP
- À la fois encrypté et authentifié
- Meilleur système actuel pour protéger le traffic, mais loin d'être idéal
- Depuis l'apparition de "Let's Encrypt", il n'y a plus d'excuse pour ne pas protéger le traffic de son site

HTTPS: implémentation

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

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

▸ 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 traffic
  - 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

Types de vulnérabilités

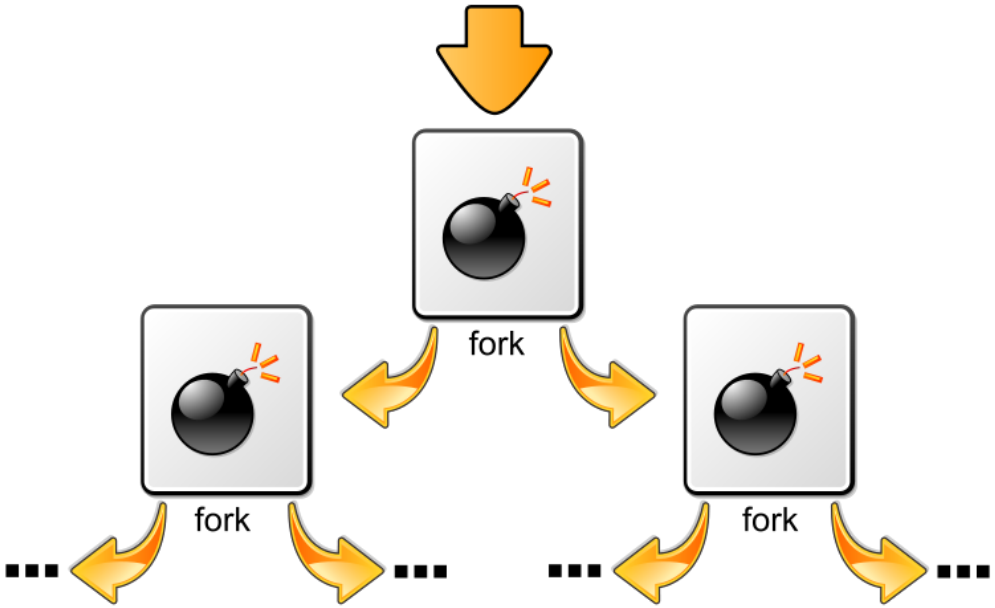
Il existe de nombreux types de vulnérabilités, mais il est pratique de les lister par type d'impact possibles:

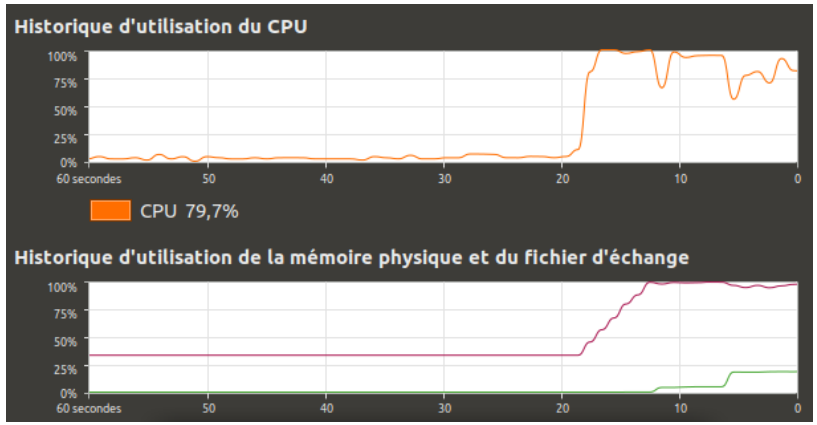
- Denial Of Service
- Information Leakage
- Man In The Middle
- Privilege Escalation
- Remote Code Execution

Plan

Exemple: Fork Bomb

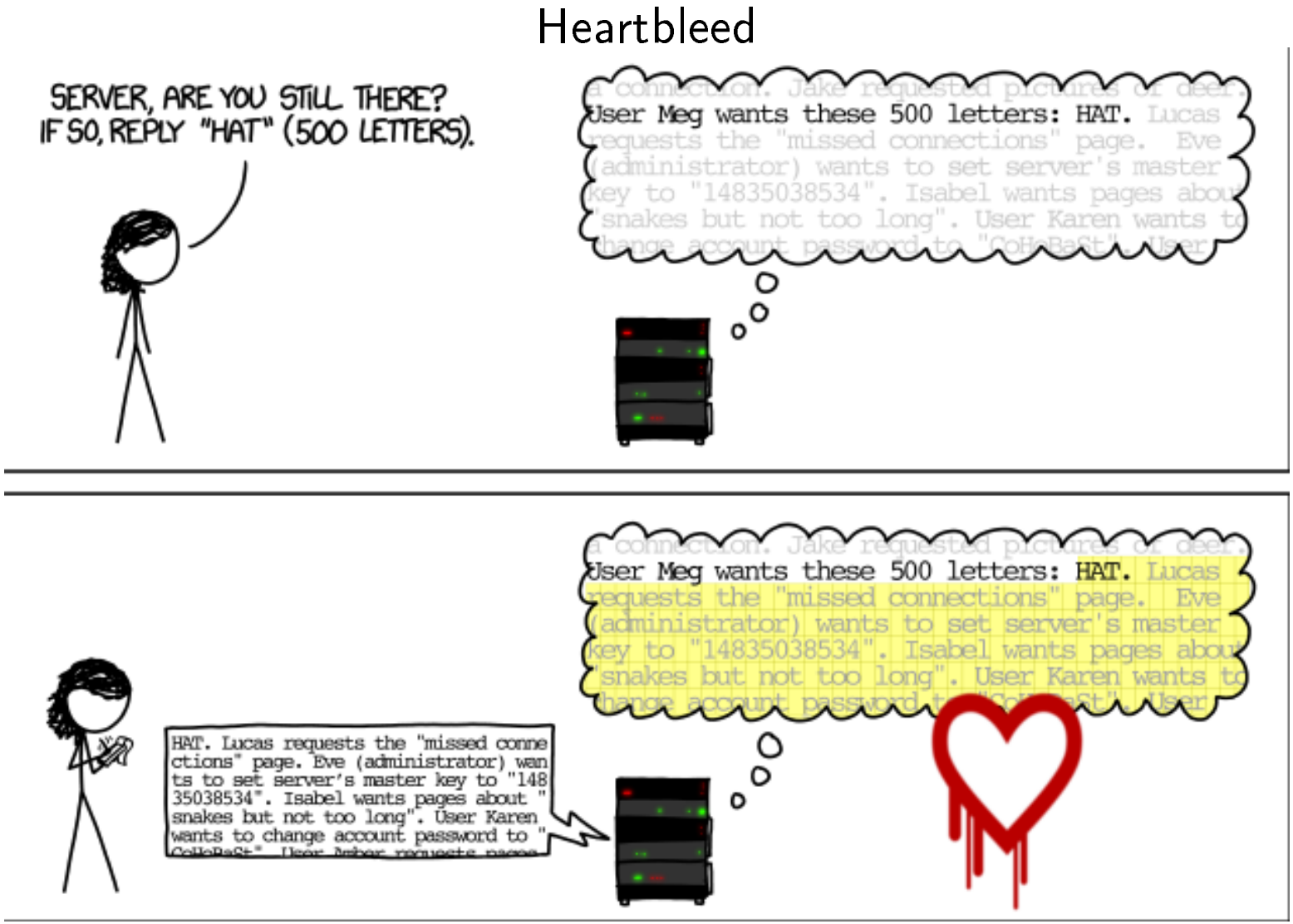
```
:(){ :|:& };:
```

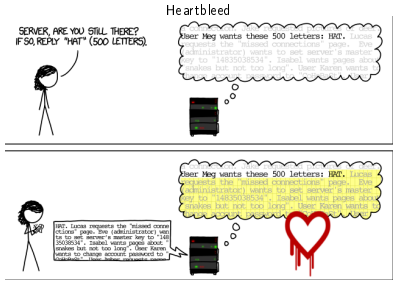




Plan

Exemple: Heartbleed





- Heartbleed: Ars Technica Article
- Heartbleed: xkcd explanation

Plan

Exemple: Superfish

Lenovo's Massive Fuckup

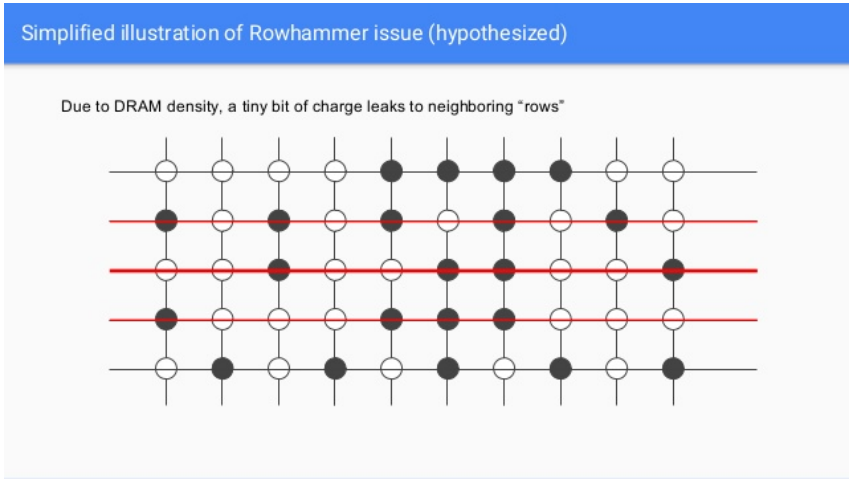
Lenovo's Massive Fuckup

- Why I don't like Lenovo

Plan

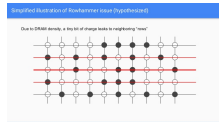
Exemple: Rowhammer

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.

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.

- Project Zero writeup on Rowhammer

Plan

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

Administration des systèmes d'exploitation - Sécurité
Vulnérabilités
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

- Ars Technica's article on Shellshock

Plan

Veille Technologique

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

- Surveillez les sources d'informations
  - CERT
  - Ars Technica
  - Slashdot
  - Podcasts de sécurité (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

└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)
- 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

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'addressage dynamique
  - De connecter multiples sites séparés de manière sécurisée

Plan

Plan

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

Règle 3-2-1

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

Plan

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

Si un incident de sécurité se produit, il est nécéssaire 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

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 dessuite, 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 ?

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 dessuite, 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 ?

- "Evil Maid" attack
- Disk Encryption is important