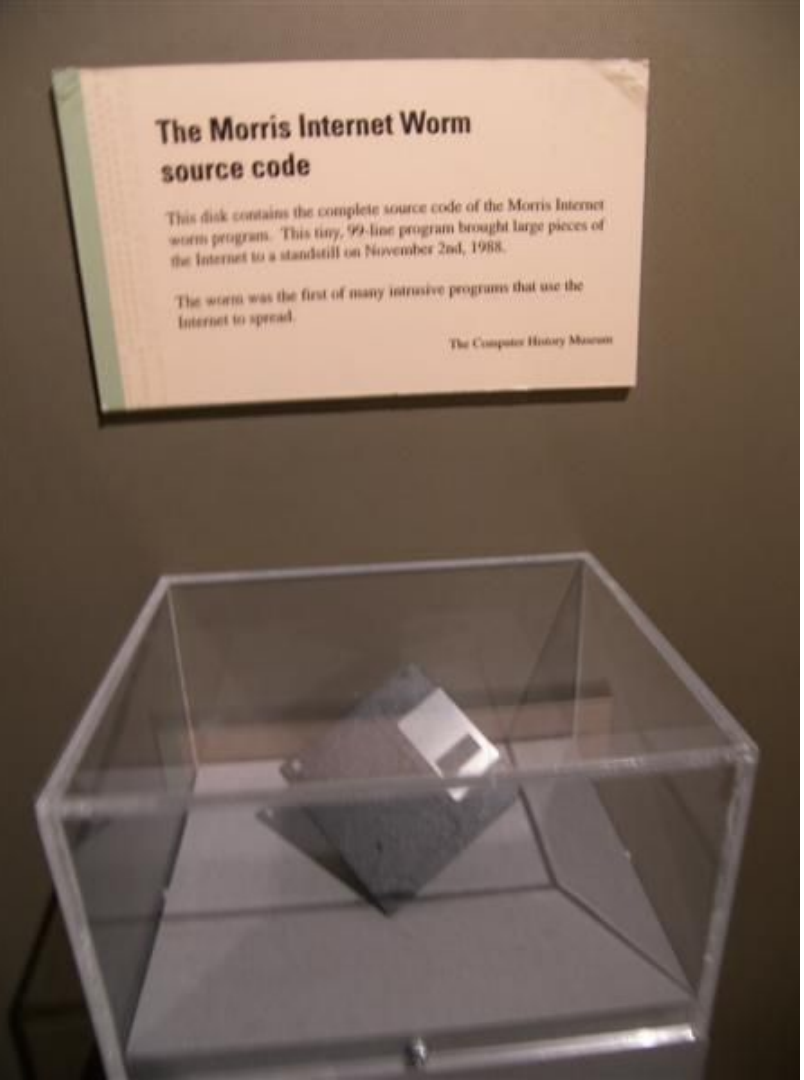
HiTeMa
Sécurité Applicative

Introduction

Lu. 15 Oct. 2018 - PHELIZOT Yvan

Quelques exemples



Morris Worm Shutdown the internet

Tech

FOLLOW MASHABLE >

22-year-old man loses $24 million worth of bitcoins in apparent scam

3 milliards de comptes piratés

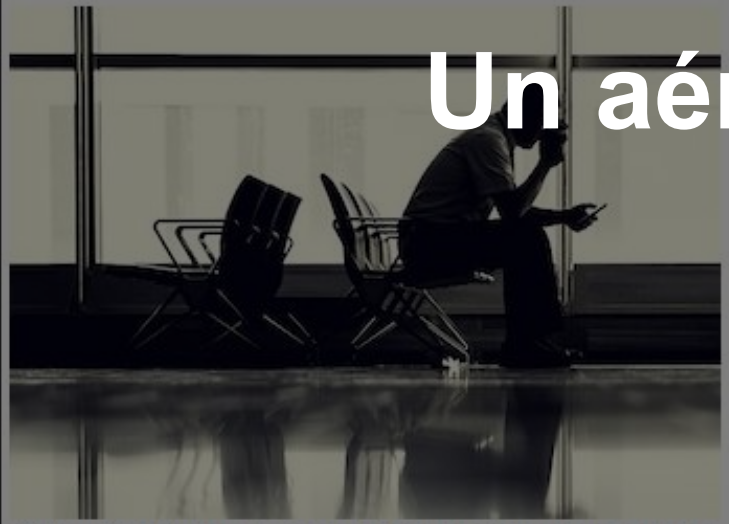
All 3 Billion Yahoo Accounts Were Affected by 2013 Attack

September 17, 2018

Bristol airport hit with ransomware attack

Robert Abel Content Coordinator/Reporter

Follow @RobertJAAbel



Bristol airport recently recovered from a ransomware attack which prompted the airport to take flight information screens offline in an effort to keep the attack contained.

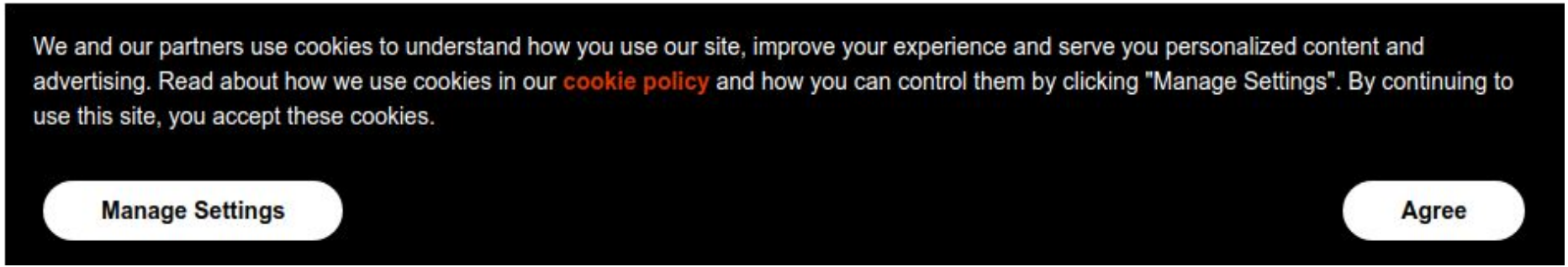
Un aéroport paralysé

The Bristol airport in the UK recently recovered from a ransomware [illegible] prompted the airport to take flight information screens offline in an effort to keep the attack contained.

This action was taken on Friday and the screens were back in operation by Sunday in “key locations” including departures and arrivals while officials are working to restore the entire site, an airport spokesperson told the BBC.

“We believe there was an online attempt to target part of our administrative systems and that required us to take a number of applications offline as a precautionary measure, including the one that

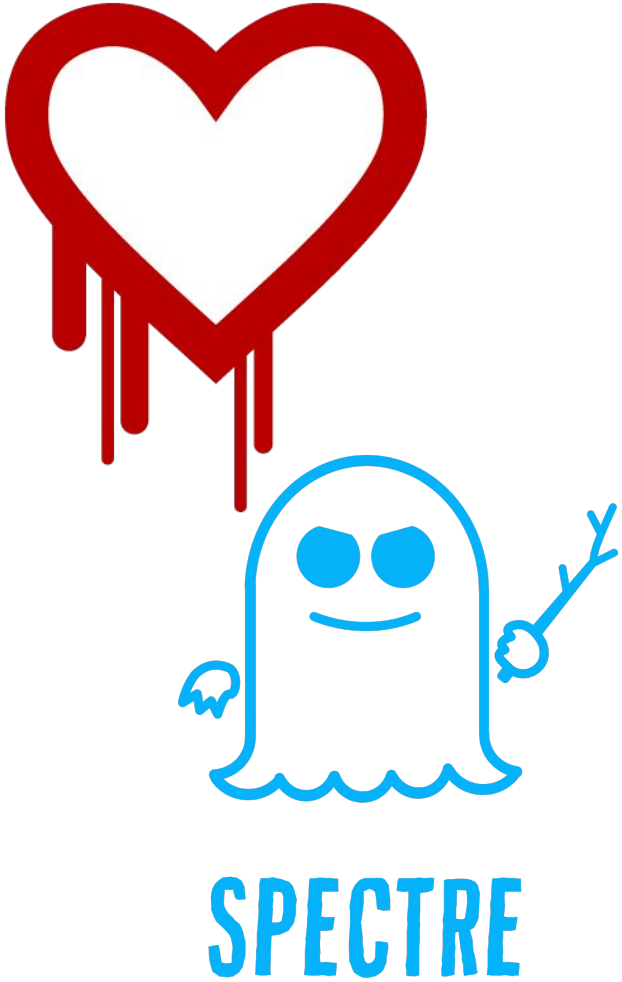
La sécurité, c’est aussi ça...




Your personal files are encrypted
Info
Your important files were encrypted on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.
Encryption was produced using unique public key RSA-4096 generated for this computer. To decrypt files, you need to obtain private key.
The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; the server will destroy the key within 72 hours after encryption completed. After that, nobody and never will be able to restore files.
Your files will be lost without payment on:

Ransomware

Heartbleed
POODLE
Meltdown
Spectre



Oups...

Ukrainian bloggers use social media to track Russian soldiers fighting in east

Using pictures and status updates as evidence, amateur investigators say they are gathering proof that the Kremlin is actively involved in conflict. RFE/RL reports

The Fifth Dimension Operations

- Land, Sea, Air, Space and Information
- Cyberwarfare
- “Foreign Policy magazine puts the size of China's "hacker army" at anywhere from 50,000 to 100,000 individuals.” (Wikipedia)
- North Korea: Bureau 121
- Syrian Electronic Army
- USA: NSA
- ...

Présentation du programme

- 15 octobre
  - Introduction
  - Architecture
- 16 octobre
  - AppSec Web
- 16 novembre
  - Mise en pratique
- 7 décembre
  - AppSec mobile
- 8 janvier
  - Secure Coding
- 9 janvier
  - Organisation
- 3 Mars
  - Mise en pratique

Qui suis-je?

- PHELIZOT Yvan
- Coach Craft chez Arolla
- yvan.phelizot@arolla.fr
- yvan.phelizot@gmail.com
- Secure Coding/Secure by (DD-)Design

Quelques instructions

Site à consulter : https://cotonne.github.com/appsec-hitema

A installer pour demain

- OWASP Zap: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- WebGoat **7:** https://github.com/WebGoat/WebGoat/releases/tag/7.1

Comment ça va se passer?
Poser des questions
Tester et explorer
Challenger
Contrôle
...

Qu’est-ce que la sécurité?

Sécurité (nom féminin)

- Situation dans laquelle **quelqu'un**, **quelque chose** n'est exposé à aucun **danger**, à aucun **risque**, en particulier d'agression physique, d'accidents, de vol, de détérioration
- Situation de quelqu'un qui se sent à l'abri du danger, qui est rassuré.
- Absence ou limitation des **risques** dans un domaine précis

Dictionnaire “Larousse”

Security?

The state of being free from danger or **threat**.

Protection against malice, mistakes and mischance

Oxford Dictionary

Sécurité === Sureté?

Pourquoi la sécurité, c’est important?

Pourquoi la sécurité, c’est important?

Entreprise

- Dégâts sur l’image (Yahoo!)
- Coûts
- Chantage (Sony 2011s)
- Arrêt

Pourquoi la sécurité, c’est important?

Pays

- Perte de démocratie (Dernières élections aux USA)
- Perte financière
- Souveraineté (cyberdéfense)
- Organisme d’Importance Vitale (OIV)

Pourquoi la sécurité, c’est important?

Individu

- Impact financier (carte de crédit, …)
- Impact humain (régime totalitaire)
- Vol d’identité
- Extorsion

Que veut-on protéger?

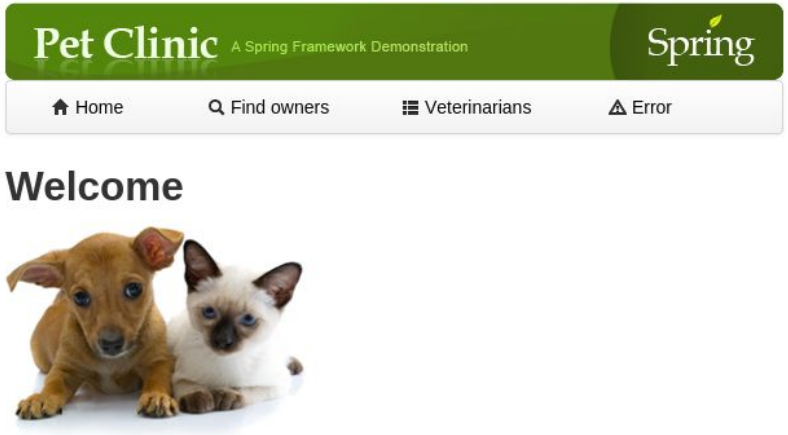
Protection des actifs(assets)

- Données clientes
- Secrets de production
- Echanges confidentielles
- Contrats
- Argent
- Réputation
- ...

Pet Clinic

- Clinique vétérinaire locale
- Site web grand public
- Prise de rendez-vous
- Carnet animal
- Paiement
- Formulaire de contact des vétérinaires

⇒ Actif?



spring by Pivotal

InfoSec?
AppSec?

InfoSec

- Sécurité de l’information
- Processus
- Definition from US law: Practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information
- Équilibre entre efficacité opérationnelle et mise en oeuvre de la politique de sécurité

⇒ Large éventail de menaces

AppSec

- Securité Applicative
- Définition ISO 27034 (Guide ISO sur la sécurité applicative):

  « La sécurité applicative est un **processus** effectué pour appliquer des contrôles et des mesures aux applications d'une organisation afin de gérer le **risque** de leur utilisation ».

- "measures taken to improve the security of an application often by finding, fixing and preventing **security vulnerabilities**" (Wikipedia 2018)
- Architecture, design, développement, test, déploiement, ...

  ⇒ On s'intéresse à l'application

Objectifs de la sécurité de l’information

Objectifs de la sécurité : CIA

CONFIDENTIALITY

INTEGRITY

AVAILABILITY

Objectifs de la sécurité : extension

- Parkenin hexad : confidentiality, availability, integrity, possesion, authenticity, utility
- Privacy

⇒ Modèle pour penser et discuter les concepts sur la sécurité

Confidentialité?
Exemple?

Confidentialité

- Capacité à protéger nos données de lecture non autorisées
- Confidentiality === Privacy?
- Exemples?
- Cas d’échec
  - Perte d’une clé USB
  - Interception d’une communication
  - Affichage d’une information (voulue ou non)

Chiffrer/To crypt

Chiffrement

Principe de Kerchoffs

Chiffrement symétrique

Chiffrement asymétrique

- Clé publique/Clé privée

Fonction de hachage et Signature

Principe de Kerchoffs

Algorithme

- Minimiser la quantité de secret
- Système non cassable, indéchiffrable

Chiffrement symétrique

m

c = E(k, m)
= m ⊕ k

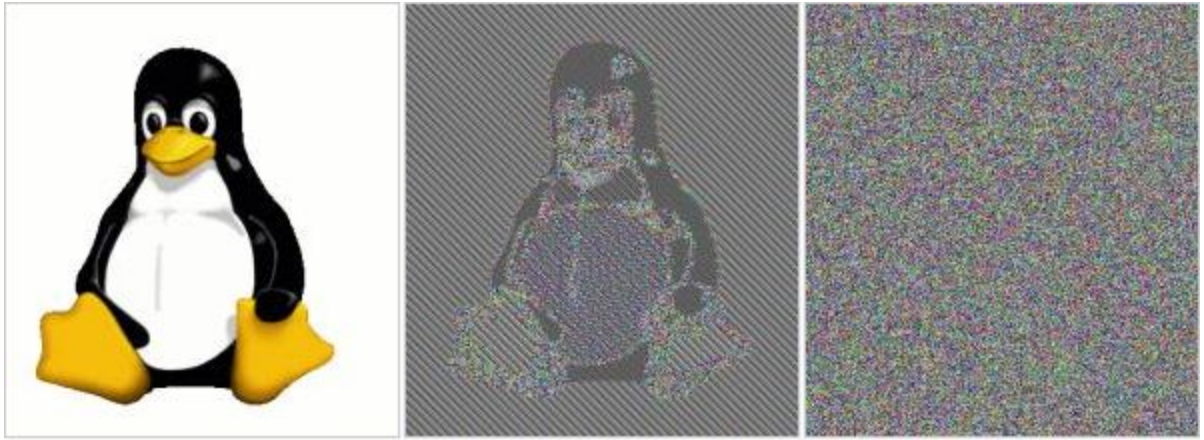
m = D(k, c)
= (m⊕k)⊕k

Chiffrement symétrique

Configuration

- Chiffrement symétrique
  - Choix de l'algorithme? ROT13? Vigenère? DES? 3DES? AES?
  - Taille de la clé?
- Chiffrement asymétrique
  - Choix de l'algorithme? RSA? EC?
  - Taille de la clé? 128, 256, 512, 1024, …?
  - Génération des clés? (PRNG)
- Choix des blocs? ECB? CBC? OFB?
- Fonction de hachage
  - Algorithme? CRC32? MD5? SHA1? SHA-512?
  - Avec ou sans sel?

ECB



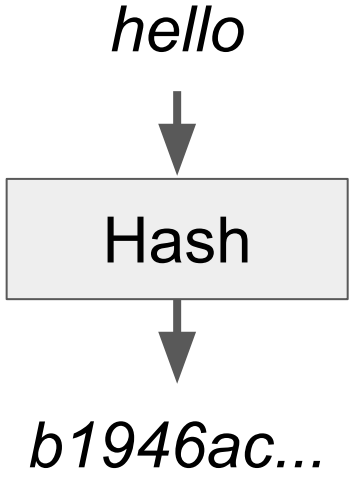
Original image | Encrypted using ECB mode | Modes other than ECB result in pseudo-randomness

Fonction de hachage

- Calcule une empreinte

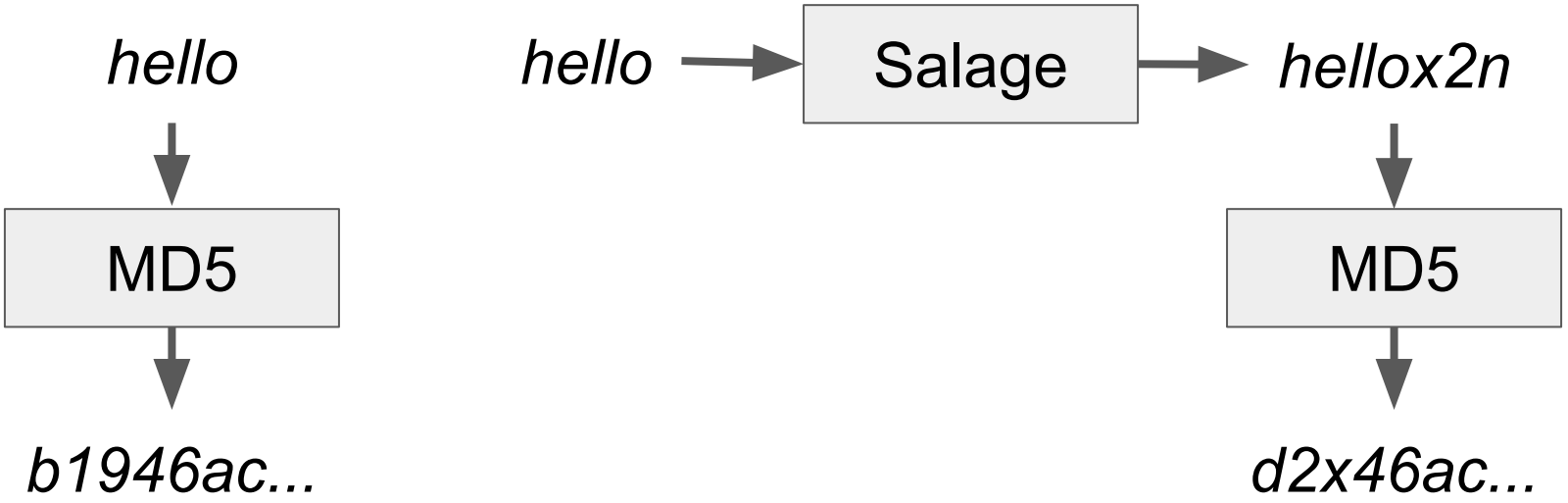
Propriétés:

- Résistance à la pré-image
- Résistance à la seconde pré-image
- Résistance aux collisions



Exemple de défense : SEL

- Collision/Rainbow table
- Solution : ajout d’un sel au hash



Attaques possibles

- **Algorithme perso**
- Fréquences
- Brute-force
- Texte chiffré seul
- Texte clair connu
- Texte clair choisi
- Texte chiffré choisi
- Injection d’erreurs
- Canaux cachés

Intégrité?
Exemple?

Intégrité

- Capacité à empêcher qu'une donnée soit modifiée par une personne non autorisée ou d'une façon non voulue
- Non seulement empêcher les modifications mais aussi être capable de revenir dans un état précédent
- Auditabilité/Accountability
- Prise de décision?
- Exemples
  - Introduction dans un système
  - Injection d'erreurs lors d'une transaction bancaire

Authentification

- Authentification : confirmer l’identité de l’utilisateur ou de l’entité
- Autorisation : donner (to grant) les droits d’accès aux ressources d’un système (fichiers, processus, …)
- Authentification ⇒ Autorisation

Authentification

- Quelque chose que l’on sait : mot de passe, question secrète, ...
- Quelque chose que l’on a : token d’authentification, téléphone, ...
- Quelque chose que l’on est : biométrie

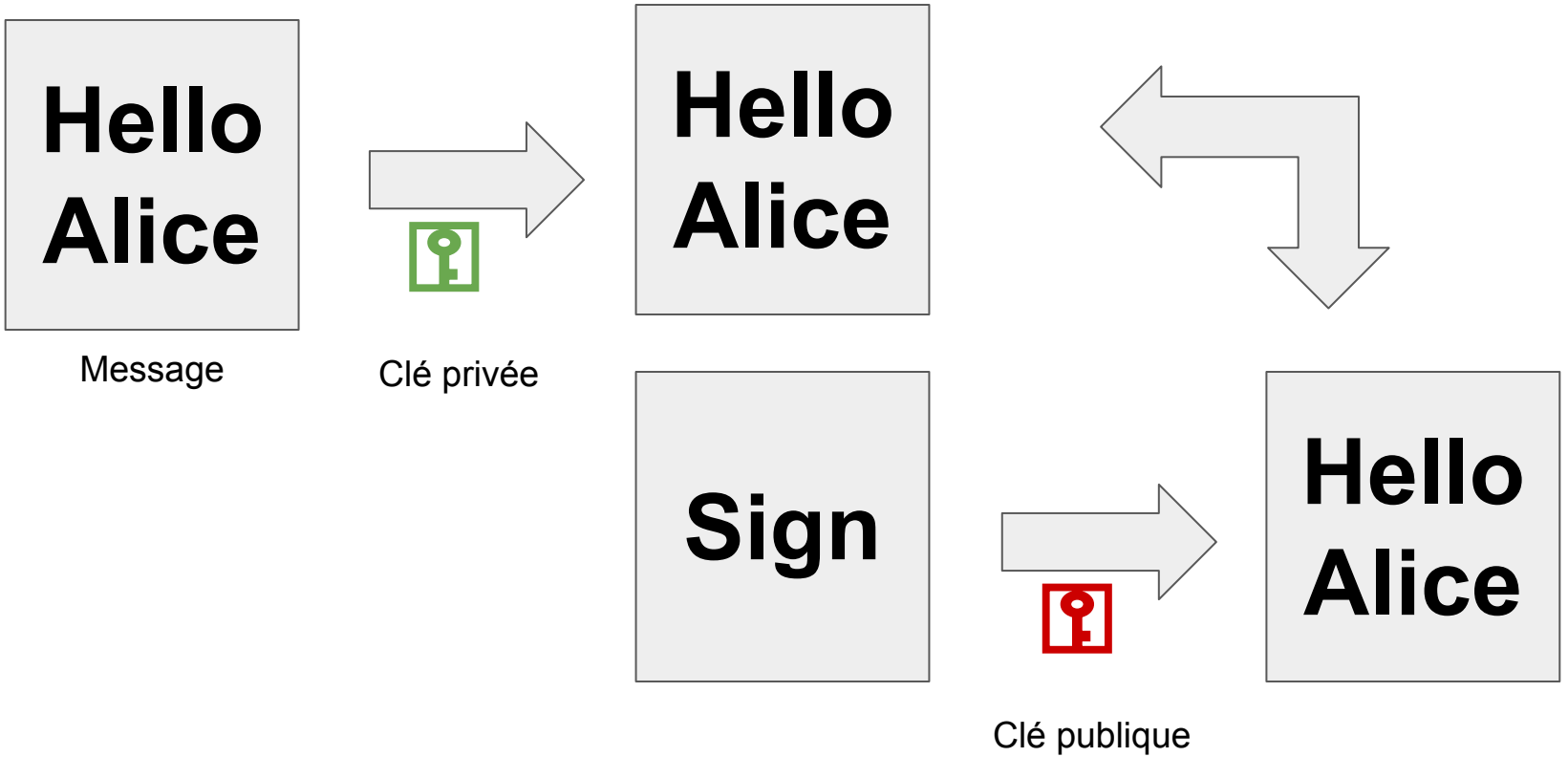
Non-répudiation

S’assurer qu’une action ne peut être remise en cause, que c’est bien la personne qui a fait l’action qui en est à l’origine

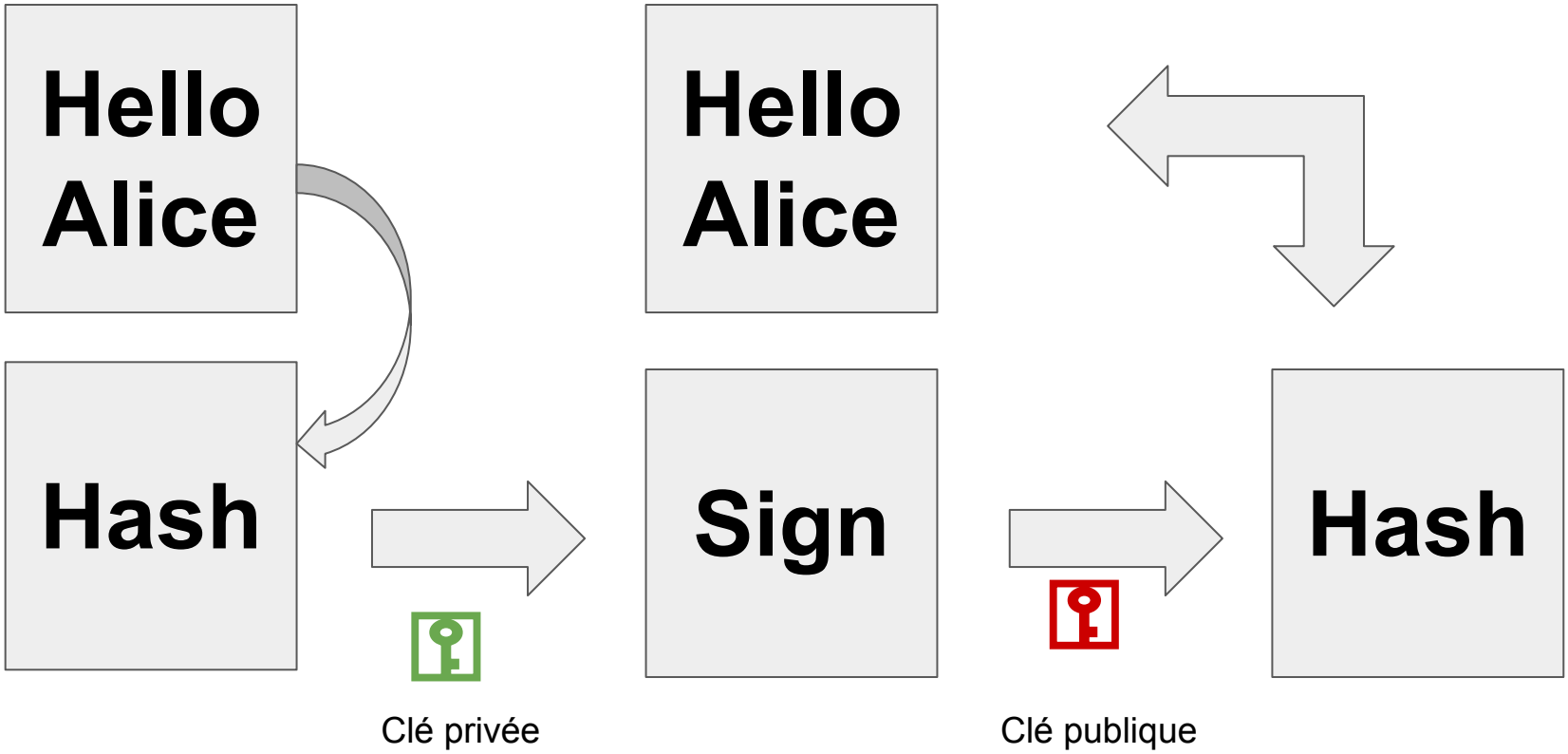
Problèmes associés

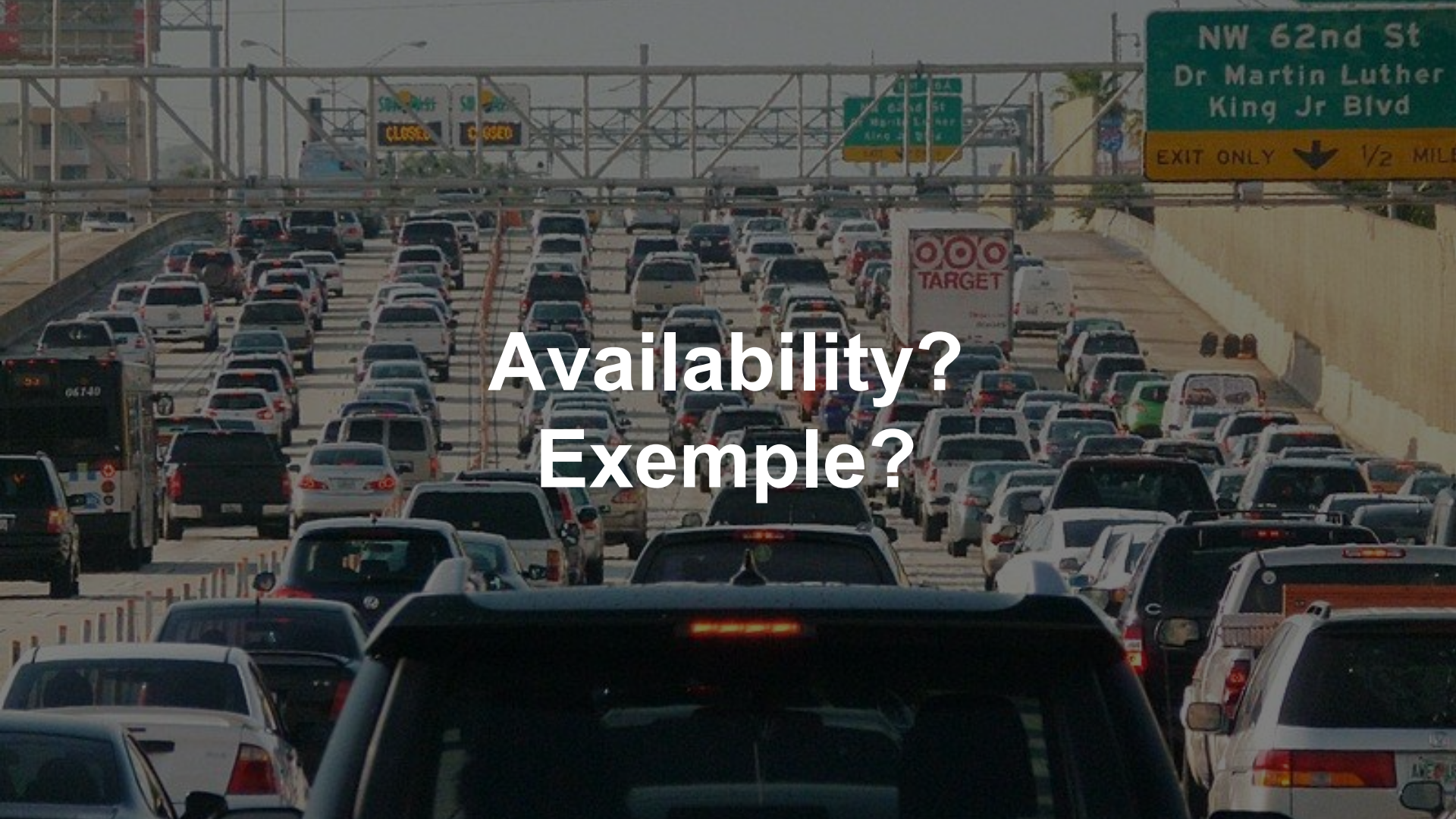
- Paiements faits mais refusés
- Contestation de propos

Signature


Hello Alice
Message
Clé privée
Hello Alice
Sign
Hello Alice
Clé publique

Signature


Hello Alice
Hash
Clé privée
Hello Alice
Sign
Clé publique
Hash



Availability?
Exemple?

Disponibilité

- Capacité à avoir accès aux données
- Exemples
  - DoS : Denial of Service
  - DDoS: Distributed Denial of Service

Ok, donc je ferme tout?

The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts.
Gene Spafford - Createur du ver Morris

Comment s’est possible ?

Vulnérabilité

- Bug ou fonctionnalité utilisable par un attaquant pour avoir accès à un actif
- Défaut
  - Volontaire: backdoor
  - Conceptuel : fonctionnalité voulue
  - Bug
- Gestion des vulnérabilités

Attaques?

Attaque/Exploit

- Action d’utiliser une vulnérabilité pour obtenir un actif
- Exploit: un logiciel exploitant une vulnérabilité

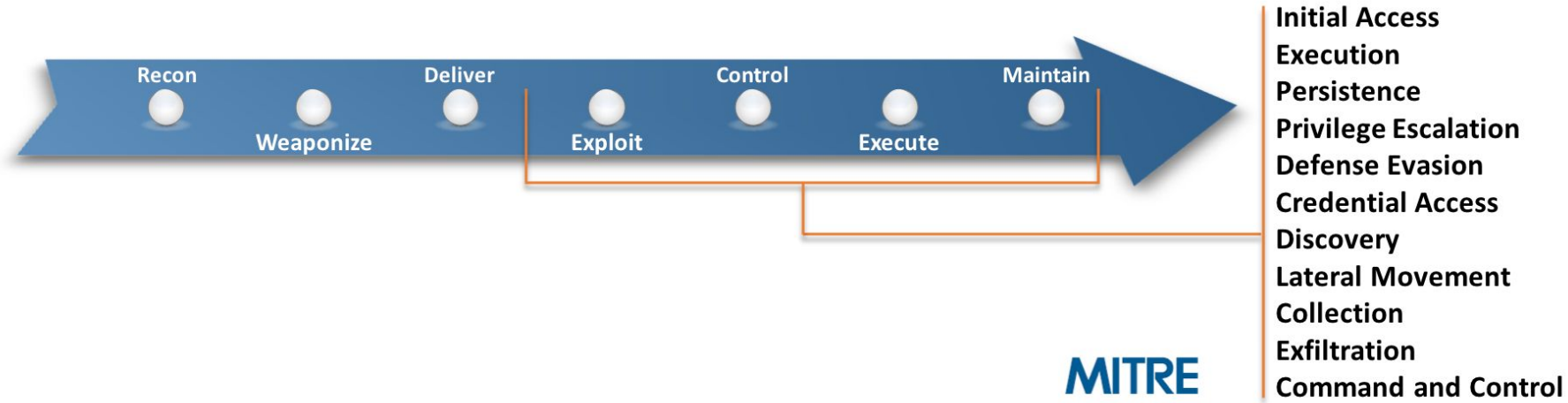
Exemple : SQL Injection & SQLMap

Des attaques complexes

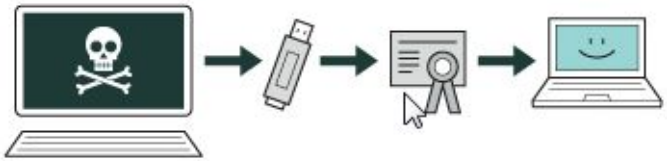
- APT: Advanced Persistent Threat
- Furtif
- Continu
- Sophistiqué

MITRE ATT&CK

- MITRE Adversarial Tactics, Techniques & Common Knowledge



UPDATE FROM SOURCE



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

Stuxnet

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't

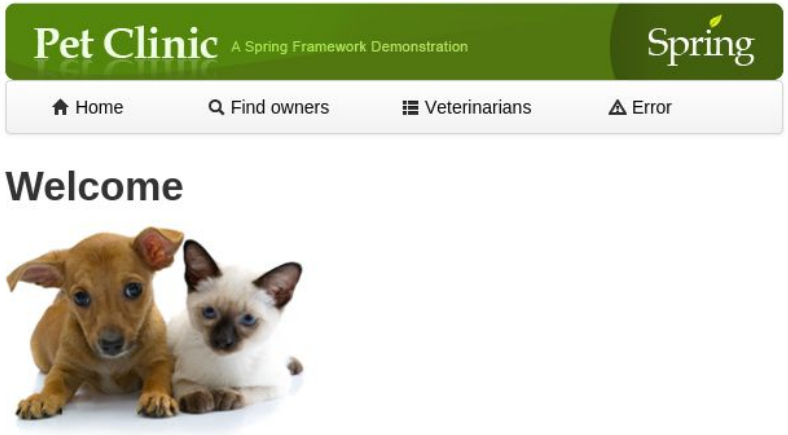
5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do

Pet Clinic

Revenons à notre clinique

Connaissez-vous des attaques?

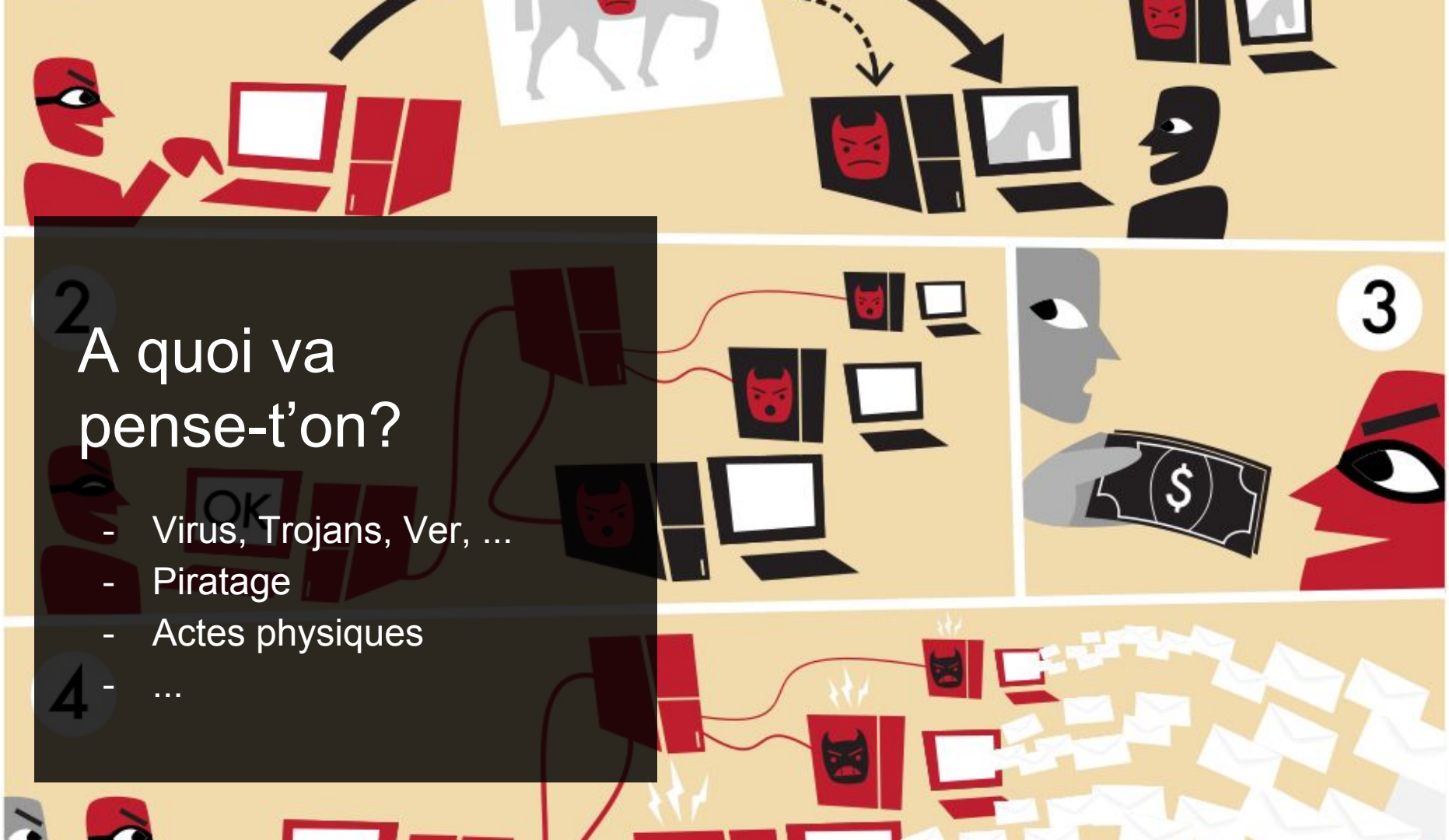


spring by Pivotal

Menaces?

A quoi va pense-t'on?

- Virus, Trojans, Ver, ...
- Piratage
- Actes physiques
- ...



Menaces

1. Action de menacer ; parole, comportement par lesquels on indique à quelqu'un qu'on a l'intention de lui nuire, de lui faire du mal, de le contraindre à agir contre son gré
2. Signe, indice qui laisse prévoir quelque chose de dangereux, de nuisible
3. Délit qui consiste à faire connaître à quelqu'un son intention, notamment verbalement ou par écrit, image ou tout autre moyen de porter atteinte à sa personne.

Larousse

Threat?

A statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not done.

A ***person*** or ***thing*** likely to cause **damage** or danger.

https://en.oxforddictionaries.com/definition/threat

Qui me menace? (Threat actor typology)

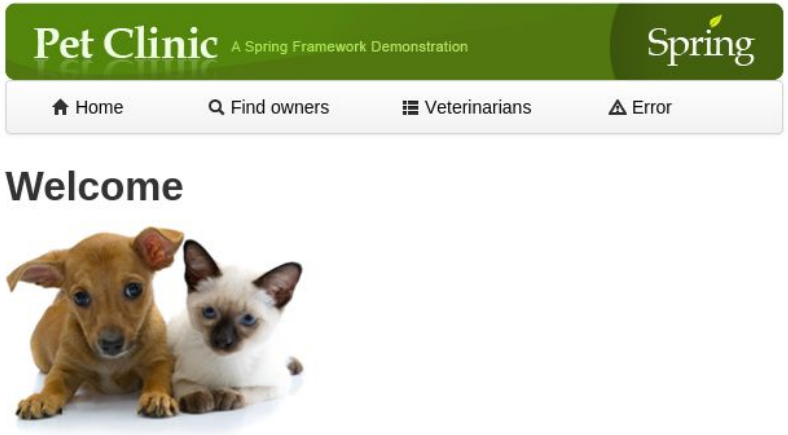
- Criminels (extortions (ransomware), voleurs (transactions bancaires), fraudeurs, scam, …),
- Hacktivists : hack + activists
- Script kiddies
- Terrorists
- Acteurs institutionnels (état, entreprise)
- Ancien employé
- Chercheurs

Bon, est-ce que je peux être attaqué par la Corée du Nord?

Pet Clinic

Revenons à notre clinique

Qui pourrait attaquer notre site?



spring by Pivotal

Qu’est-ce qu’on peut faire ?

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

— Sun Tzu, The Art of War

Qui? Threat Intelligence

- Tactiques : méthodologies, outils, …
- Techniques
- Opérations : analyse des organisations
- Stratégique : but et plan d’attaques
- Advanced Persistent Threat
- Collectes d’informations (HoneyPot, analyse Virus, …)

QQOQCP menaces

- Qui?
  - Pirate, ...
- Quoi?
  - Attaques physiques, sur un réseau, ondes, …
- Où?
  - Sur les points d’entrée
- Quand?
  - Au plus mauvais moment
- Comment?
  - Fonction de l’environnement
- Pourquoi?
  - Fun, Profit, Gloire, Vengeance, ...

Threat analysis/Threat modeling

- Connaître les ennemis
- Identifier les scénarios d’attaque
- Les prioriser
- Définir comment réagir

Limites?

Pour avoir un risque, il faut une menace et une vulnérabilité

Risque : vulnérabilité x probabilité⇒ conséquences

Gestion ⇒ Pilotage par les risques

- Éviter: éliminer, abandonner ou ne pas le rencontrer
- Réduire: Atténuer, traiter
- Partager: transférer (outsourcing/assurance)
- Prendre en charge (accepter et budgétiser)

Equilibre Coût / Conséquence

Gestion du risque

Identifier les actifs

Identifier les menaces

Évaluer les faiblesses sur les actifs

Evaluer les risques

Gérer les risques

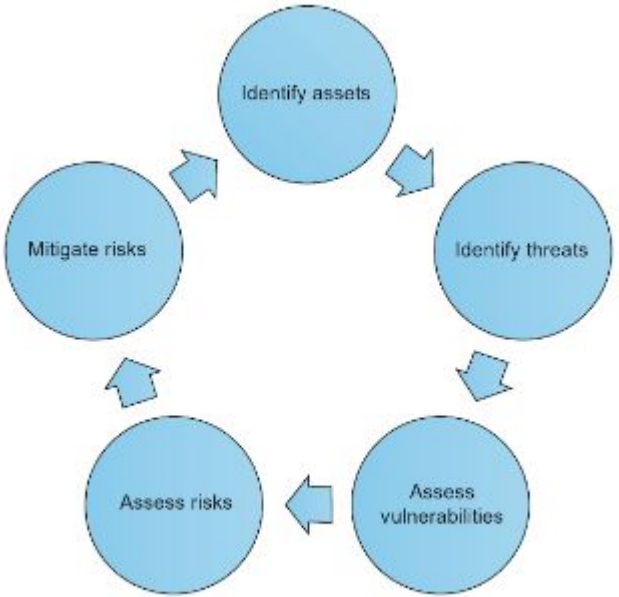


FIGURE 1.4

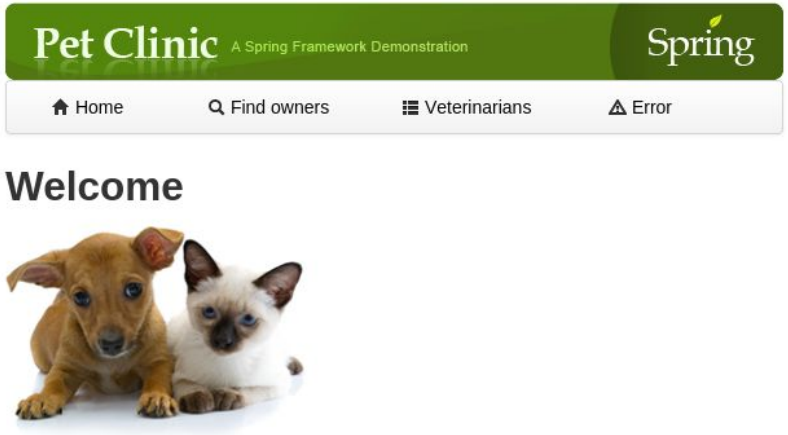
The risk management process.

Pet Clinic

Revenons à notre clinique

Quels risques ?

Quelles réponses?



spring by Pivotal

Quand est-on “sécurisé”?

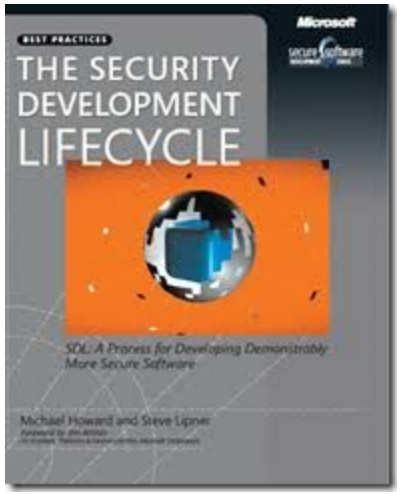
Limites

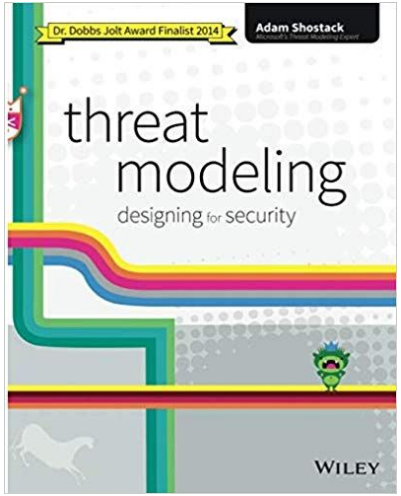
- Sécurisé à un moment
- Sécurisé à chaque niveau
- Sécurisé globalement

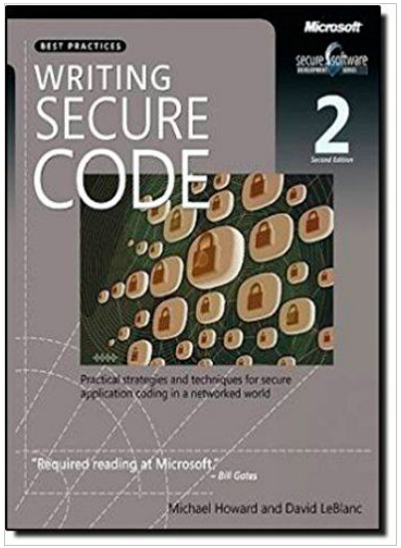
Ressources

- Standford CSS155 : computer & network security - https://crypto.stanford.edu/cs155/lectures/
- Google Online Security Blog: https://security.googleblog.com/
- Schneier on Security: https://www.schneier.com/
- OWASP Blog: https://owasp.blogspot.com/

Ressources


BEST PRACTICES
Microsoft
THE SECURITY DEVELOPMENT LIFECYCLE
SDL: A Process for Developing Demonstrably More Secure Software
Michael Howard and Steve Lipner


Dr. Dobbs Jolt Award Finalist 2014
Adam Shostack
threat modeling
designing for security
WILEY


BEST PRACTICES
Microsoft
WRITING SECURE CODE
2
Practical strategies and techniques for secure application coding in a networked world
"Required reading at Microsoft." – Bill Gates
Michael Howard and David LeBlanc

Ressources

- Magazine MISC
- CTF (root-me.org, …)
- Bug Bounties (HackerOne, …)