Compte-rendu

OSSIR Paris - 8 novembre 2011
Saâd Kadhi <saad.kadhi@hapsis.fr>

Présentation Générale

- conférence sécurité bruxelloise à caractère “technique”
- 3ème édition, 4j, env. 160 participants
- 2j formations, 2j présentations
- prix fort raisonnable, bon rapport qualité/prix
- (bien) organisée par une équipe de volontaires

- streaming live (presque tout le temps)
- 16 présentations durant les 2j
- de 10h00 à 21h30
- un seul *track*, des workshops en // + *lightning talks*
- le SSTIC belge ?

- Programme complet disponible à l'adresse http://2011.brucon.org/index.php/Schedule

- Certaines présentations disponibles en téléchargement à la même adresse

Lundi 19 sep (jour 1)

Keynote

Why Information Risk Management Is Failing, Why That Matters to Security & What You Can Do About It

Alex Hutton, Director of Operational Risk
(Financial Institution)

"thought-provoking"

- Constat
- Comment expliquer les bénéfices ?
- Comment exprimer la valeur ajoutée ?
- La SSI est une proto-science

- Exemple avec CVSS
- Jet engine * peanut butter = shiny
- ???
- La notion de risque doit prendre en compte les aspects opérationnels (i.e. ce qui se passe dans les tranchées)

- Deux écoles de pensée majeures
- *Threat-centric* (Beijtlich)
- Gestion par les risques

Les japonais n'avaient pas de mot correspondant à "risque"

- Objectif : mieux expliquer les apports de la SSI au management

- Comment ?

- DME (Data, Models, Execution)

- Sécurité : caractéristique des systèmes et pas de leurs composants

- Ce n’est pas uniquement un problème d’ingénierie

- Pouvez-vous résoudre l’ignorance des utilisateurs ?

- Ah, et arrêtons d’empiler les solutions et “agents” de sécurité

- Approche DME
- Améliorer les processus existants
- VERIS, cadriciel Verizon. Emploie une approche épidémiologique
- Que devons-nous étudier ?

- Sources du savoir (i.e. données)
- patterns, patterns, patterns
- Vers une gestion des risques basée sur des faits
- Construire des tableaux de bord efficaces avec des indicateurs censés

- Arrêtons de “fabriquer” les faits ou de les inférer pour faire de jolis camemberts hauts en couleur

- Dehors les managers du risque, bienvenue les analystes

- Nous n’avons pas besoin de plus d’outillage

- Nous avons surtout besoin de compétences, de partages des connaissances et de formations

- Le chemin que la SSI a pris est désolant
- Nous sommes entrain de créer une bureaucratie, une religion, avec des dogmes
- Parce que nous n’avons pas de solides fondations scientifiques
- Pensez ISC2

iOS Forensics: Overcoming iPhone Data Protection

Andrey Belenko, ElcomSoft

- Forensics 101 : acquisition, analyse, reporting
- Accès physique à l’équipement
- Laisser aussi peu d’artefacts que possible

- iOS, version modifiée de Mac OS X
- Passcode : si on le contourne, c’est gagné
- Keychain, chiffrée
- Stockage chiffré à partir de l’iPhone 3GS

- Mesures de sécurité iOS
- Signature de code
- Votre outil d’inforensique n’est pas signé par Apple ? dommage...
- Bac à sable

- Différentes pistes pour l'acquisition
- Interfaces exposées : *Sync, backup*
- Contournement de la sécurité et exécution de code

- Approche dite logique
- On peut demander à iTunes de produire une sauvegarde
- L’équipement ne doit pas être verrouillé
- la sauvegarde peut être chiffrée

- Approche physique
- Acquisition du FS à la ‘dd’
- Le verrouillage n’est pas un problème
- On a besoin d’un code d’exploitation ‘boot-time’ pour exécuter du code non signé
- iOS 4+ chiffre le FS

Ce n'est plus tout à fait vrai

- iOS 3-, brièvement
- contournement du passcode
- pas de chiffrement FS
- Keychain chiffrée mais mal chiffrée
- Game over si vous pouvez exécuter du code

- Améliorations notables avec iOS 4
- verrouillage bien mieux implémenté
- FS chiffré (pas les metadonnées)
- Bien meilleur chiffrement de la Keychain
- Meilleur format de sauvegarde iTunes

- AES, au coeur des iDevices
- processeur dédié, 2 clés en dur
- GID key, partagée par toutes les iDevices de même modèle
- UID key, unique à chaque iDevice
- D’autres clés générées à la demande : ‘0x835’ dérivée de l’UID + une autre dérivée de l’UID et du GID

- Contenu groupé en *Protection Classes*
- Disponible lorsque l'iDevice est déverrouillé
- Disponible au premier déverrouillage jusqu'à arrêt complet
- Toujours disponible (et donc non protégé)

- Chaque classe se voit assigner une clé de chiffrement maître
- Les clés maître sont protégées par l'UID et le passcode
- L'ensemble de ces clés constitue le *system key bag*
- */private/var/keybags/systembag.kb*

- *Escrow keybag* permet à iTunes de déverrouiller l'équipement
- mêmes clés que le *system keybag*
- Créé lors de la première association avec iTunes, stocké sur l'ordinateur
- */var/db/lockdown*, au sein d'une plist
- protégé par un passcode aléatoire de 256 bits stocké sur l'iDevice

- Le passcode est nécessaire pour déverrouiller presque toutes les clés maître

- Les transformations passcode vers clé sont lentes

- brute-force offline impossible, nécessite l’extraction de l’UID

- brute-force online lent. 2 p/s à 7 p/s (iPhone 4)

- Le *system keybag* donne une idée de la complexité du passcode

- 0 (4 chiffres)

- 1 (chiffres, !=4)

- 2 (longueur et complexité inconnues)

- On peut donc identifier les passcodes “faibles”

- Démonstration de brute-force online
- ElcomSoft toolkit
- Jailbreak pour exécuter l'attaque puis supprime le jailbreak à la fin
- 3 mins environ pour casser un passcode à 4 chiffres
- Peut nécessiter jusqu'à 40 mins sur iPhone 4

- Et ‘dd’ dans tout ça ?

- l’image est entièrement en ‘clair’ car ‘déchiffrée’ à la volée par l’iDevice (clé EMF)

- Les metadonnées sont en clair, pas le contenu des fichiers

- nécessite une double transformation

- chiffrement EMF puis déchiffrement par clé propre au fichier

- Conclusion
- L’acquisition nécessite un code d’exploitation qui s’exécute au démarrage
- L’acquisition d’une image du disque ne suffit pas
- Le passcode n’est généralement pas un problème
- Disponibilité de toolkits OSS et propriétaires

Mardi 20 sep (jour 2)

Pushing in, leaving a present, and pulling out without anybody noticing

Ian Amit, Security Art

- Infiltration

- Technique : codes d'exploitation, ne pas oublier applications client (Symantec, Adobe...)

- "Humaine" : SE (Excel chez RSA), espaces fumeur, papoter, clé USB dans le parking, phishing (point&click)

- Bien cibler
- Quelles sont les données qu’on cherche à exfiltrer ?
- Outils commerciaux “weaponisables”
- Viser à s’installer durablement (APT)

- OSINT
- Foca, Maltego, ...
- Who’s your Daddy? Facebook!

- Médias sociaux
- Ne pas hésiter à recourir à la visualisation
- Qui est connecté à qui

- Choix de la cible et de la charge utile
- ZeuS, SpyEye, Limbo
- Presque gratuit (et gratuit si on connaît les bonnes personnes)
- Il faut juste savoir “packer” pour éviter d’être détecté

- Traiter tout cela comme un projet avec des jalons et des objectifs mesurables
- Différence entre infection massive et APT
- Infection massive : 5~6 jours avant détection, mises à jour fréquentes
- APT : 5~6 mois, pas de mise à jour ou presque. La patience est vertu

- Une fois qu'on s'est infiltré
- Maintenir le contrôle
- Supposer une communication uni-directionnelle

Pas si simple

- Maintenant, il reste à exfilter les données et sortir de là en beauté

- IPS/IDS (quand c’est bien utilisé)

- DLP (quand ce n’est pas une usine à gaz)

- Quelques solutions

- SSL, PGP (avec un peu d'encodage et de XOR pour ne pas se faire prendre)

- Archiver les données et les récupérer par un autre biais

- Canaux d’exfiltration
- Facebook, Dropbox, Wordpress (commentaire contenant les données), Twitter, DNS, Wikipedia (*talk* page), imprimantes
- Services mail vers fax
- Rarement surveillés par DLP etc.

- Et s’il n’y a plus Internet ?
- Dépend du contexte et nécessite du SE
- Impression automatique des données préalablement “déguisées”
- Jamais passées à la broyeuse
- Une visite à la poubelle s’impose
- Dépend de la taille des données ;-)

- Quelques pistes avec la VoIP
- Mise en place d'un numéro de confcall, d'un PBX ou d'une boîte vocale Google par exemple
- PoC. Convertisseur données voix 16 octaves
- http://code.google.com/p/data-sound-poc/

- Conclusion
- La technologie est secondaire, cibler d’abord l’humain
- Comprendre et pirater les processus métier
- Surveiller et attendre le bon moment
- Tester, tester, tester

Botnets and Browsers
Brothers in a Ghost Shell

Aditya K Sood

- Modèle d’infection via les navigateurs
- Botnets de 3ème génération
- Toujours le même but : cybercriminalité

- Taxonomie des malwares
- Dans les processus propres au navigateur
- Dans les processus propres aux plugins invoqués par le navigateur
- Au niveau de l’OS avec interface vers le navigateur
- Modèle collaboratif entre ces différentes cat.

- Exploitation de vulnérabilités Web
- Injection de code obfusqué (JS, ...)
- Appels DOM
- Frames

- Collaboration navigateur/bot
- Utilisation de SDKs et des plugins pour s’adresser aux serveurs C2
- Pourquoi plugin ?
- Contrôle modulaire, possibilité de màj code bot et configuration, démarrage/arrêt d’autres plugins malicieux
- Excellente méthode de décentralisation

- Approche similaire aux rootkits ring 3
- DLL *hooking* et *hijacking* en userland
- injection du processus Web
- communication HTTPS
- Traçage difficile

- Montée en puissance du “Man-In-the-Browser”

- Utilisation conjointe de BEPs (Browser Exploitation Packs) et de malwares

- BlackHole + (Zeus, SpyEye, Carberp, Mebroot)

- De plus en plus fréquent

Myth-busting Risk

Jack Jones, CISO, Huntington Bank

- L’orateur se définit comme un RSSI avec un réel background technique

- Il veut comprendre les NTIC

- Un ‘risk geek’

- Définition du risque
- “Probable frequency and probable magnitude of future loss”
- “How often bad things are likely to happen and how bad they’re likely to be when they do happen?”
- Probabilité vs. Possibilité

- Pour parler de risque, il faut d'abord pouvoir le mesurer
- "oh mais ceci est subjectif"
- L'objectivité et la subjectivité font partie du même continuum
- Certaines mesures semblent subjectives alors qu'elles sont objectives (mais imparfaites)

- En tant qu’espèce, nous sommes très incompétents à l’estimation des risques

- Et cela empire car nos interactions avec les menaces “naturelles” deviennent de plus en plus rares

- Mais on peut s’améliorer avec de la volonté et par apprentissage

- Il ne faut pas chercher à prédire le futur
- Il faut comprendre les probabilités
- Précision vs. Exactitude (intervalle)

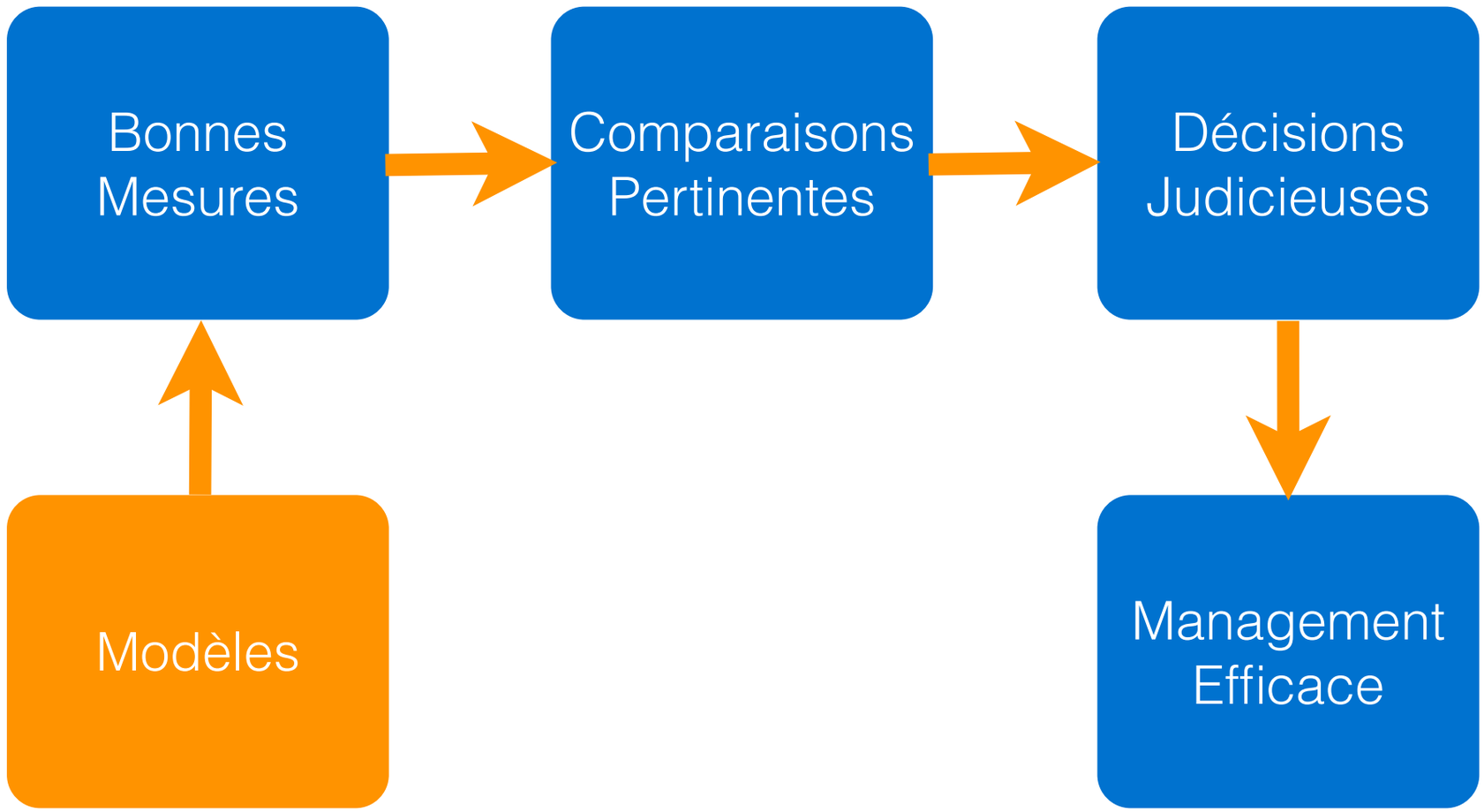
- Le management préfère (et s'attend à) l'exactitude
- Cibler l'exactitude avec une bonne dose de précision

- “Nous avons besoin de plus de données pour faire de l’analyse quantitative”

- Les indicateurs que nous employons sont souvent fumeux ou mal choisis

- Et nous avons déjà beaucoup de données

- Nous cherchons à faire des estimations


Bonnes Mesures
Comparaisons Pertinentes
Décisions Judicieuses
Modèles
Management Efficace

- Il n’appartient pas aux professionnels de la SSI de décider

- Mais ils doivent aider les décideurs

- Certes, ces derniers ne comprennent pas bien la SSI

- Ils ne sont pas pour autant idiots. Ils ne prendront pas des risques insensés

Hapsis

45 rue de la chaussée
d'Antin
75009 Paris
FRANCE
Tél. : +33 (0)1 53 16 30 60 -
Fax : +33 (0)1 53 16 30 62
Email : contact@hapsis.fr
Web : http://www.hapsis.fr/