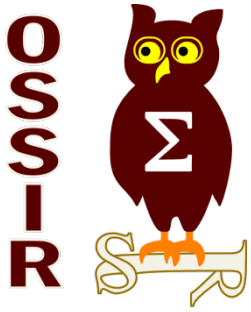
10 juin 2014



Compte rendu du SSTIC 2014

Arnaud Soullié
Ary Kokos

solucom
management & IT consulting

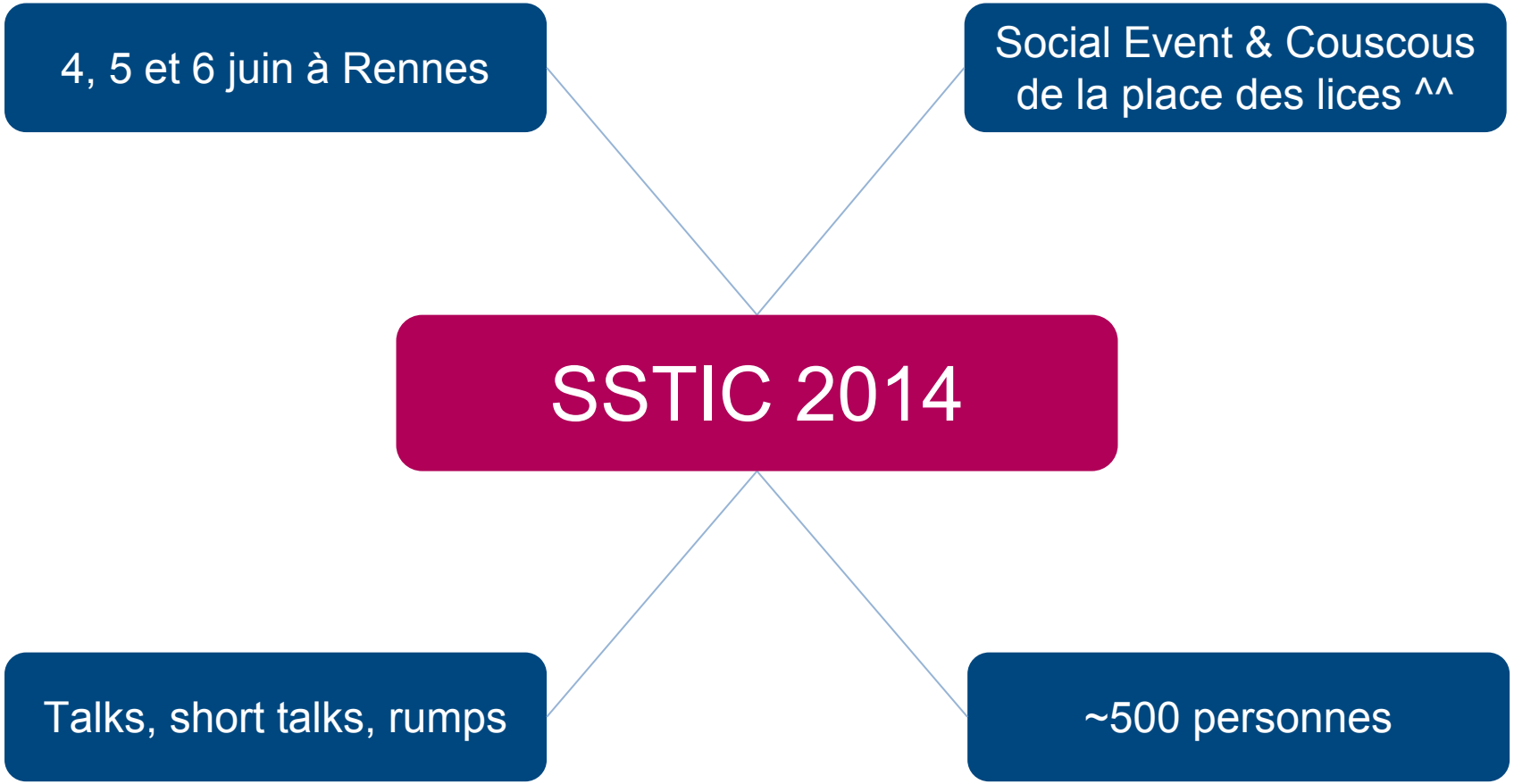
Principe

Présentation collaborative

De nombreuses personnes au SSTIC

N’hésitez pas à prendre la parole sur un des talks :)

SSTIC 2014



Disclaimer

- Les talks étaient de très haut niveau
- ~~Souvent~~ Parfois, on n'a pas tout compris ☺

DAY 1

Day 1

- Conférence d'ouverture : Proofs of concepts and tricks
- **Chemins de contrôle en environnement Active Directory**
- Analyse de la sécurité d'un active directory avec l'outil BTA
- **Secrets d'authentification épisode II : Kerberos contre attaque**

Pause

- Analyse de sécurité des modems des terminaux mobiles
- How to play Hooker : Une solution d'analyse automatisée de markets Android
- Investigation numérique & terminaux Apple IOS – Acquisition de données stockées sur un système fermé
- Catch Me If You Can – A compilation Of Recent Anti-Analysis in Malware
- [Short talk] Analyse de sécurité des box ADSL
- [Short talk] Sécurité des ordivisions // ordivision = smart TV
- [Short talk] La radio qui venait du froid

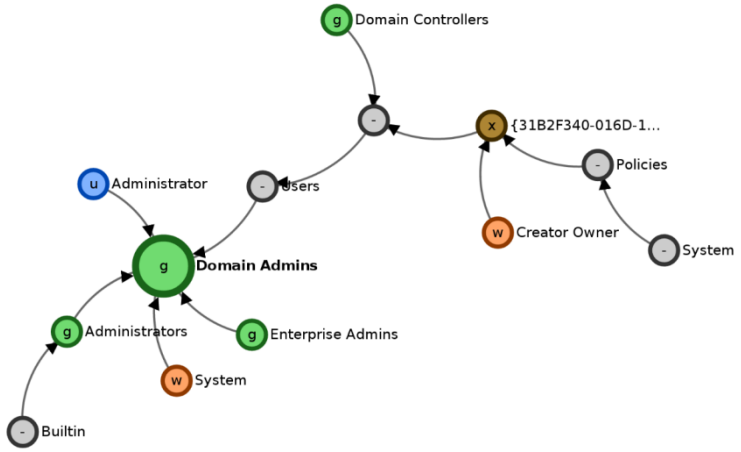
Chemin de contrôle en environnement Active Directory

« Savez-vous réellement qui est admin de votre domaine ? »

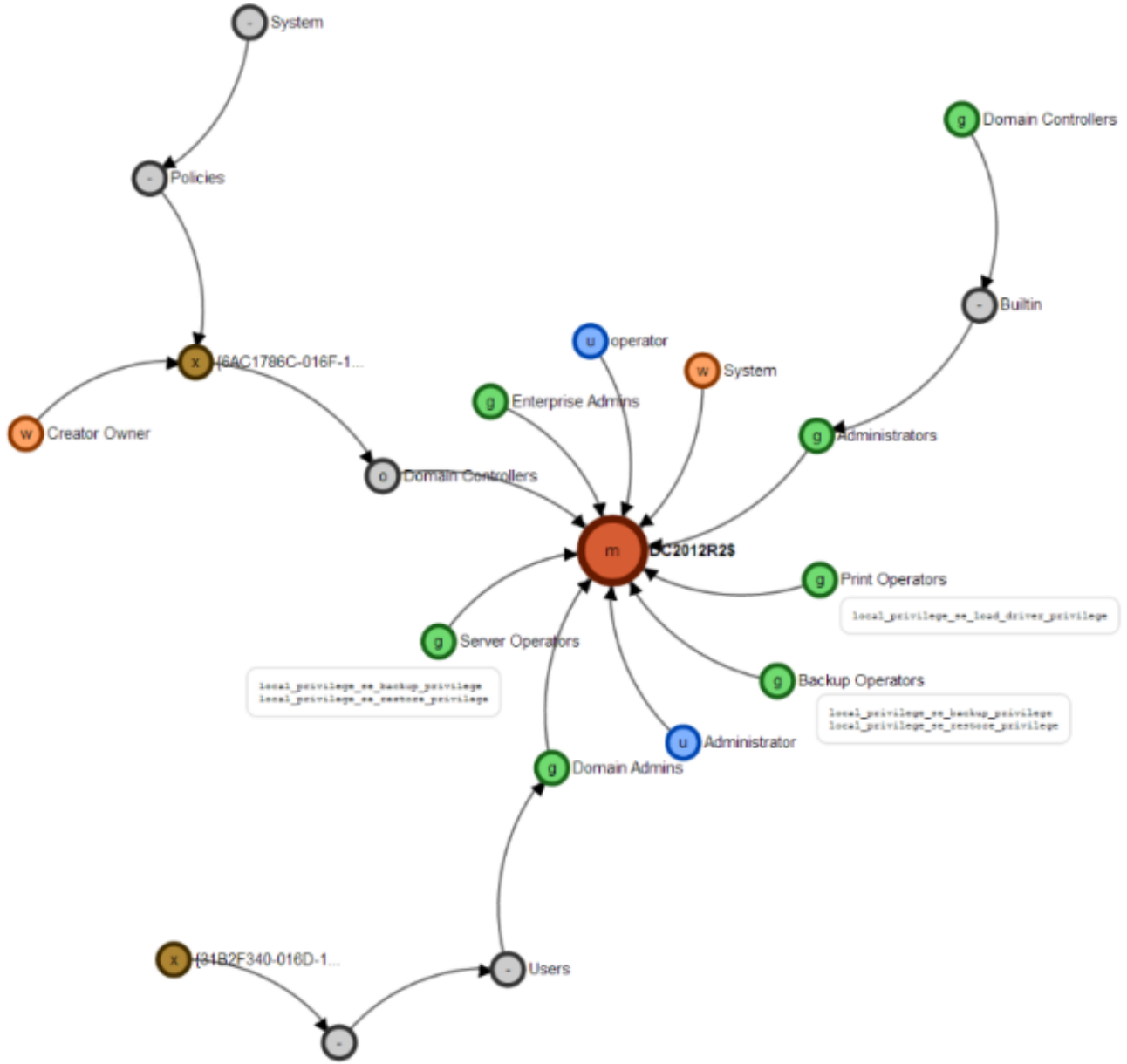
- Technique basée sur l'existence de chemins :
  - Une personne dans le groupe « Admin de domaine » est admin de domaine…mais
  - Une personne qui peut modifier les GPO de tous les serveurs est aussi admin de domaine !
  - Une personne qui est admin du poste de travail d'un admin de domaine l'est aussi !

- Comment ça marche
  - Requêtes LDAP vers le contrôleur de domaine
  - Copie avec maintien des droits sur le répertoire contena
  - + éventuellement relevé des postes locaux
  - ➔ *Accessible à tout utilisateur du domaine !!*

- Ce que ça donne



Chemin de contrôle : exemple plus complexe



Secrets d’authentification épisode II : Kerberos contre attaque

- Rappels Kerberos
- Manipulation et forgeage de tickets
  - Clefs de chiffrement = hash présents dans l’AD
  - Ajout de droits
  - Peu de logs
- krbtgt : le graal
  - Golden ticket valable 10 ans
- Clefs de chiffrement des pour connexions interdomaine aussi dans l’AD
  - Possibilité d’abuser les referal tickets
- RODC
  - Avantage : chaque RODC à son propre krbtgt

Analyse de sécurité des modems des terminaux mobiles

- Réseau : un empilement de couches historiques
  - 2G : crypto mal conçue
  - 3G et LTE : crypto bien conçue en théorie, mais qu'en est-il de l' implémentation ?
  - Implémentation d'un couer de réseau « maison » et fuzzing des staks
- De nombreuses failles identifiées
  - Et de nombreuses failles corrigées
- Chiffrement des liens
  - Aucune indication du téléphone si le lien réseau n'est pas chiffré

DAY 2

Day 2

- **Escalade de privilège dans une carte à puce Java Card**
- Recherche de vulnérabilités dans les piles USB : approches et outils
- Bootkit revisited
- Test d'intégrité d'hyperviseurs de machines virtuelles à distance et assisté par le matériel
- La sécurité des systèmes mainframes
- [Short talk] Reconnaissance de réseau à grande échelle : port scan is not dead
- **Cryptocoding**

Pause

- **Buy it, se it, break it… fix it : Caml Crush, un proxy PKCS#11 filtrant**
- Martine monte un CERT
- **Rumps**

Escalade de privilèges dans une JavaCard

- Par Guillaume Bouffard et Jean-Louis Lanet de l'université de Limoges
- La ROM de la carte à puce contient le système d'exploitation, les API et les applets Java
- Possibilité d'exécuter du code natif via l'appel à la JNI (Java Native Interface)
  - Théoriquement, pas d'interface JNI sur une JavaCard, mais cela existe sans doute pour les opérations crypotgraphiques
- Les ressources sont limitées sur une JavaCard
  - Vérificateur de bytecode déporté hors de la carte
  - Pare-feu géré par la carte
- Création de l'outil JCDA : *JavaCard DisAssembler* qui permet d'obtenir le plan mémoire d'une carte à l'aide d'un applet malformé (nécessite la connaissance des clés de chargement)
- Découverte de méthodes au comportement non-standard et possibilité de lecture de la ROM

➔ ***Certaines cartes sont toujours vulnérables***

Buy it, se it, break it… fix it : Caml Crush, un proxy PKCS#11 filtrant

- Crypto token interface
- Attaques par confusion
  - voir travaux de Graham Steel (présentation à l'OSSIR l'automne prochain)
  - Possibilité de faire sortir en clair *(ie* non wrappées*)* des clefs de chiffrement marquées comme sensibles
- ➔ Proxy PKCSc
- Exemples
  - Classique : Dissociation utilisateur / administrateur, filtrage des accès, lecture seule, forcer une politique de code PIN
  - Autre : utilisation dans une architecture MILS (partie high/low) en plaçant le proxy au niveau de l'hyperviseur
  - Autre : HSM réseau « low cost »
  - Autre : proxy pour des plateformes exotiques

Cryptocoding

- Par JP Aumasson de Kudelski Security
- Est revenu sur les récentes failles cryptographiques et leurs impacts
- Notamment OpenSSL
  - Propose énormément de fonctions
  - Supporte beaucoup d'architectures (Windows 16 bits !)
  - Quelques exemples de code incompréhensible dans OpenSSL
- En résumé
  - *Cyptographers suck at coding*
  - *Programmers suck at cryptography*

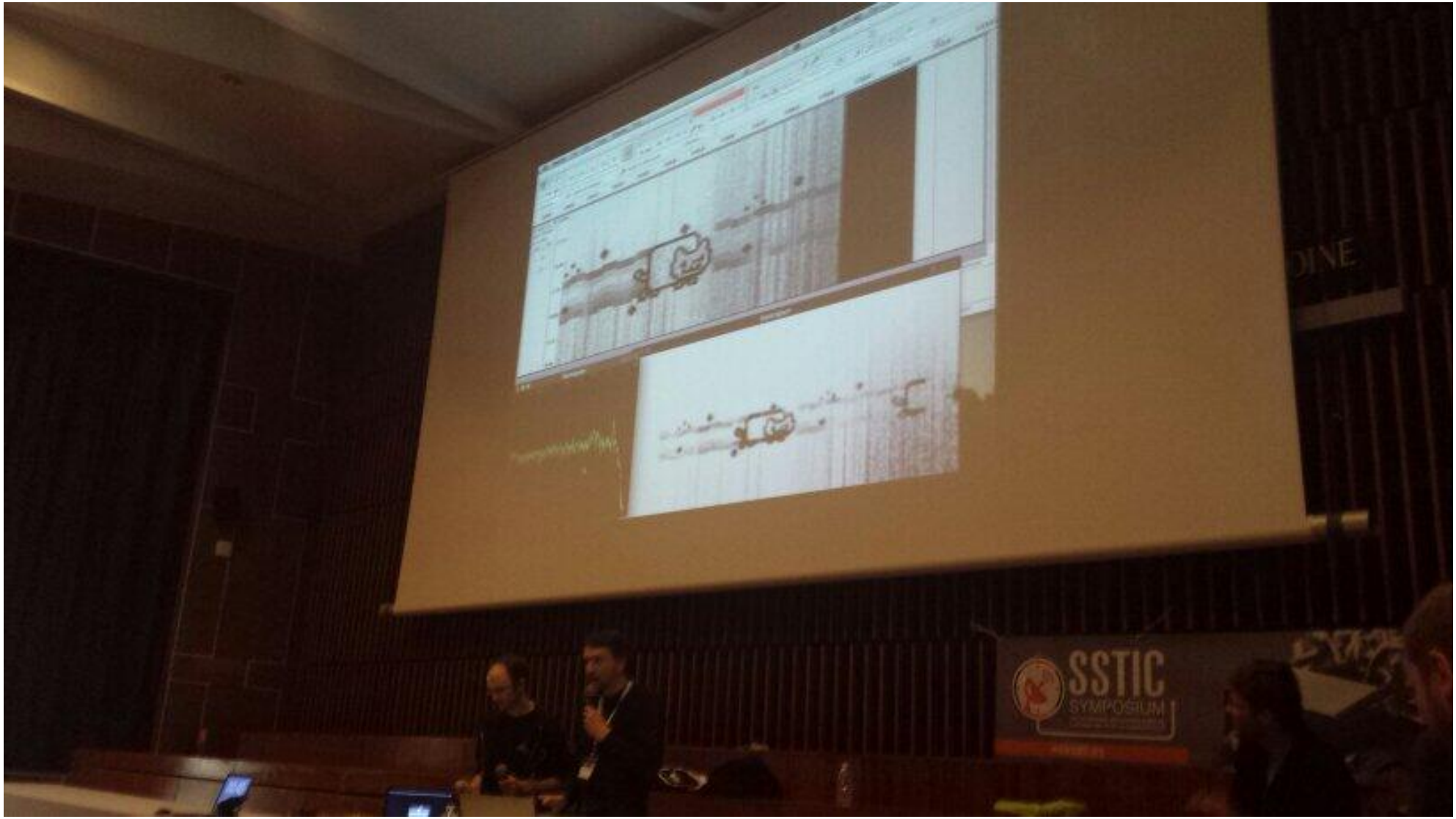
- Introduction du « *Cryptography Coding Standard* » https://cryptocoding.net

Rumps

Canal caché sonore (ultrasons)	Exemple génial avec une attaque evilmade et des chatons
Hack my swisscom box	En attendant d'avoir accès au net
IRMA	Virustotal souverain
Social engineering de l'amphi	Par JPG
Perseus #Fail	« cryptanalyse » opérationnelle en quelques minutes
Firmware.re	Firmware unpacking aaS

Et bien d'autres encore

Exfiltration de Nyan cat via ultrason



https://twitter.com/veorq/status/474564114636079104/photo/1

DAY 3

Day 3

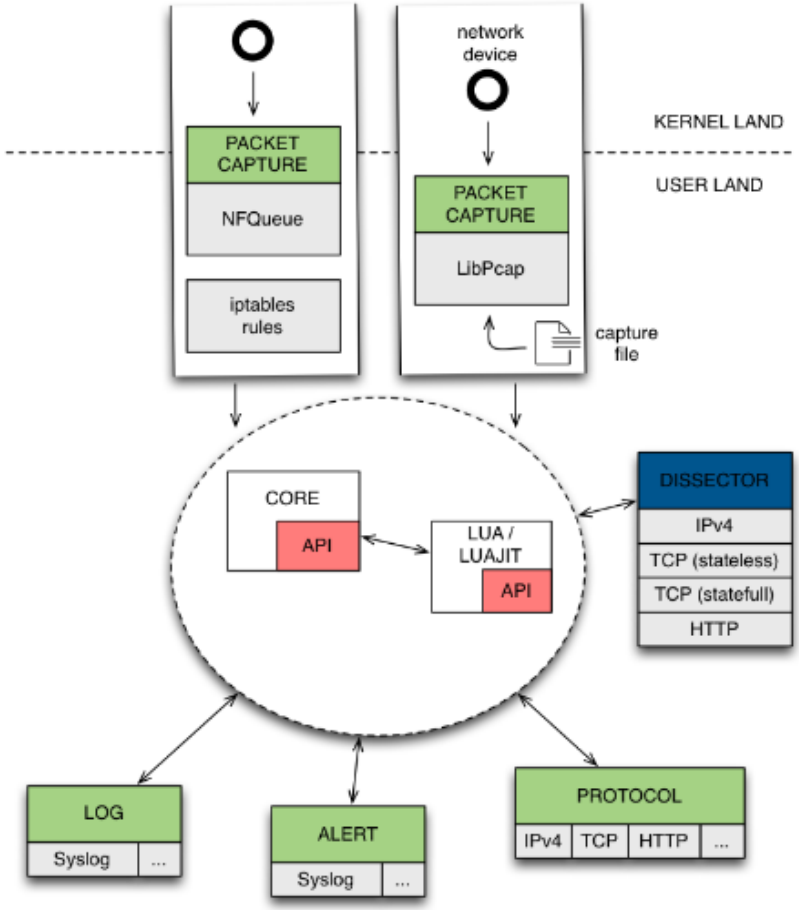
- Élaboration d'une représentation intermédiaire pour l'exécution concolique et le marquage de données sous Windows
- Obfuscation de code Python : amélioration des techniques existantes
- Désobfuscation de DRM par attaques auxiliaires
- Résultats du challenge
- Exemple de renforcement de la sécurité d'un OIV

Pause

- [Short talk] Sécurisation de la gestion dynamique des ressources dans le cloud : prise de contrôle sur le déclenchement de migrations automatiques de machines virtuelles
- [Short talk] RpcView : un outil d'exploration et de décompilation des MS RPC
- **[Short talk] Haka : un langage orienté réseau et sécurité**
- Tutorial Miasm
    4. Où l'impact des initiatives souveraines sur la balkanisation de l'internet ;)

Haka, un langage orienté réseau & sécurité

- Par Kevin Denis, Paul Fariello, Pierre Sylvain Desse et Mehdi (Arkoon)




```
icmp.grammar = g.record{
    g.field('type', g.number(8)),
    g.field('code', g.number(8)),
    g.field('checksum', g.number(16))
}
```

- Objectif : fournir un langage commun permettant de réaliser des actions de sécurité sur des paquets réseau, en ligne ou hors ligne (pcap)
- A venir : une API simplifiée et permettant la définition de machine à état

Questions ?

Arnaud Soullié
Ary Kokos

Prenom]dot] nom
[@[Solucom.fr