Détection d'intrusion 802.11

Symposium sur la Sécurité des Technologies de l'Information et des Communications

31 mai et 1-2 juin, Rennes, France

Laurent Butti – France Telecom Division R&D

firstname dot lastname at francetelecom dot com

Diffusion Libre

A propos

- Thématique « les limites de la sécurité »,
- « les limites des technologies »,
- « les limites du périmètre »…
- Ne pas oublier que l'on parle de détection d'intrusion ! ;-)

Agenda

- Contexte général
- Architecture de détection d'intrusion 802.11
- (Quelques) techniques implantées
- Démonstration
- Evolutions

Buts de la présentation

- Retour d'expérience sur la détection d'intrusion 802.11
  - Conception de nouvelles techniques
  - Développement d'une solution complète
  - Déploiement expérimental
- Possibilités de détection et de contournement des IDS 802.11
  - Et en particulier du nôtre…
- Donner un avis critique sur le domaine
  - On a fait ce que l'on a pu…
  - Des faiblesses subsistent et subsisteront : c'est intrinsèque !

Les standards 802.11

- Une norme originellement axée pour l'entreprise ?
  - Secret partagé entre tous les points d'accès et utilisateurs ?!?
- Un historique très lourd en terme de sécurité
  - Failles conceptuelles
  - Le protocole WEP présente de nombreuses faiblesses
- IEEE 802.11i (WPA2) apporte de nombreuses améliorations
  - Authentification basée sur une PSK ou une méthode EAP
  - Contrôle d'accès niveau 2 basé sur IEEE 802.1X
  - Hiérarchie de clés d'intégrité et de chiffrement
  - Confidentialité et intégrité assurées par TKIP et CCMP

Les constats actuels…

- Les réseaux 802.11 sont omniprésents !
  - Laptops, PDA, terminaux GSM, boxes, consoles de jeu…
- L'arrivée d'une technologie radioélectrique n'est pas anodine
  - En particulier en milieux « sensibles »
    - A bannir ?
- Prolifération des équipements et propagation radioélectrique difficiles à maîtriser…
  - Brèches possibles…

Origine de la détection d'intrusion 802.11

- Détecter des incidents de sécurité tels que
  - Déni de service
  - Faux points d'accès
  - Points d'accès illégitimes interconnectés au site protégé
- Entre difficile et impossible sans outils adaptés
  - Les processus de supervision « filaire » n'ont pas cette vision
- La détection d'intrusion est partie de la question suivante
  - Comment s'assurer que son infrastructure n'est pas victime de brèches induites par les technologies 802.11 ?

Diffusion Libre

Architecture développée

- Buts
  - Montée en compétence sur le domaine 802.11
  - Développement de nouvelles techniques de détection d'attaques
- Impératifs
  - Minimiser les coûts (matériel, logiciel)
  - Indépendance de l'architecture déjà déployée
  - Flexibilité et évolutivité (nouvelles normes et attaques)

Architecture développée

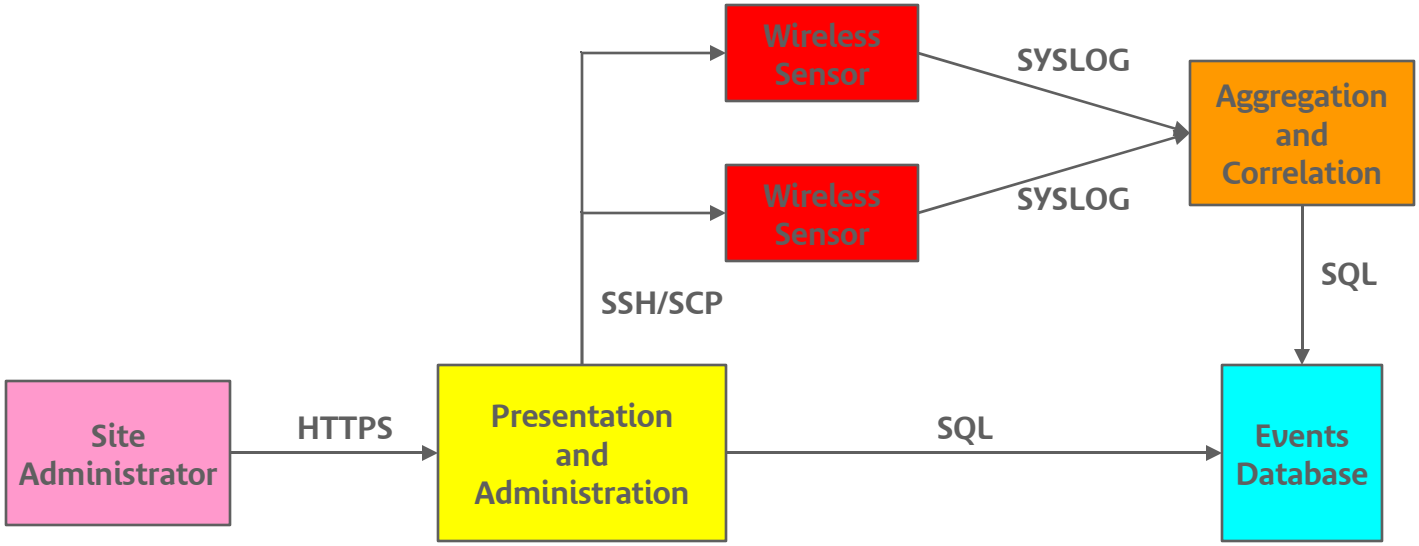
- Moteur de détection (développé de zéro en C)
  - Portable (x86 et MIPS)
  - Embarqué (Linksys WRT54G)
  - Flexible (langage de règles par signature ou comportement)
  - Evolutif (toute interface en mode « monitor » est supportée)
  - Interface SYSLOG pour la journalisation
- Règles de détection
  - 70 signatures « pattern matching »
  - 3 méthodes d'analyse pour détection d'usurpation d'adresse MAC

Architecture développée

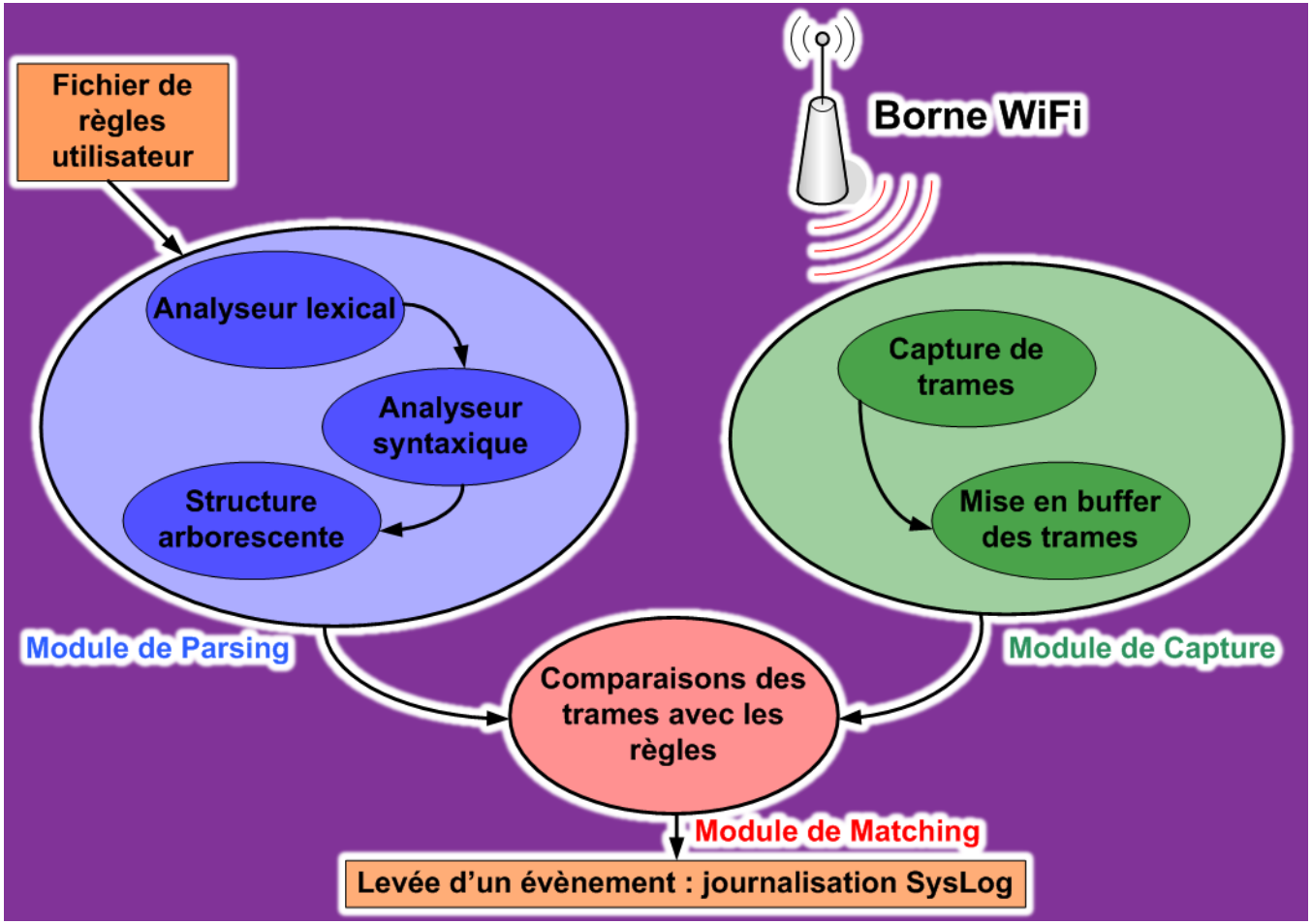
- Moteur d'agrégation / corrélation à la volée (basé sur SEC)
  - Toutes les sorties sont agrégées par défaut
  - Règle de corrélation à la volée
    - Flot de trames induisant du déni de service (de-authentification…)
    - Injection WEP
    - Fake AP
    - Usurpation d'adresse MAC
- Moteur de corrélation centralisée (en développement)
  - Règles de corrélation
    - Identification d'une même classe d'attaque de sources différentes
      - *Déni de service, Fake AP massif…*
  - Règles de qualification des points d'accès

Schéma de l'architecture

➔ Architecture de type « sur-couche »



Cœur de détection



Format de règles et de journalisation

```
listen CAP device=prism0 buffer=10s


from CAP
when packet.type = management
     do forwardto(MANAGEMENT)
<snip>
from MANAGEMENT
when packet.subtype = disassoc
     do forwardto(DISASSOC)
<snip>
from DISASSOC
when packet.mac1 = FF:FF:FF:FF:FF:FF and packet.mac2 in list("ap_whitelist")
     do log(packet.mac2 + " | " + packet.mac1 + " | DoS | medium | Broadcasted
Disassociation From Authorized AP | rssi=" + packet.prism_signal, 1) and break
```

```
MAC src | MAC dst | Classification | Severity | Signature | optional payload
```

```
00:00:00:00:00:00 | FF:FF:FF:FF:FF:FF | DoS | medium | Broadcasted Disassociation From
Authorized AP | rssi=10
```

Diffusion Libre

Capacités de détection actuelles

- Détecte les évènements tels que
  - WarDriving
  - Injection WEP
  - Déni de service
  - Usurpation d'adresse MAC
  - Faux points d'accès (outil fakeap.pl)
  - Points d'accès non autorisés
  - Réseaux ad-hoc
- Qualification et géo-localisation des points d'accès

Diffusion Libre

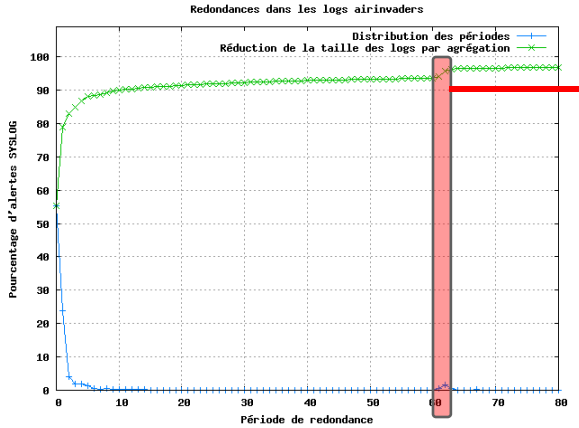
Quelques éléments sur la volumétrie

- Les balises sont (généralement) émises toutes les 100 ms
  - 10 pps => 864000 évènements par jour, par sonde et par point d'accès (au maximum) uniquement sur les balises !
- L'agrégation à la volée permet de
  - Réduire les évènements récurrents (recherche de réseaux, points d'accès signalant leur présence…)
- Agrégation par « fenêtre de temps »
  - Dimensionnement « borné » par intervalles de 65 secondes
  - 1300 évènements par jour, par sonde et par point d'accès (au maximum) uniquement sur les balises !
  - Nécessité de gérer un nettoyage des bases

Diffusion Libre

Quelques éléments sur la volumétrie

- Agrégation impérative !
  - Durée d'agrégation empirique



99% de réduction

- La corrélation à la volée permet de
  - Créer un nouvel événement corrélé d'une suite logique d'évènements
    - -Nouvelle signature, classification et sévérité
  - Exemples
    - -Sur les flots de trames (déni de service)
    - -Sur les faux points d'accès (évite le peuplement de la base avec des données « fausses »)
    - -Sur l'usurpation d'adresse MAC

Détection du point d'accès

- Un système classique de listes blanches, grises et noires
  - De nom de réseau : Service Set IDentifier
  - D'adresse MAC : Basic Service Set IDentifier
- Permet d'identifier les points d'accès environnants
  - La sensibilité des sondes est un facteur déterminant
- Mais il faut (aussi) les qualifier…

Qualification du point d'accès (par signatures)

- BSSID autorisé, ESSID autorisé
  - Nécessite une usurpation d'adresse MAC (à détecter) pour être dangereux
- BSSID non autorisé, ESSID autorisé
  - Peut être dangereux (point d'accès illégitime)
- BSSID autorisé, ESSID non autorisé
  - Peut être dangereux (point d'accès mal configuré)
- BSSID non autorisé, ESSID non autorisé
  - Peut être interférent (point d'accès voisins)
  - Peut être dangereux (point d'accès interconnecté au réseau interne du site protégé)

Qualification du point d'accès (par analyses)

- Pré-requis : base de connaissance de l'architecture
  - Inventaire par outils adaptés (cf. NetDisco)
- Recherche des adresses MAC internes dans la base de donnée qui correspondent à
  - BSSID +/-1
  - MAC destination des trames de données issues d'un client 802.11
  - MAC source d'un client 802.11
- Tentative d'association avec le point d'accès
  - Récupération d'une adresse IP si possible via DHCP
  - Requête vers un serveur interne
  - Si réponse alors interconnecté avec le réseau interne

Usurpation d'adresse MAC (1/6)

- L'usurpation d'adresse MAC permet de contourner les listes blanches de points d'accès autorisés
  - Facile à réaliser : ifconfig wlan0 hw ether 01:23:45:67:89:AB
- Difficile de distinguer deux équipements ayant les mêmes caractéristiques au niveau 802.11
  - Blanc bonnet, bonnet blanc…
- Les techniques de détection d'usurpation d'adresse MAC résident sur des astuces

Usurpation d'adresse MAC (2/6)

- Les techniques imposent les hypothèses suivantes
  - Les deux équipements (légitime et illégitime) sont destinés à parler (à un moment donné) en même temps
  - Les trames émises par ces équipements doivent être captées par les sondes de détection d'intrusion
  - Les trames émises par ces équipements doivent être stockées durant un certain temps pour réaliser une analyse des différences
- Pas de détection par signature possible
  - Détection d'anomalie grâce à l'historique

Usurpation d'adresse MAC (3/6)

- Analyse des numéros de séquence
  - Sequence Numbers présents dans toutes les trames de type management et data (Joshua Wright, 2002)
- Analyse des étiquettes temporelles
  - BSS Timestamps présents dans les trames Beacon et Probe Resp.
- Analyse des champs optionnels
  - Tagged Parameters présents dans les trames de type management
- Analyse de la qualité de signal reçue
  - Recieved Signal Strength Index en chacune des sondes pour le paquet donné, pour pour la suite de paquets d'une même source

Diffusion Libre

Usurpation d'adresse MAC (4/6)

- Analyse par volumétrie de trames
  - Statistiques sur le nombre de trames émises par un point d'accès en fonction du type de trame (Beacon par exemple), de l'intervalle d'émission (Beacon Interval par exemple) et du saut de canal
  - S'ils sont deux à parler en même temps, le saut sera probablement brusque à un moment donné

Usurpation d'adresse MAC (5/6)

- Nombreuses techniques possibles sur ces principes
  - Analyse par seuil
  - Analyse statistiques
- La détection d'usurpation d'adresse MAC est sujette à des faux positifs
  - Nécessité de corréler ces alertes par volume et par type

Usurpation d'adresse MAC (6/6)

- Analyse d'une trace réseau

Challenges détection d'intrusion 802.11

- Les chipsets et drivers 802.11 sont de plus en plus laxistes
  - Injection de trafic très permissive
    - Modification de champs critiques (BSS Timestamp, Sequence Number…)
- Implantation de nouveaux protocoles MAC en se reposant sur les couches de modulation présentes dans les chipsets
  - Protocoles propriétaires à la main (via SoftMAC ou mode « monitor »)
- Problématiques à gérer
  - Comment résister au spectre étendu des attaques ?
    - Flot sur la base de donnée, insertion de données incohérentes…
  - Comment détecter de nouvelles modes d'attaques ?
    - Les canaux cachés par exemple
  - Comment ne pas être manipulé par l'attaquant ?
    - Qualification de milliers de points d'accès virtuels ou émulés

Le compromis parfait ?

- L'agrégation impose des pertes d'information
  - Mais elle est nécessaire si l'on veut éviter les impacts
    - Attaques par flot et évènements redondants
- Ouvre la porte de nouvelles faiblesses
  - Les canaux cachés par exemple
    - Cf. Raw Covert (http://rfakeap.tuxfamily.org)
- Dilemme permanent entre capacité de détection et capacité d'utilisation de l'outil
  - Quelle fenêtre de vulnérabilité est acceptable ?
  - Et à quel prix en terme de ressources CPU, DB, compétences d'analyse…

Diffusion Libre

Quelques pistes

- Filtrer les trames 802.11 en fonction de leur conformité au standard
  - Pré-traitements pour n'analyser que ce qui est cohérent
  - Mais la porte aux canaux cachés s'ouvre alors encore plus !
    - Cf. ShmooCon 2006 – Laurent Butti & Franck Veysset
- Réaliser des statistiques sur les trames utilisées par rapport au réseau courant
  - Analyse statistiques (en cours de développement)
- Garde-fous pour qualifier les points d'accès

Evolutions en cours

- Intégration dans une architecture de supervision interne
  - Interconnexion via IDMEF
  - Plugins de corrélation centraux
  - Plugin de présentation adapté au 802.11
- Implantation de nouvelles techniques de détection

Deux autres problématiques (de taille)…

- Comment avoir une interface de visualisation utilisable ?!?
  - Les geeks veulent du pcap en live sur les sondes
  - Les admins veulent des résumés par mail
  - Les vips veulent des camemberts et des charts
  - Et… on n'est pas des ergonomes !!!
- Comment choisir la sémantique des évènements ?!?
  - Format de journalisation
  - Classification
  - Signature
  - Sévérité

Diffusion Libre

Recommandations

- Connaître son réseau est impératif (BSSID, ESSID…) !

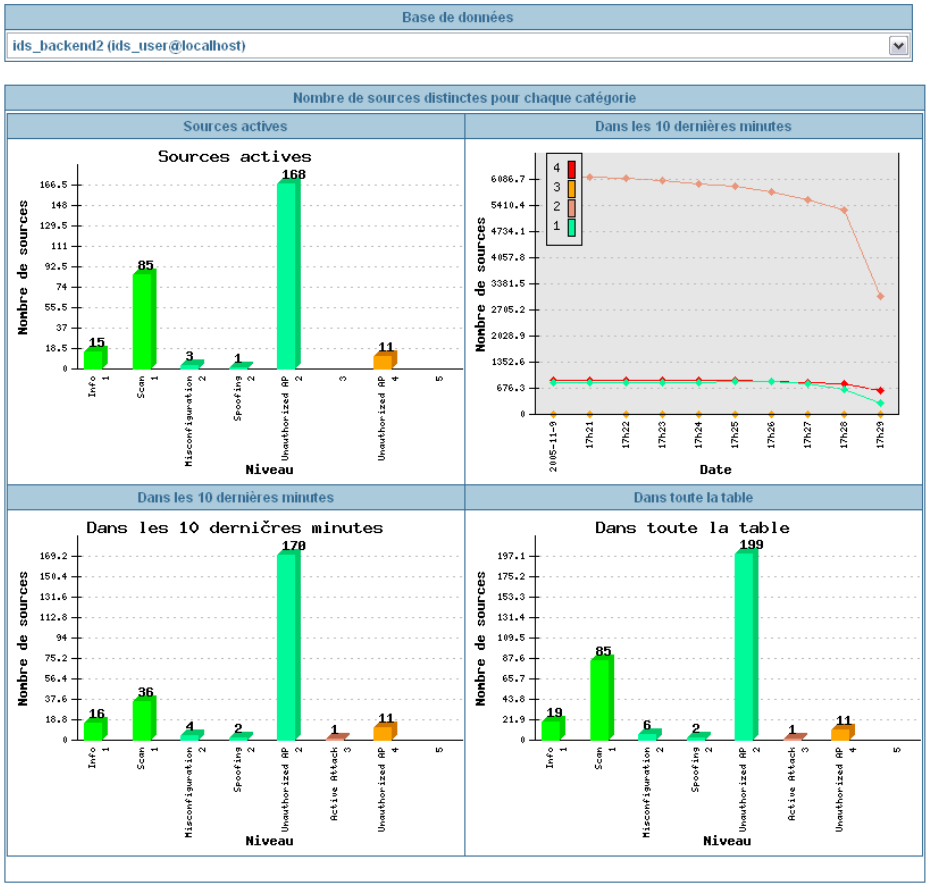
- Privilégier les solutions
  - Intégrées (infrastructure + IDS)
  - Avec des fonctionnalités de géo-localisation
  - Avec des fonctionnalités de prévention d'intrusion
    - -Attention aux problématiques juridiques et de déni de service !!!
    - -Modification de driver client pour se « protéger » ;-)

- Auditer la solution (cahier de tests)
  - Détection des attaques
  - Cibler l'IDS (flot de trames pour saturation…)

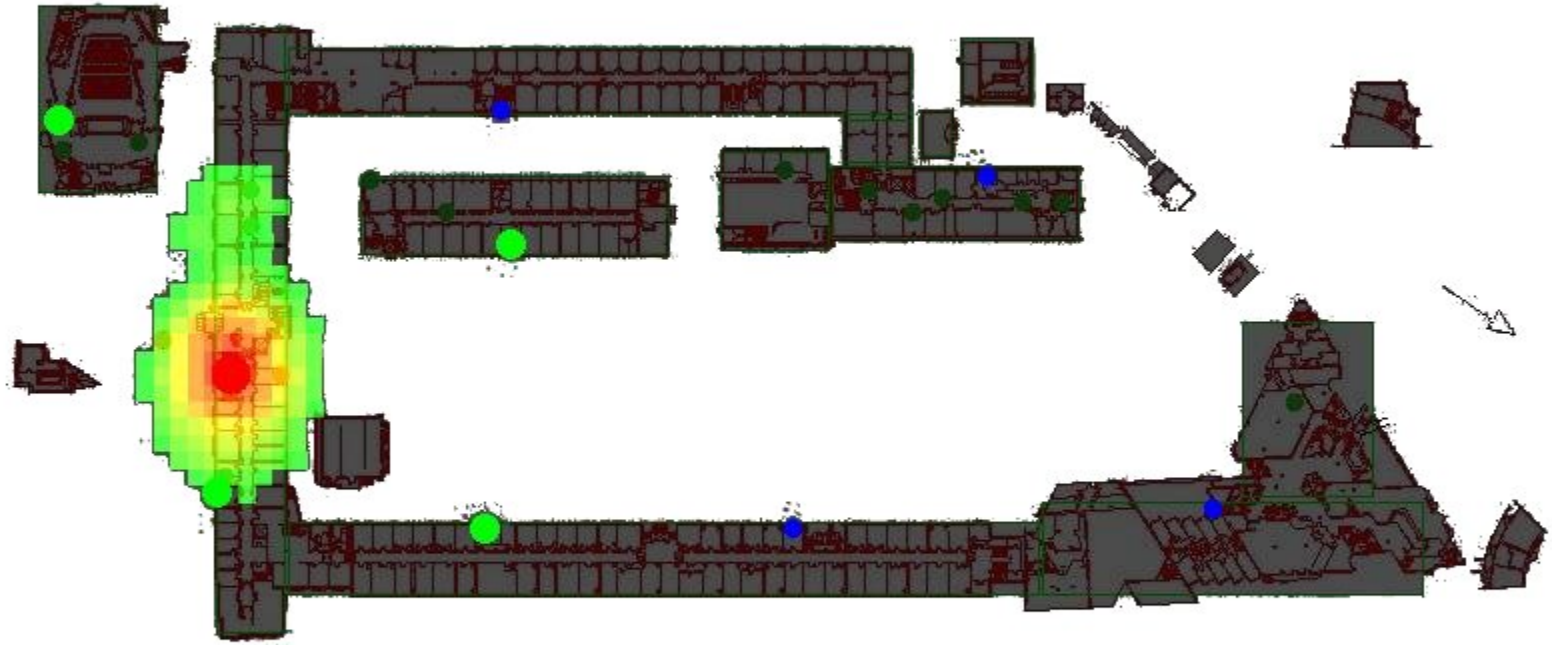
Démonstration

Diffusion Libre

Captures d'écran (GUI v1)



Captures d'écran (Géo-localisation)



Conclusions

- Domaine récent dopé par les problématiques de sécurité
- L'approche intégrée est séduisante (infrastructure + IDS)
- La grande majorité des incidents de sécurité 802.11 peuvent être détectés par les techniques décrites précédemment
- Les nouveaux risques peuvent être détectés grâce à une combinaison de détection par signature et par comportement

Conclusions

- Mais ce n'est pas une assurance tout risque
  - Probablement nécessaire pour éviter les audits 802.11 récurrents
  - Ne règlera pas la problématique (classique) des canaux cachés
- Dans tous les cas, un attaquant pourra toujours (plus ou moins) bien contourner les mécanismes de détection
  - Sur les canaux cachés, fragmentation 802.11 pour les données…
- Mais, il émettra toujours sur la voie radioélectrique
  - Efforts sur la géolocalisation très intéressants !
  - Mais non trivial… ☹