Blind xPath Injection

Kismet mapping

Laurent Licour
laurent <at> licour <dot> com

OVERLAP GROUPE

Blind xPath Injection

(la fin d'un mythe)

Blind xPath Injection

- Attaque décrite en 2004 par Amit Klein
- Whitepaper expliquant le concept
  http://www.packetstormsecurity.org/papers/bypass/Blind_XPath_Injection_20040518.pdf
- Pas de Proof of Concept publié

Blind xPath Injection

- Articles récents de Renaud Bidou
  - MISC 43 (mai/juin 2009)

  - Meeting OWASP France (06/05/2009)
    http://www.owasp.org/images/6/6b/2009-05-06-OWASPFR-WebServices.pdf

- Attaque visiblement toujours théorique

Blind xPath Injection

- Challenge Securitech 2006
  - level 2
  - web service vulnérable
  - secret à retrouver

  - mise au point d'un PoC de Blind xPath
  - ... mais fausse piste :-(

Blind xPath Injection

- Concept
  - dump complet d'un document XML
  - pas de connaissance de la structure
  - dump bit à bit du document
    - structure
    - tags
    - attributs
    - données
    - commentaires
    - ...

Blind xPath Injection

- Requis
  - application vulnérable au xPath injection
  - pouvoir distinguer une expression booléenne
    - différence d'affichage
    - différence de comportement
    - ...

Blind xPath Injection

- Release d'un code générique
  - librairie perl
  - vecteur de l'attaque
    - application locale
    - application WebGoat (OWASP)

Blind xPath Injection

- Utilisation des concepts exposés par Amit Klein
- Optimisations apportées
  - pattern matching
  - apprentissage de la structure XML déjà déterminée
  - ...

Blind xPath Injection

WebGoat-5.2/tomcat/webapps/WebGoat/lessons/XPATHInjection/EmployeesData.xml

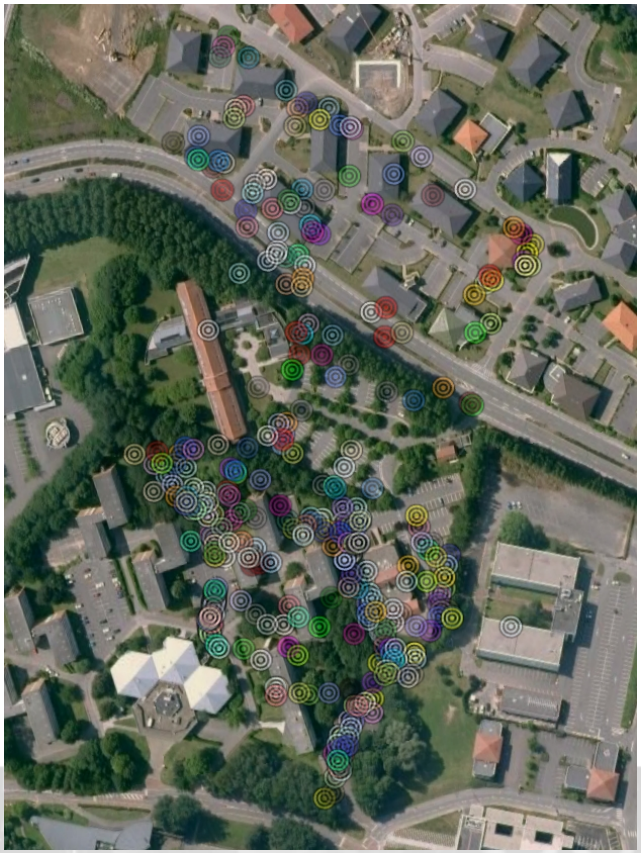
```
<?xml version="1.0" encoding="ISO-8859-1"?>
<employees>
        <employee id="1">
                <loginID>Mike</loginID>
                <accountno>11123</accountno>
                <passwd>test123</passwd>
                <salary>468100</salary>
        </employee>
        <employee id="2">
                <loginID>John</loginID>
                <accountno>63458</accountno>
                <passwd>myownpass</passwd>
                <salary>559833</salary>
        </employee>
        <employee id="3">
                <loginID>Sarah</loginID>
                <accountno>23363</accountno>
                <passwd>secret</passwd>
                <salary>123456</salary>
        </employee>
</employees>
```

2274 requêtes !!!

Kismet Mapping

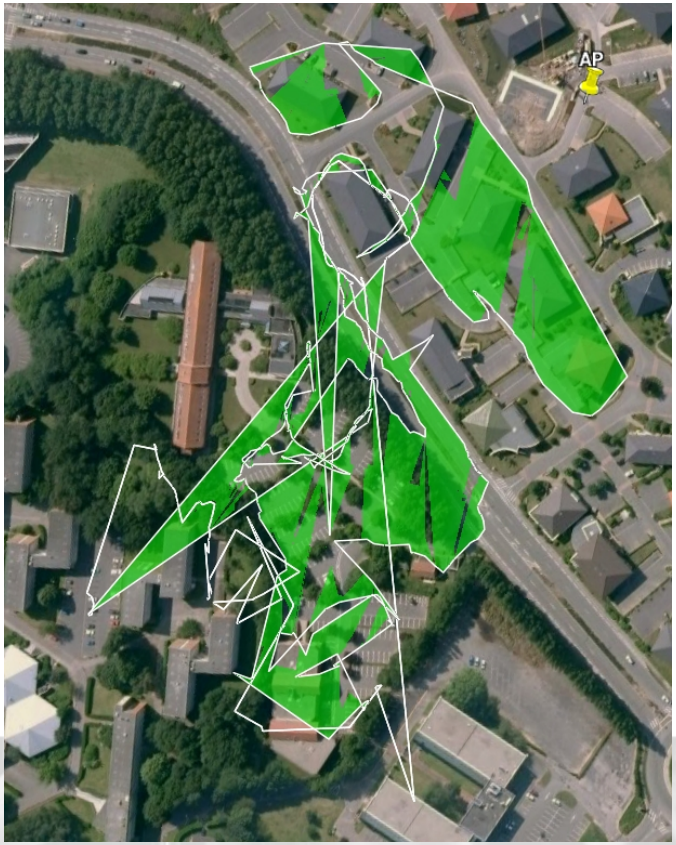
Kismet Mapping

- Mapping Kismet dans GoogleEarth
  - Wifi
  - GPS
- Nombreux projets
  - orientés wardriving
  - pas orientés couverture



Kismet Mapping

- Celui avec fonction de couverture marche mal
  - Kismet Earth



Kismet Mapping

- Enveloppe convexe

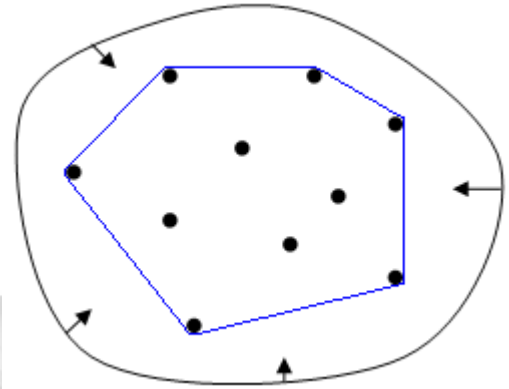
Wikipedia

"*L'enveloppe convexe d'un objet ou d'un regroupement d'objets géométriques est l'ensemble convexe le plus petit parmi ceux qui le contiennent.*"

- Enveloppe convexe

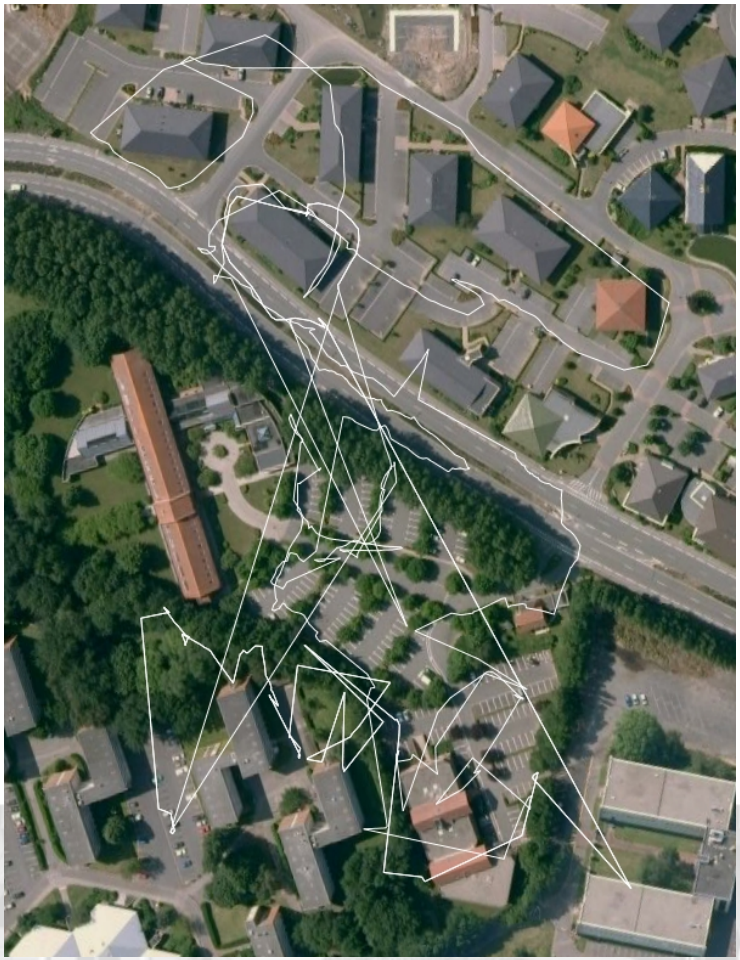
Wikipedia

"*L'enveloppe convexe d'un objet ou d'un regroupement d'objets géométriques est l'ensemble convexe le plus petit parmi ceux qui le contiennent.*"



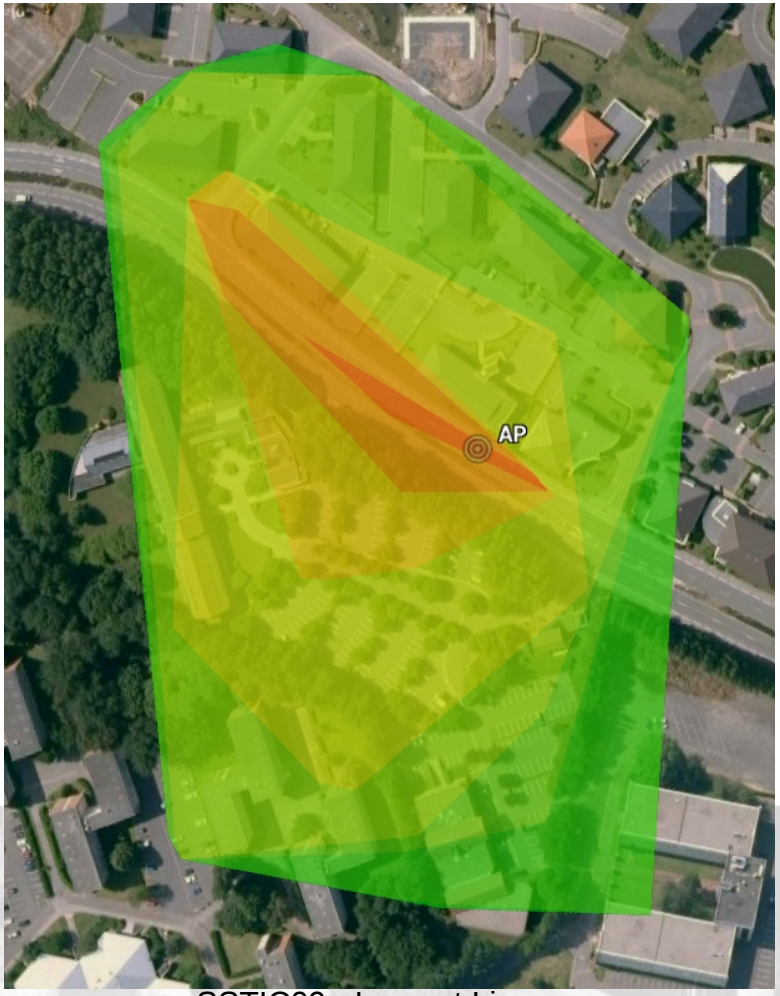
Kismet Mapping

- avec les enveloppes convexes



Kismet Mapping

- avec les enveloppes convexes



Kismet Mapping

- Patch actellement pour Kisgearth
- TODO : implementation dans GISKismet

Questions ?

codes disponibles à l'adresse :
http://www.licour.com