



# Shmoocon 2006

## Washington D.C. – 13-15 janvier 2006

Franck VEYSSET – France Telecom Division R&D

franck.veysset AT francetelecom dot com

# Agenda

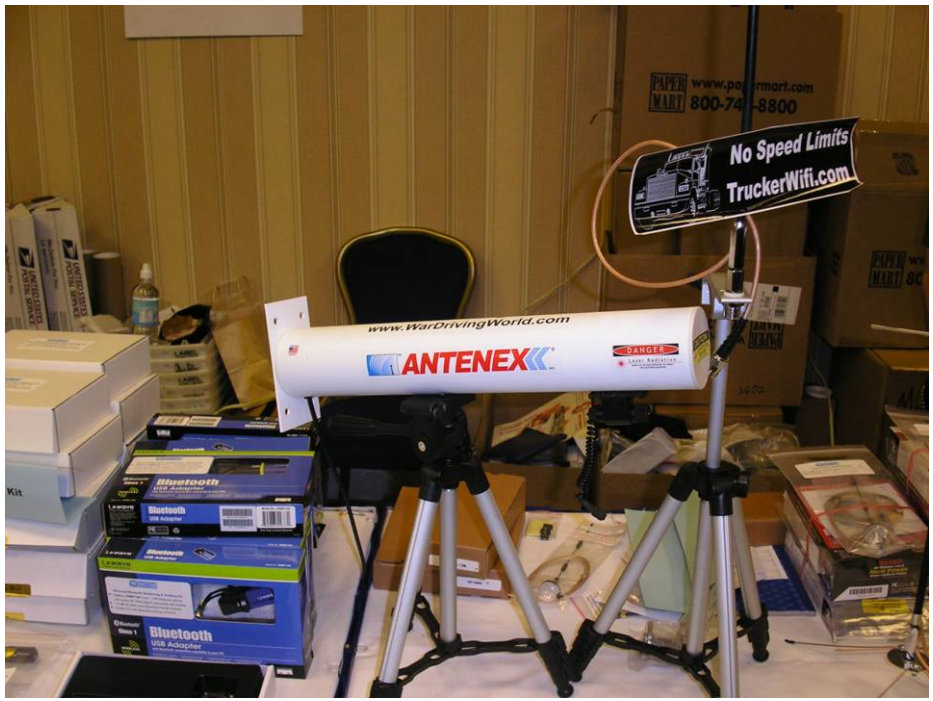
- La conférence Shmoocon
- Thématiques principales
  - WiFi
  - VoIP
  - Autres
- Conclusion
- Références

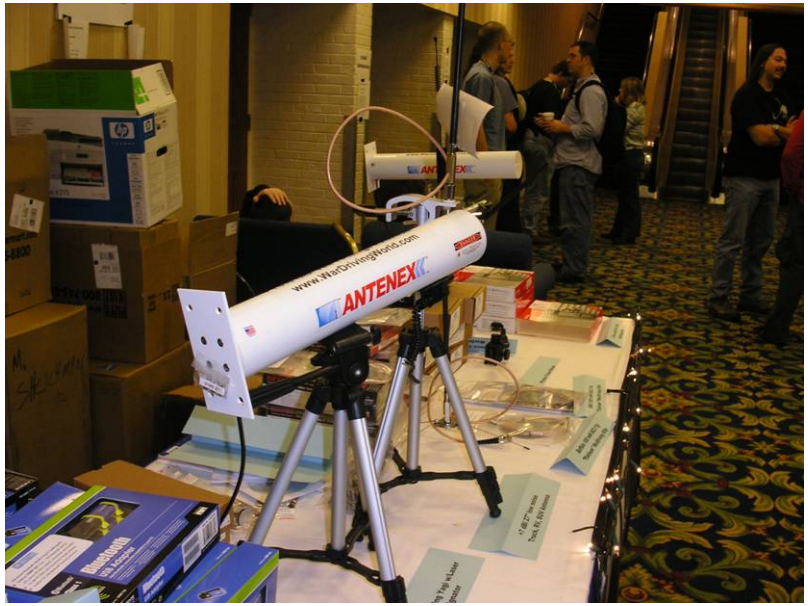
# La conférence

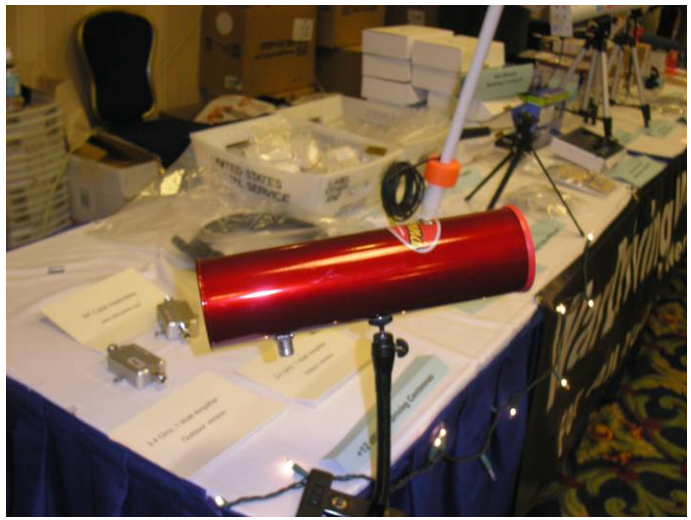
- **Deuxième édition,**
  - Autour de 800 personnes
  - Environ 40 présentations sur 3 jours
- **Organisée par le groupe de hacker « Shmoo »**
- **À Washington D.C. (proche des 3-letters agencies)**
- **Shmoo**
  - Bruce Potter (founder)
  - Des personnes de nombreuses boites de sécu
    - Snort, Immunix, PGP…

# La conférence

- **3 sessions en parallèle**
  - Build it!
  - Break it!
  - BoF it!
- **Quelques vendeurs de matériel / T-shirt**
- **Hacker arcade**
- **Social event à « Fur », la boite du coin…**


www.WarDrivingWorld.com
ANTENEX
DANGER
No Speed Limits
TruckerWifi.com
Bluetooth
USB Adapter


www.WarDrivingWorld.com
ANTENEX



# Thèmes 2006

## Quelques grands thèmes 2006

- VoIP
- WiFi

## Présentation marquantes

- Simple Nomad, *« Hacking the Friendly Skies »*
- Shawn Merdingeression, *« VoIP WiFi phone security analysis »*
- *« Anonym.OS: Security and Privacy, Everywhere You Go »*
- *« Bitchslapping Wireless IDS/IPS appliances »*
- *« WiFi Trickery, How to break, secure and have fun with WiFi »* ☺

- Dan Kaminski, *"Black Ops Of TCP/IP 2005.5"*
- Fyodor, *"Advanced Network Reconnaissance with Nmap"*

# Keynote speakers

## Vendredi : Dan Geer

- Présentation intéressante sur les problématiques de maîtrise et de complexité
- Analogie avec la biologie
- Message : Réutilisé les connaissances diverses dans la sécurité

## Samedi : Jennifer Granick

- Juriste
- Problématique de surveillance de la vie privée
- Et notamment nouveaux droits de la NSA (écoute dans « warrants »)

# « *Hacking the Friendly Skies* »

- **La conférence la plus médiatisée (/., Washington post…)**
- **Peu de nouveauté (tout est dans *Karma*)**
- **Sujet d'actualité**
  - Aéroport, Sécurité aérienne
  - Windows, WiFi…
  - Un zest « d'anti-microsoft »…

# « Hacking the Friendly Skies » - 2

- **Idée : Les PC sous Microsoft créent un réseau ad-hoc s'ils n'arrivent pas à s'associer**
  - En fait, uniquement dans certains cas…
- **Les PC Msoft n'ont généralement pas de FW**
- **Il est donc possible de les attaquer !**
- **Besoins : WiFi, ethereal, Metasploit…**

# « VoIP WiFi phone security analysis »

- **Présentation très intéressante…**
- **… mais plutôt inquiétante**

- **L'auteur révèle de nombreuses failles système dans les téléphones VoIP**
  - Pas d'attaque sur la partie VoIP

- **Sur une quinzaine de téléphone**
  - Telnet ouvert
  - SNMP read Write
  - Ports de débug (vxworks)
  - Echo, time ouverts…

# The church of WiFi…

## Présentation de travaux WiFi

- Package Kismet sous Win32 (uniquement le moteur)
- « Evil bastard », un AP outillé pour le MitM, et l'attaque
  - Dsniff, dnsspoof, webmitm, mailsnarf…

## Le plus intéressant : breaking WPA-PSK (JDUMAS)

- Démonstration d'optimisation de cassage de clés WPA
- Nécessite un pre-calcul dépendant du SSID
- Top 1000 SSID= 50% du réseau Wigle
- Performance : de 12/s à 18000/s passphrases testées

**PMK = PBKDF2(passphrase, ssid, taille du ssid, 4096, 256)**

# « Anonym.OS: Security and Privacy, Everywhere You Go »

- **Idée : CD bootable offrant des fonctions d'anonymat avancées**
  - TOR (The Onion Routing)
  - Privoxy
  - Basé sur OpenBSD
  - Mac @ / OS obfuscation
  - Proxies anonymes
  - Pf (règles firewall, aucun flux sortant non anonyme ou chiffré !)

- **Disponible sur Sourceforge**
  - http://theory.kaos.to/projects.html
  - http://sourceforge.net/projects/anonym-os/

# « Bitchslapping Wireless IDS/IPS appliances »

- **Analyse de produits de type IDS/IPS WiFi**
- **Rien de bien nouveau**
  - Les technos ne sont pas forcement mures
  - Certaines attaques ne sont pas détectées
  - Il est possible de contourner les équipements…
- **Quelques anecdotes**
  - Sur AP avec fonctions IDS
  - Si trafic SIP, alors plus de fonction IDS (pb performance)

# Autres présentations

- **Covert Crawling**
  - Technique de « web crawling » furtive, reposant sur l'utilisation de plusieurs sources, et émulant des comportements « humains »
- **Cardbus bus-mastering**
  - Peu d'information, mais sujet intéressant
  - Ressemble à la présentation « Owned by an ipod / IEEE1394 »
  - Info sur attaques via ports USB / PCMCIA…
- **Windows Vista Heap**
  - Présentation assez pointues, le dimanche matin ☹
- **Behavioral Malware Analysis Using Sandnets**
  - Analyse de malware/spyware/bot via le concept de « sandbox » étendu au réseau, et architecture associée

# *« WiFi Trickery, How to break, secure and have fun with WiFi »*

- **Présentation d'outils WiFi de type « fakeAP », « GluAP » et « covertchannel »**
  - Reposant sur l'utilisation d'injection de trafic WiFi
- **FakeAP**
  - Simulation de borne WiFi « virtuelle »
  - Maintien des contextes
- **GluAP**
  - Capture de clients WiFi
- **Rcovert**
  - Canal caché via trames « Ack » (niveau 2, radio)
- **Source des outils**
  - http://rfakeap.tuxfamily.org

# Quelques mots sur le réseau

- **Bonne couverture WiFi**
- **Bornes Cisco A/B/G**

- **Protection du réseau**
  - Fonctionnalités IDS Cisco
  - Architecture « Network Chemistry » en overlay
  - 802.11 complètement ouvert



# Questions ?

Merci pour votre attention

# Références

- **Shmoo**
  - http://www.shmoocon.org

- **Attacking Automatic Wireless Network Selection, Dino A. Dai Zovi, Shane A. Macaulay**
  **http://www.theta44.org/karma/**

- **Hacking the friendly sky**
  - http://www.securityfocus.com/brief/104
  - http://www.nmrc.org/pub/advise/20060114.txt
  - http://blogs.washingtonpost.com/securityfix/2006/01/windows_feature.html
  - http://it.slashdot.org/it/06/01/15/0815207.shtml