HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

OSSIR

CR Blackhat / Defcon

Las Vegas – 30 Juillet au 7 août 2016

Matthieu Schipman
<Matthieu.Schipman@hsc.fr>

Baptiste Dolbeau
<Baptiste.Dolbeau@hsc.fr>

Blackhat 2016 - 19e édition

- Deux parties
  - 30 juillet au 2 août
    → Trainings
  - 3 août et 4 août
    → Présentations
- 9 tracks en parallèle
  → 117 conférences
- Mandalay bay
  - Extérieur > 40°C
  - Intérieur < 20°C

Defcon 24

- Conférences
  - Du 4 au 7 août
- 4 tracks en parallèle

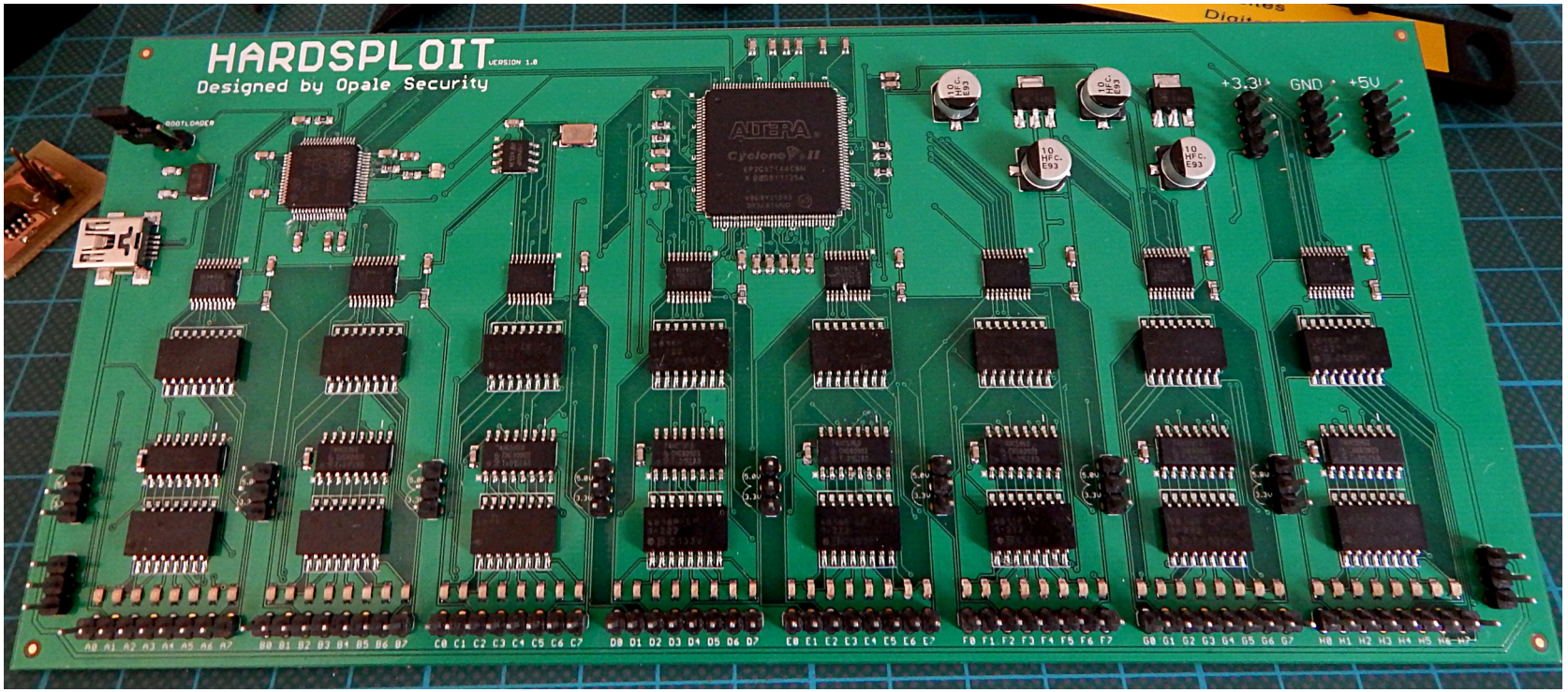
  → 97 conférences
- Bally's et Paris

- Stands & Workshops
  - IOT, Car, Hardware, SE village, crypto
  - Tampering evident & Lockpicking
  - CTF, Coiffures, Etc.

Formations
Hardware Hacking - Hardsploit

(Par Yann Allain et Julien Moinard, Opale Security)

- Audit de sécurité des micro-contrôleurs
- Framework **Hardsploit** (http://hardsploit.io)



Formations
Hardware Hacking - Hardsploit

- Un Pentester Hardware doit interagir avec différentes interfaces :
  - SPI, I2C, UART, JTAG/SWD...
- Hardsploit vise à faciliter cette étape
  - Pour se focaliser sur les vulnérabilités plutôt que l'extraction
  - Y compris pour les non électroniciens
- Composé d'une carte d'interface et d'une GUI
  - Description des composants
  - Aide au câblage
  - Commandes prédéfinies
    - Possibilité de créer également ses propres commandes

Formations
Hardware Hacking - Hardsploit

- Présentation de la démarche d'audit
  - Fingerprinting : étape très importante
    - Recherche des caractéristiques de tous les composants
    - Ports de maintenance, etc
    - Trouver les entrée/sorties correspondantes sur l'équipement
  - Interaction avec les composants, récupération des *firmwares*
    - La carte d'interface Hardsploit facilite beaucoup les choses
  - Recherche de vulnérabilités
    - Protection du code contre les manipulations ou la lecture
    - Vulnérabilités classiques (Buffer Overflow)
    - Etc.
- Beaucoup de manipulations, d'exercices, et… un challenge :)
  - Également une partie sur le SDR (Software Defined Radio)

Formations
Car Hacking Hands On - Vehicle Spy

(Par Robert Leale, CANbusHack, Inc.)

- Formation à la sécurité des véhicules
- Une partie théorique
  - ECU (Electronic Control Unit)
  - Les différents réseaux : K-line, Flexray, MOST, CAN
  - Focus sur le bus CAN, type de trames, messages
  - V2X : V2I (Vehicle to Infrastructure), V2V (Vehicle to Vehicle)
- Une partie pratique
  - Basée sur le logiciel **VehicleSpy** (https://www.intrepidcs.com/)
  - Bus CAN partagé par les stagiaires
  - Un ECU

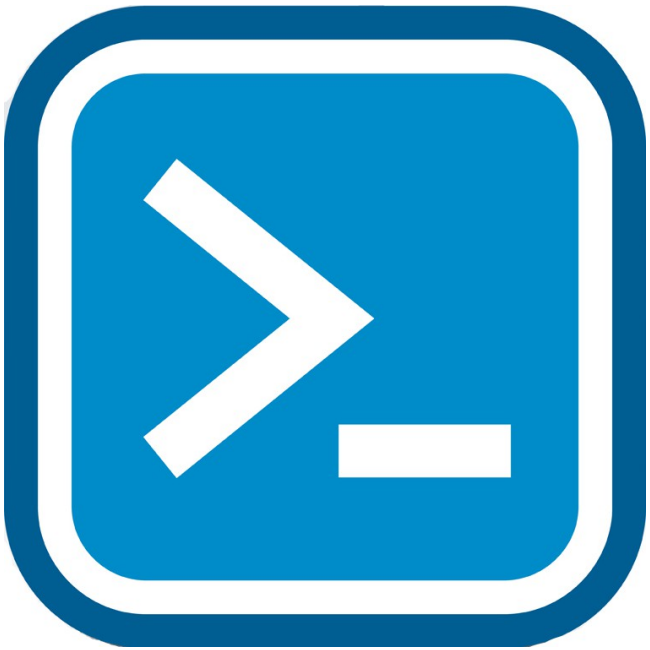
Formations
Car Hacking Hands On - Vehicle Spy

- Écoute du trafic
- Identification de l'ECU cible
- Étude des différents types de messages
- Scan des ECU (détection des services accessibles)
- Injections de paquets forgés
- Déni de service
- Récupération de la mémoire de l'ECU test
- Réalisation de scripts pour des attaques plus complexes

Formations
Offensive Powershell

(Par Matt Graeber, Will Schroeder et Casey Smith, Adaptative Threat Division)

- Audit de sécurité en entreprise



Formations
Offensive Powershell

- Objectifs :
  - Couverture des bases
  - Interactions avec WMI
  - Récupération d'information dans un domaine
    - Active Directory
    - PowerView (ps2)
  - Powersploit
  - Escalade de privilèges (PowerUp)
  - Deploiement de scripts
  - Chargement en mémoire via .NET
  -

Blackhat/Defcon Conférences

Sécurité des systèmes d'exploitation

Système d'exploitation : Linux

- Michael Leibowitz
- PoC d'un rootkit linux Ubuntu
- Spécificité : stockage dans le ramdisk
- Permet également de passer l'upgrade kernel en se réimplantant dans le prochain ramdisk

- https://github.com/r00tkillah/HORSEPILL

Système d'exploitation : iOS

- Equipe « Tencent Keen Security Lab »
- Gagnante sur « Safari to Kernel » à Pown2Own

- Sortie du cloisonnement Navigateur
- Utilisation du contexte graphique
- Récupération de privilèges
- Execution de code arbitraire sur la machine

Système d'exploitation : Windows 10

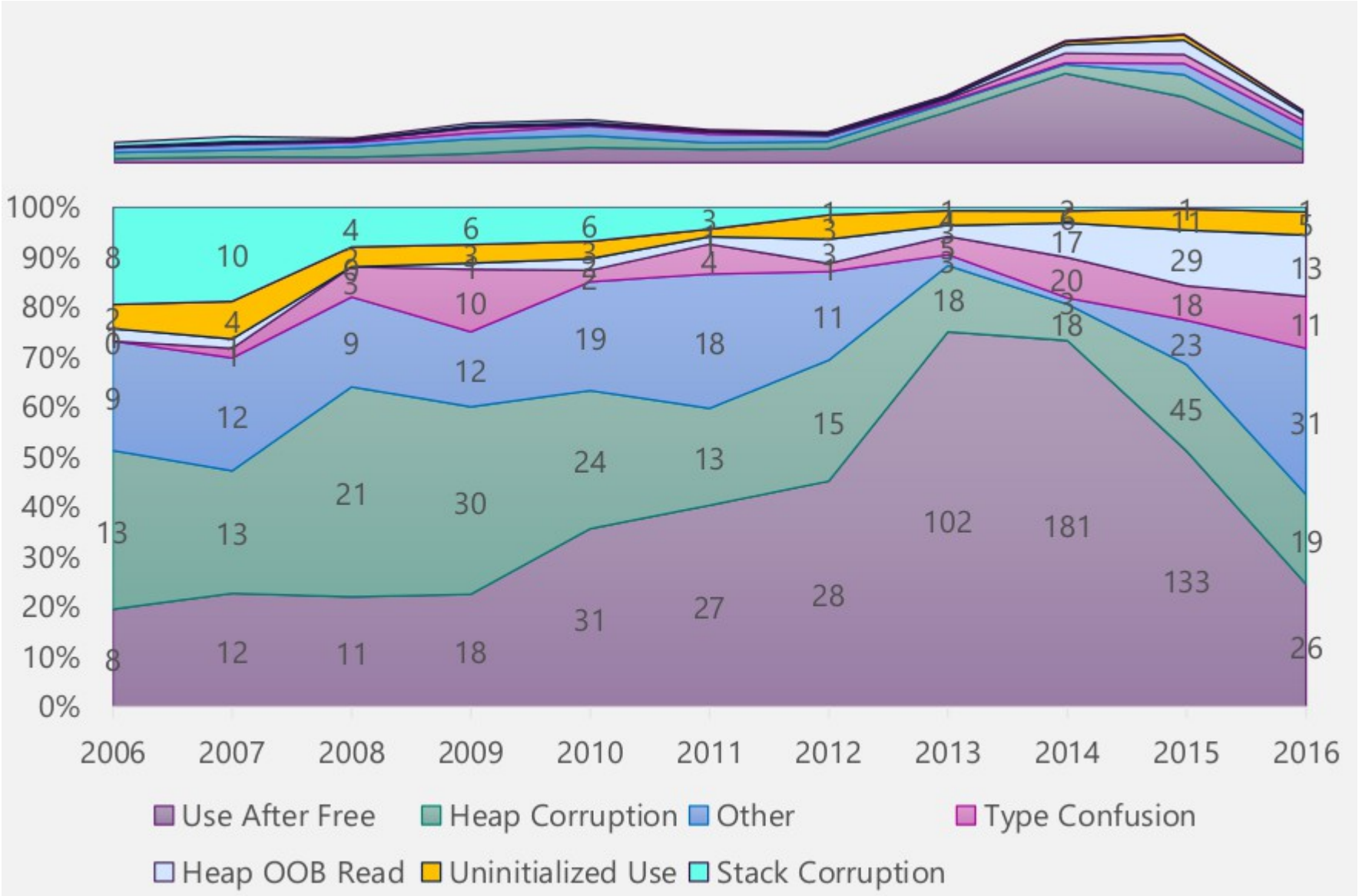
(par Matt Miller et David Weston)

- Historique de la posture sécurité de Microsoft
  - Évolution importante ces dernière années
  - Analyse de menaces, sécurité offensive

- Objectif :
  - Ne plus seulement corriger les bugs unitairement
  - Supprimer des « classes de vulnérabilités »

    Ex : nouveau Garbage Collector contre les attaques de type "use-after-free"

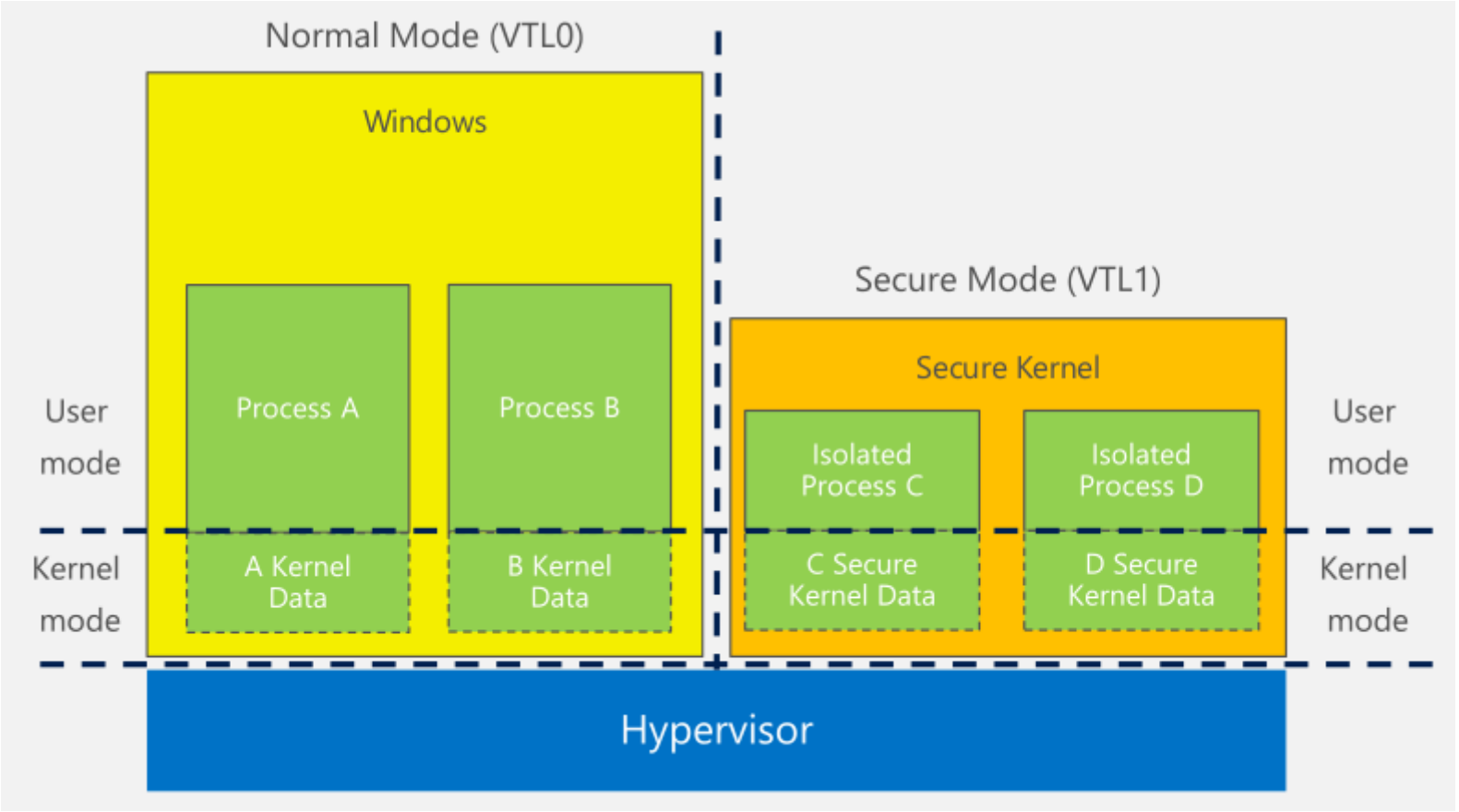
Système d'exploitation : Windows 10



Root causes of Windows, Internet Explorer, and Edge Remote Code Execution (RCE) CVEs by patch year

Système d'exploitation : Windows 10

- 2nde partie : présentation (rapide) des contre-mesures
- Ex : **Credential Guard** et **VBS (Virtualization-Based Security)**
  - Isoler les fonctions les plus critiques de l'OS dans une VM dédiée



Système d'exploitation : Windows 10

- Le processus LSA « standard » (VTL0) communique avec le LSA sécurisé (VTL1)
  - Meilleure protection des données d'authentification
- Autre ex : énorme **réduction de la surface d'attaque d'Edge**
  - Plus d'ActiveX, plus de Vbscript/Jscript, etc.
- Résultat : baisse de 56 % des RCE par rapport à IE
- Aucune des mesures présentées n'est infaillible

  (cf conférence de Rafal Wojtczuk sur les limites et contournements)
- Mais elle représentent **des avancées très intéressantes**

Entreprises - Active Directory

(Par l'équipe Adaptative Threat Division)

- Outil de graphique de chemins d'attaque
- Outil « Active-Directory-Control-Path » de l'ANSSI

- Objectifs :
  - Avoir une meilleur vue des chemins menant à un objet
    - Pour défendre
    - Pour attaquer

Entreprises - Active Directory

- Fonctionnement en deux temps
  - Extraction des informations via Powershell (powerview)
  - Population d'une base de donnée node4j

- Exemples :
  - Recherche vers un utilisateur
  - Recherche vers un ordinateur
  - Recherche vers le groupe « Domain Admins »

Blackhat/Defcon Conférences

Sécurité des véhicules

Sécurité des véhicules

- De nombreuses conférences sur ce sujet
  - Camions, véhicules autonomes, etc...
  - Majoritairement autour de la sécurité du bus CAN
- Une formation, des ateliers, un village Defcon
  - Formation VehicleSpy (2 jours) très intéressante

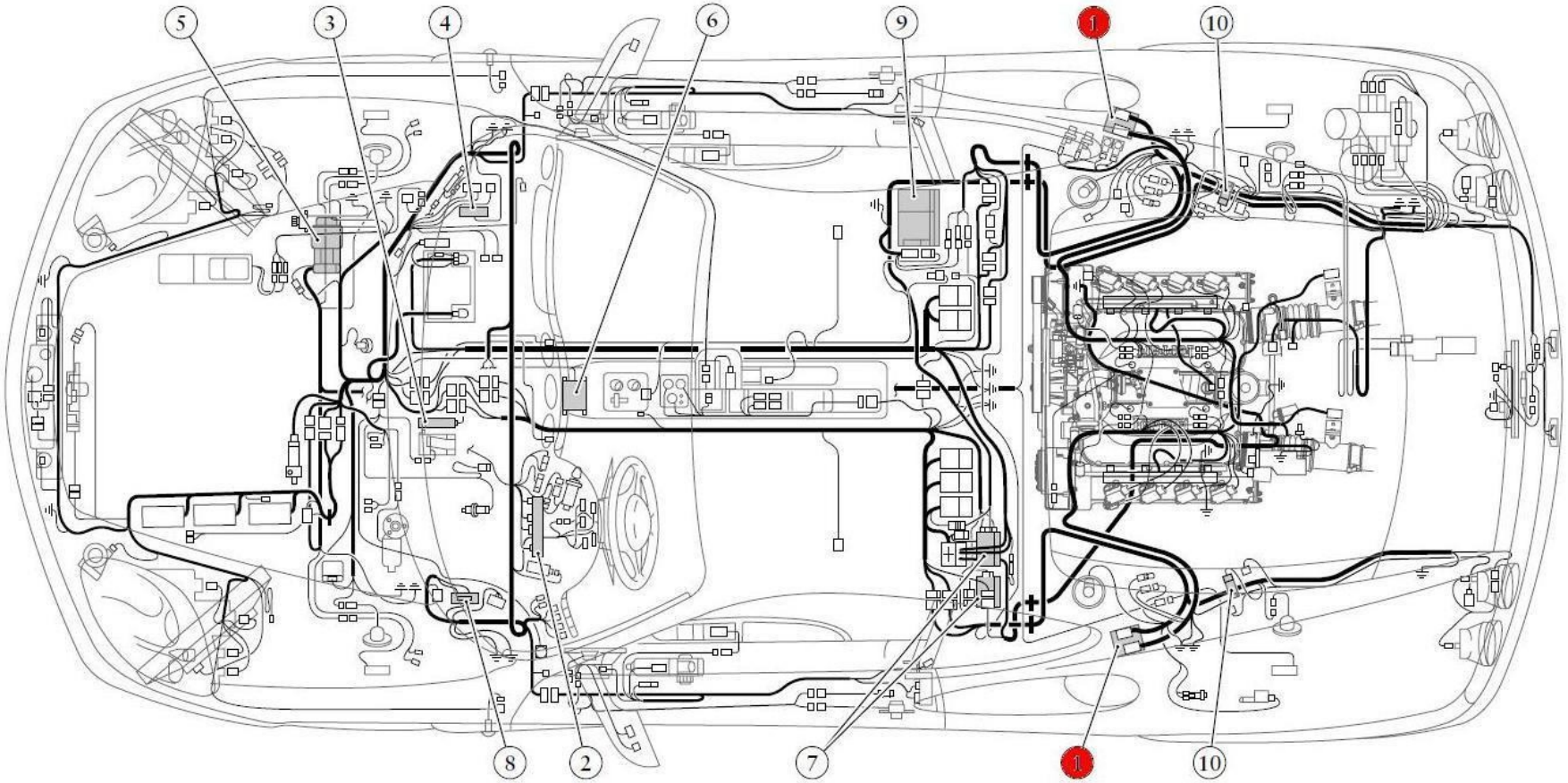
    (Car Hacking Hands On, Robert Leale, CanBusHack, Inc.)
  - « Village » avec démonstrations et conférences additionnelles
  - Ateliers permettant de se familiariser avec le hardware

Sécurité des véhicules
les ECU

- ECU = Electronic Control Unit
  - Modules électroniques contrôlant un sous-système
  - Une voiture récente peut en comporter une centaine !

- De multiples fonctions
  - Confort des passagers (climatisation, vitres, etc.)
  - Également des fonctions critiques :
    - Contrôle du moteur
    - Freinage
    - Direction

Sécurité des véhicules
Les différents réseaux



1. *Motronic (one per bank)*
2. *Instrument Panel*
3. *Air conditioning system*
4. *Shock absorber setting adjustment*
5. *ABS-ASR*
6. *Air bags*
7. *Anit-theft system*
8. *Power windows/Doors*
9. *"F1" gearbox*
10. *Catalytic converters*

Sécurité des véhicules
Le bus CAN

- CAN = Controller Area Network
  - Bus série multi-maîtres
  - Présent dans tous les véhicules (récents)
  - Segmentation du réseau en fonction de la sensibilité des ECU

- Nombreuses possibilités d'attaques
  - Dénis de service
  - Rebond entre les différents segments
    - Ex : du système multimédia vers les systèmes critiques
  - Attaques de l' « homme du milieu »
    - Récupération de données
    - Rejeu, Injection de paquets

Sécurité des véhicules
Le bus CAN

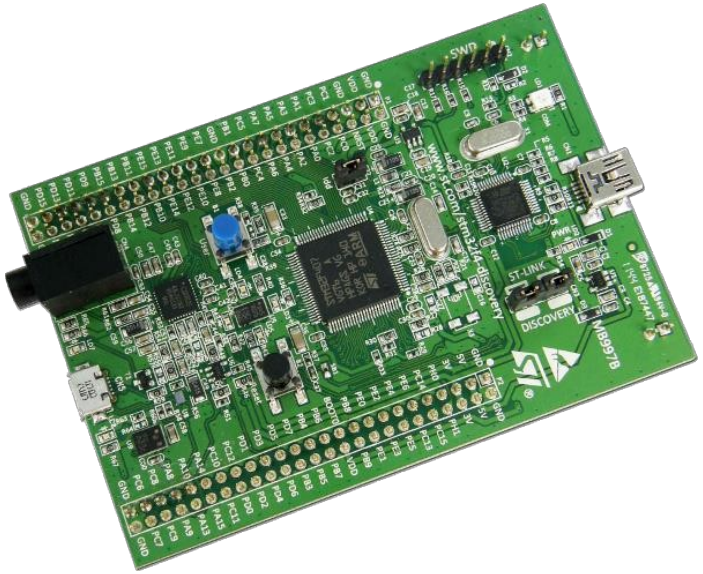
- MAIS…
  - Le bus CAN est très sensible à la latence : Interception difficile
  - Problèmes de la gestion des conflits
  - Comment accéder au bus ?
    - Connexion physique
    - Mais aussi attaques à distance (Bluetooth, WiFi, RDS...)

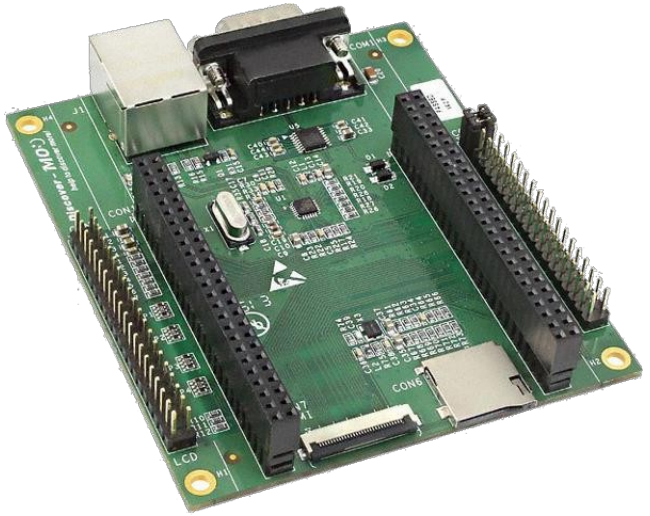
- Beaucoup de conférences présentent des outils et les moyens mis en œuvre pour contourner les restrictions
  - Cartes d'interface pour la rapidité
  - Suites logicielles plus ou moins évoluées
  - Majoritairement open-source

Sécurité des véhicules
CANspy

(par Jonathan-Christofer Demay et Arnaud Lebrun (Airbus))

- Outil open source d'analyse et d'attaque du bus CAN
- Composé d'une carte d'interface et d'une suite logicielle
- Plusieurs extensions existent déjà
  - Double CAN
  - CAN over Ethernet





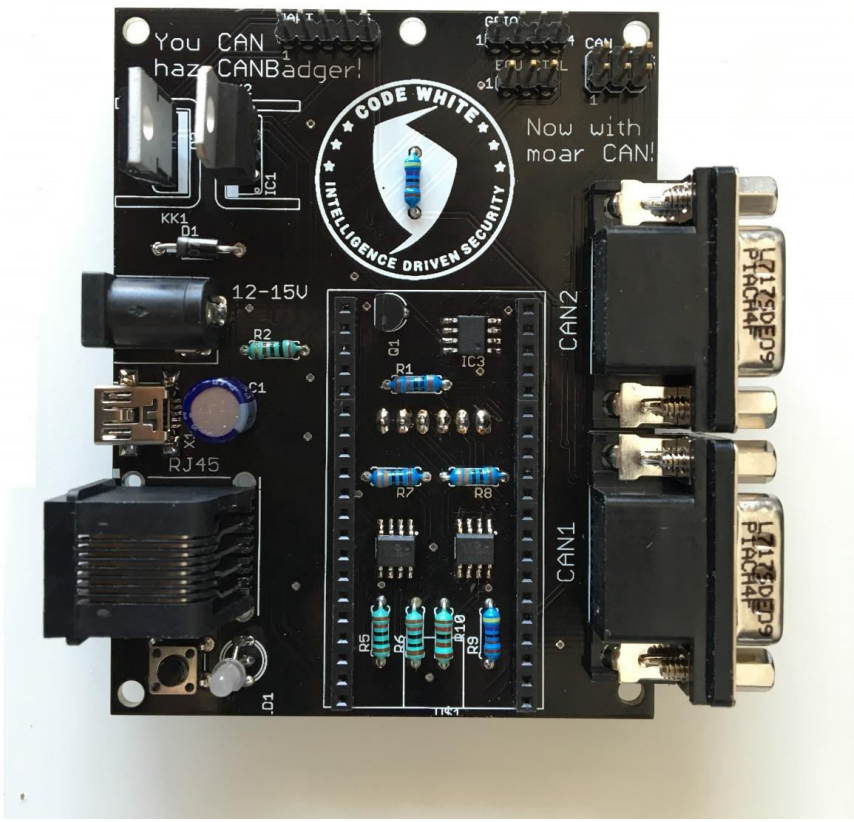
Sécurité des véhicules
CANspy

- Permet d'écouter, filtrer, injecter des paquets
- Peut fonctionner de manière autonome...
  - Des règles prédéfinies conditionnent les actions
- … ou interactive
  - Transfert sur Ethernet
  - Manipulation avec par exemple Scapy

Sécurité des véhicules
CANbadger

(Par Javier Vazquez Vidal et Ferdinand Noelsche)

- Principe identique :
  - Carte d'interface
  - Suite logicielle
- Synchronisation possible avec un "CANbadger server"
  - permet de mener des attaques beaucoup plus élaborées



Sécurité des véhicules
Injection CAN avancée

(Par Charlie Miller et Chris Valasek)

- Accéder au bus CAN ne suffit pas
- L'injection avancée de messages CAN est complexe
  - Restrictions au niveau des ECU
  - Ex : possible de modifier la direction/freinage/accélération seulement sous certaines conditions
  - Ex : envoi de messages de diagnostic permis seulement à faible vitesse
- Comment contourner ces restrictions
  - Neutraliser l'ECU légitime tandis qu'on injecte des données forgées
  - Flasher l'ECU avec un code malveillant

Sécurité des véhicules
Injection CAN avancée

- Résultat :
  - Freinage ou changement de direction à distance
  - Manipulation du régulateur de vitesse
  - Etc…

- Solutions proposées
  - Restrictions supplémentaires sur l'acceptation des messages de diagnostic par les ECU
  - Ajouter des fonctions d'IDS/IPS, ex :
    - Détection de messages dupliqués par l'ECU émetteur
    - Détection des changement de fréquence d'émission de messages
  - Signature du code des ECU (pas seulement un checksum)

Blackhat/Defcon Conférences

Conférences diverses et variées...

Études de produits de « sécurité »

- Quelques conférences portaient sur des produits de sécurité
  - Physiques
    - Verrous électroniques
  - Logiques
    - conférence marquante sur les antivirus

    (Stephan Huber et Siegfried Rasthofer)

Études de produits de « sécurité »
Verrous Bluetooth

(Par Anthony Rose et Ben Ramsey, Merculite Security)

- « Bluetooth Smart », ou BLE (Bluetooth Low Energy), ou Bluetooth 4.0+
  - Très faible consommation
  - Idéal pour les objets connectés
  - Présent dans de très nombreux équipements
    - Téléviseurs, grille pains, capteurs médicaux...
    - et… verrous électroniques (pour portes, voitures, etc.)

- Étude de différents verrous pilotés par smartphone
  - Cadenas et verrous de portes

Études de produits de « sécurité »
Verrous Bluetooth

- Résultats :
  - Mots de passe codés en dur
    - Probablement déjà tous publiés sur Internet…
  - Mots de passe envoyés en clair
    - Possible de l'intercepter, et de le changer !
  - Attaques par rejeu
    - Pas besoin de casser le mot de passe
  - Fuzzing qui désactive le verrou (mode erreur)
  - Absence d'authentification (spoofing du verrou)
  - Crypto « maison »
  - Ouverture avec un simple tournevis
  - Etc. etc. etc...

Études de produits de « sécurité »
Verrous Bluetooth

- D'autant plus alarmant que

1) Ces verrous sont de plus en plus populaires

2) Il est possible « d'industrialiser » les attaques
   - Wardriving
     - Avec un Ubertooth One (Michael Ossmann)
     - Et une bonne antenne : portée = jusqu'à 400m
   - Aussi réalisable avec un drone...

Études de produits de « sécurité »
Antivirus Android

(Par Stephan Huber et Siegfried Rasthofer)

- Étude des sept antivirus les plus utilisés sur Android
  - McAfee, Kaspersky, Avira, ESET et autres

- Résultats :
  - Absence de vérification des certificats
  - Chiffrement par du XOR avec une clef fixe
  - Exécution de code distante
  - ...

Conférences diverses
Attaque sur RSA-CRT

(par Marco Ortisi)

- Attaque de type *side channel*
  - Connue depuis 1996 (Arjen Lenstra, démonstration théorique)
  - 2001 : attaque sur PGP (Vlastimil Klíma and Tomáš Rosa)
  - 2015 : première attaque sur TLS (Florian Weimer)
    - Constatation de cas réels de fuites de clefs
- Pré-Requis :
  - Utilisation de l'optimisation RSA CRT (Chinese Remainder Theorem)
    - Très commun, permet déchiffrement et signature RSA plus rapide
  - Une erreur lors la signature RSA
  - Signature d'une valeur connue par l'attaquant

  => Fuite de la clef privée

Conférences diverses
Attaque sur RSA-CRT

- Attaque considérée « extrêmement difficile » (et donc improbable) par certains constructeurs (ex : Dell Sonicwall)
- L'auteur prouve que non :
  - Réalisation de 2 outils :
    - High Voltage! : approche active (envoie de nombreuses requêtes)
    - Piciolla : passif, analyse des captures réseau
- Les erreurs de calcul ne sont pas si rares
  - Notamment sur les systèmes embarqués
    - Surchauffe CPU, barrette mémoire défectueuse, rayonnements, etc.
  - Mais aussi sur certains boitiers de sécurité

Conférences diverses
Étude inforensique sur les SSD

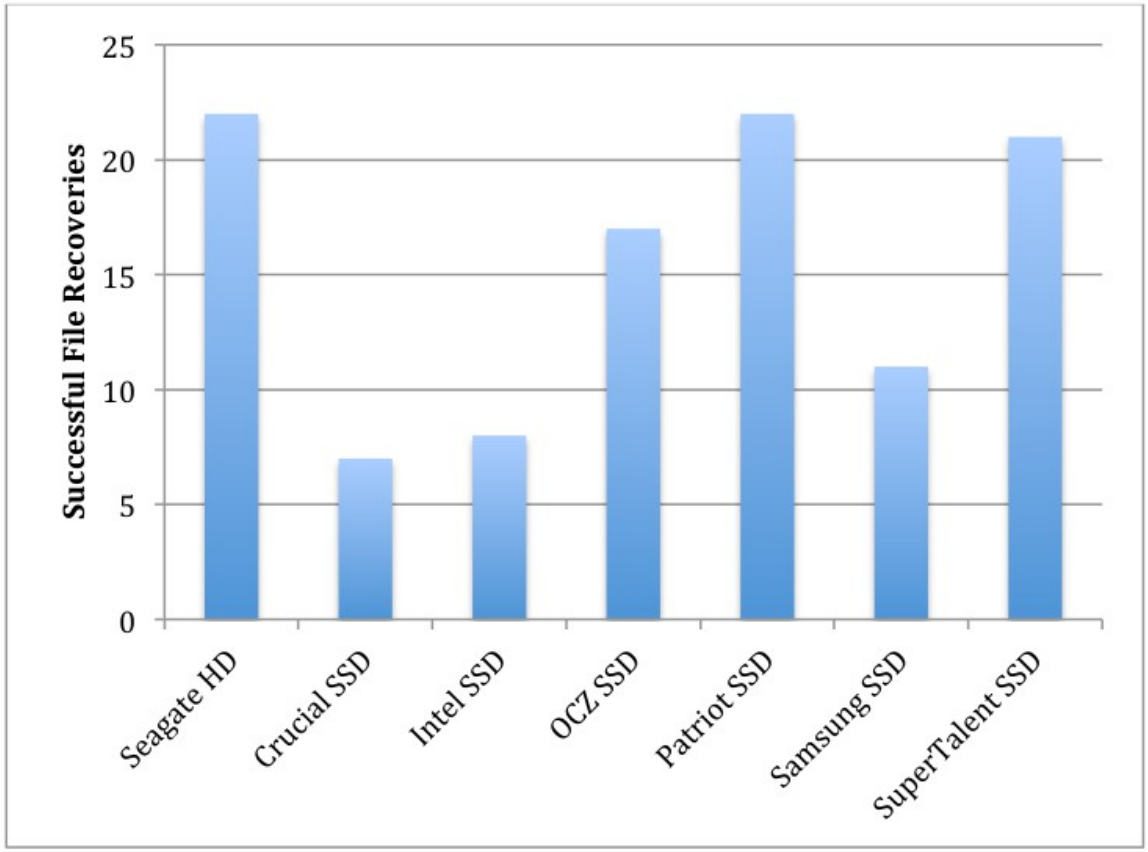
(Par Tom Kopchak)

- Comportement des SSD dans un contexte inforensique
- Les disques durs standards ont un comportement connu
  - identique quelque soit leur constructeur et leur version
- Ce n'est pas le cas pour les SSD
  - Varie selon les fabricants…
  - ...et même les versions du firmware !

- Étude avec un disque standard témoin et des SSD de différentes marques et générations
- Une suppression simple et un formatage rapide

Conférences diverses
Étude inforensique sur les SSD

- Variations très importantes :



Conférences diverses
Étude inforensique sur les SSD

- Formatage rapide (= sans écrasement) vs effacement :
  - Formatage rapide globalement plus difficile à récupérer
- Pas d'assurance de récupérer les fichiers
  - Nécessité de faire des tests préalables
  - Respecter la combinaison OS / marque du SSD / firmware

Conférences diverses
Sécurité du future

- Cyber Grand Challenge

- Organisé par la DARPA
- ~100 équipes au départ, 7 en finale

- Principe
  - Challenge 100 % autonome
  - Fuzzing du binaire
    - Développement d'exploits pour attaquer les autres machines
    - Développement de patches pour se protéger