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 – 06 au 10 août 2014

Steeve Barbeau <Steeve.Barbeau@hsc.fr>
Ines Ribeiro <Ines.Ribeiro@hsc.fr>

BlackHat 2014

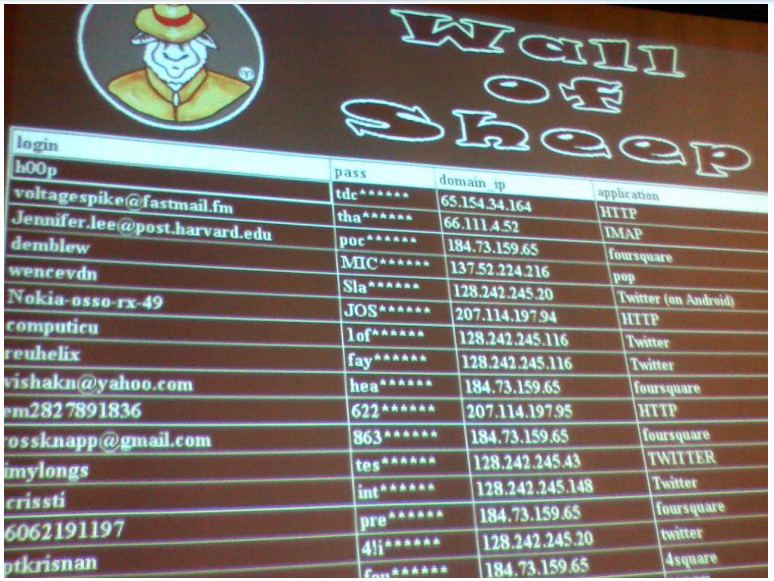
- 17e édition
  - Du 6 au 7 août
- ~10 tracks
- 8 000 participants (91 pays)
- Au Mandalay Bay
  - Clim bien trop forte
  - Temperature externe bien trop forte

Defcon 22

- Du 7 au 10 août
- 4 tracks + 101
- 16 000 participants
- Rio (dernière année)
  - Un peu loin du strip
  - Au Bally's et au Paris l'année prochaine

Stands/Workshops

- WiFi
- Lockpicking
- Social Engineering
- SCADA
- “Packet hacking”
- “Tamper evident”
- Hacking hardware



Bonus

- Pwnies Award
  - Chanson gagnante nulle
- Defcon badge challenge
- Salon de coiffure
- CTF
- Des vendeurs (matériel, T-shirts...)
- Attaques sur une voiture Tesla

- Outrepasser les IPS en utilisant une imprécision dans la définition des entêtes d'extension IPv6
  - Chaque entête d'extension possède un champ « next header » indiquant le type de l'entête suivant
    - Si le paquet est fragmenté, ce champ contient le type du premier entête non fragmentable dans tous les fragments
    - Mais seule la valeur du premier fragment est utilisée pour la recomposition du paquet
    - Alors que les IPS utilisent le next header de chaque fragment pour parser le contenu

Attacking Broadband modems
Andreas Lindh

- Conférence sur différentes vulnérabilités des modems USB Huawei et ZTE
  - Présence de CSRFs
    - Envoi de SMS vers n'importe quel numéro
    - Création d'un nouveau profil de connexion avec DNS statique
  - Persistence possible grâce à des injections XSS stockées
    - Fichiers de configuration
    - Appelés pour la page d'accueil
- Exemple d'attaque où l'utilisateur est redirigé vers un site malveillant depuis le nom de domaine qui envoie ensuite son login/mot de passe par SMS à l'attaquant

Android FakeID vulnerability
Jeff Forristal

- La chaine de certificats n'est pas correctement vérifiée, permettant d'usurper la signature du certificat
  - Processus de signature incomplet
    - Un seul élément valide de la chaine rend toute la chaine de confiance
    - L'installeur d'application vérifie l'issuer du certificat et l'ajoute à la chaine
    - L'installeur ne vérifie pas que la clef publique est effectivement signée par l'issuer
  - Les applications obtiennent certains privilèges selon leurs signataires (plugin webdev)
    - Pas besoin de demander de droits spécifiques à l'installation

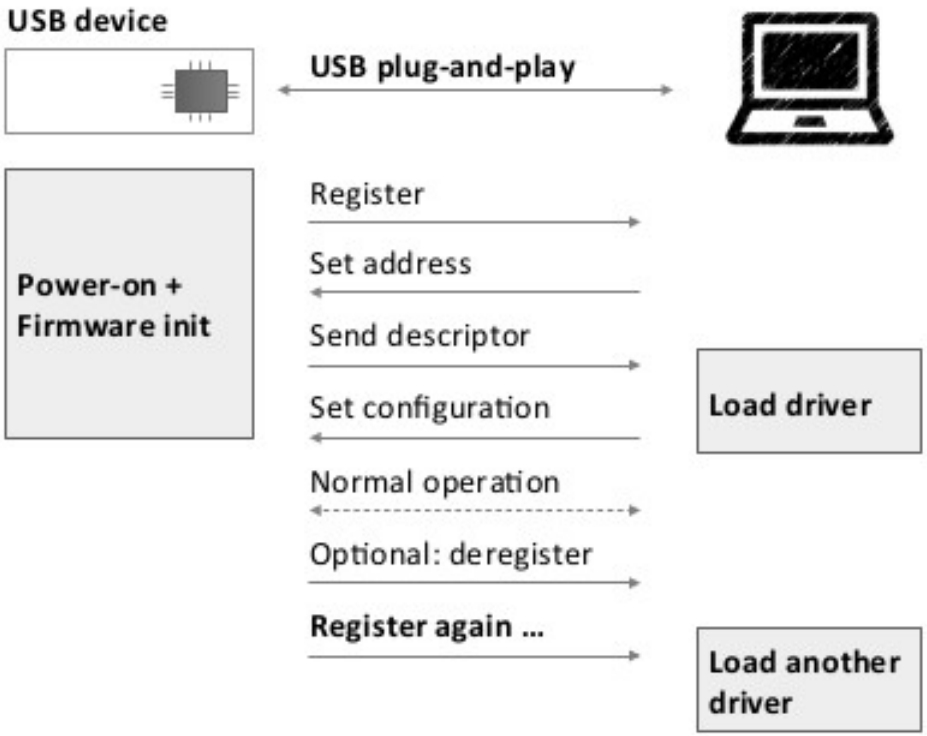
VoIP Wars
Fatih Ozavci

- Conférence sur l'outil Viproy servant à attaquer la VoIP Cisco
  - Présentation confuse et passant très vite sur tous les détails techniques

- Les widgets sont les composants graphiques d'une application
  - Possèdent divers attributs (lecture seule, activé/désactivé)
  - Accessibles à l'utilisateur courant même hors de l'application
- Si la sécurité de l'application repose sur le widget (bouton grisé, onglet caché), il est possible d'outrepasser les restrictions
  - GEMs : éléments qui présentent une fuite d'information, un callback ou une modification d'information via un widget
  - L'outil GEMminer permet de le retrouver
    - Compare pour une application les widgets selon des comptes à privilèges différents

BadUSB
Karsten Nohl - Jakob Lell

- Conférence présentant la réécriture d'un firmware USB afin de prétendre être un autre type de périphérique USB
  - Étude du firmware USB de certaines clefs USB
  - C'est la clef qui annonce qu'elle est une clef à l'ordinateur, donc comportement modifiable
  - Périphérique automatiquement monté



BadUSB
Karsten Nohl - Jakob Lell

- Différents modèles d'attaque possibles
  - Prétendre être un CD-rom d'installation pour ajouter un driver avant utilisation de la clef elle-même (modèle clefs 3G)
  - Prétendre être un clavier et envoyer des commandes
  - Lancer l'économiseur avec un prompt de mot de passe vérolé
  - Changer la configuration réseau en ajoutant une deuxième carte réseau (se presenter comme un serveur DHCP)
- Chaque type de clef USB nécessite l'étude de son firmware pour réaliser l'attaque

- EnergyWise: protocole Cisco pour la gestion de l'énergie
  - Aucun chiffrement
  - Authentification par PSK avec éventuellement timestamp
- Différentes attaques ont été découvertes
  - Analyse du protocole (pas de documentation disponible)
  - En UDP, aucun identifiant unique par paquet
    - Rejeu possible directement
  - En mode PSK sans timestamp, possible de bruteforcer la clef à partir des paquets capturés

GRR
Greg Castle

- Outil ayant pour but de réunir la définition de plein de types d'artefacts inforensiques
  - Artefacts multiplateforme (historiques web par exemple)
  - Définition de variables pour obtenir les chemins complets (répertoires d'installation, homes)
  - Automatisation du processus de remplacement des variables pour éviter les interventions humaines
- Possibilité de définir des parsers de données après la récupération

SVG: Exploiting browsers without bugs
Rennie deGraaf

- Rappels sur le format SVG
  - Chargé soit en tant qu'image, soit en tant que document incorporé
  - Gère les <script>, le CSS, les images externes
  - Sensiblement les mêmes attaques que le HTML
- Exemples d'attaques
  - Billion laughs : injection d'entité XML recursives
  - Injection de scripts modifiant la DOM (ajout d'une image vers evil.com)
  - Modification du comportement du svg s'il est dynamique
  - Ces attaques ne devraient marcher qu'en mode incorporé
    - Pourtant certains navigateurs acceptent l'exécution du contenu
- Crash de navigateurs par inclusions successives

A journey to protect PoS
Nir Valtman

- Conférence sur les différents éléments d'un PoS et comment les attaquer
  - L'application est intéressante car c'est elle qui gère les données de carte bancaire
  - Les bases de données peuvent éventuellement stocker les données de carte pour un mode hors ligne
  - Mauvaises estimations sur les PoS (pas d'accès au net, employé de confiance, démarrage sécurisé, driver de PIN Pad non modifiable)
  - Souvent, un VNC est prévu pour le support à distance
  - L'application est souvent lancée avec les droits admins, codée en Java

Capstone
Quynh Nguyen Anh

- Présentation non technique sur les raisons du developpement de Capstone
  - Outil multiplateformes/architectures
  - Support binding python et ruby (et d'autres)
  - Licence « sympa » (i.e. pas GPL)
  - Nombreuses précisions sur les instructions
  - Basé sur LLVM (fork)

Cellular exploitation on a global scale: the rise and fall of the control protocol
Mathew Solnik et Marc Blanchou

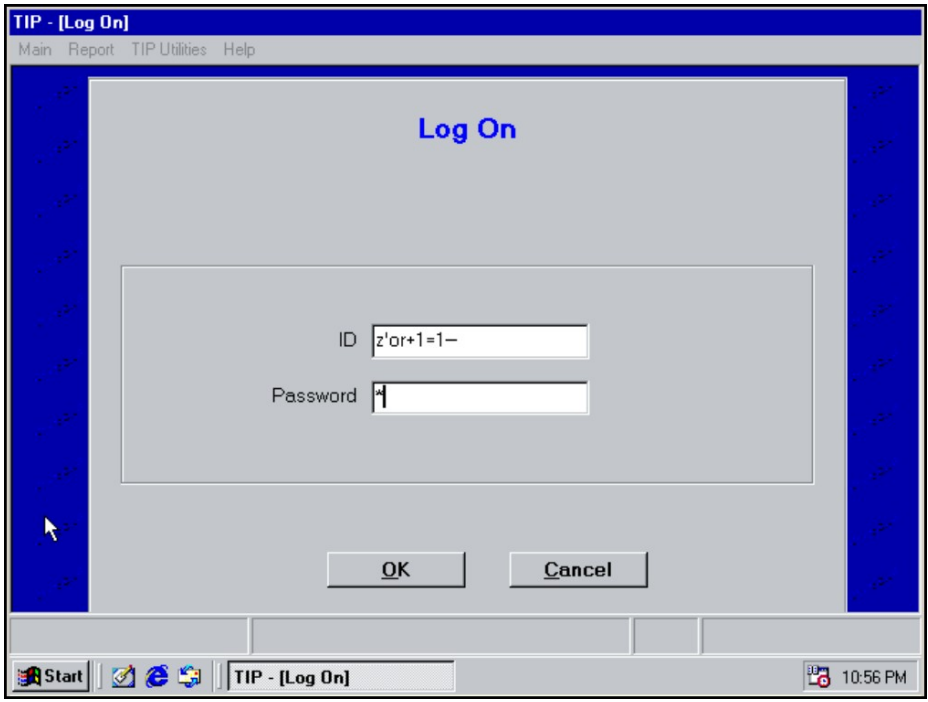
- Analyse du système de contrôle intégré aux téléphones
  - IOS (Sprint), Android, Blackberry, routeurs/PC/voitures 3G
  - Permet de reconfigurer le téléphone, le verrouiller, l'effacer, lister les processus, contrôle de l'APN, installer/supprimer des applications, etc.
- Vulnérabilités
  - Faible authentification: B64(MD5(IMEI+carrier_not_so_secret) (ou HMAC, downgrade possible)
  - Vérification SSL faible
  - Client OMA-DM vulnérable (BoF, corruption de la pile, etc.)
    - Exécution de code sur les différentes plateformes
- Pas eu de démo (manque de temps)

SATCOM terminals: Hacking by air, sea, and land
Ruben Santamarta

- Etude des firmwares d'une vingtaine d'équipements SATCOM
- Vulnérabilités classiques
  - Identifiants/Mots de passe codés en dur
  - Protocoles non sûr et non documentés
    - Lecture/Ecriture de données en mémoire
  - Portes dérobées
- Difficulté de mise à jour
- Si on a un accès physique ou réseau à un SATCOM → Game Over

Pulling the Curtain on Airport Security
Billy Rios

- Documents sur la configuration des checkpoints dispo sur Internet
  - Plan des checkpoints
  - Equipements utilisés (et autorisés)
- Problèmes
  - “Made in china”
  - Accès physiques ou cable réseau
  - Windows 98/CE/XP
  - Mots de passe faibles
  - Comptes en dur et non documentés



Learn how to control every room at a luxury hotel remotely: the dangers of insecure home automation deployment
Jesus Molina

- Chaque chambre a un iPad
  - Connecté au réseau WiFi guest
  - Permet de tout contrôler (TV, lumière, température)
- Utilisation de KNX/IP (UDP)
  - Chaque chambre dispose d'un routeur KNX (IP : 192.178.1.X)
  - Adresse KNX au format Zone/Chambre/Equipement (ex : 2/3/2)
- Contrôle de tous les équipements de toutes les chambres

Oracle Data Redaction is Broken
David Litchfield

- Fonctionnalité assez récente (Oracle 12c)
  - Permet de cacher des données à la volée (procédure DBMS_REDACT.ADD_POLICY)
  - Exemple : remplacer des données bancaires par des étoiles
- Les données étaient cependant accessibles de trois façons différentes
  - RETURNING INTO
  - Xmlquery()
  - Bruteforce dans le WHERE d'une requête SELECT
- Corrigé en juillet
- Papier: http://www.davidlitchfield.com/Oracle_Data_Redaction_is_Broken.pdf

- Récapitulatif des vulnérabilités touchant ces systèmes
  - Peu d'utilisation de SSL
  - 1/3 des certificats utilisés sont valides
  - Injection de commandes sur l'interface Web /cgi-bin/tsocmd
  - Exécution de commandes via les scripts JCL (FTP)
  - Elévation de privilèges CVE-2012-5951 sur z/OS1.1 (2001) à 1.13 (2014)
  - Casser les mots de passe de la base RACL (racl2john → JtR)
  - Privilège BPX.SUPERUSER permettant de passer root sans saisie de mot de passe

Bypass firewalls, application white lists, secure remote desktops under 20s
Zoltán Balázs

- Contexte
  - Serveur accessible uniquement via RDP (depuis certains réseaux)
  - AppLocker déployé sur les postes clients
  - Un poste client compromis (et ayant accès au serveur)
- Création de deux outils
  - Le premier simulant des événements clavier/souris pour
    - Lancer Word
    - Créer une macro chargeant une charge utile (shellcode/DLL)
  - Le second est un driver permettant de rediriger les paquets sur le port du shell en écoute
- Outils
  - https://github.com/MRGEffitas/Write-into-screen
  - https://github.com/MRGEffitas/hwfwbypass

Hack All The Things: 20 Devices in 45 Minutes CJ Heres, Amir Etemadieh, Mike Baker, Hans Nielsen

- Obtention d'un accès root sur des appareils connectés (réfrigérateur, ampoule, smart TV, lecteur Bluray, etc.)
- Utilisation de une ou plusieurs des méthodes suivantes
  - UART (Universal Asynchronous Receiver/Transmitter) via port de debug
  - Modification du système de fichiers sur eMMC (embedded Multi-Media Card)
  - Injection de commandes (via interface Web)

Abusing Software Defined Networks
Gregory Pickett

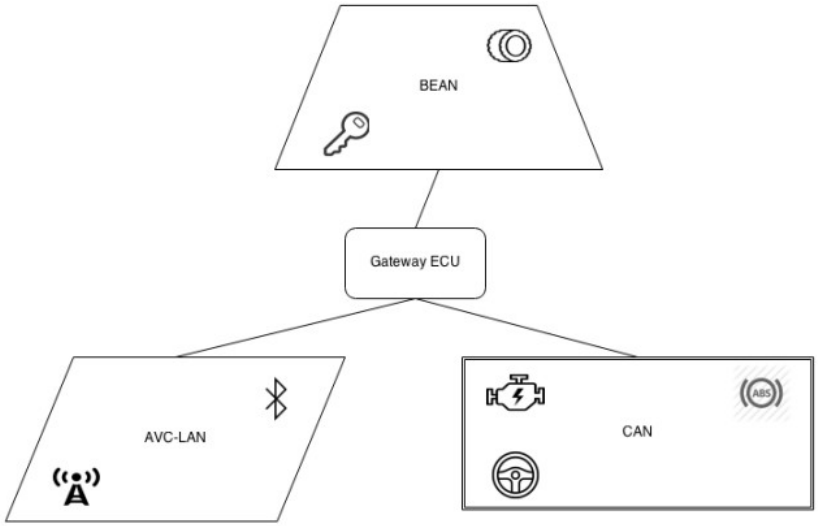
- Réseaux SDN composés de
  - Contrôleur, prenant les décisions de routage
  - Commutateurs, transmettant les paquets suivant les règles de flux
  - Protocole de communication (ex : Openflow)
- De nombreuses vulnérabilités (de jeunesse ?)
  - Chiffrement/authentification optionnel (et pas supporté par tous les contrôleurs)
  - Très sensible aux attaques par déni de service
  - Obtention et modification des flux
- Outils: http://sourceforge.net/projects/sdn-toolkit/files/

A survey of remote automotive attack surfaces
Charlie Miller et Christopher Valasek

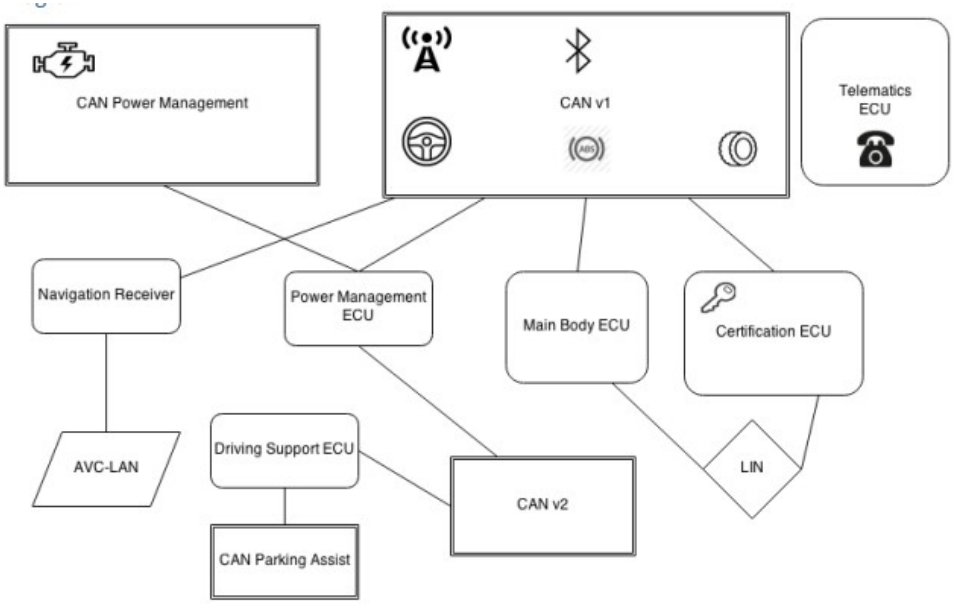
- Les automobiles contiennent de plus en plus d'ECUs pour mesurer et contrôler certains éléments (ABS, détection d'obstacle, régulateur de vitesse, etc.).
- De plus en plus connectées (navigateur, WiFi, bluetooth, etc.)
- Comparaison des réseaux de 20 véhicules
  - Différents modèles, constructeurs, années
  - Augmentation
    - Du nombre d'ECUs
    - Du nombre de réseaux
    - De la surface d'attaque
- Démo de “jailbreak” de Jeep

A survey of remote automotive attack surfaces
Charlie Miller et Christopher Valasek

Toyota Prius (2006)



Toyota Prius (2014)



Besoin de plus d'infos ?

- Blackhat
  - https://www.youtube.com/user/BlackHatOfficialYT
  - https://www.blackhat.com/us-14/archives.html
- Supports DEFCON
  - https://www.defcon.org/html/links/dc-archives/dc-22-archive.html

Des questions ?

Merci à l'OSSIR pour sa participation