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

Groupe OSSIR Paris

Compte-rendu Black Hat USA 2009

Christophe Alladoum
<Christophe.Alladoum@hsc.fr>

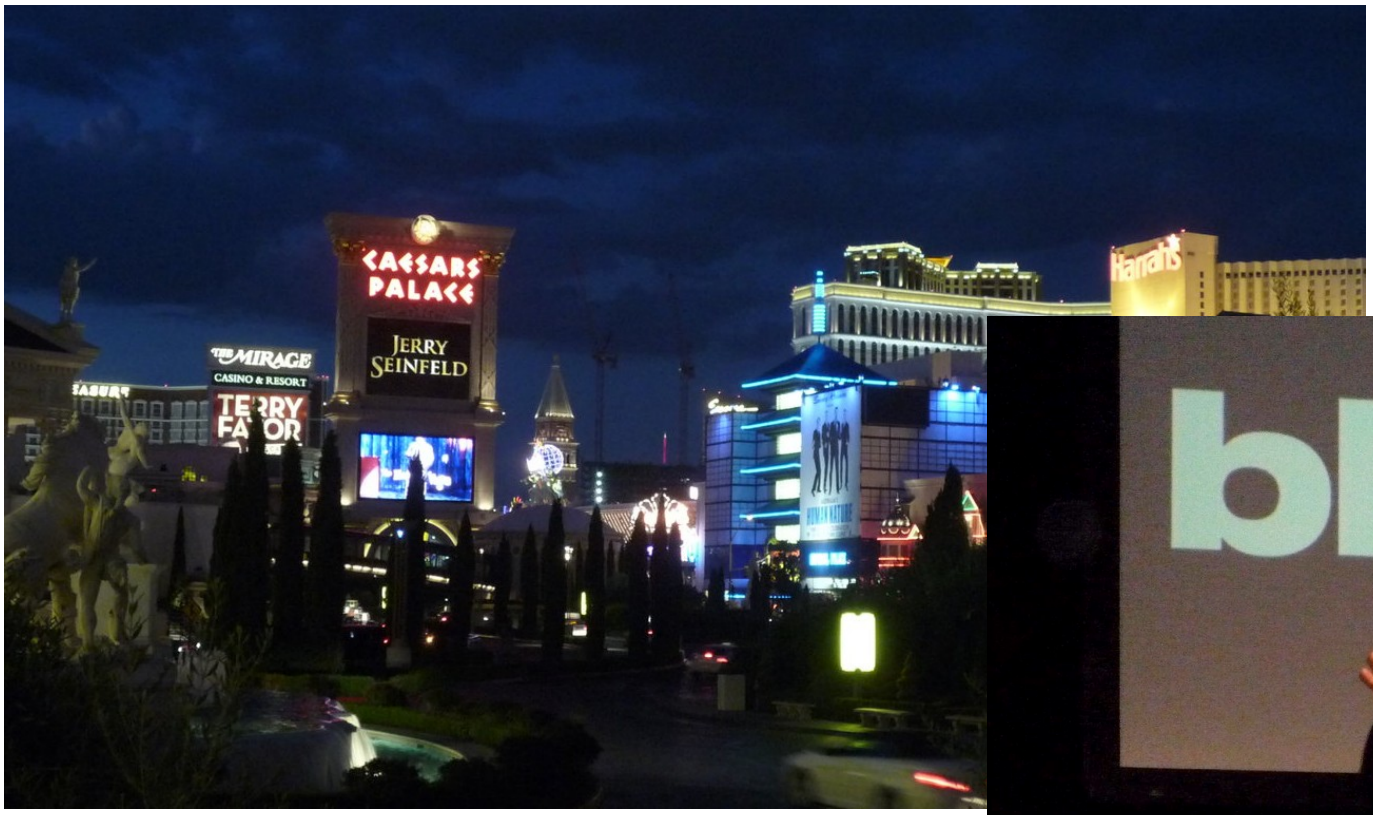
Julien Raeis
<Julien.Raeis@hsc.fr>

Black Hat USA 2009

- Dates :
  - Training : 25 au 28 juillet (sur 2 ou 4 jours)
  - Briefing : 29 et 30 juillet

- Lieu : hôtel Caesars Palace à Las Vegas
  - 8 conférences en parallèle dans les salles de bal du Caesars
  - Environ 6000 participants
- Plus de 80 conférences au total
- Merci à l'OSSIR pour sa participation !

Photos



Les « faits marquants » de 2009

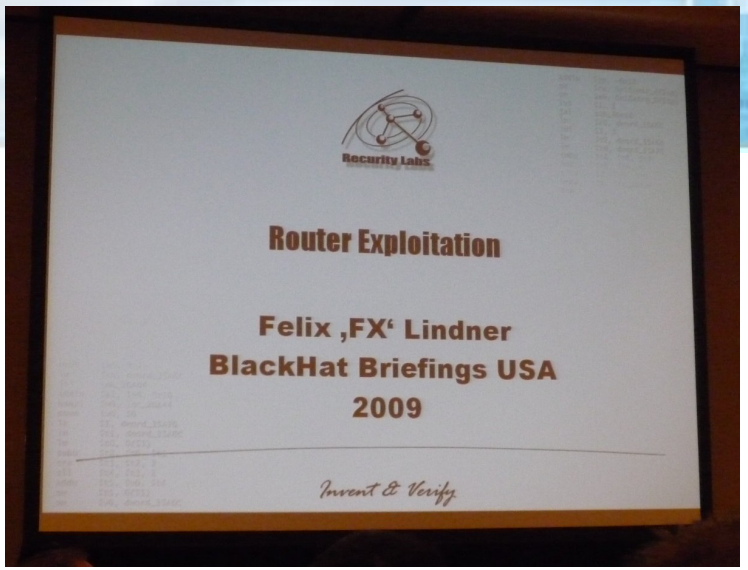
- Attaques fonctionnelles sur les implémentations SSL
- Bon nombre d'attaques très bas niveau
  - BIOS, Chipsets
  - Matériel
- Une *track* entièrement dédiée à la virtualisation
  - Première apparition de VMSafe
  - Sortie d'isolation dans VMware

- BlackHat Europe 2010 aura lieu à Barcelone

Router exploitation

- Felix 'FX' Lindner (Recurity Labs)
- Très peu de codes d'exploitation sur les équipements réseau
  - Peu de vulnérabilités publiques également
    - Cisco : 14 avis en 2008
    - Juniper ou Nortel : pas de rapports de vulnérabilités
- Quatre vecteurs possibles
  - Services réseau (HTTP, TFTP, FTP, SNMP, etc.)
  - IPv6, VoIP (Huawei active H.323 par défaut sur certains modèles)
  - Routeur « client » (telnet, SSH, tftp, authentification, DNS, etc.)
  - Paquets en transit
    - Moyen parfait pour compromettre en masse
    - Peu d'inspection de paquets (IPv6)

Router exploitation



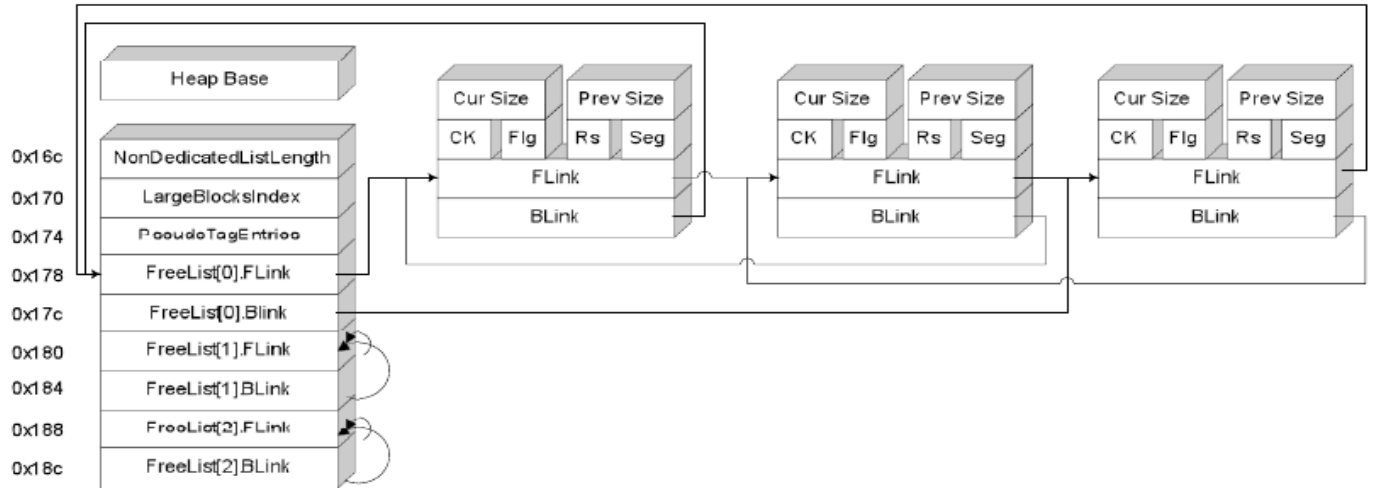
- Exploiter Cisco
  - Linux 2.4 sur Cisco 65xx et 72xx
    - Techniques « classiques »
  - IOS
    - Binaire ELF exécuté en mode Superviseur
    - Un seul tas, pas de segmentation mémoire, *threads*
      - Plantage et redémarrage en cas d'exception ou de corruption
    - Sections à des adresses statiques
    - « Every single Cisco engineer has its own Makefile »
      - 272722 images IOS différentes identifiées !
      - Difficile de trouver des adresses stables pour l'exploitation
      - Pas de symboles
    - Comment trouver une adresse de retour stable ?

Router exploitation

- L'adresse de retour
  - Adresse du tas ou de la pile imprévisible
  - Code imprévisible sans connaître la version de l'image
  - IOMEM non-exécutable
  - ROMMON est à une adresse fixe
    - Peu de versions différentes de ROMMON
    - Mais impossible à identifier à distance
  - Alternatives ?
    - Sur 1597 images différentes, quelques similarités dans le code
      - Certaines parties restent à des adresses fixes pour un numéro de version donné
      - Et il est possible de trouver la version à distance !
- *Shellcode* : création d'un VTY

Advanced Windows Heap Exploitation

- John McDonald et Chris Valasek (IBM ISS X-Force)
- **Objectif** : agréger les connaissances du tas sous Windows
- Rappel du fonctionnement du tas dans Windows depuis XP SP2 : le **Windows Heap Manager**
  - Front-end (LAL, LFR)
  - Back-end (FreeList[128])
  - Algorithme d'allocation | de libération



Advanced Windows Heap Exploitation

- Quelques techniques connus d'exploitation :
  - Lookaside List Link Overwrite
  - Bitmap Flipping Attack
- De nouvelles techniques :
  - Corruption du Heap Cache (de-sync attack)
  - Bitmap XOR Attack

Sniffing Keystrokes With Lasers/Voltmeters

- Andrea Barisani et Daniele Bianco (Inverse Path)
- Attaques sur les claviers
  - Fuites électro-magnétiques (cf. SSTIC'09 – Vuagnoux / Pasini)
  - Emanations acoustiques
- Fuites électro-magnétiques des claviers PS/2
  - Faible blindage, fuites vers la terre, fréquence d'horloge distinctive
  - Expérience : filtrage des fuites enregistrées vers la terre avec un filtre passe-bande (10 – 16.7 kHz) puis isolation des signaux
  - Attaque valable jusqu'à 20 mètres au moins
  - Coûte moins de $150

Sniffing Keystrokes With Lasers/Voltmeters

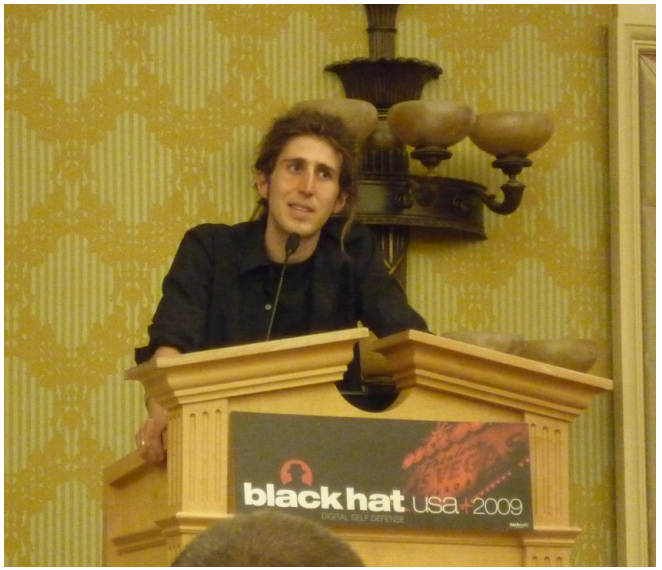
- Émanations acoustiques
  - Utilisation d'un microphone laser
  - Pointé sur l'ordinateur portable
  - *Dynamic time warping* pour mesurer les similarités des signaux reçus
    - Technique de score des ondes
  - Ensuite, *pattern matching* pour retrouver les correspondances avec les lettres
    - Cette étape reste manuelle...
- Une vidéo amusante, mais malheureusement pas de démo :(

Demystifying Fuzzers

- Michael Eddington
- Retour d'expérience du créateur du *fuzzer* Peach pour la conception d'outils de *fuzz*
  - Définition du *fuzzing*
  - Circonscrire la surface à *fuzzer* (résultat attendu, injection de données totalement/partiellement aléatoire, ...)
  - Assurer la reproductibilité des plantages
- Comparatif des différents *fuzzers* OpenSource et commerciaux
  - Type de format *fuzzé* (réseau, application, système de fichier)
  - Maintenance en Juillet 2009 ?
  - Portabilité

More Tricks for Defeating SSL

- Moxie Marlinspike
- Rappels sur les certificats X.509 et les chaînes de confiance
- sslsniff : attaque de l'intercepteur pour tromper les utilisateurs
- sslstrip :
  - Intercepte les requêtes HTTPS
  - Initie la connexion chiffrée
  - Renvoie la page en HTTP au client, sans chiffrement
- Acheter un certificat :
  - Validation automatique quasi-systématique
  - Contact administratif du Whois



More Tricks for Defeating SSL

- Ainsi, pour acheter
  - www.hsc.fr => contact de hsc.fr
  - Pour acheter banqueenligne.hsc.fr => idem
  - Dans le *DistinguishedName*, le champ *CommonName* est défini comme une chaîne Pascal, « longueur + chaîne »
    - Pas de caractères « spéciaux » dans une chaîne Pascal
    - **banqueenligne.com\0.hsc.fr** est valide
    - Le contact de hsc.fr sera contacté...
  - Du côté des implémentations...
    - Traitement du *CommonName* comme une chaîne C (strcmp(), etc.)
    - Résultat : banqueenligne.com\0.hsc.fr => valide pour banqueenligne.com !
  - Encore mieux : ***\0.hsc.fr** :)

More Tricks for Defeating SSL

- Amélioration de l'attaque
  - Exploit à distance dans une des implémentations...
    - (AAAAAAAAAAAAAAAAAAAAA\0OVERWRITE).foo.com
  - Révocation avec OCSP
    - L'URL OCSP est dans le certificat
    - Interception des requêtes, réponses forgées avec le code « 3 » pour « Try again later »...
    - Implémentations dociles
  - Mises à jour automatiques de Firefox et Thunderbird
    1. Activées par défaut :(
    2. Mais pas signées :)
    3. …
    4. Profit !

Our Favorite XSS Filters and How to Attack Them

- Eduardo Vela et David Lindsay (IBM X-Force)
- Etat des lieux des XSS et de leurs filtres
  - Côté client : **IE8** (inclus), **Firefox** (NoScript), **Opera**
  - Côté serveur : **PHP-IDS, mod_sec**
- Contournement des règles de filtrage par plusieurs stratégies :
  - En utilisant des règles HTML :
    - <img src='x:alert(alt)' onerror=eval(src) alt=0>
    - <object data="javascript:alert(0)">
  - Par le JavaScript :
    - alert(document.cookie) <=> alert(document['cookie']) <=>with(document) alert(cookie)

Our Favorite XSS Filters and How to Attack Them

- Faille à venir **HTML5** :
  - → </a onmousemove='alert(1)'>
- Pollution des paramètres (?param=value1&param=value2)
- Unicode (dans Java, fork depuis 3.0)
  - Problème niveau serveur (ex: PHP) et niveau client (ex: Firefox)
  - → <img src="x:gif" onerror="window['al\u0065rt']('unicode xss')">

- Règles prédéfinies de **mod_sec** insuffisantes, doit être maintenu régulièrement
- **PHP-IDS** plus exhaustif MAIS a ses inconvénients (faux positif, utilisation CPU)
- **IE8** inclut des filtres mais qui peuvent être défaits (utilisation de {} pour passer des commandes JS)
- **FF** + **NoScript** : globalement fiable même si nuit la fluidité d'utilisation

Black Ops of PKI

- Dan Kaminsky (IOActive)
- « Crise de l'authentification »
  - Mots de passe souvent faibles
  - Utilisation de certificats X.509 pour tout le monde ?
  - Comment avoir confiance ? (cf. CCC 2008 – Lenstra / Sotirov)
- Présentation de quelques banalités sur les CA et X.509
- Une CA de VeriSign utilise encore MD2RSA
- La solution selon Kaminsky ? DNSSEC !
  - Au moins ses cookies sont bons

Internet Spec Ops : Data Mining

- Paul Vixie, Chris Lee et Andrew Fried (ISC)
- *Objectif* : utiliser le Data Mining dans des attaques de grande envergure
- Cas d'une infection classique *« malware.exe »*
  - Collecte d'information de l'entourage de la victime et propagation
  - Scan d'hôtes précis
  - *Comment traiter ces informations pour circonscrire l'attaque ?*

- **Data Mining** :
  - Obtenir des statistiques : GeoLocIP, numéro d'AS, pays touchés
  - Anticiper les mesures : identification (blocage) de NS

Introducing Ring -3 Rootkits

- Alexander Tereshkin, Rafal Wojtczuk (Invisible Things Labs)
- Ring -3 ?
  - Ring -1 == Virtualisation
  - Ring -2 == SMM (cf. SSTIC'09 - Duflot)
  - Ring -3 == Northbridge (MCH)
- Dans un chipset
  - CPU à part entière
  - Accès privilégié à la mémoire et à la carte réseau
  - *Management Engine* (AMT / ME) avec interface HTTP
  - Mémoire stockée dans l'eeprom du BIOS (SPI)
    - Impossible d'y écrire des données non signées...

Introducing Ring -3 Rootkits

- AMT (Active Management Technology)
  - Désactivé par défaut
    - Mais portions de code tout de même exécutées... périodiquement !
    - Possibilité de *hooker* ces portions pour exécuter notre code
  - AMT chargé dans les 16 Mo les plus hauts dans la mémoire
    - Accès bloqué par le Northbridge
    - Accès possible en exploitant la faille de *memory remapping* sur les chipsets Q35 d'Intel (cf. BlackHat USA 2008 – Rutkowska)
    - Ne marche plus sur les Q45...
- Preuve de concept publiée le 25 août 2009

Photos

Attacking SMS

- Zane Lackey et Luis Miras
- Forge de messages (SMS, MMS, EMS) sur les réseaux GSM
- Intérêt du SMS/MMS :
  - Envoi de contenu
  - Modification de paramètres de configuration
  - Store-and-forward, assure la réception du message
- Analyse des étapes pour la forge :
  - Encodage / décodage
  - Utilisation d'un terminal pour l'envoi
  - Contourner les mécanismes à la réception
- Découverte de bug dans le parser UDH de l'Android et dans le CommCenter de l'iPhone, entrainant des crashs.

Attacking SMS

- Utilisation des messages Over-The-Air (OTA) pour modifier la configuration des téléphones.
  - N'indique pas forcément l'émetteur
  - Ni les modifications apportées
  - → Idée : envoyer un message OTA pointant vers un serveur sous contrôle

- Création d'un PoC pour exploiter ce problème d'architecture T.A.F.T
  - non publique

Attacking Intel® Bios

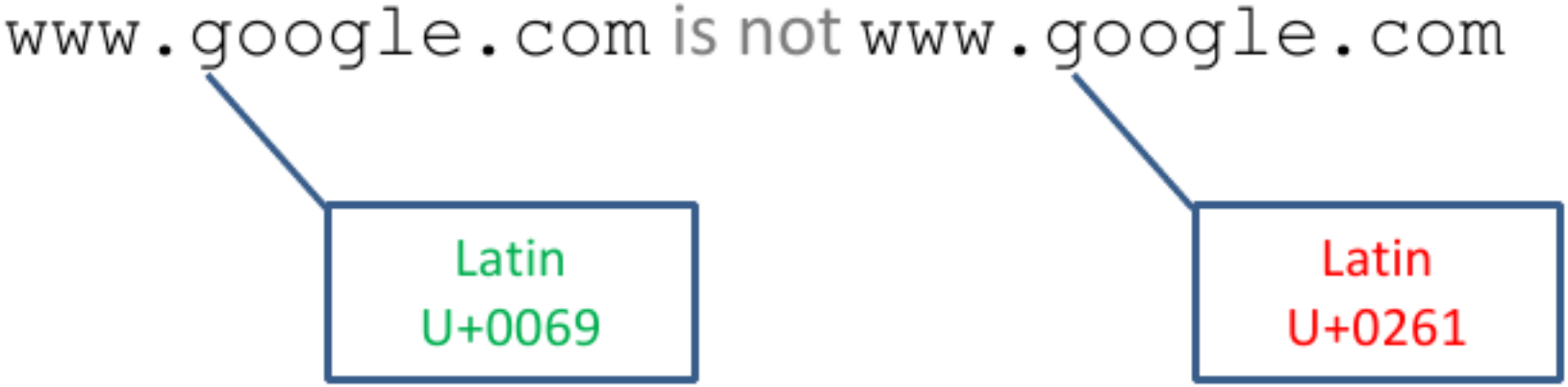
- Rafal Wojtczuk, Alexander Tereshkin (Invisible Things Labs)
- Reflasher un BIOS, déjà fait ?
  - Infection des tables ACPI (John Heasman et Loic Duflot)
  - CORE Security : *patch* et calcul de la somme de contrôle
    - Mais maintenant, images signées...
- Comment faire ?
  - Exploiter un *bug* dans le code du BIOS
    - Très peu d'interactions possibles avec le code du BIOS
    - PXE arrive bien trop tard...
    - Exploitation des mises à jour avec une image contenant notre code
    - Mais l'image est signée
      - Sauf... l'image de *boot splash*, au format JPG ou BMP

Attacking Intel® Bios

- Débordement de tampon dans les BIOS Intel
  - Fonction de décompression de l'image
  - Débordement d'entier lors du calcul H x L x P de l'image
    - *Bug* très classique...
  - Permet l'exécution de code arbitraire
    - Écrasement du gestionnaire de fautes de pages #PF
    - Génération d'une faute de page
- Post-exploitation
  - Contrôle sur le BIOS signifie souvent contrôle sur la SMM
  - Notamment, la routine de gestion de la SMM
  - *Rootkits* « Ring -2 »

Unraveling Unicode

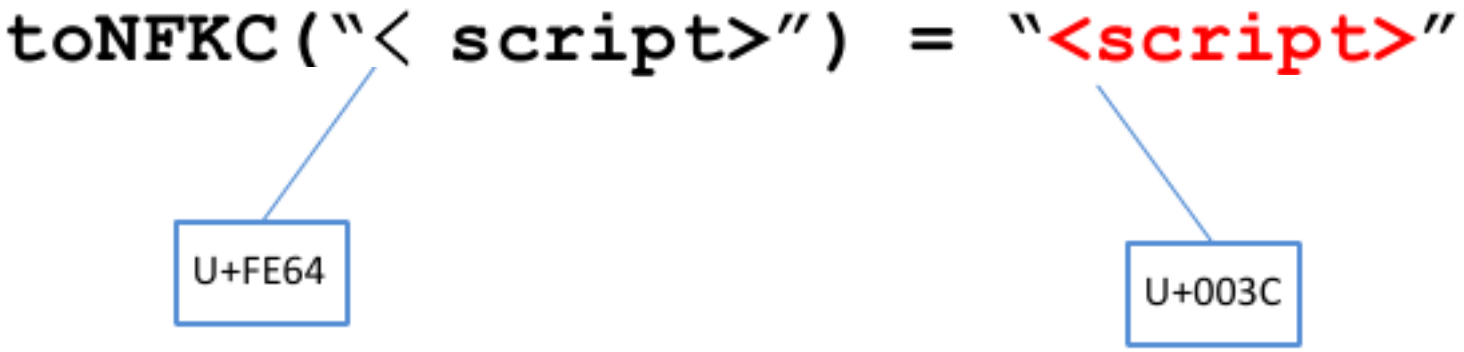
- Chris Weber
- Unicode : unifier tous les caractères sous une seule norme
- Problème : les applications/protocoles actuels peuvent mal gérer certains caractères (en particulier sur les tables UTF-16, UTF-32)
  - Ces attaques engendrent des comportements imprévus
    - Rien : le caractère n'est pas ou mal affiché
    - Plantage (DoS, *buffer overflow*...)
    - Transformation (contournement des filtres anti-spam, XSS, ...)



Unraveling Unicode

- Attaque par similitude (ex : `1 et l, rn et m`)

- Fonctions de normalisation :
  - NFKC && NFKD : peuvent permettre de l'injection HTML



  - Nombre croissant de vulnérabilités autour d'Unicode

SADE: Injecting agents in to VM guest OS

- Matthew Conover (Symantec)
- SADE = « SteAlthy Deployement and Execution »
  - Produit Symantec d'administration de parc virtualisé
  - Utilise l'API VMSafe pour contrôler les Vms
- Principe :
  - Avant : machines physique avec des agents de toutes origines (Anti-Virus, sauvegarde, etc.)
  - Après : machines virtuelles, avec des agents exécuté « à la demande » par une VM de « sécurité » via VMSafe
  - Code exécuté directement dans les OS invités
    - Logiciels malveillants ne peuvent rien faire contre... tant qu'ils n'ont pas la main sur l'hyperviseur !

Is Your Phone Pwnd ?

- Kevin Mahaffey, Anthony Lineberry et John Hering
- Mobile insuffisamment pris en compte dans les politiques de sécurité:
  - Offre des fonctionnalités/services évolués (se rapprochent des PCs)
  - Utilise des connexions persistantes
  - Permet l'installation d'applications tiers
  - Un bug reporté met plusieurs mois avant d'être pushé
    - ➔ Cible privilégié pour une attaque
- Création d'un outil de *fuzzing*, FuzzIt
  - Semblable à Scapy pour forger des messages GSM
  - Découverte d'un bug dans le SDP de l'iPhone
    - Entrainait une plantage de l'iPhone
    - 4 mois pour intégrer le correctif

"Smart" Parking Meter Implementations, Globalism, and You

- Joe Grand, Jacob Appelbaum & Chris Tarnovsky
- Attaque des systèmes de parcmètres de San Francisco
  - Deux types : simple emplacement et multi-emplacements
  - Modèles purement mécaniques remplacés au début des années 90
  - Modèles hybrides (mécaniques/électroniques) en place
  - Modèles entièrement électroniques en cours de déploiement
- Interfaces limitées
  - Pièces de monnaie, cartes bancaires, cartes à puce
  - Administration par GPRS ou port série

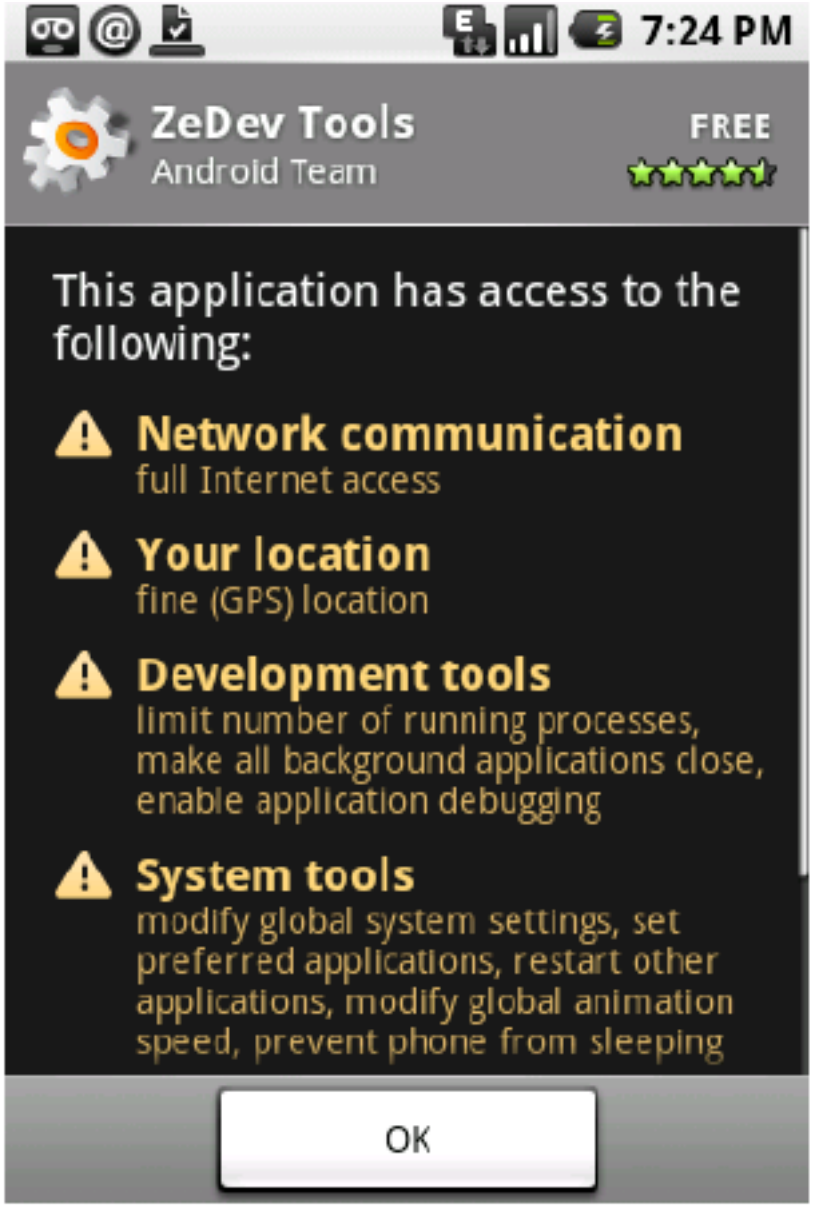
"Smart" Parking Meter Implementations, Globalism, and You

- Achat de parcmètres sur eBay (!)
- Extraction du code de la mémoire flash ou de la ROM
  - Désassemblage, etc.
  - But : trouver les points d'entrée pour les administrateur
  - Tout est en clair...
- Attaque des cartes à puce de paiement
  - « Désencapsulation » des cartes
    - Décapage des puces à l'acide nitrique, etc.
  - Création de « Yes Cards » avec crédits infinis

Exploratory Android Surgery

- Jesse Burns (ISEC Partners)
- Android = application Java tournant sur un Linux
- Système de permissions : Unix + Android (+ utilisateur)
- Isolation des applications en 2 niveaux :
  - Possède un unique UID et appartient à un ou plusieurs groupes *Unix-like* (inet, bt, music...)
  - Système de permissions Android définies dans le Manifest (*android.permission.READ_CONTACTS*)
- Le *Manifest* définit ce que l'application peut faire
- Ajout de 2 nouveaux modes au noyau :
  - Binder : interface de gestion des IPC
  - Ashmem : zone mémoire partagée

Exploratory Android Surgery



Exploratory Android Surgery

- Quelques outils pour l'exploration d'Android :
  - C'est un Linux ! /proc, dmesg, /sys
  - Logcat, ou toute application avec la permission READ_LOGS
  - /proc/binder et /proc/binder/proc
  - /data/system/packages.xml
  - ManifestExplorer
  - Intent Sniffer / Fuzzer faits par l'iSec

Cloudburst - Hacking 3D and Breaking out of VMware

- Kostya Kortchinsky (Immunity Inc.)
- Sortie d'isolation est un des objectifs ultimes en virtualisation
  - Du point de vue d'un attaquant bien sûr :)
  - Très peu de cas : dossiers partagés Vmware, Xen, Virtual Server
- Périphériques virtuels sont une bonne cible
  - Émulés sur l'hôte (vmware-vmx)
  - Accédés par l'invite (par PIO ou MMIO)
  - Choix multiples (son, vidéo, CD-ROM)

Cloudburst - Hacking 3D and Breaking out of VMware

- CLOUDBURST
  - Combinaison de 3 vulnérabilités dans VMware
    - Emulation du périphérique vidéo
    - Lecture arbitraire de cette mémoire depuis l'invité
      - Commande « SVGA_CMD_RECT_COPY »
    - Ecriture arbitraire de la mémoire de l'hôte depuis l'invité
      - Utilise l'émulation DirectX 9.0
    - Quelques astuces supplémentaires pour outrepasser DEP
  - Fonctionne sous Workstation 6.5.1, Fusion et ESX 4.0 RC Hardfreeze
  - Corrigé silencieusement par VMware en mars 2009
    - Sorti dans Immunity Canvas en avril
    - Avis de sécurité VMware publié en avril

The Conficker Mystery

- Mikko Hyppönen (F-Secure)
- Conficker fait partie des logiciels malveillants « professionnels »
- Techniques d'évasion avancées
  - « Tue » les processus gênants (Process Explorer, Process Manager, TCPView, Wireshark, etc.)
  - Détecte les machines virtuelles
  - Désactive les mises à jour de sécurité
  - Placement d'ACLs pour rentre ses fichiers en lecture seule par SYSTEM
  - Attaque par clés USB même si l'Autorun est désactivé
  - Utilise de la cryptographie (RC4, RSA et même MD6 (!))

The Conficker Mystery

1er avril 2009 : on nous annonce le « Big One » avec Conficker

- Rien ne se passe pourtant
- Miko Hyppönen refuse d'en parler
  - « Ok, my talk is finished now, but I won't take any question, thank you. »

Merci !

Questions ?