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

OSSIR
Compte rendu 27C3
Berlin – 27-30 décembre 2010

- Mardi 8 février 2011 -

Benjamin Arnault <Benjamin.Arnault@hsc.fr>
Guillaume Lehembre <Guillaume.Lehembre@hsc.fr>

Plan

- Présentation de la conférence
- Faits marquants
- Résumé des conférences intéressantes

27C3

- CCC = Chaos Computer Club
- 27ème édition de la conférence depuis 1984 !
  - « We come in peace »
- Berlin (Alexanderplatz – Berliner Congress Center) du 27 au 30 décembre 2010
- Droit d'entrée très raisonnable (70€ pour les 4j)
  - Système de pré-vente depuis cette année pour le ticket 4j
  - Possibilité d'acheter des places à la journée (ou à la soirée)
- Conférences de midi à minuit passé :-)
  - ~100 conférences, ~75% en anglais, programme évolutif !
  - 3 salles en simultané + streaming, DECT et écrans LCD

27C3

- Conférence « Underground », plus que Defcon
- De nombreuses activités parallèles...
  - Crochetage de serrure
  - Construction de robots en Lego
  - Création de circuits électroniques (télécommande universelle)
  - Réseau GSM alternatif
  - Vols d'hélicoptères à 4 hélices
  - Impression en 3D
  - Jeux de lumière
  - ...

Faits marquants 2010

- Conférences GSM
  - Cassage d'une communication voix GSM en direct avec deux téléphones à $10
  - Les avancées du projet OsmocomBB
  - Exploitation de vulnérabilités au niveau « baseband »
  - Géolocalisation Android
- RFID
- SAP
- « Epic FAIL PS3 »

GSM Sniffing
Karsten Nohl & Sylvain Munaut

- Démonstration en direct de l'interception d'une communication voix sur l'un des réseaux mobile allemand
- Plusieurs étapes
  - Identification de la victime à la cellule près
    - Interrogation publique de HLR (→ IMSI et ville)
    - SMS silencieux (→ LAC & TMSI)
  - Utilisation de deux téléphones à $10 modifiés utilisant OsmocomBB (interception d'appel & suivi des sauts de fréquence)
  - Chiffrement A5/1 cassé à l'aide de « Rainbow Tables » (Kraken)
    - Récupération de la clé de session
  - Extraction de la voix !

GSM Sniffing
Karsten Nohl & Sylvain Munaut

- Principaux problèmes :
  - Non changement des clés de sessions avant un appel ou un SMS (configuration dépendant de l'opérateur)
  - Bourrage prédictible dans les trames GSM
  - Changements peu fréquents des TMSI

- Interception de données GPRS/Edge pas encore possible... à suivre

OsmocomBB
Harald Welte & Steve Markgraf

- OsmocomBB = Open Source Mobile Communication BaseBand
- Projet né en Janvier 2010
- Actuellement, quatre implémentations fermées sont utilisées par les fondeurs de puce « *baseband* »
- Approche adoptée :
  - Utiliser des puces « *baseband* » largement répandues, bon marché, aussi simple que possible et dont certaines informations ont fuité
  - Ex : Texas Instrument Calypso, Mediatek MT622x
- OsmocomBB implémente les couches 1 à 3, les pilotes matériels pour la puce « *baseband* », une GUI simpliste (téléphone & PC)
  - Couche 1 sur le téléphone, couche 2 & 3 sur le PC

OsmocomBB
Harald Welte & Steve Markgraf

- Ça fonctionne ! Démonstration d'un appel sur l'un des réseaux mobile allemand
- Implémentation permettant d'envoyer des trames arbitraires aux équipements opérateurs (BSC, MSC, SMSC, etc.)...
- Limitations actuelles : pas de mesure de cellules adjacentes, pas de *handover*, pas de trafic données (GPRS)
- « La sécurité TCP/IP devient ennuyeuse... il faut passer à autre chose »

SMS-O-Death
Nico Golde & Collin Mulliner

- SMS : vecteur d'attaque privilégié
- Injection de SMS pré-encodés au format PDU (OpenBTS)
- DoS sur la plupart des téléphones testés
  - « *Feature phone* » : Nokia, LG, Samsung, Motorola, Sony Ericson, Micromax [Inde]
  - Certains n'acquittent pas à la SMSC les SMS piégés reçus → DoS à répétition !!
- Quid d'une attaque de masse entraînant la reconnexion de centaines de milliers de téléphones en simultané ?
- Solution : MAJ *firmware*... ça existait avant l'avènement des ordiphones (*smartphone*) ?

The baseband apocalypse
Ralf Philipp Weinmann

- Travaux sur les corruptions de mémoire dans les piles des téléphones : possibilité d'exécution de code au niveau des processeurs « *baseband* » ?
- La sécurité logicielle de la partie « *baseband* » date des années 90.
  - Pas de canaris, NX, ASLR, etc.
- Plusieurs vulnérabilités découvertes par ingénierie inverse au niveau 3 des piles GSM en analysant les *firmware* ou en extrayant la mémoire
  - Débordement de tampon dans le défi/réponse GSM/UMTS chez Qualcomm
  - Débordement de tas dans le TMSI chez Infineon (CVE-2010-3838 – exploitable sur iPhone)

Android geolocalisation using GSM network – Renaud Lifchitz

- Géolocalisation sur Android : 2 méthodes
  - API Google utilisée par Maps, peu documentée
  - GeolocationAPI utilisée par Google Gears ← la meilleure
- Accès à la longitude, latitude et adresse complète
- Informations intéressantes
  - Appels : numéros et durée
  - SMS : format PDU :-)
- Moyens pour accéder à l'information
  - Permissions applicatives
  - Lecture des journaux Android
    - /dev/log/system
    - /dev/log/radio (position)

Android geolocalisation using GSM network – Renaud Lifchitz

- Scénarios d'attaque
  - Accès physique, utilisation du mode de debug USB et lecture des logs
  - Installer une application
    - Disposant des bons privilèges
      - ACCESS_COARSE_LOCATION ou ACCESS_FINE_LOCATION + INTERNET
        - Envoi direct de la position
      - READ_LOGS + INTERNET
        - Copie des données de /dev/log/radio vers /dev/log/system
        - Crash de l'application puis envoi du rapport au développeur :-)
    - Qui utilise l'Android NDK (Native Developement Kit)
      - Appel de fonctions natives (C/C++) qui s'exécutent hors de la *sandbox*
- Annonce une application permettant de dresser la carte Gmaps du parcours du téléphone avec appels et SMS

Is the SSLiverse a safe place ?
Peter Eckerslay & Jesse Burns

- Test de tous les sites IPv4 accessibles sur le port 443/TCP
- Cartographie de tous les CA
  - 52 pays
  - Plusieurs problèmes
    - Clés erronées (30000)
    - Mauvaises signatures (500 dont diplomatie.be)
    - Certificat pour localhost, mail ou des adresses de réseaux internes
    - Extended Validation non respecté
    - ...
- Prolifération : 252 sous-CA pour Deutsche Telecom !
  - Firefox et IE gardent en cache des CA intermédiaires !
- Base de données (12Go) et cartographie des CA disponibles

Data Recovery Techniques
Peter Franck

- Pré-requis à la récupération de données
  - Atmosphère saine, microscopes, beaucoup d'ordinateurs, de disques et de câbles
- Difficultés
  - Dégâts physiques, corruption des parties logicielles, défauts du contrôleur ...
- En fonction de l'ampleur des dommages,
  - Matériel spécifique peut être nécessaire
  - En dernier recours l'imagerie à force atomique
- Accés au *firmware* du contrôleur d'un disque
  - Connexion des câbles aux PIN utilisées pour définir l'état du disque
  - Invite de commande permet alors de lire/écrire des informations
    - Ex : Lire les températures ou modifier le numéro de série !

Frozen Cache
Jürgen Pabel

- La RAM contient des données sensibles (clés cryptographiques, mots de passe, etc.)
  - Récupération d'informations pendant quelques minutes (Cold Boot Attack)
- Idée : stocker ces informations dans le cache du processeur
  - Registre CR0 (x86) contrôle la mise en cache
- Étapes : Inscrire les données sensibles dans les registres du processeur, effacer les données en RAM, geler le cache CPU, écrire les données des registres dans le cache
- Protection à activer lors d'évènements précis (mise en veille, verrouillage de l'écran) car les performances du système sans cache processeur sont assez catastrophiques !

The Hidden Nemesis
Ralf Philipp Weinmann

- Attaque physique sur des ordinateurs portables
  - via le contrôleur embarqué (contrôleur de clavier amélioré)
    - activé dès qu'un poste est alimenté, même si celui-ci est éteint !
- Accès physique court et dépôt d'une porte dérobée
- Porte dérobée permettra
  - d'enregistrer des données dans la mémoire
  - de les communiquer par
    - CPU via l'ACPI, LED ou ...
    - Lampe veilleuse qui dispose d'une ligne à 10Mhz et ainsi peut servir d'antenne !
- Pour ce protéger d'une modification de *firmware*
  - base de donnée fiable des bonnes versions et de leurs empreintes

Rootkits and Troyans on your SAP landscape – Ertunga Arsal

- Panorama des attaques
  - Enregistrement d'un serveur au niveau du répartiteur de charge : MiTM
  - Exécution de commande distante sur système sous-jacent via
    - RFC directement
    - SDK et programme de test startrfc
    - Commandes intéressantes
      - Lectures de tables
      - Création ou modification de la table des utilisateurs
      - Exécution de code ABAP
  - Récupération de la clé privée utilisée pour créer des tickets SSO
  - Injection de code ABAP et de requêtes SQL
  - Compromission du client via SAPGUI

Distributed FPGA Number for the masses – Felix Domke

- Objectif : Casser le chiffrement DES des *firmware* utilisés sur la « Triforce Arcade System Board » (SEGA) à moindre coût en moins d'une semaine.
- Coût :
  - +300 processeurs Intel X5460 à 3,16Ghz : ~$150k
  - +300 PS3 : ~$93k + dev
  - 150GPU : ~$45k
  - 20 groupes de 3 FPGA Xilinx : ~1k d'occasion sur Ebay :-) + dev
- Outil Crunchy permettant de distribuer les tâches sur les FPGA.

Analysing a modern cryptographic RFID system – Milosh Meriac & Henrick Plötz

- HID iClass
- Dans le mode de sécurité standard : deux clés partagées
  - une pour l'authentification (DES)
  - une pour le chiffrement (3DES)
- Achat d'un lecteur RW400
  - Découverte d'une interface de programmation PIC sur un connecteur 6 PIN
  - Contournement du dispositif anti-copie → extraction des mémoires FLASH et EEPROM.
  - Découverte des deux clés
- RFID : encodage de la norme ISO15693 avec des commandes spécifiques (lecture, écriture, authentification, etc.) qui ont pu être découvertes

Reverse Engineering a real-world RFID payment system - Harald Welte

- Système EasyCard == NXP MiFARE
  - Utilisé pour les transports et le paiement en magasins (MAX 240€)
- Faille
  - Stockage du crédit de l'utilisateur dans la carte
- Démarche
  - Récupération des clés (méthode Dark Side avec kit MFCUK)
  - Réalisation de nombreuses transactions légitimes
    - Identification de la signification des champs de la carte
  - Modification du contenu
    - Réduire le crédit
    - Augmenter le crédit
    - Passer outre la limite journalière de dépense

Embedded reverse engineering tools & techniques – N. Fain & V. Vygonets

- Introduction didactique au hacking matériel
- Interface série : analyser les tensions sur chaque PIN
  - Outil : RS232Enum (basé sur Arduino)
- Interface JTAG : proche de résistance de tirage de 4.7k
  - Outil : JTAGEnum (basé sur Arduino)
- Extraction des informations directement d'une puce
  - Avec un peu de documentation...
- Découvrir la logique derrière les circuits imprimés
  - Outil DePCB basé sur DeGate

OMG WTF PDF
Julia Wolf

- Adobe Reader = 15 millions de lignes de code
- PDF = format normalisé par une norme ISO
  - Mais aucune méthode de validation du format !
  - Nombreuses fonctionnalités
    - OpenGL, ADBC, exécution flash, jouer des sons ou des vidéos et exécuter du javascript ...
    - Exécution de code javascript dans le navigateur à partir du javascript du PDF
- Ensemble des références présentes dans un ficher PDF ne sont pas évaluées à l'analyse du fichier !
  - Idée : inclure du code malveillant dans un fichuer PDF

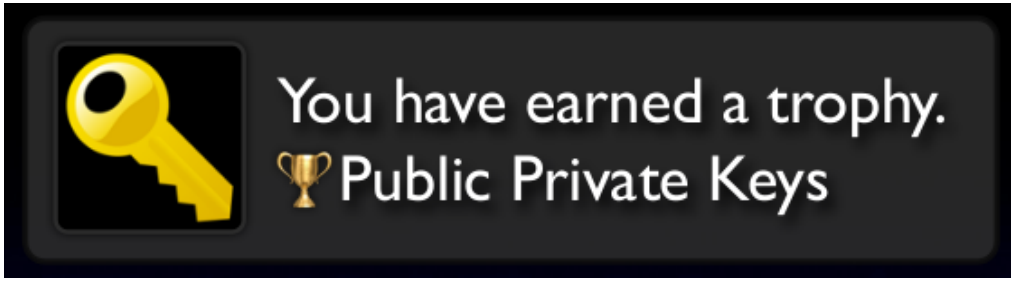
OMG WTF PDF
Julia Wolf

- Failles
  - Aucune règle ne définit qui va prévaloir
    - définition de la longueur
    - délimiteurs
  - 1024 premiers octets peuvent être de tout type
    - gif, jpeg, zip, exe
  - PDF peuvent facilement s'inclure dans un fichier GIF ou HTML
- Résultat d'évasion vis à vis des solutions antivirus
  - Solutions antivirus ne sont pas encore matures pour détecter tous les fichiers PDF forgés

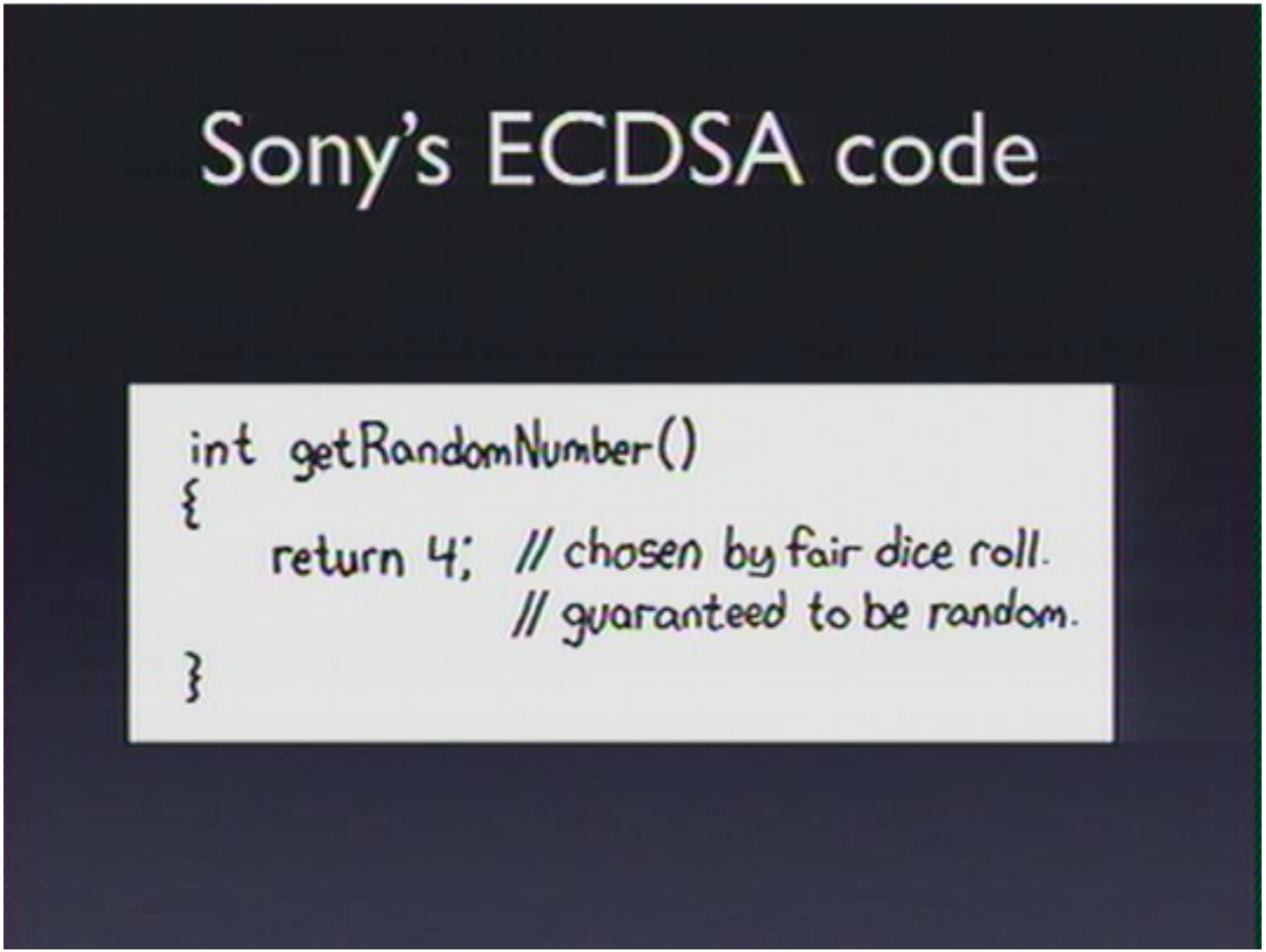
Sony cat iz Happy !

Console Hacking 2010 – PS3 Epic Fail Fail0verflow

- Objectif : exécuter du code et installer Linux
- Annonce du système d'exploitation AbestOS
  - Se charge en mémoire à la place du GameOS
- Faille critique == EPIC FAIL
  - Dans l'utilisation des courbes elliptiques pour la signature des programmes
    - Des paramètres sont publics, 2 ne doivent pas l'être m et k (la clé privée)
    - m ~~est~~ doit être une valeur aléatoire à chaque signature
    - Sony n'a pas utilisé /dev/random mais une constante !
- Fail0verflow a eu ainsi accès à la clé privée k permettant de signer tout programme



Console Hacking 2010 – PS3 Epic Fail Fail0verflow



Conclusion

- Conférences très intéressantes
  - Comme d'habitude, du très bon et du très mauvais...
- Bonne ambiance
- Vidéos (MP4) et/ou audio (MP3/OGG) disponibles
  - http://events.ccc.de/congress/2010/wiki/Conference_Recordings
- Présentations et documents
  - http://events.ccc.de/congress/2010/Fahrplan/