OSSIR

2009/06/09

SSTIC 2009

Compte-rendu et impressions

Jérémy LEBOURDAIS
jeremy.lebourdais (à) edelweb.fr

Nicolas RUFF
nicolas.ruff (à) eads.net

EdelWeb

- diffusion publique -

EADS

Préambule

- **SSTIC**
  - ✓ Une conférence unique
    - Francophone & technique
    - Universitaire & industrielle & gouvernementale
  - ✓ Créée en 2003
  - ✓ 400 personnes
  - ✓ 3 jours à Rennes
  - ✓ Evènement social important

Préambule

- **Compte-rendu non exhaustif**
  - ✓ Source officielle
    - http://actes.sstic.org/
  - ✓ Compte-rendu collaboratif
    - http://communaute.sstic.org/
  - ✓ Autres compte-rendu
    - http://sid.rstack.org/blog/index.php/347-sstic-2009-en-direct-ou-presque
    - http://bruno.kerouanton.net/blog/2009/06/08/sstic-2009-compte-rendu-des-rumps/
    - Etc.

Jour 1

- **Keynote (Pascal Andrei, Airbus)**
  - ✓ Sécurité informatique et aéronautique
  - ✓ Les circonstances étaient difficiles !
- **Code malicieux sur JavaCard (Jean-Louis Lanet, Université de Limoges)**
  - ✓ Conférence déjà présentée à CESAR
  - ✓ Contenu
    - Une applet Java malveillante peut accéder à toute la mémoire la JavaCard
    - Résultat théorique déjà connu ... mais jamais implémenté
  - ✓ Limites
    - Il faut pouvoir charger une applet sur la cible
    - Certaines cartes sont protégées

Jour 1

- **Data tainting (Florent Marceau, LEXSI)**
  - Utilisation de la méthode du data tainting pour analyser automatiquement des malwares (bancaires)
  - Récupération des chaines de caractères utilisées
  - Outil privé basé sur Qemu

- **Désobfuscation automatique de binaires (Alexandre Gazet et Yoann Guillot, Sogeti/ESEC)**
  - Dernières évolutions de l'outil Open Source METASM
  - Désobfuscation & décompilation optimisée

Jour 1

WOMBAT vs. Internet (Marc Dacier, Symantec)

- Projet européen de capture et d'analyse de malwares
- Honeypots haute interaction
- Permet de dégager des groupes d'attaquants par analyse statistique
- Résultats voulus reproductibles

ACPI & SMI (Loïc Duflot, DCSSI)

✓ Conférence déjà présentée à CanSecWest

- [1] Compromission du mode SMM en modifiant les registres MTRR
- [2] Rootkit basé sur la modification des tables ACPI
- Met à mal "l'informatique de confiance" (Intel TXT, etc.)
- Démo très explicite

✓ Limite

- Nécessite d'avoir été root sur la cible

Jour 1

- **Compromission par le bus PCI (Christophe Devine & Guillaume Vissian, Thales)**
  - Presque tous les périphériques d'un PC peuvent faire du DMA
  - Preuve de concept: carte PCMCIA à $300 permettant la compromission silencieuse d'un PC sous Windows
- **ISO 27001 (Alexandre Fernandez-Toro, HSC)**
  - Retour d'expérience sans langue de bois
  - ISO 27001 n'est souvent pas utilisé pour ça, mais améliore parfois la sécurité
- **Solution du challenge SSTIC**
- **Cocktail**

Jour 2

- **Fuzzing (Ari Takanen, Codenomicon)**
  - Passé, présent, avenir
  - Avec quelles métriques ?
  - Outils de fuzzing de moins en moins aléatoires

- **FuzzGrind (Gabriel Campana, Sogeti/ESEC)**
  - Un outil de fuzzing combinant Valgrind et un SatSolver
  - Permet d'affiner la couverture du code à chaque itération (démo impressionnante)
  - Open Source

Jour 2

- **Sécurité des architectures de convergence fixe-mobile (Laurent Butti, Orange Labs)**
  - Les opérateurs installent des équipements de collecte IP en frontal (IPSEC, RADIUS, ...)
  - Une solution pour auditer l'implémentation de ces solutions est le fuzzing
  - Utilisation de l'outil Sulley et découverte de failles (IKEv2, etc.)

- **Sécurité des SmartPhones (Romain Raboin, Atlabs)**
  - Revue des logiciels d'espionnage existants (toutes plateformes)
  - Installation silencieuse PC → SmartPhone via un appel RAPI non documenté
  - La signature ne protège de rien par défaut

Jour 2

- **Traçage des traitres en multimédia (Teddy Furon, INRIA/Thomson)**
  - Revue des techniques mathématiques de protection de contenu
  - Conférence très technique mais très bien vulgarisée
  - Pas de retour d'expérience sur l'utilisation du watermarking

- **Le vol d'informations (Marie Barel, Orange)**
  - Conférence juridique
  - Le vol d'information est un problème juridique (l'information n'est pas une chose)
  - Mais tout le reste est condamnable (intrusion, recel, etc.)

Jour 2

- **Pourquoi la sécurité est un échec (Nicolas Ruff, EADS)**
  - Démonstrations par l'exemple que la sécurité n'a pas avancé beaucoup depuis 10 ans
  - Réflexion sur son retour d'expérience
- **Protection du noyau par la virtualisation (Eric Lacome, LAAS)**
  - Identification des zones critiques du noyau Linux
  - Protection d'intégrité par un hyperviseur matériel
  - Outil Hytux (non disponible actuellement)

Jour 2

Projet SEC&SI

- 3 projets ANR (basés sur Linux) pour un système d'exploitation convivial et sûr (cloisonnement des tâches)
  - ✓Vserver
  - ✓Xen
  - ✓MAC (SELinux)
- Note: très bon "effet démo" ☺

Jour 2

Rump Sessions (x23)

- CredSSP: récupération du mdp utilisateur en clair (XP SP3, Vista, 2008 et Seven)
- La cyber-défense à l'OTAN
- Attaques via les documents LaTex
- Scapy: la doc existe! Automate à états finis
- EthyloSSTIC: ethylotest en USB
- Image VMWare des challenges SecuriTech disponible
- Boxes WiFi: clé WiFi générée en JavaScript + aléa prédictible
  - ✓ Au moins 2 FAI français concernés

Jour 3

- **XSS (Pierre Gardenat, académie de Rennes)**
  - Etat de l'art des vulnérabilités XSS
  - Démos d'attaques
  - Vulnérabilités découvertes dans des sites sociaux

- **PDF malicieux (Fred Raynal, SOGETI/ESEC)**
  - ✓ Conférence déjà présentée à PacSec et à l'OSSIR
    - Niveaux de confiance et de chiffrement
    - Outil PDF Walker
    - Possibilités du plugin IE intéressantes (JS)
    - Démo de récupération du défi/réponse NTLM en ouvrant un PDF

Jour 3

- **Backdoor J2EE (Philippe Prados, ATOS)**
  - Cas d'un développeur malveillant
  - Insertion d'un JAR dans un WAR suffit
  - Outils de sécurisation et Backdoor disponibles
  - Actes très fournis

- **IpMorph (Philippe Prigent, DiaTeam)**
  - « Mystification » de la prise d'empreinte IP
  - Masque un ou plusieurs systèmes

Jour 3

- **Analyse noyau avec Kolumbo (Julien Desfossez, Révolution Linux)**
  - Présentations des techniques anti-debug
  - Module d'analyse « furtif »
  - A terme: faire marcher un debugger « classique » sur un binaire protégé

- **GPU & sécurité (Antoine Joux, DGA)**
  - Implémentations cryptographiques sur carte graphique (GPU)

✓ Limite

  - La consommation des GPU !

Jour 3

- **Emanations compromettantes des claviers (Martin Vuagnoux, EPFL)**
  - ✓ Conférence déjà présentée à CanSecWest
    - Implémentation low cost d'une attaque TEMPEST contre les claviers (tous types)
    - Intervention très vivante !

- **L'humain le maillon fort (Dominique Chandesris, DCSSI)**
  - Intervention difficile à résumer ...
  - La sécurité informatique repose essentiellement sur l'humain et la maitrise de l'information

Conclusion

- **Des interventions de haute tenue**
  - ✓ Rien à jeter
- **Un évènement social réussi**
- **Une météo exceptionnelle**

- **Les tendances**
  - ✓ Outils de haut niveau pour analyser du bas niveau (assembleur)
  - ✓ Attaques matérielles
  - ✓ Téléphones mobiles