SSTIC 2010

Nicolas RUFF
EADS Innovation Works
nicolas.ruff (à) eads.net

10:00	Systèmes d'information : les enjeux et les défis pour le renseignement d'origine technique	Bernard Barbier
11:15	Tatouage de données d’imagerie médicale – Applications et Méthodes	Gouenou Coatrieux
12:00	Visualisation et Analyse de Risque Dynamique pour la Cyber-Défense	Philippe Lagadec
12:30	CASTAFIOR : Détection automatique de tunnels illégitimes par analyse statistique	Fabien Allard Mathieu Morel Paul Gompel Renaud Dubois
14:45	Réflexions pour un plan d'action contre les botnets	Eric Freyssinet
15:30	virtdbg: un débogueur noyau utilisant la virtualisation matérielle	Christophe Devine Damien Aumaitre
16:30	Analyse de programme par traçage	Daniel Reynaud Jean-Yves Marion Wadie Guizani
17:00	Intéressez vous au droit... avant que le droit ne s'intéresse à vous	Eric Barbry

Jour 1

- DGSE
  - Très bonne présentation des activités de la DGSE
  - Messages
    - La France a rattrapé son retard dans le domaine du renseignement
      - Effort lancé en 1985 après une quasi-disparition du renseignement
      - Malgré des effectifs faibles (3000 en France contre 6000 en UK et 150 000 aux USA)
    - La « Lutte Informatique Offensive » est un vrai défi pour l'avenir
      - La France a 10 ans de retard dans le domaine
      - Toutes les technologies sont étrangères
      - Les systèmes sont intrinsèquement vulnérables (ex. SCADA)
      - Défense (ANSSI) et attaque (DGSE) sont inséparables
      - Il faudrait commencer par se défendre correctement
      - Les administrations détectent un nombre anormalement faible d'incidents (1000 vs. 50000 par an aux USA à périmètre égal)
    - La DGSE recrute 100 ingénieurs par an
      - Et cherche surtout des « bons »

Jour 1

- Tatouage des images médicales
  - Des problématiques intéressantes
  - Mais extrêmement spécifiques au contexte !

- Cyber-défense (vue par la R&D de l'OTAN)
  - L'OTAN a les mêmes problèmes que tout le monde
    - Identifier les ressources
    - Corréler les informations
  - Développements spécifiques
    - CIAP: visualisation intelligente pour l'aide à la décision
    - DRA: analyse de risques dynamique

Jour 1

- Détection de tunnels
  - Classification statistique des flux réseau
    - Après plusieurs essais sur des flux « connus », sélection des méthodes:
      - « RandomForest »
      - « Markov cachés »
      - Heuristique de suppression des faux positifs
  - Bons résultats en laboratoire
  - Problèmes résiduels
    - Base d'apprentissage
    - Faux positifs
    - Protocoles inconnus

Jour 1

- Lutte contre les botnets
  - Propositions
    - Sensibilisation – KO
    - Durcissement (à tous les niveaux) – KO
    - Détection (groupes de travail) – OK
      - Cymru, ShadowServer, maliciousnetworks.org, Europol (base Cyborg), …
    - Lancement d'un projet Interpol en mai 2010
  - Idées
    - La cybercriminalité est mal comprise par les politiques
    - Evolution législative nécessaire (ex. spam non commercial)
    - Prendre le contrôle des botnets pour un nettoyage forcé

Jour 1

- Débogueur à base d'hyperviseur
  - Objectif: analyser des mécanismes très bas niveau
    - DRM, PatchGuard, …
  - Implémentation:
    - Injection d'un driver par DMA depuis un périphérique matériel (FPGA)
    - Virtualisation à la volée
  - Pas encore fini
    - Mais bientôt sous licence GPL
- Analyse par traçage
  - Présentation de l'outil TraceSurfer (thèse INRIA / LHS)
    - http://code.google.com/p/tartetatintools/
  - Utilisé à des fins d'*unpacking* automatique de malwares

Jour 1

- Conférence juridique
  - Eric Barbry ☺
  - On assiste à une inflation juridique
    - Surtout en 2010
  - Les entreprises DOIVENT se préparer
    - Surtout à la loi Détraigne-Escoffier !

09:00	*Présentation des résultats du challenge*	
09:45	Sécurité de la plate-forme d'exécution Java : limites et propositions d'améliorations	Christian Brunette David Pichardie Frédéric Guihery Goulven Guiheux Guillaume Hiet
10:15	Analyse de l'efficacité du service fourni par une IOMMU	Eric Lacombe Fernand Lone Sang Vincent Nicomette Yves Deswarte
11:15	Quelques éléments en matière de sécurité des cartes réseau	Guillaume Valadon Loic Duflot Olivier Levillain Yves-Alexis Perez
12:00	Honeynet Project en 2010	Sebastien Tricaud
14:30	La sécurité des systèmes de vote	Frédéric Connes
15:00	Applications Facebook : Quels Risques pour l'Entreprise ?	Alban Ondrejeck Francois-Xavier Bru Guillaume Fahrner
15:45	Projet OpenBSC	Harald Welte
16:45	*Rump Sessions*	
19:30	*Social Event*	

Jour 2

- Challenge SSTIC 2010
  - Présentation par l'auteur et le gagnant « qualité »
- Sécurité Java
  - Analyse fine des mécanismes de sécurité Java
    - A tous les niveaux: JVM, librairies standard, interfaces natives, …
  - Résultats disponibles en ligne
    - http://www.ssi.gouv.fr/site_article226.html
- IOMMU
  - Analyse de la sécurité réellement offerte par IOMMU
    - Plusieurs problèmes conceptuels identifiés
    - Ex. Tous les périphériques PCI arrivent par le même point d'entrée sur le bus PCI-X
  - Démonstration d'attaque à l'aide d'un iPod (FireWire) malveillant
    - Injecte un paquet ARP dans la mémoire du périphérique réseau depuis le périphérique FireWire

Jour 2

- Sécurité des cartes réseau
  - Une carte réseau moderne est un système complet
    - Ex. carte BroadCom à base de processeur MIPS
  - Protocoles d'administration à distance
    - Spécifiques, basés sur TCP ou UDP
      - Ex. ASF 1.0 / 2.0
    - Donc la carte inspecte (interprète) tout le trafic réseau
  - Il existe des bogues triviaux dans l'implémentation
    - Crypto faible (si existant)
    - Buffer overflow
  - Démo de prise de contrôle à distance d'une carte de manière indétectable par l'OS
  - La carte a accès complet au matériel
    - Trafic réseau, SMBus, mémoire centrale (DMA), …
  - Il est possible de charger n'importe quel firmware dans la carte
  - Limites: ces protocoles sont rarement activés par défaut (par les intégrateurs)

Jour 2

- HoneyNet
  - Présentation de l'organisation générale
    - USA, France, … mais aussi Iran, Chine …
    - Interactions inter-culturelles très intéressantes
  - Objectifs
    - Partage d'informations, d'outils et de souches
  - Objectifs du chapitre français
    - Mise à disposition de challenges
    - Partage de logs / trafic réseau
    - Recherche amont (et pas opérations)

- Sécurité du vote électronique
  - Présentation d'un résultat de thèse
  - Nouveau protocole qui résout un certain nombre de problèmes …
    - Ex. secret du vote, vérifiabilité des résultats, …
  - … mais en crée de nouveaux !

Jour 2

- Facebook
  - Démonstration d'une attaque par ingénierie sociale contre une entreprise
    - Propagation virale d'une application malveillante dans un cercle de confiance
  - Plusieurs techniques démontrées
  - Une efficacité redoutable
    - Plus de 50% des cibles infectées avec la technique la plus efficace

- OpenBSC
  - Un travail incroyable pour implémenter une BTS Open Source
    - Projet déjà présenté au CCC … ailleurs
  - L'essentiel de la sécurité GSM repose sur le secret
    - Bien que les spécifications soient publiques
  - L'autorisation de faire une démo « live » n'a pas été obtenue en temps et en heure

Jour 2

- *Rump Sessions* (15)
  - Que du bon ☺
    - Organiser SSTIC
    - Un WAF sert-il à quelque chose ?
    - *Race condition* sur la machine à café
    - Intrusion sur un BES
    - NetGlub
    - « Qsxw.fr » et « Security Garden »
    - Challenge « BOSS »
    - DESIIR
    - NTDSDump
    - ExeFilter + PDF
    - Attaque sur le protocole T3 (WebLogic)
    - « iKare »
    - TCP-over-RDP
    - Challenge DFRWS
    - HTTP-over-Oracle
    - Scapytain

09:45	Trusted Computing : Limitations actuelles et perspectives	Frédéric Guihery Frédéric Remi Goulven Guiheux
10:15	JBOSS AS: exploitation et sécurisation	Renaud Dubourguais
11:15	Audit d'applications .NET complexes - le cas Microsoft OCS 2007	Nicolas Ruff
11:45	Conférence invitée	Mathieu Baudet
14:15	PoC(k)ET, les détails d'un rootkit pour Windows Mobile 6.	Cedric Halbronn
14:45	Projet OsmocomBB	Harald Welte
15:30	Conférence invitée	Patrick Pailloux

Jour 3

- Trusted Computing
  - Tour d'horizon du « Trusted Computing » de 2000 … à 2020
  - Culturellement intéressant

- Exploitation JBoss
  - Au moins 5 vecteurs de compromission dans une installation par défaut
  - Une seule conclusion
    - Il est très difficile de sécuriser une installation JBoss
    - La moindre erreur conduit à la compromission complète du serveur

- Audit .NET
  - A vous de juger ☺

- Le projet « OPA » (par la société « MLState »)
  - Pour assurer la sécurité du Web 3.0 ☺
    - http://www.mlstate.com/opa/download_instructions_for_windows

Jour 3

- *Rootkit* pour Windows Mobile 6
  - Un outil qui dépasse de loin le stade de la « preuve de concept »
    - Interface de contrôle « *full featured* »
    - Canaux de contrôle multiples (3G / WiFi / SMS)
    - Peu gourmand en énergie et en communications
  - *Disclaimer*: il n'y a aucune sécurité dans Windows Mobile ☺

- Osmocom BB
  - Modification d'un téléphone ancien mais très répandu
  - Création d'un *firmware* Open Source
  - Pas encore complet … mais très prometteur !
    - Avec des démos qui marchent

- ANSSI (conférence de clôture)
  - La sécurité informatique est un enjeu majeur pour l'Etat
  - Reste à savoir par où commencer devant l'ampleur de la tâche …
  - La défense est privilégiée sur l'attaque
  - L'ANSSI recrute ☺

Conclusion

- Un très bon cru
  - Très peu de déchet
  - Des échanges intéressants « hors conférence »
- Toujours les mêmes problèmes
  - La pluie
  - Le Resto U
- Des messages clairs
  - L'Etat recrute ☺

Références

- http://wiki.sstic.org/

- http://sid.rstack.org/blog/index.php/410-en-direct-du-sstic
- http://sid.rstack.org/blog/index.php/411-en-direct-du-sstic-le-retour
- http://sid.rstack.org/blog/index.php/412-en-direct-du-sstic-la-revanche