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

OSSIR
Groupe Bretagne

Compte-rendu

Black Hat Europe 2008

17 Juin 2008

Benjamin Tréheux
<Benjamin.Treheux@hsc.fr>

Informations générales

- 8ème édition de Black Hat Europe
- Durée : 2 jours (27 et 28 Mars 2008)
- Lieu : Amsterdam
- 24 présentations
- 2 sessions simultanées (et non 3 comme annoncé en 2007)
  - Tenue simultanée de la 9ème édition de CanSecWest à Vancouver
  - Nombre de soumissions trop faible ?
- Sujets multiples (GSM, IOS, applicatifs, codes malveillants...)

Keynote
(Ian O. Angell - London school of Economics)

- « Sécurité informatique = métier à risque »
- Fine frontière entre utilité de l'informatique & dangers induits
- Systèmes rationnels voués à l'échec
  - Souvent fondés sur des statistiques
  - Absence ou mauvaise gestion de l'exception
- La sécurité ne peut pas reposer sur des statistiques
- Conclusion : nécessité d'apprendre à gérer les exceptions

Client Side Security
(Petko D. PETKOV - GNUCITIZEN)

- Nombreuses techniques d'attaque d'applications Web
  - Issues des recherches menées ces dernières années par GNUCITIZEN
- Attaque CSRF sur Gmail
  - Création de filtre de redirection de mails vers une autre adresse
- Exploitation de formulaires d'upload de fichiers (cross-site file upload)
- Exécution de fichiers et de commandes :
  - Via le plugin quicktime ou l'extension Firebug de Firefox
  - Via des fichiers RDP (Windows Terminal Services) et ICA (Citrix) malveillants
- Hausse future du nombre de rootkits de 4ème génération
  - Ciblent les navigateurs Web
  - Sont largement portables et difficilement détectables par les antivirus
  - Communication aisée avec l'extérieur du réseau

Security Failures in Secure Devices
(Christopher Tarnovsky - Flylogic Engineering)

- Étude de la sécurité des circuits intégrés
- Beaucoup de mensonges dans les fiches techniques
  - « The most secure hardware token in the world »
- Multiples moyens d'attaque
  - Lecture des données en clair dans la mémoire
  - Contournement du brouillage du bus de données
  - ...
- Aujourd'hui toutes les techniques de protection des circuits intégrés ont été cassées

Side Channel Analysis on Embedded Systems

(Job De Haas – Riscure) - Impact and Countermeasures -

- Tendances actuelles de sécurité des systèmes embarqués
  - Bloquer l'accès au mode debug, à la mémoire et améliorer l'intégrité du code
- Objectifs
  - Empêcher l'exécution de code non autorisé et l'accès aux données confidentielles
- Mesures effectives contre les attaques conventionnelles
- Mais pas forcément contre les attaques par canaux auxiliaires
  - Attaque temporelle : étude du temps mis pour effectuer certaines opérations
  - Cryptanalyse acoustique : étude du bruit généré par le système
  - Analyse de consommation : étude de la consommation (ex. : lors du chiffrement)...
- Démonstration de cassage de clé DES...
- Contre-mesures : Limiter le nombre d'opérations, ajouter du « bruit » (variation du temps d'exécution), insérer des instructions sans effet sur l'algorithme...

Attacking antivirus
(Feng Xue - Nevis Networks)

- Antivirus démocratisés
  - Installés sur une majorité de postes clients et de serveurs de messagerie
- Confiance « aveugle » envers ces logiciels
- Mais ils comportent des vulnérabilités
  - Découvertes par fuzzing, ingénierie inverse, audit de code et des ACL...
  - 165 vulnérabilités référencées ces 4 dernières années
  - Principalement liées aux ActiveX, moteurs et interfaces d'administration
  - Également liés au traitement des nombreux formats de fichiers
- Démo : BSOD sur simple scan d'un fichier ou appel à un activeX
- Recommandations à destination des éditeurs
  - Cycle de développement sécurisé, audit régulier, bulletins de sécurité

Crackstation
(Nick Breese - Security-Assessment.com)

- Comment convaincre son entreprise d'acheter une PS3 :)
- Justification du besoin : le cassage de mot de passe
- La PS3 possède de sérieux arguments
  - Architecture Cell dont le coeur est connecté à 8 SPU (processeurs)
  - Système d'exploitation de base = Yellow Dog Linux
  - Documentation développeur publiquement disponible
  - Support de la PS3 par de nombreuses distributions Linux
- Implémentation vectorielle du calcul de MD5
  - Permet d'appliquer une même opération à plusieurs données
  - Théoriquement 1,9 milliards de calculs MD5/s

Developments in Cisco IOS Forensics
(Felix Lindner - Recurity Labs)

- Cisco largement répandu en entreprise ► Cible de choix
- Compromission de ces équipements impossible à gérer
  - Moyens actuels insuffisants (monitoring, débugging, enquête après incident)
  - Supervision via SNMP n'indique pas la raison d'un redémarrage
  - Accès à l'équipement parfois impossible (réseau/console)
- Futures versions d'IOS généreront un fichier "crashinfo"
  - État de l'équipement avant le crash, copie partielle de la pile et du tas...
- Mais l'information recueillie reste limitée
  - ne contient que les causes probables identifiées par les fonctions d'analyse simple de l'IOS
  - Insuffisant pour identifier le type et le résultat d'une attaque
  - Ne permet pas non plus la détection d'images modifiées

Developments in Cisco IOS Forensics
(Felix Lindner - Recurity Labs)

- Autre méthode d'analyse
  - Analyser IOS comme un unique processus et non comme un OS
  - Sauvegarder toute la mémoire du processus dans un fichier « core »
- Avantage
  - Image complète de l'état de l'équipement
  - Analyse en profondeur « à la demande » en cas de suspicion
- Fonctionnalité peu utilisée
  - Peu d'outils permettent d'exploiter les informations des fichiers « core »
- Outil en cours de développement (Cisco Information Retrieval)
  - Reconstruit la mémoire + Liste des processus (et infos associées)
  - Détecte les tentatives d'exploitation ou de modification d'images IOS
  - Extrait le trafic réseau au format PCAP...

Iron Chef - John Henry Challenge

(Jacob West et Brian Chess - Fortify Software)

- Concours de revue de code : automatique **vs** manuelle
  - Outil automatique utilisé : Fortify Source Code Analysis
- 2 équipes de 2 personnes
- 45 minutes
- Code source dévoilée au début de l'épreuve (JForum)
- Critères de jugement : qualité, originalité et présentation des découvertes
- Résultats obtenus sensiblement identiques
- Ex-aequo à "l'applaudimètre"

Exposing Vulnerabilities in Media Software
(David Thiel - iSEC Partners)

- Utilisation du fuzzing sur les formats de fichiers audio et vidéo
- Plusieurs points d'entrée
  - Métadonnées
    - Titre de l'album, commentaires...
  - Trame
    - Nombre de trames, canaux, fréquence...
- Utilisation de Fuzzbox dédié au format audio (python)
- Étude de cas du format Ogg-Vorbis
  - Démonstration de fuzzing sur ce format
- Conclusions :
  - Considérer les flux audio et vidéo comme potentiellement malicieux
  - Inciter les éditeurs à fuzzer leur propres formats et applications

0-Day Patch - Exposing Vendors (In)Security Performance
(Stephan Frei et Bernard Tellenbach - ETH Zurich)

- Étude comparative des performances de Microsoft et Apple
  - Domaine d'étude : gestion des vulnérabilités et diffusion des correctifs
  - Période de référence : 6 dernières années
  - Base de l'analyse : 27000 vulnérabilités publiques
    (Sources : IBM-SS, SecurityFocus, Secunia, CERT, SecurityTracker, SecWatch et FrSirt)
- Définition d'une nouvelle métrique d'évaluation
  - « Taux de correctifs 0-day »
  - Nb de correctifs émis le jour même de la divulgation publique d'une faille
- Conclusions
  - Globalement, temps entre divulgation et correctif en baisse
  - Projets de développement majeurs = moins d'émissions de correctifs
  - Nombre moyen de vulnérabilités non corrigées : Microsoft (→) - Apple (↑)

Biologger - A Biometric Keylogger
(Matthew Lewis – IRM plc)

- Beaucoup de systèmes biométriques utilisent TCP/IP
  - Facilite l'intégration aux infrastructures existantes
- Données souvent transmises non chiffrées
- Présentation d'une implémentation de "keylogger" biométrique
  - Capture les données biométriques en transit
  - Simple interception du trafic réseau
  - Potentiellement à la portée d'un grand nombre de personnes
- Conclusion
  - Sécurité par l'obscurité != sécurité
  - Être prudent quant-au routage de ce type de trafic réseau

The Fundamentals of Physical Security
(Deviant Ollam - Open Organization of Lockpickers)

- Présentation sur le « Lockpicking »
- Description des différents types de serrures
- Analyse de leurs vulnérabilités
- Démonstrations en direct (avec caméra)
  - Retrait de menottes avec un bout de métal
  - Ouverture d'un cadenas avec une canette découpée...
- Évocation d'un certain nombre de recommandations
- Atelier pratique en fin d'intervention
  - Prêt et vente de petits kits
  - Utilisation de serrures de plus en plus difficiles à ouvrir
- Rq : http://www.hsc.fr/ressources/presentations/crochetage_2006/Clusif.Nov.2006.html

Detecting Mobile Phone Spying Tools
(Jarno Niemela - F-Secure)

- Menaces déjà observées sur les téléphones mobiles
  - Virus, vers, troyens et applications visant une unique cible
- Menaces non encore observées
  - Rootkits, vers autonome (sans interaction de l'utilisateur), spywares à distribution massive et malwares visant à générer d'importants profits
- Outils d'espionnage = applications installées sur le téléphone
  - Applications non illégales en soi, mais utilisation illégale (sauf justice)
  - En pratique : beaucoup les utilisent de manière illégale
  - Cas d'utilisation : divorces, espionnage industriel et des employés...
- Objectifs
  - Vol d'informations : SMS / MMS / e-mail / Liste des appels...
  - Enregistrement / interception / mise en conférence discrète d'appels...

Detecting Mobile Phone Spying Tools
(Jarno Niemela - F-Secure)

- Nombreux périphériques et plates-formes cibles :
  - Symbian, Windows Mobile, LG, Sony Ericsson, Nokia...
- Exemples d'outils : Neo-Call (Symbian), FlexiSpy (Nokia, Symbian)
- Moyens de détection :
  - Connexions non sollicitées et/ou redémarrages intempestifs
  - Boites de dialogue apparaissant et disparaissant immédiatement
  - Augmentation notable de facture
  - Antivirus (peu de signatures actuellement)
  - Analyse du trafic réseau, du système de fichiers et des processus
    - Outils : F-Explorer, Efileman, EzFileMon, EzSniffer, Y-Browser, Y-Tasks, Resco Explorer, Resco registry editor, acbTaskMan

URI Use and Abuse

(Nathan McFeters, Rob Carter et Billy Rios - E&Y et Microsoft)

- URI existantes : http://, ftp://, telnet://, aim://, firefoxurl://, picasa://, itms://...
- URI associés à une application dans la base de registre
- Applications finalement accessibles au travers du navigateur
- Notamment par l'exploitation de failles de type XSS
- Exemples récents
  - Débordement de pile dans Trillian, MS07-035 (Iframe.dll)...
- Indépendant du système utilisé
  - Présentation sur Windows Mobile à Black Hat US ?

LDAP Injection & Blind LDAP Injection

(Chema Alonso et Jose Parada Gimeno - Microsoft)

- Rappel des concepts de base sur LDAP et les injections
- Quelques démonstrations d'injections (classique et en aveugle)
- Tests menés sur sur OpenLDAP et ADAM (AD)
- Quelques conclusions
  - Filtre du type (attribut=valeur) sans opérateur logique (peu intéressant)
    - (attribut=**valeur)(filtre_injecté**) ► filtre_injecté ignoré
  - Filtre de type (**|**(attribut=valeur)(2nd_filtre)) ou (**&**(attribut=valeur)(2nd_filtre))
    - (&(attribut=**valeur)(filtre_injecté)**)(2nd_filtre)) ► filtre_injecté interprété ► 2nd_filtre ignoré (malformé)
    - ou : (&(attribut=**valeur)(filtre_injecté))(&(1=0**)(2nd_filtre))
    - ou : (&(attribut=**valeur)(filtre_injecté**)(2nd_filtre))
- Recommandation : Filtrage des saisies utilisateurs

Malware on the Net - Behind the Scenes
(Iftach Ian Amit - Finjan)

- Evolution de « malware » à « crimeware »
  - Malware à but lucratif (exclusivement)
- Exemples de prix pratiqués
  - rapport financier=5 000$, spécification produit=1 000$, CB+PIN=500$
- Crimeware de plus en plus difficile à détecter
  - Obfuscation de code dynamique, modification régulière des binaires...
- Véritables « boites à outils » clés en mains (ex. : Neosploit)
  - Forme binaire, mécanismes de licences, de gestion d'utilisateurs...
- De plus en plus intégrés à des sites légitimes
  - De moins en moins de ressources récupérées sur des sites externes
- Développement futurs : Gadgets (Vista), Troyen Web2.0...

DTRACE: The Reverse Engineer's Unexpected Swiss Army Knife
(David Weston et Tiller Beauchamp - SAIC)

- DTRACE initialement introduit en 2004 dans Solaris 10
  - Objectif : debug en temps réel sur les systèmes de production
- Outil constitué de multiples composants
  - Répartis entre le noyau et l'espace utilisateur
  - Liés ensemble par le langage de script D
- Intérêts
  - Communication bi-directionnelle entre mode utilisateur et noyau
  - Suivi précis et à la demande de toute activité du système, au travers de scripts D relativement simples (ou framework Ruby plus évolué)
- Outil pratique pour les travaux d'ingénierie inverse
  - Détection de débordements de tampon sur la pile et sur le tas...
  - Association avec IDA Pro pour visualiser les blocs de code exécutés

Spam-Evolution
(Aseem "@" Jakhar - IBM Internet Security Systems)

- SPAM difficile à contrer
  - Affecte l'humain et non la machine (≠ malware)
  - Message facilement modifiable pour échapper aux filtres
  - Proviennent souvent de sources légitimes mais compromises...
- Objectifs : commercial / phishing / malware
- Moyens de défense
  - Listes blanches/noires, Greylisting, SPF (Sender policy framework), DKIM (Domain Keys Identified Mail), HashCash, Filtres de chaîne de caractères/d'expressions régulières/bayesien/OCR, Signatures, Systèmes de réputation
- Importance de filtrer les SPAM en entrée **et en sortie**
  - Évite de se faire blacklister

Intercepting Mobile Phone/GSM trafic

(David Hulton et Steve - Pico Computing, Inc.)

- Interception du trafic entre le téléphone et la BTS
- Équipements permettant de recevoir le trafic
  - Téléphones (Nokia, Ericsson...), USRP, Intercepteurs commerciaux...
  - Prix des intercepteurs commerciaux : entre 70 000 $ et 1 000 000 $
- Protection des données radio
  - Algorithmes A5/0, A5/1, A5/2 ou algorithmes propriétaires
  - IMSI (numéro unique d'identification d'un utilisateur dans la SIM)
- Cassage du chiffrement des communications (A5/1)
  - Élaboration de Rainbow Tables (2To – temps de calcul : 3 mois)
  - Ensuite avec un FPGA (ou un botnet) : temps de cassage = ~30 min

Antiphishing Security Strategy
(Angelo P.E. Rosiello - The European House)

- Institutions financières = 1ère cible des attaques par phishing
  - 96,9% des attaques recensées en Mai 2007
- Différents types d'attaques :
  - e-mails spoofés, messageries instantanées, téléphone, exploitation de vulnérabilité dans les navigateurs...
- Plusieurs moyens de défense au niveau du poste de travail
  - Liste noire de sites de phishing (utilisé par la plupart des navigateurs)
  - Analyse de page statique (analyse du contenu des pages)
  - Analyse du flux d'information (où sont envoyées les informations)
  - Similitude visuelle ou de mise en page (Comparaison d'arbres DOM)
    - DOMAntiphish

Bad Sushi - Beating Phishers at Their Own Game
(Nitesh Dhanjani, Billy Rios - E&Y et Microsoft)

- Étude des sites de phishing et des compétences des phishers
- A l'origine et de manière générale
  - La plupart des phishers ne sécurisent pas leurs serveurs
  - Peu de créateurs de framework mais beaucoup d'utilisateurs
- La tendance évolue
  - Recopie de sites légitimes de plus en plus précise
  - Sécurisation des serveurs
  - Transmission et stockage chiffrés des informations récoltées
- Présentation de quelques exemples d'attaques
- Aucune solution abordée

Hacking Second Life
(Michael Thumann - ERNW GmbH)

- Composants du jeux
  - Serveur d'authentification : Gère l'authentification et détermine les simulateurs correspondant à la région du joueur
  - Serveur utilisateur : Gère les sessions de messageries instantanées
  - Serveur de données : Gère les connexions aux BD (centrale, journaux, inventaire, recherche)
  - Serveur d'espace : Gère le routage des messages entre les différents lieux Les simulateurs s'enregistrent sur ce serveur et prennent connaissance de leurs voisins
  - Base de données centrale: Inventaire, facturation...
  - Simulateur : Simule une région de 256x256m du monde virtuel
  - Grid : Le monde virtuel basé sur les simulateurs
  - Viewer : Logiciel client permettant de jouer au jeu
  - Avatar : Votre personnage dans le jeu

Hacking Second Life
(Michael Thumann - ERNW GmbH)

- Points intéressants à attaquer
  - Le viewer (client - opensource) *[~Légal]*
    - Vol d'identité
      - Compte défini dans le répertoire local nommé « firstname_lastname »
      - Mot de passe enregistré dans firstname_lastname\user_settings\password.dat
        - XOR (Adresse MAC + MD5 (password)) > password.dat
        - Cassable (md5crack, mdcrack, rainbowtables)
    - Triche
      - Modification du code du client ou de la mémoire, écoute du trafic réseau...
      - Pour amasser de l'argent (230 L$ = 1US$)
  - Les serveurs de Linden Labs *[Illégal]*
    - Environnement Apache / Squid (reverse proxy + HTTPS) sur Debian
    - Installation par défaut non durcie
- Attaques possibles depuis le monde virtuel via le langage LSL
  - SPAM, attaque de vrais serveurs Web (injection SQL, XSS...), slikto :) ...

New Viral Threats of PDF Language
(Eric Filiol - ESAT)

- Étude visant à identifier les fonctionnalités à risque des PDF
- Démarche suivie :
  - Étude des fonctionnalités du langage et des vulnérabilités intrinsèques
  - Étude des vulnérabilités d'un logiciel de lecture de PDF (Adobe Acrobat Reader)
  - Développement d'une preuve de concept
- Une simple lecture d'un PDF dans Acrobat Reader permet :
  - De lancer un exécutable ou d'imprimer un document du disque dur
  - D'établir une connexion vers une ressource externe (Phishing)
  - De voler des documents au travers du réseau
- Vérifier l'intégrité et les droits d'accès à AcroRd32.dll & RdLang32.xxx
- Vérifier l'intégrité de la base de registres, limiter les contenus actifs et utiliser la signature numérique

Investigating individuals and organizations using open source intelligence

(Roelof Temmingh, Chris Böhme - Paterva et Pinkmatter Solutions)

- Internet regorge d'informations sur les personnes (et les organisations)
- Informations intéressantes s'il est possible de les corréler
- Création de l'application Maltego (v2)
  - Collecte les informations sur une personne ou une organisation
  - Utilise les moyens gratuits (moteurs de recherche, DNS, Whois, ...) afin de corréler les informations
  - Visualisation graphique du résultat (entités, liens, poids...)
- Exemples d'utilisations possibles
  - Ressources humaines
  - Atteinte à l'image d'une personne ou d'une organisation
  - Influencer l'opinion publique
  - Influencer les sondages politiques...

Conclusions

- Un certain nombre de points positifs :
  - Keynote plutôt réussie
  - Présentations techniques variées
  - « Social Event » toujours aussi apprécié
- Et de points négatifs :
  - Peu de nouveautés
  - Moyens de protection toujours aussi peu développés
- Documents pour approfondir :
  - Site Black Hat : http://www.blackhat.com/html/bh-europe-08/bh-eu-08-archives.html
  - Newsletter HSC : http://www.hsc-news.com/archives/2008/000044.html

Questions

?