OSSIR
Groupe Sécurité Windows

Réunion du 11 juin 2007

Compte Rendu
SSTIC 2007

EdelWeb

Jérémy LEBOURDAIS
EdelWeb
jeremy.lebourdais (à) edelweb.fr

Mickaël DEWAELE
EdelWeb
mickael.dewaele (à) edelweb.fr

Plan

- Introduction
- Présentations du Mercredi 30 Mai
- Présentations du Jeudi 31 Mai
- Rump Sessions et Social Event
- Présentations du Vendredi 1er Juin
- Conclusion

Introduction

- Conférence sur la sécurité devenue incontournable en France
- Qualité des présentations
- Se déroule à Rennes
- Quelques chiffres
  - 5ème édition
  - 210 places vendues en moins de 4 jours
  - 3 jours de conférences
  - 25 rump sessions

Première journée: Mercredi

Prise en compte des nouveaux risques SSI : un défi pour les petites ou moyennes entités publiques – Stéphane Cottin et Jérôme Rabenou 1/7

- Rôle du Conseil Constitutionnel
  - Résultats et litiges liés aux élections
  - Publication des documents d'Etat classés confidentiels
- Difficultés techniques et organisationnelles d'intégrer la sécurité
  - Ouvertures aux NTIC augmente potentiellement la menace
  - Les moyens ne sont pas au niveau des besoins (LOLF)
  - RSSI mal vu par les utilisateurs
  - RSSI seul n'est pas suffisant

Vers un marquage spatio-temporel des documents électroniques– Philippe Balbiani 2/7

- Théorie sur le marquage des documents
- Marquage temporel -> marquage spatio-temporel
- Idée : composition des deux protocoles :
  - Utilisation en séquence topographique puis horodatrice
- Limites pratiques
- Le problème reste ouvert, pas de réponse actuelle

Secrets d'authentification sous Windows – Aurélien Bordes 3/7

- Rappel des bases d'authentification et de gestion des mots de passe sous Windows
  - LM, NTLM, Kerberos
- Utilisation des condensats gardés en mémoire pour les authentifications non interactives
- Les démos :
  - récupération du condensat LM, puis déchiffrement
  - récupération du condensant NTLM pour rejouer un challenge et accéder au domaine

Attaques par analyse de canaux cachés et de fautes. Application aux algorithmes à spécifications secrètes – Christophe Clavier 4/7

- Attaque de cartes à puces en boite noire
  - Analyse par mesure de temps
  - Analyse par mesure de consommation de courant
  - Analyse de fautes différentielle (DFA) et collisions (CFA)
- SCARE (Side Channel Analysis for ReverseEngineering)
  - Retrouver une clé secrète
  - 2003: Révélation de fonctions d'algorithmes non connues

CryptoPage : une architecture efficace combinant chiffrement, intégrité mémoire et protection contre les fuites d'informations – Guillaume Duc, Cyril Brulebois et Ronan Keryell 5/7

- Confiance portée sur Hardware
- Architecture sécurisée basée sur l'infrastructure HIDE
  - Amélioration des limites du projet HIDE (Hardware support for leakage-Immune Dynamic Execution)
- Protection des données de bout en bout
  - Chiffrement des données en mémoire
  - Protection des bus contre la fuite d'information
- Impact sur les performances seulement de 3%

Mécanisme d'observation d'attaques sur Internet avec rebonds – Éric Alata, Ion Alberdi, Vincent Nicomette, Philippe Owezarski et Mohammed Kaaniche 6/7

- Etude des activités pirates sur les attaques par rebonds
- Mise en place de pot de miels avec redirections dynamiques
  - L'activité depuis le serveur compromis est redirigée sur un pot de miel
- Utilisation de Netfilter et du module CONNTRACK
  - Alternative entre espace noyau et utilisateur
- Limites : possibilité de détecter le pot de miel

Découverte de réseaux IPv6 – Nicolas Collignon 7/7

- Techniques/Outils classiques de scan IPv4 plus possible
  - Scanner un réseau /64 dure 585 millions d'années
- Scan des IP locales à distance: pas de vérification du périmètre des adresses
- Routage intégré au niveau des routing headers
- Sherlock
  - Outil de scan avec sondes
  - Informations découvertes au fur et à mesure alimentent le moteur de scan

Seconde journée: Jeudi

Recherche de vulnérabilités dans les drivers 802.11 par techniques de fuzzing – Laurent Butti et Julien Tinnès 1/8

- Pas/peu de prise en compte de la sécurité dans le développement de drivers
- Découvrir des failles dans les drivers
  - Obtenir un accès système
  - Critique (non authentifié et non associé)
  - Indépendance des couches supérieures
- « Fuzzing » ?
- Explication de la démarche de création de l'exploit
- Faille MadWifi: 1ère faille publique 802.11 distante sous Linux ! (exécution de code en ring0 ☺)

Exploitation en espace noyau – Stéphane Duverger 2/8

- « Thème » dans la continuité de la présentation précédente (très technique)
- Explication sur la représentation d'un processus sous Linux 2.6
- Spécificités d'un shellcode en mode noyau
  - Process context
  - Interrupt context
- Infection
  - GDT (initialisée au démarrage, environ 65ko de libres)
  - Modules
- Exploitation des drivers madwifi / broadcom

De l'invisibilité des rootkits : application sous Linux – Eric Lacombe, Frédéric Raynal et Vincent Nicomette 3/8

- Etat de l'art des rootkits
- Elaboration d'un rootkit
  - Architecture
  - Communication
  - Evaluation d'un rootkit
- Explications sur la création d'un rootkit « furtif »
- Limites du rootkit présenté (dissimulation)
  - Nombreux appels système
  - Dissimulation du rootkit
  - Dissimulation des processus
- Beaucoup de travaux pour dissimuler les rootkits, quels moyens pour les détecter demain ?

Analyse statique par interprétation abstraite – Xavier Allamigeon et Charles Hymans 4/8

- Analyse statique du code source – dédié aux buffers
- Traçage des allocations mémoire
- Les tas ne se chevauchent pas -> organisation par bloc
- Newspeak : langage simplifié pour faciliter l'analyse

Metasm, l'assembleur – Yoann Guillot 5/8

- Framework pour manipuler des blocs de code exécutable
- Développé en Ruby
- « Scapy » du code exécutable
- Prévu d'être intégré à MetaSploit
- Démonstration de l'outil

Indiscrétion et « zones constructeurs » des disques durs – Laurent Dupuy 6/8

- Présentation de la norme ATA
- Fonctionnalités (peu connues ?) de protection des disques
  - Mots de passe au niveau du disque
  - Effacement sécurisé
  - ...
- Commandes peu ou non documentées
  - Utilisation du connecteur « Master/Slave »
  - Zone HPA
- Recommandation: Chiffrement intégral du disque et utilisation des moyens de protection du disque

Autopsie d'une intrusion « tout en mémoire » sous Windows – Nicolas Ruff 7/8

- Comment récupérer le contenu de la mémoire vive (mots de passe, outils en mémoire, …) ?
  - Virtualisation: parfait mais encore peu répandu
  - Firewire: peu fiable
  - Carte d'acquisition: cher, peu accessible, contournable
  - Crashdump: écrasement du pagefile.sys
  - Dump de la mémoire par le réseau: (trop) long, nécessite d'avoir d'autres informations
  - Hibernation: format propriétaire, uniquement les pages mémoire utilisées
- Outils encore jeunes
- Nécessite des compétences fortes (analyse du dump mémoire en partie manuelle)

Confidentialité et cryptographie en entreprise – Marie Barel 8/8

- **Historique de la législation sur la cryptographie**
  - **(Lente) Libéralisation des moyens de cryptographie (LEN)**
- **Chiffrement des données est un problème en entreprise**
  - **Droit de l'employeur sur les données du salarié**
  - **Limite Privé/Professionnel**
- **Réglementation en entreprise**
  - **Importance de la charte !**
  - **Basée sur la jurisprudence**

Rump Sessions

- 4 minutes par sessions
- Beaucoup de rumps ! (25)
- Des sujets variés
  - Le debugging furtif sous Windows (Nicolas Brulez)
  - Petit Trojan hardware (Stéphane Jourdois)
  - Fiabilité des logiciels antirootkit sous Windows (Thomas Sabono)
  - Chiffrement over HTTP (Renaud Feil)
  - …
- Et aussi…
  - Elektronik Supersonik (DJ Julien, Raph et Yoann)
  - tHTP (Guillaume Arcas)
  - SSTIC 5.0 (Nicolas Fischbach et Frédéric Raynal)

tHTP

Social Event

© C. Blancher

Troisième journée: Vendredi

Démarches de sécurité & Certification : atouts, limitations et avenir – Christian Damour 1/6

- Explication détaillée sur les démarches de certification (Critères Communs)
- Les pièges à éviter, conseils et solutions
- Marché de la certification en croissance
  - Dématérialisation et mondialisation des échanges
  - Dépendance de plus en plus grande des organisations par rapport aux technologies employées

VOIP, une opportunité pour la sécurité ? – Nicolas Dubée 2/6

- Retour d'expérience sur la sécurité VOIP
- Présentation des protocoles VOIP (SIP, RTP, H323, …)
- Problème: protocoles complexes (SIP notamment)
- Risques induits par la VOIP
  - Dommages collatéraux: intrusion VOIP et rebond dans le SI
  - Confidentialité des échanges: utilisation de protocoles supplémentaires, problèmes (ex: transcodage)
- Solution pratique: pont matériel qui chiffre le flux voix

Sécurité d'OpenDocument et Open XML (OpenOffice et Ms Office 2007) – Philippe Lagadec 3/6

- Comparatif de la sécurité des documents OpenOffice et MsOffice
- Plus de langages supportés pour les macros, donc plus de complexité, …
- Problème des objets OLE: format non ouvert, donc peu analysable, fuites d'informations possibles
- Parades
  - Blocage de certains paramètres sous Office 2007 par GPO
  - Pas de OLE, utilisation de formats tels que PDF par une imprimante virtuelle
  - Suppression des macros
  - Analyse des fichiers ZIP et XML

Evolution des attaques de type « Cross Site Request Forgery » - Louis Nyffenegger / Renaud Feil 4/6

- Attaque CSRF: sans JavaScript, sans Cross-Site Scripting …
  - Exploitation d'une requête prédictible
  - Ex: *http://www.hsc.fr/changePassword?value=newpass*
- Attaque connue depuis plusieurs années
- Maintenant dans le top 5 de l'OWASP
- Beaucoup (trop) de sites web vulnérables
- Démonstration pas à pas
  - Persistance du code malveillant
  - Interactivité
- Impact réel !
- Protections
  - Renforcement des navigateurs, utilisation de deux navigateurs (lourd)
  - Jeton aléatoire (assez simple)

La cryptographie au secours du vote électronique – Marc Girault 5/6

- Vote hors ligne : contrôlé par autorité électorale / déconnecté
- Vote hybride : contrôlé par autorité électorale / relié en réseau
- Vote en ligne : non contrôlé par autorité électorale / relié en réseau
- Beaucoup d'avantages au passage du vote en ligne
- Pas infaisable si on s'y prend bien, mais la solution n'est pas envisageable pour demain
- Sujet encore sensible: fiabilité, nombreux problèmes récents avec les machines à voter, confiance dans le système, …

Etat de l'art – cassage de mot de passe – Simon Maréchal 6/6

- Actuellement
  - Logiciels de cassage peu optimisés
  - Processeur Pentium très lent pour ce type de calcul
- Utilisation des processeurs CELL (PlayStation 3) pour casser les mots de passe
- Optimisation des instructions (utilisation de tous les cœurs en même temps)
- Résultats (à confirmer)
  - NT Hash: AMD64 3500+: 11M mdp/s, PS3: 180M mdp/s …
  - MD5: PS3: 120M mdp/s
- Bonne idée pour se faire payer une PS3 ☺

Conclusion

- Haut niveau technique
- Qualité des conférences
- MISC interactif ?
  - Présentation
  - Lecture de l'acte
  - Discussion avec l'auteur (autour d'un verre ☺)
- Rumps sessions et Social Event !
- Actes disponibles (actes.sstic.org)
- Merci beaucoup à Nicolas Ruff, ainsi qu'au CO du SSTIC

Quelques comptes-rendus

- http://bruno.kerouanton.net/dotclear/index.php/2007/06/04/117-sstic-compte-rendu
- http://nonop.blogspot.com/2007/06/sstic-2007.html
- http://sid.rstack.org/blog/index.php/2007/06/04/193-le-sstic-2007-comme-si-vous-y-etiez-ou-pas
- http://yom.retiaire.org/doku.php?id=le_sstic_est-il_toujours_le_sstic

Questions / Réponses ?