Compte-rendu de la 16 ème conférence du FIRST

Michel.Miqueu@CNES.fr

Olivier.Castan@certa.ssi.gouv.fr

Introduction

- FIRST association (de droit américain) des CERTs (~ 150)
- Conférence annuelle accueillie à Budapest du 13 au 18/06/2004
- Ouverte à tous, public hétéroclite
- 5 continents inégalement représentés
- Programme
  - “Tutoriels” (2 jours)
  - Sessions (niveau # autres conférences)
- Prochaine conférence

Establishing a Formal Program Vulnerability Discovery

- Mission “Vulnerability Discovery and Avoidance” (WDA) au lieu du schéma usuel de découvertes a posteriori pour limiter la diffusion des vulnérabilités
- Coordination et mise à jour d'un document :
  - Identification et recensement des acteurs compétents avec leurs techniques
  - Création d'une taxonomie des défauts (XML)
  - Bonnes pratiques de programmation

Inside Microsoft Security

- 3 heures pour quelques planches... des relations publiques (sconant@microsoft.com)
- Des informations ayant un intérêt :
  - 6 semaines en moyenne pour un cycle (évaluation, correctif, tests et diffusion)
  - Le rythme mensuel de diffusion (hors urgence) est un besoin client : pourrait évoluer avec la demande
  - Gestion des priorités (sujet alors brûlant : SP versus faille IE)

Workshop on Network Flow Analysis

- Netflow et suite Argus (http://www.qosient.com/argus/)
- Capture des paquets passive
- En cas de commutateur :
  - Port monitor
  - Ettercap (mais arp-spoofing)
- Tcpdump et Ethereal pour les nuls...
- Knoppix et dérivées (machines Intel)

Fighting Internet Diseases: DDoS, Worms and Miscreants 1/6

- Présentation Riverhead/Colt
- La menace :
  - Une organisation hiérarchique : commanditaire, maîtres, “zombies” (évolution vers 100 000/réseau)
  - 4000 attaques/jour 40 à 200/h (source Caïda)
  - Professionalisation (extorsion, cassage de clés, spam,...)
  - Marché parallèle de réseaux d'attaque, mercenaires abordables (~ 100$)
  - Evolution du niveau des attaquants (anticipation et réaction aux parades)

Fighting Internet Diseases: DDoS, Worms and Miscreants 2/6

- Les moyens :
  - Paquets IP quelconques (sauf la destination)
  - Falsification de la source inutile (nombre)
  - Diversification :
    - Niveau applicatif (non “vu” par le réseau)
    - Requêtes DNS récursives (DNS root protégés par routage unicast)
    - Mot de passes par défaut sur routeurs
    - DDoS des infrastructures (BGP, OSPF)
  - 2 valeurs critiques : bande passante et paquets/s

Fighting Internet Diseases: DDoS, Worms and Miscreants 3/6

- Quelques caractéristiques :
  - Classe A virtuelle reçoit les ACKs en cas de spoof
  - 58% des attaques < 15 mn : réaction et analyse ?
  - Préférence UDP (90%) sur TCP depuis 2003
  - Min 30j avant l'exploitation massive d'1 vulnérabilité
  - Contaminations cycliques avec l'extinction des machines personnelles
  - botnets sur canaux IRCs populaires (pbs de logs : taille, langues,...)

Fighting Internet Diseases: DDoS, Worms and Miscreants 4/6

- Détection :
  - Remontée au NOC
  - “backscatter traceback” (http://www.secsup.org/Tracking/)
  - Cisco Netflow + console
  - Recopie (“optical splitters”)

Fighting Internet Diseases: DDoS, Worms and Miscreants 5/6

- Atténuation des dommages :
  - ACLs de proche en proche (! cpu => turboACLs)
  - Cisco CAR (bande passante limitée par protocole,...)
  - “Null0 routing” ou “blackholing” (! ICMP type 3)
  - “Egress filtering” : classes non allouées,... (! liste non figée)
  - “Ingress filtering” : limite le spoof des zombies
  - Cisco uRPF : teste si le retour est sur la même interface (pb avec routage asymétrique)
  - Réseau FAI : NSP-SEC

Fighting Internet Diseases: DDoS, Worms and Miscreants 6/6

- Ne pas reconfigurer sous attaque !!!
- Les produits dédiés :
  - Console Netflow et émission d'ACLs : Arbor Peakflow, Reactive Networks
  - Commutateurs, pare-feux en coupure : Mazu Networks
  - Equipements compagnons des routeurs détournant et filtrant le flux suspect : Riverhead Networks (rachat par Cisco)

European Security Research

- Présentation commission européenne
- ENISA (directeur italien nommé entre temps) et PCRD
- Quelques cauchemars : e-justice, “digital passport”,...

Welcome Address

- Intervention secrétaire d'état
- Hongrie peu avancée en sécurité
- Actions en cours :
  - CERT national,
  - Centre de compétence antiviral.

Vulnerability Analysis, Reporting and Handling 1/2

- Intervention Microsoft
- Sites Microsoft : 4000 attaques/j, 1+ DDoS
- Evolution constatée : remontée dans la pile ISO
- Le patch facilite l'écriture des exploits (min. 9j)
- => étudie d'autres manières de corriger (comportemental,...)
- Lutte : récompenses, expertises pour forces de l'ordre

Vulnerability Analysis, Reporting and Handling 2/2

- Le problème des particuliers :
  - ~30% des particuliers ont des spywares (34M annoncés par Gator)
  - Spywares : 50% des remontées Docteur Watson et 30% des appels chez les grands assembleurs
  - 20% des bots d'après Earthlink
- Evolution de la culture chez Microsoft : preventive -> reactive -> proactive
- Principe de la défense en profondeur (exemple avec WebDAV sous 2003 : service inactif par défaut, 16k max pour une url,...)
- L'application à 2k avec 1 SP serait difficile

A Framework for Collection and Management of Intrusion Detection Data Sets

- Présentation laboratoire de Los Alamos
- Problème pour gérer un nombre conséquent de traces :
  - Base avec 10 milliards d'enregistrements,
  - Croissance de 50 millions par jour
- Comparaisons entre MySQL et des index en arbre B+ statique
- Supériorité des arbres en terme de stockage et de rapidité lorsqu'il y a beaucoup de réponses, mais requêtes simples

Public Monitoring

- Organisation de la veille au CERT/CC

The Incident Response Team Objective in the RIPE Database

- Depuis 2003 la base de données RIPE inclut des champs pour décrire l'équipe de sécurité de rattachement

Network Monitoring and Web Portal Site Project in AP Region

- Mise en place du coordination dans la région Asie Pacifique : Japon et Corée
- Mise en place de sondes réparties
- Corrélation des sources
- Exportation au format IODEF

Internet Threat Detection System Using Bayesian Estimation

- Détection automatique d'anomalies réseau
- Sondes distribuées
- Comparaison avec un filtre prédictif Bayésien et éventuelle alerte
- Site http://www.clscan.org (pratique du Japonais recommandée !)

Security Implications of IPv6 1/2

- IPv6 est couramment disponible
- La transition IPv4-IPv6 repose sur des protocoles complexes souvent mal interprétés par les pare-feux (6over4 = SIT, Teredo IPv6 sur UDP,...)
- L'"underground" à déjà investit IPv6 (ftp, IRC, Web, portes dérobées avec tunnel dans Ipv4,...)
- Les 64 bits de poids faible (dérivés du MAC) : risque pour la vie privée, fuite d'information. Si aléatoire (boot, intervalles réguliers), la machine devient difficile à identifier.

Security Implications of IPv6 2/2

- Transition : un énorme sous-réseau pour chaque adresse IPv4
  - Scan a priori impossible
  - Sauf si choix par défaut connu (Windows, Linux)
- Outils de sécurité (pare-feux, sondes,...) traitent rarement l'encapsulation des protocoles

Defense in Depth: Protecting Against Zero-Day Attacks 1/2

- Evolution des exploits :
  - 1er débordement de tampon publié en 96 dans BugTraq
  - 96 débordements dans la pile, 98 dans le tas
  - 2000 débordement d'un octet (TESO)
  - 2001 formats de chaîne et débordements d'entiers
- Quelques caractéristiques :
  - Réseau : requête mal formée, longues, shellcode
  - Localement : pointeurs écrasés, shellcode, appels systèmes

Defense in Depth: Protecting Against Zero-Day Attacks 2/2

- Traitement :
  - Réseau : sonde, pare-feu, nettoyage (urlscan)
  - Localement modifications du noyau : canaris, pile et tas non exécutables, modifications aléatoires des adresses des librairies (GOT, PLT)
- Voir PaX sous Linux (http://www.grsecurity.net)

Computer Forensics in a Global Company

- La parole a un sponsor majeur
- Gros problème : le respect des droits nationaux quand on est une multi-nationale...

FIRST – The Road Ahead

- De la coordination vers l'opérationnel
- Loin du consensus (implication “nationale”, de défense,...)

ARAKIS – An Early Warning and Attack Identification System

- Présentation du CERT Pologne
- Site http://arakis.cert.pl (en polonais) qui agglomère les données de pare-feux protégeant 2000 adresses, 4 honeyd et des renifleurs basés sur la libpcap (C/Perl/PHP)
- Futur : support de Netflow

Deploying New Wireless Standards in Corporate Environments

- Présentation FT R&D
- Utiliser WPA au lieu d'IPSEC dans la pratique (en attente du 802.11i) :
  - Authentification EAP-TLS avec FreeRadius (lacune : ne supporte la reprise de session TLS – réauthentification complète à chaque changement d'AP)
  - Le matériel n'est pas suffisant, mise à jour du logiciel (XP >SP1)
  - Goulet d'étranglement potentiel : transfert des CRLs vers le serveur Radius

The CSIRT and Wireless Security Breaches

- Présentation Cisco
- Sécurisation a priori
  - Dissimulation : puissance, non diffusion du SSID
  - Filtrage des MACs
  - Authentification LEAP
- Attaques
  - Point d'accès sauvage (le + souvent interne)
  - Collecte et analyse hors ligne (Kismet, asleap)
  - Fausses adresses MACs
- Outil détection d'APs sauvages à venir

APCERT, TF-CSIRT Activity Updates

- L'APCERT se lance dans la TI
- La TF-CSIRT continue à parler des projets financés par l'UE (dont EISPP) en 2002-2003

FIRST at WSIS: The Security in the Emerging Information Society

- Présentation D. Crochemore, Steering Commitee, CERTA
- Le Sommet Mondial pour la Société de l'Information (ONU) fait travailler conjoitement gouvernements, secteur privé et ONGs
- FIRST reconnu comme ONG, en phase avec plusieurs points du plan d'action
- But du FIRST auprès du SMSI : étendre son audience

US-CERT and Collaboration with CSIRTs

- Ou comment le CERT-CC va rentrer dans le giron du DHS
- Recours aux ISACs
- Exercice d'alerte en octobre 2003

Why a Business Needs to Set Up a Cyber Threat Analysis Unit

- Les techniques de l'espionnage classique adaptées à l'espionnage économique
- Moteur de recherche : http://www.copernic.com

Critical Infrastructure Protection – A Business View

- Les leçons des banques allemandes durant la période de la FAR

What Went Wrong ? 1/2

- Retour d'expérience par ancien membre de Paraprotect
  - L'équipe de sécurité compétente et bien entraînée mais qui ne prend pas en compte la continuité de l'activité
  - Le client n'est pas toujours compétent : prévoir au delà du matériel annoncé
  - Equipe leurrée par un rootkit avant que ce soit la mode : corréler avec l'extérieur du système

What Went Wrong ? 2/2

- Equipement égaré pendant le voyage : redondance, polyvalence
- Administrateur qui n'assume pas et qui bricole : vérifier toutes les informations
- International, difficulté à trouver de bons contacts : intérêt du FIRST

UNIX and Linux Based Rootkits: Techniques and Countermeasures 1/2

- Evolution :
  - Modifications des programmes d'administration
  - Modification de quelques appels du noyau à l'aide d'un module (Adore, SucKIT, AdoreNG)
- Protection :
  - Désactiver les modules
  - Protéger /dev/kmem (nécessite avec un noyau avec extensions MAC)
  - Module anti-rootkit

UNIX and Linux Based Rootkits: Techniques and Countermeasures 2/2

- Détection :
  - Les sommes de contrôle pour détecter les incompétents
  - Faire une copie connue des structures sensibles du noyau (kstat)
  - Mesure de la durée des appels systèmes
  - Analyse hors ligne (TCT)

Assemblée Générale

- 2 motions
  - Modifs du SC (CA) (non votée)
- Nouveau Steering Committee
  - 2 US
  - 1 Brésil
  - 1 Japon
  - 6 Européens (1 Français)

Conclusions/Questions

- Présence de Microsoft malgré un public peu favorable...
- La menace organisée n'est plus du FUD
- Rééquilibrage de la prédominence américaine au FIRST
- http://www.first.org/conference/2004/proceedings (disponible en janvier)