Cert-IST
Computer Emergency Response Team
Industrie Services et Tertiaire

Nomenclature : **CERT-IST/315/06/001/CR/I**
Edition : **1**
Révision : **0** Date : 10/08/2006

Référence. : **3AT 40014 0001 CRZZB**

Compte-rendu de la conférence SSTIC - Rennes juin 2006

Rédigé par :	Stéphane Rozes	le : 29/05/2006	
Vérifié par :	Philippe Bourgeois Anne-Laure Bouillot	le : 9/08/2006	

Pièces jointes : *Néant*

9, rue du Président Allendé 94 526 Gentilly Cedex - France
Tél. : 05 34 35 33 88
E-Mail : cert@cert-ist.com
Web : www.cert-ist.com

Sommaire

1. INTRODUCTION 1
1.1. Objet du document 1
2. LES PRÉSENTATIONS 1
2.1. Introduction de la conférence : Puissance militaire et modernité 1
2.2. Epyks: reversing Skype (Fabrice DESCLAUX - EADS) 2
2.3. Plus cela change... (Pierre VANDEVENNE - DataRescue) 3
2.4. Outrepasser les limites des techniques classiques de Prise d'Empreintes grâce aux Réseaux de Neurones (Carlos SARRAUTE & Javier BURRONI - Core Security Technologies) 3
2.5. La sécurité matérielle: le cas des consoles de jeux (modchip) (Cédric LAURADOUX - INRIA Projet CODES) 4
2.6. Regards croisés de juristes et d'informaticiens sur la sécurité informatique (Marion VIDEAU - Institut Gaspard Monge - & Isabelle DE LAMBERTERIE - CNRS) 5
2.7. Playing with ptrace() for fun and profit (Nicolas BAREIL - EADS) 7
2.8. Contournement des I(D|P)S pour les nuls (Renaud BIDOU - Radware) 8
2.9. Diode réseau et ExeFilter : 2 projets pour des interconnexions réseau hautement sécurisées (Philippe LAGADEC – DGA/CELAR) 9
2.10. Dissection des RPC Windows (Nicolas POUVESLE - Tenable Network Security) 11
2.11. Qualification et quantification des risques en vue de leur transfert : la notion de patrimoine informationnel (Jean laurent SANTONI - Marsh Risk Consulting France) 12
2.12. Les évolutions de l'implémentation des spécifications du TCG au sein de la plateforme Windows (Bernard OURGHANLIAN – Microsoft France) 13
2.13. La sécurité, problème majeur pour les plateformes de diffusion multimédia sur des réseaux hétérogènes (Ahmed reda KACED - ENST Paris - & Jean-Claude MOISSINAC) 13
2.14. Sécurité des offres ADSL en France (Nicolas RUFF - EADS) 14
2.15. Et si les fonctionnalités des processeurs et des cartes mères pouvaient servir à contourner les mécanismes de sécurité des systèmes d'exploitation ? (Loïc DUFLOT & Olivier GRUMELARD - DCSSI) 15
2.16. La mobilité sous IPv6 et ses implications pour la sécurité (Arnaud EBALARD - EADS - & Guillaume VALADON - The University of Tokyo - Esaki Lab / LIP6, Paris) 17
2.17. Vulnérabilité des postes clients (Gaël DELALLEAU & Renaud FEIL - Ernst & Young) 17

2.18. Mécanismes de sécurité et de coopération entre nœuds d'un réseau mobile "ad hoc" (Pietro MICHIARDI - Eurécom) 18

2.19. Les défis du management de la sécurité (des systèmes d'information) (Sylvain RAVINET – Adenium) 19

2.20. Détection de tunnels en périphérie du réseau (Guillaume LEHEMBRE & Alain THIVILLON - HSC) 20

2.21. SSI : quelles responsabilités ? (Marie BAREL – Links conseil) 22

2.22. Evaluation du coût de la sécurisation du système DNS (Daniel MIGAULT - FT - & Bogdan MARINOIU) 24

2.23. Corruption de la mémoire lors de l'exploitation (Samuel DRALET & Francois GASPARD - étudiant) 24

2.24. RFID et sécurité font-elles bon ménage ? (Gildas AVOINE – MIT - USA) 25

2.25. Détection d'intrusion dans les réseaux 802.11 (Laurent BUTTI - FT) 26

2.26. Faiblesses d'IPSec en déploiements réels (Yvan VANHULLEBUS (NETASQ) 27

2.27. Rump Sessions 28

3. CONCLUSION 29

Gestion documentaire

Bordereau d'indexation

Titre	**Compte-rendu de la conférence SSTIC - Rennes juin 2006**
Référence	**3AT 40014 0001 CRZZB**
Nomenclature	**CERT-IST/315/06/001/CR/I**
Confidentialité	**Diffusion limitée aux Partenaires**"
Auteur	**Stéphane Rozes**
Mots clés	
Volume (car.)	57765
Nb. de pages	37
Résumé	Ce document constitue le compte-rendu de la conférence SSTIC qui s'est déroulée à Rennes les 31 mai et 1er et 2 juin 2006.

Diffusion du document

Destinataire	Société
Membres Partenaires	**ALCATEL, CNES, FRANCE TELECOM, SANOFI-AVENTIS**
Pierre Forget	**Cert-IST**

Historique des versions

Version	*Date*	*Rédacteur*	*Objet de la modification*	*Pages*		
				Ajout	*Modif.*	*Supp.*
0.1	29/05/06	S. Rozes	Création du document	Toutes		
1.0	10/08/06	S. Rozes	Prise en compte des remarques internes		Toutes	

Glossaire

ACL	Access Control List - Liste de contrôle d'accès
ARP	Address Resolution Protocol - Protocole réseau de niveau 2
ATM	Asynchronous Transfer Mode – Mode de transmission par cellule
BHR	Black Hole Routing - Protocole/technique lié au routage
CADHO	Collect and Analysis of Data from Honeypots - Projet sur les pots de miel
CESTI	Centre d'Evaluation de la Sécurité des Technologies de l'Information
CCIPS	Computer Crime and Intellectual Property Section - Organisme américain
CDP	Cisco Discovery Protocol - Protocole réseau de Cisco
CERT	Computer Emergency Response Team
CPU	Central Processing Unit - Processeur
CVE	Common Vulnerabilities and Exposures - Standard de référencement de vulnérabilités
DCSSI	Direction Centrale de la Sécurité des Système d'Information
DDoS	Distributed Denil Of Service - Déni de service distribué
DHCP	Dynamic Host Configuration Protocol - Protocole d'allocation d'adresse IP
DNS	Domain Name Service - Protocole de nommage
GSM	Téléphone mobile
HIDS	Host based Intrusion Detection System - Détecteur d'intrusion système
HTTP	HyperText Transfer Protocol - Protocole web
HTTPS	HyperText Transfer Protocol Secured - Protocole web sécurisé
ICQ	Phonétiquement "I seek you" : Messagerie instantanée
IP	Internet Protocol
IPSec	Protocole de sécurité pour les communications réseau
ITSEC	Critères harmonisés pour l'évaluation de la sécurité des systèmes et produits informatiques
LLS	Licence Logging Service - service de gestion des licences des systèmes Microsoft Windows
LSASS	Local Security Authority Subsystem Service - Service gérant la sécurité des systèmes Microsoft Windows
MOA	Maître d'OuvrAge
MOE	Maître d'OEuvre
MMQ	Microsoft Message Queue - Gestionnaire des files d'attente des systèmes Microsoft Windows
NTLM	New Technology Lan Manager - Méthode d'authentification des systèmes Microsoft Windows
NIDS	Network Intrusion Detection System - Détecteur d'intrusion réseau

NUMA	Non-Uniform Memory Access - Technologie multiprocesseurs
OLE	Object Linking and Embedding - Fonctionnalité de Microsoft Windows permettant d'empaqueter des objets
OSI	Open System Interconnection
PC	Personal Computer
RFID	Radio Frequency Identification – Système d'identification par radiofréquence
RPC	Remote Procedure Call – Appel à des procédures distantes
RPF	Reverse Path Forwarding - Protocole/technique lié au routage
RTP	Real-Time Transport Protocol - Protocole de transport de données en temps réel
SGDN	Secrétariat Général de la Défense Nationale
SHA-1, SHA-256	Algorithmes de signature numérique
SI	Système d'Information
SIP	Session Initiation Protocol - Protocole de signalisation pour la voix sur IP
SMB	Server Message Block - Protocole de partage de ressources
SMP	Symmetric MultiProcessing - Technologie multiprocesseurs
SMS	Short Message Service - Messagerie pour les portables
SQL	Structured Query Language - Langage pour les bases de données relationnelles
SRTP	Secure RTP
SSH	Secure Shell
SSI	Sécurité des Système d'Information
SSTIC	Symposium sur la Sécurité des Technologies de l'Information et des Communications
TCP	Transport Control Protocol - Protocole de transport de la pile TCP/IP
TOE	Target Of Evaluation - Cible d'évaluation
UPnP	Universal Plug and Play
VRF	VPN Routing/Forwarding - Protocole/technique lié au routage
WEP	Wired Equivalent Privacy - Protocole de sécurité pour les communications sans-fil
WPA	Wi-Fi Protected Access - Protocole de sécurité pour les communications sans-fil

Documents

Documents Applicables

	AUCUN

Documents de Références

[DR1]	Actes de la conférence SSTIC

1. INTRODUCTION

1.1. Objet du document

La conférence SSTIC (Symposium sur la Sécurité des Technologie de l'Information et des Communications) s'est déroulée les 31 mai et 1 et 2 juin derniers à Rennes. Cette conférence regroupait près de 400 personnes dont de nombreux universitaires et militaires, ainsi que des membres des CERT français (CERTA).

Les présentations techniques étaient d'une manière générale orientées recherche et développement (pas de présentation commerciale). Parallèlement au côté technique, des présentations juridiques et organisationnelles venaient également étayer ces trois jours.

Les actes de la conférence **[DR1]** peuvent être consultés au Cert-IST ou en ligne à l'adresse suivante : http://actes.sstic.org/SSTIC06/ .

2. LES PRESENTATIONS

2.1. Introduction de la conférence : Puissance militaire et modernité

L'introduction de la conférence a été faite par Gérard BEZACIER (Général de Corps d'Armées commandant de la région terre nord-ouest et officier général de la zone de défense ouest) et a eu pour sujet l'évolution des enjeux stratégiques dans le monde de demain.

Cette introduction a permis de faire un tour d'horizon géopolitique sur le monde qui nous entoure.
Il en ressort des tendances assez fortes. Les stratégies de défense classiques ne sont plus adaptées au monde moderne. En effet, l'"Etat souverain" est devenu de plus en plus faible face aux nouvelles menaces que sont les réseaux mafieux et le terrorisme international. La menace n'est plus l'Etat voisin, mais des organisations internationales. Ces organisations s'appuient sur la "misère" matérielle de certaines populations, mais aussi sur le manque d'instruction/de connaissances de ces dernières afin de mieux les contrôler/endoctriner.

La défense des pays démocratiques doit alors s'adapter aux situations modernes où les ennemis de la paix (groupes terroristes) se dissimulent désormais dans des populations pacifiques et parfois extérieures au conflit. La prolifération des échanges à travers le monde (échanges commerciaux, échanges

d'informations) et la constance dans les flux migratoires des hommes (généralement des pays les moins riches vers les pays les plus riches) ne font qu'aggraver cette problématique de la sécurité des Etats.

La prolifération des armes reste également une préoccupation majeure. En effet, il est avéré que certaines organisations criminelles sont plus riches que certains états. Cette richesse financière donne à ces dernières une capacité de destruction illimitée fournie par les armes modernes. De plus, une tendance récente dans les "conflits" met en valeur une utilisation de plus en plus systématique des populations civiles comme bouclier humain, otages, …

Cet état de fait tend à démontrer que l'affrontement inter-armée est dépassé.

On voit également la limite de la haute-technologie (on ne peut tout voir/savoir) et sa récente illustration dans le conflit en Irak.
Le champ d'action devient aussi différent. Les actions terroristes se déroulent généralement en ville (terrain que l'armée moderne ne maitrise pas pleinement).

Il en ressort ainsi que les systèmes classiques de défense sont devenus obsolètes !!

Le monde occidental sait gagner des batailles, mais ne sait pas gagner des guerres ou faire la paix de manière durable (conflits au Vietnam, en Afrique, en Irak, …).

La seule solution aux conflits modernes reste le pouvoir de la Politique.

2.2. Epyks: reversing Skype (Fabrice DESCLAUX - EADS)

Cette présentation avait pour objectif de découvrir les "secrets" du logiciel de téléphonie sur IP "Skype". On retiendra de cet exposé que le logiciel "Skype" donne une impression de boite noire où tout paraît obscurci.

Le trafic réseau est de même type que celui des logiciels P2P (beaucoup de machines connectées). Le logiciel "Skype" est capable de réutiliser des accès au relais HTTP (proxy) afin de se connecter aux autres nœuds du réseau. Afin de dissimuler son trafic, "Skype" chiffre les communications réseaux avec l'algorithme de chiffrement RC4 (la clé de déchiffrement dépend du couple adresse IP/numéro de port).

Toutes ces propriétés font que les administrateurs réseau ont d'énormes difficultés à distinguer le trafic normal du trafic "Skype". De plus, si on veut effectuer des opérations de "reverse-engineering", on s'aperçoit vite que le code sensible du logiciel est chiffré. La procédure de déchiffrement se lance au début lors de l'exécution en mémoire. Enfin, pour se protéger, le binaire de "Skype" détecte les débogueurs connus et effectue un test d'intégrité du binaire afin de vérifier si ce dernier n'a pas été altéré.

Cette présentation orientée "chiffrement du code" n'a pas apporté de réponse concrète sur les moyens de se prémunir d'une utilisation abusive de "Skype".

2.3. Plus cela change... (Pierre VANDEVENNE - DataRescue)

Intervention annulée

2.4. Outrepasser les limites des techniques classiques de Prise d'Empreintes grâce aux Réseaux de Neurones (Carlos SARRAUTE & Javier BURRONI - Core Security Technologies)

Cette présentation relativement scientifique (illustrée par de nombreuses formules statistiques) avait pour objectif de faire un état des lieux sur un projet lié à la prise d'empreinte (détection à distance des systèmes d'exploitation) dont les calculs associés sont modélisés au travers d'un réseau de neurones.

On retiendra de cet exposé que les techniques "anciennes" s'appuient sur les réponses de la pile TCP/IP du système pour deviner le système d'exploitation utilisé.

Aujourd'hui et notamment pour les systèmes Microsoft, on s'appuie principalement sur les réponses des services DCE RPC. Mais les outils actuels ont cependant encore des limites :

- ils cherchent à déceler la version qui se rapproche "le plus" des résultats obtenus,
- ils ne marchent pas avec des systèmes non standards,
- ils sont incapables de reconnaître des informations "clés".

Il faut savoir que pour les systèmes Microsoft, les informations retournées par le service "portmapper" DCE RPC de Windows (requête sur le port 135) permettent de connaître les services RPC enregistrés et en fonction de leurs caractéristiques d'en déduire le système d'exploitation hôte.

Ces échanges ont été modélisés par des réseaux de neurones afin de connaître les versions, éditions, Services Packs de Windows à partir des informations fournies par le service.

L'idée est de modéliser la correspondance des points finaux avec les versions d'OS dans un réseau de neurones (multicouches : 3 couches).

- Couche d'entrée (1 neurone pour chaque UUID, 1 neurone pour chaque point final)
- Couche d'entrée cachée (combinaison de neurones)
- Couche de sortie (1 neurone pour chaque version de Windows, 1 neurone pour chaque version et

édition de Windows - standard, professionnelle – et 1 neurone pour chaque version et SP de Windows)

- Il faut ensuite "entraîner" (initialiser) le réseau (10350 générations)
    - Recalculer le poids pour chaque entrée/sortie

Les tests en laboratoire ont montré que cette méthode était plus fiable que les méthodes classiques basées sur les services DCE-RPC.

Pour les systèmes autres que Microsoft Windows, la méthode proposée s'est basée sur le fonctionnement de NMAP vis-à-vis des réponses des piles TCP/IP distantes (suite de 9 tests).

La méthode de la société "Core" se base sur les 1684 signatures de NMAP (ensemble de règles décrivant comment un système d'exploitation répond aux tests).

- Chaque signature est comparée, et un score est assigné (nombre de règles qui concordent/nombre de règles traitées).
- Le résultat est obtenu en calculant le "best fit" basé sur la distance de Hamming.

D'un point de vue théorique, l'espace des résultats comporte 560 dimensions (c'est l'ensemble de tous les résultats possibles).

Le projet a alors consisté à utiliser un réseau de neurones organisé de manière hiérarchique (système d'exploitation important ou non, famille du système d'exploitation, version) : 5 réseaux de neurones (système d'exploitation intéressant ou non, famille du système d'exploitation, version Linux, version Windows, version OpenBSD) ont été nécessaires pour modéliser le comportement de l'outil de prise d'empreinte (avec 1 neurone pour chaque flag/option TCP).

Un souci de ressources s'est rapidement posé à ce niveau car pour entraîner un réseau (entrées = réponse de machines / sorties = système d'exploitation de la machine), représentant 1684 signatures, il faudrait 15 000 machines !!!

Plusieurs évolutions sont envisagées pour cette étude :

- Optimiser NMAP pour générer moins de trafic, détecter la présence de garde-barrière et leur version
- Détection des systèmes d'exploitation via les Sun RPC/Portmapper
- Détection des clients de messagerie via les en-têtes des e-mails

2.5. La sécurité matérielle: le cas des consoles de jeux (modchip) (Cédric LAURADOUX - INRIA Projet CODES)

Cette présentation était basée sur la sécurité "physique" des consoles de jeu.

Les consoles de jeu, les systèmes bancaires ou les systèmes militaires ont les mêmes problématiques vis-à-vis de la sécurité "matérielle".

Les "**modchips**" sont des composants matériels (généralement des puces) permettant de contourner la sécurité des consoles de jeu.

- Firmware "bootland" : mise à jour de la mémoire ROM ou de la mémoire FLASH
- Capteur de signaux : détournement des signaux

En électronique, une problématique essentielle est le problème du rejeu. Une solution est basée sur le fait que le processeur a au moins une fois accès aux données de façon sûre : prise d'empreinte à ce moment

- Stockage des données dans un arbre de Merkle, mais cela entraîne un problème de mise en pratique (puissance de calcul et bande passante)
- Solution orientée écriture : "Incremental Hash function"
- Solution orientée lecture : "Incremendtal Verification Hash founction"

En conclusion, la sécurité ne va pas de pair avec les notions de performance/rentabilité/flexibilité. Il reste des problèmes au niveau du processeur avec les canaux "cachés". Cependant, il existe des solutions matérielles comme les "Trusted Platform Module" (TPM - https://www.trustedcomputinggroup.org/groups/tpm/), mais elles ont encore des faiblesses au niveau du rejeu.

2.6. Regards croisés de juristes et d'informaticiens sur la sécurité informatique (Marion VIDEAU - Institut Gaspard Monge - & Isabelle DE LAMBERTERIE - CNRS)

Cette présentation très intéressante s'est proposée de monter l'ambigüité des aspects légaux de la sécurité informatique par deux exemples :

- Détention de virus et mise à disposition de virus
- Accès à des données appartenant à un tiers

Pour la détention de virus ou la mise à disposition de virus : Il existe un arsenal répressif créé en 2004 (LCEN) **Art 323-3-1 du Code Pénal** qui permet de sanctionner la détention de virus avant qu'il ne soit introduit frauduleusement dans un SI.

- Cette loi reste très restrictive vis-à-vis de la "recherche" en matière virale car elle affecte de facto la détention de codes malveillants.
- Cependant, dans le projet de loi initial, une exception au délit existait quant à la détention de code viral pour des besoins de recherches.

- Des débats parlementaires ont alors été engagés sur le problème de la confiance envers les organismes faisant de la "recherche" (certains sont sûrs d'autre moins).
- Une modification du texte a été proposée pour introduire une notion de "motif légitime" de la recherche.

Un problème majeur avec la jurisprudence en matière de délit informatique est la difficulté de passage entre la notion de sécurité physique vers la sécurité logique.

Le vocabulaire, les métaphores, influencent énormément la perception du problème.

L'affaire "Kitetoa" (accès à une base de donnée non protégée via le web, où l'accusé a été désigné coupable puis relaxé) est pris en exemple sous l'angle d'un autre modèle de réflexion : le **modèle logique client/serveur** (une requête et une réponse).

Que se passe-t-il pénalement lorsqu'on obtient de quelqu'un des informations ? Qui plus est des informations confidentielles (via l'alcool ou le charme) ?

De par la loi, **le dépositaire du secret est responsable** !

Cet exemple montre bien qu'il faut réfléchir à des modèles liés à la logique plutôt qu'au monde physique (le débiteur d'alcool ou de charme doivent-ils prouver la légitimité de leur activité ?).

Pour aller plus loin dans cet exemple, nous pouvons aussi revenir sur la signification des notions de "**système de traitement automatisé de données**" et de "**données personnelles**".

L'article **226-17 du Code Pénal** précise que **le responsable de données doit prendre des mesures pour les protéger**.

Il en va de même pour la perception de l'intégrité des données.

La notion d'intégrité en informatique (non modification) est différente de l'intégrité en droit (qualités attendues d'un écrit signé traditionnellement : durabilité, fidélité fiabilité).

Que signifie : garantir l'intégrité ? La signature électronique n'a t'elle pas pour objectif d'apporter cette garantie ?

L'article 1316-1 Code Civil mentionne que l''écrit électronique est similaire à l'écrit sur support papier sous réserve d'identifier la personne dont il émane et qu'il soit stocké de manière à en conserver l'intégrité.

Quel statut donner au matériel informatique et au logiciel ?

Sur quel élément porte la nécessité de l'intégrité :

- En informatique : sur ce que l'on signe
- En droit : sur ce que l'on voit

A-t-on des outils de cryptographie qui prennent en compte l'aspect temporel du problème. Les protocoles de cryptographie sont adaptés dans l'espace (transmission) mais mal/pas dans le temps (nécessité juridique).

L'éclairage des archivistes a permis de remettre en cause le lien entre l'authenticité et l'authentification (qui sont deux concepts différents).

Le "Forum des droits de l'Internet" a proposé 3 critères cumulatifs de conservation de document :

- Lisibilité du document (accès au document)
- Stabilité du document (les informations contenues dans le document restent les mêmes)
- Traçabilité du document (présentation et vérification de l'ensemble des traitements lors du processus de conservation)

En conclusion, cet exposé a montré les limites vis-à-vis de la sécurité informatique (Cf. les deux exemples ci-dessus). Cependant, il existe une régulation juridique de la sécurité informatique qui garantit à la Recherche sa liberté de recherche. De même, une recherche commune sur la sécurité informatique et juridique doit être mise en avant (cas de l'écrit et de la preuve électronique).

2.7. Playing with ptrace() for fun and profit (Nicolas BAREIL - EADS)

Cette présentation technique avait pour objectif de montrer les possibilités de la fonction de débogage Unix "ptrace()".

Il existe 3 modes de traçage d'un programme/processus :

- Mode pas à pas
- Par appel système
- Traçage passif

Les utilisations classiques de "ptrace()" sont l'attachement à un processus, le suivi des lectures/écritures mémoire.

Mais "ptrace()" peut permettre également

- la manipulation des signaux (processus tracé à la réception de chaque signal : SIGTRAP)
    - Il y a ici un problème de suivi des processus enfants (il faut surveiller les appels système "fork()" pour tracer les processus enfants)
- l'accès à l'espace mémoire en lecture
- l'injection de code
    - Cette injection peut être réalisée dans la pile, dans les espaces de "padding" des fichiers ELF, ou même n'importe où (on écrit sur les instructions pointées par le pointeur "eip" dans la pile du système)

Des applications pratiques d'une utilisation détournée de "ptrace" permettent de :

- Faire inter-opérer un téléphone IP "classique" avec "Skype" (traçage de la fonction de chiffrement des paquets)
    - Un processus ne peut être tracé que par un seul déboguer à la fois. Certains programmes utilisent des techniques d'auto-traçage pour empêcher tout autre traçage.
- Contourner des environnements restreints ("chroot").
- Attaquer un navigateur Mozilla
    - Faire un "connect()" dans Mozilla et détourner le descripteur de fichier vers un processus malicieux qui lit les données.

En conclusion, on peut retenir également que la fonction "ptrace()" a des fonctionnalités limitées, qu'elle est non portable, et qu'elle contient des bogues historiques. L'avenir est tourné vers l'utilisation de fonction de type "d-trace" (Solaris), qui sont des fonctions de haut niveau et scriptables.

2.8. Contournement des I(D|P)S pour les nuls (Renaud BIDOU - Radware)

Cette présentation avait pour objectif de montrer que l'exécution d'un programme d'exploitation MS03-026/RPC-DCOM (utilisé par le ver "Blaster") **connu** pouvait encore contourner les IDS/IPS ("Intrusion Prevention System") récents (SNORT avec toutes les signatures).

Cette démonstration s'appuyait sur l'utilisation des caractéristiques propres aux services RPC qui permettent de modifier le trafic réseau généré par les communications RPC :

- propriété de fragmentation RPC de niveau 7 (OSI).
- possibilité de lancer plusieurs requêtes RPC simultanément et de changer de contexte au sein des connexions.
- multiplexage de plusieurs requêtes (phase "bind" et données) dans un même paquet ("pipeline").

Les tests réalisés sur trois produits (Snort et deux autres produits anonymes) ont été effectués en utilisant

les techniques suivantes :

- Fragmentation de niveau 3 (réseau) et 4 (transport) (L3/L4).
- Fragmentation du programme d'exploitation via une fragmentation au niveau applicatif (fragmentation RPC) (utilisée conjointement avec la fragmentation de niveau inférieure L3/L4 et la technique de"pipeline"). Cette situation peut également entraîner un déni de service de l'analyseur.
- Insertion d'identifiants de contexte erronés (oblige l'analyseur à suivre les contextes).
- "Obfuscation" de code (masquage du code).

Les résultats des tests ont montré que les 3 IDS peuvent être abusés par un programme d'exploitation dont les propriétés "réseau" ont été légèrement modifiées.

En conclusion, l'auteur a voulu montrer que cette expérience n'était pas novatrice et que les IDS/IPS restent des systèmes complémentaires de la sécurité

2.9. Diode réseau et ExeFilter : 2 projets pour des interconnexions réseau hautement sécurisées (Philippe LAGADEC – DGA/CELAR)

Cette présentation avait pour objet de présenter deux projets de recherche du CELAR nommés "diode réseau" et "ExeFilter".

Le projet "**Diode réseau**" se propose d'implémenter un transfert de données de manière uni-directionel en utilisant une diode électronique qui ne laisse passer le courant électrique que dans un sens.

La "Diode réseau" est utilisée typiquement pour l'interconnexion de 2 réseaux de niveaux de sécurité différents. Le sens de transfert dans notre cas étant d'Internet vers le LAN (du "bas" vers le "haut") afin d'empêcher la fuite d'information vers l'extérieur.

Cette technique peut être utilisée pour des services de transfert (transfert de fichiers, synchronisation de répertoire, courriers, remontée d'évènements, recopie de base de données).

La solution matérielle proposée est une diode réseau matérielle afin d'avoir plus de robustesse que les gardes-barrière applicatifs et permettant de garantir la confidentialité du réseau critique. Cette diode est couplée avec des fibres optiques (plus robustes).

L'équipement "Diode CELAR" est constitué en 2 parties :

- Interconnexion physique (Fibre Optique entre 2 PC)
- Un logiciel émetteur/récepteur

La version 2 de "Diode CELAR" est écrite en Python (débit de 12 Mbits, portable sous Linux et Windows).

Le CELAR a développé un applicatif de transfert de fichiers : "blindFTP"

- Emetteur : surveille un répertoire et ses modifications, il envoie les fichiers modifiés dans des datagrammes au serveur haut.
- Récepteur : reçoit les datagrammes et reconstruit les fichiers afin de les mettre à jour.

La problématique de perte de datagrammes par le serveur haut reste à améliorer.

D'autres applications sont néanmoins possibles : recopie automatique de fichier depuis Internet (signature anti-virus, patches, …)

- Exemple avec 2 serveurs Microsoft WSUS

Une démonstration a été effectuée en séance.

En conclusion, cette nouvelle technologie ne demande qu'à être éprouvée dans des environnements opérationnels pour juger de sa pertinence. Mais le modèle reste séduisant avec une séparation de la partie "sécurité" au niveau matériel (100 à 200 euros pièce) et de la partie "service" au niveau logiciel.

Le projet "**Exefilter**" propose quant à lui un outil afin de filtrer des codes malveillants pour ne laisser passer que les formats maitrisés. Il permet entre autres la suppression des codes exécutables et autres contenus actifs (via une politique de filtrage).

Pour cela il effectue une analyse de l'extension ET du contenu à partir du principe de liste blanche (tout ce qui n'est pas autorisé est interdit).

Il peut nettoyer les fichiers HTML des scripts (JavaScript) et les fichiers Word des macros.

"Exefilter" peut être couplé avec une diode réseau pour nettoyer les fichiers envoyés vers le "haut".

C'est un outil de conception générique modulaire qui peut être intégré dans des serveurs "proxy", des scanners, ….

Le développement de ce logiciel peut être l'objet d'un partage des sources de type https://admisource.gouv.fr/

2.10. Dissection des RPC Windows (Nicolas POUVESLE - Tenable Network Security)

Le but de cette présentation technique était de faire un état de l'art sur le fonctionnement des services RPC Microsoft qui ont été la source de nombreuses failles (vers "Blaster", "Sasser", "Zotob").

Il est intéressant de retenir que l'objectif de RPC est d'offrir aux développeurs une interface de programmation qui prend complètement à sa charge toute la gestion des transferts de données entre le client et le serveur.
Les services RPC supportent plusieurs protocoles de transport : TCP, UDP, HTTP ("RPC over HTTP") et "Pipe Windows". Un service RPC est identifié par :

- un "**endpoint**" ou "point final" (ensemble de protocoles de transport)
  - Port TCP, UDP, HTTP ou "Pipe Windows"
- un **numéro de service** (UUID - "Universal Unique IDentifier")

Les failles RPC sont, dans un premier temps, des failles de programmation classiques (débordement de pile, de tas, mais aussi débordement d'entier). Il existe également des failles "conceptuelles". La plus connue est le fait qu'il était possible d'obtenir des informations sur les services RPC en utilisant une session "nulle" ("NULL sessions"). Ce problème a été corrigé dans SP2 de Windows, le SP1 de Windows 2003 et l'UR1 de Windows 2000.

Il existe également des problèmes liés à la conception même de l'architecture RPC. Par exemple, tous les services RPC sont gérés par un même processus, ce qui donne l'accès à certains "points finaux" via d'autres interfaces RPC (permet de contourner les IDS et autres politiques d'accès). Par exemple, si l'accès est impossible à un service RPC à cause d'un mécanisme d'authentification, on peut utiliser un service RPC sans authentification (ex : le service "Serveur") pour rebondir vers le service désiré.

On peut aussi noter que les services RPC de Windows sont également utilisés par des produits tiers et que ces derniers peuvent être également sensibles à des problèmes de sécurité (ex : vulnérabilité dans le logiciel de sauvegarde de Veritas permettant un accès complet à distance à la Base de Registre - **CERT-IST/AV-2005.232**).

Pour sa part, **Microsoft a effectué un audit approfondi sur la majorité des services RPC de Windows XP SP2 et Windows 2003 SP1** (suppression des fonctions à risque, diminution du nombre d'informations disponibles sans authentification, suppression des contournements d'authentification).

En conclusion, les services RPC restent incontournables (facilités de programmation). Microsoft a consenti un effort non négligeable pour leur sécurité, mais les failles RPC Windows restent toujours présentes dans les applications tierces.

2.11. Qualification et quantification des risques en vue de leur transfert : la notion de patrimoine informationnel (Jean laurent SANTONI - Marsh Risk Consulting France)

Cette présentation avait pour objectif de présenter un aperçu du problème de qualification et quantification des risques en vue de les rendre assurables.

Pour évaluer un risque, il faut définir ce qu'est "**l'information**" ?

Avant l'information dépendait du support. Par exemple à l'époque du Minitel, si on voulait arrêter la diffusion d'une information, le fournisseur (France Télécom) pouvait arrêter sur demande sa diffusion. Mais maintenant avec Internet c'est plus difficile car comment interdire une information en France émise depuis un site web à l'étranger ?

Quelle est la valeur de l'information ? Cela reste difficile à évaluer.

Il a donc été inventé la notion de **patrimoine informationnel** (environnement maitrisable, quantifiable).

C'est un modèle en plusieurs couches :

- Couche physique
- Couche transport (échange d'info)
- Couche applicative

Avant, l'assureur indemnisait les "**sauvegardes**" (assurait la perte de données). Aujourd'hui, on assure les "**flux**", mais cela ne rentre pas dans le cadre traditionnel. Il n'y a pas d'assurance de quelque chose qui est dynamique.

- Exemple des flux TV vis-à-vis des droits TV (Coupe du Monde, JO)

On doit alors se soucier de la perception de la valeur d'un flux vis-à-vis de l'utilisateur.

En conclusion, lors de la sécurisation d'un SI, il faut prendre un compte l'aspect économique/juridique des données protégées pour une meilleure adéquation. On assure les risques qui peuvent apporter préjudices au fournisseur du service ou aux utilisateurs (hélas souvent inconnus - internautes).

2.12. Les évolutions de l'implémentation des spécifications du TCG au sein de la plateforme Windows (Bernard OURGHANLIAN – Microsoft France)

Cette présentation technique avait pour but de présenter le mécanisme de protection des données dans le prochain système d'exploitation de Microsoft : **Windows Vista**.

Ce mécanisme de chiffrement de données, appelé "**Bitlocker Drive Encryption**", est principalement dédiée aux PC portables, principale source de la fuite du patrimoine informationnel de l'entreprise (vol, perte, …), ou à des PC dans des environnements agressifs. Pour cela, les besoins de Microsoft étaient de :

- Trouver un mécanisme de chiffrement qui agisse "au dessous" de Windows (afin de ne pas redévelopper les applications)
- Sécuriser les données système, les données utilisateur et la Base de Registre
- Fournir un fonctionnement transparent (utilisation aisée)

La solution proposée par Microsoft a été de chiffrer (presque) tout le disque en utilisant une puce **TPM** ("Trusted Platform Module"). Cette solution permet d'éviter le contournement du boot Windows et permet aussi une authentification à plusieurs facteurs avant l'amorçage.

Un TPM est une puce électronique effectuant des opérations de chiffrement. Elle permet de générer et de stocker des clés, d'effectuer des opérations de signature numérique, et elle détient les empreintes ("hashes") de la plate-forme. Le TPM permettra également l'authentification des logiciels (le TPM contient le "hash" des logiciels chargés et du BIOS). Le déchiffrement s'effectuera à la volée. Selon Microsoft, les opérations de chiffrement/déchiffrement à la volée seront peu perceptibles. Ainsi, la partition Windows contiendra :

- Le système d'exploitation chiffré
- Le fichier de pagination chiffré
- Les données utilisateur chiffrées

Nota : Comme cela a été mentionné par le CERTA lors du Forum annuel du Cert-IST, il est indispensable pour les entreprises d'analyser ce chiffrement avant de déployer Vista. La problématique ici est celle du recouvrement des données : comment l'entreprise pourra-t-elle récupérer les données chiffrées par Windows Vista sur un poste.

2.13. La sécurité, problème majeur pour les plateformes de diffusion multimédia sur des réseaux hétérogènes (Ahmed reda KACED - ENST Paris - & Jean-Claude MOISSINAC)

Cette présentation relativement technique a permis de faire le point sur un travail de recherche dans le domaine des plates-formes multimédia.

La problématique posée était de sécuriser des données multimédia "adaptables" (restitution des données en fonction du système final (PC, PDA) et des contraintes de l'utilisateur). Pour cela il fallait faire face au problème de l'hétérogénéité des réseaux (Internet, GPRS, 821.1) et équipements (problème de reconnaissance du format) et problème de la sécurité des échanges.

La solution présentée était basée sur l'utilisation de AMCA ("Adaptive Multimedia Content Authentication" - authentification – signature) au niveau des relais ("proxies") d'adaptation. Elle permet de modifier du flux tout en préservant l'identité de l'émetteur (structure de type "arbre de Merkle").

2.14. Sécurité des offres ADSL en France (Nicolas RUFF - EADS)

Cette présentation qui avait été annulée l'année dernière avait pour objectif de faire un état des lieux de la sécurité des boitiers ADSL proposés par les fournisseurs du marché français. Cependant, les aspects non techniques ne sont pas abordés (responsabilité FAI/constructeur/utilisateur-final) dans cet exposé.

Avec l'explosion de l'ADSL en France, de nombreux modems sont vendus sur le marché avec les offres des fournisseurs d'accès (FAI). Mais quel est le niveau de sécurité de ces équipements ?

Une étude a été effectuée sur les boitiers des principaux acteurs de l'ADSL en France. Il en ressort que les boitiers ADSL du marché sont basés principalement sur du matériel de type "tout en un" (généralement du "Broadcom" avec un processeur MIPS32). Mais ce matériel permet une analyse bas niveau via le port série ou le port de test JTAG ("Joint Test Action Group").

Les systèmes d'exploitation rencontrés sont :

- VxWorks : système très fermé, prévu plutôt pour le monde industriel, sans véritable prise en compte de la sécurité
    - N° de séquence TCP prédictible,
    - Serveur web minimaliste (mot de passe par défaut en clair dans les scripts HTML)
- Linux

Les boitiers ADSL comportent généralement plusieurs interfaces réseau :

- Interface LAN : services FTP, SSH (parfois), Telnet, HTTP, UPnP ("Universal Plug And Play")
- Interface WAN : port administration (parfois)

Plusieurs comptes utilisateur sont également présents sur le système d'exploitation des boitiers :

- Utilisateur (le nom de ce compte est souvent trivial)
- Support
- Opérateur
- Constructeur

Certains de ces comptes sont explicitement mentionnés dans la documentation constructeur, mais pas tous (comptes opérateur et constructeur).

L'authentification reste souvent faible (pas de mot de passe, mots de passe triviaux ou documentés sur Internet).

Dans certaines configurations, il est possible de lancer des commandes privilégiées (ex : "debug") et de sauvegarder ou restaurer la configuration sans pour autant posséder de privilèges particuliers.

La sécurité Wifi est très dépendante du constructeur. On y rencontre de tout :

- Aucune sécurité
- WEP
- WEP + Rotation des clés (mais cela nécessite une carte ou un pilote spécifique)
- WPA (sur les modèles récents)
- Contrôle d'accès basé sur les adresses MAC
- Contrôle matériel (bouton pour déclencher les associations) ou logiciel

L'étude s'est aussi intéressée à l'infrastructure du réseau ADSL. Les réseaux ADSL sont opérés sur des réseaux de transport de type ATM qui ont généralement des caractéristiques assez communes. De plus, les serveurs de mise à jour peuvent être un maillon faible (injection de faux "firmwares")

  - Service FTP anonyme soit via un serveur chez le FAI (mode "pull") ou sur le modem (mode "push")

Il en est de même pour les serveurs de téléphonie ou TV. Enfin, le réseau d'administration peut comporter des brèches.

En conclusion, les modems peuvent être analysés et des failles simples existent. Elles pourraient être exploitées pour installer dans ces boitiers de "nouvelles fonctionnalités" malveillantes : réseaux de "bots", écoute et redirection du trafic client, fraudes sur les offres opérateur, ou attaques de type dénis de service distribués "DDoS" vers l'opérateur. Cependant, il a été mentionné que les opérateurs corrigent petit à petit ces faiblesses.

2.15. Et si les fonctionnalités des processeurs et des cartes mères pouvaient servir à contourner les mécanismes de sécurité

des systèmes d'exploitation ? (Loïc DUFLOT & Olivier GRUMELARD - DCSSI)

Cette présentation avait pour objectif de présenter un moyen de contourner les mécanismes de sécurité en utilisant les fonctionnalités bas-niveaux des processeurs.

Le système d'exploitation est un média de communication entre l'utilisateur/application et le matériel. Le noyau du système agit donc en coupure (notion de privilèges des tâches).

Sur le système **OpenBSD**, il existe une fonctionnalité de réduction de privilèges (appelée "SecureLevel") qui permet de désactiver les privilèges inutiles après le démarrage. Cette fonction est dérivée de la capacité POSIX 1003.1e (retirée) précisant que les utilisateurs privilégiés n'ont pas besoin de l'ensemble des privilèges.

- Ex : sous Linux, privilèges d'entrées/sorties CAP_SYS_RAWIO

Dans le cadre de cette présentation, le cœur de l'architecture d'un PC se décompose comme suit :

- Des fonctionnalités au niveau de la carte mère (IRQ, DMA, …)
- Un processeur Intel x86
- Un mode d'adresses réelles
- Un mode protégé : mode nominal processeur (32bits) – protection mémoire (Privilèges processeur : Anneaux / Ring), protection des I/O
- Un mode 8086 virtuel

Cette présentation montre ainsi qu'il est possible de contourner ces mécanismes de protection sur un système OpenBSD, **via l'ouverture du serveur graphique X**.

Cette démonstration se base sur le fait qu'un utilisateur peut passer en mode "Mode System Management" sur le processeur :

- Mode de maintenance (gestion de l'alimentation, lancement de code constructeur)
- Notion d'accès mémoire via SRAM ("System Random Access Memory").

Le scénario utilisé est le suivant :

- Passer en mode "System Management" (SM) avec sauvegarde du contexte processeur
- En mode SM, on a accès à toute la mémoire et aux E/S via le mécanisme PIO
- Sortir du mode SM (restauration du contexte)

Le détournement du mécanisme se décompose alors comme suit :

- Rendre la "System Management Random Access Memory" (SMRAM) accessible en mode protégé" (D_OPEN = 1)

- Ecrire une routine de traitement de la "System Management Interrupts" (SMI) bien choisie en SMRAM
- Supprimer les accès à la SMRAM (D_OPEN = 0)
- Si nécessaire autoriser les SMI
- Déclencher une SMI (cela peut nécessite l'accès à certains ports PIO)
- Accéder en écriture à la zone des adresses basses de la mémoire vidéo

Sur le système OpenBSD, cette attaque permet à une personne ayant les privilèges du serveur X d'acquérir les privilèges noyau.

En conclusion, les auteurs ont insisté sur le fait qu'il s'agit d'un problème de fond et qu'aucune erreur d'implémentation n'est exploitée. Néanmoins, ce type d'exploitation est (pour l'instant) confiné dans un environnement bien précis (système OpenBSD, utilisateur local ayant les privilèges du serveur X).

2.16. La mobilité sous IPv6 et ses implications pour la sécurité (Arnaud EBALARD - EADS - & Guillaume VALADON - The University of Tokyo - Esaki Lab / LIP6, Paris)

Cet exposé technique avait pour but de présenter les enjeux de la sécurité vis-à-vis de la mobilité sous le protocole IPv6.

Le protocole IPv6 engendre un **changement fonctionnel** par rapport à son homologue IPv4. La communication est de bout en bout, le protocole de résolution d'adresse ARP est intégré dans le protocole ICMP, …
IPv6 engendre également un **changement structurel**. Les en-têtes ont des tailles fixes, la fragmentation s'effectue à la source, il n'y a pas de notion de "checksum".

La suite de cet exposé a présenté les mécanismes de communication d'IPv6 ainsi que les protections envisagées (IPSec pour protéger la signalisation, …).

2.17. Vulnérabilité des postes clients (Gaël DELALLEAU & Renaud FEIL - Ernst & Young)

Le but de cet exposé était de montrer que les limites de la sécurité d'un SI reposaient souvent sur la sécurité des postes clients.

Aujourd'hui, le maillon faible de la sécurité des SI reste le poste de l'utilisateur. Il est ainsi possible d'identifier à distance les logiciels utilisés sur ces postes et leur environnement, d'y faire exécuter un code malveillant connu sans être détecté par l'anti-virus, ou d'utiliser le navigateur pour rebondir sur l'Intranet du SI.

Les outils actuels protègent des attaques non ciblées (virus, spyware, ...), mais ne protègent pas des attaques ciblées.

Trois exemples type ont été présentés afin de monter ces faiblesses. Le premier concerne l'identification à distance (la prise d'empreinte, ou "Fingerprint") des logiciels client, par exemple du navigateur web utilisé par la victime. Cette méthode se base sur un script HTML présent dans une page web malveillante qui permet de récupérer des informations dans les logs du serveur web complice.

Le second exemple étudie la limite des outils de protection comme les anti-virus. Certains anti-virus utilisent des techniques "comportementales" pour identifier les codes malveillants, et exécutent le code suspect dans une machine virtuelle pour identifier son action exacte. Malheureusement, l'étude montre qu'il est facile de mettre en échec ce type d'anti-virus. Si le code malveillant mesure le temps d'exécution de certaines instructions clé, il verra tout de suite s'il est en environnement simulé (temps plus long) et pourra adopter alors un comportement inoffensif qui trompera de ce fait l'anti-virus.

Enfin, le dernier exemple s'appuie sur l'utilisation malveillante du navigateur de la victime pour accéder à des données internes (Intranet).

En conclusion, les auteurs ont voulu démontrer les dangers des postes clients dans une infrastructure maitrisée. Néanmoins, tous ces scénarios nécessitent la participation "involontaire" de la victime et ne peuvent être automatisés de bout en bout.

2.18. Mécanismes de sécurité et de coopération entre nœuds d'un réseau mobile "ad hoc" (Pietro MICHIARDI - Eurécom)

Cette présentation avait pour but d'évoquer un mécanisme de sécurité dédié aux réseaux sans fil de type "ad-hoc".

Un réseau sans-fil "ad-hoc" est un réseau maillé où chaque nœud participe au réseau.

Il existe 2 types d'environnements "ad-hoc":

- "Managed environment"
    - **Confiance a priori**

- L'authentification garantit la confiance
- Nécessité d'une infrastructure pour l'authentification (application militaire)

- "Open environment"
  - **Pas de confiance a priori**
  - L'authentification ne garantit pas le fonctionnement normal du réseau

Une attaque **passive** classique peut être initiée par un nœud qui ne coopère pas au réseau et "économise" son énergie pour sa propre communication. On parle de nœud "**égoïste**" (cas étudié).

Une attaque **active** classique reste le déni de service.

Des tests ont montré que 10 à 15% de nœuds égoïstes entraîne une dégradation de 60% du réseau.

L'idée de base contre les nœuds égoïstes est d'associer l'utilisation du réseau avec une métrique de réputation (nom du projet : **CORE**).

La réputation n'est pas utilisée comme métrique de routage, mais plutôt comme une métrique de "confiance"…

La règle de conduite étant que la réputation est difficile à construire, mais facile à perdre.

Ce modèle a été validé par une simulation et par un modèle analytique (utilisation de la théorie des jeux). La limite rencontrée vis-à-vis du modèle de base est que la topologie n'est pas prise en compte.

En conclusion, le modèle CORE ne consomme pas de l'énergie, ne surcharge le trafic existant et semble robuste contre les attaques.

2.19. Les défis du management de la sécurité (des systèmes d'information) (Sylvain RAVINET – Adenium)

Cet exposé avait pour but de présenter les défis liés aux risques auxquels est confrontée la sécurité des SI.

Commentaire [b1] : Je trouve l'expression bizarre…

Les risques de la SSI sont de deux types :

- risques accidentels (dangers)
- menaces (malveillance)
  - Ex : arrêt de la climatisation dans les salles informatiques !

Les moyens vulnérables identifiés dans un système d'information sont le personnel de l'entreprise,

l'organisation, le matériel/bâtiment.

Les conséquences d'une attaque ou d'un incident sont de l'ordre de l'atteinte à la **disponibilité**, l'**intégrité** et la **confidentialité**.

Aujourd'hui, on assiste à une nouvelle vision de l'informatique vis-à-vis de la productivité de l'entreprise.
La sécurité tend à s'associer à une notion de **résilience** : capacité de robustesse au "choc" et de retour à la "normale", mais le retour n'est pas forcement vers la "normale" (car le modèle est amené à changer suite au renforcement des moyens de protection).

Il faut faire face aussi aux différentes entités agissant autour de la SSI qui sont de différentes cultures et origines :

- Niveau international (lois européennes)
- Niveau national (DCSSI)
- Niveau entreprise (DSSI)
- Niveau équipe d'exploitation

Il existe des outils, mais qui restent pour l'auteur insuffisants pour évaluer les risques.

Il faut cartographier les risques en fonction de leur probabilité de survenance et leur impact

Il faut choisir une organisation qui prévoie l'**avant**, le **pendant**, l'**après**.

2.20. Détection de tunnels en périphérie du réseau (Guillaume LEHEMBRE & Alain THIVILLON - HSC)

Cet exposé avait pour objectif de présenter la problématique des tunnels au sein d'un SI.

Un tunnel permet de contourner la politique de sécurité pour accéder à des protocoles et ressources non autorisés.

Généralement, ces tunnels se basent sur l'utilisation des protocoles standards **HTTP, HTTPS, ICMP, DNS**.
Il est à noter que les tunnels sont parfois utilisés à des fins légitimes.

Exemple de tunnels : le tunnel HTTP

Un tunnel HTTP/HTTPS peut utiliser la méthode CONNECT sur un relais applicatif (Cf. article du *Bulletin Sécurité n°53 du Cert-IST* – "Le danger des serveurs de relayage dédiés au trafic web").

Il peut aussi utiliser des requêtes HTTP classiques de type GET ou POST sur des CGI ou des URL.

Voici une liste de quelques outils dédiés aux tunnels HTTP :

- HTTP : GNU HTTPTunnel, LoopHole, FirePass
- HTTPS : OpenVPN, Stunnel, SSL Tunnel
- Il existe des tunnels HTTP commerciaux (Hopster, ..) pour l'accès aux services IM, P2P, IRC

Exemple de tunnels : le tunnel ICMP

Les données échangées entre les deux bouts du tunnel sont stockées dans la charge utile du paquet ICMP.

Voici une liste de quelques outils dédiés aux tunnels ICMP :

- Loki
- PingTunnel
- Skeeve

La détection de ce type de tunnel peut être déclenchée par l'observation d'un nombre anormalement élevé de paquets ICMP.

Exemple de tunnels : le tunnel DNS

Les données échangées entre les deux bouts du tunnel sont stockées dans les champs A, TXT, KEY.

Une parade à ce type de tunnel est d'utiliser des serveurs DNS internes et de filtrer les trafics DNS illégitimes.

Voici une liste de quelques outils dédiés aux tunnels DNS :

- NSTX
- Oxyman
- DNS2TCP

Il existe aujourd'hui plusieurs méthodes afin de détecter des tunnels.

La première d'entre elles est **l'examen des journaux** : User-Agent inconnu, volume de données suspect, écart-type entre les requêtes (journaux Bind). Cependant, elle ne permet pas une analyse protocolaire, ne donne pas la durée des connexions TCP et ne fournit que des informations partielles.

Une autre solution est la **détection à la volée** par l'analyse du trafic HTTP : méthode inconnue, en-têtes

HTTP incorrects (absence de champ Host), User-Agent inconnu (assez efficace), réponse du serveur incorrecte (ex : version HTTP).

L'examen du trafic HTTPS (trafic chiffré) reste un élément à part, mais peut être basé sur l'analyse de :

- L'utilisation de la méthode CONNECT avec des destinations numériques/adresses IP (normalement les noms de machines dans ce type de trafic sont FQDN) ou sur un port inhabituel
- L'absence de champ Host dans la méthode CONNECT
- La génération de trafic non SSL sur le port 443
- La présence de certificats numériques suspects

Enfin, la troisième méthode est la **détection statistique**. Elle se base sur la durée de connexion (en moyenne, une connexion ne dure pas plus de 10 minutes), la répartition des échanges vis-à-vis des protocoles asymétriques classiques comme HTTP/HTTPS/SMPT/POP (ratio UPLOAD/DOWNLOAD ou inverse < 0.3), la taille moyenne des paquets (une vraie connexion "bourre" les paquets), la forme temporelle (surveillance du mode protocolaire).

Les auteurs ont ensuite présenté leur outil "**MolTunnel**" s'exécutant sous Unix et permettant de détecter des tunnels. Cet outil n'a pas de prétention d'exhaustivité (tentative de généricité par rapport aux signatures des IDS) et est probablement contournable. Il se base sur une détection au fil de l'eau.

Cependant il reste sujet à quelques problèmes liés au manque de fiabilité de la librairie LIBNIDS (s'il y a une perte de paquets alors l'analyse ne se fait pas), à la difficulté engendrée par l'écriture d'un analyseur de protocole HTTP complet (mod_gzip, transferts chuncked, …) et par la difficulté à détecter certains tunnels.

En conclusion, cet outil peut évoluer (réseau de neurones ? transformées de Fourier ? couplage avec un IDS qui analyse les protocoles). Il reste aussi le problème de la capacité de traitement par rapport au volume de données. Il ne faut pas oublier que des vendeurs de gardes-barrière proposent eux-aussi leurs propres tunnels (VPN SSL)… et qu'avec la version Web 2.0, peut-être que toutes les métriques utilisées pour l'analyse statistiques seront remises en cause…

2.21. SSI : quelles responsabilités ? (Marie BAREL – Links conseil)

Cet exposé avait pour objectif de présenter les responsabilités liées à la profession de RSSI.

La profession de la SSI est aujourd'hui dans la tourmente (nouvelles lois, contraintes et nouvelles sources de responsabilité, nouveaux risques faisant appel à des compétences plus larges, responsabilité plus large : civile, pénale, personnelle ou du fait d'autrui, …).

Pour illustrer ce fait, l'auteur propose une analyse de cas basée sur :

Responsabilité du fait d'un préjudice causé à un tiers au travers du système d'information

- Défaillance de la sécurité du système causant une perte de données à caractère personnel

Les données sensibles se doivent d'être protégées par la loi (affaire Kitetoa)

- Attaque par rebond : un serveur de messagerie utilisé comme relais pour envoyer un virus

Responsabilité pénale et intention délictueuse, responsabilité civile en vue de la réparation du dommage ; faute non intentionnelle.

Responsabilité engagée du fait des agissements d'un salarié

- Agissement d'un salarié à l'insu de l'employeur

L'employeur est responsable civilement d'où l'importance de la qualité des chartes d'usage des ressources informatique.

Responsabilité engagée du fait des mesures de cyber-surveillance opérées sur le réseau d'entreprise

Exemple de la cyber-surveillance (ex: contrôle de la messagerie) ou du "nettoyage" (si découverte de photos érotiques dans un bureau, on recherche sur le PC de l'utilisateur d'autres documents à caractère tendancieux).

Cette pratique est interdite à moins qu'un **risque ou un évènement particulier** ne soit prouvé.

Mais comment qualifier ce risque ?

Responsabilité engagée du fait d'un défaut de suivi de la réglementation

Cette responsabilité peut se matérialiser par les dispositions relatives à la collecte, la conservation des traces.

En conclusion, l'auteur se veut néanmoins rassurant en proposant une méthode permettant de faire face à ces responsabilités. Cette méthode passe par la mise en place d'une "**Politique de Gestion des Risques Juridiques**" (PGRJ) passant par :

- un tableau de bord des risques juridiques,
- une charte,
- une veille régulière,
- une formation et sensibilisation des collaborateurs.

2.22. Evaluation du coût de la sécurisation du système DNS (Daniel MIGAULT - FT - & Bogdan MARINOIU)

Cet exposé avait pour objectif de présenter le cout en termes d'utilisation de ressource de la sécurisation d'un système DNS.

Le système DNS est un système de nommage qui est la cible d'attaques courantes telles que les dénis de service (DoS), le "Poisonning", le "Spoofing", le "Phishin/Pharming", le "Tracing" et les attaques de type MiM ("Man-in-the-Middle")

Les solutions de sécurité pour faire face à ces problèmes sont l'utilisation d'**IPSec** (sécurise le transport) ou **DNSSEC** (sécurise les données).

DNSSEC sécurise à 2 niveaux. Il sécurise les enregistrements avec une signature (en local) et établit une chaine de confiance entre différents serveurs avec une clé d'identification et un mécanisme de délégation (niveau global).

L'auteur se propose de faire un comparatif des performances entre DNSSEC et DNS+IPSec en termes de charge machine, trafic réseau, temps de mise à jour…

En conclusion, il n'existe pas de solution miracle. Le couple DNS+IPSec obtient des temps de réponse plus faibles et une capacité de traitement des requêtes par la plate-forme plus courte, mais DNSSEC a une capacité de traitement de requêtes par le serveur de nom plus courte.

2.23. Corruption de la mémoire lors de l'exploitation (Samuel DRALET & Francois GASPARD - étudiant)

Cet exposé avait pour objectif de présenter des moyens d'exploiter une vulnérabilité tout en restant "caché" en mémoire, sans écrire quoi que ce soit sur le disque dur.

Des chercheurs se sont alors penchés sur ce problème et ont essayé de mettre au point des mécanismes de furtivité utilisés lors de l'exploitation d'une vulnérabilité réseau. Ces mécanismes sont assez éloignés des techniques implémentées par les "rootkits" traditionnels, car ils tendent à simuler le comportement de certains éléments du système d'exploitation en se mettant en coupure entre le code "malveillant" et le système (ces mécanismes étant bien entendu embarqués dans le programme d'exploitation).

La première solution de furtivité a été appelée "Syscall Proxy". C'est une solution de type client/serveur qui simule les appels système sur une machine distante :

- Serveur : "shellcode" lancé lors de l'exploitation (machine compromise)
- Client : librairie d'appel système (machine du pirate)

Cependant, cette technique engendre beaucoup trop de communications réseaux et nécessite de ré-implémenter tous les appels système.

L'autre solution, nommée "Userland excve", permet de simuler le comportement de l'appel système "execve" pour exécuter un binaire en mémoire. Cependant, cette méthode a de nombreuses limitations (il faut éviter le "swap" sur le disque dur, le programme binaire doit être "petit", un binaire dynamique n'est pas conseillé).

En conclusion, les auteurs ont voulu montrer que l'audit de la mémoire vive est aussi important qu'une analyse disque.

2.24. RFID et sécurité font-elles bon ménage ? (Gildas AVOINE – MIT - USA)

Cet exposé avait pour objectif de présenter la sécurité du système RFID ("Radio Frequency IDentification").

RFID est une technologie basée sur une puce ("Tag") passive qui se sert de l'énergie du lecteur RFID pour envoyer ses informations. Les applications RFID devenant de plus en plus variées (identification : traçabilité pour remplacer les codes barre, passeport, etc, ou authentification : badge d'accès, clé de démarrage voiture, ...), l'évaluation du niveau de sécurité sous-jacent est rapidement devenu un impératif. Il en ressort que cette technologie est soumise aux risques classiques en matière de sécurité informatique :

- **Déni de service** : il est difficile de se protéger contre ce type d'attaque. Il faut s'adapter !
- **Fuite d'information** : cette faiblesse est due à la facilité du "tag" à répondre sans l'accord de son "porteur" (problème des passeports, des cargaisons de camion de marchandises). Une solution est alors d'éviter de stocker des informations sensibles sur les "tags".
- **Usurpation d'identité** : il faut utiliser un protocole de chiffrement (cryptographie symétrique) afin que le "tag" envoie la réponse chiffrée.
- **Traçabilité malveillante** : il faut empêcher qu'une relation entre les "tags" et le "lecteur" ne soit découverte (ex : empêcher de déduire que les "tags" RFID représentent des "agents secrets") car les tags ne peuvent pas être éteints et répondent sans l'accord de l'utilisateur. La solution du chiffrement des communications est encore proposée afin que le "tag" renvoie une valeur indistinguable d'une valeur aléatoire. Cependant le corolaire de cette solution est que le lecteur doit utiliser toutes les clés (algorithme symétrique) car il ne connaît pas qui est derrière l'information.

Un autre type de malveillance liée à la technologie RFID est d'effectuer des attaques par relais dans

lesquelles l'adversaire intercepte et renvoie le trafic RFID. Une des solutions préconisées contre ce type de technique serait de calculer le temps de réponse du "tag".

Une petite vidéo très pédagogique a permis de montrer qu'il était tout à fait possible de contourner la protection RFID (authentification) de la procédure de démarrage de certaines voitures américaines.

Des informations sur les aspects RFID sont proposées sur le site de l'auteur à l'adresse suivante : http://www.avoine.net/

2.25. Détection d'intrusion dans les réseaux 802.11 (Laurent BUTTI - FT)

Cet exposé avait pour objectif de présenter un détecteur d'intrusion pour les réseaux sans-fil développé par le laboratoire de recherche de France Telecom.

Les réseaux sans-fil s'étant de plus en plus démocratisés dans les entreprises, de nombreuses recherches ont été lancées concernant la sécurité des réseaux Wifi et notamment sur la mise au point de détecteur d'intrusions (IDS) dédiés à cette technologie. Le laboratoire Recherche & Développement de France Telecom a présenté l'état des lieux de son projet d'IDS Wifi. Le but de cet IDS est de pouvoir détecter en priorité les attaques par déni de service, les injections de trafic, l'usurpation d'adresse MAC, les faux ("rogue") points d'accès (AP) et les AP illégitimes interconnectés au site protégé.

Les caractéristiques techniques de cet IDS sont les suivantes :

- Moteur de détection écrit en langage C et embarqué sur un point d'accès de type Linksys WRT54G (avec "OpenWRT"),
- Langage de règle/signature ou de comportement (flexibilité),
- Interface de journalisation de type "syslog",
- Moteur d'agrégation et corrélation à la volée (basé sur SEC "Simple Event Correlator" - http://www.estpak.ee/~risto/sec/).

En conclusion, les résultats constatés ont permis de détecter des actions malveillantes de type "WarDriving", "Injection WEP", ….

La détection de l'usurpation d'adresse MAC reste cependant problématique car l'usurpation d'adresse MAC est facile à effectuer, mais difficile à détecter. Cependant des techniques existent pour tenter de faire face à ce problème (par le calcul de la volumétrie des trames, mais cela nécessite une forte corrélation). Un autre élément, qui est la programmation de plus en plus laxiste des "chipset" et pilotes ("drivers") 802.11, tend à

rendre les détections plus problématiques

2.26. Faiblesses d'IPSec en déploiements réels (Yvan VANHULLEBUS (NETASQ)

Cet exposé avait pour objectif de présenter les faiblesses des implémentations et configurations du protocole de sécurité IPSEC.

L'auteur a proposé un bref aperçu d'IPSEC où on peut retenir que :

- le mécanisme ESP chiffre les données
- le mécanisme AH permet de faire un "hash" uniquement (en-tête IP)
- le protocole IKE permet l'échange des clés et la constitution du "tunnel" IPSec

Les implémentations IPSec font face à de nombreuses menaces qui sont :

- Déni de service : bloquer les négociations /bloquer le trafic
- Corruption : modifications aléatoires, modifications contrôlées
- Interception des données
- Accès non autorisé

Il existe 2 types de faiblesses : les faiblesses protocolaires et les faiblesses d'implémentation

Faiblesses protocolaires :

Une faiblesse bien connue est la faiblesse du **mode "agressif" combiné avec un secret pré-partagé** : l'attaquant se met en coupure pour récupérer les informations afin de retrouver la clé pré-partagée. Afin de mener à bien cette attaque, le pirate interroge directement une extrémité. Pour cela il faut une proposition valide (DES/MD5, ….), une durée de vie valide et un identifiant valide.

Une autre faiblesse est contenue dans la **génération des clés de session** (elles sont dérivées les unes des autres) si une clé est cassée on peut trouver la suivante facilement. Pour pallier ce problème, il est nécessaire d'utiliser le mode "PFS" (régénération de clé indépendante).

L'authentification faible de type **Xauth** souffre aussi de la présence d'algorithme faible.

Enfin, dans le **mécanisme ESP**, il est potentiellement possible de **permuter des bits** (l'algorithme CBC permet la permutation de certains bits). Mais cela reste très difficile à exploiter en pratique et peut être corrigé par l'utilisation d'empreinte ("hash").

Faiblesses d'implémentation :

Il existe encore des clés uniques et non renouvelées dans certaines implémentations du fait, entre autres, que le protocole d'échange des clés IKE reste assez complexe à implémenter.

Le test PROTOS de l'université d'Oulu en Finlande a permis de montrer que de nombreux équipements IPSec étaient sensibles à des dénis de service (avis **CERT-IST/AV-2005.442**).

Une vulnérabilité dans un serveur VPN de Cisco permet un accès non autorisé sur l'équipement (**CERT-IST/AV-2005.130**).

Une vulnérabilité dans le garde-barrière FW-1 de Checkpoint permet d'exécuter du code sur l'équipement (**CERT-IST/AV-2004.140**).

Ensuite, viennent des problèmes de choix cryptographique (utilisation d'algorithme de chiffrement trop faible), puis des problèmes d'utilisation avec des configurations trop permissives (configuration de type "obey"), ou une gestion de la PKI un peu hasardeuse, …

En conclusion, l'auteur met l'accent sur le fait qu'une bonne prise en compte des problèmes de sécurité liés à IPSec passe avant tout par une bonne communication des différents acteurs.

2.27. Rump Sessions

Des sessions "sauvages" ont été aussi proposées en fin de journée le 1er juin. Ces sessions de courtes durées et dont les intervenants volontaires n'étaient pas programmés à l'avance ont abordé des sujets d'actualité tournant autour du thème de la sécurité.

On retiendra de ces sessions, quelques sessions intéressantes :

- Organisation les 28-30 novembre 2006 à Supelec (Rennes) : Sécurité et convergence voix-données : www.rennes.supelec.fr/JSSI
- Photorec
  - Outil de récupération de fichier endommagé : www.cgsecurity.org
- Risque viral sous OpenOffice (utilisé par la gendarmerie)
  - D'après des recherches faites sur la robustesse de la suite bureautique "OpenOffice" (utilisée, entre autres, par la gendarmerie) vis-à-vis des virus, il en ressort que le risque viral est plus élevé que sous la suite bureautique de Microsoft. En effet, "OpenOffice" supporte de nombreux langages de script évolués (scripts shell, VBScript, …) et ne

propose pas de mécanisme de sécurité vis-à-vis des macros. Ainsi, un vieux virus macro sous Microsoft Office peut être utilisable sous "OpenOffice".

- Détection des attaques par collision en Wifi
  - Ajout d'un flag ("Coll"/"No Coll)" dans l'en-tête du paquet sensible
- ASLR – Windows Vista : cas de contournement de protection
  - ASLR - "Address Space Layer Randomization" permet le chargement des processus, DLLs, pile et tas à des adresses arbitraires afin d'accroître la protection contre les débordements de pile. Cependant ce mécanisme souffre d'une mauvaise "randomization" (1/256)

    La "Randomization" s'effectue au reboot, mais il n'existe que 1/256 possibilités pour l'exploiter
- USBDumper
  - Aujourd'hui, les clés USB ont supplanté les disquettes et les autres supports de sauvegarde amovibles. Leur utilisation intuitive leur offre un grand succès. La contrepartie à cette popularité est qu'on accorde une confiance quasi-illimitée à ce support et qu'on n'hésite pas à utiliser cette clé sur n'importe quel ordinateur. Il a ainsi été proposé dans cette présentation un petit logiciel qui permet de copier sur le disque dur local, à l'insu du propriétaire de la clé UBS, toutes les données de cette clé lorsque cette dernière était enfichée sur le système. Il est à noter que ce programme "malveillant" aurait pu aussi introduire sur cette même clé un fichier vérolé, supprimer tous les fichiers, …. Ce type de démonstration permet de prendre conscience qu'une clé USB reste un équipement qu'il faut manipuler avec précautions et qu'il ne faut pas utiliser dans des environnements à risque.

3. CONCLUSION

Cette conférence d'un niveau technique élevé devient au fil des années une manifestation incontournable pour les acteurs de la sécurité en France. Les sujets abordés permettent de montrer l'état de l'art dans divers domaines de la sécurité. Cependant les solutions aux problématiques abordées restent pour l'instant au stade expérimental. Le Cert-IST se doit de participer à de telles manifestations pour avoir une meilleure visibilité de l'évolution des menaces et des avancées technologiques liées à l'utilisation de l'informatique.