

Sécurité et services publics

Intérêts et mise en oeuvre des logiciels libres

Séminaire E-Administration

19 Septembre 2002

Hervé Schauer

[<Herve.Schauer@hsc.fr>](mailto:Herve.Schauer@hsc.fr)

Hervé Schauer Consultants

[<http://www.hsc.fr/>](http://www.hsc.fr/)



- Hervé Schauer Consultants
 - Domaines de compétence
 - Type de prestations

- Sécurité du périmètre
- Sécurité e-administration
- Sécurité des serveurs web
- Sécurité dans son réseau
- Sécurité du poste de travail
 - TCPA et Palladium

Sécurité et services publics - Agenda

- La sécurité est une compétence dédiée et spécifique
- La sécurité est une expertise
- Sécurité et logiciels libres
- Exemples de logiciels libres pour la sécurité
- Conclusion
- Annexes
 - Ressources

- Cabinet de consultants en sécurité Unix, Windows, TCP/IP et Internet depuis 1989
- 13 consultants

- Expérience de la sécurité Unix depuis 1987
- Expérience de la sécurité Internet depuis 1991
- Expérience de la sécurité Windows depuis 1997

- Veille en vulnérabilités
 - vendue depuis Juin 1997
- Veille technologique et stratégique de l'actualité en sécurité
 - vendue depuis Janvier 2000
 - 6 à 8 conférences internationales par an
 - Blackhat, CanSecWest, Defcon, Eurosec, IETF, ISSE, RSA, SANS, Usenix...

HSC : Domaines de compétence

- **Sécurité réseaux IP**
 - IPsec, SSL, dénis de service, filtrage, IPv6, VLAN, 802.11, GPRS
 - HTTP, SQLnet, net8, Tuxedo, Encina, Corba, SSH, CIFS/SMB...
 - Infrastructure, infogérance, PKI, journalisation, SOC, anti-virus
 - Architecture, haute-disponibilité, routage, cloisonnement
- **Sécurité des systèmes d'exploitation**
 - Windows (NT, 2000, XP, .Net), Unix/Linux, OpenVMS, IOS, PalmOS...
- **Sécurité des applications**
 - Apache, Microsoft, Netscape, Lotus...
 - Broadvision, JAVA, Oracle Portal, PHP, Weblogic, Webmethods, Websphere...
 - Signature X.509, XML, WebSSO, interconnexions SAP...
- **Programmes consultants et bonnes relations avec les fournisseurs en toute indépendance**
 - 6Wind, Arkoon, Axiliance, Cisco, Checkpoint, Deny-All, Evidian, ISS, Microsoft, Netasq, Nokia, Nortel, Solsoft...
- **Plus de 30 produits de sécurité maîtrisés**

HSC : Types de prestations

- Études
 - Conception, architecture, assistance à maîtrise d'ouvrage, produits...
- Installations
 - Mise en place, sécurisation de l'existant
- Investigations et enquêtes après incident
- Analyses, audits et tests d'intrusion
 - Tests de vulnérabilités semi-automatiques récurrents : TSAR
- Formations
 - Sécurité Unix, Linux, Solaris, Windows
 - Sécurité réseaux TCP/IP, Internet/intranet, serveurs web
 - Détection d'intrusion, programmation sécurisée
 - Cryptographie, IPsec, PKI, DNS, Postfix, Firewall-1
- Tutoriels
 - Infosec, Le Salon de la Sécurité, Netsec, Web-Business...

Sécurité sur le périmètre (1/2)

- Sécurité entre
 - L'espace sous ma responsabilité
 - Le reste du monde
 - Accès Internet, accès distants, accès extranet, ...
- Fonctions du système de sécurité Internet
 - Filtrage IP
 - Limite les flux : HTTP, HTTPS, SMTP, DNS
 - Limite les adresses IP sources et destination
 - Journalise les tentatives infructueuses et le trafic
 - Analyse de contenu et anti-virus
 - Dans tous les flux : SMTP, HTTP, ...
 - Dans HTTP : messagerie via les courrielwebs (*webmails*), XML, SOAP, SAML, WSDL...
 - Authentification
 - Distinguer utilisateurs, applications, et ordinateurs
 - Journalisation

Sécurité sur le périmètre (2/2)

- Composants du système de sécurité Internet
 - Firewall-routeur-commutateur
 - Boîtier ou serveur de relayage applicatif
 - Services nécessaires à l'Internet
 - Exemple : DNS
- Architecture sécurisée et évolutive
- Exploitation et gestion
- Le niveau de sécurité dépend des moyens humains
 - Exploitation par des administrateurs dédiés et compétents
 - Equipe par plate-forme : réseau, serveurs et applications

- Sécurité e-administration ➤ Sécurité du commerce électronique
 - Besoins de sécurité similaires
 - Techniques de sécurité identiques
- Conception et développement des applications intégrant la sécurité dès le départ
- Architectures réseaux et applicatives en strates (*tiers*)
- Serveurs avec des systèmes d'exploitation et des serveurs web appropriés
- Gestion et supervision par des équipes compétentes

Sécurité des serveurs web (1/2)

- Firewall
 - Limite les flux aux ports 80 (HTTP) & 443 (HTTPS) sur TCP vers les serveurs web
- Relais HTTP en entrée
 - Analyse et contrôle le flux HTTP en amont du serveur web
 - Palliatif aux serveurs web et applicatifs mal conçus ou mal écrits ou utilisant des composants inappropriés
- Serveur web, exemples de risques :
 - Mauvaise interprétation des URL
 - Remontée dans l'arborescence
 - Accès aux scripts CGI
 - Prise de contrôle du serveur web et défiguration
 - Prise de contrôle du serveur au niveau système d'exploitation

Sécurité des serveurs web (2/2)

- Serveur applicatif, exemples de risques :
 - Vol de session
 - Mauvaise conception du *cookie* de session
 - Manque de contrôle des paramètres issus de l'utilisateur et de l'extérieur
 - Insertion de code HTML, de code exécutable, ou XSS
 - Falsification des paramètres numériques
 - Injection de code SQL
- Base de données, exemple de risques :
 - Manque de contrôle spécifique des paramètres issus de l'utilisateur
 - Prise de contrôle du serveur de base de donnée
 - Fonctionnement par défaut avec les privilèges maximum
 - Possibilité d'exécuter des commandes ou lire des données système
- SSL/TLS (HTTPS) ne protège **en rien** des **intrusions**

- Sécurité de son réseau interne
 - Maîtrise des communications avec l'extérieur
 - Modems, ADSL, téléphones sans-fil...
 - Cloisonnement des métiers
 - VLAN, filtrage IP, authentification et journalisation des utilisateurs
 - Construction de zones de partages dédiées pour partager des services entre administrations
- Sécurité des réseaux sans fil
 - Contournement du système de sécurité sur le périmètre
 - Note publique DCSSI du 8 Août 2002
www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002/
 - Sécurité et mobilité
 - Assistants personnels

Sécurité du poste de travail

- Les utilisateurs ont des postes de travail
 - Même si l'utilité du CPU et du stockage associé à chacun n'est généralement pas démontrée
 - Firewall personnel + anti-virus
- Le poste de travail n'est pas toujours contrôlé par celui qui l'a acheté et déployé
 - Informations renvoyées par l'utilisateur
 - Informations renvoyées à l'insu de l'utilisateur
 - Renvoi à l'installation de tout ce qu'a déclaré l'utilisateur chez le vendeur
 - Communication par les logiciels avec leur éditeurs à l'insu de l'utilisateur
 - Déclaration de toutes les licences de logiciels à Microsoft
 - Refus d'utilisation d'un réseau local sans accès à l'Internet pour cette déclaration
 - Nouvelle licences indiquant que le système d'exploitation est autorisé à envoyer des informations chez Microsoft

TCPA et Palladium

Présentés lors de la conférence Usenix Security en Juillet 2002

- TCPA (Trusted Computing Platform Alliance)
 - Initiative dirigée par Intel, avec Microsoft, Compaq, HP, et IBM
 - Ensemble de fonctions de contrôle intégrées dans les cartes mères puis dans tous les processeurs des PC
- Palladium
 - Initiative de Microsoft
 - Bâti sur le matériel TCPA
 - Système de contrôle obligatoire (*mandatory*) intégré dans Windows
 - Utilise l'accès au réseau et à l'Internet pour effectuer ses contrôles
 - Au minimum pour se connecter chez Microsoft

Sécurité : une compétence dédiée et spécifique

- Une compétence sécurité doit avoir une vision globale des choses
 - Elle doit s'adapter
 - Comprendre des éléments télécoms, réseau, système, les contraintes opérationnelles et d'exploitation
 - Apprécier la conception d'applications Windows, Java, PHP, objet, etc
 - Connaître le fonctionnement des CRM, ERP, etc
- Une compétence sécurité n'a généralement pas la compétence en
 - Qualité de service
 - Performance
 - Gestion et supervision
 - ...

Sécurité : une expertise

- Collaboration de l'intégrateur avec l'expert sécurité
 - Etudes
 - Conception d'architecture sécurisées
 - Intégration de la sécurité dans les développements
 - Installation sécurisée
- Expert sécurité indépendant de l'intégrateur
 - Assistance à maîtrise d'ouvrage
 - Audit de sécurité
 - Test d'intrusion
- Adapter sa demande à son besoin

Sécurité : comment en profiter

- Privilégier des appels d'offre adaptés
 - Séparer le contrôle de sécurité de la réalisation
 - Fixer des objectifs clairs en gardant à l'esprit ses objectifs métier
 - Supprimer le besoin de la sous-traitance
 - Impossibilité juridiques de cascades de responsabilités
 - Impossibilité d'assurance
 - Complexité
 - Proposer des montants maximum en adéquation avec les prestations demandées
- Formaliser le livrable attendu

- La liberté de savoir comment ça marche
- La liberté d'adapter et de corriger
- La liberté du développement sans contrainte
- La liberté de ses fournisseurs de service
- La liberté pour le citoyen

Logiciels libres pour la sécurité (1/3)

- Toujours vérifier l'authenticité des logiciels téléchargés

- Filtrage IP

- NetFilter (Linux)
- IP-Filter (BSD, Solaris, HP-UX)
- Packet Filter (OpenBSD)

www.netfilter.org

coombs.anu.edu.au/~avalon/

www.benzedrine.cx/pf.html

- Relayage HTTP en sortie

- Squid

www.squid-cache.org

- Relayage HTTP en entrée

- Apache

www.apache.org

- Tests de vulnérabilités

- Nessus

www.nessus.org

Logiciels libres pour la sécurité (2/3)

- Journalisation

- Modular Syslog
- NewSyslog
- Syslog NG
- Cacti
- HotSaNIC
- IPFC
- Logchecker
- Logsurf
- MRTG
- RRDTool
- Swatch

sourceforge.net/projects/msyslog/

www.weird.com/~woods/projects/newsyslog.html

www.balabit.hu/en/downloads/syslog-ng/

www.raxnet.net/products/cacti/

www.bernisys.prima.de/linux/hotsanic/

www.conostix.com/ipfc/

www.psionic.com/abacus/logcheck/

www.cert.dfn.de/eng/logsurf/

people.ee.ethz.ch/~oetiker/webtools/mrtg

people.ee.ethz.ch/~oetiker/webtools/rrdtool/

www.oit.ucsb.edu/~eta/swatch/

- Détection d'intrusion

- Prelude

www.prelude-ids.org

- Snort

www.snort.org

- Contrôle d'intégrité

- AIDE

www.cs.tut.fi/~rammer/aide.html

- Infrastructures de gestion de clés

- IDX-PKI

idx-pki.idealx.org

- Serveurs d'authentification

- Chiffrement

- Messagerie

- Serveurs web

- ...

- La sécurité est une clef de la réussite des projets
- La sécurité s'intègre dès le départ
- L'expertise en sécurité est une demande spécifique
- Le logiciel libre apporte de la sécurité
 - Indépendance et autonomie
 - Neutralité et concurrence

Questions / Réponses

www.hsc.fr

- Environ 150 présentations disponibles sur www.hsc.fr

- EFF

www.eff.org

- TCPA

www.trustedcomputing.org

- Palladium

- Il n'y a pas encore de page "Palladium" sur le web de Microsoft, mais le sujet est explicité aux URL suivantes :

www.microsoft.com/presspass/features/2002/jul02/0724palladiumwp.asp

www.microsoft.com/presspass/features/2002/jul02/07-01palladium.asp

- Give Software Users a Sincere Choice!

- Bruce Perens

www.sincerechoice.org

- Denis Ducamp, Nicolas Jombart et Jean-Baptiste Marchand pour leur relecture