Sécurité de Mac OS X

Matthieu Herrb

Novembre 2004

2004-11-03 : OpenSSH SCP Client File Corruption Vulnerability
2004-11-03 : OpenSSL Denial of Service Vulnerabilities
2004-11-01 : Apple Safari Web Browser TABLE Status Bar URI Obfuscation Weakness
2004-11-01 : RSync Configured Module Path Escaping Vulnerability
2004-10-27 : Apple QuickTime Remote Integer Overflow Vulnerability
2004-10-27 : Apple Remote Desktop Administrator Privilege Escalation Vulnerability
2004-10-27 : Apple Mac OS X Multiple Security Vulnerabilities
2004-10-27 : OpenSSL ASN.1 Parsing Vulnerabilities
2004-10-27 : OpenSSL Bad Version Oracle Side Channel Attack Vulnerability
2004-10-27 : OpenSSL CBC Error Information Leakage Weakness
2004-10-27 : Mozilla Cross-Domain Frame Loading Vulnerability
2004-10-27 : LibPNG Graphics Library Multiple Remote Vulnerabilities
2004-10-22 : CUPS Error_Log Local Password Disclosure Vulnerability
2004-10-20 : Apple Safari Cross-Domain Dialog Box Spoofing Vulnerability
2004-10-18 : TNFTPD Multiple Signal Handler Remote Superuser Compromise Vulnerabilities
2004-10-16 : Apache Mod_SSL SSL_Util_UUEncode_Binary Stack Buffer Overflow Vulnerability
2004-10-14 : CUPS UDP Packet Remote Denial Of Service Vulnerability
2004-10-06 : Apple Mac OS X ServerAdmin Default SSL Certificate Vulnerability
2004-10-06 : Apple Mac OS X Postfix Release SMTPD AUTH Username Denial Of Service Vulnerability
2004-10-05 : Multiple Vendor Telnetd Buffer Overflow Vulnerability
2004-10-04 : Libxml2 Remote URI Parsing Buffer Overrun Vulnerability
2004-10-02 : SquirrelMail Unspecified SQL Injection Vulnerability
2004-10-01 : MIT Kerberos 5 KRB5_AName_To_Localname Multiple Principal Name Buffer Overrun Vulnerabilities
2004-09-29 TCPDump ISAKMP Identification Payload Integer Underflow Vulnerability
2004-09-23 Apache ap_escape_html Memory Allocation Denial Of Service Vulnerability
2004-09-23 Apache Connection Blocking Denial Of Service Vulnerability
2004-09-23 Apache Error Log Escape Sequence Injection Vulnerability
2004-09-17 Apple iChat Remote Link Application Execution Vulnerability
2004-09-14 Apple Safari Cross-Domain Frame Loading Vulnerability
2004-09-07 OpenLDAP Ambiguous Password Attribute Weakness
2004-09-07 Apple QuickTime Streaming Server Deadlock Denial of Service Vulnerability
2004-09-07 Apple PPPDialer Insecure Log File Creation Symbolic Link Vulnerability
2004-09-07 Apple CoreFoundation Unspecified Environment Variable Buffer Overflow Vulnerability
2004-09-07 Apple CoreFoundation Privileged Plug-In Execution Vulnerability
2004-09-07 Apple Safari Large JavaScript Array Handling Denial Of Service Vulnerability
2004-09-07 KAME Racoon IDE Daemon X.509 Improper Certificate Verification Vulnerability

Plan

- Rappels sur Mac OS X
- Sécurité physique
- Installation / mise à jour
- Sécurité locale : utilisateurs et fichiers
- Sécurité des services réseau
- Sécurité des applications
- Applications sécurisées

Rappels sur Mac OS X

Système hybride :

- NextStep
- Mac OS 9 (Système de fichiers HFS+)
- Unix/BSD
- plus quelques éléments de Microsoft

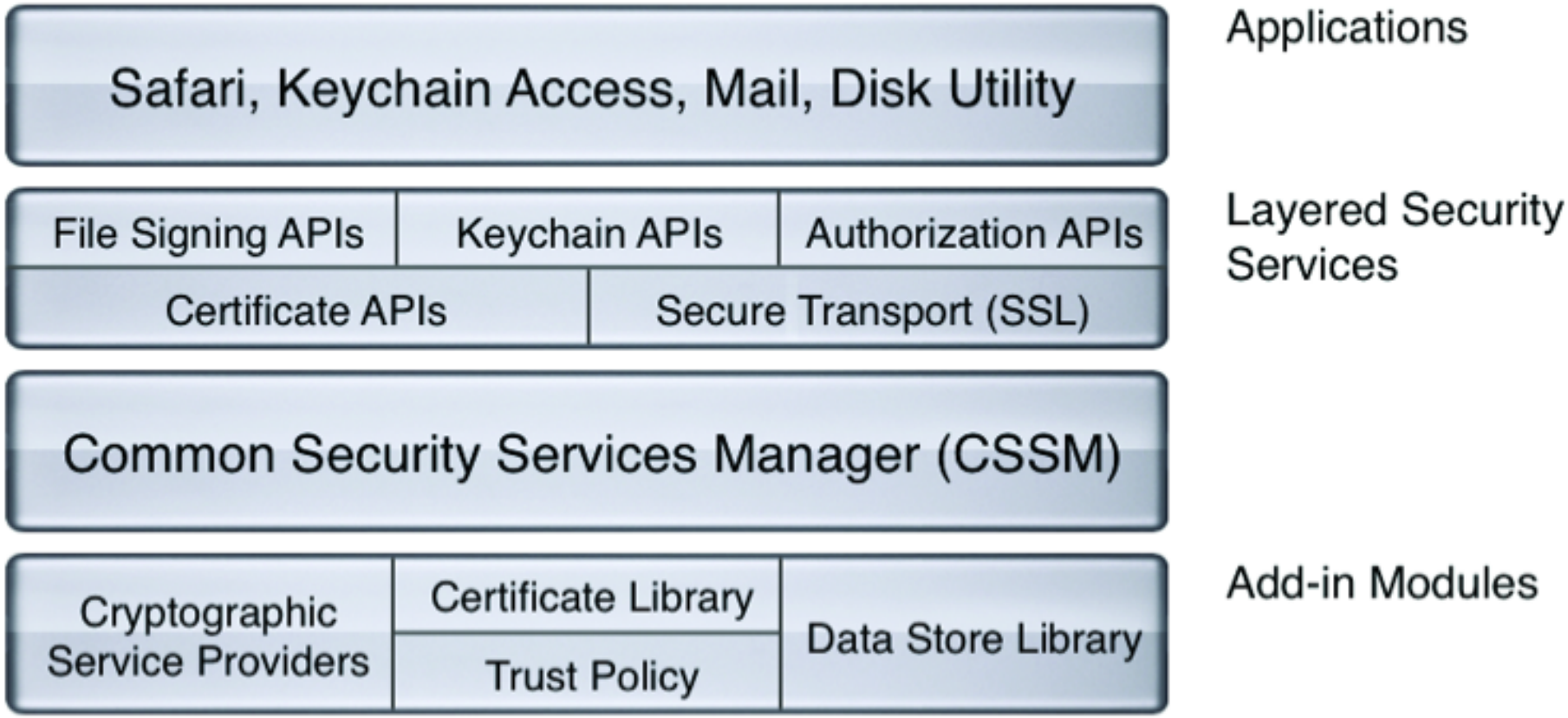
http://developer.apple.com/documentation/MacOSX/Conceptual/OSX_Technology_Overview/OSX_Technology_Overview.pdf

Core OS

- Darwin :
  - Noyau Mach 3.0
  - IOKit : gestionnaires de périphériques
  - BSD (process, file permissions, POSIX threads, TCP/IP)
  - X11
- Network support
- Velocity Engine
- Java virtual machine

CDSA

Common Data Security Architecture



Sécurité physique

Au niveau Open Firmware

http://docs.info.apple.com/article.html?artnum=106482
http://docs.info.apple.com/article.html?artnum=120095

Rend nécessaire un mot de passe pour booter un disque différent.
Empèche le boot en single-user (Cmd-S pendant le boot).

Sécurité physique (2)

Activer le mot de passe après la veille ou l'économiseur d'écran
(Utile pour les portables)

Post-Installation

- Installer les mises à jour immédiatement après installation.
- Définir un *umask* global (23 = 027) :

```
sudo defaults write  /Library/Preferences/.GlobalPreferences NSUmask 23
```

- marquer `console` comme `insecure` dans `/etc/ttys`.
  (réclame le mot de passe root pour démarrage en single-user).
- bannière de login dans `/Library/Preferences/com.apple.loginwindow.plist`.
  Exemple :

```
<key>LoginwindowText</key>  <string>L'acces a cet ordinateur est
controle. Tout abus sera sanctionne  </string>
```

- pour les logins SSH : mot clé `Banner` dans `/etc/ssh/sshd_config`

Mises à jour

- Liste :
  http://docs.info.apple.com/article.html?artnum=61798
- Mises à jour automatiques via les préférences système.
- Commande : `softwareupdate -install -req`

Anti-virus

- Mac OS X est vulnérable aux virus
- Peu attaqué pour l'instant.
- Donc anti-virus peu développés.
- Produits :
  - MacAfee : virex 7.5
  - Norton Antivirus for Mac 9.0
  - Clamav : http://clamav.or.id/snapshot/docs/MacOSX
    http://www.markallan.co.uk/software.php?page=clam
- Intéressant pour protéger les autres machines (windows).

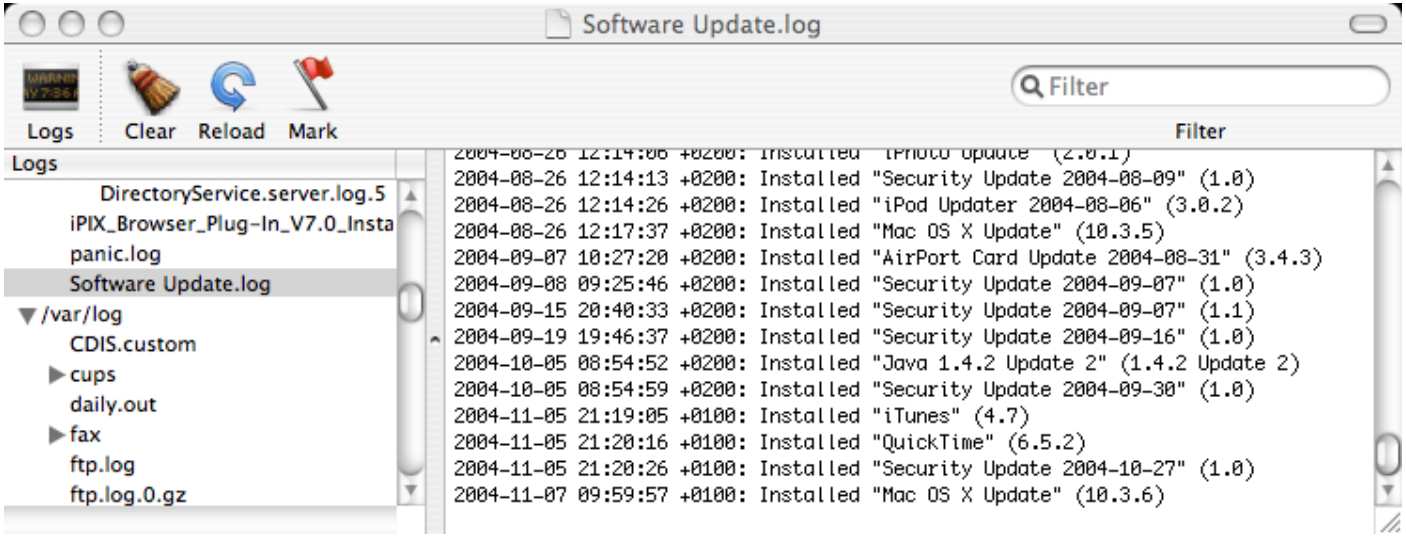
Journaux

Mac OS X utilise `syslog`.

Fichiers de log intéressants :

- `/var/log/system.log`
- `/var/log/secure.log`

`/Applications/Utilities/Console.app` permet d'accéder aux logs.



Gestion des utilisateurs et des fichiers

Modèle Unix

Les bases `passwd` et `group` sont gérées par Open Directory :
- netinfo
- LDAP
- NIS
- fichiers de `/etc/`

Droits d'accés aux fichiers : Unix (read/write/execute/setuid/setgid)

Possibilité de créer des utilisateurs avec accès restreints.

ACLs dans Tiger (Mac OS 10.4).

Attention HFS+ : case insensitive

Le compte Root ?

- Désactivé dans la configuration par défaut
- Le groupe `admin` définit les utilisateurs qui peuvent exécuter des tâches privilégiées.
- Utilisation généralisée de `sudo` et d'une API du *Security Server*.
- Avantages :
  - « bonne pratique »,
  - meilleur audit,
  - plusieurs administrateurs,
  - pas de session complète privilégiée.

Sécurité des fichiers

File Vault :

- Chiffrement des fichiers du répertoire de login des utilisateurs (clé = mot de passe) sur un volume chiffré auto-monté au login.
- Activable utilisateur par utilisateur
- Un mot de passe système pour récupérer les données en cas de perte du mot de passe utilisateur.
- Attention : Fichiers accessibles (protégés par les droits Unix) tant que l'utilisateur est connecté.

Volumes chiffrés :

- fonctionnalité de l'utilitaire disque
- créé un disque virtuel dans un fichier `.dmg` chiffré
- protection par mot de passe au montage

Réseau

Multi protocoles :

- TCP/IP (Unix/BSD, NextStep)
  - NetBIOS
  - AFP/TCP
  - Protocoles TCP/UDP classiques
- AppleTalk/EtherTalk (Mac OS)

Protocoles innovants :

- IPv6
- Rendezvous
- multicast
- IPsec + L2TP
- IEEE802.1X
- Wifi, Bluetooth, etc.

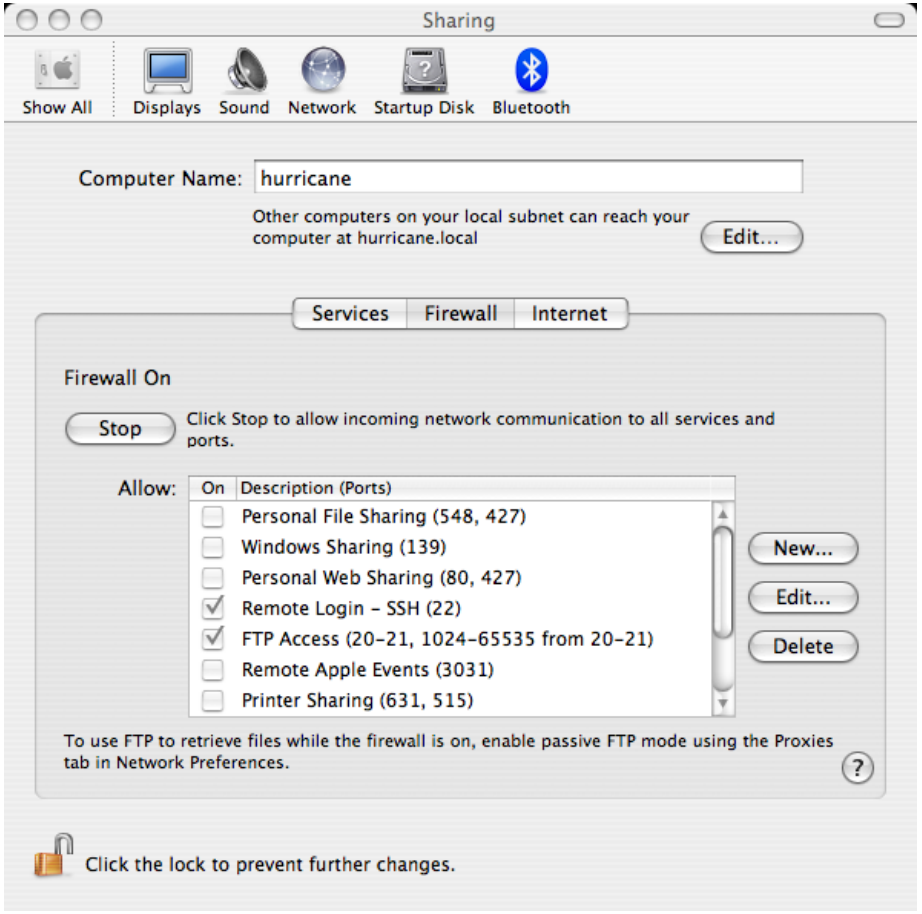
Réseau - ports spécifiques

Port	Utilisation	RFC
106/tcp	Password server	-
192/udp	Air Port Admin Utility	-
311/tcp	AppleShare IP WebAdmin	-
389/tcp	LDAP	1777
427/tcp/udp	Service Location Protocol (SLP)	2608
548/tcp	Apple Filing Protocol (AFP) over TCP	-
554/tcp	Real Time Streaming Protocol	2326
625/tcp	Directory Services Proxy	-
631/tcp	Internet Printing Procotol (IPP - CUPS)	2910
660/tcp	MacOS Server Admin	-
687/tcp	AppleShare IP Registery	-
1220/tcp	QT Server admin	-
3283/tcp/udp	Net Assistant - ARD	-
3659/tcp	SASL	-
3689/tcp	DAAP - iTunes Music Sharing	-
5009/tcp	Airport Admin utility	-
5353/udp	mDNS / rendezvous	http://www.multicastdns.org/

Firewall

ipfw (FreeBSD)

- filtrage stateful (pas via cliquodrome)
- NAT (partage de connexion réseau)
- Commande d'admin : `ipfw` ou préférences système → partage → firewall..



Rendez-vous

- Autoconfiguration d'adresses IP «link local» (à la mode IPv6) en l'absence de serveur DHCP.
  Réseau : 169.254.0.0/16
  Domaine : `.local`
- Annuaire de services disponibles.
  Utilise des protocoles multicast (mDns, SLP).
  Applications supportant Rendez-vous (non exaustif) :
  - iChat, iTunes
  - partage de fichiers
  - Safari / apache
  - Système d'impression
  - Air port
- Source de fuites d'information (SLP).
- (anecdotique : le nom va encore changer)

Partages de fichier

Protocoles : Apple Share, NFS, CIFS (plus FTP, SFTP, Webdav).

- NFS :
  - pas de configuration graphique dans Mac OS X Client
  - utilise /etc/exports à la mode BSD
- CIFS (Samba) :
  - configuration par défaut (`/etc/smb.conf`) exporte les home directories et imprimantes
  - lancé par xinetd
- Apple Share :
  - configuration par défaut exporte `${HOME}/Public`
  - utilise rendezvous

Services réseau

Services Unix traditionels (SSH, NFS, Cups, Mail, Web, etc.) :

- scripts de démarrage/arrêt dans `/System/Library/StartupItems/`
- configuration de l'activation par `/etc/hostconfig`

Services dynamiques :

- 10.2.x : `inetd` → `/etc/inetd.conf`
- 10.3.x `xinetd` → `/etc/xinetd.d/*`

Réseau avancé

Réseaux Privés Virtuels (VPN) :

- PPTP
- IPSec

Wifi :

- WEP
- 802.1X
- WPA

(Serveurs sur Mac OS X Serveur)

Sécurité des applications

Installation :

- de nombreuses applications peuvent s'exécuter de n'importe où, sans installation.
- le groupe `admin` a le droit d'écriture dans `/Applications` $\longrightarrow$ installations simples par glisser/déposer.
- Installeurs pour les applications les plus complexes.

Problèmes :

- Certaines applications (Microsoft, Adobe,...) demandent droits d'écriture pour tous dans leur répertoire !
- Certains installeurs changent les droits sur les répertoire système. (réparation par le CD d'install)
- Risques liés aux applications « gadget » : iChat, iTunes, partages Bluetooth & Wifi :
  - confidentialité
  - intrusions (social engineering)

Applications sécurisées

Mécanismes centraux du système pour la sécurité :

- trousseau de clés : mots de passe, certificats X509, etc.
- SSH

Exemple d'applications :

- Mail, Safari $\rightarrow$ utilisation des certificats
- apache + mod_ssl

Tendance renforcée dans Tiger...

Conclusion

Mac OS X est plutôt sûr par défaut.

Mais quelques problèmes :

- Quelques applications populaires à problèmes (droits d'accès),
- Beaucoup de code privilègié,
- Compromis ouverture/facilité d'utilisation vs sécurité :
  - communication sans fils airport, bluetooth
  - médias amovibles
  - rendez-vous

Bibliographie

- Apple Mac OS X Security configuration Guide, NSA, http://www.nsa.gov/snac/os/applemac/osx_client_final_v.1.pdf
- Ultimate guide to Mac OS X Security http://homepage.mac.com/macbuddy/SecurityGuide.html
- Mac OS X Server administrator's manuals http://docs.info.apple.com/article.html?artnum=50525
- Mac OS X : the Missing Manual, 3rd Ed., O'Reilly. http://www.oreilly.fr/catalogue/2841772888.html