Impression de sécurité ?

Matthieu Herrb

LAAS-CNRS

Capitoul, le 1er avril 2010

Agenda

Agenda

Problématique

- La fonction d'impression proprement dite : imprimer un document
- Impacts éventuels sur le reste du système d'information

Remarque : cette présentation peut s'appliquer à tout types de matériels « secondaires » dans un réseau : commutateurs, points d'accès wifi, téléphones, gadgets divers,...

Propriétés de sécurité

- Confidentialité
- Intégrité
- Disponibilité
- Imputabilité

Une chaîne complète

- logiciel d'impression (client/serveur)
- réseau
- imprimante
- papier

Agenda

Vulnérabilités du client ou du serveur

- décode / interprète des fichiers quelquonques
- formats complexes, fonctionnalités de scripts (PDF)
- ingénérie sociale (« *imprimez votre facture / billet électronique / ...* »)
- logiciel d'impression disposant de privilèges (exemple : `lpr` setuid `daemon`)

Ouvrir un document malicieux pour l'imprimer expose à :

- Exécution du code malveillant
- Elévation de privilèges
- Atteintes à la confidentialité / intégrité des autres documents imprimés

Risques liés au serveur

En plus :

- interface web : vulnerabilités spécifiques (XSS, CRSF)
- système d'authentification : impressions non autorisées

Protection

- mises à jour
  corrige les failles des logiciels
- filtrage réseau
  - limiter l'accès au serveur d'impression depuis clients autorisés
  - limiter les accès réseau du serveur d'impression
- anti-virus
  protège contre les documents malveillants
- ne pas imprimer n'importe quoi...

Agenda

Le réseau : un danger permanent

Souvent utilisé 2 fois (client $\rightarrow$ serveur $\rightarrow$ imprimante)

- protocoles non chiffrés (`lpd`)
- MiTM avec protocoles chiffrés :
  - implémentation vulnérable (non patchées)
  - absence de vérification de l'identité du serveur
  - clé privée accessible

$\Rightarrow$ atteintes à la confidentialité.

Agenda

Une menace considérable

- un serveur réseau complet, avec CPU, mémoire, stockage permanent
- nombreux ports ouverts (telnet, FTP, TFTP, HTTP,....)
- code complexe (interpréteurs PostScript, PDF, serveur Web,...)
- voit passer tous vos documents, y compris les plus confidentiels
- accessible de partout en interne
- quasiment pas de mise à jour logicielles
- protection par mot de passe quasi inexistante

Et pourtant une imprimante ça inspire confiance.

Risques

Tous !

- atteintes à la confidentialité / intégrité
- injection de code malicieux
- impression non autorisee
- denis de service
- prise de controle complète : remplacement du firmware pour inclure outils permanent d'attaque
- financier : consommation excessive de papier, pannes à répétitions.
- risque pour la santé (`http://www.informationweek.com/news/personal_tech/showArticle.jhtml?articleID=20120223`)

Exemples

- Imprimantes Dell/Lexmark permettant de changer le mot de passe admin sans connaitre le précédent (JSSI 2010)
- Imprimantes/Fax multi-fonctions disposant d'une fonction pour envoyer une copie par mail de chaque document envoyé ou recus.
- Accès via une vulnerabilité du serveur web à la zone de spool des documents sur un copieur/imprimante haut de gamme.
- `http://www.irongeek.com/i.php?page=security/networkprinterhacking`

Protections (?)

- Configuration des imprimantes
  - activer un mot de passe d'administration
  - desactiver les protocoles et interfaces non utilisés
  - privilégier les protocoles les plus surs
  - désactiver les serveurs web, SNMP
- Mises à jour des firmware (rares)
- Filtrage réseau
  - seul le serveur d'impression peut dialoguer avec l'imprimante
  - l'imprimante n'a pas à avoir accès à l'extérieur
- Dispositions contractuelles :
  imposer la confidentialité aux intervenants extérieurs.

Agenda

Cerise sur le gateau : le papier lui-même

- Confidentialité (laisser trainer les documents sur l'imprimante)
- Intégrité (facile de replacer un document par un autre avant que l'utilisateur ne vienne le chercher)
- Disponibilité (papier inadapté $\Rightarrow$ destruction de l'imprimante,...)
- Vol de papier à entête (ou plus) vierge

Protections

- Éducation des utilisateurs ?
- Imprimantes dédiées ?
  limiter l'accès physique.

Agenda

Un bilan peu glorieux

- Les fabricants livrent des produits sans aucune sécurité.
- Les ASR les installent et les configurent n'importe comment.
- Les utilisateurs n'en font qu'à leur tête.

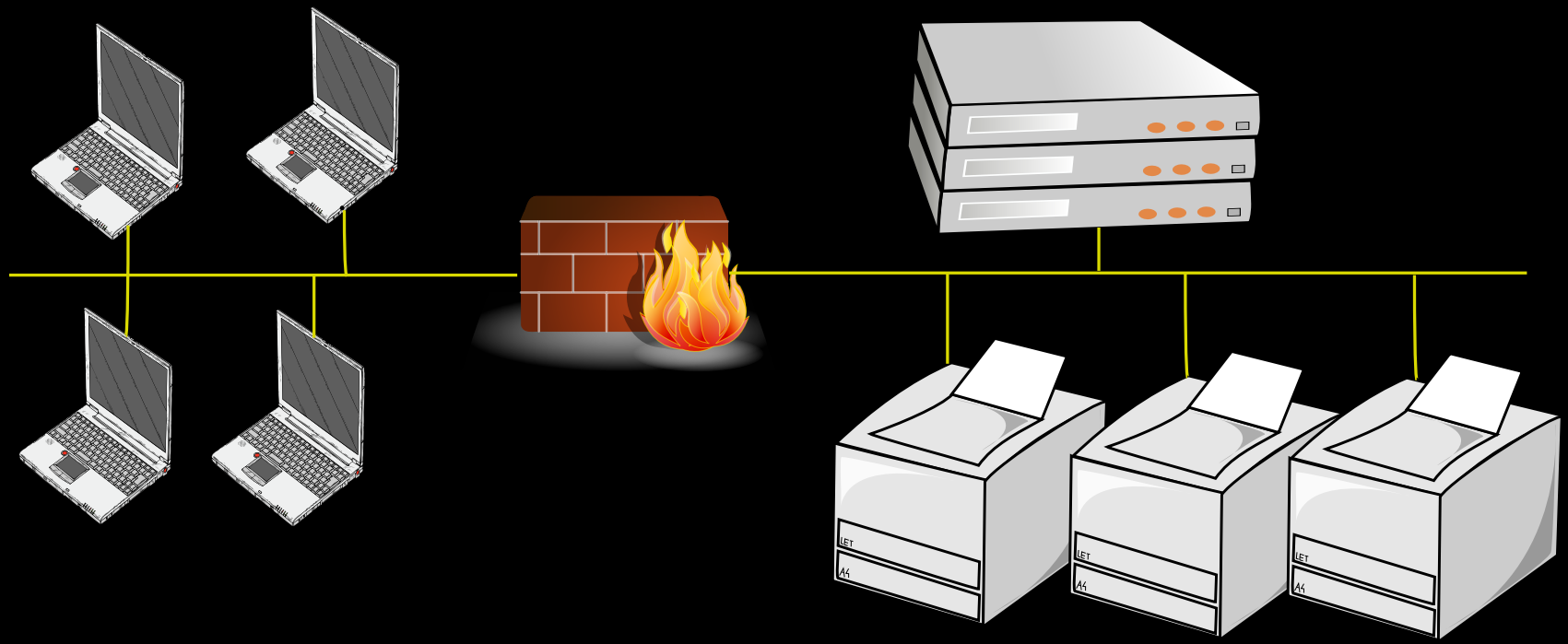
Solutions ?

- Architecture réseau adaptée,
- Journaliser les accès, contrôler les journaux,
- Centraliser la gestion du parc, garder le contrôle.

Ou alors

- Externaliser complètement le risque.

Une architecture pour sécuriser les impressions



Bibliographie

- A. Blonce, E. Filiol et L. Frayssignes, *Les nouveaux malwares de document : analyse de la menace virale dans les documents PDF*, MISC Numéro 38, Juillet/Août 2008.
- Microsoft Security Bulletin MS09-022, *Critical vulnerabilities in Windows print spooler could allow remote code execution*, 9 juin 2009.
- CERT-A, *Vulnérabilité dans CUPS*, Avis CERTA-2010-AVI-110, 5 mars 2010.
- T. Koechlin et J. Baron, *Juste une imprimante ?*, Journée de la Sécurité des Systèmes d'Information, OSSIR, Paris, Mars 2010.
- CERT-A, *Vulnérabilité dans les imprimantes laser Lexmark*, Avis CERTA-2010-AVI-137, 26 mars 2010.
- T. Schripp, M. Wensing, E. Uhde, T. Salthammer, C. He and L. Morawska, *Evaluation of ultrafine particle emissions from laser printers using emission test chambers*, ACS Journal of Environ. Sci. Technol., 2008, 42(12), pp 4338-4343.

Questions ?