# Pourquoi la sécurité est un échec

(et comment y remédier)

Nicolas RUFF
EADS Innovation Works SE/IT
nicolas.ruff (à) eads.net

# Introduction

- *Disclaimer*


  - Aucun logiciel ou site gouvernemental français ne sera blessé lors de cette présentation
  - (Vous pouvez quand même rester assis et regarder jusqu'au bout)
  - PS. Je ne suis pas sûr de la valeur juridique de ce *disclaimer*

# Introduction

- La sécurité est un échec, c'est un fait
  - La littérature regorge de détails
    - Pierre Vandevenne (SSTIC 2006)
    - Marcus Ranum (SSTIC 2008)
    - Linus Torvalds (« *security circus* »)
    - Bruce Schneier
    - DataLossDB.org
  - Vous en voulez encore ?
    - Honeypots, IPS, antivirus, Web 2.0, DLP, Cloud Computing, PCI/DSS, …
    - PHP, Debian (OpenSSL), PHP, udev, PHP, Adobe (Acrobat), QuickTime, Conficker, …

# Introduction

- En résumé …
  - Il n'y a jamais eu autant d'argent dépensé pour la sécurité
  - Mais
    - La sécurité par la technologie n'a pas fonctionné
    - La sécurité par le papier n'a pas fonctionné
    - La sécurité par l'éducation n'a pas fonctionné
- Ceci n'est pas une attaque gratuite
  - Mais une réflexion construite, issue de ma (longue et douloureuse) expérience

# Introduction

- Quelques idées personnelles sur le sujet
  - Mauvaises décisions
    - Prises il y a 30 ans: Internet, langage C …
  - Marchés captifs / *statu quo*
    - D'ailleurs personne dans cette salle ne souhaite perdre son boulot, non ?
  - Manque d'innovation / absence de prévention
    - La défense ne prend aucune initiative, l'attaquant mène la danse
    - Cf. attaques récentes via SMM ☺
  - Incompétence rampante
  - Informations majoritairement erronées

# A propos d'information

- Informations majoritairement erronées
  - Internet n'oublie rien
    - … mais le domaine évolue très vite
  - Tout le monde a quelque chose à dire
    - … mais très peu quelque chose d'intéressant
  - « *Buzz* » nécessairement engendré par les conférences de sécurité et les publications
    - On attend toujours le « *Big One* »
  - Incompétence rampante

# A propos d'information

- Ce qu'on entend

1. « Les seules attaques qui existent sont celles rencontrées dans la nature »
   - Fallait-il attendre le ver Conficker pour appliquer le correctif MS08-067 ?

2. « Les seules attaques qui existent sont celles pour lesquelles on peut acheter une défense »
   - Souvent une option à activer est beaucoup plus efficace qu'un produit …

# A propos d'information

3. « Les seules attaques qui existent sont celles que je connais / comprends / sait reproduire »
   - Le code d'exploitation pour la faille MS05-043 n'est disponible que dans le produit CANVAS. Cette attaque « existe »-t-elle ?

4. « Tout le monde fait comme ça »
   - Mais « tout le monde » a tort (puisque 100% des tests d'intrusion interne sont un succès pour l'attaquant)

5. « Nous acceptons le risque »
   - En êtes-vous *vraiment* sûr ?

# TESTEZ VOS CONNAISSANCES !

# Quizz (échauffement)

- Comment sécuriser une machine à voter ?
  - En mettant un antivirus ?
- Comment empêcher les internautes de télécharger du contenu protégé par la loi ?
  - En mettant sur leur poste un logiciel invisible, contrôlé à distance, contrôlant les accès aux fichiers et aux processus ?

# Quizz

- Quel est le meilleur mot de passe Windows ?

1. Bonjour
2. Bonjour123
3. 3!337_PwD@r00t
4. AAAAAAAAAAAAAAA

# Quizz

- Réponse (naïve)
  - #1 est vraiment mauvais, car il fait partie du trio de tête
    - « Vacances », « soleil » et « bonjour »
  - #2 et #3 sont équivalents
    - Le brute-force ne marche plus en dehors des cas triviaux
    - L'inversion du hash « LM » prend le même temps (*Rainbow Tables*)
  - #4 est le meilleur
    - Si la clé « NoLMHash » n'est pas positionnée (config. par défaut)
    - Car il ne génère pas de hash au format « LM »

# Quizz

- Réponse (complète)
  - Les 4 mots de passe sont équivalents
  - A partir du hash (« LM » ou « NTLM ») il est possible de se réauthentifier n'importe où dans le domaine
    - Attaque « *pass the hash* »
    - Cf. SSTIC 2007

# Mots de passe

- Idée reçue #1
  - « Les puissances de cassage augmentent: il faut passer le mot de passe de 7 à 10 caractères. »
    - « LM » fractionne les mots de passe en 2 blocs indépendants de 7 caractères
      - 7 caractères = 56 bits = clé DES
    - On sait depuis 1998 que l'espace de clés DES peut être entièrement exploré (« EFF DES machine »)

# Mots de passe

- Idée reçue #2
  - « Les puissances de cassage augmentent: il faut changer son mot de passe tous les 90 jours. »
    - Si « LM » est utilisé, tout mot de passe peut être retrouvé en moins d'une journée
    - Si « NTLM » est utilisé:
      - Mot de passe alphanumérique de 10 caractères
      - x 100 millions d'essais par seconde (algorithme MD4) **= 365 ans**
    - L'attaque « *pass the hash* » permet de s'authentifier sans inverser le hash
  - D'où viennent ces chiffres de 42 à 90 jours ???
    - De la perception du temps à l'échelle humaine …

# Mots de passe

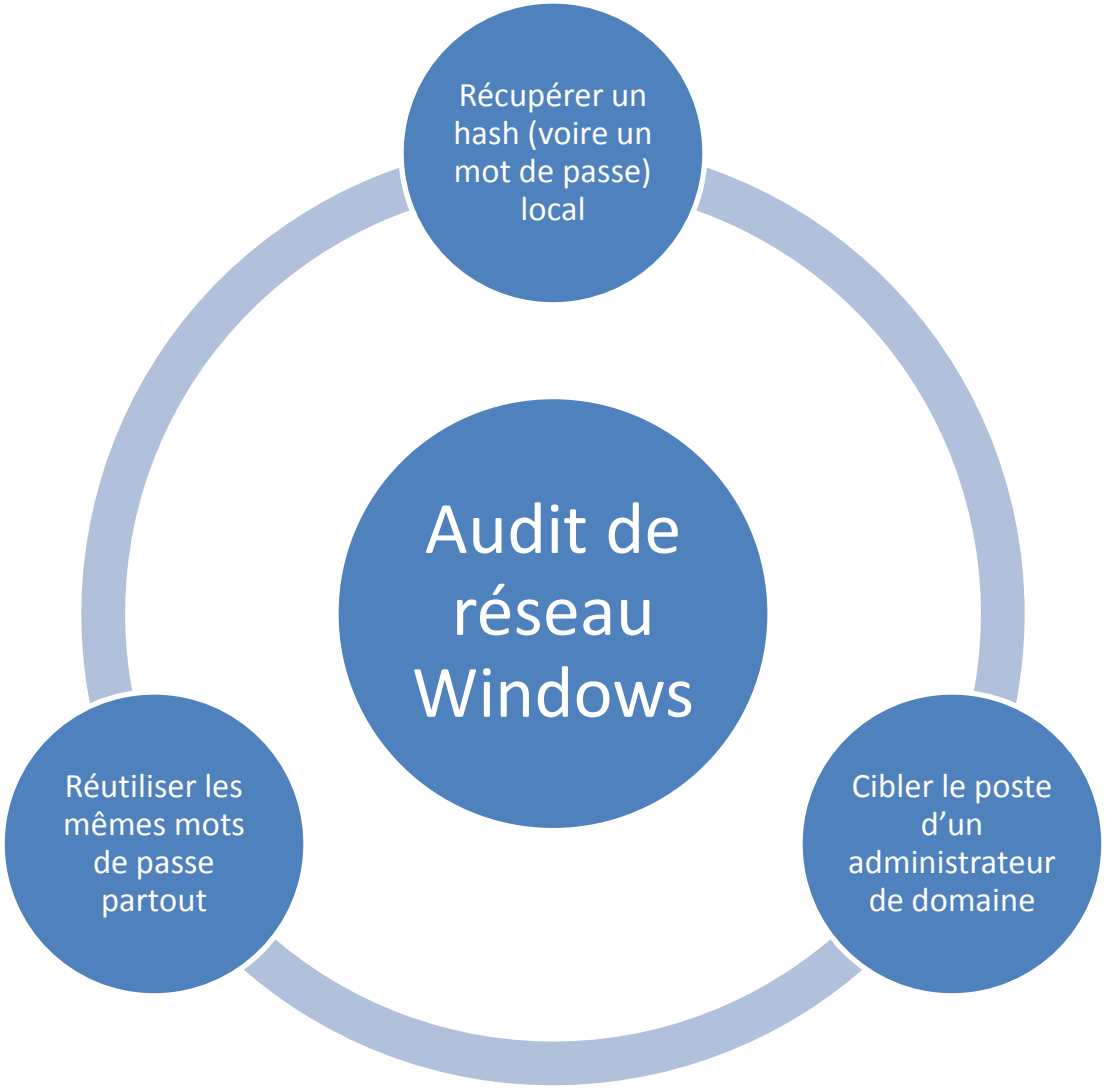
- Idée reçue #3
  - « Un bon mot de passe mélange majuscules, minuscules et caractères spéciaux. »
    - Cf. remarques précédentes
    - Soit il est nécessaire d'inverser le hash, soit on peut l'utiliser directement
    - Soit le hash est rapidement inversible (< 24h), soit il ne l'est pas en temps humain

# CONSÉQUENCES SUR LES AUDITS

# Audit(s)

- Retour d'expérience
  - Bientôt 10 ans d'expérience en:
    - Audit de produits & de systèmes (au sens large)
    - Tests d'intrusion (principalement internes)
  - Et 100% des tests « réussis »
    - Cherchez l'erreur …

# Audit(s) de réseaux



# Audit(s) de réseaux

- Si ça ne marche pas chez vous …
  - *Enjoy*, vous êtes dans le top 1% des réseaux bureautiques ☺
- Remarque: Conficker est un échec
  - Le brute-force ne marche quasiment plus en interne
    - Verrouillage de compte
    - Complexité minimale imposée
  - Il manque au moins deux choses:
    - « *pass the hash* »
    - Cas du compte administrateur local identique partout

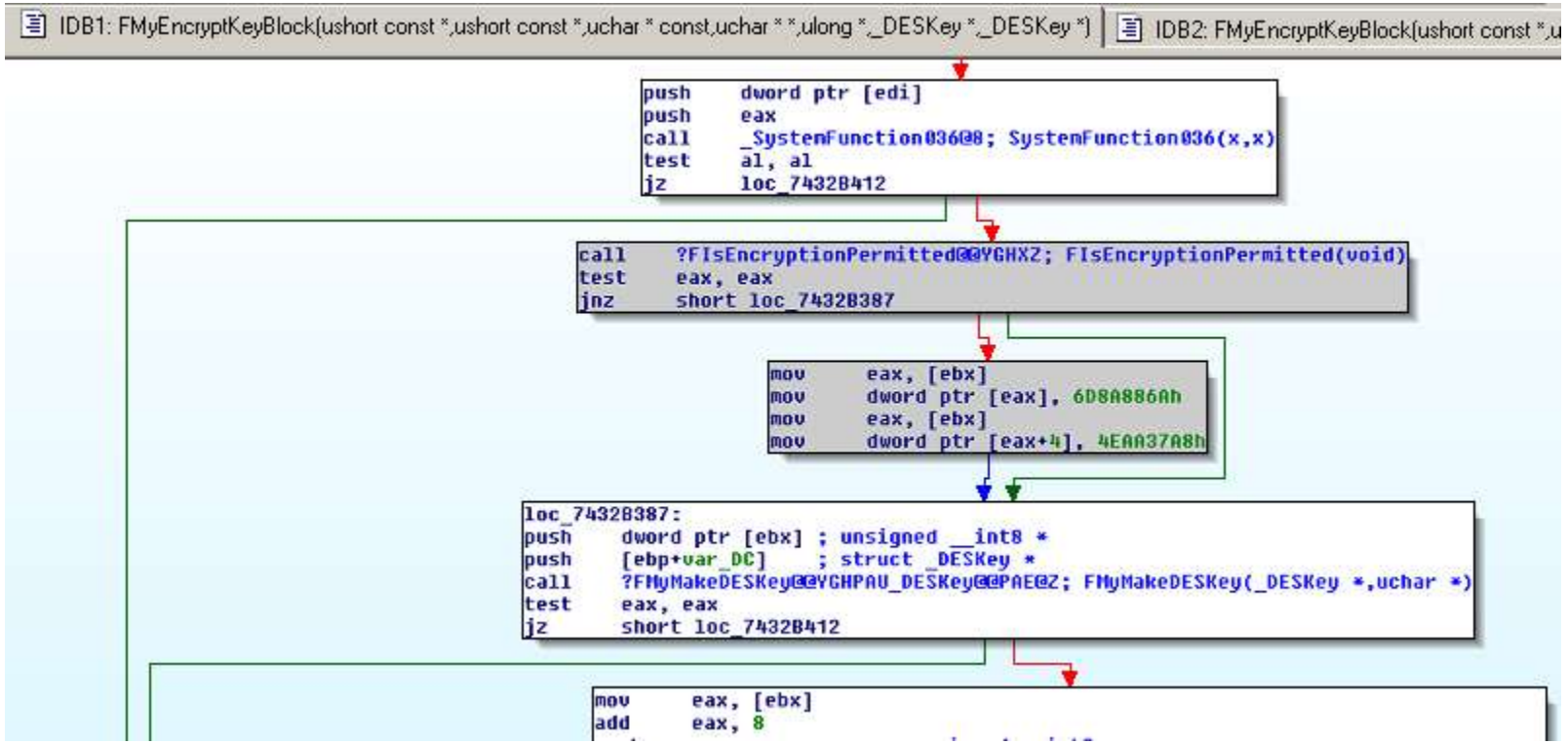
# AUDIT DE PRODUITS

# Audit(s) de produits

- *Best Of* de mes audits
  - Une liste de failles triviales et/ou de produits réputés "sûrs" …
  - MS06-077
    - Le serveur TFTP installé avec RIS sur Windows 2000 permet d’écrire des fichiers sur le serveur et s’exécute les droits SYSTEM

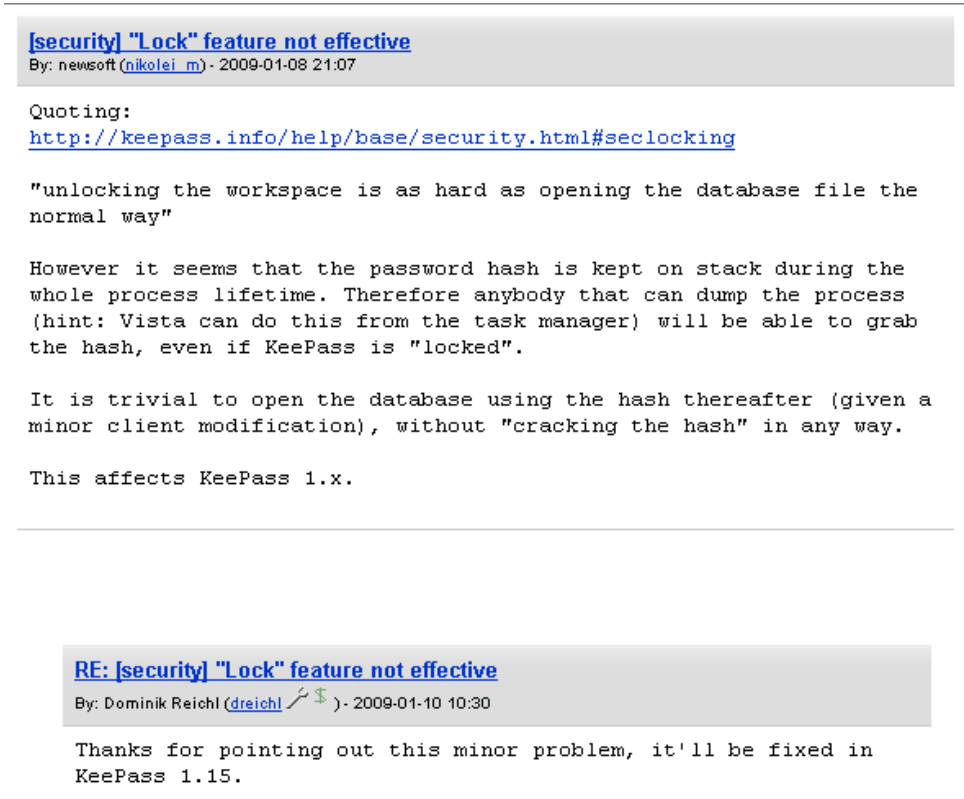
# Audit(s) de produits

- KB955417
  - (Merci à Kostya K.)
  - Le *Protected Storage* utilise une clé de chiffrement « en dur » dans les versions françaises de Windows 2000 et XP



# Audit(s) de produits

- KeePass 1.x
  - Toutes les versions antérieures à la 1.15 n'effacent jamais le hash du mot de passe en mémoire
    - Et le hash permet d'ouvrir le fichier de clés



**[security] "Lock" feature not effective**
By: newsoft (nikolei_m) - 2009-01-08 21:07

Quoting:
http://keepass.info/help/base/security.html#seclocking

"unlocking the workspace is as hard as opening the database file the normal way"

However it seems that the password hash is kept on stack during the whole process lifetime. Therefore anybody that can dump the process (hint: Vista can do this from the task manager) will be able to grab the hash, even if KeePass is "locked".

It is trivial to open the database using the hash thereafter (given a minor client modification), without "cracking the hash" in any way.

This affects KeePass 1.x.

**RE: [security] "Lock" feature not effective**
By: Dominik Reichl (dreichl ) - 2009-01-10 10:30

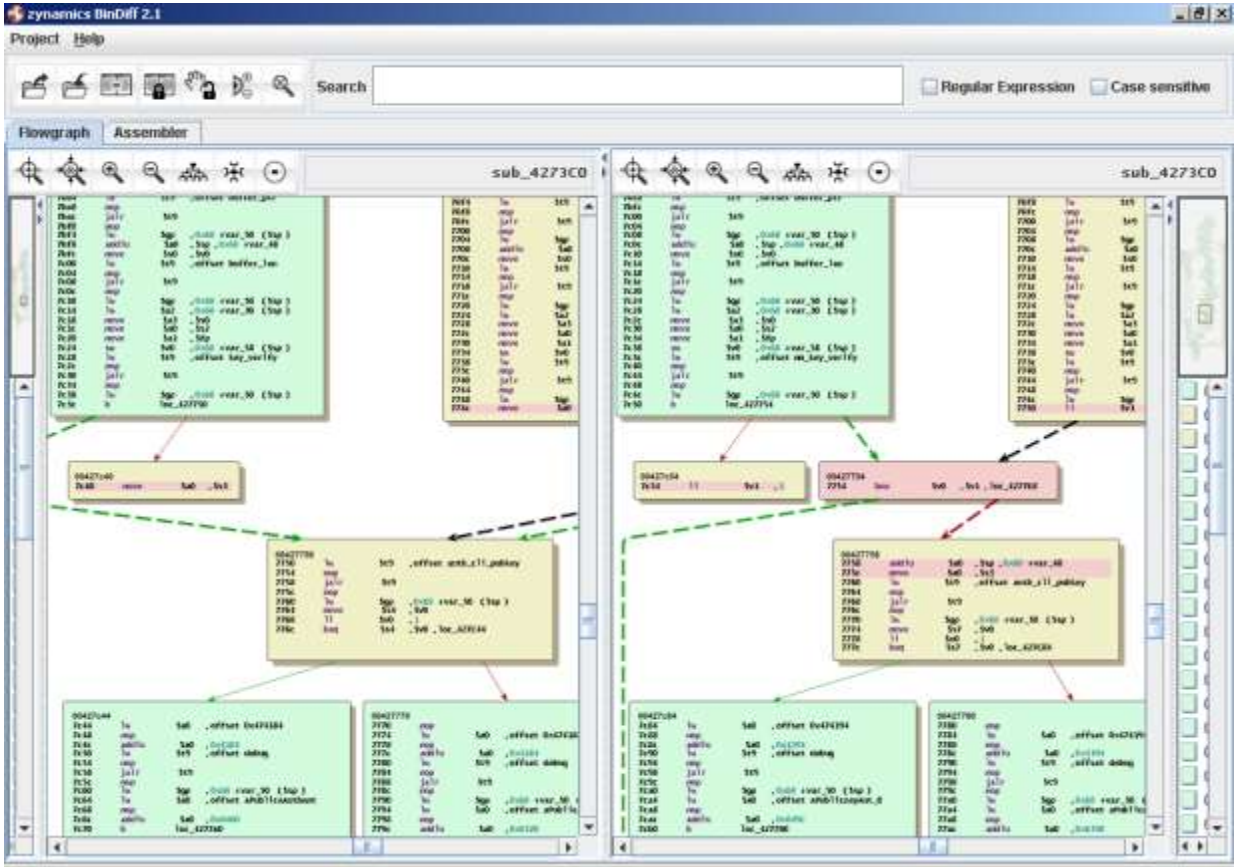
Thanks for pointing out this minor problem, it'll be fixed in KeePass 1.15.

# Audit(s) de produits

- Aruba Mobility Controller (2.x)
  - (Merci à Maxim S.)
  - CVE-2007-0932
    - $ cat /etc/passwd
      - nobody:x:99:99:Nobody:/:/sbin/nologin
      - root:x:0:0:Root:/:/bin/sh
      - arubasecretadmin:x:101:100:Aruba Admin:/:/bin/telnet2
      - serial:x:102:100:Serial:/:/bin/telnet4
    - ~/aruba/foobar/mswitch/bin$ find . |xargs grep <mot de passe secret supprimé, désolé ☺>
      - Binary file ./auth matches
      - Binary file ./login matches
      - Binary file ./fpcli matches
      - Binary file ./fpweb matches
      - Binary file ./cfgm matches

# Audit(s) de produits

- Aruba Mobility Controller (3.x)
  - http://www.arubanetworks.com/support/alerts/aid-42309.asc
    - Contournement de l'authentification SSH par clé publique



# Audit(s) de produits

- PHP/Pear Net::Ping
  - Injection de commandes par un « ; »
- McAfee ePO
  - Le paquet d'installation de l'agent embarque le login/mot de passe nécessaire à l'installation
- Etc.
  - L'infâme « ..\ », *backdoors*, clés de chiffrement « en dur », prise de contrôle à distance d'une passerelle VPN, prédiction d'aléa dans un système cryptographique, « *format string* » (en 2009), protocole propriétaire sans aucune sécurité, etc.

# Comment se protéger

- Il faut au minimum:
  - Etre courageux
  - Ne pas compter sur les autres
  - Changer de paradigme
  - Etre compétent
- Etape 1: corriger les problèmes précédents
  - Sinon inutile de passer en étape 2
- Etape 2: prendre de l'avance

# Comment se protéger

- Exemple de solution « d'avenir » (?) : la liste blanche
  - Tous les vendeurs y viennent
  - Attention: ne règle pas tous les problèmes
    - Scripts & code interprété
    - Librairies
    - Code exécuté en mémoire uniquement
  - Mais règle certains problèmes de la « vraie vie »
    - Ex. le fameux « *download & execute* » utilisé par les *malwares*

# Comment se protéger

- Faut-il dépenser de l'argent pour se faire une « liste blanche » ?
  - Existe depuis Windows 2000
    - « *Software Restriction Policies* »
  - Signer les exécutables « autorisés » avec une PKI d'entreprise
    - Encore faut-il savoir ce qui est « autorisé » …
  - Pour les pionniers, utiliser « AppLocker » de Microsoft
  - Il manque encore quelques outils
    - Par exemple, exécuter le code non signé dans une « sandbox » ?
- Donc c'est globalement faisable depuis Windows 2000

# Conclusion

- L'échec de la sécurité était programmé
  - Aux origines de l'informatique « personnelle », qui fusionne maintenant avec l'informatique d'entreprise
- Cet échec commence à se manifester depuis quelques années
  - Par l'incapacité chronique à répondre aux nouvelles attaques
- Il est temps de changer de paradigme
  - Ou le « *Big One* » va vraiment finir par arriver
- Des solutions fiables et peu chères existent
  - Principalement le courage et la compétence
  - Mais ce ne sont pas les plus répandues en entreprise