



HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet



Conférence du CLUSIF

Crochetage de serrures en environnement informatique



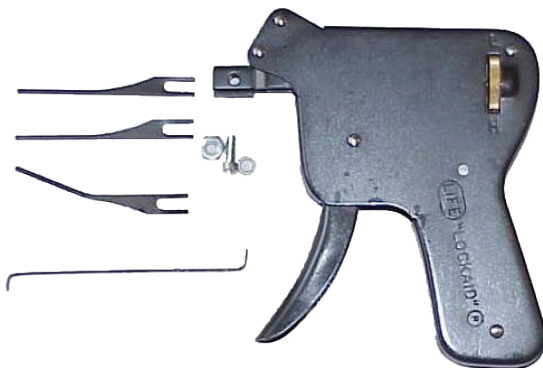
Jérôme Poggi
<Jerome.Poggi@hsc.fr>

- Quelles compétences ?
 - Présentation des outils
 - Les différentes techniques
 - Méthodes douces
 - Méthodes moins douces
 - Délais d'ouverture
- Démonstrations
 - Boîte incendie et/ou boîte à clefs générale
 - Câble ordinateur
 - Vidéos :
 - Armoire de brassage
 - Formation, « faites-le vous-même »

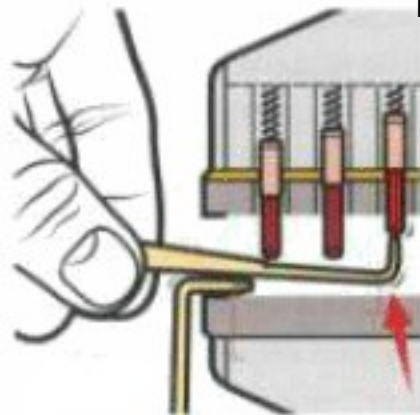
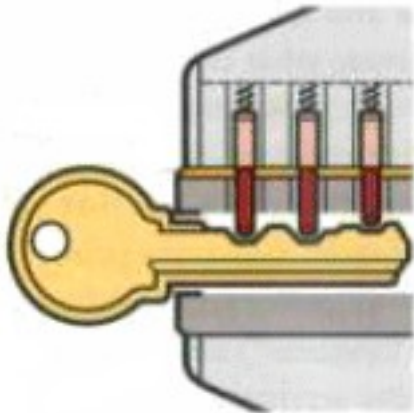
Quelles compétences ?

- De la patience
- Du doigté
- De la pratique
 - L'ouverture de serrure est un métier, alors que le crochetage est un art
- Il n'est pas nécessaire d'avoir des outils très coûteux
 - Il est souvent possible d'ouvrir une serrure avec « un truc »
- « Le sens de la bricole » et de l'imagination

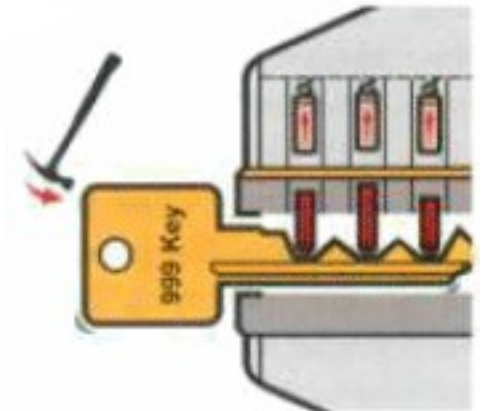
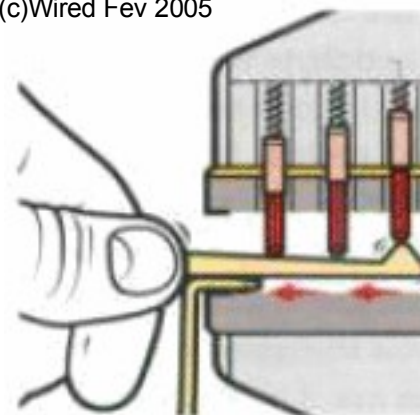
- Outils de crochetage
 - Crochets et entraîneurs
- Cales de cadenas
- Pistolet à main ou électrique
 - A choc ou vibrant
- Set de clef à percussion
- Crochets tubulaires ou parapluie



- Méthodes d'ouverture de serrures (douces)
 - Avec la clef ou un passe
 - En crochétant la serrure
 - Laisse de très très légères traces
 - En raclant la serrure
 - Use prématurément la serrure
 - Avec une clef 999
 - Use prématurément la serrure, peut casser la serrure à la longue

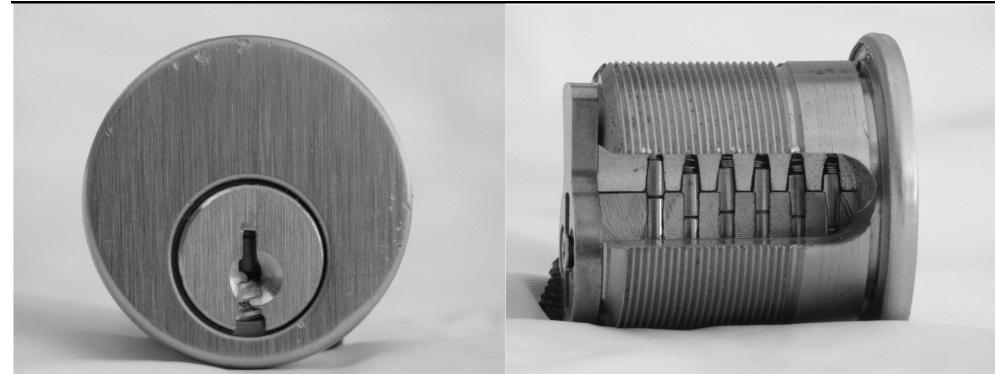


Images : (c)Wired Fev 2005



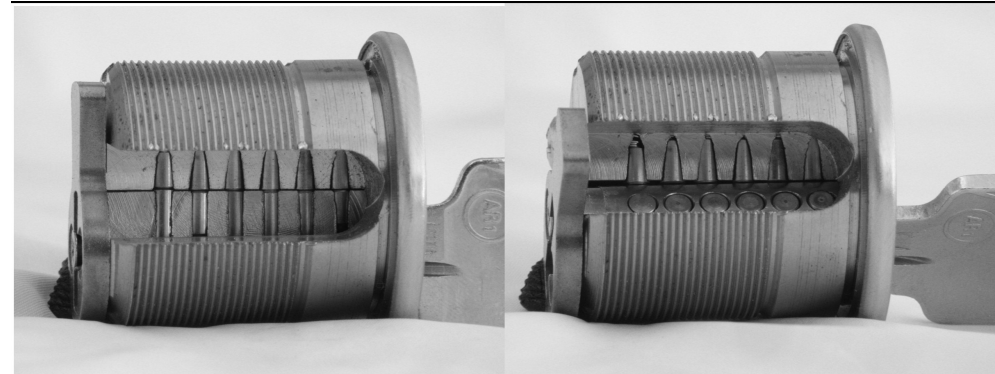
« Vue sans la clef »

Les goupilles ne sont pas alignées
le barillet ne peut pas tourner



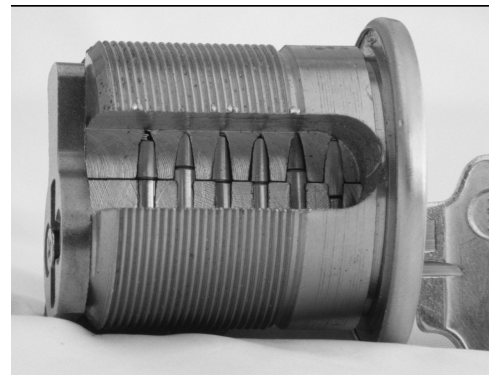
« Vue avec la bonne clef »

Toutes les goupilles sont alignées,
le barillet peut tourner
La ligne de césure est libre



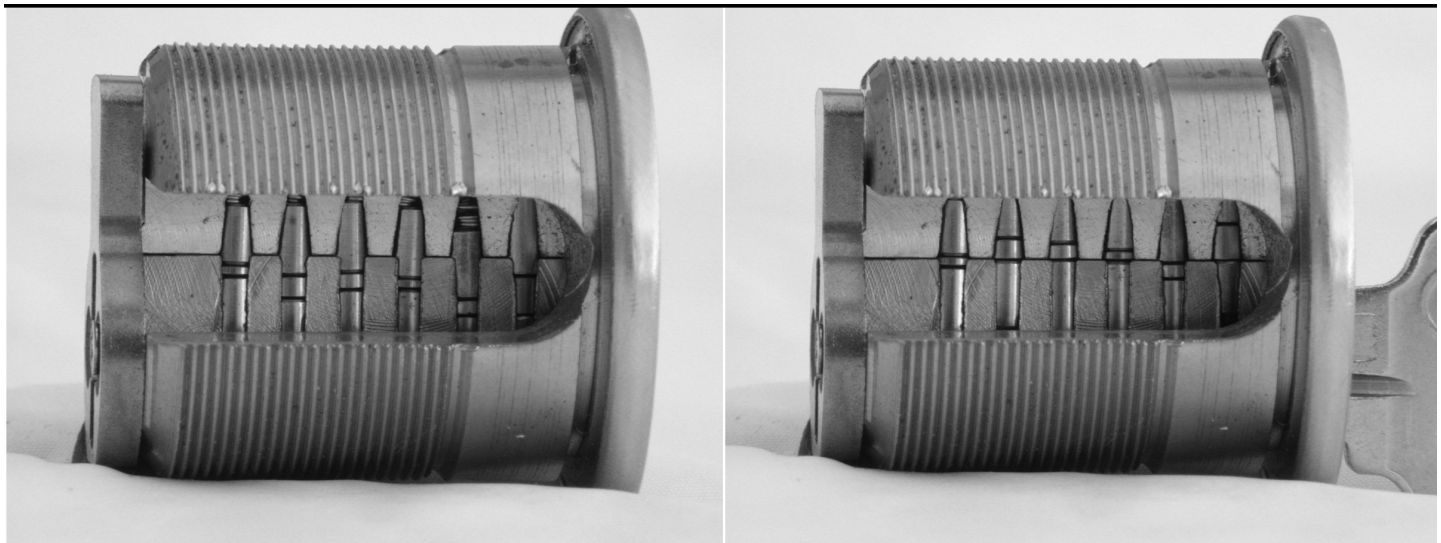
« Vue avec une mauvaise clef »

Les goupilles ne sont pas alignées,
le barillet ne peut pas tourner



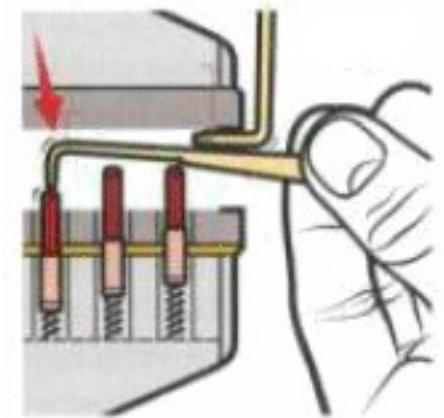
Images copyright 2003
Matt Blaze
<http://www.crypto.com/>

- Les clefs maîtres plus communément appelées « passe-partout »
 - Les goupilles sont segmentées pour obtenir plusieurs clefs valides
 - Mais le nombre est mathématiquement (2^n) où n = le nombre de goupilles
 - Très pratique dans une entreprise pour ouvrir toutes les portes en cas de problème, incendie ...
 - Rend la serrure plus vulnérable !
 - Plusieurs solutions permettent de faire tourner le barillet.

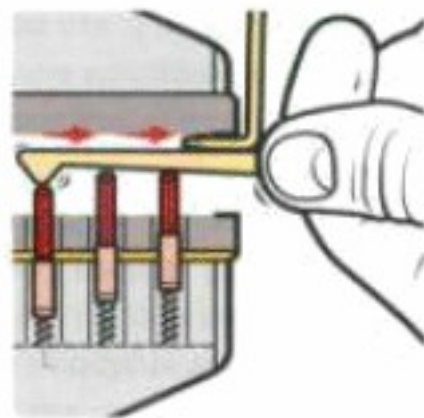


Images copyright 2003
Matt Blaze
<http://www.crypto.com/>

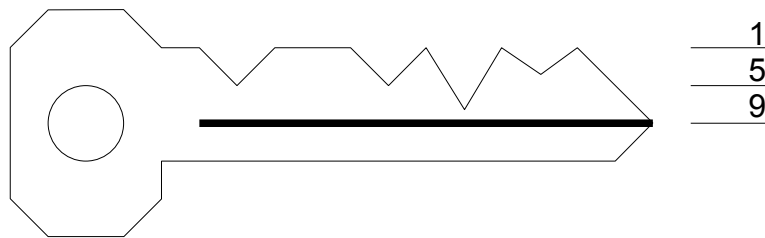
- But : utiliser les défauts, les jeux des serrures pour bloquer les goupilles sur la ligne de césure
- C'est une technique qui nécessite de l'entraînement
- Méthode :
 - Le barillet est tourné avec un entraîneur, pas trop, pas trop peu
 - Il faut pousser goupille par goupille,
 - Jusqu'à ce qu'elle se bloque sur la ligne de césure.
 - Jusqu'à ce que le barillet tourne complètement
- Il faut :
 - du toucher,
 - sentir chaque goupille,
 - connaître le mécanisme



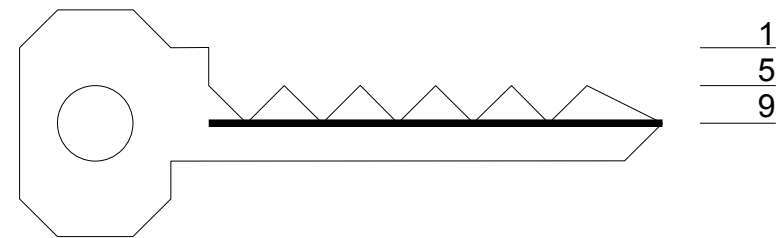
- Le raclage de serrure est comme le crochetage
 - Mais en version plus « Brute »
 - L'outil utilisé est en forme de triangle
 - faire bouger les goupilles une par une en rentrant / sortant l'outil
 - Plus ou moins rapidement
 - Plus ou moins profondément



- Technique « grand publique » depuis 2004/2005
- Appelée aussi clef 999 ou clef à percussion
 - Clef avec les plus grandes combinaisons
 - Projection des goupilles internes (ou passives) vers le haut (US, NL ...) ou vers le bas (France)
 - Clef coupée/limée à la possibilité la plus basse



Clef normale



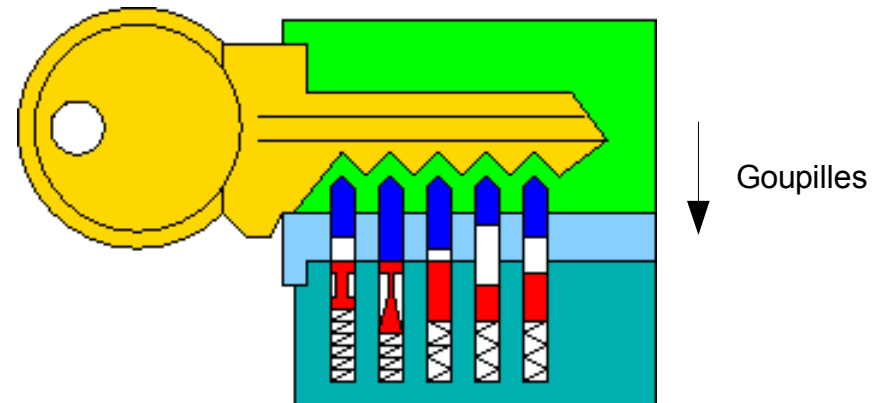
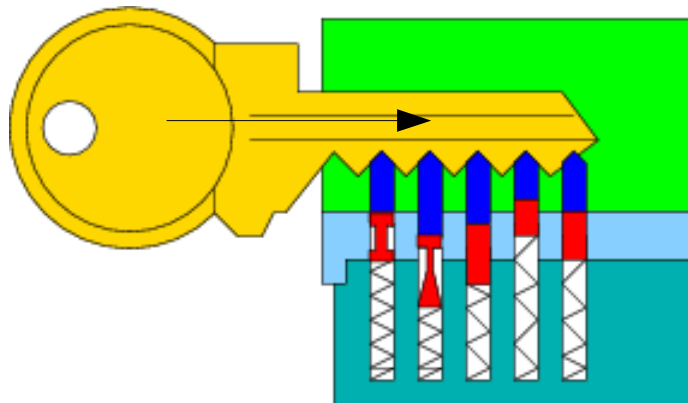
Clef 99999

- Méthode d'ouverture

- Très rapide !
- Pas de trace ! Donc pas d'effraction (au sens assurance)
- Ne demande pas de compétence spéciale !
 - Un enfant de 12 ans est capable de le faire !



- Achat sur Internet du « Kit Français » avec 17 clefs : 250€ HT



Goupilles

- Avec la clef
 - Immédiat
- En crochétant
 - Dépend de la qualité de la serrure, du jeu dans le mécanisme, des contre-mesures anti-crochetage ...
 - De la compétence du crocheteur (habileté, expérience, finesse ...)
 - De 5 secondes à ... beaucoup
- En raclant
 - Dépend de la qualité de la serrure, du jeux dans le mécanisme,
 - De 5 secondes à ... quelques minutes
- Avec une clef 999
 - En moyenne de 3 à 30 secondes suivant la complexité de la serrure

- Boîte incendie et/ou boîte à clefs générale
- Câble ordinateur
- Vidéos :
 - Armoire de brassage
 - Armoire de bureau ou tiroir de bureau
 - Cadenas
 - Serrure plate de porte avec une clef à percussion

- Soyez conscients des risques et maîtrisez les
- Pensez à la vidéo surveillance des équipements sensibles
- Utilisez des serrures/cadenas approuvés
 - Avec des protections supplémentaires
 - goupille « piègeuse » de barillet
 - Attention : serrure inutilisable après tentative de crochetage ou percussion
 - Goupilles peu profondes
 - La position basse du piston est plus haute que les autres
 - La clef à percussion n'est plus une 999999 mais une 9959959 (exemple)
 - Ne fonctionne pas avec les pistolets à chocs
 - Goupilles en forme de champignon, diabolo ... anti-crochetage
 - Nombre très important de goupilles, clef très longue ...
 - Voir <http://www.toool.nl/blackbag/?p=52>

- Internet

- MIT Guide to Lockpicking
 - <http://www.capricorn.org/~akira/home/lockpick>
 - <http://www.lysator.liu.se/mit-guide/mit-guide.html> : Version Française
 - http://www.ssdev.org/lockpicking/MIT_F/crochetage.html : version Française
- <http://www.toool.nl/index-eng.php> : *The Open Organisation Of Lockpicker*, site de Han Fey et de Barry Wels
- <http://deviating.net/lockpicking/topics.html> : Présentation très complète
- <http://www.toool.nl/bumping.pdf> : Les clefs à percussions
- <http://www.locks.ru/> Et <http://www.locks.su/bump/index.shtm> : Site Russe
- <http://www.locks.su/bump/fulltest/fulltest.shtm> : Test de multiples clefs particulières
- <http://www.toool.nl/competitie/> : Compétition et liste de clefs/serrures ouvertes
- <http://wiki.whatthehack.org/images/0/00/BumpkeyPresentatie.pdf>
- <http://www.locksport.com/> : Le crochetage de serrure vue comme un sport
- <http://www.lockpicking.pl/> : Des ressources en crochetage (en polonais)

- Vidéos
 - <http://connect.waag.org/toool>
 - <http://www.toool.nl/bumpkey-alert.wmv> (Télévision Nova)
 - <http://connectmedia.waag.org/toool/whatthebump.wmv>
- Divers
 - <http://security.org/>
 - <http://crypto.com/photos/>
- Forum de Lockpicking
 - <http://lockpicking101.com/>
- Livres
 - Steel Bolt Hacking de Douglas Chick (ISBN 0974463019)
 - Locks, Safes, & Security de Marc Tobias (ISBN 0398070792)

Questions ?