RAFALE

ARNAQUER LA FRANÇAISE DES JEUX

ANTIVOL À CODE BTWINCYCLE

CAMÉRAS DE SÉCURITÉ & VIDÉO-SURVEILLANCE

PETIT COURS INTRODUCTIF SUR LES ALARMES

PALAIS DE JUSTICE

EMPREINTES DIGITALES

TISCALI

VANLOCK

N°1 2€

RAFALE

Pour que tout s'arrête, sauf la fête.

Préambule

Rafale est un *e-zine**, paru pour la première fois en octobre 2006. Il est né des restes de la culture cyberpunk, de la scène geeko-old school et de l'imagination illégaliste qui se trouvait, depuis le début des années 2000, quelque peu en délabrement, après la mort de beaucoup d'autres zines (HVU, Phrack-fr, Noway, Noroute...). Voulant se concentrer sur l'aspect pratique des choses, et tout particulièrement sur leur détournement, Rafale, mains dans le cambouis jusqu'aux coudes, ignore les règles, les contraintes et les lois. Il ne théorise rien. Il prend acte et s'amuse, avec la connerie de la rage adolescente, avec la malice du contournement de tous les dispositifs nous environnant, avec la méchanceté de la pègre, avec la folie de la plèbe.

Ce qu'on trouvera dans ces pages ne sera rien d'autre qu'une suite de manuels pour que tout s'arrête, sauf la fête. Ce qu'on y découvre, en somme, ce sont «des techniques de cuisine pour fabriquer une radio avec un réseau de plomberie et un bout de fil ; la reproduction de la carte d'accès aux toilettes VIP du gouverneur de la banque nationale (celles pour les employés étant toujours bouchées) ; l'ouverture par magie du gros cadenas de ton ancien coffre à trésor fermé depuis ta plus tendre enfance ; la conception de blagues téléphoniques efficaces, crédibles et gratuites, avec des cours de *social engineering* en appui ; des manières de se battre pour les transports en communs et la culture gratuite grâce à des études de tickets divers ; la fabrication de son propre téléphone artisanal et l'augmentation de ses capacités et de ses utilisations» ** ; des analyse des failles des cartes bleues ou d'alarmes de grandes marques ; des comptes rendus d'exploration urbaine, du bunker aux catacombes, en passant par le Palais de Tokyo de Paris ou le réseau d'aération du métro… Il s'appelle «Rafale» mais il aurait tout aussi bien pu s'appeler «Artisanat» ou «Jean- Framboise » **. On s'en fout.

Pourquoi une sortie papier ?

Pour le plaisir de recouper les meilleurs articles, tout en retraçant au mieux l'état d'esprit de l'e-zine. A noter que Rafale, dans sa version originale, était particulièrement difficile d'accès. Pour le sérieux de la version papier, les articles ont étés retouchés — disons de manière générale au moins de moitié. Certaines parties ayant étés tronquées et d'autres d'avantage développées, pour qu'il soit plus accessible à qui voudra un minimum se pencher sur ces questions. Certains articles sont accompagnés d'encarts ou de notes qui sont, eux, écrits pour le besoin de la version papier. Aussi, de la même manière que le premier article (cf Française des jeux) n'est pas tiré de l'*e-zine* Rafale, nous tenterons, dans les prochains numéros, de diversifier nos sources. Les techniques présentées ont toutes été testées et approuvées. Et bien évidemment, ce magazine, s'il sert de cale pour ta chaise bancale, n'a pas grande utilité. Les astuces développées ici n'étant pas parfaites, elles doivent être considérées comme des pistes pour que, débordant de curiosité, tu les expérimentes et les développes à ton tour.

* ***L'e-zine Rafale consultable sur internet www.rafale.org***

** ***Rafale N°1.***

ÉDITO

Le voici. Le premier numéro. Ça fait un moment qu'il traîne quelque part, sur des disques durs cryptés ou des serveurs ougandais, va savoir. Mais il est là, tout chaud sorti des presses.

EPIER SES DISPOSITIFS, À LA LOUPE ET SOUS TOUTES LES COUTURES

Reprenant les meilleurs articles, Rafale sort aujourd'hui, comme un hommage, en version papier. Il se lit maintenant dans les chiottes, s'échange dans les troquets contre un galopin, se partage en bande organisé, au milieu de la table avec une kalash' pour presse papier. Bref, Rafale te pousse dans un monde illégaliste et malin, où tout moralisme à la con est foulé comme le raisin pendant les vendanges. Il se rit bien, jusqu'à la nausée, de toute convention.

Pour ce premier numéro, la sélection d'article s'est voulue la plus éclectique. Ils sont tous isus de l'e-zine Rafale, hormis le premier. Ils sont accompagnés de schémas barbares et de photos floues — fallait pas s'attendre à de la HD sur papier glacé. Mais ça n'enlève rien à son envie d'étudier les moyens de l'Empire. Epier ses dispositifs, à la loupe et sous toutes les coutures.

Et pour cela, au menu : du crochetage de serrure, de l'exploration urbaine, des alarmes, des fausses empreintes digitales, du piratage de caméras de surveillance... Bon appétit. ●

Sommaire

‡ **Arnaquer La française des jeux**

‡ **Antivol à code BtwinCycle**

‡ **Caméras de sécurité & vidéo-surveillance**

‡ **Petit cours introductif sur les alarmes**

‡ **Palais de justice**

‡ **Empreintes digitales**

‡ **Tiscali**

‡ **Vanlock**

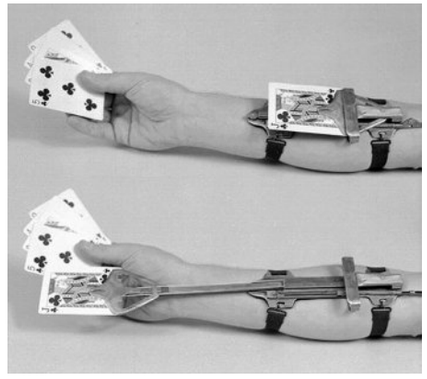
Arnaquer La Française des jeux

Modifier l'algorithme de la machine à sous ; changer les billets du loto du village ; décrypter le fonctionnement des arnaques de la fête foraine ; calculer les stats de la roulette ; savoir compter les cartes au poker ; lester une face d'un dès ; pirater le central téléphonique d'une radio pour être l'auditeur gagnant.

Tricher, truquer le hasard, gagner à coup sûr, et surtout, inverser les rôles. Nous expliquerons ici une arnaque qui n'est plus opérationnelle, mais qui a, de ça quelques proches années, rempli bien des portefeuilles. Elle concerne les jeux à gratter de la Française des jeux. Pour saisir l'arnaque, expliquons avant tout le fonctionnement de ces jeux.*

Lorsque tu achète un ticket à gratter, et qu'il est gagnant, le buraliste est censé gratter le « nul si découvert », ou bien le déchirer, pour qu'il ne puisse être utilisé plusieurs fois. D'autre part, il scanne le code-barre unique du ticket, de manière à ce que le réseau informatique de la française des jeux sache que ce même ticket a déjà été gratté et que son montant gagnant a été versé. Tout cela, bien sûr, après que le buraliste t'ai donné ton dû.

L'arnaque consiste donc, dans un premier temps, à réussir à trouver des tickets gagnants qui ont déjà été grattés, mais dont le nul-si-découvert, lui, ne l'ai pas été, ou bien tout simplement qui n'ont pas été déchirés** **A**; et dans un second temps, à trouver un autre buraliste qui n'est pas connecté au réseau informatique de la Française des jeux, et qui de facto ne peut pas vérifier si le ticket qu'on lui tend a déjà été encaissé auparavant **B** .



A

Pour la recherche des tickets encaissés, il s'agira d'enfiler des gants en caoutchouc, et de planquer son ego dans ses poches. Soit, faire les poubelles des kiosques. A l'époque, ce ne serait pas exagéré d'affirmer qu'au moins un kiosque sur dix gardait les tickets encaissés intacts. Une nuit de repérage suffisait donc à trouver une poubelle emplie à ras bord de ticket déjà grattés ! Tu foutais ces tickets dans ton sac, et une fois chez toi, tu triais le reste de la nuit les tickets gagnant des perdants.

Lorsque les tickets non déchirés ont commencés à se faire rare, certains ont poussé le vice jusqu'à passer quelques heures à recoller les morceaux. Techniquement, les tickets sont constitués de deux feuilles collés l'une sur l'autre, une pour le recto et l'autre pour le verso. Ces deux feuilles, si on les détache l'une de l'autre délicatement (dans la « tranche » du ticket, donc), ne se déchirent pas. Après avoir rassemblé les bons morceaux du ticket comme un puzzle, il fallait donc, dans un premier temps, prendre un ticket non déchiré (de préférence perdant), et en garder le verso après l'avoir « découpé » dans la tranche. Dans un second temps, faire de même avec les petits morceaux du tickets gagnant, déchiré, lui. Utiliser le verso comme base, sur lequel viennent se coller les morceaux du ticket gagnant. Un tube UHU classique faisant l'affaire. Après que le puzzle soit reconstitué, nous avons un ticket gagnant prêt à être encaissé.

« Tricher, truquer le hasard, gagner à coup sûr, et surtout, inverser les rôles. »

B

Comment savoir si un buraliste n'était pas connecté au réseau informatique ? Déjà, quelques indices étaient parlants. Les petits kiosques des boulevards (en forme de baraque à frite sur le trottoir) l'étaient rarement. Le petit tabac du coin de la rue aussi. Et puis les bureaux de tabac excentrés des centre-ville. Pour avoir confirmation, il suffisait de faire une tentative avec un ticket gagnant de un ou deux euros. Tu le refourguais au kiosquier, et s'il le scannais avec son appareil et qu'une expression d'incompréhension bâtarde se dessinait sur sa face, c'était foireux. Il fut une époque où les kiosques non-informatisés était encore grouillants...

Et là, ne restait plus qu'à empocher la somme du ticket à gratter. Nous laisseront le soin à l'imagination de tout un chacun de s'amuser à calculer le pactole d'une seule poubelle récupérée... Inverser les rôles, disions-nous. Moins par refus d'être les éternels perdants que par jouissance d'être un gagnant ponctuel.

**
Les bar-tabac qui brassent beaucoup de monde ne s'embarrassent pas à gratter le nul-sidécouvert, opération trop longue, mais préfèrent les déchirer. Nous verrons plus loin comment il est aussi possible d'outrepasser cette barrière.

*
Cela dit, reste à vérifier s'il ne reste pas des endroits reculés que le réseau informatique de la Française des jeux n'a toujours pas pénétré. Néanmoins, il semblerait qu'il soit de plus en plus difficile de trouver des tickets française des jeux intacts : soit le nul-si-découvert est gratté, soit le ticket est déchiré en confetti. Peut-être le fruit d'ordres supérieurs. Du reste, même si cette technique ne fonctionne plus, il s'agit ici d'avantage de montrer que le système est tout à fait faillible...

Antivol à code BTwinCycle

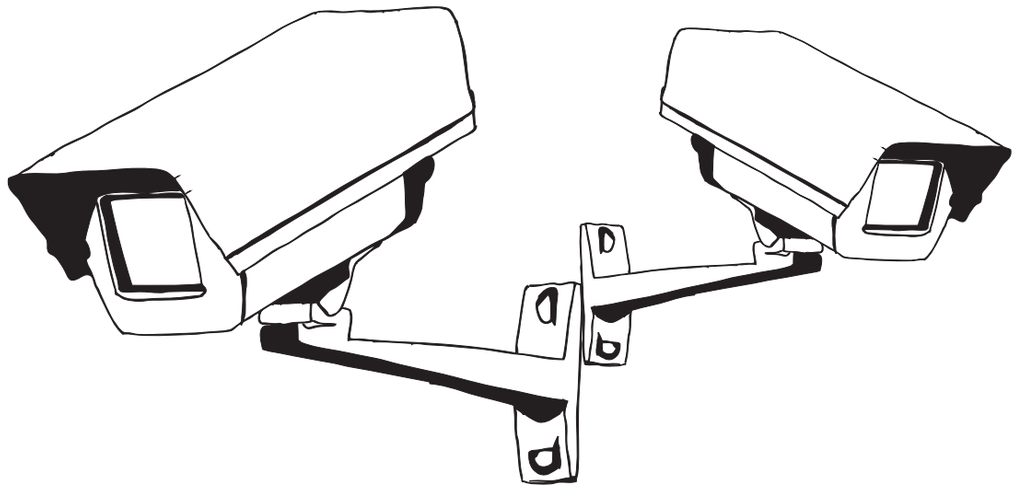
L'antivol à code que l'on peut voir sur cette image est fabriqué par la société BtwinCycle. On le trouve en masse à Decat'. Vu le prix (5€ le lot de 3), ce n'est pas la crème de la crème des antivols. Il est tout à la fois facile et rapide de découvrir son code à trois chiffres :

Comme on le voit sur la photo, l'antivol est composé de trois roulettes, une par chiffre à trouver. Soulève légèrement la première roulette et/ou fait pression dessus de façon à ce qu'elle soit collée à une des deux parois. Une fois cela fait, regarde vers l'intérieur du cadenas en faisant tourner la roulette tout en maintenant la pression, de manière à voir un trou de forme rectangulaire. Prends un marqueur et fait une petite marque sur la tranche de la roulette, au dessus de ce trou.

Répète cette opération pour les deux autres roulettes.
Enfin, place les roulettes de façon à ce que chacun de ces points soit dirigés vers le bas. Tire les deux bouts de l'antivol dans une direction opposée, ils se sépareront : l'antivol est ouvert.

Une autre technique utile pour ce genre d'antivol, ou pour des cadenas à code bon marché, fait appel à ta seule sensibilité et dextérité, sans la vue. Pendant l'opération, tu exerces une pression constante sur l'antivol (ou la hanse, si c'est un cadenas), comme si tu voulais l'ouvrir. En même temps, tu tournes doucement la première roulette, jusqu'à ce que tu sentes et/ou entende un clic. Cette roulette est bien positionnée. Reste à faire de même pour chaque roulette, jusqu'à ce que l'antivol ou le cadenas s'ouvre.

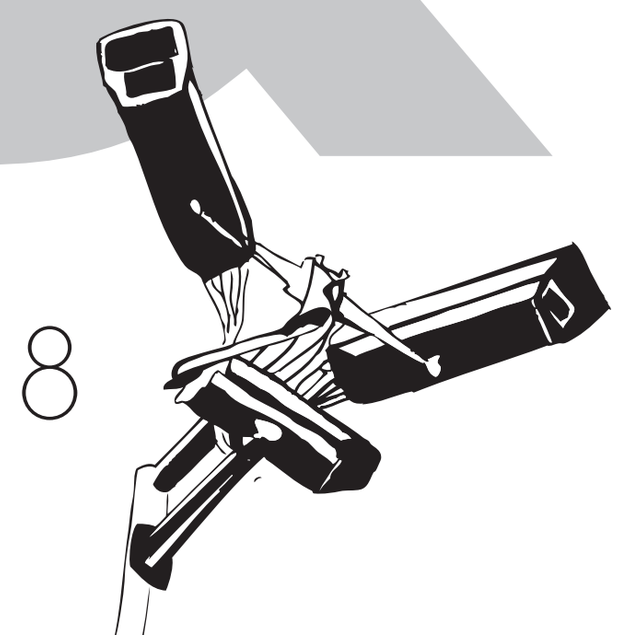
Caméras de sécurité vidéo-surveillance



600 000 en France. Publiques et privées confondues. Même les plus petits villages s'y mettent. Alors, pour ceux qui sont pas assez chauds de la cagoule pour les attaquer en mode commando de nuit, *RESTE À LES PIRATER*.

Nous nous concentrerons ici sur les caméras de surveillance reliées au Net. Les caméras IP. Étant connectées au réseau internet, elles sont forcément vulnérables aux attaques. On ne s'attardera pas sur leur fonctionnement*. Abordons d'emblée l'astuce**.

Google inclus une grande part des caméras IP dans son moteur de recherche. En tapant ces recherches dans Google — révélation — nous avons accès à des centaines de caméras de vidéo- surveillance :



```
inurl:/view.shtml
intitle:"Live View / - AXIS" | inurl:view/view.shtml^
inurl:ViewerFrame?Mode=3DRefresh
inurl:axis-cgi/jpg
inurl:axis-cgi/mjpg
inurl:view/indexFrame.shtml
inurl:view/index.shtml
inurl:view/view.shtml
liveapplet
intitle:"live view" intitle:axis
intitle:liveapplet
allintitle:"Network Camera NetworkCamera"
intitle:axis intitle:"video server"
intitle:liveapplet inurl:LvAppl
intitle:"EvoCam" inurl:"webcam.html"
intitle:"Live NetSnap Cam-Server feed"
intitle:"Live View / - AXIS"
intitle:"Live View / - AXIS 206M"
intitle:"Live View / - AXIS 206W"
intitle:"Live View / - AXIS 210"
inurl:indexFrame.shtml Axis
inurl:"MultiCameraFrame?Mode=3DMotion"
intitle:start inurl:cgistart
intitle:"WJ-NT104 Main Page"
intext:"MOBOTIX M1" intext:"Open Menu"
intext:"MOBOTIX M10" intext:"Open Menu"
intext:"MOBOTIX D10" intext:"Open Menu"
intitle:snc-z20 inurl:home/
intitle:snc-cs3 inurl:home/
intitle:snc-rz30 inurl:home/
intitle:"sony network camera snc-p1"
intitle:"sony network camera snc-m1"
site:.viewnetcam.com -www.viewnetcam.com
intitle:"Toshiba Network Camera" user login
intitle:"netcam live image"
intitle:"i-Catcher Console - Web Monitor"
```

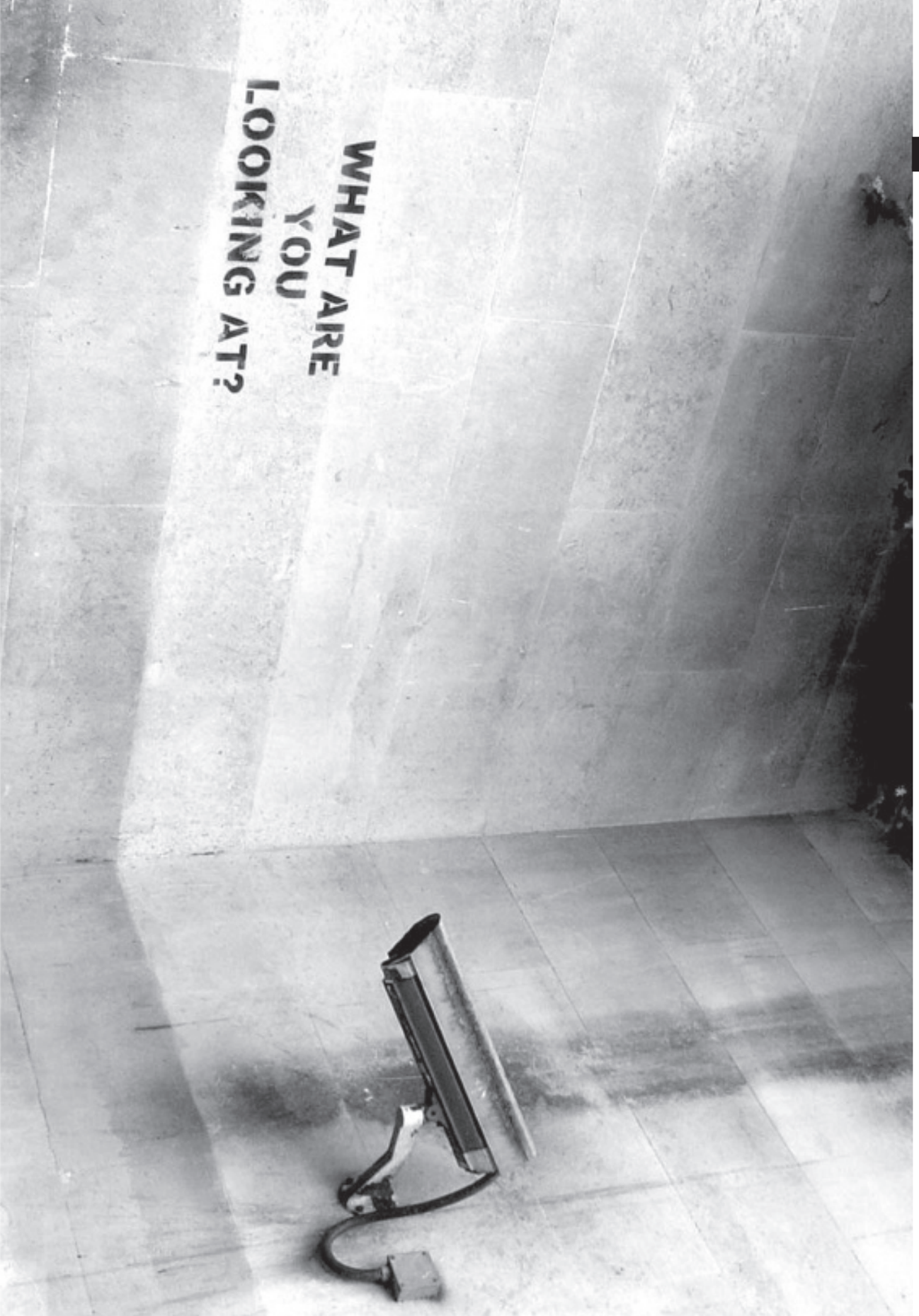
Te voilà surveillant de maison ou d'université en deux clics. Certains internautes sont tombés sur des caméras de sécurité de bases militaires…
Si tu désires te connecter sur un système particulier, une cible bien prédéfinie, il te faut trouver l'IP de l'objectif en question, et essayer de combiner son ip avec, par exemple, pour la première requête citée plus haut, /view.shtml. C'est à dire qu'en tapant la première requête dans Google, vous tomberez sur des adresses de type :
http://xx.xx.xx.xx/view.shtml
Où les «x» correspondent à l'adresse IP. Met alors l'adresse IP de la cible à la place de l'adresse trouvée via Google — et réitère cette opération avec toutes les requêtes…

Il te sera peut-être demandé un identifiant et un mot de passe. Pour certaines caméras, le mot de passe et l'identifiant de connexion sont par défaut. Et, grâce à la fainéantise des administrateurs réseau, merci, il sont très rarement modifiés! Pour exemple : la plupart des caméras de marque AXIS ont pour identifiant : root et pour mot de passe : pass .***
Après, une fois administrateur, fais-toi plaisir.

* ***De nombreux sites expliquent simplement le fonctionnement des caméras sur IP. Entre autres : http://www.europ-computer.com/dossiers/dossier_2_2.html***

** ***A souligner tout de même que toutes autres sortes d'attaques sont imaginables : les Anonymous ont fait leur les attaques DDOS. Il est envisageable de faire effondrer tout un réseau de caméras avec cette technique.***

*** **Pour connaître quels sont les identifiants et les mots de passe pour un système en particulier : le site http://www.cirt.net/passwords en propose une ribambelle. Beaucoup d'autres sites, après de brèves recherches, proposent de la même manière des listing des identifiants et mots de passe par défaut, triés par constructeurs. En dernier recours, tu peux faire tes recherches via ce genre de requête : «default pass toshiba ik», pour trouver les mots de passe par défaut des caméras IP de la marque Toshiba, type IK.**



Petit cours introductif sur les alarmes

Ce texte a pour but de te familiariser aux systèmes d'alarmes domestiques et de t'apprendre quelques techniques permettant de les contourner. Un maximum de pistes y sont avancées, sans la prétention de l'exhaustivité.
Il y a actuellement quatre voies pour s'attaquer à une alarme. La centrale, le câblage, les détecteurs, et, enfin, les avertisseurs.
Let's start!

1 • LA CENTRALE

La centrale d'alarme est le boîtier depuis lequel tout le système d'alarme est dirigé. C'est à elle que sont reliés les détecteurs, les avertisseurs, c'est elle qui contrôle le temporisateur, le composeur de numéros... Il existe différents modèles de systèmes d'alarmes, certaines possèdent plus d'options, certaines sont plus robustes...

<1>Notion de Zones

La très grande majorité des centrales aujourd'hui disposent de «contrôleurs» de zones. Une zone est en fait une entrée, sur la centrale, d'un groupement de capteurs. Cela permet de définir des zones géographiques avec les capteurs, et ainsi d'avoir soit la possibilité de pouvoir activer que certaines pièces de la maison, soit celle de pouvoir localiser plus aisément la provenance d'une intrusion. Les zones peuvent aussi servir à grouper les détecteurs en fonction de leur types (périmétriques, volumétriques, NC, NO...)

<2>Les entrées 24 Heures

Les entrées 24 heures sont des entrées, au niveau de la centrale, sur lesquelles seront raccordés les dispositifs de détection qui doivent rester en marche en permanence (tel que les détecteur incendies, les détecteurs de fumées...).
Mais elles peuvent également servir à raccorder les boucles d'auto-protection. *(voir § sur le câblage)*.

<3>Les temporisateurs

Les temporisateurs sont des dispositifs qui permettent de déterminer une durée. Dans une centrale d'alarme il peut exister deux types de temporisateurs :

Les temporisateurs d'entrées

Ces temporisateurs permettent d'avoir le temps de rentrer dans le bâtiment et de désactiver l'alarme (majoritairement par le biais d'un clavier digicode) mais également d'en sortir une fois l'alarme activée. Ainsi pendant une durée de temps prédéfinie par le propriétaire la zone pour rejoindre la centrale ne réagira pas aux intrusions. Attention cependant, il se peut que se temporisateur ne soit programmé que pour «désactiver» une zone particulière (de manière logique l'entrée du bâtiment).

Les temporisateurs d'avertisseurs.

Ceux la sont ceux qui vont définir le temps durant lequel les avertisseurs (sirène,voyants lumineux...) seront activés si une effraction est constatée.

<4>Interrupteur panique

L'interrupteur panique permet d'activer les avertisseurs manuellement même si aucune détection n'a été faite.

<5>Tamper

Le tamper est une sorte d'interrupteur placé dans certaines centrales (ainsi que dans certains détecteurs comme nous allons le voir plus tard) qui «protège» le boîtier de la centrale si quelqu'un essaye de le forcer. En gros tu tapes au marteau sur la centrale et y'a des chances pour que l'alarme te pète les oreilles.

<6> L'alimentation / Les batteries tampons

Les centrales d'alarmes vont fournir l'énergie nécessaire au fonctionnement de tout les détecteurs et des avertisseurs qui y sont reliés (sauf dans le cas particulier des centrales à ondes radios). Elles sont reliées au secteur (230V). Seulement, pour prévenir des pannes Edf ou d'un coupage de ligne volontaire, elles sont souvent équipées de batteries qui permettent de faire «tampon». Ainsi, même si le courant est coupé les batteries pourront prendre le relais. Cependant ce type de batteries coûte cher (en entretien également) et peuvent donc parfois ne pas être incluses dans certains kits de système d'alarmes.
On peut toujours couper l'alimentation et attendre que la batterie soit vidée pour entrer en action. Une prise d'information sur le type de batterie qui est installée est alors utile. A savoir que certaines batteries ont des capacités d'alimentation de plusieurs dizaines d'heures... On pourrait du coup imaginer de brancher sur la centrale un dispositif qui consomme beaucoup d'énergie, pour que la batterie se vide rapidement si l'alimentation est débranchée. Ou bien plus simplement, si l'on a accès à la centrale en journée, enlever la pile. La coupure d'électricité s'envisagera plus sereinement.

<7> Le cas particulier des centrales à liaison radio

Afin de simplifier l'installation et de prévenir contre les risques d'attaques contre le câblage, certaines alarmes fonctionnent avec les détecteurs par liaison radio. Elles communiquent par un canal codé. Lorsque un détecteur s'active alors il se met à émettre vers la centrale.

Cependant il existe une faille à ce type d'alarmes. Pour peu qu'un intrus puisse atteindre la centrale d'alarme sans se faire repérer alors il pourra faire une cage de faraday * autour d'elle. Elle ne pourra ainsi plus recevoir d'infos depuis les détecteurs. A ajouter, et à prendre comme piste : les détecteurs, dans ce type de système, fonctionnent avec des piles ou des accus, il se peut donc que certains n'aient plus assez de batterie et/ou soient inactifs.

<8> Composeur téléphonique

Le composeur téléphonique a pour rôle de composer un numéro en cas de détection et de diffuser lorsque l'autre ligne décroche soit un message sonore soit un enregistrement préalablement enregistré (tout dépend du modèle de la centrale). Il rappellera tant que la ligne qu'il appelle n'aura pas décroché. Certaines centrales permettent d'enregistrer plusieurs numéros : si un ne répond pas alors elle appellera le suivant. Sachez toutefois que les composeurs téléphoniques n'appellent pas les condés : ce serait tout de même assez con qu'ils se déplacent pour chaque fausse alerte.

Qui donc que ça appelle alors ?
•• Soit le propriétaire a soumis un abonnement à une compagnie privée de surveillance. Auquel cas ce sera cette compagnie qui sera contactée.
•• Soit ça appelle un voisin, ou quelqu'un qui a la possibilité d'arriver sur les lieux assez vite pour faire une vérification. Il y a ici fort à parier que cette personne appellera à son tour les flics...

Pour mettre à mal les composeurs, il suffit de débrancher ou de couper la ligne téléphonique au niveau des répartiteurs téléphoniques **.

<9> Les clés de commande à distance

Par clé j'entends également l'ensemble des dispositifs de type digicode. Ces clés de commande à distance permettent de désactiver l'alarme depuis l'extérieur du bâtiment, pour ne pas avoir à mettre en place de temporisateur.
Difficile de trouver des parades clefs-en-main. Peut-être des pistes : Si la clé est de type digicode, la technique du talc qui saupoudre les touches (pour découvrir lesquelles sont utilisées) est envisageable. Restera à trouver l'ordre des chiffres***.
La clé peut être une serrure cylindrique. En cette situation le crochetage reste la voie la plus certaine****. Enfin nous pourrions envisager de pirater la liaison, en envoyant un faux message de désactivation de l'alarme.*****

<10> Les entrées NC et NO

Les entrées dites NC et NO sont les entrées (au niveau de la centrale) sur lesquelles sont branchés les détecteurs.
•• NC signifie Normaly Closed : ce seront donc les détecteurs fermant le circuit qui y seront branchés. Si le détecteur se déclenche, il ouvre le circuit et l'alarme se déclenche.
•• NO signifie Normaly Open : ils ferment le circuit lorsqu'ils détectent une intrusion.

* *Une cage de Faraday est une enceinte utilisée pour protéger des nuisances électrique et électromagnétiques. Elles sont utilisés souvent en électronique, pour effectuer des mesure précises.*
Plus concrètement, lorsque tu enveloppes d'aluminium un antivol de vêtement ; ou lorsque, à l'intérieur de ton sac, tu couds une doublure avec un sac isotherme, les portiques antivols ne sonnent pas : tu as fabriqué une cage de Faraday. Pour la centrale à ondes radios, on peut tout a fait envisager de la recouvrir d'aluminium sur plusieurs couches.

** *Ce sont soit, les vieilles armoires vertes qui se trouvent dans les rues, avec marqué PTT dessus ; soit des petits boîtiers blanc ou gris, à deux mètres de hauteur, sur les façades des maisons ou sur des poteaux électriques.*

*** *Dans le prochain numéro sera détaillée une technique permettant de trouver le plus rapidement possible des codes PIN (Personal Identifiant Number. Mot de passe à chiffres... à ne pas confondre avec le code PIN des cartes SIM).*

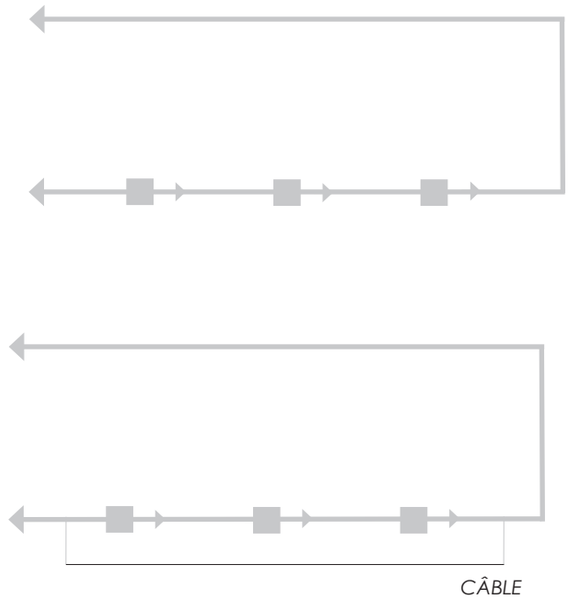
**** *Pour le crochetage des serrures tubulaires, voir dernier article.*

***** *Au regard du niveau de technicité de cette pratique, nous ne la développerons pas ici.*

2 • LE CÂBLAGE

Revenons rapidement sur sur les notions de NC et NO :

NC : Normaly Closed. Ce type de détecteurs, puisqu'il déclenche l'alarme quand il ouvre le circuit, se branche en série. On obtient schématiquement un circuit comme on le voit sur le schéma :

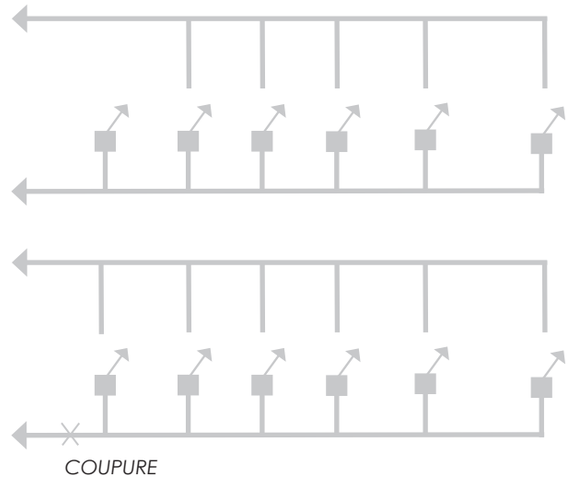


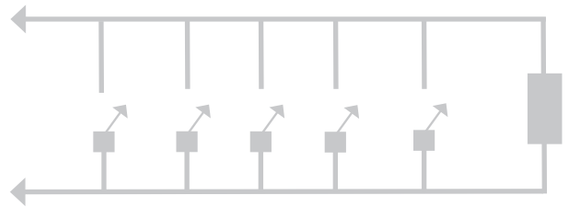
Les plus malins auront donc remarqué qu'en branchant un câble contournant les détecteurs, on rend ces derniers totalement inutiles.

NO : Normaly Open signifie qu'en position normale le courant ne passe pas sur le circuit, seulement lorsque un détecteur s'enclenche. Les circuits de ce type sont donc en parallèle. Schématiquement ça donne :

Mais là encore, il suffira de couper un câble pour désactiver tout les détecteurs se situant après.

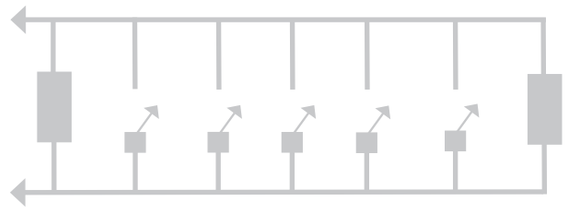
Schématiquement, ça donne les deux schémas ci-contre :





Alors à ce moment la on se dit que les NO sont plus faciles à désactiver que les NC. Hélas tout n'est pas si simple. Il est en effet possible que le système d'alarme possède des dispositifs afin de contrer ces méthodes.

Boucle à impédance fixe :
Les boucles à impédance fixe sont des circuits sur lesquels une résistance de valeur fixe est placée en bout. La centrale mesure cette impédance, et si elle change alors elle déclenche l'alarme. Regardons schématiquement ce que ça donne sur un système NO:



Comme vous pouvez le voir la boucle du système est fermée mais avec une résistance. Si vous tentez de couper le câblage alors il n'y aura plus de courant du tout. Si en théorie tu peux faire quelque chose pour parer à se problème, la pratique reste plus compliquée. Le moyen qui semble être le plus simple est de créer une dérivation à la base de la boucle, dérivation qui possède une impédance identique, puis ensuite de couper le câble.

Le problème étant de connaître au préalable l'impédance de la boucle. Petit point positif cependant : ce type de boucle à impédance fixe n'est pas disponible sur de nombreuses centrales...

Les boucles d'auto protection :
Ces boucles sont en fait un câble qui est ajouté à ceux déjà présents. Il sera en permanence parcouru de courant et relié à une entrée 24 heures. L'intérêt est que si quelqu'un essaye de couper le câble alors l'alarme se déclenche. Il ajoute donc une difficulté lors d'une tentative de dérivation.

petit cours introductif sur les alarmes

3 • LES DÉTECTEURS

< 1 > Détecteurs périmétriques

Les détecteurs périmétriques surveillent un point ou une ligne, et non un volume. Si il y en a quelque part ils devraient se situer sur les portes, les fenêtres, parfois sous les tapis.

Détecteurs d'ouverture :

Ce sont bien évidement les plus courants. Les modèles les plus utilisés sont ceux à lame souple (ILS). Leur principe est simple : deux fines lames conductrices sont enfermées dans une ampoule. Le tout enfermé dans un bloc de plastique. Vient ensuite une deuxième partie, qui n'est rien d'autre qu'un aimant. Lorsque la porte ou la fenêtre est ouverte, l'alarme se déclenche car l'aimant ouvre le circuit. Ces détecteurs peuvent être mis hors service en utilisant un deuxième aimant afin que les lames souples ne bougent pas. Cela dit, méfiance : des modèles à encastrer dans les montants existent, et sont dans ce cas peu visibles, voire carrément invisibles.

Détecteurs de chocs :

Ils servent à détecter les chocs (et les bris de vitre) pouvant être à l'origine d'une tentative d'intrusion. Il existe pas mal de modèles différents se basant sur différentes technologies. Malheureusement pas grand chose à ajouter, si ce n'est d'éviter de faire des chocs.

< 2 > Détecteurs volumétriques

Détecteurs à infrarouge passifs (IRP):

C'est aujourd'hui les plus courants. L'infrarouge va détecter toutes les variations fortes de température. En gros si tu marches devant, ta température corporelle déclenche l'alarme. Afin de définir l'angle et la vision, le capteur est équipé de lentilles. Ces lentilles (dites lentilles de Fresnel) permettent d'adapter le capteur pour que son champ d'action soit fonction de la pièce : le champ de détection sera faible si le capteur est posé au bout d'un couloir. Certains IRP sont parfois équipés de décompteurs. En gros il vont déclencher l'alarme que s'ils voient deux fois une source de chaleur en un certain temps. Ça permet parfois de pas déclencher lorsque un chien passe devant, ou bien plus simplement d'éviter les fausses alertes. Aussi, certains ont une protection du boîtier (tamper) qui signale toute tentative de forçage... Bien que leur contournement paraisse difficile, il faut noter que ce sont des système très peu sensibles aux variations lentes de chaleur. Il est donc possible de ne pas déclencher l'alarme en passant lentement...

******

Détecteurs hyperfréquence :

Juste histoire de les mentionner. En gros ils ont un peu le principe d'un radar ; ils utilisent l'effet Doppler. Ils coûtent relativement cher donc ils sont surtout sur les bâtiments considérés comme sensibles . Bref, faisons court : ces détecteurs sont blazants. Point intéressant cependant : la plupart des alarmes, du moins celles à bas-coût, n'ont, comme détecteurs, que des ILS et/ou des infrarouges.

******

En tapant « Myth Buster Motion Sensor » dans google vidéo, tu tombes sur une émission-à- la-con américaine (Myth Buster), diffusée sur discovery channel, qui se fixe pour objectif de démonter somme de légendes urbaines. Ici, deux techniques fonctionnent pour contourner un détecteur volumétrique : celle de passer très lentement (en considérant que le détecteur est dans une pièce de passage, un couloir par exemple, et que l'objectif est dans une pièce sans détecteur volumétrique) ; et celle de passer dans la pièce en se cachant derrière un drap, qui est tenu tendu à bout de bras...

petit cours introductif sur les alarmes

4 • LES AVERTISSEURS

Son et lumière résumeraient bien l'esprit. Ce sera les deux types d'avertisseurs présents sur une centrale d'alarme. La seule chose à savoir est la suivante :

•• Soit l'avertisseur est branché sur la centrale sans pour autant disposer de capacité tampon en énergie. En ce cas, il suffit de couper le câble.

•• Soit il dispose d'une batterie. Alors il faudra bien faire attention de tout foutre en l'air en même temps, histoire qu'il ne parte pas sur sa réserve.

Le conseil-à-la-bien : il va de soi qu'il sera toujours préférable de prendre des informations sur la marque et les capacités de l'alarme avant de passer à l'action.

Pour neutraliser les avertisseurs, plusieurs voies sont possibles. Déjà, si des avertisseurs sont présents à l'extérieur, tu peux soit l'arracher comme un bourrin et le plonger dans un sceau d'eau, ou, s'il est protégé et/ou bien fixé, une bombe de peinture noire cachera la lumière rouge, pendant que de la mousse expansive bien appliquée réduira considérablement les décibels de la bêbête. Plus facile encore, couper simplement les câbles s'ils sont apparents. Évidemment, tout ceci après avoir neutralisé la ligne téléphonique.

UE* Report :

Palais de justice de Bruxelles

UE, comme Urban Exploration (et pas Union Européenne...)

Ah, la Belgique!

Je me rappelle très bien la première fois que je suis allé à Bruxelles. La copine qui me faisait visiter la ville m'avait emmené sur un des points les plus élevés, avec une vue imprenable du haut de la colline sur la ville. Le temps n'était pas terrible et pour tout dire, je me moquais un peu de la vue, car à ma gauche, il y avait un échafaudage sur le plus beau bâtiment de Bruxelles : *Le palais de justice de Bruxelles.*

Il faut dire que cet édifice en impose. Il est tout simplement gigantesque et nombreuses sont les légendes à son sujet.

L'échafaudage est tout frais, il faut en profiter, certaines statues ne sont pas encore masquées par les poutres Je décide donc d'y aller la nuit (bien entendu), habillé de gris. La palissade se passe facilement, comme souvent, grâce aux profils non linéaires des murs, plutôt difficiles à coller. Ce premier échafaudage est plutôt basique. Une succession d'échelles permet d'accéder aux premières statues. Enfin presque. Il manque quelques mètres. Ça devient une habitude, j'en démonte une partie pour la remonter ailleurs. Voilà, j'y suis : la première statue. Je dois dire qu'être déjà à ce niveau sur l'édifice me gonfle de joie. On parle d'un palais de justice! Et il est beau. Belge, certes, certains s'en sont enfuis, mais un palais de justice quand même! Quelques photos faites, je continue en direction du deuxième échafaudage. Celui qui enrobe la tour principale et donne accès au dôme. L'ascension est toujours aussi facile, doublée de silence, l'échafaudage étant garni de planches. Ça me change des français, métalliques et souvent grinçants. Photos sur le dôme, photos sur les statues (notamment celle qui tient les tables de la loi, je m'assieds dessus, bien entendu!).

Reste à entrer dedans!

...certains s'en sont enfuis...

Ah tiens, une fenêtre mal fermée.

Une bonne pression, elle s'ouvre toute seule, le loquet en haut et en bas n'était pas enclenché. L'aubaine! La salle est assez mystérieuse, toute bleue, avec des arches en forme de pétales et un grand trou au milieu de la pièce. Y a pas à dire, c'est beau! Je peux aller partout ou presque, quelques portes récalcitrantes s'ouvrant (comme dans les films, c'est magique) grâce à une carte en plastique. La sécurité, c'est un métier.

Entre escaliers, colonnes et vue imprenable sur la cour des pas, l'heure tourne. Il faut rentrer, surtout que je ne sais toujours pas si un gardien traîne dans les parages. Je prends donc le chemin inverse ou presque pour descendre, referme tout derrière moi et me dirige vers la station de métro Louisa pour prendre un taxi. Il est 3h du matin. J'entends crier «Édouard» de l'autre côté de la rue.

Des amis qui reviennent d'une soirée. Nous rentrons ensemble, le temps de raconter quelques anecdotes. Le lendemain, je retournais de jour, officiellement, à l'intérieur du palais. Vue inhabituelle car pour une fois, j'étais en bas.

RÉCUPÉRER ET FALSIFIER DES EMPREINTES DIGITALES

• PART I •

Récupérer des empreintes digitales sur un objet.

Pour faire les tests, il est préférable d'utiliser une empreinte digitale déposée sur une bouteille en verre. De manière générale, une bonne source d'empreintes pour nos contrefaçons sont les verres, les poignées de porte, ou tout support lisse. Deux solutions s'offrent à toi pour faire ressortir les empreintes :

1.LA SOLUTION DES CONDÉS SCIENTIFIQUES

Il te faut l'espèce de petit pinceau qui sert à badigeonner la surface où l'empreinte est déposée.
Et de la poudre, qui se fixera sur les matières organiques. Pour le pinceau, un pinceau à maquillage fait l'affaire. Pour la poudre, en théorie, on utilise de la poudre noire pour les surface blanches, et de la poudre blanche, à base d'aluminium, pour les surfasses lisses (bois, verre, mur, etc.). En réalité, la poudre noire peut s'utiliser dans toutes les situations, et est plus facile à fabriquer.

Une fois que tu as badigeonné l'empreinte de poudre et qu'elle est bien ressortie, tu colles un morceau de gros scotch transparent dessus, en tentant de l'appliquer bien uniformément sur l'empreinte, sans former de bulles. Puis tu le décolles, pour enfin le recoller sur une feuille de papier blanc. Ainsi l'empreinte peut être prise en photo ou scannée facilement, avec des contrastes déjà bien mis en valeur.

2. LA SOLUTION SUR LE POUCE

Cette technique exploite les propriétés du cyanoacrylat, le produit principal de la superglue. Les vapeurs du cyanoacrylat (d'ailleurs fais belek : les vapeurs sont bien toxiques) se fixent sur le gras ou la sueur qui composent l'empreinte. Tu mets l'équivalent d'un tube de superglue dans un bouchon de bouteille, et tu mets l'endroit de l'objet où l'empreinte doit se révéler au dessus du bouchon. Il faut que le bouchon touche l'objet, et qu'il y ait le moins possible de fuites, pour que les vapeurs restent presque enfermées dans le bouchon. Au bout d'une dizaine de minutes, les vapeurs du cyanoacrylat vont se déposer sur la surface et vont faire ressortir l'empreinte en blanc.

FABRIQUER DE LA POUDRE NOIRE DE CARBONE

Récupérer les mines d'un crayon de papier en le découpant avec un cutter, puis les écraser dans un pilon, jusqu'à l'obtention d'une poudre noir très fine.

LES MAGASINS JOUET CLUB

offrent des sortes de kits de la police scientifique pour les moins de 8 ans. Il n'empêche que leur base de matériel, dont le pinceau et la poudre, sont tout à fait concluants. Usez du double fond de votre sac : ils osent vendre ça une bonne trentaine d'euros.

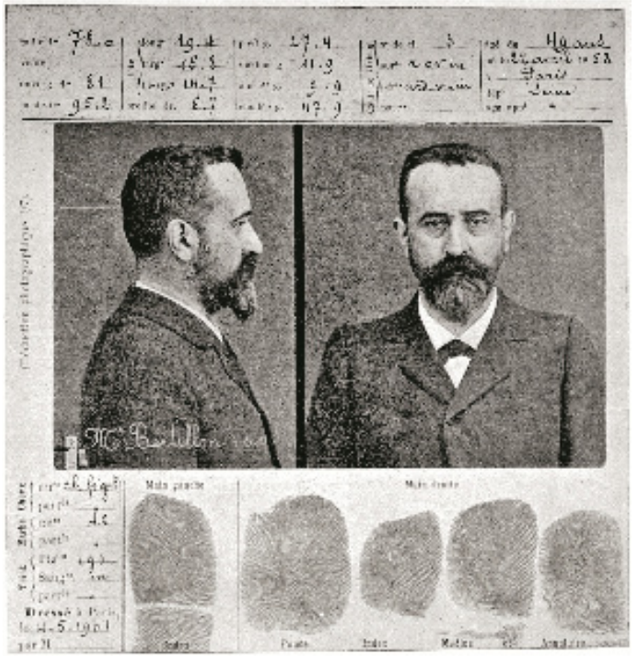
PART II

Falsifier des empreintes digitales

Une fois l'empreinte mise en valeur, prends la en photo avec un appareil photo numérique. Importe-là dans ton ordi, et traite la avec un logiciel de traitement d'image, de manière à faire ressortir au maximum l'empreinte digitale*.

L'idée, ensuite, est de créer un moule transparent de l'empreinte à coller sur les doigts. L'image traitée, et dont le contraste est inversée pour créer le négatif — le moule—, doit être imprimée sur une glissière de transparent. Ces transparents utilisée pour les rétroprojecteurs. Évidemment, de la même manière qu'il aura fallu un appareil numérique avec une assez bonne résolution pour la photo de l'empreinte, il faudra ici une imprimante laser de bonne qualité. L'avantage de l'imprimante laser étant qu'elle permet d'avoir du relief lorsqu'on imprime sur un transparent…
Puis, versez un boudin de colle à bois en tube, à la base de l'empreinte, avant de l'étaler harmonieusement, grâce à un stylo bien rond. Après que la colle ait séchée (quand elle est transparente), elle est retirée délicatement pour pas la déformer, et est coupée à la taille du doigt. Ne reste plus, enfin, qu'à coller cette fausse empreinte sur le doigt grâce à du vernis à ongle.

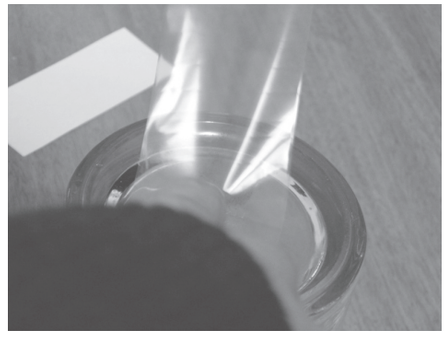
Voilà de quoi usurper de nombreuses identités...
À VOS MASQUES, PRÊT, PARTEZ !



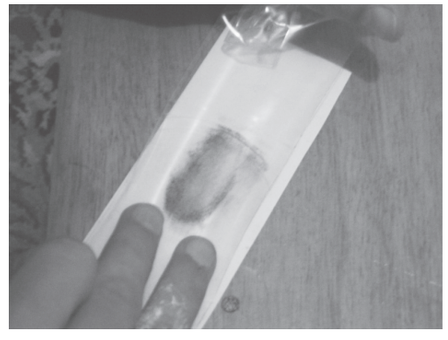
* **Pour le traitement de l'image, la procédure exacte n'est pas détaillée dans la mesure où elle diffère selon le logiciel utilisé. En revanche, voici quelques indications. La première des choses est de passer l'image en noir et blanc. Ensuite tu pousse les contrastes à leur maximum, pour que l'empreinte soit le mieux dessinée possible ; qu'il ne reste quasiment plus de parties plus ou moins grises. Et enfin, tu inverse les contrastes : le blanc devient noir, et le noir devient blanc. En effet, ce que tu vas imprimer sur le transparent sera un moule, et doit donc être le négatif de l'empreinte.**

Avec fausse CNI, faux passeports, fausses empreintes, vous voilà bien armés.
Rafale #4

1 ▪ La surface où l'empreinte est déposée est saupoudrée de poudre noire. Avec un pinceau fin et souple, l'excès de poudre est éliminé.



2 ▪ Du gros scotch transparent est apposé sur l'empreinte, en évitant de faire des bulles ; puis et retiré...



3 ▪ ... pour être ensuite redéposé sur du papier blanc : le contraste est idéal pour être pris en photo ou scanné.

4 ■ De la superglue est déposée dans un bouchon de bouteille.

5 ■ Ici, l'empreinte se trouve sur le cul du bocal. Le bocal est donc simplement posé sur le bouchon.

6 ■ La photo de l'empreinte prise avec un pied, pour n'avoir aucun flou. Il est conseillé de déposer derrière l'empreinte, de l'autre côté du verre, du papier noir, pour augmenter le contraste.

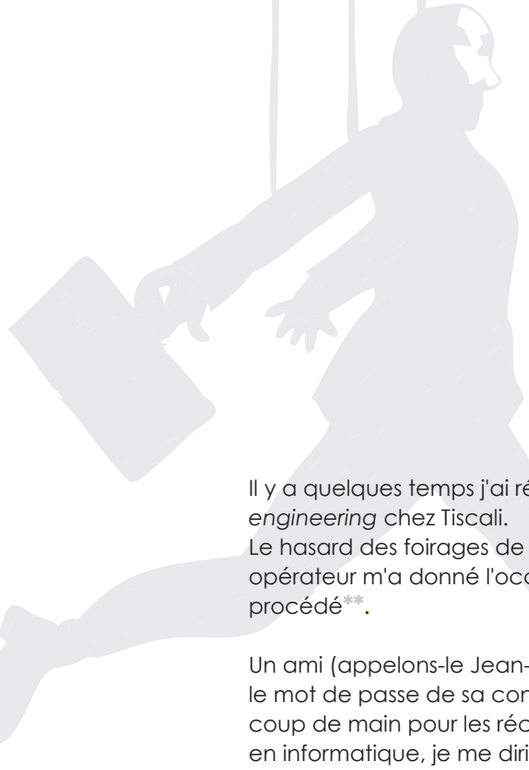
7 ■ L'empreinte prise en proto... il faudra bien la nettoyer sous un logiciel de traitement photo.

8 ■ Le traitement de l'empreinte sous Gimp.

9 ■ L'impression de l'empreinte depuis un imprimante laser, sur une feuille transparente de rétroprojecteur.

10 ■ De la colle à bois est déposée sur l'empreinte, en étalant une couche la plus fine et harmonieuse possible.

11 ■ Après séchage, la colle est transparente. Il suffit de la décoller sans l'étirer, de la découper à la taille du doigt, puis de la coller sur le doigt avec le vernis à ongle.



UN PEU DE *SE* CHEZ TISCALI SCARLET

Il y a quelques temps j'ai réussi à faire un gentil *social engineering* chez Tiscali.
Le hasard des foirages de connexion chez cet opérateur m'a donné l'occasion d'expérimenter ce procédé**.

Un ami (appelons-le Jean-Paul) avait perdu le login ET le mot de passe de sa connexion. Je voulais lui filer un coup de main pour les récupérer, mais, étant une brêle en informatique, je me dirige vers la hotline de Tiscali La connexion était au nom de son père (disons «Billy Bob»), je savais que sur ces vieux comptes de cet opérateur, le login était la première lettre du prénom, suivie des 3 premières lettres du nom de famille, suivies de 4 chiffres et, enfin, du @tiscali.be. Le sien, recomposé, devait donc être quelque chose comme BBob1234@tiscali.be.

On va voir ici comment j'ai finalement pu tout récupérer avec comme seuls outils : un nom, un prénom, un téléphone, une adresse et trois hotliners.

Voici la retranscription des trois appels. Je vous passe les détails de l'attente avec les petites musiques insupportables…

* **Le social engineering est une technique — un art de vivre, presque — d'acquisition déloyale d'informations, en exploitant les faille humaines et sociales de la structure cible. Longtemps utile au secteur de l'espionnage industriel, elle s'est démocratisée dans le mouvement hacker suite à la parution en 2002 du livre «** *L'art de la supercherie* **» de D.K. Mitnick.**

1er appel :

HOTLINER 1 : Bonjour, bienvenu chez Tiscali, que puis-je pour vous ?
MOI : Bonjour, j'ai perdu le login et le mot de passe de ma connexion, pouvez-vous m'aider SVP ?
HOTLINER 1 : Bien sûr, quel est votre login svp ?

(Commentaire : Bon déjà ça commençait bien, il comprenait que la moitié de ce que je lui demandais.)

MOI : Je l'ai perdu aussi.
HOTLINER 1 : Ah ! Et vous vous appelez ?
MOI : Et bien la connexion est au nom de mon père, Billy Bob.

(Commentaire : bien évidemment je mentais. Mais il fallait bien se mettre dans la peau de celui que j'incarnais.)

HOTLINER 1 : Hum... et vous avez perdu le login ET le mot de passe ??
MOI : Oui mais je crois que le login était BBob5768@tiscali.be... enfin il me semble...

(Commentaire : Il est important d'hésiter un peu dans cette dernière phrase comme si on essayait de se souvenir du login qu'on ne connaît pas.)

HOTLINER 1 : Votre login est BBob0785@tiscali.be. Je vais faire une demande pour vous envoyer votre mot de passe par la poste.

(Commentaire : Ça m'emmerdait par la poste, il le fallait tout de suite à mon pote...)

MOI : Mais j'en aurais besoin tout de suite, je dois recevoir des mails importants!
HOTLINER 1 : Désolé, c'est tout ce que je peux faire, ça arrivera d'ici 5 jours. Bonne journée!
MOI : Bon tant pis... bonne journée.

Après cette première conversation, j'avais donc pu récupéré le login complet, mais par la poste, c'est lent. Il me fallait donc retéléphoner, en espérant tomber sur un autre hotliner pour chopper le mot de passe.

> *Bonjour, bienvenu chez Tiscali que puis-je pour vous ?*

2ème appel :

HOTLINER 2 : Bonjour, bienvenu chez Tiscali, que puis-je pour vous ?
MOI : Bonjour, j'ai perdu le mot de passe de ma connexion, mon login est BBob0785@tiscali.be, pouvez-vous m'aider SVP ?
HOTLINER 2 : Oui bien sûr, puis-je avoir votre nom, prénom et date de naissance svp ?

(Commentaire : Merde, la date de naissance... je la connais pas)

MOI : En fait c'est au nom de mon père, son nom est Billy Bob, pour la date de naissance, je vais demander, un instant s'il vous plaît.
MOI À JEAN-PAUL : JP, c'est quoi la date de naissance du père ?
JP : Ah ben je sais pas... attends... non je sais pas.

(Commentaire : Ah le chien!)

M À HOTLINER 2 : Heu désolé je sais pas...
HOTLINER 2 : Mwai... votre adresse ?
MOI : 25 rue du chou ardent

(Commentaire : C'était la vraie adresse du pote)

HOTLINER 2 : Je ne peux pas vous donner le pass comme ça, désolé, vous ne vous souvenez vraiment pas du tout du pass ?
MOI : Non mais j'ai une liste avec des codes un peu partout, le mot de passe est peut-être dedans, vous pouvez me donner les 2/3 premiers caractères s'il vous plaît ?
HOTLINER 2 : Oui les deux premières lettres sont "aj".

(Commentaire : J'avais pas de liste bien sûr... Je fais alors semblant de chercher en froissant du papier...)

MOI : Ah ben non désolé... vous pouvez-pas me l'envoyer par la poste ?
HOTLINER 2 : Si, je vais faire une demande. Bonne journée...
MOI : Bonne journée.

Bon c'était le moment de faire le troisième essai, après ça j'abandonnerais. Je décidais de cracher direct toutes les infos que j'avais, en surjouant un type agacé et innocent :

3ème appel :

HOTLINER 3 : Bonjour, bienvenu chez Tiscali, que puis-je pour vous ?
MOI : Bonjour, j'ai perdu mon mot de passe chez vous, vous pouvez m'aider ? Je me souviens que les 2 premières lettres étaient "aj" mais sinon je sais plus.
HOTLINER 3 : Bien sûr, je peux avoir votre login svp ?
MOI : BBob0785@tiscali.be.
HOTLINER 3 : Nom et prénom ?
MOI : Billy Bob

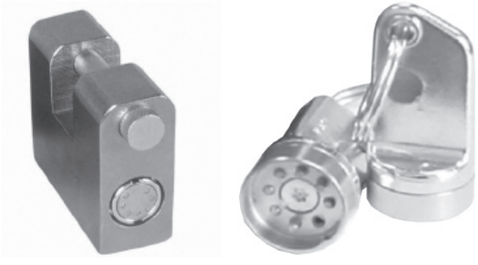
(Commentaire : Il cherche dans sa base de données...)

HOTLINER 3 : Vous dites que votre mot de passe commence par...
MOI : "aj" je pense...
HOTLINER 3 : C'est bien ça, votre mot de passe est le ajD85m3 .
MOI : Ah très bien merci beaucoup...
HOTLINER 3 : De rien, bonne journée.
MOI : Bonne journée à vous aussi!

Vanlock fuckfest

Hep! Pour cet article, j'ai réuni, pour vous chers lecteurs et lectrices fanatiques de crochetage de serrure, tous les éléments nécessaires pour être en mesure de déverrouiller les serrures Vanlock. Ces serrures servent à plusieurs applications de la vie courante, cadenas ou armoire haute sécurité, machine distributeur de sodas... Ce sont des serrures de type radiale (Radial pin tumbler). Le crochetage de ces serrures est différent de celui des serrures paracentriques classiques. Normal. Cela-dit, il repose sur l'exploitation des mêmes failles de la serrure : les minuscules irrégularités dans l'alignement des goupilles *.

Pour saisir la technique de crochetage, il est conseillé de comprendre le fonctionnement d'une serrure. Et pour ce faire, rien de mieux que le « Guide MIT de crochetage de serrure », chopable sur le net en deux clics.



Intéressons-nous à la manière de fabriquer une clef universelle pour ces serrures.

INGRÉDIENTS

◊ Deux gros trombones
◊ Une gomme à effacer
◊ Une pince coupante
◊ Une feuille de papier calque
◊ Un crayon de graffite ou un fusain

1 _ LA PRISE DE L'EMPREINTE

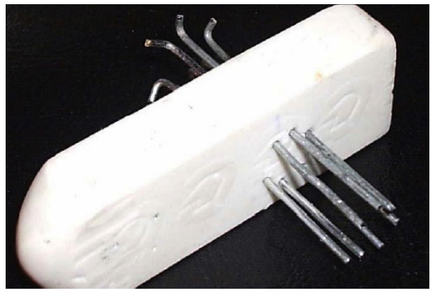
Cette étape est simplissime et te permettra d'obtenir les mesures exactes de la clef, par contre elle te demande de sortir sur le terrain et de prendre une emprunte au calque, c'est à dire prendre l'emprunte de la surface circulaire de la serrure. Il s'agit simplement d'appliquer le papier calque sur la surface de la serrure et d'agiter délicatement un crayon ou un fusain sur le papier afin de faire ressortir les traits circulaires émanant des goupilles et de la serrure elle même. Ce qui devrait donner ce qui suit ci-dessous.

2 _ LE TRANSFERT

Le transfert de l'emprunte consiste à faire apparaître l'emplacement des goupilles sur une gomme à effacer pour ensuite être en mesure de placer les tiges qui serviront pour la partie principale de notre clef magique. Cette étape ne consiste strictement qu'à perforer le papier, là où les marques des goupilles sont apparues lors du calque, sur la surface de la gomme afin de faire le marquage (transfert) du relevé que l'on a fait plus tôt.

3 _ L'ASSEMBLAGE

À ce stade-ci, nous avons obtenu, par le biais d'un duplicata de la surface d'une serrure suivi du transfert de l'emprunte recueilli, l'ébauche de ce qui sera notre gomme à effacer magique : la clef. Pour cette étape, redressez vos trombones de façon à les avoir bien droit, sans aucune irrégularité. Une fois redressés, coupez sept bouts de 5 centimètres. Maintenant, il ne reste qu'à enfoncer le plus verticalement possible les portions de trombones aux emplacements précédemment inscrits durant le transfert du calque. Et voilà, d'un coup de baguette, nous obtenons un objet mystérieux que l'on peut admirer, c'est notre clef :



4 _ L'OUVERTURE DE LA SER--RURE

Cet outil fonctionne de la même façon que ceux spécialement vendus pour crocheter les serrures radiales. Le coût démentiel en moins... Il suffit d'enfoncer chacune des broches, une par une, de jouer en sens horaire afin de profiter du lest mécanique des composantes de la serrure pour ensuite être en mesure de déverrouiller le dispositif.
Après quelques utilisations, tu remarqueras que la gomme se fissure. On peut imaginer le même système avec un matériau plus rigide, comme du PVC ou du liège.

FIN DU N°1

RAFALE est du côté de Bonnie and Clyde.
RAFALE n'aime pas le management.
RAFALE te souffle à l'oreille le chemin de la porte de sortie.
RAFALE défonce les murs en crépi avec son front.
RAFALE aime les écarts, les interstices et les failles.
RAFALE n'aime pas les poucav et les insignes.
RAFALE lime des passes-partout dans une cave.
RAFALE séquestre le DRH avec couteau-suisse et cure-dent...
RAFALE est de ces honnêtes bagarreurs qui dégueulent sur le trottoir, la tête haute.
En somme, et c'est bien là la moindre des choses, si tu ne portes ni képi ni casque homologué sur ton booster, RAFALE est de ton côté.

FIN DU N°1

RAFALE est du côté de Bonnie and Clyde.
RAFALE n'aime pas le management.
RAFALE te souffle à l'oreille le chemin de la porte de sortie.
RAFALE défonce les murs en crépi avec son front.
RAFALE aime les écarts, les interstices et les failles.
RAFALE n'aime pas les poucav et les insignes.
RAFALE lime des passes-partout dans une cave.
RAFALE séquestre le DRH avec couteau-suisse et cure-dent...
RAFALE est de ces honnêtes bagarreurs qui dégueulent sur le trottoir, la tête haute.
En somme, et c'est bien là la moindre des choses, si tu ne portes ni képi ni casque homologué sur ton booster, RAFALE est de ton côté.

POUR CONTACTER "RAFALE VERSION PAPIER"
rafale-papier@riseup.net

CHACUN SA ROUTE, CHACUN SON CHEMIN, PASSE LE ZINE À TON VOISIN

2€