" Au milieu d' une petite rue, stationne une camionette a vitres teintees. A l' interieur, une antenne pointe vers le ciel. Elle est dirigee vers la fenetre du bureau situe au troisieme etage d' un immeuble. L' ingenieur redigeant sa strategie prochainement mise en oeuvre contre ses concurrents ne se doute de rien. Ce qui s' affiche sur son ecran est en cours de capture, reproduit et enregistre dans le van qui se trouve a quelques metres plus bas . . . "

I- GENERALITES

1. Signaux parasites

Tout matériel ou système qui traite ou transmet, sous forme électrique, des informations est sensible à des perturbations électromagnétiques temporaires. Ces perturbations, qualifiées de signaux parasites, sont provoquées par les variations du régime électrique, dans les différents circuits du matériel considéré durant son fonctionnement.

Généralement les signaux parasites se manifestent sous la forme :

- d'ondes électromagnétiques qui se propagent par rayonnement dans l'espace environnant ;
- de courants de conduction qui se propagent le long des différents conducteurs reliés au matériel concerné.

La plupart du temps, il y a interaction des deux modes de propagation. Les perturbations rayonnées provoquent des courants induits dans les conducteurs reliés au matériel ou situés dans son voisinage tels que les lignes d'alimentation, les lignes de transmission ou d'autres conducteurs (canalisation de chauffage, tuyau d'eau, fer à béton, etc...).

De même, un conducteur non blindé qui véhicule des perturbations peut se comporter en antenne émettrice et, rayonne à son tour des parasites dans l'espace environnant.

Parmi l'ensemble des signaux parasites générés durant le fonctionnement des matériels, il en existe qui sont représentatifs des informations traitées. Leur capture et leur analyse sont peuvent permettre la restitution des informations. Ces signaux sont ainsi qualifiés de "signaux parasites compromettants".

2. Compromission électromagnétique

2.1. Définition

La compromission électromagnétique peut se définir comme étant la révélation d'informations confidentielles à des personnes qui n'ont pas à les connaître.
Cette capture illicite d'information est réalisée par l'intermédiaire des signaux parasites compromettants. L'information représente le phénomène générateur et les signaux parasites le phénomène résultant ; l'exploitation du lien entre les signaux parasites et l'information traitée permet, à partir de la connaissance du phénomène résultant, de remonter au phénomène générateur.

La corrélation, entre les signaux parasites compromettants et l'information, peut se manifester sous différents aspects. En général, lorsqu'elle est traduite au niveau électrique, l'information se présente sous la forme d'une succession d'impulsions, chacune étant représentative d'un double changement d'état stable du régime électrique établi. Ces changements d'états successifs provoquent, dans les différents circuits du matériel considéré, des perturbations présentant des caractéristiques qui sont en relation avec les impulsions elles-mêmes. Les perturbations peuvent prendre naissance, soit durant le front montant de l'impulsion, soit durant le front descendant. Elles peuvent également être générées à chaque front des impulsions. Si les informations sont exploitées en mode parallèle, les parasites engendrés possèdent, en plus, une amplitude proportionnelle au nombre d'impulsions présentes simultanément.

L'exploitation des perturbations, c'est-à-dire la connaissance de leurs positions relatives, de leurs niveaux, permet de recréer des impulsions identiques à celles qui sont à l'origine de ces perturbations et ainsi, révèle les informations qui sont traitées. La capture et l'exploitation des signaux parasites compromettants dans le but de connaitre des informations traitées sont la compromission électromagnétique.

2.2 Un mythe de Hackers ?

Le procédé technique nécessaire pour réussir la compromission magnétique ne demande pas de grandes connaissances, ni de grands moyens financiers. Le materiel minimum est constitue d'une antenne, d' oscillateurs, pour synchroniser les fréquences verticales et horizontales, et d' un recepteur. Ce dernier peut être un téléviseur ordinaire, accompagné d'un magnetoscope.
L'enregistrement des informations interceptées et traitées permet une analyse plus simple et plus efficace.

On peut avoir l'impression que tout cela n'est qu'un mythe de hackers.
Au cours d'une exposition, l'IUT d'Aix-la-Chapelle a expérimenté ce phénomène. Les professeurs et chercheurs ont démontré qu'avec un simple téléviseur et environ 2000 francs de matériel, la compromission éléctromagnétique était réalisable, aussi simple qu'un jeu d'enfant. La distance entre la source des signaux parasites et le récepteur dépend de la quantité des sources d'émissions

electromagnetiques proches; elle oscille entre quelques mètres et 1 km. Même le fonctionnement simultané de plusieurs machines (une salle info par exemple) n'est pas une protection efficace. Il est possible d'isoler des signaux distincts en provenance de 25 ordinateurs differents, situés dans un faible périmètre.

Les vieux téléviseurs soviétiques en noir et blanc sont un bon matériel peu coûteux pour ce procédé. Etant donné que la réception était très mauvaise du temps de l'ex-Union Soviétique, la population équipait ses postes de puissants récepteurs, capables de capter des signaux très faibles.

II- RECEPTION DES RADIATIONS ELECTROMAGNETIQUES

1. Emissions électromagnétiques - Généralités

Concrètement, les câbles des matériels en fonction agissent comme une antenne pour transmettre directement les signaux, ou reçoivent même le signal puis le ré-émettent encore plus loin de la source. Il est possible que les câbles transmettent les signaux de manière plus efficace que les équipements eux-mêmes.
Les plus forts signaux sont généralement entre 60 et 250 MHz, certaines exceptions de signaux très puissants dans la bande TV peuvent atteindre 450 à 800 MHz.

La reconstitution des informations par compromission électromagnétique n'est pas limitée aux ordinateurs et aux matériels digitaux, elle est efficace pour tous les montages générant des radiations éléctromagnétiques.

2. Capture des radiations électromagnétiques

Les radiations émettent les informations sans synchronisation des lignes, à cause de la résolution, du phénomène de réflection, des interférences, ou des variations de tolérance des composants. Donc, s'il y a 3 différents signaux sur la même fréquence, par réglage fin de la fréquence de réception, par manipulation de l' antenne, et modification de la synchronisation des lignes, il est possible de caler la réception sur chacun des 3 signaux séparément, et ainsi lire les informations affichées à l'écran. Par cette technique, il est possible également de distinguer les différents équipements situés dans une même pièce.

Le signal reçu par le récepteur TV ne contient pas les informations de synchronisation. Cela signifie que l'image affichée sur l'écran TV, pendant la réception des radiations émises par une unité vidéo, va osciller sur l'écran, dans les directions verticales et horizontales, car les fréquences de synchronisation de l'unité vidéo et celles de la TV ne sont pas les mêmes.
La qualité de la réception peut être améliorée en générant extérieurement les signaux de synchronisation nécessaires, et les associer au récepteur TV.

Avec cette extension au récepteur TV, tout type d'unité vidéo peut faire l'objet de compromission éléctromagnétique, à condition qu'elle génère un niveau de radiation assez élevé. L'extension peut être développée et construite par tout électronicien amateur en quelques jours, je vous fais confiance pour cette partie.

Quelques moniteurs sont construits sur le même principe que les télévisions en noir et blanc. Les oscillateurs de synchronisation libre dans un récepteur TV peuvent parfois générer approximativement la même fréquence que celle utilisée par le moniteur.
La compromission éléctromagnétique peut même s'appliquer accidentellement dans ce cas.

3. Reconstruire la synchronisation

La méthode la plus simple et la moins coûteuse pour reconstruire une synchronisation dans un récepteur TV est l'utilisation d'un montage incluant 2 oscillateurs électroniques:

- un oscillateur ajustable pour les fréquences 15-20 kHz, pour générer le signal de

synchronisation horizontale
- un oscillateur ajustable pour les fréquences 40-80 Hz, pour générer le signal de synchronisation verticale.

Les 2 signaux peuvent être combinés et ajustés par le séparateur de synchronisation du récepteur TV.
Il est bien connu que la relation entre les fréquences de synchronisation verticales et horizontales est:

*f(hor) = k * f(vert)*

où k est le nombre de lignes affichées sur le moniteur.
Il est de plus pratique de seulement générer la fréquence de synchronisation horizontale, et de calculer la fréquence de synchronisation verticale en divisant f(hor) par k.
Une fois que le nombre de lignes a été déterminé, la synchronisation peut être restaurée en ajustant seulement un oscillateur.
La figure 1 montre un dispositif de compromission électromagnétique dans lequel ce type de resynchronisation est employé.

III- MESURES ET NORMES FRANCAISES

1.1. Compatibilité électromagnétique

La compatibilité électromagnétique (CEM), d'après la définition qu'en donne la norme française NF C 98020, c'est l'aptitude d'un dispositif, d'un appareil ou d'un système à fonctionner de façon satisfaisante dans son environnement électromagnétique, sans produire lui-même des perturbations électromagnétiques intolérables pour d'autres matériels, appareils ou systèmes.
La CEM résulte de la réduction et de la maîtrise des signaux parasites d'origine électrique.

Le domaine couvert par la CEM est un domaine extrêmement vaste qui s'étend à tous les matériels électriques, depuis les équipements industriels, scientifiques et médicaux (ISM) jusqu'aux équipements domestiques. Il concerne également les appareils de traitement de l'information (ATI).

Le domaine de la CEM s'appuie sur une réglementation émanant d'organismes nationaux et internationaux dont les principaux sont :

- La CEI (Commission Electrotechnique Internationale) et ses Comités d'Etude ;
- Le CISPR (Comité International Spécial des Perturbations Radioélectriques) ;
- Le CENELEC (Comité Européen de Normalisation Electrotechnique).

La réduction des parasites s'obtient en grande partie par un choix judicieux des composants. D'une manière générale, les composants à base de technologie dite rapide, c'est-à-dire présentant des durées de commutation très brèves, les machines tournantes et les alimentations à découpage sont à écarter car génératrices de perturbations.

1.2. Blindage

La méthode pratique la plus efficace pour atténuer, voire supprimer, l'énergie en provenance directe d'une source consiste à insérer un blindage entre l'organe émetteur et l'organe récepteur (au sens large du terme). Un bon blindage doit empêcher les signaux créés de sortir d'une enceinte ou les réduire suffisamment pour qu'ils ne puissent pas perturber le fonctionnement d'équipements voisins. De même, un bon blindage doit empêcher un appareil sensible de recevoir des signaux indésirables qui l'entourent et qui nuiraient à son bon fonctionnement.

Si l'on place un blindage sur le trajet de l'énergie rayonnée par une source, cet écran provoque un affaiblissement, de l'énergie rayonnée, qui est fonction de l'efficacité de blindage et qui correspond à la somme des pertes par réflexion et par absorption.

Ces deux éléments dépendent du type de rayonnement. La réflexion augmente avec la fréquence en champ magnétique et diminue en champ électrique. L'absorption augmente avec la fréquence, la perméabilité du matériau et son épaisseur.

1.3. Limitation de la propagation par rayonnement

La limitation de la propagation par rayonnement consiste :

- soit à confiner, artificiellement, les signaux parasites dans un volume donné et prendre des mesures particulières pour qu'ils n'en sortent pas. C'est le cas lorsque l'on installe les matériels de traitement dans une cage de Faraday ;
- soit à aménager, autour des équipements, des zones dans lesquelles des dispositions sont prises afin d'empêcher la capture des signaux parasites compromettants. Les dimensions de ces zones sont déterminées de façon que les signaux qui seraient captés en dehors de celles-ci ne présenteraient plus une amplitude suffisante permettant leur exploitation.

1.3.1. Utilisation d'une cage de Faraday

La cage de Faraday est une enceinte blindée, constituée de parois métalliques sur ses six faces. Le blindage se comporte comme un écran électromagnétique qui empêche la propagation des ondes électromagnétiques. Les points faibles d'une cage de Faraday se situent au niveau des ouvertures qu'il convient de traiter correctement afin de ne pas dégrader les caractéristiques globales d'affaiblissement de la cage. Ces ouvertures sont essentiellement ;

- la porte ;
- les orifices, nécessaires pour assurer l'aération et la climatisation du local ;
- les passages de câbles pour relier les matériels exploités dans la cage avec l'environnement extérieur (lignes de transmission, alimentation de la cage en énergie électrique, déport d'alarme, ...).

Toutes les liaisons traversant la paroi de la cage doivent être munies de filtres adéquats. L'utilisation de fibres optiques pour acheminer les informations hors de la cage est la meilleure des solutions car la fibre optique est insensible aux rayonnements électromagnétiques.

La mise à la terre de la cage de Faraday s'effectue à partir d'un point unique situé sur la paroi extérieure de la cage. Les matériels situés à l'intérieur de la cage sont raccordés individuellement, directement sur la paroi interne de la cage ou bien sur une barre de raccordement reliée à la cage.

1.3.2. Aménagement de zones de protection

Lorsque le matériel utilisé pour le traitement des informations n'est pas installé dans une cage de Faraday, il y a lieu de l'entourer d'une zone de protection qui comporte une zone de sécurité électromagnétique et une zone de couplage. Au terme "zone" se rattache une notion de volume sphérique, centré sur chaque équipement.

1.3.2.1. Zone de sécurité électromagnétique

La zone de sécurité électromagnétique est une zone dans laquelle des dispositions permanentes sont prises pour détecter et empêcher toute écoute électronique, activité de recherche de renseignements et mise en place de matériels d'écoute. Il convient, également, que des précautions particulières soient prises pour contrôler les mouvements des personnels, y compris des véhicules.

L'efficacité d'une telle zone croît avec sa dimension. Une distance de 100 mètres est recommandée compte tenu des possibilités actuelles d'analyse des signaux parasites.

1.3.2.2. Zone de couplage

La zone de couplage est une zone qui ne doit pas comporter d'équipement ou circuit superflu (téléphone, intercom.) susceptible de capter par couplage des signaux parasites compromettants provenant des équipements traitant les informations sensibles ou des circuits acheminant ces informations. Les circuits qui sortent de la zone de couplage doivent être filtrés et blindés. Dans ce cas, les filtres sont placés en limite ou en dehors de la zone ; le blindage des circuits est prolongé sur une distance minimale de trois mètres.

Cette zone doit être aussi exempte que possible d'objets susceptibles de se comporter comme des conducteurs ou amplificateurs de signaux parasites compromettants. Il est recommandé d'éviter l'installation des équipements traitant les informations sensibles, à proximité d'objets ou mobiliers métalliques (radiateurs de chauffage central, armoires,...), qui peuvent amplifier les signaux parasites, ce qui accroît la distance de propagation. Si ces objets n'ont pu être éliminés, leur continuité métallique doit être interrompue par une isolation idoine placée en limite ou au-delà de la zone.

Plus la dimension de la zone de couplage augmente, plus la possibilité de réinduction des signaux parasites par couplage diminue, plus l'aménagement d'une telle zone devient difficile compte tenu des problèmes d'infrastructures qui sont posés. Il est cependant recommandé de prévoir des zones de couplage, centrées sur l'équipement, de 5 mètres de rayon au minimum.

IV- POUR EN FINIR

Ce type d'espionnage est en fait plus connu sous le nom de TEMPEST, terme désignant aux Etats-Unis à la fois le standard de sécurité et la compromission électromagnétique.
Cet article est le résultat de multiples recherches à partir de documents américains (universités), français, de livres, et de textes gouvernementaux.
J'espère qu'il vous aura éclairé en ce qui concerne l'espionnage par compromission électromagnétique, pour votre soif de connaissances, ou pour la pratique. Si c'est le dernier cas, informez-moi de vos résultats (vatoo@caramail.com ou cryptel@excite.com).

vatoo.