CRYPTOWALL

Le meilleur moyen de sécuriser vos échanges

Produit i2e

ECHELON est un réseau très confidentiel d'écoute et d'analyse mondial opéré par la communauté UKUSA. Echelon intercepte les signaux radio et communications, en provenance de satellites, téléphones, faxes, e-mails à peu près partout dans le monde. Echelon inclut aussi des systèmes d'analyse et de tri des interceptions. On estime qu'environ 3 milliards de communications sont écoutées tous les jours.

Les membres de l'alliance anglophone font partie de l'alliance UK-USA, qui depuis la seconde guerre mondiale, collecte et partage les informations d'écoute. Diverses sources font état du fait que ces nations ont positionné des stations d'écoute et satellites pour intercepter les signaux radio, satellites, hyperfréquences, cellulaires et fibres optiques. Ces signaux sont ensuite traités par une série de super-ordinateurs, connus sous le nom de dictionnaires. Ils sont programmés pour rechercher toute communication sur la base d'un objectif de mots, mots-clefs, phrases ou même maintenant voix.

Chaque membre de l'alliance UK USA se voit assigné des responsabilités d'écoute de zone géographique.

Aux USA, la NSA (National Security Agency) avec son siège à Fort Meade, en banlieue de Washington DC, emploie 38 000 personnes et possède un budget estimé à 3.6 milliards de dollars. La NSA est chargée du codage et de la sécurité informatique de l'ensemble des organes fédéraux américains et de l'interception, au profit du département de la défense et d'autres services américains de tout type de message. Son équivalent en Angleterre est le GHHQ (Government Communications Headquater) basé à Cheltenham. De plus, d'autres organisations, plus petites, existent pour compléter ses expertises (ex :Her Majesty's Governement Communication Centre : HMGCC)

L'Australie et la Nouvelle Zélande, membre de UKUSA, ont confirmé l'existence d'Echelon (sans toutefois donner de détails sur ses performances techniques). La Hollande (qui n'est pas un membre Echelon) a aussi confirmé l'existence du réseau (à travers une étude parlementaire).

Enfin, l'ancien directeur de la CIA, R James Wolsay, a admis l'utilisation du système à des fins d'espionnage industriel. Ces informations étaient relayées aux compagnies américaines concurrentes. Les révélations par les médias d'un certain nombre de cas attestent d'une utilisation d'Echelon dans ce sens.
Airbus a par exemple perdu un contrat de 6MM de dollars avec l'Arabie Saoudite, après révélation par la NSA de l'existence d'intermédiaires dans la négociation.

Le système permet l'interception de toute communication hertzienne dans le monde : téléphone longue distance ou mobile, fax, e-mail, télex, à raison de deux millions d'écoutes par minute.
Les conversations locales, par câble, ne seraient pas épargnées et la NSA y a également accès grâce à la complicité de grands opérateurs de téléphonie. Echelon compterait ainsi une dizaine de stations d'écoute du programme, telles que Menwith Hill en Grande-Bretagne, membre de l'Union Européenne, Bad Aibling en Allemagne sous contrôle américain, ou Sugar Grove situé en Virginie, sachant que le nombre d'antennes et la taille des stations d'écoute du programme augmente régulièrement depuis que la guerre économique a succédé à la guerre froide après l'effondrement du bloc soviétique.

Un premier rapport en 2000, sur Echelon, a conclu à un espionnage économique de grande ampleur de l'Union Européenne par les Etats-Unis. De même, un rapport réalisé en 1999 pour le ministre français de la Défense intitulé « Sécurité des systèmes d'information, dépendances et vulnérabilités » soupçonne l'existence de liens entre la firme américaine Microsoft, dont le système d'exploitation Windows équipe neuf ordinateurs PC sur dix fabriqués dans le monde, et les services de renseignements américains. Ce document révèle l'existence de programmes espions et de formules mathématiques permettant de décrypter un message intercepté dans les produits vendus par Microsoft.

Initialement créée pour écouter les communications militaires et diplomatiques des blocs de l'Est pendant la Guerre Froide, début des années 60, Echelon est maintenant soupçonné de rechercher des pistes et détecter des plans liés au terrorisme, à la drogue, mais aussi de l'intelligence politique et diplomatique. Mais quelques critiques disent aussi, que le système est utilisé pour de l'intelligence économique et de la surveillance de personnes.

En mai 2001, un rapport sur Echelon recommande, entre autre, d'utiliser régulièrement le cryptage pour protéger ses communications et échanges. En Angleterre, le gouvernement a mis en place une loi (Regulation of Investigatory Power Act) qui donne le pouvoir aux autorités de demander à tout citoyen de remettre ses clefs de cryptage, sans avoir recours à une ordonnance judiciaire.

L'écoute des téléphones mobiles, au travers d'Echelon a permis la localisation puis l'arrestation en mars 2003 de Khalid Shaikh Mohammed.

En avril 2004, l'Union européenne décide d'attribuer 11 millions d'Euros au développement de la sécurisation des communications, basée sur la cryptologie, par un système théoriquement inviolable par Echelon ou un autre système d'espionnage.

Le système de cryptographie d'**i2e**, unique et innovant, a été développé à ce moment-là, financé par les instances européennes et françaises. Les recherches sur ces produits ont été initiées en 1998 et se sont considérablement accélérées avec l'aide du financement des gouvernements européens et français.

Connu sous le nom de Cryptowall, cet ensemble de cryptage est l'outil le plus robuste et le plus puissant contre Echelon, puisqu'il utilise un procédé d'encryptographie très complexe (courbes elliptiques) que très peu d'organisations au monde comprennent. Nos procédés sont complètement uniques et offrent une solution inviolable au système d'espionnage Anglo-américain.

Les produits Cryptowall sont utilisés pour sécuriser tous types de transmission (voix, données, vidéos), sans se soucier du type du moyen de communication (téléphone, wifi, internet, ...).

Les intérêts vitaux de la Libye ne seront pas épargnés par le système Echelon.
Le Ministre de l'Intérieur français dispose d'une réelle connaissance corroborée par une collaboration avec la société spécialisée dans ce domaine. Il nous appartient par conséquent de vous assister à mener une investigation approfondie sur la nature des informations risquant d'être obtenues via Echelon. Que celles-ci soient liées à la défense militaire, l'industrie ou le commerce et plus généralement aux intérêts fondamentaux du pays.

GEOLOCALISATION

Les antidotes d'i2e

Les moyens de communication modernes présentent deux grandes faiblesses :

- La première réside dans la confidentialité de la communication et tous les systèmes existant pour les écouter (ex Echelon). La solution existe à travers les produits i2e : Cryptowall.
- La seconde réside dans la localisation géographique de la source de la communication.

Ceci est communément appelé la Géolocalisation et c'est une opération très simple à réaliser. Des systèmes existent qui permettent de localiser un GSM, tant en mode communication, qu'en mode stand by, avec une précision de quelques décamètres et ce en quelques secondes.

Thuraya, Inmarsat ou Irridium, qui comportent des téléphones plus sophistiqués, sont encore plus faciles à localiser du fait de l'implantation dans leur système d'une balise GPS.
Enfin, les localisations de téléphones fixes sont par définition connues.

Afin de protéger un individu contre la géolocalisation, la seule solution valable repose sur le leurrage par des relais multiples, constituant ainsi un mini réseau propriétaire mobile, avant de se reconnecter au réseau publique.

Par le biais de cette solution, le dernier point pour accéder au réseau public (qui est le point qui sera localisé et à ce titre qui sera à risque) est un relais mobile. La personne à protéger sera distante de plusieurs km de cette source localisée.
La distance peut être plus grande selon le nombre de BTS propriétaires (relais) qui sont déployés.

i2e peut offrir diverses solutions afin de garantir la non-traçabilité des émetteurs. Les solutions de « multirelayage » sont étudiées au cas par cas, selon le nombre de relais, la configuration des moyens à protéger et enfin le secteur géographique à protéger.