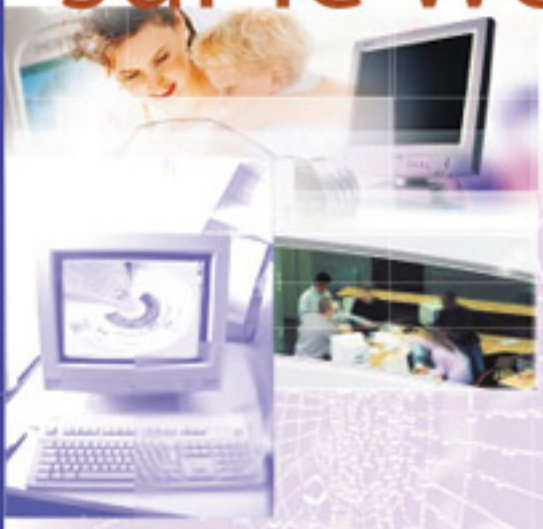
« La piraterie sur le web »

Mardi 19 février 2002

Euroscience Léman
http://www.euroscience.org

Café des Sciences

La piraterie sur le web



Intervenants :

Stéphane Koch
Correspondant pour l'Ecole de Guerre Economique

Nicolas Giannacopoulos
Diplômé de l'Université de Genève (Sciences politiques), Directeur exécutif de Inside.co

Ricardo Sibilia
Diplômé de l'Ecole Polytechnique Fédérale de Zürich (Physique)

Entrée libre

Mardi 19 février 2002
de 18h30 à 20h00

Espace commun du BAC (Bâtiment d'Art Contemporain), MAMCO
10 rue des Vieux-Grenadiers, 1205 Genève
Parking Plainpalais - Bus 1 et 4, arrêts "Bains" et "Cirque"

Avec le soutien de l'Association du Personnel du CERN, du Département de l'Action sociale et de la Santé du Canton de Genève, du Département des Affaires culturelles de la Ville de Genève, de la Loterie Suisse Romande, de la Fondation Wilsdorf, de Firmenich SA, et de la Passerelle Science-Cité de l'Université de Genève.

« La piraterie sur le web »

Lundi 4 mars 2002, 19h-20h30, ForuMeyrin

L'AFFICHE L'INTRO LE COMPTE RENDU

Les échanges de toutes sortes sont facilités à l'extrême par le web: des forums, des vidéoconférences, le commerce à distance, ou tout simplement la célérité des courriers électroniques ou la convivialité des chats, tout cela participe de la société de communication. Une certaine partie du monde découvre le nouvel horizon des échanges quasi instantanés, mais....

- Les transactions sur le web sont-elles vraiment sûres?

- Les renseignements sur soi que l'on donne sont-ils vraiment cantonnés à la stricte confidentialité ?

Mais, donc... des pirates furtifs ou autres affreux (freaks) qui pénètrent un système, qui volent des codes ou des données concernant des cartes bancaires ou des secrets industriels, voire des données sensibles, il en existe de toutes sortes. Certains le font dans un but lucratif, d'autres pour le fun (pour jouer), peu importe: ces petits malins donnent des sueurs froides aux concepteurs de systèmes dits sécurisés.

On entend souvent dire que certains de ces as du clavier reconvertis gagneraient des sommes importantes: c'est vrai ?

Reste la question des virus:
- Qu'est-ce que c'est ?
- Comment ça marche ?
- Comment les reconnaître ?
- Les éviter ?
- Pourquoi se répandent-ils si vite?

On parle de manque de diversité des logiciels, le quasi monopole de Microsoft facilitant les choses. Un peu comme si toutes les banques enfermaient les sous qui leur sont confiés dans le même modèle de coffre-fort, avec la même serrure...
Est-ce que c'est vraiment comme ça que vont les choses?

Alors, ce 19 février, comme à chaque fois que nous nous rencontrons, vous en avez l'habitude peut-être, venez poser les questions qui vous viendront à l'esprit concernant ce sujet. La spontanéité est la bienvenue, inutile donc de tourner sept fois la langue dans la bouche avant de parler!

Intervenants:

Stéphane Koch, correspondant pour l'Ecole de Guerre Economique

Nicolas Giannacopoulos, diplômé de l'Université de Genève (Science politiques), Directeur exécutif de Inside.co

Ricardo Sibilia, diplômé de l'Ecole Polytechnique Fédérale de Zürich (Physique).

Pour en savoir plus:

http://www.infosurance.ch ou http://www.infosurance.org
http://www.infowar.com

« La piraterie sur le web »
ou
« Espionné par Internet »

Mardi 19 février 2002

L'AFFICHE L'INTRO LE COMPTE RENDU

Intervenants :

· **Stéphane Koch :**
président d'Internet Society, Genève.

· **Riccardo Sibilia :**
diplômé EPFZ en physique, spécialiste de la guerre de l'information et de la sécurité informatique, Genève.

· **Nicolas Giannakopoulos :**
Diplômé en sciences politiques et président de l'association Inside.CO SA, Genève.

Questions du Public :

Qu'est-ce que la guerre sur Internet ?

L'affiche indique : " Piraterie sur Internet ". Le pirate est un individu, une personne un peu mythique, entouré d'un grand halo avec un chapeau à plumes, avec une jambe de bois, un sabre clair qui pourfend les gens, qui les perce pour les voler. Est-ce que sur Internet, les pirates ont aussi cet aura quelque part, de gens qui effectivement percent des secrets, rentrent dans les choses et attirent une certaine admiration de la part d'un certain nombre de gens ?

Vous avez parlé des dangers disons d'État à État ou d'organisations, je crois que pour un grand nombre de gens ici, il serait bon de revenir sur les intrusions dans la vie privée, le fait que si l'on communique, ne serait-ce que pour acheter un livre chez Amazon, on ne puisse pas être fiché malgré les dénégations disant qu'on ne communiquera pas votre nom … Quel est l'état à la fois du droit et de la pratique en ce domaine ?

N'existe-t-il pas des petits logiciels qui rendent opaques notre ordinateur personnel ?

J'aimerais savoir dans quelle mesure, actuellement, avec les possibilités de cryptage qui existent, un vrai espionnage économique, informatique est possible si des dispositions sont correctement prises pour que les flux de données soient correctement cryptés ? S'il n'y a pas une sorte de complicité passive de la part de la victime, est-ce que l'on peut vraiment espionner de manière électronique, sans qu'il y ait un contact physique avec l'entreprise ?

Stéphane Koch parle de la carte Cumulus, vous parlez de micro-puce que l'on s'injecte, est-ce que l'on peut imaginer qu'avec une carte Cumulus, on puisse nous suivre, nous retrouver. Est-ce que ça peut faire partie du possible ?

Je voudrais peut-être revenir aux choses de base, c'est que les inventeurs de l'Internet, du Web ont voulu un système qui soit très ouvert, libre où il n'y ait pas trop de commercial, pas trop de policiers et puis pas trop de cryptage. C'était vraiment conçu comme le moyen de communication libre. Dernièrement, il y aurait quelque chose qui est en train de s 'installer à l'intérieur même des moyens de communication du Web.

Ce que j'ai entendu était encore différent. Il s'agissait même d'une structure différente. On n'utilise que la communication du Net mais c'est un système de serveurs distribués.

Je voudrais revenir aux acteurs impliqués dans ce marché d'informations, l'intérêt effectivement d'obtenir des informations de partout. Vous avez cité l'exemple de la carte Cumulus où volontairement on se dénude, on donne des informations, c'est tout à fait légal. Vous avez aussi cité l'intérêt par exemple pour les caisses de maladie à trouver un client sain, en bonne santé, rentable. Est-ce que l'on peut s'imaginer que ces entreprises-là, en terme large, engagent quasiment des pirates pour leur procurer cette information ou est-ce que ce sont des freelances qui les approchent et disent avoir quelque chose à vendre ?

J'ai une question par rapport aux grandes oreilles américaines, cette fameuse NSA Echelon. On parlait des moyens techniques faramineux, et je voudrais savoir ce qu'il en est, ce qu'ils sont capables d'entendre ? On a vu qu'il y a toute une partie de l'information qui peut être captée par des moyens légaux, c'est-à-dire que les grandes multinationales récoltent des informations et peuvent les distribuer. Quelle quantité d'informations peuvent-elle engranger et conserver et surtout par quels moyens elle est captée ?

Est-ce que l'on peut dire qu'actuellement que tout ce qui circule sur Internet peut être intercepté réellement ou bien c'est une toute petite partie qui est ciblée ?

Comment peut-on réduire tout cet espionnage dans Internet ?

Je voudrais revenir sur le téléphone mobile parce que le téléphone cellulaire permet de localiser l'endroit d'où vous appelez. J'ai entendu dire qu'en Suisse, systématiquement, tout est enregistré donc en principe on pourrait savoir où je suis au moment où j'ai téléphoné. En plus, les GPS vont devenir banalisés dans les voitures…

Nous n’avons pas encore parlé du domaine des virus, des vers. Est-ce que ça à voir avec le piratage, l’espionnage ?

Est-il possible qu’un État espionne d’autres pays, par exemple des gens dans la recherche et retransmettre ces informations à des entreprises de son pays ?

Les grandes sociétés de télécommunication dans ce monde ainsi que les fournisseurs d ’accès Internet ne seraient-elles pas responsables de la violation de la sphère privée du fait qu’elles sont entre nous et le pirate.

Je voudrais savoir si les chain letters ne sont pas une forme de virus de piratage ?

Quelles recommandations pouvez-vous donner aux politiques pour s’opposer à ce genre de pratiques ? Quelles mesures devraient prendre les politiques pour s’opposer à l’espionnage de tout un chacun ?

Exemple de la carte Cumulus, est-ce que les politiques ne devraient pas mettre une espèce de verrou sur ce commerce d’informations ?

Résumé:

Le développement conjoint de l’informatique et des nouveaux moyens de télécommunication a permis la naissance d’un réseau mondial d’échange, l’**Internet ou Net**. Ce réseau donne la possibilité à ses utilisateurs, particuliers ou entreprises, d’envoyer des messages ou des fichiers via la ligne téléphonique à des correspondants situés à l’autre bout de la planète. L'Internet permet également de "surfer" sur le WEB (toile d’araignée mondiale), c'est à dire d'accéder à des pages web localisées sur des ordinateurs du monde entier.

Au cours de ces dernières années, le Net a logiquement connu un essor fantastique jusqu’à bouleverser nos habitudes. C’est pourquoi il constitue d’ores et déjà non seulement une révolution dans la transmission de l’information, mais également une révolution culturelle.

Cependant, si cet outil facilite grandement les échanges entre particuliers, entreprises, organisations ou grandes sociétés, il offre aussi à l’information véhiculée une plus grande accessibilité, ce qui à pour inconvénient de permettre à n’importe quel spécialiste de l ’Internet de se procurer les données les plus confidentielles. On parle alors d’espionnage sur Internet.

Les systèmes d’informations sont ainsi pénétrés par des “pirates” via le Net, dans le but de recueillir ou détourner des données. Aujourd’hui un pirate chevronné peut facilement se procurer sur Internet un numéro de carte ou de compte bancaire pour ensuite effectuer une transaction à son profit. Ces personnes malintentionnées peuvent également agir sur des “informations secrètes” échangées entre organisations ou états, dans le but de les déstabiliser. Par exemple, dans le conflit israélo-palestinien des pirates ont pu intercepter des renseignements militaires sur l’ennemi pour mieux les contrer.

Ces pratiques posent le problème fondamental de la protection des données échangées sur le Net. Ainsi, une entreprise peut être amenée à sécuriser son réseau informatique connecté à l’Internet en utilisant un “Firewall” (mur de protection) situé à l’entrée du réseau pour empêcher l’intrusion de personnes étrangères. De même, les services secrets de certains états peuvent crypter (coder) les données de fichiers classés “secret défenses” échangés sur l’Internet pour assurer leur confidentialité. Enfin, pour éviter l’espionnage industriel, de grandes entreprises peuvent recourir au cryptage de fichiers informatiques contenants les plans de futurs projets.

Sur le WEB, l’espionnage pose également le problème de la liberté individuelle et de la protection de la vie privée. Initialement le WEB a été conçu pour être un système libre et ouvert à tous. Cependant n’importe quel utilisateur peut être espionné par une société ou une organisation qui va recueillir un grand nombre d’informations le concernant (pages web visitées…) dans le but de dresser son profil psychologique et l’orienter par la suite sur des offres commerciales correspondant à ses centres d’intérêts. Aussi, pour protéger sa vie privée, il existe actuellement sur le marché des techniques, des logiciels permettant de naviguer anonymement (Anonymiser…).

Le WEB offre également un formidable espace pour propager, sous prétexte de liberté d ’expression, des idées parfois contraires à la morale (sites néonazis ou pédophiles). L ’espionnage Internet peut alors jouer un rôle positif et permettre à des organismes de surveillances du WEB, non seulement d'identifier et de censurer les sites web concernés, mais aussi de traquer et punir les contrevenants.

Avant tout, il y a donc nécessité de mettre en place un droit international devant être respecté par tous les utilisateurs du Net, quel que soit le pays où ils résident, et une police pour le faire respecter. Actuellement une stratégie de contrôle et de surveillance, basée sur les nouvelles technologies, est développée par certains Etats pour d’une part lutter contre la piraterie Internet et, d’autre part garantir que l’information échangée est conforme à la morale.

Si la surveillance Internet nécessite de ficher des millions de personnes (Interpole) et de recueillir un grand nombre de renseignements, elle n’en reste pas moins le seul moyen efficace, avec le cryptage, de lutter contre l’espionnage et les effets pervers du Net. Cette lutte, qui s’annonce déjà difficile, va être amenée encore à se renforcer avec le développement constant de l’Internet.