Le Hacking

M1 Information Communication, option NPJ - Promo 2012-2013 // ICOM, Université Lumière Lyon 2

Par Blaise Fayolle, Mathilde Régis, Wildried Devillers, Pauline Bouveau

1ère partie : les premiers pas du hacking

Lorsqu'on parle de « pirate », on ne pense pas forcément aux "pirates du net". Pourtant, ils sont bien présents dans le monde entier, et, en terme de hacking, ils n'en sont pas à leur coup d'essai. On va s'intéresser ici plutôt au Hacking et donc aux hackers, de leur naissance, jusqu'à la démocratisation d'Internet (avec des grandes figures du hacking). Nous allons pour cela recenser les différents types de hackers, comprendre leurs intentions et leur fonctionnement, mais également nous intéresser aux techniques qu'ils utilisent. Il sera également intéressant de nous pencher sur le côté législatif relatif au hacking en France et aux USA.

- **Qu'est-ce que le Hacking ?**

Selon John Drapper, considéré comme le père du hacking, c'est "l'art de savoir et de pouvoir modifier un programme, une machine, de façon à ce qu'il fasse ce que vous voulez qu'il fasse et non ce pour quoi il a été conçu."
Un hacker est alors une personne qui recherche la maîtrise totale des outils qu'il utilise - ordinateurs, logiciels, téléphones ou autres-, pour en comprendre le fonctionnement profond et qui n'hésite pas à le modifier pour l'adapter à ses besoins.

1- Les origines : Le Tech Model Railroad club

En 1959 leTech Model Railroad Club (TMRC), une association d'étudiants du MIT possédant comme son nom l'indique une maquette avec des trains électriques.
Pour la faire fonctionner, ils détournent la technologie de composants électroniques, dédiés par exemple à la téléphonie, et utilise le terme de hacking pour définir leurs actions
Quelques années plus tard, le MIT se munit de son premier ordinateur. Les membre du TMRC s'y intéressent et essayent de lui faire faire de nouvelles tâches, en créant de nouveaux programmes par exemple. Ils transposent leur mentalité de hacker a l'informatique.C'est le début du Hacking.

- ## L'éthique du hacking

L'éthique du hacking a été créé au MIT. C'est grâce à Steven Levy, un journaliste spécialisé dans le domaine de l'informatique, que l'idée a été vraiment diffusée.

Il publie un livre dans lequel il met en avant 6 règles de l'éthique du hacker :
Dans son livre ***Hackers : Heroes of the Computer Revolution,*** publié en 1984.
L'auteur de l'éthique du hack moderne invite à ne plus regarder le hacker comme étant uniquement « un étudiant imaginatif et audacieux » ou « un spécialiste en informatique », mais à étendre cette vision du hacker à l'ensemble de la société et même à la « planète ».

- L'accès aux ordinateurs - et à tout ce qui peut nous apprendre comment le monde marche vraiment - devrait être illimité et total.

- L'information devrait être libre et gratuite.
- Méfiez-vous de l'autorité. Encouragez la décentralisation.
- Les hackers devraient être jugés selon leurs œuvres, et non selon des critères qu'ils jugent factices comme la position, l'âge, la nationalité ou les diplômes.
- On peut créer l'art et la beauté sur un ordinateur.
- Les ordinateurs sont faits pour changer la vie.

2- Phreaking/ blue box

Dans la pensée commune le hacking commence avec l'intrusion dans les systèmes informatiques, en réalité les premiers hackers sont des gens qui se sont introduits dans le réseau téléphonique.

En 1957, Joe Engressia trouve le moyen de passer des appels gratuitement grâce en d'un simple sifflotement.
Il se rend compte qu'en sifflant dans le récepteur du téléphone, la sonorité reproduite permettait de signaler au serveur téléphonique que la ligne qu'il utilise est libre et qu'il a raccroché alors que ce n'est pas le cas.
La légende urbaine veut que ce soit John Draper aka Captain Crunch qui découvre cette technique en 1969 grâce à un simple sifflet trouvé dans un paquet de céréale.
C'est la naissance du phreaking, une contraction de phone et de freak.

Pour simplifier son utilisation et être plus performant, Captain Crunch fabrique un petit boîtier qui émet ce son correspondant à la fréquence 2600 hz : la bluebox
Grâce a cet outil, la pratique du phreaking se démocratise et s'étend aux États-Unis et dans le reste du monde.
Le réseau téléphonique devient pour les phreakers une sorte de réseau social, où ils organisent des conférences téléphonique, échange sur leurs pratiques,...
Mais c'est surtout un nouveau terrain d'exploration pour les hackers en soif de découvertes et d'accès à l'information. Ces derniers parviennent à s'immiscer dans n'importe quels réseaux, en dupant les compagnies de téléphone.
Ce sont les premiers à avoir développé une sensibilité et une démarche propre au hacker informatique
En 1971, un article de Ron Rosenbaum publiés dans esquire met fin à l'age d'or des phreakers, avec cet article tout le monde veut se munir d'une bluebox, le réseau téléphonique est envahi.

3- Législation à l'époque

Des agents spécialisés de la compagnie de téléphone se rendent chez les hackeurs pour faire pression sur leurs parents (beaucoup sont mineurs à l'époque). Beaucoup d'avertissements

de ce type sont réalisés. Les hackeurs désignent ces agents en les appelant M. Duffy Il rend visite aux hackers pour les menacer (la dissuasion fonctionne pendant quelques temps)

En parallèle, l'Etat américain prend des mesures informelles pour punir les hackeurs. La possession d'une Bluebox peut conduire jusqu'à 2 ans de prison. Captain Crunch est inculpé par le FBI pour fraude électronique, il passe 4 mois en prison. C'est la peine la plus lourde parmi les hackers puisque Captain Crunch est considéré comme le pilier du système.

4- Le Home Brew Computer Club et l'arrivée des ordinateurs personnels

Révolution dans le monde de l'informatique et développés par des entreprises mais également par des des hackers, les PC sont apparus quand la dimension et les coûts de production ont été suffisamment réduits pour en permettre l'accès au grand public.
Les premiers ordinateurs accessibles au public sont disponibles en kit (Alter 8800) que l'on peut assembler chez soi, une aubaine pour les bidouilleurs en tout genre.

En 1975 un groupe de passionnés d'informatique et des micro-ordinateurs se forme : c'est la création du Home Brew Computer Club,
Ils se retrouvent pour la première dois pour parler du Alter MITS et réfléchissent à de nouvelles manières d'utiliser les ordinateurs.
Le groupe se retrouve tous les quinze jours pour discuter technique de programmation, de fabrication, ils partagent leurs connaissances, leurs programmes.
L'échange d'information est primordial au sein du groupe, il y a une sorte de fierté de faire part de ses découvertes, de ses avancées. La mentalité du hacker commence à prendre forme traduit par une importance du partage et de l'accès total à l'information.
Elie F. décrit d'ailleurs le Home Brew Computer Club comme un repère de hackers avec un partage total d'information.

L'apparition des PC attire une génération de hacker passionné par l'accès à une technologie informatique qu'ils peuvent enfin maîtrisée, transformée,...
Ils se mettent donc à fabriquer leurs propres ordinateurs, expérimentent de nouvelles techniques
Avec ces expérimentations, l'informatique connaît de réelles avancées, on pensera notamment à Steve Vozniak le co-fondateur d'Apple (membre du HBCC)
Certains composants et programmes des ordinateurs ont pour source les hackers.

5- Le chaos computer club (CCC)

'Le Chaos Computer Club e. V. (CCC) est la plus grande association de pirates de d'Europe. Depuis plus de trente ans, nous fournissons des informations sur des problèmes techniques et sociétaux, comme la surveillance, la vie privée, la liberté d'information, le hacktivism, la sécurité des données et d'autres sujets autour de la technologie et des questions de piratage'

Fondé en 1981, il rassemble poignée de hackers passionnées par les réseaux informatiques et la programmation. Ces derniers militent pour une liberté de l'information totale et étudient la répercussion de la technologie sur la société.

Ils portent également un regard critique sur la concentration des informations dans un même système ou sur le net. Comme par exemple la concentration d'informations sur les différentes plates-formes de la Galaxie Google : Drive, répertoire, boite mail, Google +,...

Une réunion annuelle est organisée depuis 1984 entre noël et le nouvel an, le 'Chaos Communication Congress'

Ils s'attachent à mettre en évidence les failles des systèmes de sécurité des entreprises et des administrations
Leur action la plus connue est sûrement le 'BTX-hack' : en 1984 le CCC détourne 135.000 DM sur le compte en banque de la caisse d'épargne de Hambourg qui utilisait le protocole BTX proclamé inviolable. Le lendemain, ils rendent la somme dans son intégralité et montrent les failles de ce système de sécurité.
Les médias et la justice critiquent cette action qu'ils jugent illégale alors que le CCC agit dans une logique totalement désintéressée.

En 2006 : Le CCC publie un rapport dans lequel il montre qu'il est facile de manipuler les ordinateurs utilisés pour les élections. Le rapport est sérieusement pris en compte par la cour constitutionnelle fédérale qui se penche sur le problème. depuis plusieurs municipalité ont renoncé à utiliser ces ordinateurs.

Le Homme Brew Computer Club et le Chaos Computer Club, bien que très réputé dans le monde informatique ne sont que deux groupes de hacker parmi tant d'autres. Aujourd'hui il existe une multitude de groupes dont on ignore même l'existence.

2ème partie : La démocratisation d'Internet

La démocratisation d'Internet dans les pays occidentaux des années 2000 donne aux hackers un bien plus grand terrain d'expérimentation.

1- Une communauté de hackers

Les compétences se sont transmises et continuent à se transmettre :
On trouve de nombreuses conférences annuelles sur le hacking. Depuis 1992, la Defcon réunit les hackers à Las Vegas. La conférence black Hat précède la Defcon depuis 1997 et rassemble officiellement des experts des agences gouvernementales américaines et des industries, américaine ou non, avec les hackers les plus respectés de "l'underground". En Europe, des conférences ont lieu depuis 2000, et il existe le très réputé Hackfest au Québec.

On trouve désormais des magazines spécialisés sur le Hacking. Le plus connu est "2600", un trimestriel qui explique comment infiltrer, modifier, ou neutraliser des applications et des réseaux informatiques à l'aide de procédés technologiques ou d'ingénierie sociale.

Sur le réseau, on trouve évidemment de nombreux forums de discussion en ligne, et des logiciels malveillants automatisant la découverte et l'exploitation de vulnérabilités informatiques sont désormais disponible sur le marché.
Un peu partout dans le monde, se créent des écoles de hacking.

2- La formation de hackers professionnels

En France, l'Université de Valenciennes forme des anti pirates, des "hacker éthiques", depuis 2008 dans le cadre d'une licence professionnelle CDAISI (collaborateur pour la défense et l'anti-intrusion des systèmes informatiques). Les élèves y apprennent les techniques des pirates car pour eux, il est indispensable d'avoir les moyens de défense basés sur les méthodes utilisées par les attaquants. C'est donc de la protection informatique dans une forme offensive, mais utilisée dans un but bienveillant. Pour éviter toute dérive, la promotion est placée sous la surveillance de la DCRI (Direction centrale du renseignement intérieur) et un avocat spécialisé suit constamment les travaux des élèves. C'est apparemment un secteur professionnel qui embauche puisque 100% des étudiants diplômés ont trouvé rapidement un emploi.

Chez les hackers, on trouve différents niveaux d'expériences:

On appelle les "script kiddies" les débutants qui ne disposent que de connaissances rudimentaires – voire inexistantes – sur les langages de programmation qui constituent l'architecture d'internet et des applications informatiques. Ils doivent recourir à des applications malveillantes conçues par des pirates beaucoup plus expérimentés qui automatisent la découverte et l'exploitation des vulnérabilités.

Ceci est un exemple, cliquez sur le lien de téléchargement pour obtenir le cours complet.