Martin.Ouwehand@epfl.ch,
Domaine IT, EPFL

Dix ans de sécurité informatique à l'EPFL

J'ai succédé en 1996 à Didier Wagenknecht en tant que responsable de la sécurité informatique à l'EPFL et ce numéro spécial du FI est donc une bonne occasion de survoler ce qui s'est passé pendant ces dix ans, ce qui a changé en bien ou en mal et ce qui continue à préoccuper tous ceux qui à l'EPFL contribuent à la sécurité des ordinateurs et du réseau, parmi lesquels il serait impardonnable de ne pas mentionner Christian Raemy (qui a pris en charge à partir de 2002 tout ce qui touche à la sécurité de Windows, domaine bien sûr toujours plus prépondérant, où chacun a pu constater que ses talents et ses compétences étendues font merveille) et Richard Timsit (qui a mis au point le réseau de quarantaine, voir ***http://dit.epfl.ch/page59201.html***).

Ce qui s'est amélioré

L'expérience m'a vite montré que ces quatre mesures permettent d'éviter 99% des piratages:

1. ne laisser tourner que les services réseau nécessaires,
2. les protéger par un contrôle d'accès,
3. appliquer les correctifs (*patch* en jargon anglo-informatique),
4. et enfin avoir un antivirus à jour.

Rien que de très raisonnable: un service réseau inutile que vous laissez actif ne servira qu'à un pirate qui pourra s'y connecter de l'autre bout d'Internet pour profiter d'un bug; mais si ce service est indispensable à votre collaboration avec les chercheurs de l'Université de Freedonia, il ne devra être accessible qu'à ces chercheurs et non à tout Internet et il faudra tenir à jour le logiciel correspondand pour vous protéger même contre l'improbable pirate *freedonien*. De ce point de vue, la situation en 1996 était catastrophique et elle l'est restée au moins jusqu'en 2000: dans l'installation par défaut fournie par les constructeurs d'ordinateurs étaient inclus un grand nombre de services réseau installés *au cas où*, bien entendu ouverts à tout Internet, et les fournisseurs publiaient épisodiquement des mises à jour que chacun devait aller chercher et installer *manuellement*, ce qui n'était fait en général qu'après avoir été victime d'un piratage... C'est ainsi que plusieurs dizaines d'ordinateurs de l'EPFL furent piratés en 1998 à cause d'une vulnérabilité dans le logiciel serveur Imapd (voir ***http://www.cert.org/advisories/CA-1998-09.html***) qui n'était en fait utilisé sur aucun d'eux ou encore, en 2001, plusieurs utilisateurs de Frontpage découvrirent grâce au vers *Code Red* que ce logiciel d'édition de pages HTML transformait silencieusement leur station de travail en serveur Web.

L'industrie informatique en a tiré les leçons et tout ceci appartient au passé: il n'y a aujourd'hui plus de systèmes d'exploitation ou d'antivirus qui ne soient capables de se tenir à jour automatiquement et les configurations par défaut sont nettement plus sûres, les services réseau encore actifs découlant de choix explicites de l'usager au moment de l'installation du système. De même, pratiquement tous les systèmes offrent un contrôle d'accès réseau (*firewall* local), bien que ce soit un domaine où des améliorations sont encore possibles: à l'heure actuelle, ce contrôle est implémenté à un niveau trop bas dans le système d'exploitation, et basé sur la notion de *port* réseau difficile à saisir par le novice et inadapté dans le cas d'utilisation de ports éphémères (il serait préférable selon moi que ce contrôle se *rapproche* de l'applicatif). Enfin, depuis peu on voit des restrictions également dans les accès réseau vers l'extérieur, ce qui contribue beaucoup à limiter la propagation de virus et de vers en cas d'infection: l'antivirus VirusScan 8.0i, largement déployé, à l'EPFL offre une telle fonctionnalité.

Ce qui n'a pas changé

Commençant par un point où la stabilité est une bonne chose, on peut se réjouir qu'il soit aussi rare aujourd'hui que ça ne l'était en 1996 qu'un membre de notre École ne s'adonne au piratage en utilisant son infrastructure informatique, le nombre de cas sur ces dix ans se comptant sur les doigts d'une main (ceci dément l'avis répandu que les problèmes de sécurité proviennent surtout de l'intérieur, même s'il est vrai qu'un *insider* aigri pourra faire beaucoup plus de dégâts que les milliers de pirates qui chaque année *scannent* un site, mais à l'aveugle). Ces quelques incidents m'ont permis de découvrir une autre constante: alors que beaucoup de spécialistes soulignent que l'aspect organisationnel et institutionnel de la sécurité informatique doit être pris en compte

Bien que l'EPFL gère son parc informatique comme toute grande entreprise, en l'espace de deux semaines deux de ses étudiants ont été accusés de hacking. La direction a réagi mais n'a guère les moyens d'enrayer ce fléau

par Elaine-Lise Bashet

Quand les pirates usent et abusent de l'école

Mai 1999 – quand le piratage à l'EPFL faisait les titres du Matin

à un niveau élevé du *management*, elle semble être conçue à l'EPFL essentiellement comme un problème technique, à résoudre par des informaticiens. Dans les cas évoqués ci-dessus, il n'a donc jamais été très clair, qui devait les traiter, en déterminer la gravité ou définir les sanctions. Il est cependant possible que les solutions qui se sont dégagées, de même que plus généralement la gestion de la sécurité informatique à l'EPFL, faite de négociations et de concertations au coup par coup (la COSI - Coordination Opérationnelle des Services Informatiques - joue là un rôle important), soient plus adaptées à la structure hétérogène de notre site que des directives rigides qui resteraient lettre morte.

Passant ensuite aux points où on peut regretter qu'aucun progrès n'ait été réalisé, on mentionnera en premier lieu que la qualité des logiciels reste extrêmement médiocre du point de vue de la sécurité informatique. On peut faire remonter en effet la plupart des incidents de piratage à des erreurs de conception ou d'implémentation commises par les programmeurs, telles que le célèbre dépassement de mémoire tampon (*buffer overflow* en jargon anglo-informatique) qui est encore de nos jours un des problèmes les plus répandus, alors qu'on sait depuis le *ver de Morris* en 1988 (environ 10% des 60'000 ordinateurs que comptait Internet à cette époque en furent victimes, voir ***http://www.ietf.org/rfc/rfc1135.txt***) à quel point il est dangereux. Pour résumer, on peut dire qu'il s'agit simplement de naïveté de la part des programmeurs, qui par exemple prévoient un emplacement en mémoire de dix octets, bien assez selon eux pour stocker le *username* qu'ils demandent à l'usager, sans imaginer que le pirate essayera d'entrer un *username* beaucoup plus long et composé d'octets soigneusement conçus pour détourner à son profit la logique du programme. Il faut donc croire que le consommateur moyen se soucie assez peu de ces problèmes de sécurité pour que les éditeurs de logiciels ne trouvent pas d'intérêt économique à étoffer leurs équipes de programmeurs de spécialistes prenant en charge la sécurité et la robustesse des logiciels dès leur conception et qu'ils s'en remettent aux solutions génériques évoquées plus haut, *firewall* local et mises à jour automatiques.

Mais ces mesures restent inefficaces contre les vulnérabilités des scripts *(contenu actif)* accessibles par le Web: il n'y a en général pas de contrôle d'accès réseau sur les sites Web, qui n'ont souvent de sens que s'ils sont ouverts à tout Internet et d'autre part ces scripts sont assez spécifiques pour qu'ils ne soient pas inclus dans le système de mise à jour automatique. C'est ce qui explique que le piratage passant par le Web (protocole HTTP) est resté un souci constant au cours de ces dix années, de la première vulnérabilité de 1996 dont je me souvienne, dans *phf* (voir ***http://www.cert.org/advisories/CA-1996-06.html***) à toutes celles qu'on signale en 2006 dans divers logiciels écrits en PHP (à titre d'exemple, le dernier qui a attiré mon attention au moment où j'écris ces lignes concerne le *Content Management System* Joomla, voir ***http://www.joomla.org/content/view/1510/74/***). J'irai même jusqu'à dire que dans le monde Unix/Linux ce sont actuellement les seules vulnérabilités qui donnent encore lieu à des incidents de piratages.

Ce qui a empiré

Les pirates de 1996 étaient essentiellement des étudiants, ou du moins leurs attaques provenaient des réseaux de diverses universités aux quatre coins de la planète, et ils paraissaient mus par le côté *fun* ou *sport*, visant avant tout à prendre le contrôle du plus grand nombre possible d'ordinateurs, mais ne les utilisaient guère que pour partir à la recherche d'autres ordinateurs à pirater pour augmenter leur score, ou dans le pire des cas, pour chahuter des groupes de discussion sur IRC *(Internet Relay Chat)*. Par contre, les pirates d'aujourd'hui sont clairement passés aux activités criminelles et sont en premier lieu intéressés par les gains rendus possibles par le contrôle d'ordinateurs piratés, par exemple dans le soutien logistique aux *spammers* (récolte d'adresses e-mail à spammer sur les machines piratées ou utilisation de celles-ci pour l'envoi de spam), le *phishing* (escroquerie consistant à mettre en place un site Web ressemblant à celui d'une banque pour tromper ses clients et accéder ainsi à leur compte) ou le stockage et la dissémination de fichiers audio/vidéo enfreignant les droits d'auteur. De même, alors qu'il y a dix ans il pouvait se passer plusieurs jours, voire semaines, entre deux incidents de sécurité informatique, de nos jours les pirates sont à l'origine d'un *bruit de fond* permanent de *scans* (recherche d'ordinateurs vulnérables), de telle manière qu'il est devenu pratiquement impossible d'arriver au bout de l'installation de Windows sur un ordinateur connecté à l'Internet sans être piraté, à moins de se placer derrière un *firewall*. Un autre signe qui montre que les pirates sont de nos jours beaucoup plus hargneux est le raccourcissement du temps entre la publication d'une vulnérabilité (ou le simple fait qu'il en existe une, par exemple parce qu'un éditeur de logiciel publie un correctif) et les premiers incidents où ils l'exploitent à leur profit; alors que cette durée se mesurait autrefois en semaines, voire en mois, en 2006 deux ou trois jours suffisent en général, avec même parfois des *zero day exploits*, c'est-à-dire des vulnérabilités connues et exploitées par les pirates avant que le fournisseur du logiciel ne soit au courant et ait pu mettre au point un correctif.

Pour conclure je mentionnerai un phénomène assez récent qui a rendu plus difficile la gestion de la sécurité informatique à l'EPFL: la différence entre l'extérieur et l'intérieur de notre réseau s'atténue à mesure que le prix des ordinateurs portables baisse et que leur usage et celui du Wi-Fi se répand. Cela entraîne en effet que beaucoup de membres de l'EPFL utilisent le même laptop à la maison ou en voyage et se connectent par la suite sur un point d'accès de notre réseau pour leur travail ou leurs études, avec le risque de laisser des virus ou des vers *attrapés* à l'extérieur se propager dans notre réseau. Dans le cas du vers *Blaster* de l'été 2003, nous sommes même sûrs que c'est de cette manière qu'il s'y est faufilé, puisque nous avions fermé au niveau du routeur nous reliant à l'Internet les ports réseau qu'il utilisait pour se propager. Ceci rend nos défenses à ce niveau (projet DIODE, voir ***http://dit.epfl.ch/page51041.html***) moins efficaces qu'on ne pouvait l'espérer, bien qu'elles restent indispensables. Dans un proche avenir, on se prémunira contre ce nouveau problème en effectuant un contrôle plus poussé des ordinateurs portables au moment où ils se connectent à notre réseau.