L'OTP, ou mot de passe à usage unique (One Time Password) :

un résumé proposé par André Liechti, directeur technique de SysCo systèmes de communication SA

La problématique

Que ce soit dans le monde professionnel ou pour les particuliers, l'accès aux différents services passant par Internet (ou interne à une entreprise) se fait encore très régulièrement à l'aide d'un nom d'utilisateur (qui est souvent l'adresse email) et un mot de passe.
Ceci peut s'avérer très dangereux car souvent, le même mot de passe est utilisé, et ce tant pour se connecter au réseau de l'entreprise à distance que pour se connecter à d'autres services sur Internet.

Le problème, c'est qu'un mot de passe "traditionnel" n'offre plus le niveau de sécurité requis pour assurer une protection efficace des informations numériques. En effet, il peut être en principe facilement trouvé, et cela à l'aide de différents principes.

Je vous citerai tout d'abord quelques techniques ne nécessitant pas de connaissances informatiques particulières;

- regarder discrètement "par-dessus l'épaule", une opération qui ne demande aucun moyen technique mais qui est toujours très efficace, éventuellement en filmant discrètement le clavier avec un téléphone portable

- installer physiquement un petit appareil (que l'on appelle keylogger (http://www.commentcamarche.net/contents/virus/keylogger.php3) entre le clavier et l'ordinateur, appareil qui procédera à l'enregistrement de toutes les touches tapées sur le clavier. Ces petits périphériques s'achètent pour moins de 100.- sur Internet (http://www.keelog.com/fr/).

- l'ingénierie sociale, qui consiste à obtenir l'information désirée en exploitant les failles humaines. Citons par exemple le fait d'appeler quelqu'un dans une entreprise (et depuis la salle d'attente, comme cela la personne "ciblée" voit qu'il s'agit d'un appel interne) en indiquant que l'on travaille au service informatique, qu'il y a un problème de sécurité des données et qu'il faudrait immédiatement que vous disposiez de son mot de passe pour aller consolider la sécurité.
  La même démarche peut être faite en appelant chez un particulier (en passant par les renseignements au 1811, en demandant le numéro de téléphone d'une personne puis en demandant d'être relié, ce qui affichera chez votre destinataire non pas votre numéro, mais un numéro spécial de Swisscom (058 219181)), puis en racontant une histoire suffisamment crédible pour tenter d'obtenir le mot de passe désiré

- deviner le mot de passe en connaissant un peu la personne (prénom du conjoint et des enfants, année de naissance, nom de l'animal de compagnie, etc.)

Ensuite, quelques techniques nécessitant plus de compétences:

- installer un petit logiciel qui enregistrera toutes les touches saisies sur le clavier (parfois, les virus font se genre de choses)

- l'attaque par dictionnaire, qui consiste à faire fonctionner un programme informatique qui essayera tous les mots de passe "traditionnels" statistiquement répandus (par exemple les prénoms, les lieux géographique, les noms d'animaux, les suites de lettre sur un clavier, etc.)

- l'attaque par force brute, qui consiste à faire fonctionner un programme informatique qui essayera systématiquement toutes les combinaisons de chiffres, de lettres et de symboles spéciaux

- l'écoute du trafic des données sur un réseau informatique (on dit "sniffer" le réseau dans le jargon), principalement avec les connexions qui ne sont pas chiffrées (site dont l'adresse est uniquement http et non pas https, comme par exemple en allant sur Facebook en tapant simplement www.facebook.com, alors que l'on pourrait tout aussi bien saisir https://www.facebook.com car Facebook propose une connexion cryptée)

Comment faire pour lutter contre cela ?

Pour remédier à cela, il existe notamment ce que l'on appelle l'authentification forte, à savoir l'utilisation d'éléments inviolables et qui ne peuvent pas être volés.

Cela existe depuis fort longtemps pour se connecter en ligne à notre banque par exemple. Malheureusement, jusqu'ici, c'était souvent des solutions plutôt onéreuses, en général propriétaires, qui demandent un arsenal technique ou logistique important (par exemple distribuer des calculatrices et des cartes à puce à tout le monde, envoyer régulièrement des listes à biffer, se munir d'un lecteur d'empreinte, envoyer un code par SMS, etc.).

Quel technique existe alors aujourd'hui pour protéger "fortement" ses accès sans se ruiner ?

Il y a quelques années, plusieurs acteurs du marché de l'authentification forte se sont mis ensemble afin de créer en collaboration un standard pour la génération de mots de passe unique, standard que l'on appellera OATH.

Enfin quelque chose de standard, et comme ces normes sont donc publiées, on trouve beaucoup de solutions financièrement abordables, même très abordables puisque divers produits gratuits issus de la communauté Open Source existent !

Et tout le monde s'y met, et même Google propose depuis environ une année la possibilité de se connecter par un mot de passe à usage unique à ses services Internet (http://www.google.com/support/a/bin/answer.py?answer=1037451), ceci à l'aide de son "Google Authenticator".

Comment fonctionne alors le mot de passe à usage unique, appelé OTP (One Time Password) ?

Il s'agit de faire générer automatiquement des mots de passe (généralement de 6-8 chiffres ou caractères) par un petit appareil dédier à cet usage. Chaque minute environ, un nouveau mot

de passe est affiché, et si il est utilisé, ce mot de passe ne pourra plus être utilisé une seconde fois, même dans la seconde qui suit.

En fait, si le principe existe depuis longtemps (RSA propose un produit de ce genre depuis des années sous le nom de SecurID), la mise en place d'une norme et surtout l'avènement des smartphones permettent de déployer massivement ce genre de solution.

Beaucoup de générateurs de mots de passe à usage unique compatibles OATH sont disponibles sur les différents "Markets" des smartphones, que ce soit sous Android, iPhone, BlackBerry ou encore Windows Mobile. Il en existe même en Java, ce qui permet de les installer sur quasiment tous les autres téléphones, comme par exemple ceux de type Nokia tournant sous le système Symbian.

A l'usage, il faudra normalement toujours saisir un utilisateur et un mot de passe à l'écran, puis il faudra encore saisir le mot de passe à usage unique, et c'est seulement après la saisie de ce trio gagnant que l'accès va se faire.

Avec les smartphones, il existe également une variante du principe, puisqu'il est possible de saisir un code PIN sur le téléphone, et la génération du mot de passe à usage unique se fera en tenant en plus compte du code tapé. Ainsi, même en cas de vol du smartphone (sans qu'il soit protéger, ce qui n'est pas très malin...), la génération du'un mot de passe à usage unique n'est toujours pas possible !

Mais comment le serveur de l'autre côté peut connaître tous ces mots de passe ?

Chaque générateur de mot de passe comporte un numéro de série électronique, et ce numéro de série électronique est lié à une formule mathématique qui est connue par le générateur de mot de passe et par le serveur.

Ensuite, il y a deux variantes.

Dans le premier cas, ceci généralement pour des générateurs de mots de passe sous forme de porte clé,
on applique donc cette formule mathématique en incrémentant un paramètre d'une unité à chaque génération de mot de passe, la génération se faisant un presant sur un bouton du porte clé (ou dans le cas d'un smartphone en cliquant sur un bouton de génération).

Dans l'autre cas, le paramètre est le temps qui passe que l'on découpe en tranche de 30 secondes par exemple, et on numérote chaque tranche en partant de la référence 0 pour la première tranche fixée au 1er janvier 1970.

Le générateur tout comme le serveur en font de même, et le serveur accepte les codes dans une certaines tolérances (disons les 20 prochains attendus dans le cas d'une génération en pressant une touche, et les codes d'il y a plus ou moins 10 ou 20 minutes pour les codes basés sur des tranches horaires).

Dès qu'un code est correct, le serveur sait de quel code il s'agit, il va donc pouvoir se synchroniser sur ce code et refuser ce code et tous les codes antérieurs.

Pourquoi avoir crée une librairie en Open Source appelée multiOTP, et quels sont les avantages ?

Chez SysCo (http://www.sysco.ch/), nous voulions pouvoir proposer à nos clients une solution d'authentification forte avec génération de mots de passe uniques qui soit abordable, car nous travaillons essentiellement avec des PME.

Après avoir étudié le marché des solutions existantes, il n'y avait rien de vraiment satisfaisant, notamment si l'on voulait pouvoir faire fonctionner cela sous Linux ET sous Windows, ce dernier étant fortement répandu dans les PME.

Nous avons donc développé notre propre librairie (http://www.multiOTP.net/), et comme nous sommes également des utilisateurs de solutions Open Source, nous faisons parfois quelques développements en Open Source afin de "renvoyer l'ascenseur". Afin de pouvoir proposer une solution complète et gratuite fonctionnant sous Windows, nous avons également utilisé un produit annexe fourni par un développeur turc (http://www.tekradius.com/ (anglais) avec lequel nous avons collaboré afin d'y ajouter certaines fonctionnalités.

De plus, contrairement aux solutions propriétaires bridées et "hermétiques", un connaisseur pourra analyser le code, que ce soit pour s'assurer du niveau de sécurité des algorithmes obtenus ou pour proposer des modifications et des améliorations. C'est un argument non-négligeable pour des logiciels de sécurité, notamment pour s'assurer qu'aucun mouchard d'agences fédérales ou d'organisations malveillantes n'est installé à l'intérieur de la librairie.

En utilisant cette librairie, contrairement aux produits commerciaux ou les numéros de série électroniques sont fournis et stockés par le fabriquant, c'est l'utilisateur de la librairie qui peut générer ses propres numéros de série électroniques.

Ainsi, cela nous met à l'abri d'un vol massif de numéros de série chez le fabricant, comme par exemple le cas de RSA qui s'est fait voler des données en mars de cette année (http://www.zdnet.fr/actualites/anatomie-d-une-attaque-rsa-disseque-l-intrusion-dont-il-a-ete-victime-39759722.htm), données utilisées ensuite vraisemblablement (http://www.securityvibes.fr/menaces-alertes/lockheed-martin-rsa-hac/) pour pénétrer notamment dans les systèmes informatiques du fournisseur de la défense américaine Lockheed Martin (tiens, on pourrait leur proposer notre librairie ;-)

Cette libraire (qui s'installe donc du côté du serveur, de l'application Internet ou du site web concerné) est compatible avec un grand nombre de générateur de mot de passe, que ce soit ceux à la norme oath (dont Google Auhtenticator, iOTP sous pour iPhone, DroidOTP pour Android, ou tout autre clé physique compatible), mais aussi ceux utilisant le protocole ouvert mOTP, protocole qui génère le mot de passe à usage unique en se basant sur le temps.

Quels sont les coûts pour la mise en place de cette librairie multiOTP ?

Côté coûts, il n'y a aucun frais de licence, et la mise en place peut se faire par le service informatique interne de la PME interne, ou alors en mandatant son prestataire informatique habituel, ce qui se limitera à payer le temps de l'installation qui ne dépassera pas la demi-journée.

Pour les générateurs de mot de passe à usage unique, on en trouve de très bons gratuits sur les différents Store des smartphones, inutile de payer pour cela.
Enfin, si l'on désire acheter quelques clés physiques de type porte-clés, il faudra compter CHF 50 à 80.- selon le modèle choisi, peut-être un peu moins en les achetant directement à l'étranger via Internet

Du côté des entreprises, quelles sont les personnes intéressées à mettre en place cette librairie ?

Notre librairie est notamment fournie par un distributeur suisse pour certains de leurs produits de sécurité dont la solution payante ne fonctionne que sous Windows! Sinon, nous avons déjà installé ce système dans différentes PME en suisse romande, comme par exemple chez vos consœurs, les radios locales romandes RJB, RTN et RFJ. (ndlr : lors de la mise en service, je leur ai demandé si j'osais les citer, et j'ai reçu leur approbation).

Plusieurs intégrateurs suisses et étrangers nous ont également indiqué utiliser cette librairie pour mettre en place une authentification forte chez leurs clients. Il arrive parfois que nous fournissions du support supplémentaire pour des cas particuliers, ce qui nous amène à recevoir occasionnellement un « don » PayPal de l'un ou l'autre des intégrateurs utilisant notre librairie.

Dans le cadre de l'Application Security Forum de 2011 (http://www.appsec-forum.ch), un forum francophone se déroulant les 26 et 27 octobre 2011 à la Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud et qui va traiter de la sécurité logicielle en générale, nous allons animer un atelier d'une demi-journée expliquant comment intégrer l'authentification forte dans des applications. A noter que cet atelier proposé le mercredi après-midi 26 octobre est gratuit pour les étudiants, et chaque participant recevra un générateur de mot de passe à usage unique sous forme de porte-clés. Le lendemain, la participation à l'une ou l'autre des 18 conférences proposées est gratuite pour tout le monde.

Liens :
Lien sur la librairie multiOTP développée André Liechti : http://www.multiOTP.net/
SysCo systèmes de communication sa : http://www.sysco.ch/
Application Security Forum : http://www.appsec-forum.ch
Projet mOTP : http://motp.sourceforge.net/ (anglais)
L'initiative pour une authentification ouverte (oath) : http://www.openauthentication.org/ (anglais)

Micro-CV d'André Liechti
Intéressé très tôt par l'électronique et l'informatique (il a écrit ses premières lignes de codes à l'âge de 12 ans sur un Commodore VC-20), André Liechti a tout d'abord obtenu un diplôme d'Ingénieur ETS (HES) en électronique à Saint-Imier (Suisse) avant de poursuivre par un diplôme d'Ingénieur EPF en Systèmes de Communication à Lausanne (Suisse) et à l'Institut

Eurécom de Sophia-Antipolis (France). Son travail de diplôme effectué dans la Silicon Valley en 1997 le conforte dans l'idée de créer une entreprise dans le domaine des systèmes de communication à son retour.

Directeur technique de SysCo systèmes de communication sa depuis 1998, André Liechti est également chargé des cours "Applications Internet" pendant une dizaine d'années à l'Ecole d'Ingénieurs de Saint-Imier (actuellement HES-SO) ainsi que pour des études post-grades. Il est aussi actif dans la communauté open source, et principalement en PHP. Son expertise en sécurité informatique l'amène notamment à développer la librairie multiOTP, une librairie open source en PHP permettant d'intégrer de l'authentification forte selon des protocoles standards dans de nombreuses applications, offrant ainsi une alternative libre facile à mettre en œuvre.

RTS – Emission « On en parle », 07.11.2011