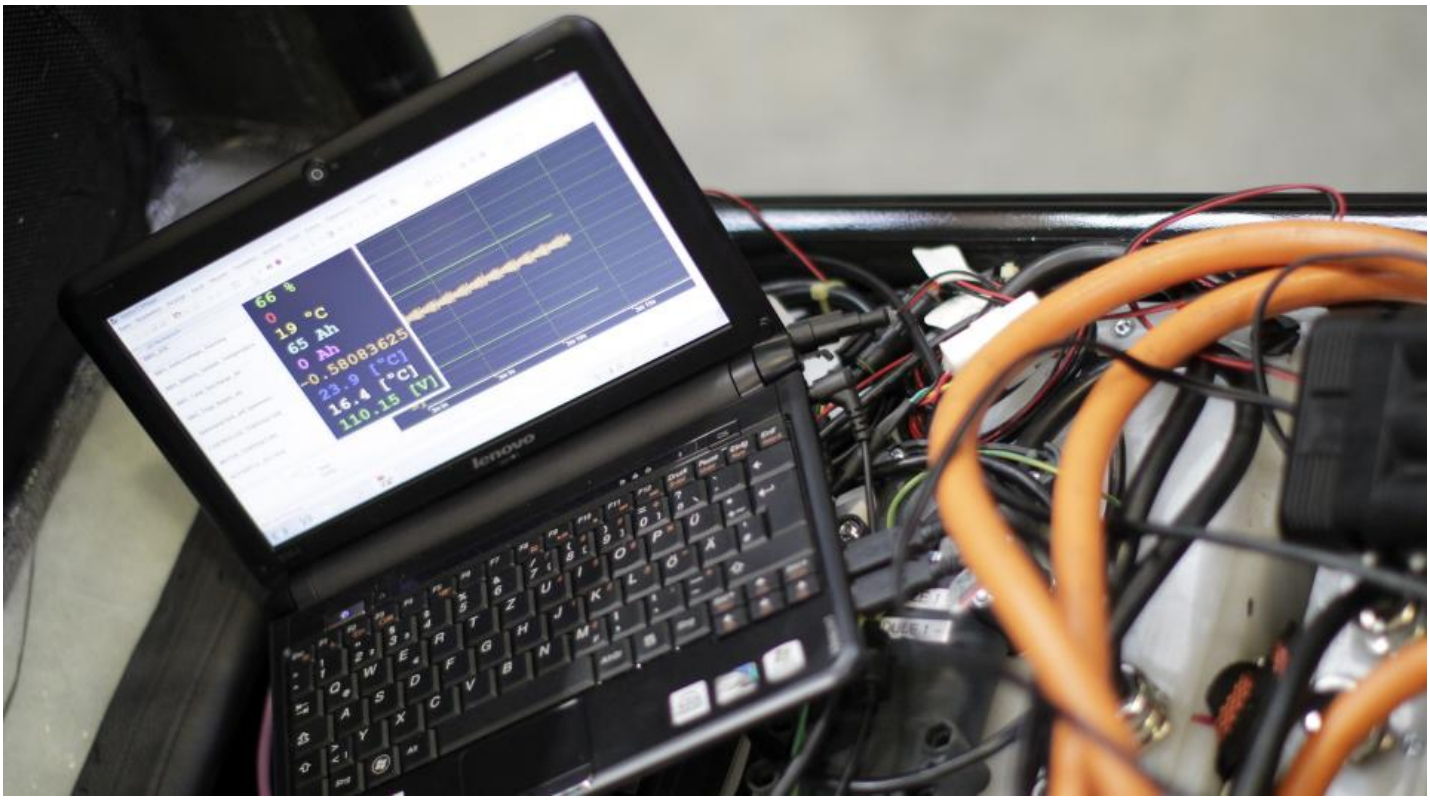
08 juin 2014
Logiciel de cryptage

Mais que s'est-il vraiment passé chez Truecrypt ?



Depuis le mercredi 28 mai, le site dédié au logiciel de chiffrement TrueCrypt affiche une mise en garde concernant les dangers potentiels de son utilisation. Chez les cryptologues professionnels et amateurs du monde entier, c'est la consternation et la confusion.

Avec H16

Une tempête a soufflé la semaine dernière sur Internet. Oh, pas une de ces tempêtes médiatiques basée sur un lolcat truculent, un président enscooterifié ou un buzz médiatique facile, et c'est probablement pour cela que vous n'en avez pas entendu parler. Il n'en reste pas moins que ce qui s'est passé autour de Truecrypt est particulièrement intéressant.

Avant d'aller plus loin, rappelons que Truecrypt est un logiciel gratuit, dont le code source est disponible, qui permet de chiffrer des données sur un disque dur. Le chiffrage est ainsi fait que l'utilisateur légitime, qui fournit son mot de passe au démarrage de la machine, ne voit pas la différence avec un disque dur normal (non chiffré) ; l'encryptage est réalisé à la volée, de façon transparente pour le système d'exploitation ou l'utilisateur. En revanche, un utilisateur qui ne dispose pas de la clé d'accès ne pourra pas lire le disque ainsi chiffré.

Ce logiciel existe depuis une dizaine d'années, et son mode de fonctionnement très simple mais efficace lui a valu une excellente renommée auprès de ses millions d'utilisateurs. Le cryptage utilisé (qui peut être basé sur AES, Serpent et Twofish) est suffisamment solide pour que le FBI, notamment, ne parvienne pas à le casser dans une affaire financière où des disques, saisis comme pièces à conviction, n'ont pas livré leurs secrets après des mois d'analyse par le bureau fédéral américain.

C'est donc avec consternation que mercredi 31 mai, la page officielle du logiciel qui présentait le produit a été remplacée par une page rudimentaire expliquant essentiellement que Truecrypt n'est pas sûr, et que l'utiliser ne permet pas d'assurer la confidentialité de ses données. La consternation est d'autant plus grande que l'ensemble du message est rédigé et signé avec les clés habituelles des développeurs officiels du produit, et qu'il invite les utilisateurs à se rabattre sur Bitlocker pour Windows, produit notoirement connu pour disposer de facilités spécifiques de décryptage pour les autorités américaines. Or, jusqu'à présent, Truecrypt avait pour lui d'avoir résisté à l'épreuve du temps en n'ayant jamais présenté de grandes vulnérabilités. En outre, un audit de la cryptographie utilisée est actuellement en cours pour déterminer sa solidité générale. Les failles rapportées en avril dernier ne montraient en tout cas rien qui permette de classer le produit comme à ce point dangereux à utiliser. D'ailleurs, l'un des pontes de la cryptographie, Bruce Schneier, expliquait récemment continuer à utiliser le produit malgré les quelques problèmes découverts.

Le reste de l'audit permettra peut-être de trouver une faille suffisamment importante pour remettre en cause le modèle utilisé par Truecrypt depuis 2004, année de son apparition, mais on peut légitimement en douter. En tout cas, les exécutables des versions historiques, disponibles sur la version précédente du site avant ce revirement dramatique, n'ont pas montré d'anomalies douteuses.

La situation est donc particulièrement étrange puisqu'on découvre qu'une équipe, qui a travaillé pendant dix ans sur un produit qui a déjà largement prouvé son efficacité, vient de saborder complètement son travail en redirigeant ses utilisateurs vers des alternatives douteuses. Les rumeurs vont évidemment bon train sur les forums spécialisés, mais essentiellement, trois hypothèses surnagent au milieu des différentes possibilités plus ou moins farfelues :

- D'une part, il pourrait bien y avoir une grosse faille de sécurité, grosse au point que les développeurs ont préféré saborder leur outil plutôt que l'admettre ou tenter de la réparer. C'est évidemment une réaction très étrange d'autant que le code source, largement disponible, aurait permis une correction rapide par la communauté des développeurs intéressés à la survie et à la maintenance du projet.
- D'autre part, il pourrait s'agir d'une méthode de la part de l'équipe de développement pour laisser tomber tout support du produit, et inciter (par la peur, donc) le reste du monde à reprendre en charge le développement. Cette hypothèse intéressante est développée ici, et permet en tout cas de relativiser la disparition de la page officielle et des codes sources des précédentes versions. Du reste, internet étant ce qu'il est, on trouve facilement des bibliothèques qui contiennent toutes les versions de Truecrypt jusqu'à mercredi dernier.
- Enfin, la nouvelle page du site rapidement bricolée tendrait à faire penser à un « warrant canary », expression américaine utilisée dans un cas assez spécifique de législation américaine : en substance, lorsqu'un fournisseur de service reçoit une assignation secrète (essentiellement celles en lien avec le Patriot Act, article 18 U.S.C. §2709(c)), il lui est interdit de divulguer à des tiers son statut légal (grossièrement équivalent à une mise en examen), mais il peut, sur demande d'un client, indiquer si, sur une période donnée, il n'était pas sujet à une telle assignation. Par analogie, l'acte étrange de l'équipe de développement de Truecrypt serait une forme de mise en garde minimaliste permettant de prévenir les utilisateurs que l'ensemble de l'équipe a subi des menaces ou des pressions de la part d'une organisation gouvernementale et qu'à ce titre, l'ensemble des développements de Truecrypt est sujet à caution.

L'avenir dira peut-être ce qu'il en est exactement, mais au-delà des péripéties qui secouent actuellement le monde de la cryptographie et celui, plus large, des logiciels de chiffrement de disques à la volée, on peut néanmoins noter qu'encore une fois, la communauté Internet a prouvé sa capacité d'organisation. En effet, moins d'une semaine après l'annonce surprise de l'abandon de Truecrypt est apparu un nouveau site, Truecrypt.ch, dont les auteurs entendent reprendre le flambeau, incorporer les corrections éventuelles que l'audit, toujours en cours, auraient jugées nécessaires, et maintenir le code actuel. On ne peut, à ce stade, présumer de la capacité de ce binôme de développeurs à maintenir le code et le produit, mais leur prompte réaction montre en tout cas que le chiffrement de données personnelles est une idée jugée suffisamment importante pour mobiliser rapidement les énergies.

Et c'est le cas : d'un côté, nous avons des institutions gouvernementales dont les moyens grossissent de façon exponentielle, et dont le but ultime est bien de tout savoir sur vos plus intimes motivations, vos convictions religieuses, politiques ou sentimentales. Pour celles-là, la cartographie précise de chaque être humain est devenu un préalable non seulement nécessaire mais aussi techniquement réalisable (ce qui est encore plus effrayant) à leur soif inextinguible de contrôle. Ces institutions ne reculeront devant aucun moyen pour vous ficher, quand bien même (de l'aveu même de ceux qui y travaillent) la masse de données résultante ne leur sera pas utile pour remplir leur ordre de mission officiel. Terrorisme, crimes et délits, oubliez ça : ces technologies servent d'abord et surtout à surveiller tout le monde.

De l'autre, il n'existe guère que ces moyens cryptographiques pour se préserver quelques domaines de vie vraiment privée, où l'État et ses agences ne pourront venir mettre leur yeux. Il est donc absolument impératif que des systèmes voient le jour, soient maintenus et massivement utilisés pour assurer à chaque humain un minimum de protection contre les grandes oreilles gouvernementales.

Cette affaire Truecrypt montre encore une fois qu'aucune technologie n'est acquise, aucune sécurité n'est trop forte contre les moyens que déploient les États pour asservir leurs populations. Et cette affaire montre aussi, heureusement, que nombreux sont ceux qui en ont conscience et qui sont prêt à sacrifier leur temps et leur savoir pour calmer les ardeurs gouvernementales.

NB : Cet article a été préalablement publié surle blog d'Hasthable