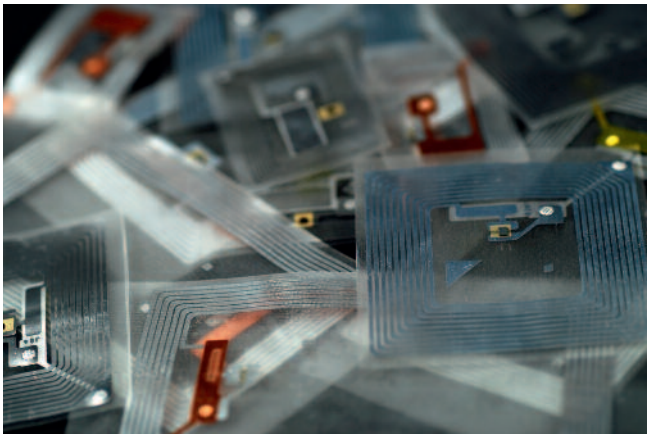
Le défi de la sécurité des systèmes informatiques ouverts

MAI 2013

De nos jours, les systèmes de sécurité informatique sont mis à rude épreuve : stockage de données dans le *cloud* (informatique en nuage), micropuces omniprésentes, réseaux sociaux… Non seulement la communication permanente sur le réseau expose les systèmes cryptographiques à des légions de connexions menaçantes, mais les mécanismes de sécurité doivent en plus désormais fonctionner sur des appareils à faibles capacités de calcul, comme les téléphones portables. Les anciens algorithmes sont ainsi devenus lourds et vulnérables aux usurpations d'identité et autres violations de la vie privée. Reconstruire cette sécurité est un défi auquel participe l'Institut Mines-Télécom, et en particulier l'équipe R3S (Réseaux, systèmes, services et sécurité) de Télécom SudParis, dirigée par Maryline Laurent. Le travail de ces chercheurs consiste à mettre au point de nouvelles architectures et techniques cryptographiques avancées, en collaboration avec d'autres laboratoires de recherche et des industriels.

Un des problèmes pour la sécurité est le stockage sur des *clouds* : « *Aujourd'hui, un système pourvu d'un seul point d'entrée est relativement facile à sécuriser,* explique Maryline Laurent, *mais quand un* cloud *se trouve distribué sur tout équipement disposant de ressources de stockage (disque), alors protéger les données confidentielles face à d'éventuels malfaiteurs est un véritable problème.* » Les particuliers sont tout autant concernés que les industriels, car les box — les boîtiers des fournisseurs d'accès à l'internet — relient les appareils de la maison au monde entier.



L'équipe R3S travaille donc en coopération avec les opérateurs téléphoniques, comme Orange, pour concevoir des solutions capables d'améliorer la sécurité des contenus. Leur stratégie : les rendre confidentiels et anonymes. « *Sur un réseau,* explique Maryline Laurent, *chaque utilisateur se voit attribuer un identifiant unique pour être reconnu. Nous avons utilisé une approche à deux étages, le premier étage permettant de chiffrer les données à l'aide d'une clé symétrique et le second étage permettant de sécuriser dans le* cloud *la clé symétrique à l'aide de la méthode dite* Id-Based *; la clé qui permet de chiffrer et déchiffrer, la clé symétrique, est générée par l'utilisateur à partir de son identifiant.* » De cette manière, un intrus ne peut non seulement pas lire les données qu'il dérobe, mais il ne peut même pas savoir à qui elles appartiennent.

De plus, la méthode *Id-Based* habituelle ne semblait plus suffisante pour un système aussi ouvert qu'un *cloud*. En effet, ce n'est plus seulement un utilisateur, mais des groupes entiers d'utilisateurs qui partagent et accèdent aux mêmes données. Une subtilité supplémentaire a donc été trouvée : « *Pour augmenter la sécurité, nous avons décidé que notre cryptage* Id-based *générerait sa clé non plus uniquement à partir de l'identifiant, mais aussi à partir des données elles-mêmes.* » Cela donne un *cloud* original, où chaque donnée possède son propre identifiant, qui est une sorte de résumé de son contenu. Il faut alors savoir ce que l'on cherche pour le trouver.

Sécuriser un système passif : le défi

Toutefois, cette sécurité requiert de la part de l'utilisateur beaucoup de puissance de calcul. Or, de nos jours, les systèmes sont de plus en plus portables et réduits. « *Un autre défi,* raconte Maryline Laurent, *consiste à pouvoir authentifier rapidement des appareils comme des* smartphones, *qui doivent se limiter à des calculs simples.* » Que ce soit par un mot de passe ou par un autre moyen, cette authentification doit apporter la preuve que l'utilisateur du réseau est bien celui qu'il prétend être.

Maryline Laurent a dirigé des travaux sur un cas extrême de manque de puissance, les puces RFID (*Radio Frequency Identification*). Celles-ci sont minuscules, mais permettent d'identifier un objet à distance. Le manque de sécurité des puces RFID est la raison pour laquelle l'Europe est extrêmement réticente à leur utilisation. Un nouveau règlement européen doit d'ailleurs permettre d'actualiser le règlement général sur la protection des données. Aux États-Unis, la volonté des groupes industriels a déjà bien installé ces puces RFID dans les usages. Elles remplacent par exemple toutes les étiquettes et codes-barres chez le grand distributeur Walmart. Intégrées aux objets du quotidien, elles permettraient de scanner à la volée un sac à main pour savoir s'il contient le briquet que l'on cherche, ou une bague volée. Mais la vie privée est alors très rapidement menacée : sans authentification robuste, n'importe qui peut fouiller votre sac à main sans permission ! Réussir à bloquer ces accès serait le sésame pour ouvrir le marché européen aux puces RFID.

Pour résoudre le problème du manque de puissance, il a fallu innover. « *Nous avons repris la méthode NTRU (*N-th degree truncated polynomial ring*), une méthode à clé publique très prometteuse, et nous l'avons adaptée. Il est désormais possible de répartir les calculs cryptographiques à effectuer : toute la charge de travail est donnée au serveur et la puce RFID n'a plus que quelques opérations binaires à effectuer.* »

Techniquement, ce qui a été développé est un système d'authentification mutuelle, très léger, dont le principe de calcul a consisté à passer le NTRU en espace polynomial binaire et à proposer une nouvelle méthode de génération/multiplication de polynômes. « *On peut désormais réaliser des multiplications par de simples opérations de décalages.* »
Les RFID bénéficieront ainsi d'une authentification forte. « *Notre projet sur les RFID est très avancé et nous a permis de déposer deux brevets. Et bien entendu, si ce cryptage fonctionne sur des puces passives, il fonctionne sur n'importe quelle machine.* »

Reprendre le contrôle de son identité

Ces deux développements permettent de sécuriser des données, mais il y a un autre aspect à prendre en compte pour que les systèmes méritent la confiance des utilisateurs. Il s'agit de la mise en mouvement des données : la sécurité des flux. « *L'exemple classique,* raconte Maryline Laurent, *est celui de Facebook ; revenez un an après vous être désinscrit, vous vous rendrez compte que toutes les données de votre profil ont été conservées. Cela n'est pas compatible avec le droit à l'oubli préconisé par la réglementation européenne. Dans les réseaux sociaux actuels, les utilisateurs perdent le contrôle sur les informations qu'ils transmettent et qu'ils génèrent. Ils ignorent tout de la localisation de leurs données, si elles sont dupliquées et qui y a accès.* »
L'équipe de Maryline Laurent coopère sur ce problème avec le W3C (*World Wide Web Consortium*), l'organisme qui s'occupe de la normalisation des technologies du web. L'idée est de tester sur un outil, nommé *MyProfile*, des solutions qui permettent à l'utilisateur de gérer l'accès et la diffusion de ses données dans son réseau social. Entre autres, l'utilisateur y contrôle physiquement ses données, comme si elles se trouvaient sur son ordinateur personnel. Ce ne sont pas les données de l'utilisateur qui sont transmises, mais seulement leur localisation sur le disque dur, ce qui est rendu possible avec la technologie du web sémantique. Le réseau doit ensuite y accéder à chaque fois. De cette manière, si l'utilisateur souhaite les supprimer, nul ne peut plus y avoir accès.
Malheureusement, il sera difficile de faire adopter aux réseaux sociaux ces technologies respectueuses, qui sont clairement à leur désavantage. Il faut donc créer des réseaux concurrents. Le grand public est de mieux en mieux sensibilisé aux risques et il souhaitera *a priori* migrer vers des réseaux qui respecteront sa vie privée, où il aura un meilleur contrôle et saura ce que deviennent ses données.

Une sécurité à entretenir

Malgré toutes ces mesures, est-il possible d'être vraiment en sécurité ? Nous confions toujours plus de nos secrets à un nombre croissant d'acteurs. En fin de compte, la vulnérabilité ne vient pas tant du système que de l'utilisateur lui-même : « *Il est mal armé pour maîtriser l'étendue de ses prises de décisions sur la sécurité de ses données et de son système,* regrette Maryline Laurent. *Notre rôle en tant que chercheur est de concevoir des solutions pour préserver l'usager des risques liés aux nouvelles technologies, le guider dans ses prises de décisions, et le mettre en confiance, pour qu'il sache que ses efforts ne seront pas vains.* »

La chaire Valeurs et politiques des informations personnelles

Titulaire d'un doctorat en sciences de l'informatique, Maryline Laurent est devenue spécialiste de la sécurité dans les réseaux IPv4 et IPv6 (*Internet Protocol*). Professeur à Télécom SudParis, elle anime depuis plusieurs années des recherches sur les problématiques de sécurité et de protection des données personnelles dans le *cloud*, les systèmes contraints, les réseaux sociaux et la gestion d'identités. C'est ce qui lui vaut aujourd'hui de co-animer la chaire pluridisciplinaire de l'Institut Mines-Télécom lancée en 2013, intitulée Valeurs et politiques des informations personnelles.
L'objectif de cette chaire est de contribuer aux réflexions sur la régulation juridique, éthique, économique et technique des informations personnelles et des identités numériques. La pluridisciplinarité est donc la clé de cette équipe : si Maryline Laurent s'occupe des aspects techniques, elle travaille au sein de cette chaire avec une juriste, un philosophe et un économiste ! C'est leur complémentarité qui permet d'espérer un jour pouvoir apporter des réponses à une vraie problématique sociétale.

- **www.informations-personnelles.org**

Rédaction : Umaps - Mise en pages : *implica* CR&A - Crédit photos : Alberto Lozano (Dreamstime.com), Institut Mines-Télécom

Suivez l'actualité recherche & innovation de l'Institut Mines-Télécom

http://blogrecherche.wp.mines-telecom.fr et www.twitter.com/Mines_Telecom

Contact Information
recherche & innovation
recherche@mines-telecom.fr
Institut Mines-Télécom
46 rue Barrault - 75634 Paris cedex 13
France
www.mines-telecom.fr

À propos de l'Institut Mines-Télécom

L'Institut Mines-Télécom est un établissement public dédié à l'enseignement supérieur, la recherche et l'innovation dans les domaines de l'ingénierie et du numérique. Il est composé des dix grandes écoles Mines et Télécom sous tutelle du ministre du Redressement productif, deux écoles filiales et compte deux partenaires stratégiques et un réseau de onze écoles associées.

L'Institut Mines-Télécom est reconnu au niveau national et international pour l'excellence de ses formations d'ingénieurs, managers et docteurs, ses travaux de recherche et son activité en matière d'innovation. Les écoles de l'Institut Mines-Télécom sont classées parmi les toutes premières grandes écoles en France.

L'Institut Mines-Télécom est membre des alliances nationales de programmation de la recherche Allistene, Aviesan et Athena. Il entretient des relations étroites avec le monde économique et dispose de deux instituts Carnot. Chaque année une centaine de *start-ups* sortent de ses incubateurs.