Labo story

Toujours un pas d'avance sur la malveillance

Laboratoire de sécurité et de cryptographie
Collaborateurs: 9
Site internet:
↪ lasecwww.epfl.ch

↪ INFORMATIQUE: Assurer la fiabilité des échanges menés sur le net et déjouer, en amont, les attaques informatiques sont les buts du laboratoire de sécurité et de cryptographie de l'EPFL.

Sarah Perrin
Médiacom
Photos: Alain Herzog

Paiements en ligne, opérations bancaires et autres communications numériques… Le nombre d'échanges réalisés sur le net va croissant et assurer leur sécurité est une tâche de plus en plus complexe. Ce d'autant plus que de nouvelles formes d'attaques sont toujours inventées par les hackers ou les cyber-espions. Pour les déjouer, une seule arme s'avère véritablement efficace: anticiper et avoir constamment un pas d'avance.

Dirigé par le professeur Serge Vaudenay, le Laboratoire de sécurité et de cryptographie de l'EPFL comprend une équipe d'une dizaine de chercheurs spécialisés en maths, informatique et systèmes de communication.

Ces spécialistes planchent pour trouver, en amont, toutes les failles possibles des systèmes de sécurité existants et développer les réponses et outils adéquats pour s'en protéger. Il y a trois ans, l'équipe avait par exemple testé des claviers d'ordinateurs et mis au jour qu'il était possible de les pirater à distance en interceptant les ondes électromagnétiques qu'ils dégagent et ainsi d'en espionner la frappe. Une nouvelle qui avait été relayée dans de nombreux journaux.


Serge Vaudenay


Ioanna Boureanu

Le laboratoire travaille également sur la fiabilité des documents biométriques, des puces RFID ou des systèmes de communication sans fil. Le tout en ne perdant jamais de vue la nécessité de respecter la sphère privée et les libertés individuelles.

TESTER LA RECETTE

Active au Laboratoire de sécurité et de cryptographie depuis une année, **Ioana Boureanu** est chargée de vérifier la fiabilité des protocoles de sécurité, ces séries d'étapes et de règles établies pour que deux ordinateurs – par exemple celui d'une banque et celui de son client – puissent échanger des données et opérer des transactions. «C'est un peu comme une recette, illustre la chercheuse d'origine roumaine. Il comporte un certain nombre d'ingrédients, que les deux parties qui veulent entrer en communication doivent utiliser de la même manière.»

La jeune post-doc vérifie notamment que la sécurité d'un protocole soit assurée dans le temps, même après l'ouverture de nombreuses sessions. Elle teste également sa composabilité, c'est-à-dire si un protocole reste sûr s'il est associé à un autre protocole.

Son travail consiste aussi à concevoir de nouveaux protocoles, destinés à renouveler régulièrement les anciens et rendre les échanges plus sûrs et efficaces. «Cela demande beaucoup de maths et d'imagination, décrit-elle. La technologie avançant, il faut toujours inventer du neuf pour être sûr que nos algorithmes ne puissent pas être craqués.»

DES INFOS TOP SECRÈTES QUI DOIVENT LE RESTER

Le système de chiffrement – cipher en anglais – consiste en la définition d'algorithmes qui codent des données de manière à les rendre impossibles à décrypter si on ne possède pas la clé adéquate. Cette méthode est notamment utilisée lors de transactions réalisées par carte de crédit et pour le transfert d'informations top secrètes.

Doctorante au Laboratoire de sécurité et de cryptographie depuis trois ans, **Aslı Bay** les analyse et les teste pour en trouver les moindres faiblesses qui pourraient être utilisées par des hackers. «Ces méthodes de chiffrement sont des éléments très sûrs, et les failles sont très rares, précise la spécialiste originaire de Turquie. Le standard AES, le plus utilisé, n'a par exemple jamais pu être cassé. Mais il est nécessaire de créer de nouveaux systèmes de chiffrement régulièrement et de les mettre à l'épreuve, pour s'assurer qu'ils restent fiables dans un environnement où les ordinateurs deviennent de plus en plus puissants.»


Aslı Bay

UN SYSTÈME DE CHIFFREMENT À INVENTER

Avoir un œil affûté sur l'avenir, c'est aussi anticiper l'avènement de… l'ordinateur quantique. Doctorant fraîchement débarqué au labo, **Alexandre Duc** commence à travailler sur le design d'un système cryptographique adapté à cette nouvelle technologie dont parle tout le monde informatique. «C'est un vrai challenge», s'enthousiasme le jeune chercheur valaisan.

Induit par la miniaturisation toujours plus grande des composants électroniques, l'ordinateur quantique est théoriquement capable de réaliser simultanément une quantité astronomique de calculs et de simuler une infinité de processus physiques. Surtout, il peut déchiffrer tous les systèmes et protocoles de sécurité existants en un rien de temps, les rendant ainsi immédiatement caduques… Même s'il faudra encore des années avant de voir un tel ordinateur apparaître dans les ménages, il s'agit de s'y préparer, souligne Serge Vaudenay.

PAS DE FRITURE ENTRE SOI ET SA VOITURE…

Ouvrir, à distance et par un simple clic, les portes de sa voiture ou le portail de sa maison, c'est bien pratique. Mais il s'agit de s'assurer que personne d'autre ne puisse le faire en interceptant le canal de communication existant entre la puce RFID située sur la clé de contact et son lecteur implanté dans le véhicule…

Afin de parer à ce genre d'attaque, **Katerina Mitrokotsa**, chercheuse post-doc (Marie Curie Fellow) d'origine grecque, au laboratoire depuis deux ans, travaille sur les protocoles délimiteurs de distance (distance-bounding protocols). En calculant le temps que mettent les ondes électromagnétiques à atteindre le lecteur RFID et la qualité de leurs perturbations, ce type de protocole permet de s'assurer que la clé est bien à proximité du véhicule au moment de la commande d'ouverture.

Dans le cadre d'un important projet, la jeune scientifique planche aussi sur la sécurité des données biométriques et le respect de la vie privée des individus. Il s'agit de développer un outil qui trie les informations pouvant être transmises de celles qui doivent rester secrètes et assure ainsi que les premières ne soient pas liées à une identité. «C'est utile dans le domaine de la santé, précise Katerina Mitrokotsa. Une personne pourra par exemple se rendre dans une pharmacie, faire connaître, grâce à un document numérique, les détails de sa maladie et obtenir les bons médicaments, sans pour autant avoir à divulguer son nom ou en laisser une trace informatique.» Ξ


Alexandre Duc


Katerina Mitrokotsa