Nancy, le 09 novembre 2018

COMMUNIQUÉ DE PRESSE

Une nouvelle percée en sécurité informatique

Des failles de sécurité dans le protocole mobile 5G

Jannik Dreier, maître de conférences à l'Université de Lorraine (Télécom Nancy), en collaboration avec des chercheurs de l'ETH de Zurich (Suisse) et de l'Université de Dundee (Ecosse) ont soumis la future norme de communication mobile 5G à une analyse de sécurité précise. **Leur conclusion : une protection de données améliorée par rapport aux normes précédentes 3G et 4G mais des failles persistent.**

Les deux tiers de la population mondiale, soit environ cinq milliards de personnes, utilisent quotidiennement un téléphone mobile. Ils se connectent au réseau mobile via leurs cartes SIM, passent des appels, envoient des SMS, échangent des images ou effectuent des achats. À maintes reprises, des criminels ont pu accéder à des communications lors de la connexion de l'appareil au réseau afin d'intercepter des conversations ou de voler des données. La cinquième et dernière génération de communications mobiles (5G) prévue pour un déploiement d'ici 2020 devrait offrir aux utilisateurs plus de sécurité. Afin de garantir cette sécurité, le périphérique et le réseau doivent pouvoir s'authentifier l'un et l'autre au moment de la connexion au réseau. En même temps, les échanges de données, l'identité et la localisation de l'utilisateur doivent rester confidentiels. Cela a donc été mis en œuvre via un protocole de communication appelé Authentification and Key Agreement (AKA) depuis l'introduction de la norme 3G.

La norme de communication mobile 5G ne corrige pas toutes les lacunes

À l'aide de l'outil de vérification de protocoles de sécurité Tamarin développé par l'ETH de Zurich, l'équipe PESTO de Nancy, commune à Inria et au Loria, et le CISPA de Sarrebruck, l'équipe de chercheurs a examiné de plus près le protocole 5G AKA. L'outil a permis d'identifier automatiquement les hypothèses de sécurité minimale requises pour atteindre les objectifs de sécurité définis par le standard proposé par le projet de partenariat de troisième génération (3GPP). « L'analyse a montré que le protocole était insuffisant pour atteindre tous les objectifs de sécurité critiques avec les hypothèses énoncées dans le standard », précise Jannik. En particulier, une implémentation trop rapide, mais respectant la norme, pourrait aboutir à une situation où un utilisateur est facturé pour les appels d'un autre utilisateur.

Correction d'erreur possible avant le lancement de la 5G

Le nouveau protocole améliorera considérablement la protection des données par rapport aux technologies 3G et 4G. Notamment, le 3GPP a réussi à combler un écart avec la nouvelle norme qui était auparavant exploitée par les intercepteurs IMSI (International Mobile Subscriber Identity). Avec ces appareils, l'identité internationale d'abonné mobile d'une carte de téléphone portable pouvait être lue pour déterminer l'emplacement d'un appareil mobile et suivre un utilisateur. Pour ce faire, l'appareil avait seulement besoin d'écouter les transmissions entre le téléphone mobile et l'antenne du réseau mobile. Cet écart est désormais comblé avec le 5G AKA. Cependant, les chercheurs ont déterminé que le protocole permettait d'autres types d'attaques de traçabilité. Lors d'attaques, le téléphone mobile n'envoie pas l'identité complète de l'utilisateur, mais un attaquant peut identifier un téléphone, et le tracer. Vu les faiblesses identifiées, si la nouvelle technologie de communication mobile est introduite avec ces spécifications, cela peut entraîner de nombreuses cyberattaques et des conséquences sur la protection de la vie privée. L'équipe de chercheurs est donc en contact avec le 3GPP, l'organisme de standardisation réunissant les industriels de la téléphonie afin de mettre en œuvre conjointement des améliorations du protocole 5G AKA.

Leur publication scientifique a été présentée lors de la prestigieuse conférence CCS 2018 (Computer and Communications Security) à Toronto en octobre dernier, une des plus grandes conférences internationales en matière de sécurité informatique.

CONTACTS PRESSE

Fanny LIENHARDT
Chargée de relations presse - Université de Lorraine
06 75 04 85 65

Olivia BRENNER
Responsable de communication - Loria
06 20 46 44 22

Le Loria, Laboratoire lorrain de Recherche en Informatique et ses Applications est une Unité Mixte de Recherche (UMR 7503), commune à plusieurs établissements : le CNRS, l'Université de Lorraine et Inria. Notre recherche est menée au sein de 28 équipes structurées en 5 départements, dont 15 sont communes avec Inria, représentant un total de plus de 400 personnes. Le Loria est un des plus grands laboratoires de la région lorraine. En savoir plus : **www.loria.fr**