Bureau presse et promotion
Faubourg de l'Hôpital 41
2000 Neuchâtel
Tél. +41 32 718 10 40
bureau.presse@unine.ch
www.unine.ch/communication

COMMUNIQUÉ DE PRESSE

Rendre les courriels de la Poste encore plus sûrs

Neuchâtel, le 27 juin 2023. **Améliorer la sécurité d'un service d'e-mails, c'est le défi qu'a relevé un étudiant en informatique de l'Université de Neuchâtel, le temps d'un master réalisé auprès de la Poste suisse. Pascal Gerig présentera son travail dans le cadre du 17e congrès international ACM DEBS 2023 qui se tient du 27 au 30 juin à Neuchâtel. Cette rencontre annuelle entre académie et industrie fait le point sur les avancées technologiques des systèmes informatiques en réseau, incluant la sécurisation des transmissions de données, l'internet des objets, la blockchain et le Big Data.**

Depuis 2019, le site informatique de la Poste à Neuchâtel est devenu le centre de compétences national en matière de vote électronique et de cryptographie. A l'Université de Neuchâtel, l'Institut d'informatique (IIUN) s'intéresse depuis longtemps à la sécurité des transmissions d'informations en réseau. La proximité géographique aidant, l'IIUN s'est approché de la Poste pour proposer cette collaboration entre les deux institutions, le temps d'un projet de recherche.

Le travail de master de Pascal Gerig a porté sur IncaMail, un service de courriel sécurisé proposé par la Poste. Cette thématique, visant à renforcer la sécurité informatique de ce service pour autant déjà garantie, entrait parfaitement dans le cadre académique de l'UniNE.

Sous la co-supervision de Pascal Felber, Valerio Schiavoni et Jämes Ménétrey, respectivement professeur, maître-assistant et doctorant à l'IIUN, ainsi que celle de Florian Stoller, développeur responsable d'IncaMail à la Poste, le jeune chercheur a mis au point un prototype qui accroît significativement les performances de cryptage d'IncaMail. Ce travail a notamment débouché sur une augmentation de la vitesse du chiffrement et du déchiffrement des messages, sans affecter outre mesure la taille des fichiers attachés.

« La nouvelle architecture réduit l'utilisation des ressources de la Poste, minimise le trafic client-serveur et renforce le dispositif de sécurité tout en diminuant la base de calcul de confiance (*trusted computing base*) », écrivent Pascal Gerig et ses collègues dans l'article scientifique relatif au projet. De plus, les opérations cryptographiques côté client étant allégées, l'efficacité et la sécurité des échanges via IncaMail s'en trouvent bien améliorées. Reste maintenant à transformer cette preuve de faisabilité en une solution applicable à l'ensemble du système.

Référence scientifique :
Pascal Gerig, Jämes Ménétrey, Baptiste Lanoix, Florian Stoller, Pascal Felber, Marcelo Pasin, and Valerio Schiavoni. 2023. Preventing EFail Attacks with Client-Side WebAssembly: The Case of Swiss Post's IncaMail: (Industry and Application Track). In The 17th ACM International Conference on Distributed and Event-based Systems (DEBS '23), June 27–30, 2023, Neuchatel, Switzerland. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3583678.3596899
Ou en cas de non-activation : https://arxiv.org/abs/2306.13388

Bureau presse et promotion
Faubourg de l'Hôpital 41
2000 Neuchâtel
Tél. +41 32 718 10 40
bureau.presse@unine.ch
www.unine.ch/communication

En savoir plus :
Le congrès ACM DEBS 2023 et son programme à Neuchâtel
https://2023.debs.org

Contacts :
Dr Valerio Schiavoni, Institut d'informatique
Tél. +41 32 718 27 32 ; valerio.schiavoni@unine.ch

Prof. Pascal Felber, Institut d'informatique
Tél. +41 32 718 27 09 ; pascal.felber@unine.ch