Proposition de stage de Master (2021)

Sujet

Analyse de systèmes d'authentification biométrique

Contexte

La biométrie désigne la reconnaissance automatisée des personnes sur la base de leurs caractéristiques physiques, biologiques ou comportementales. Les caractéristiques biométriques ne pouvant être perdues ou oubliées, les solutions d'authentification biométrique sont généralement préférées à leurs homologues à base de mots de passe. Bien que les solutions biométriques soient plus pratiques et plus rapides à utiliser, elles ne sont pas exemptes de vulnérabilités. Si elles ne sont pas bien protégées, elles sont vulnérables aux attaques par usurpation d'identité et aux fuites de données personnelles. Les données biométriques servent d'identifiant personnel unique et à long terme, et sont donc classées comme des données personnelles hautement sensibles, relevant du règlement général sur la protection des données (RGPD).

Avec un système biométrique, les utilisateurs sont authentifiés sur la base d'un score de similarité, calculé à partir des données biométriques qu'ils ont enregistrées et des nouvelles données biométriques qu'ils fournissent. L'objectif du stage est de produire des attaques contre des systèmes d'authentification biométrique et leurs briques sous-jacentes. Une attaque peut consister à augmenter le taux d'erreur de reconnaissance d'un système. Il peut aussi s'agir d'apprendre des informations sur la vie privée, comme retrouver les données biométriques d'un individu à partir des données enrôlées pourtant protégées, ou encore relier des données biométriques enrolées auprès de plusieurs fournisseurs de service.

Face aux vulnérabilités mentionnées et aux exigences réglementaires, la communauté a proposé des schémas de protection biométrique, ainsi que des protocoles de reconnaissance biométrique préservant la vie privée. Avec la popularité des appareils mobiles intelligents, certains standards de sécurité tels que FIDO [1] et BOPS [3] ont également émergé. La grande majorité de ces mécanismes et protocoles, y compris les standards, ne sont pas systématiquement accompagnés d'analyses de sécurité formelles. Ce stage s'inscrit dans une partie d'un projet de recherche (PRIVABIO), dont le but est de mieux comprendre la sécurité des systèmes biométriques, de définir des modèles de sécurité appropriés et de proposer des primitives et des protocoles adaptés. Plusieurs aspects seront traités durant ce stage :

- Il s'agira d'étudier des schémas de protection biométrique et d'exhiber des attaques dans les modèles de sécurité proposés par les auteurs. En particulier, l'étudiant pourra parcourir [5, 4] pour plus de détails sur les schémas crypto-biometriques, ou encore [8, 6] pour des détails sur les schémas biométriques assurant une propriété de révocabilité des données. Les attaques proposées pourront élever le taux de fausses acceptations, mettre à mal la révocabilité des données protégées, ou encore porter atteinte à la vie privée des utilisateurs.
- Face à la quasi absence d'analyses des standards impliquant la biométrie, à quelques exceptions [7], une partie du travail sera consacrée à un examen des standards FIDO UAF [2] et BOPS [3], ainsi que des protocoles faisant intervenir des mécanismes de calcul sécurisé (calcul multi-parties, chiffrement fonctionnel).

Travail à effectuer

Le stagiaire épaulera l'équipe pour faire évoluer l'état de l'art sur la sécurité des données biométriques. Un des aspects du stage sera d'étudier des primitives de transformation biométrique afin de produire de nouvelles attaques, en les associant à des problèmes théoriques connus. Ensuite, un examen critique des protocoles de reconnaissance biométrique devra être effectué, incluant les standards FIDO et BOPS. Enfin, une partie du travail consistera à implémenter et documenter ces attaques.

Profil recherché

- Master 2 ou école d'ingénieurs dans le domaine de la cybersécurité
- Connaissances en cryptotologie, algorithmique, complexité
- Connaissances en machine learning bienvenues
- Bonne maîtrise d'un langage de script, *Python*, *R* ou *Matlab*.

Superviseurs

Kevin Atighehchi (kevin.atighehchi@uca.fr), Paul-Marie Grollemund (paul_marie.grollemund@uca.fr) et Pascal Lafourcade (pascal.lafourcade@uca.fr)

Organisme d'accueil

Ce stage se fera à l'Université Clermont Auvergne, sur le campus des Cézeaux ou sur le site délocalisé d'Aurillac.

Indemnisation

Gratification de stage.

Candidature

Pour candidater, merci d'envoyer aux 3 contacts ci-dessus votre candidature composée d'un CV et d'un bulletin de notes.

Références

[1] FIDO Alliance. https://fidoalliance.org/overview/. Accessed May 3, 2020.

[2] FIDO UAF Specifications. https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-uaf-protocol-v1.2-rd-20171128.html. Accessed May 3, 2020.

[3] IEEE Standard for Biometric Open Protocol. *IEEE Std 2410-2019 (Revision of IEEE Std 2410-2017)*, pages 1–134, 2019.

[4] Xavier Boyen. Reusable cryptographic fuzzy extractors. In *ACM Conference on Computer and Communications Security*, pages 82–91. ACM, 2004.

[5] Ran Canetti, Benjamin Fuller, Omer Paneth, Leonid Reyzin, and Adam D. Smith. Reusable Fuzzy Extractors for Low-Entropy Distributions. In *Advances in Cryptology - EUROCRYPT 2016*, pages 117–146, 2016.

[6] Jun Beom Kho, Jaihie Kim, Ig-Jae Kim, and Andrew Beng Jin Teoh. Cancelable fingerprint template design with randomized non-negative least squares. *Pattern Recognition*, 91 :245–260, 2019.

[7] Olivier Pereira, Florentin Rochet, and Cyrille Wiedling. Formal Analysis of the FIDO 1.x Protocol. In Abdessamad Imine, José M. Fernandez, Jean-Yves Marion, Luigi Logrippo, and Joaquin Garcia-Alfaro, editors, *Foundations and Practice of Security*, pages 68–82, Cham, 2018. Springer International Publishing.

[8] Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle. Enhancing security and privacy in biometrics-based authentication system. *IBM Systems J.*, 37(11) :2245–2255, 2001.