Proposition de stage de Master (2022)

Sujet

Attaques sur des systèmes biométriques

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. Les schémas de biométrie révocable que l'on attaque sont composés de deux étapes. La première est l'extraction de caractéristiques d'une image biométrique. Cette étape comprend le passage de l'image à travers un filtre basé sur un noyau. Une fois un vecteur de caractéristiques obtenu, une projection secrète est utilisée pour produire un gabarit biométrique. Rechercher des préimages à un gabarit biométriques permet à un attaquant d'usurper l'identité d'un utilisateur légitime. Ces attaques consistent à formuler des programmes quadratiques à contraintes quadratiques et à les résoudre. Cependant, la résolution de ces programmes peut être longue.

L'objectif du stage est d'améliorer les attaques proposées par l'équipe. Pour cela, le stagiaire sera amené à chercher des relaxations des systèmes quadratiques non convexes. En outre, il optimisera nos stratégies ou en développera d'autres visant à résoudre ces systèmes, par exemple en utilisant des algorithmes génétiques. Il élargira également la portée de ces attaques à de multiples noyaux.

Travail à effectuer

Au cours de son stage, le stagiaire sera amené à effectuer les tâches suivantes :

- Implémenter et améliorer les attaques sur les schémas de biométrie révocable.
- Choisir les algorithmes de résolutions de système linéaire adapté aux problèmes traités.
- Comparer les performances de ces attaques avec système linéaire et algorithme génétique.
- Proposer une approche hybride système linéaire et algorithme génétique.
- Faire un comparatif des temps d'exécutions de chaque attaque suivant le noyau.

Profil recherché

- Master 2 ou école d'ingénieurs.
- Bonne maîtrise d'un langage de script.
- Connaissance en recherche opérationnelle.
- Maitrise de LaTeX.
- Connaissances en machine learning et imagerie bienvenues.

Superviseurs

Kévin ATIGHEHCHI, Paul-Marie GROLLEMUND et Axel DURBET

Organisme d'accueil

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

Indemnisation

Gratification non imposable au taux légal de $3,90€$/h.

Candidature

Pour candidater, merci d'envoyer aux 3 contacts ci-dessus (kevin.atighehchi@uca.fr, paul_marie.grollemund@uca.fr et axel.durbet@uca.fr) votre candidature composée d'un CV, d'une lettre de motivation ainsi qu'un bulletin de notes.

Références

[1] Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[2] Kevin Atighehchi, Loubna Ghammam, Morgan Barbier, and Christophe Rosenberger. Greyc-hashing : Combining biometrics and secret for enhancing the security of protected templates. *Future Generation Computer Systems*, 101 :819 – 830, 2019.

[3] Xingbo Dong, Zhe Jin, and Andrew Teoh Beng Jin. A genetic algorithm enabled similarity-based attack on cancellable biometrics. In *2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–8, 2019.

[4] Axel Durbet, Pascal Lafourcade, Denis Migdal, Kevin Thiry-Atighehchi, and Paul-Marie Grollemund. Authentication attacks on projection-based cancelable biometric schemes, 2021.

[5] Loubna Ghammam, Koray Karabina, Patrick Lacharme, and Kevin Thiry-Atighehchi. A cryptanalysis of two cancelable biometric schemes based on index-of-max hashing. *IEEE Transactions on Information Forensics and Security*, PP :1–12, 03 2020.

[6] Wei-Yu Han and Jen-Chun Lee. Palm vein recognition using adaptive gabor filter. *Expert Systems with Applications*, 39(18) :13225–13234, 2012.

[7] Jens Hermans, Bart Mennink, and Roel Peeters. When a Bloom Filter is a Doom Filter : Security Assessment of a Novel Iris Biometric Template Protection System. In *BIOSIG 2014 - Proceedings of the 13th International Conference of the Biometrics Special Interest Group, 10.-12. September 2014, Darmstadt, Germany*, pages 63–74, 2014.

[8] Andrew Teoh Beng Jin, Tee Connie, and David Ngo Chek Ling. Remarks on BioHash and its mathematical foundation. *Inf. Process. Lett.*, 100(4) :145–150, 2006.

[9] Andrew Teoh Beng Jin, David Ngo Chek Ling, and Alwyn Goh. Biohashing : two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, 37(11) :2245–2255, 2004.

[10] Patrick Lacharme, Estelle Cherrier, and Christophe Rosenberger. Preimage Attack on BioHashing. In *SECRYPT 2013 - Proceedings of the 10th International Conference on Security and Cryptography, Reykjavík, Iceland, 29-31 July, 2013*, pages 363–370, 2013.

[11] Alessandra Lumini and Loris Nanni. An improved BioHashing for human authentication. *Pattern Recognition*, 40(3) :1057 – 1065, 2007.

[12] R. Mehrotra, K.R. Namuduri, and N. Ranganathan. Gabor filter-based edge detection. *Pattern Recognition*, 25(12) :1479–1494, 1992.

[13] Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. Zerocoin : Anonymous Distributed E-Cash from Bitcoin. In *IEEE Symposium on Security and Privacy*, pages 397–411. IEEE Computer Society, 2013.

[14] Christian Rathgeb, Harald Baier, Christoph Busch, and Frank Breitinger. Towards Bloom filter-based indexing of iris biometric data. In *International Conference on Biometrics, ICB 2015, Phuket, Thailand, 19-22 May, 2015*, pages 422–429, 2015.

[15] Andras Rozsa, Albert E. Glock, and Terrance E. Boult. Genetic algorithm attack on minutiae-based fingerprint authentication and protected template fingerprint systems. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, June 2015.

[16] Andrew Beng Jin Teoh, Wai Kuan Yip, and Sangyoun Lee. Cancellable biometrics and annotations on BioHash. *Pattern Recognition*, 41(6) :2034–2044, 2008.

[17] Olufunke Vincent and Olusegun Folorunso. A descriptive algorithm for sobel image edge detection. January 2009.