Synthèse de l'article:
"Preimage Attack on BioHashing"

Sécurité des systèmes embarqués

AKKAL Aghilas
Numéro d'étudiant : 19009504

L'article s'intitule : ***Preimage Attack on BioHashing*** (ou: Attaque pré-image sur BioHashing) fut rédigé par : ***Patrick Lacharme***, ***Estelle Cherrier*** et ***Christophe Rosenberger*** à l'occasion de la conférence internationale sur la sécurité et la cryptographie (International Conference on Security and Cryptography ***'SECRYPT'***, ***2013***, ***Iceland***) et fut publié le ***26 Juin 2014*** sur L'archive ouverte pluridisciplinaire ***HAL*** (https://hal.archives-ouvertes.fr/hal-01015274).

Avant la parution de l'article, les trois chercheurs discutent les différentes solutions disponible pour la protection des méthodes d'authentification biométriques et cela grâce à la ***cryptographie biométrique*** ou la ***biométrie annulable***. Ces modèles de protection biométrique dépendent fortement des modalités biométriques et du niveau de sécurité requis.

Nos auteurs expliquent que les cryptosystèmes biométriques associent une clé secrète à une protection biométrique pour la protéger, cette dernière comprend un ***engagement flou*** et les ***coffres floues***, les engagements flous sont basés sur la correction d'erreur de codes et ne nécessitent pas le stockage du modèle biométrique. et ils citent de nombreuses applications sur données sur l'iris (***Hao et al., 2005***) ou systèmes multimodaux (***Cimato et al., 2008***).

Le ***concept de biométrie annulable*** quand à lui repose sur une transformation des données biométriques brutes, le principe consiste à ***générer un nouveau modèle biométrique***, à partir du vecteur d'entités biométriques ainsi qu'un nombre aléatoire 'seed', un peu comme un schéma d'authentification à deux facteurs qu'on utilise souvent pour sécuriser l'accès à nos réseaux sociaux par exemple, ce ***qui permet de ne pas garder de trace*** de l'entrée d'origine (visage ou doigt).

La reconstruction de modèles biométriques suffisamment similaires, appelés ***attaque de pré-image***, est le ***défaut majeur*** pour les schémas biométriques annulables, car dans ce cas, le système d'authentification pourrait être facilement usurpé.

La ***principale contribution*** de cet article est de tester, comprendre et analyser cette vulnérabilité de la biométrie annulable. les chercheurs proposent ***une nouvelle méthode*** pour générer un vecteur de caractéristique biométrique qui se rapproche le plus de la caractéristique biométrique d'origine (visage ou doigts généralement), basée sur des ***algorithmes génétiques*** (qui, pour rappel sont des techniques qui existent déjà dans le domaine de l'intelligence artificielle). cela va dans le sens de trouver des failles solides et reproduisible afin de pousser la technologie a y remédier à ces dernières.
Il est à noter qu'un algorithme génétique simule des modèles de calcul déterminant la valeur optimale d'un critère en simulant la évolution d'une population et survie des individus les mieux équipés et passent ainsi les paramètres d'une génération à la suivante.

Les auteurs remarquent que l'algorithme ***Biohashing*** est ***facile à inverser*** si le nombre aléatoire utilisé comme 'seed' est connu (et ils ont évité de suivre cette technique, vu que c'est déjà confirmé et assez facile à reproduire). Mais, la ***caractéristique biométrique reconstruite*** (appelé la ***pré-image***) n'est pas nécessairement proche du modèle d'origine. Dans cet article, ils se sont surtout ***demandé*** si c'est suffisant pour un intrus de récupérer, ***à partir*** de la connaissance d'un ***BioCode intercepté*** et du nombre aléatoire ***'seed'*** extrait des données d'empreintes brutes originales de l'utilisateur (et pas les données originales elles-mêmes) de tromper le système.

Ils ont appliqué le processus selon deux méthodes: ***LBPFT**** et ***Gabor**** et l'évolution de la fonction fitness montre que le BioCode généré, étant donné le ***FingerCode*** approximatif, est ***très similaire*** à celui intercepté. La différence moyenne résultante démontre aussi l'efficacité de l'approche proposée pour le Fonction LBPFT contre le Gabor car sa distance entre le FingerCode réel et approximatif est assez élevé entre le vrai FingerCode et celui approximatif.

En plus, afin de ***vérifier*** si le FingerCode approximatif est vraiment utile pour un intrus, les trois chercheurs ont ***entrepris une autre expérience***, la conclusion de cette expérience est que l'attaque proposée ***correspond bel et bien aux résultats attendus*** et révèle une ***grande faille*** de sécurité si le BioCode et les seeds aléatoires sont stockés dans la même base de données. C'est aussi un problème de confidentialité car un intrus serait capable de générer d'autres BioCodes pour usurper l'identité du véritable utilisateur.

Cet article propose ***une nouvelle façon*** d'approcher les vecteurs caractéristiques biométriques originales du modèle transformé dans un schéma ***biométrique annulable***. Elle ***utilise des algorithmes génétiques*** et révèle des problèmes de sécurité et de confidentialité concernant la biométrie annulable. Cette attaque permet à un intrus de récupérer un modèle biométrique, similaire à l'original modèle.
Les expérimentations avec l'algorithme de BioHashing montrent donc clairement l'importance de stocker les données aléatoires 'seeds' en dehors du Biocode (une autre base de donnée séparée). Points de vue de ce document

D'ici plusieurs perspectives s'ouvrent et sont à étudier, tel que la robustesse de différents transformations de caractéristiques à utiliser dans le contexte d'un système biométrique annulable, afin d'améliorer les performance, et pas que la sécurité de ce dernier.
Encore plus de question se posent, sur la sécurité des méthodes d'authentifications biométrique actuelles, notamment qu'elles sont de plus en plus utilisé dans notre quotidien, nos données risquent elles d'être facilement piratées ? y'a t'il vraiment aucune moyen d'y remédier à toutes ses failles ? et quelle serait le moyen biométrique le plus sécurisé que la société pourrait utiliser ?

Cet article à éclaircit un point qui m'était jusqu'à maintenant pas aussi claire, notamment sur les failles qu'on ne considère pas vraiment lorsqu'on choisit de s'identifier avec nos visages ou doigts et les mesures prises en compte pour les sécuriser.

* *(Modèle binaire local invariant de rotation (LBPFT) avec 152 paramètres. Il s'agit d'une méthode de classification de la texture invariante en rotation, présentée dans la référence (Guo et al., 2010))*

** *(Fonction de Gabor (Manjunath et Ma, 1996) avec 256 paramètres. basés sur une fonction du noyau gaussien modulée par une onde plane sinusoïdale, avec plusieurs orientations et échelles différentes, et sont utilisées pour la représentation de la texture)*