Etat de l’art sur les méthodes de détection du texte et de la dynamique de frappe au clavier via le son

Mikael LEGRAIN, Titouan PETIT

UNIVERSITÉ
CAEN
NORMANDIE

Résumé :

La sécurité informatique base aujourd’hui ses méthodes sur des aspects souvent mathématiques de par le chiffrement, parfois sur des techniques liées aux réseaux et aux protocoles, mais également sur la biométrie pour identifier un individu. Ces dernières années, le développement du matériel connecté a motivé à la normalisation de ces méthodes, mais les attaques cherchant à les contourner également. L’idée de cet état de l’art est donc de s’intéresser à des méthodes de biométrie douce en ayant comme objectif d’utiliser un canal assez peu répandu, celui du son.

Afin de pouvoir identifier un individu uniquement avec le son que produit son clavier lors de la frappe, nous avons plusieurs points sur lesquels il faut s'interroger. Le principal étant de trouver une manière efficace de capter avec précision ce qui est frappé sur le clavier uniquement avec le son. C’est d’ailleurs la motivation principale de cet état de l’art. Les aspects qui en découlent sont alors d’analyser la dynamique des frappes afin de pouvoir différencier les habitudes de frappes voire même d’identifier l'individu derrière le clavier. L’idée finale de cette recherche serait alors d’essayer de mettre au point un protocole biométrique consistant à identifier un individu enrôlé non pas par un secret qu’il doit indiquer mais par la manière dont il recopie une phrase quelconque.

Synthèse :

Globalement, plusieurs approches de ce problème existent. La première consiste à rechercher toute solution ou outil déjà existant permettant soit d’identifier ce qui est frappé au clavier uniquement via le son, soit de se baser sur la dynamique de frappe et d’en identifier l’individu qui en est à l’origine. La seconde regarde plus globalement les projets existants et de comprendre leur fonctionnement et efficacité pour essayer de s’inspirer de potentielles pistes de travail.
Bien entendu, les deux parties sont complémentaires. Pour parvenir à des résultats proches de ceux déjà existants sur des projets finis, il est possible d’utiliser le travail déjà réalisé par certaines personnes si ces derniers le fournissent en libre accès.

Intéressons-nous d’abord aux différents projets existants et aux différentes approches que ces derniers ont pris. Le point de départ est commun à tous ces projets, il faut, en se basant sur un signal sonore, pouvoir savoir ce qui est frappé au clavier et d’avantage identifier la manière dont cela est fait. Deux types d’identification sont alors distinguables.

Identification de l'individu

La première approche est celle de l’article “*I Know Your Keyboard Input: A Robust Keystroke Eavesdropper Based-on Acoustic Signals*” (1) qui utilise plusieurs sources de captation du son pour pouvoir trianguler la position de chacune des frappes en se basant sur le délai de perception d’un son entre les différents canaux. Dans l’idée, dès lors que deux micros capturent un même son, la différence de position entre les deux capteurs permet de localiser relativement précisément l’endroit auquel le son est émis. Cette précision est soutenue par la présence des “points de repère” que sont les “grosses touches”.

En effet, les touches Espace, Entrée et Contrôle émettent un son particulier et simplement différentiable des autres, ils sont alors utilisés pour synchroniser la position des micros par rapport à celle du clavier. L'avantage de cette approche est également son plus grand défaut, il faut utiliser plusieurs capteurs. Même si l'attaque décrite est intéressante, elle ne correspond pas à l'utilisation que nous recherchons. L'idée serait de préférer une captation en mono pour pouvoir l'utiliser de manière plus générale sur une majorité de machines en utilisant leur micro interne.

Une deuxième approche provient de l'article *"Biometric Authentication via Keystroke Sound". (3)* Ceci est une méthode d'authentification. La méthode utilise l'analyse de deux comportements. Le premier comportement analysé est visuel avec un caméra placée au-dessus du clavier. Grâce à un appel d'algorithme sur la vidéo enregistrée, on sait quel sujet tape au clavier. Le deuxième comportement analysé est audio. Grâce à la biométrie, on authentifie le sujet comme étant un utilisateur légitime. La partie qui serait la plus intéressante dans notre cas serait la partie analyse audio qui pourrait nous aider à identifier un sujet.

Nom du papier	Précision de l'identification d'un individu	Training Data	Facilité de mise en place	Observations	Implémentation disponible
I Know Your Keyboard Input (1)	91.52%	Non	Moyen	Marche avec la synchronisation des outils	Non
Keystroke Sound (3)	EER 25%	Oui	Facile	training, enrollment, and authentication.	Non

Tableau récapitulant les différences et spécificités entre différentes études

Identification d'un mot

La deuxième identification ne se base donc plus sur l'identification des touches par leur position mais sur la signature sonore de chaque touche. Une majorité des solutions suivantes utilisent soit l'apprentissage automatique pour identifier les subtiles différences phoniques émises par chaque touche soit une estimation de la probabilité d'occurrence de chaque lettre étant donné les fréquences d'apparition des lettres d'une langue. Cette partie a pour avantage de s'intéresser à de plus petits outils ayant un contexte d'utilisation réduit et certains d'entre eux sont accessibles pour pouvoir réaliser une prise en main.
Les outils principaux sont alors *Keytap (9)* qui entraîne une intelligence artificielle à différencier les subtilités avec une phase d'apprentissage. *Keytap2 (10)* veut contourner ce problème en se basant sur les spécificités de la langue, en l'occurrence la langue anglaise. *Keyboard Acoustic Emanation (7)* base son analyse sur de la clusterisation et une approche plus mathématique de la question. Du traitement de signal à l'analyse finale, l'idée est de baser l'analyse sur différentes propriétés mathématiques ou statistiques des sons émis et des mots ainsi frappés.

Nom du papier	Précision de l'identification d'un mot	Training Data	Facilité de mise en place	Observations	Implémentation disponible
Keytap (9)	~	Oui	Facile	Meilleur sur les claviers mécaniques	Oui
Keytap2 (10)	~	Non	Moyen	En cours de développement, Sensible à la langue anglaise	Oui
Keyboard acoustic emanations (7)	~ 83% sur les mots ~ 94% sur les lettres	Non	Moyen	Sensible à la langue anglaise	Non

Tableau récapitulant les différences et spécificités de différents projets

Critique :

Même si les différents projets cités ci-dessus ont tous des natures, objectifs et résultats pouvant varier, nous pouvons grandement nous inspirer des approches de certains d'entre eux. Dans l'idée, un choix doit être fait pour la manière la plus en accord avec notre vision sur la manière dont il faut récupérer et identifier le son. En effet, selon le type de détection que nous choisirons pour la suite de notre projet, la nature de la capture changera en conséquence. Une majorité des recherches citées ici ont comme point de vue une attaque la plus discrète possible. Bien souvent, la capture se fait à l'encontre de la connaissance de l'utilisateur et l'objectif est donc de subtiliser un texte secret comme un mot de passe ou un message tapé. Cette vision diffère de la nôtre car nous voulons que l'utilisateur soit averti de son enregistrement pour un biais biométrique. Nous pouvons tout de même noter l'efficacité de certaines approches.

Conclusion :

Pour conclure, nous pouvons alors dire que de nombreuses solutions semblent exister pour répondre à notre problème et que certaines semblent plus appropriées. En ce qui concerne la meilleure de ces stratégies, nous ne pouvons nous arrêter sur aucune en particulier à l'heure actuelle étant donné le manque d'expérimentation. Seuls les chiffres décrits dans leurs présentations étaient ici cités. Globalement, nous pouvons exclure certaines visions trop proches d'une attaque discrète car nous avons comme objectif d'avertir l'utilisateur lors de l'utilisation de notre produit final. Ainsi, la direction de notre projet s'oriente vers l'utilisation de *Keytap (9) et Keytap2 (10).* Pour cela, il est nécessaire d'effectuer une phase d'expérimentation et de prise en main sur ces outils avant toute décision finale.

Références

Articles :

1. *I Know Your Keyboard Input: A Robust Keystroke Eavesdropper Based-on Acoustic Signals* MM '21: ACM Multimedia Conference from https://dl.acm.org/doi/abs/10.1145/3474085.3475539?casa_token=a_i8odJIilIAAAAA%3A-NsPtnrJN1yqwzBi1YtLKoMjLL-bobY2ofXTxj7TcCkUrll5BXu8oz-4_3ePIb9QlDcN_E0m8BLp-jU
2. *Comparing Anomaly-Detection Algorithms for Keystroke Dynamics*. (n.d.). CMU School of Computer Science. Retrieved December 1, 2021, from https://www.cs.cmu.edu/~maxion/pubs/KillourhyMaxion09.pdf
3. Dickens, C. (n.d.). *Biometric Authentication via Keystroke Sound*. MSU CSE. Retrieved December 1, 2021, from https://www.cse.msu.edu/~rossarun/pubs/RothKeystrokeSound_ICB2013.pdf
4. *Fusion et biométrie douce pour la dynamique de frappe au clavier*. (n.d.). Archive ouverte HAL. Retrieved December 1, 2021, from https://hal.archives-ouvertes.fr/hal-01406711/
5. *A Survey of Keystroke Dynamics Biometrics*. (2013, August 4). Hindawi. Retrieved December 1, 2021, from https://www.hindawi.com/journals/tswj/2013/408280/
6. *User Verification based on Keystroke Dynamics: Python code*. (2017, July 26). Machine Learning in Action. Retrieved December 1, 2021, from https://appliedmachinelearning.blog/2017/07/26/user-verification-based-on-keystroke-dynamics-python-code/
7. Keyboard Acoustic Emanations Revisited University of California, Berkeley https://www.cse.msu.edu/~rossarun/pubs/RothKeystrokeSound_ICB2013.pdf

Codes Github :

8. *goncalopp/keystroke_dynamics: a keystroke dynamics algorithm in python (recognizes a person by the way s/he types)*. (n.d.). GitHub. Retrieved December 1, 2021, from https://github.com/goncalopp/keystroke_dynamics
9. *Keytap* (2020, December 13). GitHub. Retrieved December 1, 2021, from https://github.com/ggerganov/kbd-audio/
10. *Keytap2 - acoustic keyboard eavesdropping based on language n-gram frequencies · Discussion #31 · ggerganov/kbd-audio*. (2020, December 13). GitHub. Retrieved December 1, 2021, from https://github.com/ggerganov/kbd-audio/discussions/31