Attaque acoustique sur clavier

INFO 910 - Cryptologie

Steeve CIMINERA
Romain SANCHEZ

2019 - 2020

Introduction

Depuis un certain nombre d'années, on peut entendre parler d'attaques sur des ordinateurs liées au émanations qu'ils peuvent produire. En effet, les émanations électromagnétiques et optiques d'une machine ont déjà étées utilisées dans un certain nombre d'attaques.
Par exemple, Markus G. Kuhn, de l'université de Cambridge à été capable de reconstruire l'affichage d'un écran à tubes cathodiques à partir de ses émanations de lumière dans son article "Optical Time-Domain Eavesdropping Risks of CRT Displays", et un groupe de chercheur à été en mesure de reconnaître les opérations d'un processeur à partir du bruit que ce dernier pouvait émettre lors de calculs.
Comme on peut le constater, un certain nombre d'éléments composant un ordinateur peuvent produire des émanations de différents types, qui peuvent potentiellement donner de l'information à un attaquant.

La question qui se pose est la suivante : Peut-on analyser les bruits produits par un clavier pour déterminer ce que l'utilisateur saisit ?

Trois contacteur mécaniques de type Cherry MX

Si on part du principe que les touches d'un clavier pourraient émettre des sons différents lorsqu'on les frappes, on pourrait alors déterminer quelle séquence de touches à été saisie à partir du son produit par le clavier.

Nous étudierons deux articles liés à l'écoute des émanations acoustiques émises par un clavier, à savoir :

- "Keyboard Acoustic Emanations" de Dmitri Asonov et Rakesh Agrawal du centre de recherche d'IBM Almaden en 2004.
- "Keyboard Acoustic Emanations Revisited" de Li Zhuang, Feng Zhou et J. D. Tygar de l'Université de Berkeley en 2005.

Expérimentations

Afin de se rendre un peu mieux compte de ce qu'il se passe au niveau acoustique dans un clavier, nous avons réalisé plusieurs enregistrements.

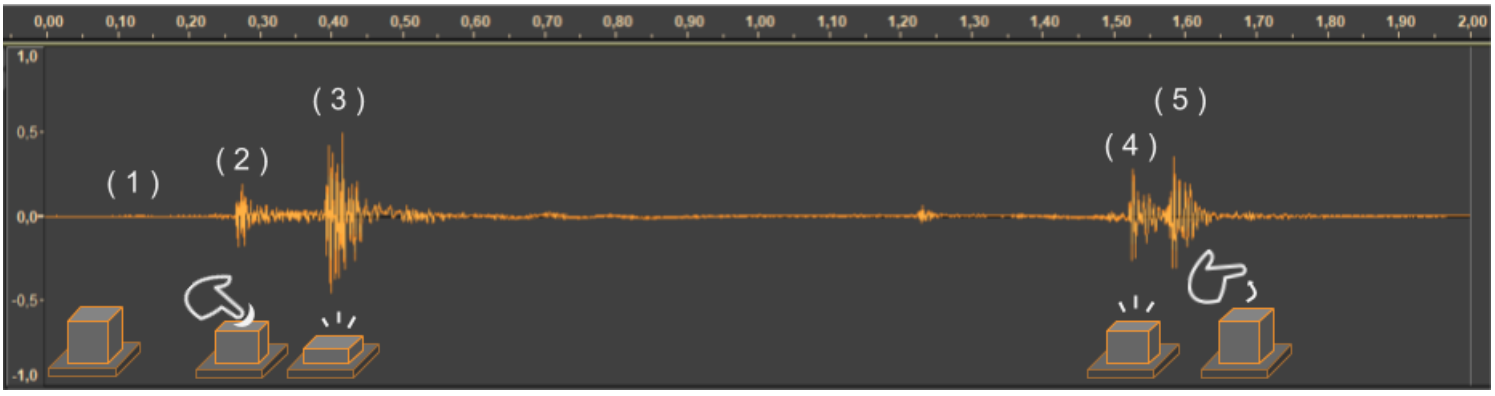
Ils ont étés réalisés à l'aide d'un ZOOM H4N PRO, sous forme de fichiers *waveform* (.wav) 96 kHz - 24 bits. L'idée étant de pouvoir profiter d'enregistrements de très bonne qualité.

Ces enregistrements nous ont permis de déterminer :

- La durée moyenne d'une frappe se situe entre 100 et 200ms.
- La différence de taille entre les touches provoque une différence de son discernable à l'oreille nue (un "A" opposé à la barre d'espace par exemple)
- Des enregistrements de bonne qualités (comme ici) permettent de capturer des détails non cités dans les études (par exemple le bruit dû au jeu entre une touche mécanique et son contacteur : le pic (2) sur l'image ci dessous)

Ces conclusions sont bien évidemment à prendre avec un grain de sel, nous ne sommes pas des professionnels dans les domaines abordés.

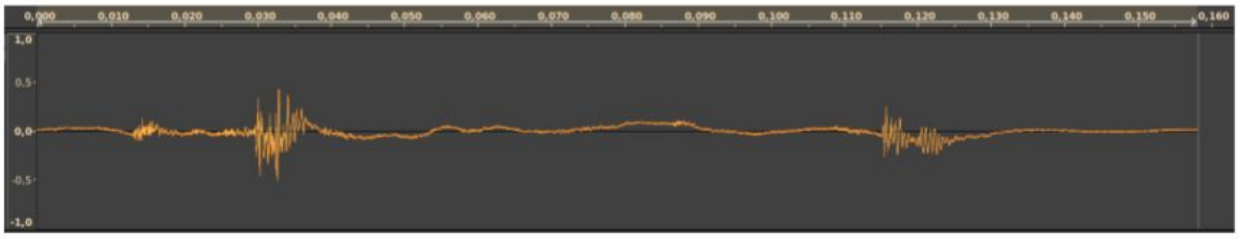
Les illustrations de signal et spectres qui suiverons proviennent de nos enregistrements.



Analyse acoustique d'une frappe

(1) - Touche du clavier intacte
(2) - Bruit de l'impulsion du doigt sur la touche (dû au jeu)
(3) - Bruit de l'activation du contacteur de la touche
(4) - Bruit de relâchement du contacteur de la touche
(5) - Bruit de relâchement du doigt sur la touche

Touche “A”



Barre d’espace

Différences acoustiques (et visuelles) de touches de tailles différentes

Maigre analyse acoustique d’une phrase

Analyse Acoustique

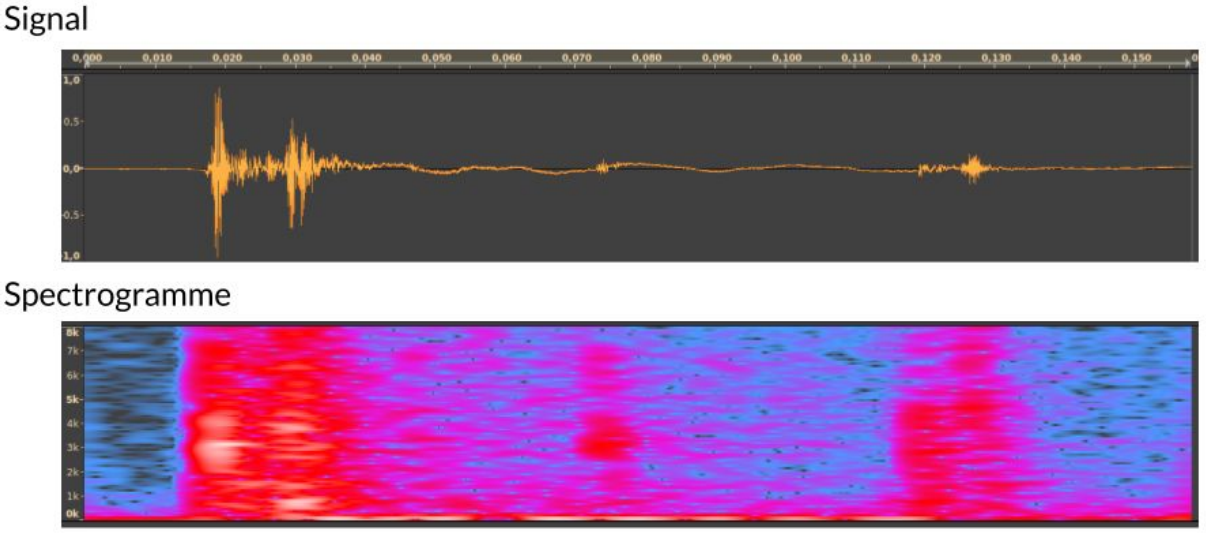
La première méthode d'attaque par l'intermédiaire de sons émis par le clavier est l'analyse acoustique. Celle-ci est décrite dans l'article "Keyboard Acoustic Emanations" de Dmitri Asonov et Rakesh Agrawal du centre de recherche d'IBM Almaden publiée en 2004.
Elle réside en la constitution d'un réseau de neurones à partir de sons émis par un clavier, puis en l'écoute des sons émis par ce dernier dans le but de retrouver quelles touches ont étés saisies par un utilisateur.
Lorsque les conditions nécessaires sont réunies, Asonov et Agrawal sont parvenus à obtenir un taux de reconnaissance du texte saisis de 80%.

Principe de l'attaque

L'attaque repose sur l'hypothèse que les sons émis par les touches d'un clavier sont différents les uns des autres.
L'attaque peut être réalisée par l'intermédiaire d'un simple micro qui enregistre les sons des touches frappées par un utilisateur.
En amont, il est nécessaire d'entraîner un réseau de neurones en enregistrant et en traitant les sons produits par le clavier.

Le réseau de neurones

Comme expliqué précédemment, cette attaque utilise un réseau de neurones permettant de classifier les clics du clavier.
Pour chacune des touches du clavier, on enregistre 10 sons produit par son activation.
Cependant, les fichiers contenant les sons d'une frappe de touches sont de base trop lourds pour que le réseau de neurones soit efficace. C'est pourquoi il est nécessaire de traiter les sons obtenus. Pour cela, on associe à chaque son un spectre, correspondant à sa transformée de Fourier. On obtient donc les traits principaux du signal, constituant une entrée valide au réseau.



20

Cliquer sur une touche produit deux pics sur le graphiques de fréquences du son enregistré. Le premier correspond à l'appui et le second au relâchement de la touche.
La distribution des fréquences est calculée pour les sons de chaque touches, puis on normalise le résultat de manière à obtenir un résultat entre 0 et 1.

Pour chaque touche, on enregistre le son de 10 clics.
En moyenne 0.5 reconnaissance sur 20 est incorrecte.

L'expérience

L'expérience à été répétée à de multiples reprises, mais en changeant les paramètres d'enregistrement. Dans de bonnes conditions, cette méthode permet de retrouver 80% des caractères saisis par un utilisateur.

1) Différentes distances entre le micro et le clavier

Jusqu'à présent, la distance entre le clavier et le micro était de 1m. La procédure à étée répétée en augmentant peu à peu la distance, et les résultats ont montrés que cette dernière est efficace jusqu'à une distance d'environ 15m, sans baisse de qualité de la reconnaissance.

2) Différents claviers

Plusieurs tests ont étés menés en entraînant le réseau de neurones avec un clavier en particulier, puis en écoutant la saisie sur un autre clavier.
Comme attendu, la qualité de la reconnaissance est nettement plus faible que sur une écoute du même clavier que celui utilisé pour la reconnaissance, puisque les touches ne produisent plus le même son. Néanmoins, 50% des touches enregistrées sont toujours identifiées, ce qui est insuffisant pour écouter tout le texte saisis par un utilisateur, mais donne tout de même de précieuses informations à un attaquant.

IBM keyboard S/N 0953260

Clavier utilisé lors de l'entraînement du réseau de neurone (contacteur ressort)

3) Différents types de saisie

Les résultats présentés jusqu'à présent ont étés obtenus à partir de la saisie d'une seule et même personne. Or il est possible que la méthode de saisie soit différente en fonction des personnes (force impliquée dans la frappe d'une touche, vitesse de saisie, etc…). On souhaite donc connaître l'impact du style de saisie sur la reconnaissance.
Dans le cas où seule la force de frappe change (la personne à l'origine de l'entraînement du réseau de neurones reste la même), aucune altération de la qualité de la reconnaissance n'est observée.
En ayant une personne qui entraîne le réseau de neurones différente de celle qui saisie, on observe cette-fois une très faible altération dans la reconnaissance.
En d'autres termes, cette méthode de reconnaissance peut être utilisée peu importe la personne et le type de frappe, tout en restant efficace.

Limites de la méthode

Comme on a pu le voir, cette méthode permet à un attaquant, si les conditions sont réunies, d'obtenir des informations sur un texte, en pouvant aller jusqu'à 80% des caractères saisis.
Les limites de cette méthodes résident pourtant dans les conditions nécessaires à une reconnaissance efficace. En effet l'étude réside dans l'analyse des données acoustiques récupérées par un attaquant.

1) Entraînement du réseau de neurones

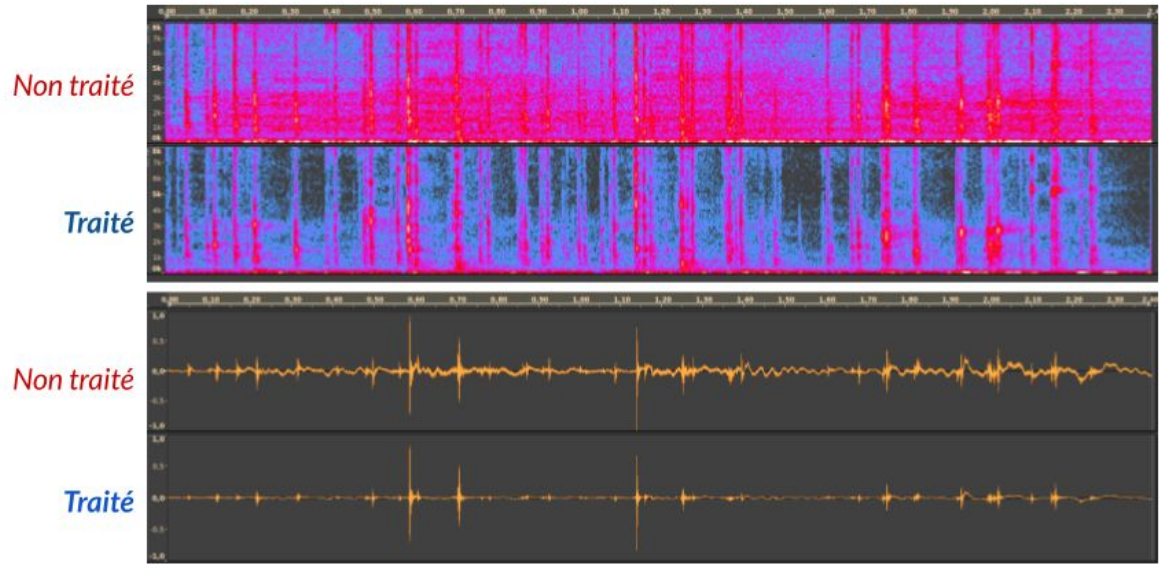
Dans un premier temps, il faut entraîner un réseau de neurones avec le clavier qu'on souhaite écouter. En souhaitant écouter un clavier différent du clavier utiliser pour l'entraînement, cette méthode donne des résultats corrects pour environ 25% des caractères, ce qui est souvent trop peu pour trouver le texte saisis.

2) Écouter une personne différente

De la même manière, si l'entraînement est effectué par une personne et qu'on souhaite écouter une personne différente, on constate une baisse de précision. Cet impact est peu important, mais il reste tout de même présent ce qui peut altérer la qualité d'une analyse.

3) Bruits parasites

De plus, distinguer le son produit par une touche n'est pas toujours évident. L'étude à été réalisée dans un environnement calme, mais en se plaçant dans un cas plus réaliste, comme dans un bureau, des bruits pourraient parasiter l'enregistrement et rendre l'identification du son difficile, voir impossible.



Un signal avant et après traitement des bruits parasites

C’est en pratique très difficile de réunir ses conditions. Une attaque reposant sur cette technique peut alors se trouver plus ou moins efficace.
Néanmoins, elle donne tout de même de l’information à un attaquant, et comme l’indiquent Asonov et Agrawal, il est important de limiter au maximum ce genre de fuites de données, en mettant par exemple au point des claviers silencieux.

Analyse Statistique

La seconde méthode est plus efficace que la première, et Li Zhuang, Feng Zhou et J. D. Tygar de l'Université de Berkeley en sont à l'origine, dans l'article "Keyboard Acoustic Emanations Revisited" publié en 2005.
Cette méthode donne des résultats encore plus impressionnants, puisque sur 10 minutes d'enregistrement d'une saisie de texte en anglais, 96% des caractères sont reconnus.
Elle repose sur la combinaison de machine learning et de techniques de reconnaissance de texte.

De plus, elle est beaucoup plus simple à mettre en place dans un cas réel. Contrairement à la méthode précédente, il n'est pas nécessaire d'entraîner un réseau de neurones à partir du clavier qu'on souhaite écouter ce qui permet notamment d'écouter les sons peu importe le clavier.

En outre, il est aussi possible de reconnaître des textes aléatoires. Le taux de reconnaissance est cette fois plus faible, puisqu'une partie de l'analyse de fait de façon statistique (A partir du début d'un mot il est possible de supposer quelle est la lettre suivante pour former le mot complet dans la langue étudiée), mais reste impressionnant. Pour des textes aléatoires de 5 caractères, 90% sont trouvés en moins de 20 essais, et pour des textes de 10 caractères, 80% sont trouvés en moins de 75 essais.
En d'autre terme il est assez facile de trouver un mot de passe avec cette méthode, même s'il est constitué aléatoirement.

Principe de l'attaque

Pour attaquer un utilisateur, il suffit de trouver un moyen d'enregistrer ce que ce dernier saisis. Il faut ensuite traiter le son enregistré, et on peut sortir de cette analyse un certain nombre d'éléments, en plus du texte supposément saisi. Il est possible de déterminer si la séquence de touches à été saisie par la même personne, avec le même clavier et avec les mêmes conditions d'enregistrement.
Comme dit plus tôt, la reconnaissance du texte se fait sans entraînement de l'algorithme par l'intermédiaire d'enregistrement des sons produits par l'activation des touches du clavier. On utilise cette fois une approche statistique, et plus une simple comparaison des sons.
Quand un utilisateur saisit du texte en anglais, le nombre de mot du dictionnaire anglais limite les combinaisons de touches possibles, et la grammaire du langage limite les combinaisons de mot. En d'autres termes, une phrase saisie par un utilisateur à un sens et est composée de mots présents dans le dictionnaire.

1) Traitement de l'enregistrement

Une fois le son de la saisie enregistré, il faut le traiter. Dans l'étude menée par Asonov et Agrawal, les sons avaient étés traités par l'intermédiaire d'une FFT (Transformée de Fourier).

Ici, la technique du cepstre à aussi été utilisée dans le but de comparer l'efficacité des deux traitements.
En fin de compte, les résultats obtenus avec le cepstre sont plus précis qu'avec une simple FFT du son enregistré.

2) Unsupervised key recognition

Dans un premier temps, on regroupe les touches du clavier dans une des K classes d'un ensemble à partir de leur sons (produits par d'un clavier quelconque). Pour les trier, on utilise des méthodes de classifications standard. Le nombre de classes K est choisi de manière à ce qu'il soit légèrement plus grand que le nombre de touches du clavier. A partir des échantillons enregistrés et des contraintes du langage, on peut établir une classification des caractères saisis dans les K classes.
Cependant, les algorithmes de regroupement peuvent être imprécis. On peut parfois avoir des frappes d'une même touches qui se retrouvent après classification dans des classes différentes. Dans chaque classe, on pourra retrouver la touche avec une certaine probabilité d'apparition. Dans une bonne classification, on a pour chaque touche une classe qui aura une probabilité plus forte que pour les autres.
Une fois la distribution des touches déterminée, on essaie de retrouver la séquence de touches la plus probable à partir d'un enregistrement.
Cependant, cela ne reste pas suffisant pour avoir des résultats précis. On utilise donc un Modèle de Markov Caché. A l'aide de ces derniers, on peut alors déterminer la corrélation entre des touches tapées en séquence.

Prenons l'exemple suivant :
L'algorithme mis en place détermine que la lettre courante à analyser peut être soit un "h" soit un "j".
L'algorithme a déterminé que la lettre précédente du mot était un "t".
Alors la lettre à une chance plus importante d'être un "h", puisque la séquence "th" est plus souvent présente dans les mots anglais que la séquence "tj".

Cette étape à elle seule permet d'obtenir des taux de reconnaissance légèrement au dessus de 60% des caractères, et autour des 20% de reconnaissance pour des mots.

3) Vérification de grammaire et épellation

Pour être encore plus précis, on va ensuite utiliser une étape de vérification de grammaire et d'épellation. En utilisant un dictionnaire anglais et un modèle statistique de la grammaire anglaise combinée au Modèle de Markov Caché, on va améliorer la précision de notre algorithme, et donc le taux de reconnaissance.
On arrive alors à un taux de reconnaissance au delà des 70% pour des caractères et environ 50% de reconnaissance pour des mots.

C’est beaucoup mieux, mais cela reste toujours inférieur au résultats obtenus par la technique d’Asonov et Agrawal.

4) Feedback-based training

La dernière étape est l'entraînement par rétroaction ou “Feedback-based training”. Elle permet d’obtenir une classification des frappes de touches sans être basée sur la grammaire du langage. La grammaire du langage nous permet de prévoir et mieux identifier les mots de la langue écoutée. Cependant un utilisateur ne saisit pas toujours des mots et phrases qui ont du sens, c’est le cas par exemple lorsqu’il doit renseigner un mot de passe (qui serait bien choisi). Cette classification des touches permet de reconnaître des textes aléatoires.
On sait que les mots qui n’ont pas étés corrigés par les étapes précédentes ont plus de chance d’être corrects que ceux corrigés. On va alors prendre les mots qui ont moins d’un quart de leurs caractères corrigés, et on les utilise pour entraîner le classificateur.
La phase de reconnaissance est de nouveau exécutée et traite les nouveaux échantillons obtenus par le passage précédent. On obtient alors un taux de reconnaissance plus élevé.
On récupère de cette nouvelle reconnaissance le nombre de corrections apportées au texte comme indicateur d’amélioration. On répète la procédure plusieurs fois, jusqu’au moment où l’indicateur nous montre que la reconnaissance du texte ne progresse plus.
Cette classification permet d’obtenir des résultats plus précis, puisqu’on arrive à des taux de reconnaissance pouvant aller jusqu’à 92% en moyenne.

L’expérience

1) Matériel utilisé

Pour réaliser l’expérience, un clavier classique et un **simple micro (à environ 10$)** ont été utilisés. Il n’est donc pas nécessaire de posséder un matériel coûteux pour mettre en place l’expérience, et donc une attaque.

2) Différents environnements

Dans un environnement bruyant, on s’attend à ce que la reconnaissance soit moins efficace, puisque l’algorithme utilisé pour détecter le début d’une frappe de touche (et ensuite l’analyser) échoue parfois à cause des bruits parasites.

	Ensemble 1		Esemble 2		Ensemble 3		Ensemble 4	
	Mots	Lettres	Mots	Lettres	Mots	Lettres	Mots	Lettres
Unsupervised learning (%)	74.57	87.19	71.30	87.05	56.57	80.37	51.23	75.07
Feedback-based training (étape 3) (%)	90.46	96.34	89.30	96.09	83.13	94.72	79.51	92.49

Les tests sur les ensembles 1 et 2 ont étés réalisés dans un environnement calme, tandis que les tests des ensembles 3 et 4 ont étés réalisés dans des environnements bruyants.

Tout d'abord, l'enregistrement est soumis à l'étape "unsupervised training" qui mène à des résultats d'environ 80% de reconnaissance.
Ensuite, plusieurs passages par l'étape "Feedback-based training" (ici 3 passages) améliorent le taux de reconnaissance.

Ces résultats permettent de montrer que la correction utilisant le modèle du langage améliore fortement le taux de reconnaissance des mots, et que le taux de reconnaissance dans un environnement calme sont légèrements meilleurs que dans un environnement bruyant. Néanmoins, après plusieurs passages par l'étape de "Feedback-based training", on corrige peu à peu les erreurs dues au bruit parasites, et on observe que la différence du taux de reconnaissance entre environnement calme et bruyant diminue elle aussi.
De plus, si le mapping des positions des touches a été bien corrigée après plusieurs passages par l'étape de feedback, on peut atteindre de taux de reconnaissance allant jusqu'à 96% pour des caractères.

3) Comparaison des techniques de classification

Dans l'expérience d'Asonov et Agrawal, la classification des touches avait été possible par l'intermédiaire d'un réseau de neurones. Dans cette expérience, les chercheurs ont souhaité comparer plusieurs méthodes de classification dans le but de déterminer quelle est la meilleure. La classification linéaire, gaussienne et par réseau de neurones ont été comparées.
Le tableau suivant donne les taux obtenus pour chaque méthode.

	Réseau de neurones		Classification linéaire		Classification gaussienne	
	Mots	Lettres	Mots	Lettres	Mots	Lettres
Reconnaissance (%)	81.42	91.93	90.46	96.34	83.86	93.60

Comme on peut le constater la classification linéaire donne les meilleurs résultats.

4) Durée minimale d'enregistrement

Enfin, une dernière question s'est posée. Jusqu'à présent des enregistrements entre au delà de 10 minutes étaient utilisés. Mais quelle est la durée minimale d'un enregistrement nécessaire pour que l'utilisation de l'algorithme soit efficace ? En effet on a besoin d'un montant minimum de données (et donc de sons différents de clics) pour le faire fonctionner correctement. L'expérience à été reproduite à partir de "morceaux" du premier ensemble de données. Le graphique suivant montre que 5 minutes d'enregistrement ont été nécessaires pour que la reconnaissance atteigne des taux corrects.

5) Analyse avec différents claviers

Etant donné que cette méthode ne repose pas uniquement sur l'écoute acoustique des sons produit par la frappe d'une touche comme celle d'Asonov et Agrawal, on s'attend à ce que la reconnaissance soit possible peu importe le clavier utilisé.

L'expérience décrite précédemment à donc été reproduite une fois de plus, mais avec trois claviers différents, et un âge différent (Le premier clavier était utilisé depuis 6 mois, le second depuis 5 ans et le dernier était neuf).

Le tableau suivant présente les résultats obtenus avec ces trois clavier, et comme on pouvait s'y attendre les taux de reconnaissance sont très proches de ceux obtenus dans la première partie de l'expérience.

	Clavier 1		Clavier 2		Clavier 3	
	Mots	Lettres	Mots	Lettres	Mots	Lettres
Reconnaissance (%)	82.63	93.56	82.29	94.42	74.87	89.81

En conclusion n'importe quel clavier peut être soumis à une reconnaissance utilisant l'algorithme mis en place par Li Zhuang, Feng Zhou et J. D. Tygar.

Pistes pour améliorer la reconnaissance

1) Intégrer les touches rémanentes

Dans cette expérience, seules les touches en minuscules et certains caractères spéciaux ne peuvent être reconnus. Une des améliorations à apporter à cette méthode de reconnaissance serait d'ajouter la combinaison de touches qui est plus difficile à identifier.
En effet utiliser des touches comme "Ctrl", "Shift" ou "Alt", revient à actionner la touche, puis une ou plusieurs autres, dans le but de réaliser une action. Déterminer la séquence correspondante est alors plus difficile que dans un cas classique, puisque cette fois la première touche est maintenue. Sur le spectre de fréquence, on ne retrouve donc plus les deux pics correspondant à l'appui sur la touche puis son relâchement. Ceci rend l'identification de la touche plus difficile avec la méthode de traitement du son utilisée dans cette expérience.

2) Analyser des langages de programmation

L'expérience à été réalisée en anglais, mais il est aussi possible de remplacer l'anglais par une autre langue, à partir du moment où on possède les données liées au dictionnaire et aux règles de grammaire de cette dernière.
Utiliser des contextes différents, comme par exemple dans un environnement de développement pourrait se révéler intéressant.
Chaque langage possède aussi ses règles, c'est pourquoi appliquer cette expérience à un langage de programmation semble être possible. En revanche, on retrouve dans ces langages des caractères spéciaux beaucoup plus présents que dans des langues humaines, ainsi que des calculs ou formules mathématiques qui sont plus difficiles à prévoir.
Ce type d'écoute pourrait être utilisée pour de l'espionnage industriel.

3) Traitement des bruits parasites

Enfin, si d'autres sons sont présent dans l'environnement écouté, ils peuvent interférer avec le son produit par l'utilisateur, ce qui peut rendre la reconnaissance moins efficace. Ces dernières années, de nouvelles techniques de traitement du son sont apparues dans le but d'éliminer des sons parasites. Intégrer ce type de traitement dans cette expérience pourrait permettre de récupérer plus aisément un texte saisis dans n'importe quel type d'environnement, ainsi que grandement améliorer son efficacité.

4) Analyser d'autres appareils

On sait maintenant que les claviers mécaniques peuvent donner de l'information à un attaquant assez aisément par une simple écoute des sons que ses touches produisent. Mais qu'en est-il d'autres appareils ?
Asonov et Agrawal se sont posé cette question, et ont essayé de réaliser leur expérience sur d'autre appareils.

a) Ordinateurs portables

Les ordinateurs portables possèdent des claviers construits différemment et qui sont moins bruyants.

Comme attendu, les résultats se sont montrés moins précis qu'avec un clavier d'un ordinateur de bureau. En effet, sur 20 clics de touches, 2 reconnaissances sont incorrectes.

b) Téléphones portables

Au début des années 2000, la plupart des téléphones portables possédaient des claviers physiques, et actionner des touches pouvait faire du bruit.

Cette fois, l'expérience s'est révélée efficace puisque sur 20 clics, toutes les reconnaissances sont correctes.

Asonov et Agrawal ont poussés un peu plus loin l'analyse, en entraînant le réseau de neurones à partir d'un téléphone, puis en essayant la reconnaissance sur un appareil différent mais restant similaire au premier.

La qualité de la reconnaissance est alors moins bonne, mais il reste possible d'attaquer un téléphone différent puisqu'un attaquant récupère de l'information sur le texte saisis.

Solutions pour contrer les attaques

Comme on a pu le voir, ce type d'attaque, même si elle ne sont pas fiables à 100%, permettent de donner un certain nombre d'informations à un attaquant.
Pour les contrer on peut imaginer plusieurs solutions :

1) Travailler sur le bruit produit par les touches des claviers :

L'une des pistes concernant la différence de bruit produit par les touches du clavier est la plaque présente sous les touches. En effet selon Asonov et Agrawal, la manière dont sont agencées les touches du clavier sur cette plaque provoquerait les différences de son. Il faudrait alors travailler sur des claviers construits différemments.

La seconde est la construction de claviers totalement silencieux. Il existe aujourd'hui des claviers plus silencieux que les claviers mécaniques, mais les sons qu'ils produisent pourraient toujours suffire à donner de l'information à un attaquant.
Un certain nombre de dispositifs existent dans le but de réduire le son émis par la frappe sur une touche comme par exemple des joints amortisseur en silicone. Les utiliser peut être une première solution contre ce type d'attaque.

L'utilisation de claviers non mécaniques pourrait aussi être une solution. On voit de plus en plus de claviers lasers qui présentent l'avantage de ne pas produire de bruit lorsqu'on les utilise.

Enfin, on pourrait également imaginer des claviers qui produisent l'inverse du bruit produit par la touche lors d'un clic. Cette solution, s'il est possible de l'implémenter, annulerait le son produit par une saisie de texte, et rendrait l'attaque inefficace.

2) Utiliser des mots de passes longs et aléatoires

La seconde attaque présente des résultats aussi impressionnant puisque de part sa nature elle est en mesure, en s'appuyant sur les dictionnaires et grammaires des langues, de déterminer les caractères qui ont le plus de chances d'apparaître dans un contexte donné. C'est aussi cette particularité qui fait que la reconnaissance de chaînes de caractères aléatoires est plus difficile.
Avec cette attaque statistique, les chercheurs sont en mesure d'identifier des chaînes de caractères aléatoires courtes (entre 5 et 10 caractères).
Un premier mécanisme de défenses contre ce type d'attaques serait d'utiliser de bons mots de passes, composés de nombreux caractères aléatoires.

3) Utiliser l'authentification à deux facteurs :

Un autre moyen de sécuriser au maximum un compte est l'authentification à deux facteurs. Cette méthode permet d'avoir une seconde sécurité, dans le cas où un mot de passe serait trouvé par un attaquant

4) Travailler dans un environnement sécurisé

La dernière solution consiste à travailler dans un environnement depuis lequel on peut être certain de ne pas être écouté. Ce n'est pas une solution toujours évidente à mettre en place,

mais en travaillant dans des salles isolées phoniquement, et en s’assurant qu’aucun micro n’est présent, il est possible de limiter les risques, puisque pour ce type d’attaque, l’attaquant a besoin d’avoir un dispositif d’enregistrement non loin de la personne à écouter.

Keyboard Acoustic Emanations :
https://web.eecs.umich.edu/~genkin/teaching/fall2018/EECS598-12_files/kbdacoustic.pdf

Keyboard Acoustic Emanations Revisited :
https://www.researchgate.net/profile/Feng_Zhou56/publication/220593625_Keyboard_acoustic_emanations_revisited/links/5770085108ae621947487a14.pdf

Acoustic Cryptanalysis :

https://link.springer.com/article/10.1007/s00145-015-9224-2

Images et animations des claviers :
http://xahlee.info/kbd/keyboard_switch_mechanisms.html

Comparaisons des sons des claviers :
http://xahlee.info/kbd/mechanical_keyboard_noise_comparison.html