Méthode de détection multi-modale de comportements anormaux en sécurité informatique

Baptiste Leterrier
silkke
Email : baptiste.leterrier@silkke.com

Alexis Bitaillou
Polytech Nantes
Email : alexis.bitaillou@etu.univ-nantes.fr

Benoît Parrein
Polytech Nantes
Email : benoit.parrein@univ-nantes.fr

Remi Lehn
Polytech Nantes
Email : remi.lehn@univ-nantes.fr

***Résumé*—L'authentification est une phase importante. Elle permet d'autoriser ou non un utilisateur à accéder à des ressources. Le mot de passe est le moyen d'authentification le plus courant en informatique. Malheureusement, il peut être vulnérable aux attaques. Afin d'augmenter la sécurité lors de l'authentification, nous cherchons un moyen d'authentification ne reposant pas uniquement sur le mot de passe.**

1. Introduction

La sécurité en informatique est le deuxième aspect le plus important après la disponibilité. Les logiciels de sécurité habituels (antivirus, parefeu, etc) ne suffisent plus pour détecter les menaces. Par exemple, une personne ayant un accès physique peut contourner le couple identifiant - mot de passe et ainsi dérober des données. La détection de comportements anormaux permet d'ajouter une strate supplémentaire de sécurité. La détection de comportements essaye de déterminer si les actions de l'utilisateur sont conformes à un profil établi. Le profil peut contenir par exemple les processus, l'activité réseau, les appels systèmes. La difficulté intervient lors de la création du profil. Si le profil est statique, le moindre comportement légèrement déviant peut déclencher une alarme et augmenter le nombre de faux-positifs. Si il est trop dynamique, il risque de rester dans une phase d'apprentissage indéfiniment et fera perdre en granularité de détection (seuls les événements vraiment déviant seront détectés). Dans tous les cas, la détection de comportement anormaux relève d'un problème d'apprentissage et de décision.

2. Présentation de la problématique

2.1. De la faiblesse des mots de passe

L'authentification sur un système informatique, se fait traditionnellement par un identifiant et un mot de passe. Ce mode d'authentification constitue le principal moyen d'authentification sur les systèmes informatiques. Sa simplicité a contribué à son adoption. Néanmoins, il est possible d'usurper l'identité de quelqu'un grâce à la connaissance de ces paramètres. En effet, certains identifiants sont standardisés comme les identifiants administrateurs, par exemple "root" sur les systèmes Unix. Malheureusement, le mot de passe est lui aussi attaquable. La puissance de calcul disponible a beaucoup augmenté. L'utilisation des cartes graphiques pour le "cracking" a diminué sensiblement le temps des attaques comme le montre [1]. Il montre une réduction de 99.7% du temps d'attaque par rapport à la force brute sur processeur.

2.1.1. Les précédentes tentatives. Diverses alternatives ont été étudiées et développées. Ces alternatives sont axées sur l'identification biométrique, l'authentification matérielle et d'autres éléments mémorisables. Par exemple, l'empreinte digitale peut être utilisée pour identifier et authentifier une personne. Mais l'empreinte digitale est une donnée personnelles, son utilisation est soumise à restriction. Le résultat n'est pas exact. Comme décrit dans [2] , l'identification biométrique évalue la probabilité qu'un échantillon soit proche d'autres échantillons de référence et prend une décision. Ces alternatives sont potentiellement complexes à mettre en place et ne garantissent pas nécessairement de résultats. Un système d'authentification seul est insuffisant. En effet, le contournement des systèmes d'authentification est inévitable. Même les systèmes biométriques sont contournables comme exposé dans [3].

2.1.2. A la fusion des techniques. A défaut de créer de nouvelles techniques, les recherches se portent la fusion de techniques existantes. Par exemple, dans [4], la dynamique de la frappe de clavier et la reconnaissance faciale sont utilisées. Les deux techniques ont des précision différentes. La difficulté intervient lors de la fusion des données et de la prise de décision. Il faut pondérer le poids de chaque métrique pour aboutir à une tendance.

3. Plan de l'étude

Il existe déjà des papiers sur les différentes méthodes d'authentification. Le premier objectif est d'établir un comparatif des techniques existantes. Notre comparatif s'effectuera sur différents critères. Par exemple, les moyens techniques nécessaires, les nombres d'échantillons nécessaires à l'apprentissage, la précision sont des critères utilisables.

Nous pourrons essayer de trouver de nouvelles méthodes. En effet, nous pouvons tenter de créer une méthode d'authentification. Toutes les méthodes n'ont pas été découvertes. Néanmoins, nos moyens sont limités. A défaut de créer une nouvelle méthode, nous pouvons fusionner des méthodes préexistantes.

4. Etat de l'art

4.1. Dynamique des frappes de clavier

Le clavier est un des premiers périphérique d'un ordinateur. Son principe n'a pas évolué depuis des décennies. La frappe (dans son rythme, sa force) varie d'une personne à une autre, ce qui fait que notre frappe est unique, comme nos mains par exemple.

4.1.1. Présentation. Le clavier est présent sur quasiment sur tous les ordinateurs. De plus, la disposition des touches est relativement standardisé. L'utilisation de la frappe de clavier comme moyen d'identification n'est pas un concept "récent". En 1993, [5] utilise ce concept pour ce qui semble la première fois. Ils mesurent le temps de pression et le temps de relâche de chaque touche. A partir de ces deux mesures, plusieurs métriques peuvent être calculeées. La métrique plus évidente est la vitesse de frappe (pour un mot donné). La durée entre chaque pression peut être une métrique utilisable pour un même mot. Enfin, on peut calculer la durée de la pression.

La dynamique des frappes n'est pas utilisable dès sa mise en place, un temps d'initialisation est requis. Un apprentissage est nécessaire pour utiliser la dynamiques des frappes. La quantité d'échantillons dépend de la méthode de décision. La méthode de décision peut être statistique ou par réseau de neurones (comme dans [6]).

4.1.2. Intérêt de la proposition. L'identification par la dynamique des frappes est une technique intéressante. Le clavier est un périphérique répandu. Il est donc plus facile d'intégrer cette technique sur des équipements existants. Certaines métriques restent valables même sur des claviers virtuels.

Sur les systèmes dérivés de Unix, la mise en œuvre semble relativement simple. Dans [5], ils utilisent une application pour d'intercepter les événements depuis le serveur X.org.

De nombreuses expérimentations ont déjà été effectué. La technique est donc relativement éprouvée. Les résultats sont généralement bons avec cette technique. La précision garantie est en moyenne proche des 80%.

4.1.3. Limites de la proposition. L'identification par la dynamique des frappes n'a pas que des avantages. Comme le résume [7], le résultats sont très variables. Le taux est influencé par la méthode de décision. Comme le montre [5], parfois, il n'y a pas de vraie différence entre une méthode de décision triviale comme la distance géométrique et une méthode de décision plus complexe comme un réseau de neurones avec rétro-propagation. Dans l'article, la différence est d'environ 2%. La différence d'écart peut se justifier dans ce cas par le faible nombre de couche du réseau de neurones, le nombre de participant ainsi que le nombre d'échantillons.

Le nombre d'échantillons a une grande important et varie en fonction de la méthode de décision. Le nombre d'échantillons nécessaire n'est malheureusement pas prédéfini. De plus, la base d'apprentissage doit être régulièrement mise à jour. La dynamique frappe étant une donnée biométrique, elle dépend de l'état biologique de l'utilisateur à un moment t. L'âge, l'expérience, la santé de l'utilisateur peuvent modifier cet état et donc la précision de l'identification. Les effets d'un changement de modèle de clavier n'a pas été évalué.

Cette technique, si elle n'est pas encadré, peut devenir dangereuse car il est possible de modifier le programme pour le transformer en enregistreur de frappes (keylogger).

4.2. Son des frappes de clavier

Une variation de la dynamique de frappe consiste à utiliser le son de la frappe. L'objectif est donc d'utiliser le son du clavier pour identifier une personne. Comme pour la dynamique de frappe de clavier, le son de la frappe permet d'obtenir des métriques aux valeurs "uniques" pour chaque personne.

4.2.1. Présentation. Le clavier est souvent présent avec un ordinateur. Lorsqu'un microphone est présent, on peut enregistrer le bruit de la frappe sur le clavier. [8] utilise cette idée. La frappe au clavier est une caractéristique propre à chaque humain. Elle est fonction de du corps et en partie du clavier. L'objectif est d'enregistrer le son de la frappe du clavier pour un mot donné. Cette technique n'est pas utilisable instamment. En effet, une durée d'initialisation est nécessaire. L'apprentissage dépend de la méthode de décision.

Le son des frappes de clavier n'a pas été beaucoup étudié. A notre connaissance, [8] est le seul article traitant du sujet.

4.2.2. Intérêt de la proposition. Le son de la frappe de clavier peut être facilement intégré aux ordinateurs portables. En effet, la plupart des ordinateurs portables sont doté d'un microphone intégré. Pour les ordinateurs fixes, la situation est complexe. Tous les ordinateurs fixes n'ont pas de microphone.

Les résultats des expérimentations sont bons. Dans [8], le moins bon résultat est 88% de précision. Mais les tests sont effectués uniquement sur 4 groupes distincts.

4.2.3. Limites de la proposition. Cette technique a quelques inconvénients. La capture du son n'a pas été testé dans un milieu bruité. Le bruit pourrait diminuer la précision. Dans un environnement type "open space", le micro pourrait capturer le bruit d'un autre clavier.

L'étude [8] a testé avec un seul et unique clavier. Dans le cas où l'utilisateur n'a pas d'ordinateur déterminé, l'impact du changement de clavier n'a pas été mesuré.

4.3. Mouvement de la souris

Bien que crée après le clavier, la souris s'est imposé comme outil d'interface homme-machine. Le nombre de touches est limité, mais la souris transmet ces déplacements.

4.3.1. Présentation. Après la utilisation du clavier, la souris est utilisé pour l'identification d'utilisateur. L'objectif est d'utiliser les déplacements, les accélérations et les clics effectués avec la souris. Les accélérations sont calculés à partir des mouvements. Cette technique n'est pas utilisable instamment. En effet, une durée d'initialisation est nécessaire. L'apprentissage dépend de la méthode de décision. La technique est relativement jeune car elle est utilisé que depuis quelques années.

4.3.2. Intérêt de la proposition. La technique est conceptuellement relativement simple. Intuitivement, il semble que si l'utilisateur est une personne relativement âgée, les accélérations de la souris seront faibles et de courte durée.

Le matériel nécessaire pour la mise en œuvre de cette technique est relativement abordable et/ou disponible.

En utilisation supplémentaire/complémentaire, l'utilisation de la souris prend plus d'intérêt. [9] et [10] l'utilisent en complément du clavier.

4.3.3. Limites de la proposition. Cette technique présentes quelques inconvénients. L'utilisation de la souris n'est disponible que dans un contexte d'identification continue. Il n'est pas pertinent de capturer des évènements sur une durée très courte. Au moins, le cas n'est pas évoqué dans [10].

Dans [10], les résultats sont relativement décevants, la précision est borné entre 45% et 60%. Cela implique la nécessité de l'utiliser en tant que technique complémentaire et/ou supplémentaire.

Dans [9], le nombre d'évènements utilisés est relativement important. Le stockage de tous ces évènements doit avoir un coût. Le coût peut être en stockage et/ou en temps de collecte avant apprentissage.

4.4. Identification à partir des réseaux wifi

La diversification et la multiplicité des moyens d'interactions utilisés par les personnes souhaitant interagir avec le monde numérique ce sont depuis quelques années beaucoup d'accélérés.

En témoigne l'augmentation des ventes de matériel biométrique simple où la diffusion des systèmes d'authentification avec token par exemple token RSA.

Si des système d'acquisition externe permettre en effet de récolter des informations d'identification ou d'authentification, il convient de constater que de nombreuses outils déjà présent dans le milieu personnel ou professionnel en informatique peuvent servir de vecteurs complémentaires d'acquisition de l'information et peuvent parfois même voir leur usage évoluer.

4.4.1. Présentation. La technologie WiFi est intégrée depuis plusieurs années dans le monde de l'informatique et aujourd'hui est de retour dans les innovations de par l'explosion de l'utilisation de périphériques mobiles (smartphones, tablettes) mais aussi de l'arrivée de l'internet des objets (IOT) [11]

La couverture lieu de travail et depuis longtemps une réalité mais on constate aujourd'hui l'acquisition de nouveau terrain notamment les villes par les offres de wifi gratuit ou encore la simplicité d'implémentation à la maison par les fonctions de routeur wifi offerts par les modems des principaux opérateurs.

Le wifi étant basé sur des ondes radios il est possible de voir les points d'accès WiFi Hotspot comme des balises rappelant les radars. L'émission des ondes et leur captation par un système approprié ou le routeur en lui-même permet d'estimer la qualité du signal et donc de déduire la présence d'obstacles. Cette méthode est déjà utilisé pour optimiser le débit et la couverture du réseau en milieu clos [12].

Si la surveillance des réseau wifi rend possible la localisation en intérieur de différents périphériques notamment grâce à leur adresse MAC, l'extension de la possibilité de détecter les obstacles a fait naître l'idée de l'utilisation des points d'accès wifi comme balise de détection de personne.

La surveillance des périphériques connectés ou non au réseau donne déjà une indication quant à la présence d'une personne, toutefois il n'assure pas que la personne est bien présente physiquement dans les lieux et impose de plus la mise en place d'une table de relation faisant le lien entre les personnes et les périphériques qu'elles possèdent.

Utiliser le wifi comme support d'identification des personnes est une idée très récente reposant sur des travaux avant-gardistes en utilisant des technologies avancées. Ceci explique sa diffusion réduite et son aspect expérimental.

Ces travaux s'appuie sur les méthodes d'identification humaine originellement réservé au domaine biométrique (empreinte digitale,voix) et ont marqué une avancée importante dans le domaine de l'interaction homme-machine. [13]

L'identification humaine grâce aux canaux wifi ouvre la voie à une méthode moins intrusive que celles actuellement connues et nécessitant la présence proche de la personne ou provoquant un arrêt de son activité pour s'identifier. Une autre problématique est aussi la disponibilité des outils permettant la capture.

Si des essais ont été effectués avec des standards radar classiques, leur diffusion dans le domaine public ou professionnel reste limité au cercle des avertis. Utiliser le wifi comme support de capture permets donc de s'affranchir de cette contrainte et de disposer de tout un panel de points de

collecte déjà déployés dans divers environnements (bureaux, maisons)

4.4.2. Présentation. Les mesures s'appuie sur les reliquat généré par une personne au niveau des ondes wifi. La corpulence la manière de se déplacer ou encore les gestes effectués permettre une différenciation précise entre divers individus.

Cette approche permet une identification précise sans toutefois mettre en danger la vie privée comparée à d'autres méthodes.

En effet les premières tentatives de collecte de l'attitude et du comportement basé sur les mouvements nécessitait l'utilisation de caméras, ce qui impose des contraintes tels que le besoin de ligne de vue mais aussi la perte de vie privée de par la nécessité de capter continuellement l'attitude d'une personne.

La notion pratique et aussi perdu par la nécessité de placer plusieurs caméras à différents endroits le Cousson retrouve alors augmenté quand bien même cette méthode a prouvé son efficacité.

Ces travaux ont toutefois servi de point de départ à la constitution d'un ensemble de données permettant d'identifier les points de posture d'attitude et de mouvements clés à l'identification précise d'une personne.

Cette utilisation du Wifi n'est toutefois pas nouvelle puisque des des produits basé sur le wifi permettent déjà d'évaluer la chute de personne dans le milieu industriel.

Plusieurs méthode et outils sont toutefois nécessaire à l'extraction d'informations.

Le premier outil utilisé pour ses détection est le channel state information (CSI). Il permet d'étudier la manière d'un signal se propage dans un milieu connu en analysant par exemple les pertes de signal avec la distance.

Le second outil est l'analyse en composantes principales. Issu du monde géométrique et statistiques cette méthode permet de sortir des informations principales d'un nuage de variables corrélées. Ici son application concernant la dispersion des ondes radio permet d'ordonner un nuage de multiple points. N'ayant pas grande importance ensemble, l'ACP mettra en exergue les tendances de dispersion menant à la constitution d'un modèle.

La transformée en ondelettes discrète (DWT : discrete wevelet transform) permet de capturer la fréquence et la position de points dans le temps. Par transformations successives, il devient possible de reconstruire une image en deux ou trois dimensions.

Enfin le Dynamic Time Warping (DTW) déformation temporelle dynamique permet la mesure de similarité entre deux suites. Cet algorithme sert notamment à combler les vides de captation possible dans un environnement bruyant radiologiquement.

La combinaison de ces quatre outils associée à des interfaces wifi compatible permet la collecte de données, la suppression du bruit ambiant et l'extraction d'une onde correspondant à l'activité d'une personne.

La capacité sommaire mais toutefois existante des ondes wifi à traverser les surfaces peu absorbante permet l'implantation de ces points de collecte en divers endroits accessible.

De plus la corrélation entre une personne et son "bruit radio" n'est pas nécessaire.

4.4.3. Intérêts de la proposition. Cette méthode a été testée sur un panel de 9 personnes et indique des résultats très probants. La mise en place de cette solution requiert la mise en place de sondes, mais l'analyse des résultats peut-être fait grâce à une puissance de calcul limité. La création d'une signature initiale peut-être fait relativement rapidement par un processus de calibration requérant que les personne effectuent une certaine suite de mouvements connus à l'avance par le système.

La vie privée est aussi préserver de par l'absence de données identifiantes. Seule la corrélation entre les résultats et les personnes peut remettre en cause ce principe mais il a été prouvé que cela n'était pas nécessaire. La mesure servant de signature et donc à l'identification.

4.4.4. Limites de la proposition. La solution présentée met en avant certaines limites dans un environnement radio bruyant. La collecte est alors plus difficile et les résultats seront moins précis. Un travail supplémentaire de nettoyage peut-être effectué mais avec un risque de perte de précision.

Les environnements avec beaucoup de personnes rendent aussi la capture des mouvements plus complexes puisque le système n'a pas conscience. De la multiplicité des personnes se focalisant exclusivement sur les mouvements défauts positifs peut-être relever. À noter aussi que ces travaux se focaliser exclusivement sur les attitudes durant la marche ce qui peut-être non fiable dans un environnement professionnel ou les personnes sont assises à leur bureau.

Enfin si ce système permet de différencier les personnes dans un environnement, il ne permet toutefois pas leur authentification. Il est donc insuffisant pour prétendre à être un moyen de sécuriser correctement une infrastructure.

5. Preuve de concept

Afin de tester nos hypothèses, une preuve de concept est en cours de développement. Cette preuve de concept est composée de différents éléments. On peut le diviser en 3 parties (collecte, évaluation, exploitation). Un agent a été réalisé afin de collecter différentes métriques. Il a été développé pour les environnements Microsoft Windows et Canonical Ubuntu 16.10. Il permet notamment de récupérer les différentes frappes au clavier et de les corréler avec l'activité système, les processus etc. Pour prendre une décision, nous développons une application permettant de réaliser un apprentissage.

Cette approche vise à identifier une corrélation en le rythme de frappe et l'activité de l'utilisateur, dans le but de créer une tendance permettant de l'identifier dans le futur.

6. Conclusion

Les premiers résultats ont permis d'aboutir sur un ensemble de données d'apprentissage. Cet ensemble est actuellement utilisé dans un réseau de neurones qui permettra de potentiellement établir une tendance servant à l'identification d'un utilisateur.

Références

[1] T. Murakami, R. Kasahara, and T. Saito, "An implementation and its evaluation of password cracking tool parallelized on gpgpu," in *2010 10th International Symposium on Communications and Information Technologies*, Oct 2010, pp. 534–538.

[2] K. Nandakumar and A. K. Jain, "Biometric authentication : System security and user privacy," *Computer*, vol. 45, no. undefined, pp. 87–92, 2012.

[3] N. M. Duc and B. Q. Minh, "Your face is not your password face authentication bypassing lenovo–asus–toshiba," *Black Hat Briefings*, 2009.

[4] A. Gupta, A. Khanna, A. Jagetia, D. Sharma, S. Alekh, and V. Choudhary, "Combining keystroke dynamics and face recognition for user verification," in *Computational Science and Engineering (CSE), 2015 IEEE 18th International Conference on*, Oct 2015, pp. 294–299.

[5] M. Brown and S. J. Rogers, "User identification via keystroke characteristics of typed names using neural networks," *International Journal of Man-Machine Studies*, vol. 39, no. 6, pp. 999–1014, 1993.

[6] S. Ravindran, C. Gautam, and A. Tiwari, "Keystroke user recognition through extreme learning machine and evolving cluster method," in *2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Dec 2015, pp. 1–5.

[7] A. Peacock, X. Ke, and M. Wilkerson, "Typing patterns : a key to user identification," *IEEE Security Privacy*, vol. 2, no. 5, pp. 40–47, Sept 2004.

[8] M. Pleva, E. Kiktova, P. Viszlay, and P. Bours, "Acoustical keystroke analysis for user identification and authentication," in *2016 26th International Conference Radioelektronika (RADIOELEKTRONIKA)*, April 2016, pp. 386–389.

[9] L. Fridman, A. Stolerman, S. Acharya, P. Brennan, P. Juola, R. Greenstadt, and M. Kam, "Multi-modal decision fusion for continuous authentication," *Computers & Electrical Engineering*, vol. 41, pp. 142–156, 2015.

[10] S. Mondal and P. Bours, "Combining keystroke and mouse dynamics for continuous user authentication and identification," in *2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)*, Feb 2016, pp. 1–8.

[11] W.-F. Alliance, "Wi-fi alliance®introduces low power, long range wi-fi halow™," 2016. [Online]. Available : https ://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-low-power-long-range-wi-fi-halow

[12] M. Nowicki and J. Wietrzykowski, "Low-effort place recognition with wififingerprints using deep learning," *arXiv preprint arXiv :1611.02049*, p. 10, 2016.

[13] Z. W. M. L. Z. Y. Tong Xin, Bin Guo, "Freesense :indoor human identification with wifi signals," *arXiv preprint arXiv :1608.03430*, p. 6, 2016.