Résumé de l'article de recherche Telepathwords

Nicola Spanti

Janvier 2017

Table des matières

1 Article de référence

Ce document est un résumé en français d'un article de recherche en anglais. L'article en question est "Telepathwords : Preventing Weak Passwords by Reading Users' Minds". Il est issu de la collaboration de *Carnegie Mellon University* (Saranga Komanduri, Richard Shay, and Lorrie Faith Cranor) et *Microsoft Research* (Cormac Herley and Stuart Schechter). Il a été présenté durant le 23e *Security Symposium* de USENIX.

— ISBN : 978-1-931971-15-7
— Date : 20-22 août 2014
— Page web : `https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/komanduri`
— Article (en PDF) : `https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-komanduri.pdf`
— Résumé audio en anglais (MP3) : `https://2459d6dc103cb5933875-c0245c5c937c5dedcca3f1764ec ssl.cf2.rackcdn.com/sec14/komanduri.mp3`
— Résumé vidéo en anglais (MP4) : `https://2459d6dc103cb5933875-c0245c5c937c5dedcca3f1764ec ssl.cf2.rackcdn.com/sec14/komanduri.mp4`

2 Résumé

2.1 Introduction

Les mots de passe sont une méthode d'authentification courante. Malheureusement les individus choisissent souvent des mots de passe prédictibles (mots du dictionnaire, remplacement de la lettre "o" par le nombre zéro, etc). Pour tenter de remédier à ce problème, des chercheurs proposent *Telepathwords*. Ce système tentent de deviner quel mot de passe un individu va taper,

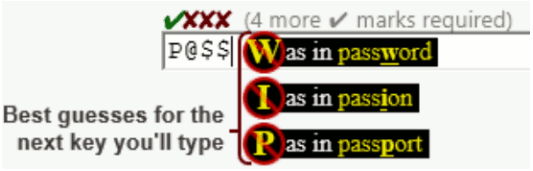

FIGURE 1 – L'interface graphique proposée

et l'informe de ses prédictions. Cela permet d'inciter ou obliger à s'enregistrer avec un mot de passe jugé imprévisible par le système. En d'autres termes, celui-ci permet de définir des bonnes conduites ou des régles pour un mot de passe. Il a été comparé avec d'autres pour évaluer son efficacité en fonction de différents critères.

2.2 Interface utilisateur

À côté de la zone de saisie du mot de passe, l'individu est informé des 3 lettres que le système juge les plus probables qu'il tape, celles-ci sont barrés pour mettre en avant qu'il est conseillé de les éviter. Il est également affiché la raison qui a déterminé à chaque prédiction de lettres. De plus, au dessus de chaque lettre tapée, il est indiqué si c'était ou pas une des lettres anticipées par le système (ou un de ses substituts courants comme l'arobase "@" pour la lettre "a"). Au dessus de la zone de saisie, il peut également être notifié un nombre minimum de lettres non anticipées à ajouter pour que le mot de passe soit accepté. Ainsi, l'utilisateur ou l'utilisatrice est informé·e en temps réel de la robustesse de son mon mot de passe, tout en sachant pourquoi, comme l'illustre la figure **??**.

2.3 Architecture

Telepathwords utilise une architecture client-serveur. Cela permet d'avoir beaucoup de données du côté du serveur pour faire la meilleure prédiction possible. En effet, les tests ont été faits avec 1,5Go de données. De plus, dans le cadre du Web (dans lequel l'usage des mots de passe est courant), une telle quantité de données est actuellement inacceptable.

Le mot de passe final sera envoyé en clair pour le serveur, lui envoyer les versions intermédiaires n'est donc pas problématique. Il faut néanmoins chiffrer le transport. On peut noter qu'il y a un risque de latence avec cette architecture, on peut l'amoindrir avec un cache.

2.4 Algorithmes de prédiction

Plusieurs algorithmes de prédiction sont utilisés. Il donne des prédictions et des raisons qui sont notés. Ainsi uniquement les mieux notées sont présentées à la personne tapant un mot de passe.

Ils utilisent un modèle de données optimisé pour prendre peu de place et être rapide à parcourir vers l'avant (c'est-à-dire les prochaines lettres). De plus, les majuscules et les espaces ont été enlevés.

Les algorithmes mis en place permettent de détecter :

— *les séquences de caractères courantes*, que ce soit à l'intérieur d'un mot (par exemple "prédi" pourrait être suivi de "re" ou "iction") ou à la suite d'un mot (par exemple "vie" pourrait être suivi par "privée" ou "intime"), avec la gestion des séparations par des nombres ou des caractères non alphanumériques (pour gérer des cas comme "pa1234ssword" et "12x34y678z9") et les substituts courants (comme le dollar "$" pour un "s")
— *la proximité des caractères sur un clavier*, ce qui permet d'éviter "123456" ou "azerty", mais cela suppose de connaitre la disposition du clavier
— *les répétitions*, par exemple "xyabcabcabc" ou "abcdefabc"
—