Dynamic Authentication by Typing Patterns TJHSST Senior Research Project Research Paper Computer Systems Lab 2009-2010

Luke Knepper
luke@lukeknepper.com

October 28, 2009

Abstract

This project will analyze and test the accuracy of dynamic typing pattern authentication methods. The program will generate a dynamic set of text that the user will be prompted to type, and then it will feed the user's typing characteristics through neural network structures. Experimentation will be done to determine the most accurate neural network structures and data collection conditions. This process will be an improvement on normal typing pattern authentication techniques, which use static passwords rather than dynamic text.

Keywords: authentication, security, typing patterns, neural networks

1 Background

1.1 Introduction

Current authentication techniques span all three tiers of security:

- Tier 1 - Identification (usernames)

- Tier 2 - Knowledge and Possession (passwords, ID cards, security questions, etc.)
- Tier 3 - Skills and Capabilities (captchas, voice recognition)

In the online world, usernames can be stolen, passwords and security questions can be guessed, and captchas can be cracked. The process of analyzing typing patterns, a tier 3 security method, has been around for decades, but only recently has been put to use commercially. Currently, commercial products only analyze the user's typing patterns when the user is typing their password, a simple, static word. Any computer hacker can easily write a keylogger to record the user's keystrokes when typing this word and then simulate that process to gain access to the user's account.

2 Research

There is currently a patent (US 6151593) for an authentication scheme by typing pattern analysis. This method reads in the time between keystrokes for a user when typing their password and then trains a three-layered neural network to this combination. It does not allow for a dynamically-generated content to be used, and does not test the different lengths of passwords. This is the most basic application of typing techniques for authentication, and this project will extend beyond these simple methods.

Multiple typing pattern log-in software packages exist, such as Psylock, but they all have the same weakness as the patent above: they rely on a static password instead of dynamic typing content and therefore can be easily hacked.

An independent team of researchers, headed by Peacock et al., tested the effect of many variations, including neural network set-up, password length, acceptance stringency, data used, and function used. They found the most effective neural network structure from their tests was to use a set-up where many independent neural networks are trained on different cores (i.e. parallel processing) using randomly generated starting weight vectors. During the training, the best weight vectors are picked and created using genetic algorithms. They found the smaller (more stringent) acceptance ranges came up with a good amount of false alarms (when it didn't let the correct user in, happened 22% of the time) but also minimized break-ins (when the incorrect user was let in, happened 3% of the time). They also found the

most effective password length was 7 characters, a mid-sized password (the longer passwords had no break-ins but many false alarms, and the shorter passwords had many break-ins). They concluded that a linear evaluation function was more effective than a quadratic function and that averaging was more effective than counting each training run. They suggest their results can be improved (75% success, 22% false alarm and 3% break-in for their best algorithm).

Another team working under L. Maisuria compared the accuracy of neural networks compared to cluster algorithms. A multi-layered perceptron-based neural network which learned on the Hebbian learning theory was used, as were ten different metrics to compare the clusters for the clustering.
They tested the different algorithms by recruiting twenty volunteers to participate in three different sittings. In the first sitting, they all trained their neural networks by typing in their password sixty times. In the next sittings, they attempted to log in to their accounts and break into the accounts of others. The sittings were spaced out by one week.
The study found that the clustering methods were slightly more accurate than the neural networks in rejecting impostors. They only found an average of 80% to 90% accuracy in rejection rate, not enough to comprise a stand-alone security system but certainly good enough to be used in conjunction with traditional methods. They found that all keystrokes should be measured, including the beginning and end strokes to the enter key, for the highest accuracy. They found that allowing impostors to observe the users typing before attempting to break in to their accounts had little effect on the accuracy.

3 Procedure

A simple proof-of-concept was completed in October '09. The program prompts two users to both type a sentence and uses their data to train a simple single-layer neural network. It then prompts the users with a third sentence and instructs one of them, whose identity is unknown to the computer, to type the third sentence. It runs the final data through the trained neural network and determines which user typed the third sentence.

4 Results and Conclusions

The proof-of-concept program has been tested twenty times, with the results shown below:

- Trial 1 – Correct
- Trial 2 – Correct
- Trial 3 – Correct
- Trial 4 – Correct
- Trial 5 – Correct
- Trial 6 – Correct
- Trial 7 – Correct
- Trial 8 – Incorrect
- Trial 9 – Correct
- Trial 10 – Correct
- Trial 11 – Correct
- Trial 12 – Correct
- Trial 13 – Correct
- Trial 14 – Correct
- Trial 15 – Correct
- Trial 16 – Incorrect
- Trial 17 – Correct
- Trial 18 – Correct
- Trial 19 – Correct
- Trial 29 – Correct

There were 18 correct runs, 2 incorrect runs out of 20 total runs, for a 90% accuracy overall. This shows that the concept can be used and refined to create an accurate authentication system, however it supports the idea that it cannot be a standalone system but instead will have to be used hand in hand with traditional authentication methods, such as passwords and usernames. The simple structure of the neural network leaves much to be desired.

References

[1] Cho, S. and Han, D. "Apparatus for authenticating an individual based on a typing pattern by using a neural network system." http://www.freepatentsonline.com/6151593.html

[2] Peacock, A. et al. "Typing Patterns: A Key to User Identification." http://www2.computer.org/portal/web/csdl/doi/10.1109/MSP.2004.89

[3] Maisuria, L. "A COMPARISON OF ARTIFICIAL NEURAL NETWORKS AND CLUSTER ANALYSIS FOR TYPING BIOMETRICS AUTHENTICATION."