A Deep Learning approach to Keystroke Dynamics

Nathan Horsley

Supervised by Neill Campbell

Keystroke Dynamics?

Keystroke Dynamics is a method of authenticating a user based on timing information from the way a person types as a biometric identifier.

It's not what they type, but how they type!

Keystroke Dynamics can be used to provide one of the factors of Multi-Factor Authentication. There are three different factors that make up MFA, which are:

1. Something you know (Password)
2. Something you have (ID Card)
3. Something you are (Biometrics)

Figure: Different factors of authentication

Keystroke Dynamics is a form of Behavioural Biometrics which have some advantages over other factors and other biometric methods:

1. Biometric factors, when done correctly, are very hard to forge, they use unique characteristics such as a fingerprint which can't be stolen or forgotten like an ID card or password.
2. Biometric factors can often require expensive additions to hardware, such as a fingerprint scanner. However, Keystroke Dynamics simply use your keyboard (there has even been work with mobile touch screen keyboards).
3. As it can gain information whilst you type, it is not intrusive to the user and can be done in the background of them typing their password.
4. Due to it's non invasiveness, it can also be used to authenticate continuously rather than just at the beginning of a session.

Deep Learning?

Deep Learning is a form of Machine Learning which consists of having layers of neurons which apply weights to its inputs and produce an output. By changing these weights with respect to a cost function and labeled output these *neural networks* can learn to complete complicated tasks such as image classification and speech recognition.

Figure: The structure of a single neuron.

Timing Information from Typing

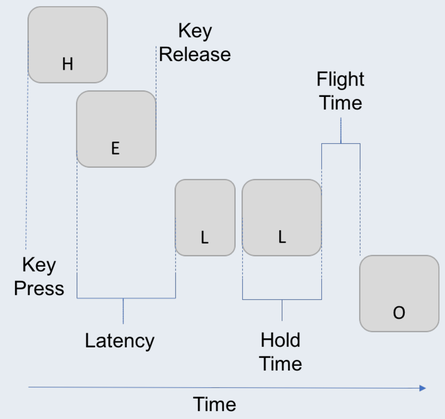

Figure: How timings can be extracted from typing.

Existing Work

Much of the existing work in Keystroke Dynamics has created datasets that can be used for research. These can be split into two different types:

1. **Static** - using a short phrase (possibly the user's password) a user can enter during the initial log in phase to help decide on authentication. One of the most used datasets in this area is the CMU dataset which has every user typing the same password 400 times. Each model is evaluated with their equal error rate and zero miss rate.
2. **Continuous** - Authenticating over a window of text such that a user can be continually authenticated even after logging in. These datasets are much harder to collect and can be further split into transcribed or free text. An example dataset containing both transcribed and free text is the dataset provided by the University of Clarkson where 39 users participate in giving an average of 21,000 raw keystrokes each.

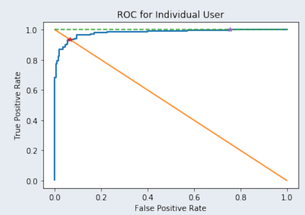

Figure: ROC Curve from following the CMU evaluation (Scaled Manhattan Distance). EER: 0.065, ZMR: 0.755

n-graphs

Timing information such as Latency can be used for each n-graph to build up a profile of the user (i.e a user may consistently type "he" at a similar speed on each occasion) and then you can test how later samples deviate and therefore decide whether to continue to give this user access.

Digraph	Trigraph
H E	H E L
E L	E L L
L L	L L O
L O	

Figure: A table of the Digraphs and Trigraphs produced when typing "HELLO"

The Project

The existing Keystroke Dynamics research does not contain much about Deep Learning, why?

- Because Deep Learning has only recently become feasible due to its hardware requirements to gain results?
- There isn't enough data?
- The dataset is not suitable for Deep Learning?
- The task is not complex enough to need Deep Learning?

And other questions to explore with Deep Learning in this field:

- Can Neural Networks outperform the other methods?
- If the information is sequential can LSTMs or RNNs give good results?
- Can Neural Networks use only timing information, with no knowledge of which digraph (n-graph) it came from?
- What security implications are there to Keystroke Dynamics?