Miyahara, Ryan

Dhavalikar, Rahul

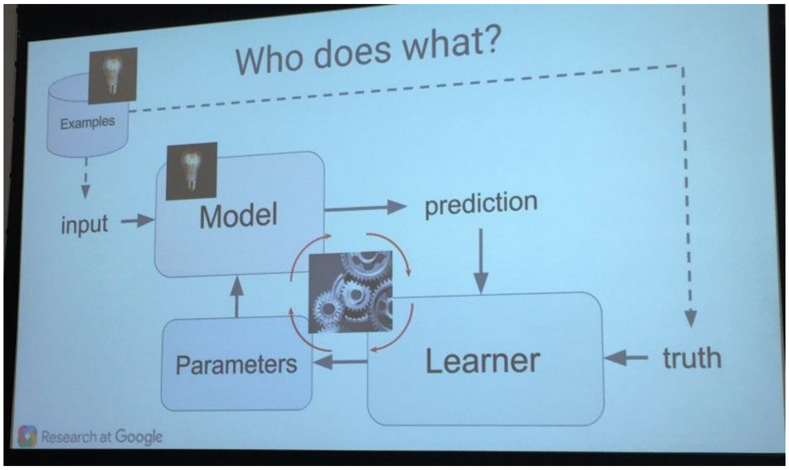
CS 35L, Lab 6

March 16, 2018

Machine Learning Based Smartphone Security

The ACM news article I researched was, "Russian experts submit 'impenetrable' smartphone protection system". The article introduced a new form of Smartphone security titled InCallAuth in which the program uses a combination of machine learning, biometric data, and artificial neural networks to create a model illustrating the way a user picks up their phone. According to the developer's description of his program, everyone differs in the way they pick up their phone. By following this model, the phone is able to recognize who is picking up the phone and if it should unlock itself. A small understanding of machine learning, biometric data, and artificial neural networks is necessary for understanding how InCallAuth works.

Machine learning is a process where a computer uses examples to create a model which predicts what future correct outcomes will look like. Below is a diagram from Google's "Machine Learning 101" presentation on November 3, 2015 (Sullivan). The diagram on the left shows us the process takes in examples and uses the input to create a model which is repeatedly tested

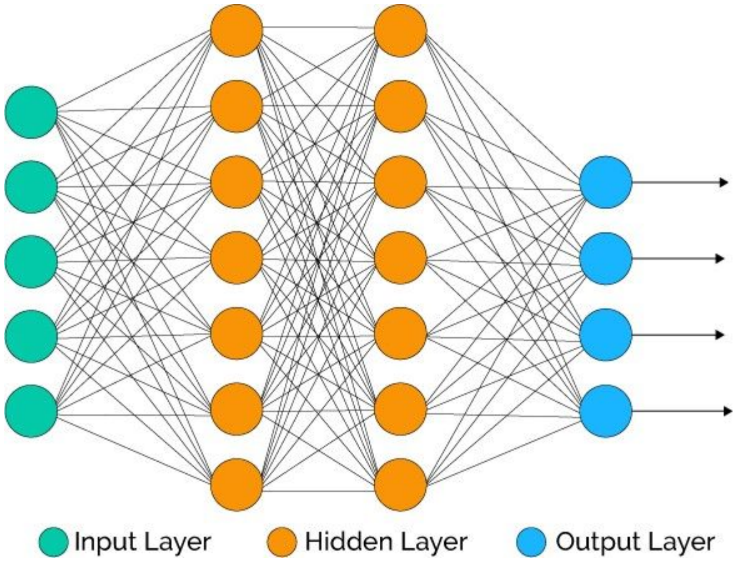


https://martechtoday.com/how-machine-learning-works-150366 against the “truth”. This “truth” is basically letting the process know if a correct prediction has been made or not. After the learning process takes place, the incorrect predictions are used to adjust the “parameters”. The process then makes a new model which, in theory, should become more accurate over each iteration (Sullivan).

In the case of the InCallAuth, the initial examples are created when the user is asked to pick up their phone 10 times. This is then turned into a model. Every time the user picks up their phone, which would happen very often in a real world application, the model becomes more and more accurate over time. An incorrect response is recorded when the user picks up their phone and it does not unlock. In this case, they are prompted for a password or pin in the same way most phones prompt their users today (Eremin).

To input the data for the machine learning program, the program must collect biometric data using the phone’s on board sensors. In this case, the sensors being used are the accelerator, gyroscope, and light sensor. The accelerator is used to measure the speed and acceleration at which the phone is moved from a pocket or a table, to the user’s desired viewing position. The gyroscope allows the angles at which the user holds their device to be recorded. Meanwhile the light sensor picks up if the phone is facing the user’s face for a call (Eremin). With the biometric data picked up by these sensors, the process is able to record data on the user and implement it in the machine learning model.

Lastly, InCallAuth utilizes artificial neural networks. While the concept as a whole is too in depth to explain here, the main points needed to understand InCallAuth are best illustrated in the diagram below. Each circle within the diagram represents a node. An input node, colored green in the diagram, represents a piece of input from the phone’s sensors. A hidden node,



https://www.xenonstack.com/blog/data-science/overview-of-artificial-neural-networks-and-its-applications

colored orange in the diagram, represents the algorithm changing the input into something useful for the program. The blue nodes are the output nodes of the diagram. These nodes are formatted to provide some sort of useable information for the program. Each node is connected to others through lines called connections. Like machine learning, the model for the program is constantly changing based on the correctness of the output. Artificial neural networks are used with machine learning to creating a changing model that becomes more accurate over time (Basheer & Hajmeer).

Unfortunately, InCallAuth's developers do not post very much news on their groundbreaking program. On top of this, the Institute of Cyber Intelligence Systems at the National Research Nuclear University MEPhI, where InCallAuth is being developed, is in Russia. This means all of their documentation is in Russian. Despite this, I was able to find that an Android release is expected soon. Its initial release date was February 2018, but has been pushed back to an unknown date (National Research Nuclear University).

This program may be the future of Smartphone security, but its current issue is power consumption. Machine learning programs are computationally expensive. This drains the battery at rates much higher than usual, especially considering the program has to be running while the phone is in standby. Running this program in an everyday setting where users are unable to keep their phones plugged in at all times is unrealistic due to the battery drainage from the program (Eremin). I personally believe that once this issue is addressed properly, InCallAuth will become the main form of Smartphone security. It is near impossible to completely mimic the way a person picks up their phone, making this implementation extremely secure. On top of this, the phone would unlock itself by the time the user looks at it making it more convenient than a pin or password. The increased ease of use will attract both technically savvy users as well as the general public.

The Institute of Cyber Intelligence Systems at the National Research Nuclear University MEPhI's program, InCallAuth, utilizes advanced concepts such as machine learning and artificial neural networks to create a simple yet effective form of Smartphone security. By recording the way the user picks up their phone, InCallAuth can unlock the phone by the time the user has moved their phone to their viewing position. In addition, the program currently holds a 95% success rate and is much more secure than the current pin system that most Smartphones use today (National Research Nuclear University). Its higher security and accessibility could potentially make this program the future of security.

Works Cited

Sullivan, Danny. "How Machine Learning Works, As Explained By Google." *MarTech Today*, 3 May 2017, martechtoday.com/how-machine-learning-works-150366.

Eremin, Alexandr. "InCallAuth." Prezi.com, 11 Nov. 2016, prezi.com/grrtqmczaihj/incallauth.

National Research Nuclear University. “Researchers develop biometric app for smartphone security.” Phys.org - News and Articles on Science and Technology, phys.org/news/2017-03-biometric-app-smartphone.html.

Basheer, I.A., and M. Hajmeer. “Artificial Neural Networks: Fundamentals, Computing, Design, and Application.” *Journal of Microbiological Methods*, pdfs.semanticscholar.org/fc40/ad1238fba787dd8a58a7aed57a8d020a6fdc.pdf.