Password-less Behaviometrics Authentication on Touchscreen Devices

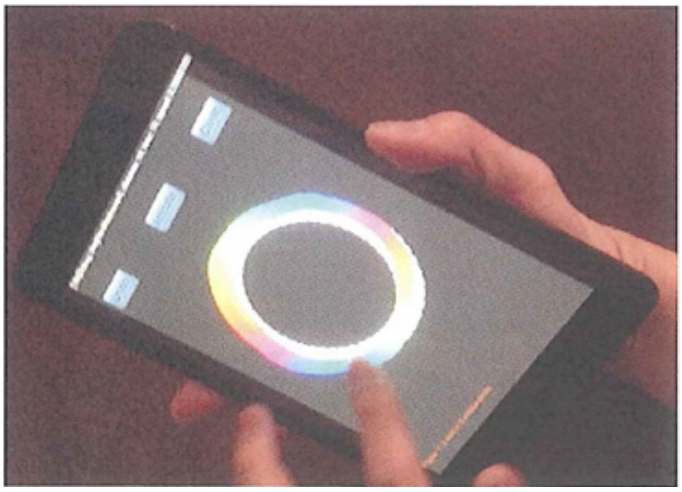
OU ID: #13020

Overview

Researchers at Ohio University have developed a novel, secure, single-factor, behavioral biometric user authentication that is compatible with virtually all touchscreen devices. The technology is based on the precedent fact that no two people move quite the same way. The intent is to create a secure method of user authentication that is convenient and impossible to hack into or falsify. Although human movement patterns are unique to the individual, no two movements are exactly the same. This means that even if you perfectly duplicated a previous movement, the advanced algorithm would recognize it as an attempt to hack. As a result, the technology provides an unparalleled level of security that allows users to safely conduct transactions on any device without fear of their online security being compromised. Prototype versions of the technology have been developed for iOS and Android devices, although it is not limited to these operating systems. Initial internal testing of the authentication algorithm shows proof-of-concept, confirming the algorithm's ability to distinguish between individuals.

Commercial Applications

- Personal Identification on touchscreen devices, both public and private
- Online/mobile banking and Commerce
- Hospitals/Healthcare
- Military Installations



OHIO UNIVERSITY
1804

Password-less Behaviometrics Authentication on Touchscreen Devices

OU ID: #13020

Benefits

- Does not require users to memorize anything, such as passwords, secret questions, or PIN numbers
- Nothing to lose: Current 2-factor authentication uses cell-phones as the 2nd factor, which could be lost or stolen
- Does not require additional, expensive equipment such as fingerprint or vein readers
- Due to natural intra-individual biological variability in human movement patterns, theft of the authentication would be impossible; hacking yields useless data

Inventors

Chang Liu, Ph.D obtained his doctoral degree from the Department of Information & Computer Science at the University of California at Irvine in 2002. In the same year, he joined the faculty of the School of Electrical Engineering and Computer Science at Ohio University. Dr. Liu is the founding director of the VITAL (Virtual Immersive Technologies and Arts for Learning) Lab at Ohio University. Dr. Liu has published over thirty refereed papers and won over twenty grants totaling over five million dollars. He was the recipient of the 2009 Marvin E. and Ann D. White Research Award and the 2007 Advanced Technology Summit Award for Leadership.

Lee Hong, Ph.D. received his doctoral degree in Kinesiology from the Pennsylvania State University in 2007. He has held faculty positions at Louisiana State University and Indiana University Bloomington prior to joining the Biomedical Sciences faculty at Ohio University. Dr. Hong performs research on the patterns of variability inherent in brain function and behavior in humans and animals. He has received over $500,000 in research funding, and has 37 journal papers and 4 handbook chapters.

Contact Us

Ohio University Technology Transfer Office
340 W State Street
Athens, OH 45701
740.593.0976
techinfo@ohio.edu
https://www.facebook.com/OUTechTransfer

OHIO UNIVERSITY

Password-less Behaviometrics Authentication on Touchscreen Devices

OU ID: #13020

Frequently Asked Questions

Why is there a need for this technology?

With data breaches becoming almost daily news, credit card information is being trafficked for fraudulent purchases. Currently there is no way to prevent thousands or even millions of fake credit card transactions from occurring in an instant. Even the online currency Bitcoin has fallen prey to online fraud. Yet, all that is needed to prevent these hacking attacks is another layer of protection to secure online transactions.

What problem does our technology solve?

Our technology provides a safe and secure mode of authentication that does not require an individual to memorize different user names and passwords. Essentially, we seek to replace the password with movement behavior to: 1) remove the need for memorization; and 2) eliminates the hacking problem, both over the shoulder and with brute force computing. The technology that we have developed is the future of user authentication, has the potential to usher in a new era of highly secure e-commerce and cyber security.

Our technology is a natural "liveness" test requiring data input through the touchscreen sensors in order to complete a transaction. This slows down the transaction process, where a hacker must take the time to generate a matching gesture pattern for a single transaction. At the minimum, our invention prevents large-scale credit card attacks from occurring.

How does this technology work? What are the basics of using it?

In the simplest sense, the gesture produced by the user works as a password. The best analogy for the process of using this technology is an ATM card, with the process always starting with the user demonstrating that he/she is who they claim to be when the account is opened at the bank. Just like with an ATM PIN, the user then picks a template (a symbol such as a heart, beta, alpha, etc.) and generates a "reference" movement by tracing the shape of the symbol. This information is then stored so that the next time this person wants to use the card, he/she will be presented with the original symbol and is asked to trace the shape once again. Data generated from this new movement is then compared against the reference movement in order to authenticate the user. Anytime the user wants to make a purchase, a screen with the template pops up and the user produces their natural gesture trace and the transaction is only authorized when the appropriate gesture with matching behaviometrics is generated.

Passwordless Behaviometrics Authentication on Touchscreen Devices

OU ID: #13020

How does the invention distinguish between different people? How will we know if it is the same person?

A critical point of distinction between the movements of individuals lies in its dynamics, that is, how the action unfolds in both space and time. In Figure 1, we provide screen-captures from the table to demonstrate in how differently two individuals perform a movement. Immediately, there are a few visible differences. First, the movement on the right was much slower and took more time to complete. Second, the curvature of the movement on the right is different. An invisible aspect to this difference is that the user on the right initiated the movement at the curved segment, while the user on the left started at the bottom of the "tail."

The algorithm that we have developed and tested uses a multi-point matching system by requiring different movement criteria to be satisfied within a certain threshold, in addition to some of the visibly different characteristics mentioned earlier. This approach accommodates inherent variability from one movement to the next to reduce the number of false negatives while completely preventing false positives. However, our algorithm goes beyond simply matching the coordinates of the movement in time and space. Instead, we have devised a number of innovative approaches of capturing how the movement unfolds in space and time that can be used as criteria for the multi-point matching process.

Figure 1: Screen capture from a tablet of two different individuals tracing the symbol Beta.
For illustration purposes, movement speed is denoted by the space between dots

Can a smart hacker simply shift the data by random amounts and beat the authentication system?

No. Because of our multi-point matching algorithm, the data must maintain its "shape" and the relativity of space and time in human movement. A random adjustment in time that alters its temporal characteristics will disrupt the movement flow in space. Similarly, random shifts in the spatial characteristics of the movement disrupt its flow in time.

OHIO UNIVERSITY
1804

Password-less Behaviometrics Authentication on Touchscreen Devices

OU ID: #13020

Why provide users with a template to trace? Doesn't that make the movement easier to reproduce and copy?

There are many advantages to providing a template. The rationale for this is similar to Microsoft's picture password. Users can effectively select their own template image and trace whatever aspects of the image they choose (as long as the movement generates enough data points for matching), as presented in Figure 3. This increases the uniqueness of each template-gesture matching. However, instead of capturing the pixels positions of each gesture, the goal of our approach is to use the intrinsic dynamics of a user's movements on the multi-touch screen as a unique identifier, this means including movement velocity, and phase.

Figure 3. Screenshot of a user completing a movement trace on a self-selected image. Users will be able to decide which aspects of the image they would like to trace and use this as their "password."

Most importantly, templates provide a universal method of authentication that transcends all cultural boundaries. This technology is especially salient in countries where handwritten signatures are not used, such as Taiwan, China, Korea, and Japan. Images, alphabets, and symbols can easily be replaced by a Kanji, Hanja, or Chinese character.

Figure 4. Screenshot of a user completing a gesture tracing of a Chinese character. Mandarin, Korean, and Japanese literate users will be able to use an actual pass"word."

OHIO UNIVERSITY

Passwordless Behaviometrics Authentication on Touchscreen Devices

OU ID: #13020

Will this approach really work?

Yes, we have already tested the efficacy of our detection algorithm by requiring different people to reproduce the template tracing process with movements separated by minutes, hours, and even days. Figure 2 is a presentation of real data that we have collected and serves as an illustration of how one of the movement variables used as a matching criterion differs between two people. With the blue lines representing the reference movement from one user, the red lines belong to another user's attempts to trace the same symbol. What is immediately apparent is that not only are the red and blue vastly different from one another, the red lines are lay almost perfectly on top of one another.

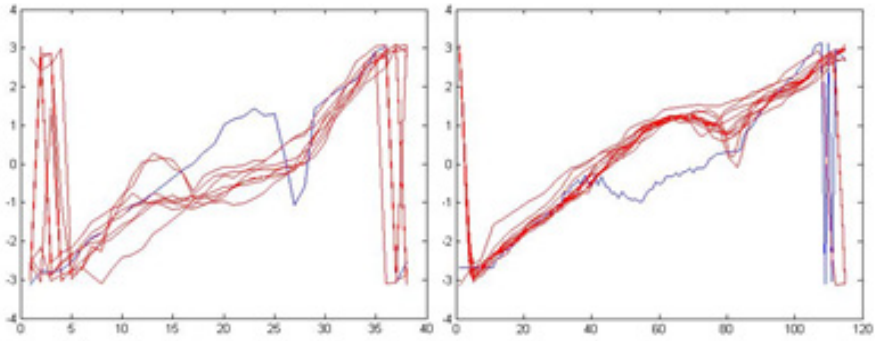


Figure 2: Example of a criterion comparison.

Data taken from repeated trials over many weeks shows a clear difference between two individuals on even just one point of multi-point matching system

What is the rationale behind our solution?

One of the most remarkable aspects of human movement is that it is both stable and variable at the same time. For example, most of us can visually recognize a good friend from a long distance away, simply by the way they walk. While there are some inherently repetitive characteristics that are unique to each individual, just like snowflakes, no two movements performed by the same person are identical. We see this phenomenon all the time in video games or movies. Even with the most modern of technologies, motion capture and human animators are still required to create animation in games and movies as repetitive movements that are identical immediately give the player or viewer the sensation that the action is "bizarre" or "fake."

What then gives a person's movements its characteristic quirks? How we move depends greatly on our body shape and proportions. In the simplest sense, our muscles are springs and limbs are like pendulums, each with its own mechanical resonant properties. The human brain exploits these natural properties of our body to generate movements with an economy of effort. Our invention effectively channels differences in body bio-mechanics into a simple movement on a multi-touch screen.

Password-less Behaviometrics Authentication on Touchscreen Devices

OU ID: #13020

Can this really stop an over-the-shoulder hack?

Yes. While PINs, passwords, and simple gestures can be easily caught by an attentive observer, reproducing movement dynamics are virtually impossible. We prevent the over-the-shoulder hack by insuring that matching the gesture in terms of position coordinates alone is insufficient. Speed and dynamic variability (speeding up and slowing down during the movement) are captured as data for matching as well. This would mean that the observer would have to know when to speed up and slow down during the movement, while also completing the action in a relatively similar amount of time.

Why not just use fingerprint biometrics?

Biometrics, PINs and passwords, all face one simple problem. Data that are a 100% match with target or reference is expected for ideal authentication. Because human movements are never identical (even after millions of repetitions of the same movement); simply feeding in data that match reference movement completely will be rejected. Furthermore, this can be used as a flag to indicate that there has been a breach in the data store.

Fingerprint biometrics also requires specialized sensors that increase cost and size of the device. In addition, to protect the security of the biometric information, the biometrics must be revocable. This means that each device must have a unique, encrypted sensor-fingerprint combination that cannot reverse engineered. Unfortunately, this also means that the data can only be stored securely on the device and cannot be shared with a server for authentication. As a result, it will require a massive overhaul of credit card readers and online service software in order to accept fingerprints as a layer of protection for financial transactions. Our new approach allows the reference identification traces to be stored by an account provider for authorization purposes without any fear of data theft.

Most importantly, our technology can be implemented using current infrastructure without any new equipment and minimal updates to existing software.

What is the value of implementing this technology?

The recent LexisNexis study of identity fraud shows that merchants actually pay $2.79 for every dollar of fraud losses. In 2012, there was $21 billion in fraud losses, which would equate to a true loss of over $58 billion. Even if the deployment of our technology is only able to cut these losses in half, it would amount to a savings of ~$29 billion annually. There are also indirect benefits in terms of reduce time to resolve disputed charges and also increased consumer confidence. As a result, the likely net monetary value is tremendous over the long-term.