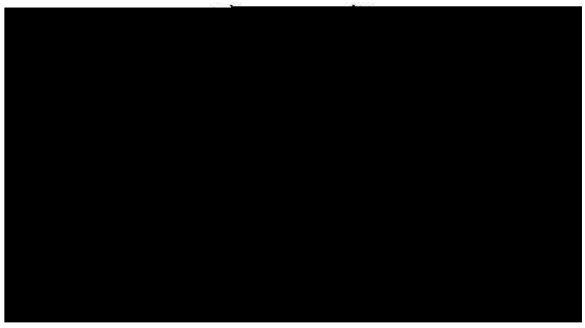
Implementing A Password-less Behaviormetric Authentication

Chris Dunham

CAPS795

Dr. Lonnie Decker

12 July 2023



□ □□□□□□□□

This paper examines the differences between password-based and password-less authentication systems. In the evolving security landscape, there is a need to fix the most common reason supplied for data breaches that is lost or stolen passwords. Addressing the methods and reasons for compromising passwords is exhausting and expensive, and all those efforts eventually fall flat due to one reason…humans are fallible. This research will attempt to show that a password-less behaviormetric based system is a viable alternative to any password-based system, and that they are not only cost-effective but also increase productivity by reducing the amount of time spent on rectifying issues with password-based systems.

□ In□□odu□□on□

For most of my professional career, I have been either working on a helpdesk or engaged in some sort of systems administration role. Until the advent of single sign-on (SSO) technology, I estimate that I spent 80% – 90% of my work hours dealing with forgotten or expired passwords. Now, even though SSO has been widely implemented, I still see roughly 50% of all helpdesk tickets generated for multiple clients are password related issues. The costs for a business to deal with these issues are not insignificant. If you calculate the loss of productivity and the loss of capital involved in paying a user to sit there while the ticket is resolved and the technician to resolve the ticket…it begins to add up. Each single incident might be a miniscule amount of the workday, but after doing some calculations (based on my last two clients for an average) it's telling.

The average time spent on a password related call is fifteen minutes per call. Now, rounded up, that costs the business $5 per call just to pay each technician. This desk gets an average of 1500 password related tickets per month. That is $7500 per month that it costs to have

authentication). These systems mean that you must have one or more methods of authenticating the system before you can access it. While this is much better, it can still be compromised by an attacker that gains access to both authentication methods. This brought me to look at the other two methods of authentication which are “something you are” and “somewhere you are”.

You are unique in the universe. There is not another you anywhere, and you, in your

entire body shape is in front of your computer when you're using it instead of someone else. Many of us already wear a smart watch or something similar like a fitness tracker. This could also be used to track your health statistics and as proximity monitor (which is no worse than current smart card technology). The list of what can be accurately measured increases every day. While any one of these factors can theoretically be spoofed, once you add more than one of them to the mix that chance goes down significantly. If you add, for example, 20 tracked factors…the chance of spoofing all of them simultaneously becomes astronomically impossible. It could still theoretically be done, but there would be no practical method for a human to do so.

Through this research, it became my goal to find a practical solution for using this type of technology in a corporate setting in order to provide a more secure environment and entice widespread adoption by introducing the significant cost savings associated with its

The article from Optimal IdM, [illegible] explores why biometrics are

- B□h□□o□m□□□□□u□h□n□□□□on□M□□hod□□

This article (*M t-;t c d -c* 2007) explores a patent application for a behaviormetric authentication device that uses multiple simultaneous touch patterns to recognize fingerprints. Instead of one single print being scanned you would have multiple input types such as timed tapping, pressure, finger size, finger spacing, and hand spacing (Dunham, 2022).

The initial idea was to save businesses money (and possible security breaches) by eliminating the need for passwords. This article (Long, 2017) explores the amount of time lost by having to type your password by providing the base amount of time used to do calculations in the paper (Dunham, 2022).

- B□h□□o□m□□□□□u□h□n□□□□on□Expl□n□□on□

This paper shows performance metrics for various behaviormetric systems (Sugrim et al., 2019). This is highly important because it shows the failure rate for current systems and where improvements need to be made before this type of system can be implemented (Dunham, 2022).

The book, *t-; t-;n jf M t nf t-;n* is one in a series of books on quantitative human behavior. It explains the statistics behind identifying quantitative individual variables for behaviormetric databases (Dunham, 2022).

- T□□hnology□□dop□on□

An article from eSecurity Planet shows a survey wherein they discover percentages of small businesses and enterprises that utilize MFA (multi-factor authentication). They also survey independent hackers and try to glean what the current easiest way to gain access to privileged information is (Dunham, 2022).

protection. They explore the fields of healthcare, banking, security and authentication, digital security, mobile payments, checkout-free shopping, and multimodal authentication. While not in depth it provides a good starting point for future research.

□ □□□□□□□h□□□□gn□

The primary aim of my research is to eliminate password-based authentication in favor of biometric and behavioral based authentication to drastically improve system security and reduce the amount of time and money that is expended on password-based issues.

To perform this research, I used one year of historical data that reflects the time expended on password-related issues. This allowed me to extrapolate the financial expenditures necessary over the course of a year for the comparison of the expected costs of the new system. I also calculated the expected expenditures on new hardware and software over the estimated population as well as estimated the standby hardware necessary for losses. I also researched the possibility and costs of providing the necessary hardware on demand from an external vendor in order to prevent having to warehouse hardware assets that may not be necessary.

All materials and data were gathered from my current client's databases in order to provide a real-world example of what we currently expend on password-based systems. I utilized ServiceNow reporting tools to gather this information from my client. I also used my business account for Amazon to source pricing for necessary hardware for the new system estimates. In addition, I polled multiple software vendors for the software necessary to make the various hardware systems work together.

I chose this method because a demonstrable financial benefit and increased productivity will demonstrate to businesses that this is a viable and preferred method of authentication. Even

if the financial estimates end up roughly the same

- □□□□□o□d□En□□y□T□m□□

While the time spent on entering your password may seem innocuous, over time it adds up. It has been estimated that we spend roughly 36 minutes per month typing passwords. Even if you are using biometrics to bypass typing, you would still spend roughly the same amount of time due to misreads and having to do multiple attempts at scanning. Based on the numbers from the first section, that adds up to 244,800 hours for a company that has 34,000 personnel using a computer. For my supported clients alone (3000 personnel…mostly sales), that totals approximately $522,288/year that must be spent for the time we pay people to just login to their machines.

- □o□□□n□□□□nu□□

The true loss of revenue is incalculable for this cli

- Com□n□d□o□l□

The combined expenditure totals come out to just under $22 million dollars. While some of this total is speculative due to not being able to determine actual sales losses, the potential for cost savings is enormous.

- B□h□□o□m□□□□Co□□□

The costs associated with implementation of a behaviormetric system will vary depending on the number of factors that are tracked. For this research I chose five factors: facial recognition, fingerprint scanning, typing cadence, mouse behavior, and retinal scanning. Facial recognition scanning and fingerprint scanning are already built into the latest Windows based machines in the form of Windows Hello. Most laptops used by my client have fingerprint scanners built into the machine, but there are a handful of desktop devices that do not (approximately 1500). These will require fingerprint scanners and cameras in order to utilize the sof.479431(s)-9(n)-0.956dl

With the current headcount this would cost $408,000 annually. For retinal scanning I went with eyeLock. The retinal scanning hardware can be had for $220/unit which is a cost of $7.5 million. While this is a substantial investment for retinal

□ Con□lu□□on□

In conclusion, I believe this research shows that the implementation of a behaviormetric authentication system would be demonstrably better than utilizing the current method which becomes more of a security liability daily. It has already been proven that biometric authentication in conjunction with passwords is better than passwords alone, and removing the

□ □□□□□n□□□

A . PayScale. (2023). https://www.payscale.com/research/US/Job=Insurance_Salesman/Salary

. Mouseflow. (2023, June 20). https://mouseflow.com/

BMS. (2022). . The Behaviormetric Society. http://bms.gr.jp/en/about/shuisho/

Boeckelman, C. (2021, September 22). . GetFeedback. https://www.getfeedback.com/resources/online-surveys/distribute-online-surveys-get-quality-responses/

Dunham, C. (2022). . [Unpublished manuscript].

. eyeLock. (2022, October 27). https://www.eyelock.com/

Fries, J. (2020, August 19).

Kimura, K. (2023, April 29). [illegible] c [illegible] c c t . SpringerLink. https://link.springer.com/book/9789811307300

Long, T. (2017, November 1). [illegible] t nt ty [illegible] t n y [illegible]