Implementing A Password-less Behaviormetric Authentication

Chris Dunham

CAPS795

Dr. Lonnie Decker

12 July 2023

Table of Contents

❖ Abstract

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.

❖ Introduction

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

passwords reset…and that is not accounting for anything except wages paid to my employees. There is also the loss of productivity/wages from inactive users. Now, this will vary widely, but we have everything from newly hired salespeople to c-suite users. Fifteen minutes of that salesperson's day could have cost the company a million-dollar deal. Fifteen minutes of the c-suite user's time could also cost a significant amount. The other inherent problem with passwords is that they are more likely to cause security breaches than any other user activity. The loss from a data breach could be incalculable. These considerations and numbers show that a solution to this issue should be a welcome one at the very least.

Now, of course, pricing schemes that have been presented to the client already reflect this, but the real cost savings are not based on the $5 dollars that I must pay someone to work the ticket. The real cost savings are in the fact that I do not have to hire as many people when the volume is reduced by half, and I can offer those savings to my clients if we no longer have to deal with password issues. If your IT department is internal, it is a fantastic way to show value added from what is traditionally a cost center for almost every enterprise.

The purpose of my research has been to find a way to eliminate password-based authentication strategies all-together. If the number one cause of security breaches can be fixed with minimal effort, why would you not implement that system instead of your current vulnerable one? Of course, we cannot just get rid of the need to authenticate, but there are multiple methods of authentication. The most traditional, which are password-based systems, are based on the idea of "something you know". It is the idea that you have a secret that only you know to access a secure system. This premise is inherently flawed because there are multiple ways for others to gain access to that secret. We have supplemented "something you know" with "something you have" such as the various methods of implementing MFA (multi-factor

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 entirety, cannot be spoofed. For a password-less system to work, we must explore ways to authenticate using a truly unique method…yourself. To that end biometric technology has been developed, but unfortunately the primary biometric authentication methods such as fingerprints, retinal scans, and facial recognition can all be spoofed. It is difficult, but it can be done…which only means it will get easier as time and technology progress. Something better is necessary to truly secure a system, and that is where my research led me. While biometric scanners may be able to be fooled, you can only do so many at once. I began to ask myself, what if instead of just one or two biometric signatures we used four…and then instead of using four how about we use eight? I discovered that research into systems just like this has been started and the technology required is also becoming available. Biometric access is part of it, but there is also software that can record your typing cadence. It does not record individual keystrokes, so there is no security issue there, but it can get used to how you type and lock your computer if it is radically different. Other software can track other behavioral traits you might have such as, do you typically use the mouse wheel to scroll, or do you click on the arrows, or possibly you grab the scroll bar and scrub through. It can also track your mouse hand movements to see how much you move your mouse when you do move it. Weight sensors can be added to your chair to measure your weight and shut down access if there is a weight fluctuation that suggests you are not the one sitting in your chair. Cameras can be used to not only provide facial recognition, but also to show that 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 implementation.

❖ Literature review

It is important to gather knowledge about the topic of behaviormetrics in order to learn what can be implemented at this time and what would need further research. Therefore, I am conducting a literature review on information I have gathered (Dunham, 2022).

• Biometric Authentication Methods

Much research on biometric authentication methods has been expounded on, and it is becoming commonplace in many enterprise environments to integrate this technology. What needs to be researched here is how to integrate this technology into the "living" mesh that is behaviormetrics (Dunham, 2022).

The article from Optimal IdM, *Behavioral Biometrics explained,* explores why biometrics are important for behaviormetrics to work. There are three types of identification methods. Knowing something such as a password or PIN, having something such as a common access card (CAC) often referred to as a smart card, or being something like yourself with your own unique fingerprints. Physical characteristics are essential to both biometric and behaviormetric authentication (Dunham, 2022).

The next article (*How is behavioral biometrics used for authentication?* 2022) explores how biometric factors are used to track patterns which is the core of behaviormetrics. This is necessary to know how certain biometric tracking will be integrated into the whole (Dunham, 2022).

In an article about a specific camera used for biometrics (O'Brien, 2021), it is discussed how the Air Force is developing a camera for biometric recognition that doesn't just look at facial features and try to match them, but also maps muscle movements that are unique to that individual by measuring it not only with visual references but with things like infrared spectrum as well (Dunham, 2022).

Another article (*What is biometric authentication? use cases, Pros & Cons* 2022) discusses what biometric authentication is and more importantly why it is important going forward due to the lack of secrecy needed. It also discusses use cases for biometric security and asks what the downside to using biometrics is as well (Dunham, 2022).

In a NIST special publication (Padgette et al., 2017), they detail security measures to take when using Bluetooth devices. This is especially important with more MFA schemes using mobile devices or Bluetooth attached devices (such as keyboards) where Bluetooth security could be a risk factor.

- ## Behaviormetric Authentication Methods

This article (*Multi-touch device* 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).

- ## Behaviormetric Authentication Explanation

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, *Estimation of Mutual Information* 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).

- ## Technology Adoption

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).

The BMS prospectus discussed the Behaviormetric Society as a whole and their goals of continuing research into behaviormetrics at the quantitative level and promoting research with multiple different disciplines involved (Dunham, 2022).

The password-less strategy from Microsoft (Matarazzo, 2022) covers the methodology and process of implementing or changing over to a password-less system. It covers the multiple stages needed to successfully deploy this authentication method (Dunham, 2022).

- ## Hindrances to Adoption

In an article by Jonathan Fries, he explains why behavioral metrics should be used to promote your team to succeed. While this has nothing to do with behaviormetrics per se, I believe it shows how a system like behaviormetrics must be introduced in a positive manner or it will be rejected by the users in the same manner they reject other behavioral tracking introduced by their companies or supervisors (Dunham, 2022).

In *Exploring Social Processes* (Kimura, 2023), the author explores sociological attitudes and beliefs. This is another book in the series about quantitative approaches to behaviormetrics related to human behavior. It shows statistical methods to explore interpersonal relationships and attitudes based on factors such as social status, gender, and age (Dunham, 2022).

In an article by Jeff Goldman, he details multiple reasons why MFA is not used by most small to mid-sized organizations. The article also makes a point of showing why relying on password policies only is one of, if not the, largest known weakness in corporate security and, by proxy, small to mid-size business security as well.

- ## Future Considerations

In *The future of biometric technology – what's next?* (Veriff, 2022), the author touches on multiple ways that biometric technology could be used to increase security, convenience, and

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.

❖ Research Design

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 for both platforms, I believe it will still show that this is the preferred method due to the added security value.

❖ Research Findings

For the current password-based technology information I gathered data from the client's ticketing software (ServiceNow). This data includes self-service, phone, and email-based tickets for a total of 50001 for the fiscal year (March 2022 – March 2023). I then filtered all the services that do not use the current single sign-on (SSO) solution in place as these would not benefit from the proposed authentication system. This resulted in a total of 41687 tickets that could benefit from a behaviormetric/biometric solution. This number of tickets is a mix of supported services and includes account locks as well as password resets. This activity averages 10.38 minutes per interaction (which includes calls and emails) for a total of 7211.85 hours. The average pay rate for a technician is $18.50/hour for a total of $133,419.24/year spent helpdesk personnel for assistance with password tickets. As I did not have individual pay rates for the users, I extrapolated an estimate of their hourly rate based on information provided by payscale.com The most common associates we interact with are insurance salespeople who make an average salary of $34,706/year plus average commissions of $13,500/year for a total of $48,206. Converting this to an hourly wage showed a result of $23.18/hour, which adds up to $167,170.71/year. The total between both users and technicians was $300,589.95/year. This combined figure is the first step in calculating how much time passwords cost every year. Other factors that must be considered are time spent entering passwords, possible loss in revenue due to the sales agents being on the phone with the help desk, and the cost of the contract.

- ### Password Entry Time

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.

- ### Loss in Revenue

The true loss of revenue is incalculable for this client without being given specific financial information, however, I can estimate based on the average time for calls. If the agent is off the phones for 10 minutes on average, that is one potential inbound call missed by that sales agent. The current average health plan across all types in the US was just under $500. $500 per call in potential lost revenue could cost them up to $21 million dollars over the course of a year.

- ### Contract Costs

Based on provided proprietary data on the contract, I found that the contract was negotiated for roughly $3 million for the base cost per year. This includes 2000 password tickets per month in the price of the contract with a $15 charge per ticket for every ticket over that number. With an average of 3474 password tickets per month, that total is approximately $265,320/year over the contract costs.

- Combined totals

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.

- Behaviormetric Costs

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 software. Prices for hardware were obtained from amazon.com as that is our current purchasing order method. Preferred fingerprint scanners are $26.75/unit and webcams for facial recognition are $29.99/unit. This is an estimated cost of $40,125 for fingerprint scanners and $44,985 for webcams for a total of $85,110. For typing cadence software, I chose TypingDNA. Based on their pro level pricing, this provides 50 authentications per user per month for $1. While this solution is similar to typing in your password, it is a randomized string of words, and cannot be compromised in the way a password can. Their authentication method has a less than .1% chance of false authorization currently and is being actively improved. It also allows API integration into software that requires authentication without having to wait on a mobile MFA solution (e.g., Okta Verify, Duo, Microsoft Authenticator, etc.) to prove authentication. Users should only have to authenticate once per day with this factor, so the 50 authentications per month should be more than enough.

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 scanning, this hardware has an additional benefit of not being able to be spoofed by non-living materials. The software also integrates with SSO solutions and Active Directory, so there is no added cost for keeping an additional database or the associated hardware/software/maintenance costs. Finally for mouse usage tracking I went with Mouseflow. This software can be used to track user behavior and send alerts when the use pattern is significantly different than usual. If the alert triggers it can then prompt the user for additional authentication. They only post pricing for standard usage and not enterprise, but for illustrative purposes, I used their "pro" pricing level which allows 150,000 recordings per month over an unlimited userbase with the intention of recording individual usage at least once per week to allow for pattern alterations over time as well as pattern re-learning due to possibility of the loss of use of a hand for a period. The pricing for this tier is $399/month for a total of $4788/year. This comes to a grand total of $7,997,898.

- ## Cost Comparison Analysis

The cost difference between these two methods is significant at approximately $14 million. It is even more significant when you understand that is only for the first year. The current authentication method price is annual. There will be small cost derivations from year to year based on call volumes and personnel changes, but the price is almost fixed. The $8 million price tag for behaviormetric implementation is a one-time cost with the exception of software licensing, which would decrease the following year to less than $40,000 annually plus an estimated 10% of current annual expenditures ($2.2 million) due to the estimated reduction in tickets.

❖ Conclusion

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 most common cause for security breaches from this equation would make vastly more effective. The cost analysis also shows that while there is a significant upfront investment, there are significant savings to be made year over year. While there is further research to do for other factors such as futureproofing and user satisfaction, I do believe that authentication has to move in this direction regardless of the findings. Sticking with the current password-based methodology is simply inviting further security breaches and the loss of data and revenue.

❖ Areas of Future Research

As I mentioned in the conclusion, one of the areas of future research I determined is that of user satisfaction. Anecdotally, users are prone to not utilizing a system correctly if they are frustrated by using it. Making sure that the system is unobtrusive is paramount to user acceptance. I do not believe, however, that getting user opinion before the system is implemented would necessarily be useful. I think users would have to use the technology firsthand to have an informed opinion and not be biased by what they've read or seen in media or from sensationalized accounts. Further future research would also need to explore the longevity of the hardware and software solutions suggested. Most of this equipment has not been around for very long, and a proper test run would give more valuable as to this method's effectiveness. Along those lines, future research would also need to consider the rapidly evolving methods for

different biometric and behaviormetric detection and whether or not one or more of those options would be a more secure option.

❖ References

Average insurance salesman salary. PayScale. (2023). https://www.payscale.com/research/US/Job=Insurance_Salesman/Salary

Behavior analytics for optimal website ux. Mouseflow. (2023, June 20). https://mouseflow.com/

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

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

Dunham, C. (2022). *Literature Review*. [Unpublished manuscript].

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

Fries, J. (2020, August 19). *How positive behavioral metrics can boost software teams - dzone devops*. dzone.com. https://dzone.com/articles/how-positive-behavioral-metrics-can-boost-software

Goldman, J. (2017, August 16). *Most small to mid-sized organizations don't use multi-factor authentication*. eSecurityPlanet. https://www.esecurityplanet.com/networks/most-small-to-mid-sized-organizations-dont-use-multi-factor-authentication/#:~:text=While%20only%2038%20percent%20of%20large%20organizations%20don%E2%80%99t,recent%20KnowBe4%20survey%20of%202%2C600%20IT%20professionals%20found.

How much revenue are missed phone calls costing your practice?. Healthcare Marketing Agency. (2017, June 16). https://www.practicebuilders.com/blog/how-much-revenue-are-missed-phone-calls-costing-your-practice/

Hunt, J. (2022, May 4). *What is the average health insurance premium?*. The Balance. https://www.thebalancemoney.com/what-is-the-average-health-insurance-premium-4586358

Incognia. (2022, April 27). *How is behavioral biometrics used for authentication?*. Incognia. https://www.incognia.com/the-authentication-reference/how-is-behavioral-biometrics-used-for-authentication

Justia. (2007, September 17). *Multi-touch device behaviormetric user authentication and dynamic usability system*. Justia. https://patents.justia.com/patent/20080092245

Kimura, K. (2023, April 29). *Exploring social processes (excerpt)*. SpringerLink. https://link.springer.com/book/9789811307300

Long, T. (2017, November 1). *We spend 36 minutes a month typing the nearly 200 passwords we all have!*. EFTM. https://eftm.com/2017/11/we-spend-36-minutes-a-month-typing-the-nearly-200-passwords-we-all-have-44652#:~:text=Well%2091%25%20of%20us%20know%20it%E2%80%99s%20risky%20reusing,and%20in%202016%20alone%204.2%20passwords%20were%20stolen.

Matarazzo, P., Czechowski, A., Sherer, T., Schonni, N., & Halfin, D. (2022, November 23). *Password-less strategy*. Microsoft Learn. https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/passwordless-strategy

OneSpan. (2022). *What is biometric authentication? use cases, Pros & Cons*. OneSpan. https://www.onespan.com/topics/biometric-authentication

Optimal IdM. (2020, November 17). *Behavioral Biometrics explained*. Optimal IdM. https://optimalidm.com/resources/blog/behavioral-biometrics-explained/

O'Brien, T. (2021, May 13). *Creepy new Air Force camera can identify and track you from far, Far away*. Engadget. https://www.engadget.com/2011-05-20-creepy-new-air-force-camera-can-identify-and-track-you-from-far.html

Padgette, J., Bahr, J., Batra, M., Holtmann, M., Smithbey, R., Chen, L., & Scarfone, K. (2017, May). NIST Special Publication 800-121, Revision 2: Guide to Bluetooth Security. NIST.

Recognize people by the way they type. Continuous Endpoint Authentication + Smart 2FA " TypingDNA. (2023). https://www.typingdna.com/

Sugrim, S., Liu, C., McLean, M., & Lindqvist, J. (2019, February 27). *Robust performance metrics for authentication systems*. jannelindqvist.com. http://jannelindqvist.com/publications/NDSS19-robustmetrics.pdf

Suzuki, J. (2019). *Estimation of mutual information*. SPRINGER Verlag, SINGAPOR.

Veriff. (2022, March 14). *The future of biometric technology - what's next?* Veriff. https://www.veriff.com/blog/the-future-of-biometric-technology