Entrepreneurship Research Paper

Christopher Wheeler

Old Dominion University

Entrepreneurship in Cybersecurity (CYSE 494)

Brian K. Payne, PhD

June 20, 2022

How many times has an individual created an account on a website or accessed an existing account using their login credentials only to receive a login error to something along the lines of, "*user account credentials could not be verified*"? They then click the "forgot password" link and go through the verification process to recreate a password. They click refresh and go to the login page and again are greeted with, *"user account credentials could not be verified"*. They try again, *"user account credentials could not be verified"*. They painstakingly continue this cycle and finally receive the message, *"user account has been locked, please contact customer service"*.

There is no doubt that passwords are necessary for personal accounts and computer security. Password security practices are taught to meet a certain criterion, be frequently changed, and never written down. With this sort of password complexity, it creates safer websites and makes it extremely difficult for someone other than the user to access their account and personal information. While making access difficult for a potential hacker, simultaneously the user may experience the same difficulty in an attempt to access their own information.

It is inevitable that individuals will forget their password, write them somewhere where others can have access to, or lock themselves out due to too many attempts for what they believe to be the correct password. To make this process easier which in turn leads to an account being less secure, an individual will use simpler passwords or continue to use the same password with minimal changes every time that password dialog box pops up stating their password is to expire in 14 days.

This vicious cycle is ever occurring, causes frustration for the user, and a weakened security for their account and entity they are trying to access. Not only these few instances, but there is also a loss of time for an employer when their employee is not working, or a system is

down because of a login issue. This costs time and money and with the saying in business, "*time is money".*

While there are many solutions to this password complexity and access problem, which some are already in use and on the market, my solution is to bring existing technology and protocols into one source of software and hardware for individual and or business use. I would bring into the solution public key encryption to aid passwords being secure and not having to remember or write down multiple lengthy passwords for various accounts. I would include biometrics such as iris scanning, fingerprint validation along with voice recognition.

Another facet of technology to contribute to the multi-factor validation would include a tangible security token. The combination of these security factors would follow a cybersecurity password framework of *something you have, something you know, and something you are*, all of which would lead to minimizing the need to memorize lengthy passwords or run the risk of the passwords falling into the wrong hands.

In the Deep Dive article titled, *5 password management trends businesses need to know*, the authors describe this very problem with passwords and password protection that when the time comes to update a password, short cuts will be used, and an annoyance will ensue. "Frustrated over the process, many are quick to settle on an easy-to-remember password, prioritizing convenience over security." (Edie, Hickey, and Schwartz, 2018). The authors reinforce that there is a problem by stating that, "…individual password management and security behaviors are, more often than not, insufficient and lagging." (Edie, Hickey, and Schwartz, 2018).

There are advances in technology that could ease the burden of password security. Instead on just a user entering their password and being granted access into a website or an account, multi-factor authentication (MFA) can be implemented. This multi-factor authentication can come in the form of a text code that is sent to the user's phone, a preset access pin-number, and or a geographic authentication. In the event a hacker did crack or come into procession of a user's password, they still would be unable to gain access without the implemented multi-factor authentication. (Edie, Hickey, and Schwartz, 2018).

Technology is advancing everyday with just about everything being connected to the internet or the capability to be connected to the internet. "The more services are offered to the general public – with additional features for convenience and usability that rely on the internet – the wider the window of opportunity for attackers." (Kessem, 2018). With technology advancing so is crime. Criminals are now looking to personal data such as social security numbers and financial information which has a higher street value than someone's wallet with maybe a small amount of physical cash in it. "Recent data breaches have been a resounding wake-up call to the fact that new methods are needed to validate our identities online." (Kessem, 2018).

The typical username and password authentication are not able to secure accounts from hackers like they did when the internet and computers were first beginning introduced and evolved into our world as we know it. IBM security reinforces new security implementation and of what my product and others will bring to the market in the future:

> Evolution in authentication schemes that move away from passwords has thus been a natural and necessary progression to help secure both individual identities and the organizations providing consumers with services. In an effort to replace traditional passwords, biometric authentication options – such as fingerprint or facial recognition, keystroke dynamics and voice recognition – are becoming more widespread and are seeing increasing popularity amongst the general population. The use of fingerprints to access the latest smart devices is now pervasive, and newer identification models, like facial recognition, quickly rose to the forefront in 2017. (Kessem, 2018).

To fully address societies problem at hand, entrepreneurs and developers must first dissect the issue from all angles and use different thought processes. The entrepreneurs and developers then need to proceed with the wants and needs of the business and customers they seek to sell their product to. Research into the latter found what users want from their password credentials. That is, something short, making it easy for the end user to remember, be able to use on many different accounts or systems, and then a minimal requirement to change their password. (Choong, Theofanos, and Liu, 2014).

Although, a nice concept on paper, this sort of request is truly not feasible in the sense of keeping networks or accounts secure. On the other hand, passwords cannot be so restrictive that they are not able to be recalled easily and need to be reset constantly. One study conducted in regard to passwords resetting and generating new ones every quarter (three months) resulted in an employee spending 12.4 hours a year on this security feature. (Choong, Theofanos, and Liu, 2014). 12.4 hours per year spent on password issues seem far-fetched but thinking about large companies with minimal IT support leads me to think this data to be plausible thinking about the amount of time I have waited on hold or dealt with password issues.

Furthering this research and adding context to the issue revealed that typical login issues to include password errors could be minimized with better and frequent cybersecurity training. Employees were more understanding when they were briefed on the reasoning behind password

complexity and the data breaches that have stemmed from cyber-attacks. With this data and information brought beforehand and frequently, places a greater importance on password protection and complexity. Typically, humans are curious creatures and desire to know the *who, what, why, and where?* It is easier to get workers on board if they know the justification and reasoning behind a practice or policy.

So, what does an entrepreneur, computer engineer, and developer due next to curb this password issue making them password(less)? One may think that with the information presented the logical thing to do would be implement facial, voice, and fingerprint recognition across all networks and devices. This would be astronomically difficult and expensive if crammed into a short period of time. With this thought process of moving to the other end of the spectrum of relying on account verification to come from an individual's DNA has spurred many to research and hypothesize, *how safe is our DNA really?*

Back to looking at the issue and problem set from all angles, think about the DNA and Genealogy companies that take a swab of an individual's saliva, run it through a DNA algorithm, and print out interesting facts. These facts are quite interesting if I may say so myself. They can trace our DNA to a country or countries or origin along with possible long-lost relatives. Now think about all that data. One's DNA is thought to be relatively safe and secure, but now there is a complete database with an individual's complete molecular makeup. Sounding doomsday pepperish, this is how these developers must think. (Rizkallah, 2018).

Voicemails, pictures, door handles, and even hair can leave traces of an individual's identity that can be repurposed to infiltrate accounts causing a cataclysmic data breach. I love technology but even reading these articles forces one to play devil's advocate and think scientifically or the worst-case scenario. This then pushes us towards the middle of the

cybersecurity spectrum. Password and identify protection need to have the best of both words. Passwords, biometrics, and tangible security tokens or cards to complete the multi-factor authentication computer networks need to continue to be secured properly.

To continue with the analogy of looking at the problem at hand from all angles, another angle to consider is privacy of personal identifiable information (PII). One can imagine that the majority of people wish their personal identifiable information would remain private and on a need to know basis. This could be medical or financial information with the people needing to know are their doctors or medical providers and their financial institutions where their accounts are held. The complexity is changed with a third party being involved with password protection or how an individual's DNA is stored or verified for account access. This is an additional aspect of concern to be addressed and added to the list of customer wants and needs.

To start on the path to the solution of safeguarding personal identifiable information and password protection one can begin looking into the process of cryptography. Cryptography has been around for an extremely long length of time. The type of cryptography is what has changed throughout the years, but the main concept has stayed the same. "Cryptography is the art, science, practice, and study of securing communications. At its essence, cryptography is used to keep messages and data away from anyone who may be snooping, but it can also be applied in many other ways." (Anon, n.d.). My product will use cryptography in the form of encryption with *public-key cryptography*. While the exact implementation into the product is still being tested, public-key cryptography only allows the recipient of the 'code' (password) the key to unlock the 'message' which would verify the user granting them access to their accounts.

Password and password protection is not limited to the computer world of cyber security but effects the majority of aspects individuals interact with on a daily basis. This also includes

my personal life and academia of reaching classes and other disciplines outside my major of cybersecurity. I cannot think of a class outside of cybersecurity where I did not need some sort of login credentials for the class. I either needed to login to the school's website and or another website to access the books and homework assignments.

Another aspect relating to the problem I am developing a product for is related to science classes. The professors teach a scientific method of coming up with a solution to a problem. No matter how big or small the problem is, the process remains the same. One does some research or a particular issue, develops a hypothesis, conducts experiments, records the results of the experiment, and then reflects on the process of what worked and what did not. At the conclusion of the analysis the process is typically started over whether the experiment was a success or not in an attempt to better the product and ensure it cannot fail.

English courses and even strength training/physical fitness followed a similar process. Writing an essay or report started with a subject (problem) and end goal in mind (solution). Brainstorming was conducted to generate ideas and get the brain working. A rough draft was written with the main components and ideas listed out. The rough draft was revised and revised adding more and more detail until a final product emerged. With the physical aspect a problem or goal was thought of. Wanting to be stronger, more flexible, or just overall in better health and physical shape. A solution was developed either as a single component or a combination. This included a diet plan and a strength/flexible program.

With these instances mentioned although not directly related to the cybersecurity curriculum or computer world, the problems and how one gets to the solution through a process can be directly related to different curriculums.

Whether my innovations are effective or not can be interpreted in a few different ways. I would consider being effective in the process of developing a solution to the problem I have identified. I mapped out the process I would follow and go down the path I have identified. Using a sports analogy would be putting myself in the game and not just sitting on the sidelines watching. Whether the product be a success or not I would still consider myself being effective in the attempt to bring my visualization to life from a personal point of view.

Being effective would be having the product work and bring ease of use for an individual and or business. There would be actual value brought to fortition where the end goal was achieved. I did my homework and due diligence, secured funding and partners, and then found an actual buyer for the product. All parties involved would be happy and satisfied with the result which would signify being effective. Finally in terms of being effective from a business standpoint. Profits and growth are realized. This product continues to work as advertised with minimal interruptions, it is updated and fixed as problems arise, and continues to bring in revenue. One or a combination of these three instances being achieved, I could easily say I was effective in my undertaking.

Following the research, hypothesize, experiment, and analyze process is what I will need to continue to do to turn my innovation into a reality. I have just barely scratched the surface of the problem I am attempting to solve. Yes, it has affected me and been bothersome. Yes, I have read a few articles that depict the problem along with seeing some of my peers be affected with this issue as well. Yet, I still need to do more research into the problem and see if it is truly an issue so great that is worth a vast amount of time, energy, and money being put into to develop a viable solution.

Next, I need to put more attention and devote time to hypothesize the problem I am attempting to develop a solution for. Scientifically put if I create ‘X’ what will ‘Y’ be? I need to seek out assistance from my peers and others to help see the issue from all angles. I need to see how others view the problem and what possible solutions they may have. Experimentation is to try and try and really put my product to the test of use. The product then needs to be rolled out for different individuals to use and see if it is worthwhile. If the product is worthwhile, would these same individuals pay for it?

Finally, I would need to analyze my product and process. I would really scrutinize every aspect in an attempt to find weaknesses or poke holes in the product. I feel this would be the final stage before it available to be released to the public market. Throughout this process I was seeking out professional from all disciplines. Computer Engineers, financial/business consultants, and marketing professionals. I would need to assemble a team that would enable to bring this idea into reality.

With my product tried and tested, my team fully assembled and on board, the next steps would be to secure funding. Thinking ahead, my team and I devoted our own funds into the company to develop a product. Now to further promote this product and be successful a higher level of funding and investment is going to be needed to make this successful. This money would be used to mass produce the product and implement into other existing products to include software, hardware, and firmware we deemed necessary.

In summary of this entrepreneurial project was to find a problem that plagues one’s everyday life or something that is an issue someone has observed. The project instills the entrepreneurial mindset of opportunity is all around, one just needs to know where to look and what to look for. This project was just that. A different way of thinking and understanding that

great products or services are just developed quickly and that overnight success we might think they are. We do not see the behind the scenes and everything that has gone into the development of that product or service.

For my project I observed a problem that I have encountered very frequently. The problem was with passwords. I have a lot of different accounts and websites I use that require a username and password. Seems like every other time I have unable to enter the correct password and have to reset it just to find the reset password is not working after I just created it. This is the problem I set to solve. I will solve this problem by creating software and hardware that can be implemented across any network and component. This will forever ease the burden or less the need for password memorization and possible account hacks to someone finding or figuring out your password. The solution with come in the form of multi-authentication factorization. Make sure you keep your mind and eyes peeled for the next time your login process is simpler than ever.

Overall, I learned that the entrepreneurial process is not being in the right place at the right time or being dealt an instant success opportunity. The process is just that, a process to follow. It is up to the individual of how they follow the process and that they are the true creator of their own destiny. From the outside in it seems like a lot of hard work but will pay off in the long run. Details that others might find value in is that one needs to be organized in their details and thought organization. Be able to focus on different aspects of the project and really dissect each one and get fully involved. Since I do not have any entrepreneurial background and this is the first class of this kind, I find it hard to think of what I would change or doing differently. I am not sure if this class is offered as a regular semester class which would be able to offer a greater context and expound upon more but being a six-week course, I do not think I would

change anything if the director were to seek me out as a future consultant or the class nor do I think I will follow through with this product development to be a success case for the course. As the saying goes, *knowledge is power*, I truly think whether someone wants to become an entrepreneur or not this course gives a great overview if someone changes their mind, they have a good foundation to start on.

References

1. Anon, D. (n.d.). *An Introduction to Cryptography.*
2. Brooks, S., Garcia, M., Lefkovitz, N., & Nadeau, E. (2017) *An Introduction to Privacy Engineering and Risk Management in Federal Systems – NIST.* Retrieved May 19, 2022, from An Introduction to Privacy Engineering and Risk Management in Federal Systems (nist.gov).
3. Choong, Y., Liu, H., Theofanos, M. (2014). *United States Federal Employees' Password Management Behaviors – a Department of Commerce Case Study – NIST.* Retrieved June 16, 2022, from https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7991.pdf.
4. Eide, N., Hickey, A., Schwartz, S.A., (2018). *5 password management trends businesses need to know*. CIO Dive – Deep Dive.
5. *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1). (2018). NIST.
6. Kessem, L., (2018). *IBM Security: Future of Identity Study*. IBM Security.
7. Rizkallah, J. *Hacking Humans: Protecting Our DNA from Cybercriminals.* (2018).
8. *Understanding Cybersecurity & Privacy Best Practices.* (2018).