Paper 2 Summary

[Rui Zhao](https://unomaha.instructure.com/courses/43633/users/40845)

All Sections

11 unread reply.2424 replies.

Search entries or author Filter replies by unreadUnread     Collapse replies Expand replies

[Subscribe](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

[Collapse Subdiscussion](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)[Chris Schmitt](https://unomaha.instructure.com/courses/43633/users/36306)

[**Chris Schmitt**](https://unomaha.instructure.com/courses/43633/users/36306)

Mar 20, 2021Mar 20 at 11:31am

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

Chris Schmitt

CSCI 8410

Paper Summary 2

Well, a little over 10 years later and we are still using passwords as a means of authentication for most online applications. The article highlighted many of the problems that password authentication has when it comes to the standard non-IT user. Passwords are and will be one of the main and easiest means of authentication. The article discussed seven different “barriers” that stand in the way of moving from the traditional alphanumeric password and onto a more secure authentication method. One of the main barriers, in my opinion, was user reluctance and usability. This barrier still plagues us today because most users want a simple easy to use application and do not think twice about authentication unless it is currently trending in the news due to a data breach. Despite the hundreds of data breaches that have occurred in the last 10 years (several of which could have been prevented if the user enabled Multi-factor-authentication) users would still opt for easily guessable passwords or recycle them from other sites. Even companies that offer multi-factor as a secondary “secure” login method, the average user will ignore the warning and continue without it. We saw this recently with the Ring Security Alarm system. Users were having their accounts compromised due to bad or recycled passwords despite Ring offering multi-factor authentication (which would have prevented this issue). This alone shows that users will ignore whatever security features are offered unless they are required. After the security issue, Ring began forcing its user-base to enable multi-factor authentication. More companies are starting to offer similar authentication methods and most banking/financial applications already implement a form of multi-factor. Applications could require users to have 32-character random passwords but that would still not fix the issue of users recycling their passwords across multiple accounts and as mentioned in the article, users will either forget it or litter their desk with post-it notes. Also, if a company makes their login process too cumbersome for the average user, they could easily switch to another company that offers a similar process with an easier-to-use application and logon process.

                Today, however, with nearly everyone being connected via smartphones or similar technology, companies are starting to require users to have multi-factor authentication, whether that be a physical token (Yubi-key, smart card), SMS or Voice message, or a push notification, alongside their password. Companies like LastPass and BitWarden offer “password vaults” that require the users to set up a single “Master Password” to log into the application and access lists of randomly generated passwords for their accounts. Google created an authenticator app that can be used to authenticate to other websites that decide to implement multi-factor which can take the burden off the company by giving their users the ability to login via a password and Google authenticator code.

                Passwords and authentication will always be an issue for the foreseeable future, at least the next 10-15 years. We live in a time where most of the older people did not grow up with technology and are still struggling with it. My parents are a good example, I talk to them about password managers or multi-factor authentication, but they will still default to easy-to-use login methods. Once the generation that grew up on technology becomes the older generation, I feel we would finally be able to do away with passwords altogether. Even today, there are several people without a smartphone. Requiring multi-factor or cumbersome login procedures would hinder those people's ability to access their accounts.

[Rui Zhao](https://unomaha.instructure.com/courses/43633/users/40845)

[**Rui Zhao**](https://unomaha.instructure.com/courses/43633/users/40845)

Mar 24, 2021Mar 24 at 4:06pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

"user reluctance and usability" -  a very good point! and it can even be applied to the password-based authentication. Many people, including researchers and engineers, agree that the more secure we want it be the more cumbersome it will be.

[Collapse Subdiscussion](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)[Andrew Storms](https://unomaha.instructure.com/courses/43633/users/105646)

[**Andrew Storms**](https://unomaha.instructure.com/courses/43633/users/105646)

Mar 22, 2021Mar 22 at 9:24am

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

Andrew Storms

CSCI 8410

Paper 2

                One form of intrusion is taking the mobile device community by storm in recent years. The use of backdoor programs to create ease-of-use access to organization’s systems, including Apple, has become a growing threat to security over the last 5-10 years. One particular concern regarding backdoor programs is the laws and restrictions that come with the use of them. Government intervention regarding backdoor programs has been slim to none, with continued push by individual states to have forced federal programs or legislation that will monitor or control the use of backdoor programs by organizations or businesses in the United States. While this push has continued for many years, there has been a sever lack of direct action taken by the higher government to place laws for the use of backdoor programs. One major case regarding the legitimate use of backdoor programs in the United States was the case of Apple vs. the FBI. The FBI wanted decrypted access to the shooter in San Bernardino in 2017. To do this, Apple would have had to implement the use of a backdoor system update that would allow for this type of intrusion into the user device. The issue sparked a mountain of different legal and ethical issues. Apple refused to allow the use of this type of technology to potentially put millions of users at risk, as this could not be done to just one device but had to be pushed out to the whole network. The FBI argued that crucial information regarding the shooting was housed on the phone and needed to be accessed. In an eventual lawsuit, Apple won the request to refuse this service to the FBI and keep the information private.

                Following this, there has been an even greater push for legislation regarding backdoor programs and there implementation during certain situations, including situations like this.

[Rui Zhao](https://unomaha.instructure.com/courses/43633/users/40845)

[**Rui Zhao**](https://unomaha.instructure.com/courses/43633/users/40845)

Mar 24, 2021Mar 24 at 4:07pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

Is it for the paper 2?

[Collapse Subdiscussion](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)[Jeff Smolinski](https://unomaha.instructure.com/courses/43633/users/79659)

[**Jeff Smolinski**](https://unomaha.instructure.com/courses/43633/users/79659)

Mar 22, 2021Mar 22 at 10:55am

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

In the world of cybersecurity, the interests of system availability usually conflict with both the confidentiality and integrity concerns of that same system. Arguably, this conflict is no more apparent than in the realm of authentication. Specifically, passwords and password policy.

Notwithstanding this paper age, many of its points are still relevant today.

Among the barriers to moving beyond passwords the author mentions two realities. First, if an organization implements a more stringent authentication protocol that is also more obtrusive to the user they risk losing market share to competitors with less obtrusive, and probably less secure, authentication schemes. Second, older companies have to support legacy systems and cost benefit analyses often dictate that it is cheaper to maintain the current authentication backend then to innovate.

This paper also illustrates how users treat passwords. Namely they often chose weak passwords out of convenience, they frequently forget passwords, they store copies of passwords in vulnerable places (like under a keyboard), and they use the same password for multiple accounts.

I don’t think the author could have fathomed how many accounts a user would have 2019. Now, the average email address has approximately 130 accounts associated with it and about 61% of people reusing their password [source (Links to an external site.)](https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic).

Similarly, this work proposes multi-factor authentication (MFA) as a minimally invasive way to bolster security. Specifically, the author suggests that cell phones may prove beneficial for MFA, but at the time people often didn’t own a cell phone or did not carry their cell phones with them. Now, that is rarely the case. In fact 81% of Americans owned a smart phone in 2019 compared to the 35% in 2011 according to the [Pew Research Center (Links to an external site.)](https://www.pewresearch.org/internet/fact-sheet/mobile/).

Today, cell phones are ubiquitous and have become a common delivery system for utilizing MFA through schemes like: one time codes, biometrics, email, and push notifications from other services. Nevertheless, cell phones are not a bulletproof MFA solution. They present: most of the risks associated with hardware tokens; especially loss and theft, they are still prone to malware which is a major concern of this paper, and they also carry the all risks inherent in the chosen MFA scheme itself.

These truths lead us to a conclusion which still holds true today. Secure authentication methods must both cause minimal friction to the user experience and be readily integrated into legacy authentication frameworks. Given these considerations, it seems that we will be stuck with passwords until an acceptable alternative is created.

[Rui Zhao](https://unomaha.instructure.com/courses/43633/users/40845)

[**Rui Zhao**](https://unomaha.instructure.com/courses/43633/users/40845)

Mar 24, 2021Mar 24 at 4:10pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

So the adoption of a security technology really needs to be aligned to the requirements including security requirements as well as other requirements such as the budget, right? That is what we have learned from the previous chapters.

[Collapse Subdiscussion](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)[Zidong Liu](https://unomaha.instructure.com/courses/43633/users/86488)

[**Zidong Liu**](https://unomaha.instructure.com/courses/43633/users/86488)

Mar 22, 2021Mar 22 at 11:53am

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

Zidong Liu

CSCI 8410

Paper Summary 2

                Passwords are still the main means of authentication on the Internet, even in the face of major problems related to password forgetting and theft. In fact, despite a large number of alternatives, we must remember more passwords than ever before. Although passwords have always provided us with convenience, it cannot be denied that the static nature of passwords allows attackers to have multiple unauthorized accesses. User passwords may also be stolen through phishing, social engineering, man-in-the-middle and keylogging attacks, so more and more people are aware of the security issues of passwords.  
                In this article, the reasons why we are making such slow progress in replacing problematic cryptosystems are presented. One is due to availability issues, the cost of tokens and support (including replacement), the need for server changes, and the growing key chain problem are that it is used in some security settings, but there are unresolved problems in deployment, privacy, and authentication from untrusted hardware. Second, passwords are widely used to protect various services. From financial transactions to free webmail and social networking sites. So far, no one identity verification alternative is suitable for all these services and fierce competition in various industries. In fact, many of the most difficult problems in Internet security can be attributed to authentication, and when we say authentication, we usually mean authorization. So far, the cost of some of the solutions is relatively high, and it is difficult to be reasonable.  
                Perhaps in the future, a large number of reasonable solutions will be used to replace the password problem. The most important of these solutions can ensure the safety of users and can measure the economic loss. These problems of replacing passwords will be studied all the time.

[Rui Zhao](https://unomaha.instructure.com/courses/43633/users/40845)

[**Rui Zhao**](https://unomaha.instructure.com/courses/43633/users/40845)

Mar 24, 2021Mar 24 at 4:13pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

"In fact, despite a large number of alternatives, we must remember more passwords than ever before" -> that is true. In order to help end users on managing their passwords, researchers have proposed many types of password managers as well as password stretching (for the generation purpose) systems.

[Collapse Subdiscussion](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)[Frank Tursi](https://unomaha.instructure.com/courses/43633/users/46026)

[**Frank Tursi**](https://unomaha.instructure.com/courses/43633/users/46026)

Mar 22, 2021Mar 22 at 2:37pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

Frank Tursi  
CYBR 8410  
Paper Summary 2

This paper written over a decade ago describes that alphanumerical passwords are the primary use of authentication in digital security and it carries a myriad of problems that makes it antiquated. There have been a number of alternatives to basic password authentication such as multi-factor authentication with a security token or mobile device, biometrics, graphical passwords, public key infrastructure, etc. While they each can help remediate issues or fill certain requirements when replacing alphanumeric passwords, there has been no solution that fulfills all requirements needed from an alternative. Some solutions may overcomplicate use for an end-user and lower the overall security if the user avoids it. Too many competing technical solutions can contribute to this issue as well. As long as the consequences of the poorer security are outweighed by the costs of implementation and usability issues, we can expect organizations to use the same authentication methods unless they are forced their hand by government regulation.

[Rui Zhao](https://unomaha.instructure.com/courses/43633/users/40845)

[**Rui Zhao**](https://unomaha.instructure.com/courses/43633/users/40845)

Mar 24, 2021Mar 24 at 4:15pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

"there has been no solution that fulfills all requirements needed from an alternative." -> it is true! unfortunately there probably will not be any better solution than password in the close future as researchers can foresee.

[Collapse Subdiscussion](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)[Jesse Hays](https://unomaha.instructure.com/courses/43633/users/11487)

[**Jesse Hays**](https://unomaha.instructure.com/courses/43633/users/11487)

Mar 22, 2021Mar 22 at 4:47pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

Jesse Hays

Rui Zhao

Distributed System Security

15 Feb 2021

**Reading Summary**

Passwords: If We’re So Smart, Why Are We Still Using Them?

                Passwords are an issue that will continued to be exploited wherever possible. One thing I think would be a good idea is the issue it brought up of some places have an on-screen keyboard rather than a physical keyboard. They would use this to save themselves of a keylogger. It also brough up the issue of malware being on the system and ruining that method. What if the system required the first half being used on a physical keyboard and the second half being put in via the on-screen keyboard? This would help the complexity of being able to steal the password via a keylogger or a session recording.

                I do believe an MFA attached to your mobile device is a great addition to security. While the user could lose the device, or have it stolen it is generally something that would be harder to procure or get around for the malicious user.

                A good point is the goals among stakeholders. The idea that having a too complex authentication could deter your customers to your competitors. The loss of potential business may not be worth the unknown increase is security.

                It mentions smartcards as a possible alternative and I have wondered why on the civilian side we don’t ever do anything like this? In the military to access anything we must log into our computers via a smart card and a pin to that smart card. The likely reason is the same as why it is still a basic authentication for most, cost, and as mentioned earlier, the potential to lose customers due to it’s complication.

[Rui Zhao](https://unomaha.instructure.com/courses/43633/users/40845)

[**Rui Zhao**](https://unomaha.instructure.com/courses/43633/users/40845)

Mar 24, 2021Mar 24 at 4:21pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

"They would use this to save themselves of a keylogger" -> well it is true for the hardware-based keyloggers but not the software-based keyloggers.

"What if the system required the first half being used on a physical keyboard and the second half being put in via the on-screen keyboard? " -> So in order to defeat the keyloggers, a group of researchers, many years ago, proposed a solution in the OS that can encrypt the communication channels between the physical keyboard and the OS kernel. In such a case, any eavesdropper, no matter on the physical cable or in the OS, cannot see what is really transmitted from the keyboard to the OS.

MFA indeed has already been adopted by more and more organizations. It seems to be a great add-on to the password-based authentication regarding the security, the cost, and the usability.

[Collapse Subdiscussion](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)[Xavier McCaig](https://unomaha.instructure.com/courses/43633/users/17725)

[**Xavier McCaig**](https://unomaha.instructure.com/courses/43633/users/17725)

Mar 22, 2021Mar 22 at 7:21pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

Xavier McCaig

CYBR 8410

Paper 2

22 March 2020

This work describes the state of password usage as the primary method of authentication to digital systems as of 2009. While citing a number of issues which are still present in the modern authentication context, the work mentions the early stages of what is now a popular security measure, Multi-Factor Authentication, as implemented via SMS by Bank of America. Additionally, early authenticator applications were mentioned for usage with eBay, PayPal, and AOL. Alongside MFA, graphical passwords and cryptographic certificates were mentioned as potential solutions for password woes. The years since the work's publication have proven the authors to be right in many ways - ease of use often trumps legitimate security concerns both for the firm and the customer, which, though implemented to some degree, ultimately led to the demise of graphical passwords and cryptographic certificates for common consumer authentication. On the same hand, the increasing ubiquity and sophistication of smartphones since 2009 created the perfect environment for MFA technology to take hold - as now, SMS- and authenticator- based MFA is extremely popular, especially for applications requiring greater security. Regardless of the current state of password usage, the authors were absolutely correct in that such changes are typically symptomatic of economic and social effects, not security, and until a population recognizes a shift in cost-benefit with respect to security, no change will occur.

[Rui Zhao](https://unomaha.instructure.com/courses/43633/users/40845)

[**Rui Zhao**](https://unomaha.instructure.com/courses/43633/users/40845)

Mar 24, 2021Mar 24 at 4:24pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

Let's see how long there will be a brand-new authentication method that will eventually replace the password-based authentication.

[Collapse Subdiscussion](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)[John Kieran](https://unomaha.instructure.com/courses/43633/users/6118)

[**John Kieran**](https://unomaha.instructure.com/courses/43633/users/6118)

Mar 22, 2021Mar 22 at 8:26pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

John Kieran   
CYBR-8410   
Paper 2 summary

**Summary**

This paper attempts to compare non-password authentication mechanisms, specifically the security improvements offered by each method and analyzes the rate of adoption.  Methods studied include those we have been exposed to in class: hardware tokens, biometrics and two-factor authorization.  Many of the reasons listed for low rates of adoption can be condensed into cost, e.g. the cost of a security breach or fraudulent activity is less than the “hassle” of dealing with improved security devices.

**Critique**

This is a very well-rounded paper which considers many aspects surrounding the future of user authentication and authorization.  I like how the researchers weighed the costs and benefits of each method and discussed why little progress has been made and why passwords are still so ubiquitous.  However, users have been comfortable using the tried-and-true password methods despite the near daily headlines of security breaches.  Until the cost of a breach or fraud is worth the investment of more security, users will likely not move away from traditional passwords.

**Reflection**

This was more of thought experiment than academic research.  Society is at a crossroads now with our entire lives in digital systems which we access daily.  These digital lives must be secured from malicious actors who seek to profit from personal or financial data.  A password is often not enough to secure the digital vault and improvements must be made.  However, like all things, there is a cost to increased security which some users are not willing to invest or simply do not trust.  Biometric readers are becoming more commonplace on mobile devices, but often these do not interface with the digital accounts we use.  Two-factor authentication strikes a solid balance between cost, convenience, and effectiveness.  For example, a simple one-time passcode sent to a user’s mobile device after entering a password for a banking service is little more than a small inconvenience which can protect them from a digital robbery.

[Rui Zhao](https://unomaha.instructure.com/courses/43633/users/40845)

[**Rui Zhao**](https://unomaha.instructure.com/courses/43633/users/40845)

Mar 24, 2021Mar 24 at 4:26pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

"Two-factor authentication strikes a solid balance between cost, convenience, and effectiveness. " -> exactly! that is why it has been widely adopted.

[Collapse Subdiscussion](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)[Stevie Siy](https://unomaha.instructure.com/courses/43633/users/29318)

[**Stevie Siy**](https://unomaha.instructure.com/courses/43633/users/29318)

Mar 22, 2021Mar 22 at 8:31pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

Written in 2009, this article was written to question the wide usage of passwords as user authentication methods, and most of the points they made hold true to this day. Even 12 years ago, the overall security of passwords was a security issue worth examining. This group of researchers determined seven main reasons that passwords were not scrapped back in 2009: diversity of services to protect, too many options to choose from, different values of security and usability, a scarcity of proof that passwords were at fault for data loss, user stubbornness to sacrifice convenience for security, individual control of end-user programs sticking with the way things have always been, and that the fact that there is not one single governing body for the internet to change the standard for authentication. Clearly, most of these are still issues that exist today. In addition to this commonality, the authors make predictions of where we will be in a few years' time at the end of the paper. For one, they felt it would take a major economic catastrophe to force a move on past passwords. In the time since then, there have been a number of major data breaches that were attributed to password-related attacks. However, it seems that the balance of convenience and security still leans toward convenience from both parties: users and developers. First hand I noticed this when UNO began to require DUO mobile multifactor authentication for single-sign-on to UNO services. My peers were inexplicably upset to take the extra 15 seconds to respond to a notification pushed to the phone they always carried anyway. No matter how many times password authentication methods are breached, nor how large the enormous pile of evidence against passwords grows, users are stubborn and it is cost-efficient to continue to implement the password authentication systems we see today.

[Rui Zhao](https://unomaha.instructure.com/courses/43633/users/40845)

[**Rui Zhao**](https://unomaha.instructure.com/courses/43633/users/40845)

Mar 24, 2021Mar 24 at 4:31pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

"Clearly, most of these are still issues that exist today. " -> that is why we are still reading this paper in this course.

"My peers were inexplicably upset to take the extra 15 seconds to respond to a notification pushed to the phone they always carried anyway." -> it happened not only to students but also to many faculty and staff members here. As users, we just want to have something easy to operate on. It is human nature, which might be very hard to change.

[Collapse Subdiscussion](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)[Jensen Miller](https://unomaha.instructure.com/courses/43633/users/2767)

[**Jensen Miller**](https://unomaha.instructure.com/courses/43633/users/2767)

Mar 22, 2021Mar 22 at 9:31pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

Jensen Miller

Paper 2 Summary

The title of this paper is “Passwords: If We’re So Smart,Why Are We Still Using Them?” It is a joint effort between private, public, and university researchers studying the effectiveness of passwords, their potential in the future, and possible replacements or improvements for them going forward. The paper was written in 2009 so it is a look into the past on what people expected going forward.

As it stands it seems like we stand at pretty much the same point that we did back then. Passwords are easily stealable, breakable, commonly weak, and easy to forget for some. We are seeing a larger scale roll-out of 2-factor and almost universal usage on high importance accounts (financial, investing, etc.). What is really jarring is how they refer to SSL as only being common on banking sites. That is something that has most certainly changed. Also, they refer to the “sitekey” image software on banking sites. That was a revelation because, for the longest time I had an image associated with my bank account login and I thought it was just a strange personal choice. I had no idea it was an additional security measure. It has vanished in a site overhaul they made a while back but it still stuck in my head.

It seems that they were on-point with their prediction of a slow gradual rollout of improved security schemes. With two-factor now being almost commonplace it seems that that was the security improvement that the market chose. PCI and PII security was driven both by government regulation and industry standards so it moved a little faster to one time keys and tighter transaction security. It certainly seems like there hasn’t been a big enough breach to result in a complete shift away from passwords and at this point I don’t think that will ever happen. I think that a new product will spring up that allows for easier identification, and we will gradually shift almost entirely away from passwords out of convenience.

But, who knows. Technology is an incredibly volatile field and security just as much so.

[Rui Zhao](https://unomaha.instructure.com/courses/43633/users/40845)

[**Rui Zhao**](https://unomaha.instructure.com/courses/43633/users/40845)

Mar 24, 2021Mar 24 at 4:38pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

"That was a revelation because, for the longest time I had an image associated with my bank account login and I thought it was just a strange personal choice." -> yes, many years ago some banks used this strategy to serve as 2nd authentication factor and to differentiate humans from machines (similar to CAPTCHA and re-CAPTCHA). I can still remember when I was living in Colorado, the bank of ENT was using this scheme.

I heard that at UNO, instead of using the DUO mobile app, we can also request a hardware token that serves as the 2nd factor.

Edited by [Rui Zhao](https://unomaha.instructure.com/courses/43633/users/40845) on Mar 24 at 4:39pm

[Collapse Subdiscussion](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)[Khedir Qassim](https://unomaha.instructure.com/courses/43633/users/102151)

[**Khedir Qassim**](https://unomaha.instructure.com/courses/43633/users/102151)

Mar 22, 2021Mar 22 at 10:42pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

**Passwords: If We’re So Smart, Why Are We Still Using Them?**

The article spots the light on one of most important and basic user authentication method which is alphanumeric password. The purpose of this article which was written in 2009 is to compare and question the wide use of passwords usage and problems associated with it, such as users choosing weak passwords, forgetting passwords, storing copies, and using the same password for multiple systems that make them vulnerable to brute force attacks and man in the middle attacks etc. however with all these problems, passwords remained the dominated method of access control.

The article also discussed some of proposed alternates to basic passwords such as using multi factor authentication by using physical, biometric tokens or cellphones and public key infrastructure, but these alternatives have been limitedly used due economic and other technical reasons. In addition, the article mentioned the on-screen keyboard techniques and SiteKey as other two strong alternatives to overcome keystroke and malware attacks and provide more robust user authentication especially in financial institutions.

The article discussed seven important barriers moving beyond password which are diversity of requirement, competing technical proposals, competing goals among stakeholders, scarcity of loss data, user reluctant and usability, Individual control of end-user platforms and finally no single organization can impose a solution. Out of all these seven barriers the most common one could be the user reluctance and usability since many users even after a decade of publishing this article still tend to use weak and simple guessable password.

The last part of the article explains in sort of questions and answers some of the possible and better solution towards some solution techniques beyond passwords which are now commonly used in our daily life by giving example from real life experiences such as using smartcard PIN and EV-SLL certificates in some countries beside some major security improvement that have been adopted over the past decades to better strengthen the user’s authentication and access controls.

In conclusion, despite passwords being weak, they will continue to be largely used in the next few years in my opinion. In the meantime, there are also some trends that slowly moving towards using passwordless techniques based on 2nd factor authentication or some biometric authentications like touch ID or other key fob or mobile token apps that don’t not require users to remember their password. According to Gartner, by year 2022 60% of large and global enterprises and 90% of midsize enterprise will implement passworless methods in more than 50% of use cases.

[Rui Zhao](https://unomaha.instructure.com/courses/43633/users/40845)

[**Rui Zhao**](https://unomaha.instructure.com/courses/43633/users/40845)

Mar 24, 2021Mar 24 at 4:45pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

"The last part of the article explains in sort of questions and answers some of the possible and better solution towards some solution techniques beyond passwords which are now commonly used in our daily life by giving example from real life experiences such as using smartcard PIN and EV-SLL certificates in some countries beside some major security improvement that have been adopted over the past decades to better strengthen the user’s authentication and access controls." -> wow this sentence is pretty long...BUT...I get it!

"According to Gartner, by year 2022 60% of large and global enterprises and 90% of midsize enterprise will implement passwordless methods in more than 50% of use cases." -> that can be true in the enterprise environment because those log in attempts can be monitored and well controlled in their LAN for example, but I doubt if it is still true in the open environment such as on the internet.

[Collapse Subdiscussion](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)[Alexander Bladow](https://unomaha.instructure.com/courses/43633/users/37067)

[**Alexander Bladow**](https://unomaha.instructure.com/courses/43633/users/37067)

Mar 22, 2021Mar 22 at 11:46pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

Alexander Bladow

CSCI 8410

Paper summary 2

             This paper was about the usage of passwords in modern authentication systems. It started off by stating the problem of the paper which is that standard password-based authentication systems tend to have a number of shortcomings, such as the user forgetting the password, it is comparatively vulnerable, and the fact users tend to use the same password on many systems. I find these to be valid points regarding the shortcomings of passwords some of which I am partial to myself. The next section within the paper presents alternatives and or augmentations to the standard password authentication system. The first one is two-factor authentication in which I agree that physical token authentication is potentially more secure, more expensive, and less convenient than the mobile device alternative that is most commonly used. Some other methods proposed would be biometric authentication, graphical passwords, on-screen keyboards each of which has upsides and downsides, such as biometric authentications increased security and its cost for implementation or how on-screen keyboards only protect against simple keylogging software and not much more compared to a standard physical keyboard password entry. After it provided some alternatives went on to describe some of the barriers that exist to move on from passwords. One of the first barriers is the fact that different organizations have a diversity of requirements regarding what their business process needs, or the fact that organizations do not report how passwords were lost meaning that it becomes difficult to fix problems due to the fact that we do not know the severity of problems. There are a number of other barriers that are described to display the difficulties that will be present in this transition if or when it happens most of these are primarily issues of work and convenience over organizational limits. The following section primarily answers questions regarding difficulties in implementation and differences between standards, and the final section here describes predictions and progress into the future which in the scope of this paper is 2019 and beyond, which due to widespread two-factor authentication pushes is starting to date the paper I feel.

Edited by [Alexander Bladow](https://unomaha.instructure.com/courses/43633/users/37067) on Mar 22 at 11:46pm

[Rui Zhao](https://unomaha.instructure.com/courses/43633/users/40845)

[**Rui Zhao**](https://unomaha.instructure.com/courses/43633/users/40845)

Mar 24, 2021Mar 24 at 4:49pm

[Manage Discussion Entry](https://unomaha.instructure.com/courses/43633/discussion_topics/427919)

"The first one is two-factor authentication in which I agree that physical token authentication is potentially more secure, more expensive, and less convenient than the mobile device alternative that is most commonly used." -> nowadays, some of these tokens are even use quantum computing techniques.