Evaluating the Viability of FIDO2 Authentication in University Environments: A Survey-Based Exploration

Ibrahim Ammar
University of Michigan—Dearborn

Armeet Chhina
University of Michigan—Dearborn

Ryan Sauer
University of Michigan—Dearborn

Abstract

In the rapidly evolving landscape of secure authentication, FIDO2 (WebAuthn), an emerging alternative to the traditional password-based approach, has gained increasing attention. While FIDO2 addresses critical weaknesses that passwords face, it has faced many perceived and legitimate concerns, preventing it from achieving widespread adoption. In the years since W3C announced WebAuthn as an official standard, there has been promising research into it's large-scale feasibility, security, and adoption. We aim to continue this by expanding the scope to include FIDO2's use within higher education. In this paper, we conducted a survey of 40 college students to gain insight into campus authentication. Our study found that while 37.5% of our participants had heard of FIDO2, only 5% are familiar with this method of authentication. We also analyze the students interest in the potential for it's integration with their schools authentication system and found that the vast majority believe their university should be aware of this option. Finally we researched potential accessibility concerns when it comes to roaming authenticators. We use this information to highlight potential needs for education around WebAuthn on campuses and the desire of the users for change.

1 Introduction

The advent of the digital era has not only transformed the way information is accessed and shared but has also heightened concerns about the security of private and sensitive data. Now, not just the national government has access to swaths of personal data, such as names, phone numbers, payment information, and social security numbers. Local institutions, educational institutions, and companies are all common organizations that will store heaps of private data on their servers. These hard drives are highly coveted by cybercriminals for their own use, selling on the dark web, or even being used as blackmail. Because of the constant threat of data being stolen, securing this information is paramount for anybody in possession of this sensitive data.

For decades, passwords have served as the standard for securing an individuals information. However, as technology as advanced, so has the sophistication of cyber threats. A password became the only gatekeeper for increasingly valuable data, prompting researchers to seek more secure alternatives [3,7]. The vulnerabilities, from susceptibility to phishing attacks t the risks associated with password reuse and centralized storage, have underscored the necessity for a paradigm shift in authentications methods.

In 2019, the announcement of WebAuthn [4] (commonly referred to as passkeys) as an internet standard marked a significant milestone in the quest for enhanced, user-friendly authentication. WebAuthn leverages public-key cryptography and roaming authenticators to attempt to usher in a new era of passwordless, secure, and fast logins. Its potential to mitigate major threats associated with passwords, particularly from a human-centric perspective, positions it as a viable alternative deserving of exploration.

Despite the growing recognition surrounding FIDO2's potential, there exists a notable lack of research specifically addressing it's use within university systems. In light of this gap, we constructed a brief survey aimed to improve the understanding of passkeys potential use at universities. We analyzed the responses of 40 college students on their perceptions of current university approaches to authentication, awareness and interest in the use of passkeys, and opinions on accessibility for student's roaming authenticators in the case a college adopted WebAuthn. We aim to answer if students felt a need for better security at their institutions, their awareness and understanding of the FIDO2 protocol, and to understand concerns related to the accessibility that is required for universities to provide given the private nature of the data they poses.

In section 2 of this paper, we review related work that has already been done to research university authentication as well as the FIDO2 protocol. In section 3, we review the methodology we used to conduct our survey including development of the questions, demographics, and the collection process. In the 4th section, we review the results we received. In section

5, we analyze the implications of the data and responses from section 4 along with describing ways our survey and results could have been improved. In section 6, we discuss potential future work that should be done within the context of passkeys and universities. Finally, in section 7, we conclude our paper and our research.

2 Related Work

In the realm of digital security, particularly in academic environments, understanding user behavior and attitudes towards different security measures is pivotal. This "Related Work" section draws upon existing studies, including those centered around alternative authentication methods, FIDO2, and authentication around universities, to contextualize our research on passkey's utility on university campuses.

Password Alternatives: As mentioned previously, there has long been a search for a comprehensive alternative and alterations [16] to passwords to improve security concerns. One example was proposed by Stajano [21] called Pico. This paper proposed utilizing a hardware token and public-key cryptography. The later makes it comparable to FIDO2. However, little came from this proposal outside of a small scale implementation by Hermans and Peeters [9] and a usability survey [2]. Another alternative that has seen use throughout many industries are FIDO U2A's [19] which have been implemented in the now fairly well known YubiKeys. This system also utilizes hardware authentication and public-key cryptography. There has been a significant amount of research into YubiKeys both technically and usability-wise. Reynolds et al. [18] found that while many users struggled to set their YubiKey up, they enjoyed the experience more than traditional passwords once all was said and done. Das et al. [6] found the system to be fairly confusing to users, causing a lack of desire for adoption. As this was a previous proposal of the FIDO alliance, the hope is that FIDO2 could improve upon some of these issues in implementation.

FIDO2: With the advent of passkeys, there as been a flurry of research both on the technical aside and for usability. Many studies have focused on the usability of FIDO2 versus traditional passwords [8, 10, 11, 17]. There have been mixed results. Some had users find FIDO2 to be more usable and acceptable than traditional passwords, while others were more mixed. However, there was a general consensus that major road blocks consisted of authenticator accessibility, account recovery, and understanding how the protocol actually works. Lassak et al. [14] interviewed 28 CISOs to better understand the slower roll out for passkeys adoption. They found many barriers, most notably regulatory requirements and account recovery. With users and CISOs alike identifying similar issues, it is good that there is already research being done to combat these issues [12]. Lassak et al. [13] studied user misconceptions about FIDO2 and attempted to improve user experience to prevent these misconceptions. They found that simple informational screens during user's setup and use allowed for a significant increase in user perception and understanding. However, there was still much work left to be done.

University Authentication: Universities have a limited amount of published research around their authentication methods relative to general industry. After implementing different kinds of MFA, Colnago et al. [5] found that users found transitioning to MFA relatively easy, despite it being a mild annoyance. Abbott et al. [1] found that university users were not disturbed by implementing MFA for accounts containing sensitive information, but there was a significant disturbance to users who had to use MFA for all accounts regardless of security need. Morii et al. [15] ran some feasibility testing for shibboleth and FIDO at their university to promising results. While there were some issues remaining, there was an improvement to security.

Given the lack of research on FIDO2's use within the university context, our goal was to extend the research of FIDO2 and university authentication systems by answering the following research questions:

1. How do students perceive the current authentication methods at their universities?
2. Are students aware of FIDO2 passwordless authentication?
3. What thoughts and concerns do students have with FIDO2's use for campus resources?
4. Are there accessibility concerns for students if they were required to use passkeys?

3 Methodology

Our study's core goal was to understand the perceptions and attitudes towards the adoption of passkey systems within university campuses, especially compared to current authentication methods. As requested by this researches requirements, the survey contained over 20 questions, logically divided into categories that reflected our four key research questions. We used both quantitative and qualitative approaches as we describe in this section.

Survey Development and Procedure The development of the questionnaire involved several stages, including an initial literature review to identify key areas of interest, drafting of questions, and a final review. We reviewed a multitude of papers that reviewed and surveyed users use of passkeys

to understand common practices and areas of improvement. After our literature review, we drafted questions to answer our research goals. In our review we sorted the final questions into the following related section:

- Demographics: covers information such as the affiliated university, position, related area of study, and current level of study.
- Current Practices and Awareness: covers questions regarding current authentication methods, devices used for access, ease of use, concerns with the current system, etc.
- Mobile Authentication: covers roaming authenticator experience and their usability
- Passkeys/FIDO2: covers prior knowledge of FIDO2, opinions on it's adoption for a university, and potential concerns within campus with it's implementation.

Participants who participated in the survey would be presented these questions in order. There was minimal logic for skipping questions. The most notable potential skipped question was related to FIDO2 awareness. If users claimed to have any level of awareness of FIDO2 or passkeys, they were asked to provide a brief description of what they knew about them. Unaware participants were not asked this question. Regardless of the participants awareness, they were then shown a simple introduction to passkeys from Amazon [20] before continuing with the survey.

Data Collection Process Due to limited collection times, the survey was distributed online, thereby facilitating ease of access and broad participation. The online distribution method was chosen for its efficiency and its ability to reach a wide audience quickly. Qualtrics was chosen as the website for the survey as it allowed for quick creation and comprehensive data analysis tools. After the survey was completed, responses were collected over a period of three weeks. The digital approach not only streamlined the process of data collection but also ensured that the responses were accurately recorded and were able to be easily and instantly analyzed.

Participant Demographics The distribution period was limited in scope due to very extreme time and resource constraints. In spite of this limitation, we managed to have a relatively diverse demographic of responses. As seen in Table 1, we had participants from 23 different universities. Their level of study ranged from first year bachelor to masters students and 11 different areas of study. We broke computer science and cybersecurity out from engineering as they are specifically relevant to the subject of the paper. The limited resources and distribution time lead to a notable abundance of participants who were from the University of Michigan—Dearborn, seniors, and computer related degrees.

Table 1: Demographic Results (n=40)

Participants University		
University of Michigan—Dearborn	15	37.5%
Boston Conservatory	3	7.5%
Roosevelt University	2	5%
Other (1 Participant)	20	50%
Level of Study		
Freshman	2	5%
Sophmore	5	12.5%
Junior	7	17.5%
Senior	17	42.5%
Recent Bachelors Degree	2	5%
Masters	7	17.5%
Area of Study		
Engineering	7	17.5%
Computer Science	15	37.5%
Cybersecurity	5	12.5%
Fine Arts	5	12.5%
Traditional Science	1	2.5%
Social Science	1	2.5%
Education	1	2.5%
Kinesiology	1	2.5%
Library Science	2	5%
Medical	1	2.5%
Economics	1	2.5%

4 Results

Our survey was conducted over the course of around 3 weeks. We had 40 participants who responded with a wide variety of experience, knowledge, and opinions, with a goal to gain insight of security and FIDO2/passkey awareness among students.

Current University Practices The participants indicated that they mainly used authentication methods such as passwords which consisted of 95% (38 out of 40 participants) of responses, followed closely by multi-factor authentication (MFA) which consisted of 85% (34 out of 40 participants). These two had a huge difference compared to the other options including Personal Identification Number (PIN), Passkeys, and Smart Cards (RFID). Even with the sum of the other options they make up 22 selections not even close to the two giants passwords, and multi-factor authentication which have become a staple for security in any situation.

From the survey results students predominantly use laptops (38 out of 40 participants), smartphones (36 out of 40 participants), and desktop computers (23 out of 40 participants) to access University resources. Only 20% (8 out of 40 participants) selected the sum of smartwatch and other. In the survey we neglected to include tablets and they were the largest selection not including the big three mentioned before.

Students also reported to use 2-3 devices which would be a combination or the selection of mainly laptops, smartphones, and desktop computers.

When asked regarding the ease of use for their current University authentication methods, majority of participants gave feedback indicating that current authentication methods are not difficult to use. 85% (34 out of 40 participants) fall into categories including "Very easy to use" and "Fairly easy to use". In fact only one participant reported negatively regarding ease of use for their university authentication method reporting it to be "Fairly difficult to use" most likely referring to the Smart Cards (RFID) method of authentication. These results suggest the students have a general satisfaction with the usability regarding the systems of authentication.

In terms of security, participants also responded positively having the greatest majority 55% (22 out of 40 participants) of the survey population perceived their method of security to be "Somewhat secure". Similarly to the ease of use question, participants are satisfied with the security of their educational establishment. Only 3 users responded negatively looking for improvement with the security in their University. The most prevalent causes for their concerns included data leaks, phishing attempts, and tracking issues with the systems used for authentication.

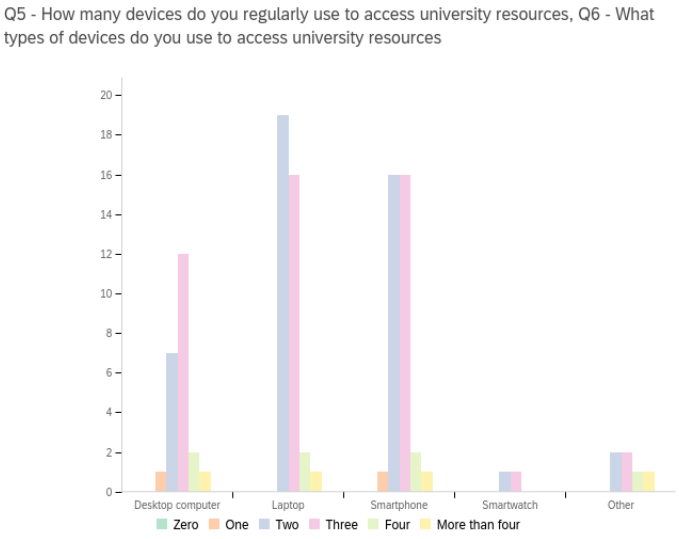

Figure 1: Graph visualizing relation between amount of devices and types of devices used to access University resources.

Familiarity with FIDO2/Passkeys The survey had three layers of familiarity with FIDO2/Passkeys for the participants shown in Figure 3 . The smallest portion 5% of the survey population (2 out of 40 participants) reported being familiar with FIDO2/Passkeys. Both participants are Seniors, studying Cyber Security, and Computer Engineering respectively. Due to their background in these fields and being in Seniors they have

Table 2: Current Awareness Results

Method of Authentication		
Passwords	38	95%
Multi-factor Authentication (MFA)	34	85%
Personal Identification Number (PIN)	6	15%
Passkeys	4	10%
Smart Cards (RFID)	12	30%
Amount of Devices (n=40)		
One	1	2.5%
Two	20	50%
Three	16	40%
Four	2	5%
More than four	1	2.5%
Ease of Authentication (n=40)		
Very easy to use	16	40%
Fairly easy to use	18	45%
Neither easy nor difficult to use	5	12.5%
Fairly difficult to use	1	2.5%
Very difficult to use	0	0%
Perceived Security of Method (n=40)		
Very secure	13	32.5%
Somewhat secure	22	55%
Neither secure nor insecure	2	5%
Somewhat insecure	3	7.5%
Very insecure	0	0%
Frequency of Phishing (n=40)		
Once a day	2	5%
Once every few days	2	5%
A few times a month	9	22.5%
Once a month	5	12.5%
Rarely	14	35%
Never	8	20%
Current Security Concerns (n=23)		
Data leaks	4	17.4%
Phishing	3	13%
Tracking	1	4.3%
No concerns	15	65.2%

some knowledge or insight regarding FIDO2. A larger portion includes 32.5% (13 out of 40 participants) of the participants indicating they have heard of FIDO2/Passkeys. Of these 13, 11 were students under the Computer Science discipline having a basic understanding of FIDO2 but not understanding the deeper technology or implementation. Lastly the majority of the population 62.5% (25 of out 40 participants) have never heard of FIDO2/Passkeys, showing a significant hole in awareness that could impact the adoption and integration of this technology within higher education.

Passkey Adoption The survey results revealed students' perspectives on the potential adoption of FIDO2/Passkey authentication within their university. A considerable majority

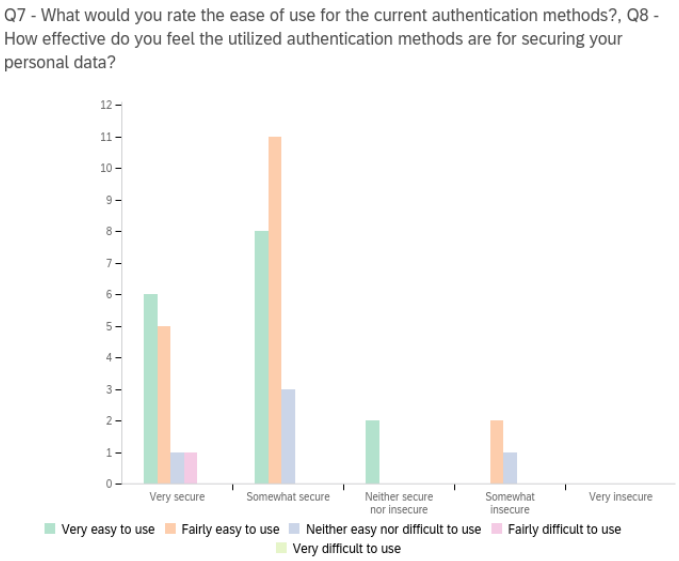

Figure 2: Graph visualizing relation between participants ease of use with authentication methods and perceived security provided by authentication method.

Table 3: Familiarity with FIDO2/Passkeys

Very familiar	2	5%
Somewhat familiar	13	32.5%
Not familiar	25	62.5%

of 62.5% (25 out of 40 participants) expressed their desire for the university to at least be aware of FIDO2/Passkey as an option, signifying a proactive stance towards newer security technologies. Moreover, 35% (14 out of 40 participants) were in favor of their university actively looking into adopting this method, indicating an openness to evolution in authentication processes.

Regarding the comfort level with employing passkeys on personal devices for university-related authentication, the majority of students showed a willingness to adapt, with 72.5% (29 out of 40 participants) indicating they would be either "Extremely comfortable" or "Somewhat comfortable". This points to a silent yet large acceptance of integrating security measures into their daily routines.

When considering the use of biometric authentication as part of the FIDO2/Passkey system, students displayed mixed feelings. A segment of 20% (8 out of 40 participants) expressed "Extreme comfort," suggesting a group of early adopters who are ready to embrace change and biometric technologies. However, a combined 27.5% (11 out of 40 participants) felt "Somewhat uncomfortable" or "Extremely uncomfortable," reflecting concerns about their privacy and the nature of biometric data. Although some did voice their main concern with biometric data including face scans, but being comfortable with other methods including fingerprint scans.

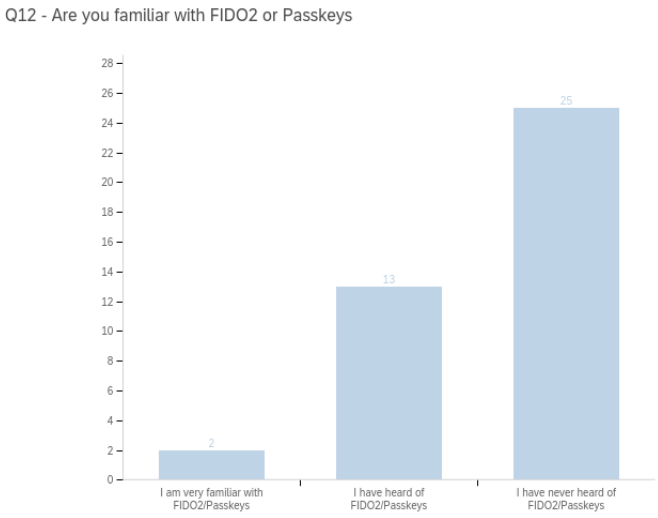

Figure 3: Graph visualizing participants familiarity with FIDO2/Passkeys.

The participants also voiced specific concerns about the shift to FIDO2/Passkey authentication methods. The predominant worry was the "Ease of use," with 70% (28 out of 40 participants) apprehensive about potential complexity. "Personal privacy" issues were the second most cited concern at 55% (22 out of 82 selections), followed by "Cost of implementation" at 32.5% (13 out of 40 participants). These apprehensions underscore the need for the university to ensure any new system is user-friendly, cost-effective, and respectful of personal privacy.

The participants express a forward-looking attitude towards the adoption of FIDO2/Passkeys, underscored by a significant interest in the university's recognition and exploration of this technology. However, alongside this enthusiasm, there is a clear call for addressing ease of use, personal privacy, and cost, which the university must consider to ensure broad acceptance and successful implementation.

Passkey Accessibility The results gave insights into potential accessibility concerns associated with the requirement to use FIDO2/Passkeys on University campus. A significant majority, 82.5% (33 out of 40 participants), expressed that the university should offer an alternative to those uncomfortable with using personal devices for FIDO2/Passkey authentication. This response highlights the need for institutional support mechanisms that provide individual privacy preferences and concerns.

Furthermore, when asked whether the university should provide students with authentication devices or methods if a student did not have access to or the ability to use a personal device, a substantial 77.5% (31 out of 40 participants) agreed that it should. This finding highlights a strong inclination towards ensuring that no student is disadvantaged due to a

Table 4: Adopting FIDO2/Passkeys Results

University and FIDO2/Passkeys		
look into adopting	14	35%
Be aware of the option	25	62.5%
Not want to look into adopting	1	2.5%
Comfort using Passkeys		
Extremely comfortable	9	22.5%
Somewhat comfortable	20	50%
Neither comfortable nor uncomfortable	8	20%
Somewhat uncomfortable	3	7.5%
Extremely uncomfortable	25	0%
Comfort using Biometric Authentication		
Extremely comfortable	8	20%
Somewhat comfortable	17	42.5%
Neither comfortable nor uncomfortable	9	22.5%
Somewhat uncomfortable	17	42.5%
Extremely uncomfortable	1	2.5%

lack of access to the necessary technology. Once again this would require support from the institutions and would be another negative factor as it would increase university costs for security.

When participants were questioned about specific concerns related to a university's transition to FIDO2/Passkeys, "Ease of use" was the foremost concern, chosen by 70% of participants, reflecting a priority for user-friendly technology adoption. "Personal privacy" was also a significant concern for 55%, and "Cost of implementation" for 32.5%, which could impact student fees and university budgeting.

These results suggest that while students are generally open to the adoption of FIDO2/Passkey systems, they also expect the university to uphold principles of accessibility and equity. This would entail providing alternative means of authentication for those who are either uncomfortable with or simply providing devices for those who don't have access to personal devices for securing their university accounts.

Table 5: Accessibility FIDO2/Passkeys Results

Should University Provide Alternate		
Yes	33	82.5%
No	7	17.5%
Concerns with FIDO2/Passkeys		
Increased risk to university security	7	17.5%
Cost of implementation	13	32.5%
Ease of use	28	70%
Personal Privacy	22	55%
Access to authenticators	11	27.5%
Other	1	2.5%

5 Discussion

The survey conducted at the University of Michigan—Dearborn has unfolded a complex and multifaceted array of perceptions towards the adoption of passkey systems in an academic setting. This discussion delves deeper into interpreting these varied perspectives, highlighting the critical nuances and underlying themes that emerged from the survey data.

Current Student Experience Our results showed that nearly all participants use passwords currently and the vast majority currently have multi-factor authentication in place at their universities. Upon further analysis, it can be inferred that those who did not claim the use of passwords selected multi-factor authentication as an authentication method and others who attended the same university claimed passwords and MFA were in use. This suggests that 100% of the participants use passwords for on their university campuses. The majority also used two to three devices when accessing resources. This implies that the majority of students currently are accessing personal or access controlled data using MFA from several devices. The general consensus was that the current methods were fairly to very easy to use with several comments about MFA being annoying, repetitive or hindering their login experience. However, the vast majority also felt that their data was at the very least somewhat secure with these methods.

This suggests that students are feeling fairly comfortable with current protocols but there is room to improve. Over 75% of students reported receiving phishing attacks with a further 32.5% claiming they receive phishing attempts more than once a month. A few comments also mentioned concerns around phishing with respect to school emails. These threats are very real for password based authentication. While MFA is implemented at the majority of these universities, their login credentials are still at risk of being stolen through these types of attacks. The education around MFA is also apparent as not a single student who has used another device to authenticate in addition to passwords feels that the extra effort has no impact on their security. We also asked users if they had any concerns related to their universities authentication methods. Several students mentioned prior breaches, personal privacy, and phishing as potential concerns of theirs with he current model. This is promising for the potential use of passkeys as two of these three concerns could be addressed. Their use within a campus would mitigate the threat of phishing credentials and potentially reduce the 25%+ who claimed MFA caused a moderate or greater amount of interruption when logging in.

Overall, it seemed that most students were, at the very least, aware of their universities methods of authentication. While most acknowledged the security benefits to added levels of security, there was a statistically significant amount of peo-

ple who found the current user experience to be somewhat troublesome.

FIDO2 Awareness When asked outright, only 5% of the responses claimed to be relatively familiar with FIDO2 or passkeys. Considering the skew towards computer and technology related majors, this is a surprisingly low result. However, 32.5% claimed to have heard of them prior to taking the survey. That still means the majority of participants were unaware of passkeys. This is displayed further with a followup requesting users understanding of passkeys if they claimed to have any level of familiarity. There were a multitude of responses that were blatant misunderstandings such as passkeys being cloud passcodes, defining thinking they were another MFA (addition to passwords), and thinking it is a program to automatically authenticate. Less than 5 responses lacked misconceptions or blatantly false information. This suggests that passkeys have not reached a broad enough audience to be known or understood. However, it is promising that over a quarter of the participants had heard of passkeys, despite not understanding them yet.

Concerns for Adoption All but one response felt that their university should at least be aware of passkeys as an option for authentication. The 25 response majority felt that they would want their universities to be aware of the option while 14 said they would want their university to actively look into adopting the technology. This shows that students, at the very least, feel that passkeys are an equally, if not more secure form of authentication than their current methods. The vast majority also felt comfortable with the idea of using personal devices as their roaming authenticators for school related logins, however there was a slight decrease in enthusiasm when it came to using biometric authentication within that category with 6 people feeling uncomfortable compared to 3.

When it comes to concerns users had with a potential shift, 28 participants were concerned about the ease of use. This was the most popular concern along with personal privacy at 22. Personal privacy is a misconception about passkeys. Users would have no login credentials stored on university hardware unlike current systems where usernames and passwords would be required. One participant specifically made a note that they were concerned about biometric data being stored. The FIDO2 protocol however, keeps all personal information on the roaming authenticator and does not send any private information to a centralized server as many other authentication methods currently do. This shows that there would need to be a lot of education around passkeys and potential risks to make users more comfortable with it's use on a college campus, especially with the level of sensitive data that they store. two more concerns that over 25% of participants selected as a concern were the cost of implementation (13 participants) and access to authenticators (11). The cost of implementing a whole new system would indeed propose a potential for overhead costs and should be researched further for universities as outlined in future work.

Accessibility As 11 participants mention in their concerns for adoption, accessibility is a major component of authentication for a university. Every student, regardless of their capabilities, must have equal access and opportunity to receive information and access their personal data. As not everyone may have access or be comfortable using certain personal devices as roaming authenticates, 82.5% of our participants said that their university should provide an alternative device for authentication. Oddly, this dropped to 77.5% in favor of universities providing alternative devices if the user did not have access to a personal device. Overall though, the majority believe that alternative options should be provided to users by the university in the case of extenuating circumstances.

Suggestions Given our results, we would suggest that universities begin implementing feasibility studies internally to see what potential roadblocks would prevent passkeys being used on campuses or what hurdles would need addressing to overcome. It is clear that students would like their universities to be aware of this emerging technology. If a university is seriously interested in implementing a WebAuthn system, there should be a significant wave of education for students on how the system works as there are serious gaps between being aware of it's existence and understanding reasonable risks. Understanding the cost of implementation both fiscally and on associated IT teams is a big must for any feasibility studies. Finally we would suggest that having an optional phase to ease students into the use of passkeys would address the concerns for ease of use. As students become better educated and more comfortable with this technology, there will be higher levels of adoption.

6 Future Work

While this study provided a solid introduction for research into the use of passkeys at universities, there are many more areas where we could have improved our work and that can be researched further.

Potential Improvements Due to our limited distribution period, a large improvement would be a more even distribution of universities, levels of experience, and majors. With this, a longer duration would also improve user response quality as people could have more time to ponder responses. In addition to improving demographics, an improvement to question quality would also be a great addition. We had around a week to develop questions which was not nearly long enough to get a large and comprehensive survey to answer our research questions. Additionally, due to the requirements of the project combined with timing, we had limited time to analyze our

results, potentially resulting in misinterpretations, overlooked data, or incorrect assumptions. Overall, more time to develop, research, distribute, and analyze the survey would have provided a much more detail oriented result.

Surveys Our survey consisted exclusively of students. There are are many other potential surveys for university affiliated people. One important area that we did not research is the university administration, professors, graduate staff, and facility staff. These are also major members of a university campus and they arguably have more stake in the conversation for it's implementation. Another specific survey that could be conducted that would gain insight would be of IT staff who work at universities. There are many concerns mentioned for the more commercial side [14] that would have similar parallels, but much different connotations on college campuses. There is a different set of data, users of that data, and levels of security that said data requires in addition to different economic structures that universities must adhere to. These surveys could offer insight into the feasibility both on the technical and feasibility side, giving a better sense of what is likely to occur in the future.

Focus Groups Another important area of research is running tests with focus groups: having staff, administration, and students physically try using passkeys over a set period of time. This would allow for a better understanding of user adoption rates, stress on campus IT teams, and perceived changes from current to new systems. Important areas of focus for this study would include having participants be required to use certain authentication methods, groups with different levels of education on passkeys, as well as groups with differing levels of prior knowledge for comparison. Without studies like this, there can be little more than speculation within this specific domain.

Feasibility Studies Universities have a plethora of different areas where authentication is employed. This includes physical authentication at buildings, virtual authentication for user access to campus resources, as well as single sign ons. Running tests and working with the relevant departments to see what it would truly take to physically transfer and verify all systems have shifted from current methods to passkey systems, necessary upgrades or changes that would need to be made to the current protocol to be compliant with relevant standards and requirements, and the educational materials to ensure all affiliated parties are informed enough to smoothly transition.

7 Conclusion

The survey-based exploration into the viability of FIDO2 authentication in university environments has provided valuable insights into student perceptions, awareness, and concerns regarding this emerging authentication method. Our analysis of the collected data highlighted several noteworthy conclusions. The majority of students currently rely on passwords and multi-factor authentication which they find easy to use but have concerns regarding potential security risks. Given the concerns, there is a desire for exploring other potential options, even if they are not adopted. In addition, we found that only a small percentage of participants were familiar with FIDO2 and there were a whole slew of misconceptions about their risks and implementation suggesting a need for further education on the subject. Finally the considerable majority believe that universities should be aware of passkeys but should also thoroughly review potential sore areas in the cases of ease of use, personal privacy, and implementation costs if they are seriously interested in implementing passkeys for their campuses. With more research into passkeys and the unique use case of a university, we can pave the way for a more secure and user-friendly authentication landscape on college campuses.

References

[1] Jacob Abbott and Sameer Patil. How mandatory second factor affects the authentication user experience. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–13, New York, NY, USA, 2020. Association for Computing Machinery.

[2] Seb Aebischer, Claudio Dettoni, Graeme Jenkinson, Kat Krol, David Llewellyn-Jones, Toshiyuki Masui, and Frank Stajano. Pico in the wild: Replacing passwords, one site at a time. 04 2017.

[3] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*, pages 553–567, 2012.

[4] John Bradley, Christiaan Brand, Adam Langley, Giridhar Mandyam, Nina Satragno, Nick Steele, Jiewen Tan, Shane Weeden, Mike West, and Jeffrey Yasskin. Web authentication: An api for accessing public key credentials level 2. Technical report, W3C, 2021. Report available at https://www.w3.org/TR/webauthn-2/.

[5] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. "it's not actually that horrible": Exploring adoption of two-factor authentication at a university. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–11, New York, NY, USA, 2018. Association for Computing Machinery.

[6] Sanchari Das, Gianpaolo Russo, Andrew C. Dingman, Jayati Dev, Olivia Kenny, and L. Jean Camp. A qualitative study on usability and acceptability of yubico security key. In *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*, STAST '17, page 28–39, New York, NY, USA, 2018. Association for Computing Machinery.

[7] Dinei Florêncio, Cormac Herley, and Baris Coskun. Do strong web passwords accomplish anything? *HotSec*, 7(6):159, 2007.

[8] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. Is fido2 the kingslayer of user authentication? a comparative usability study of fido2 passwordless authentication. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 268–285, 2020.

[9] Jens Hermans and Roel Peeters. Realizing pico: Finally no more passwords! Cryptology ePrint Archive, Paper 2014/519, 2014. https://eprint.iacr.org/2014/519.

[10] Markus Keil, Philipp Markert, and Markus Dürmuth. "it's just a lot of prerequisites": A user perception and usability analysis of the german id card as a fido2 authenticator. In *Proceedings of the 2022 European Symposium on Usable Security*, EuroUSEC '22, page 172–188, New York, NY, USA, 2022. Association for Computing Machinery.

[11] Michal Kepkowski, Maciej Machulak, Ian Wood, and Dali Kaafar. Challenges with passwordless fido2 in an enterprise setting: A usability study, 2023.

[12] Johannes Kunke, Stephan Wiefling, Markus Ullmann, and Luigi Lo Iacono. Evaluation of account recovery strategies with fido2-based passwordless authentication, 2021.

[13] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. "it's stored, hopefully, on an encrypted server'': Mitigating users' misconceptions about FIDO2 biometric WebAuthn. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 91–108. USENIX Association, August 2021.

[14] Leona Lassak, Elleen Pan, Blase Ur, and Maximilian Golla. Why aren't we using passkeys? obstacles companies face deploying fido2 passwordless authentication (extended version), 2023. Paper available at https://maximiliangolla.com/files/2024/papers/fidoobstacles-extended.pdf.

[15] Michitomo Morii, Hiroki Tanioka, Kenji Ohira, Masahiko Sano, Yosuke Seki, Kenji Matsuura, and Tetsushi Ueta. Research on integrated authentication using passwordless authentication method. In *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, volume 1, pages 682–685, 2017.

[16] Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, and Yevgeni Koucheryavy. Multi-factor authentication: A survey. *Cryptography*, 2(1), 2018.

[17] Kentrell Owens, Olabode Anise, Amanda Krauss, and Blase Ur. User perceptions of the usability and security of smartphones as FIDO2 roaming authenticators. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 57–76. USENIX Association, August 2021.

[18] Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, and Kent Seamons. A tale of two studies: The best and worst of yubikey usability. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 872–888, 2018.

[19] Sampath Srinivas, Dirk Balfanz, Eric Tiffany, Alexi Czeskis, and Fido Alliance. Universal 2nd factor (u2f) overview. *FIDO Alliance Proposed Standard*, 15, 2015.

[20] Amazon Staff. Amazon is making it easier and safer for you to access your account with passwordless sign-in, Oct 2023.

[21] Frank Stajano. Pico: No more passwords! In *International Workshop on Security Protocols*, pages 49–81. Springer, 2011.

A Appendix A: Survey

1. **Introduction**
   (a) FIDO2/Passkeys Use in the Context Of Universities
   Thank you for considering our survey. This survey is for people involved with higher education. It should take 10-15 minutes to complete.
2. **Demographics**
   (a) What is the name of the university you are affiliated with?
   (b) What is your role at this university?
   - Student
   - Faculty
   - Staff
   - Other

   (c) What is/was your major or area of study?

(d) What department(s) do you work for and with?

(e) What are you within your major?

- Freshman
- Sophomore
- Junior
- Senior
- Masters
- Doctorate
- Other

3. **Current Practices and Awareness**

(a) What authentication methods are currently used by your university?

- Passwords
- Multi-Factor Authentication (MFA)
- Biometric Authentication
- PIN
- Passkeys
- Smart Cards (RFID)
- Other

(b) How many devices do you regularly use to access university resources?

- Zero
- One
- Two
- Three
- Four
- More than four

(c) What type of devices do you use to access university resources?

- Desktop computer
- Laptop
- Smartphone
- Smartwatch
- Other

(d) What would you rate hte ease of use for the current authentication methods?

- Very easy to use
- Fairly easy to use
- Neither easy nor difficult to use
- Fairly difficult to use
- Very difficult to use

(e) How effective do you feel the utilized authentication methods are for securing your personal data?

- Very secure
- Somewhat secure
- Neither secure nor insecure
- Somewhat insecure
- Very insecure

(f) How often do you receive university related phishing attempts?

- More than once a day
- Once a day
- Once every few days
- A few times a month
- Once every month
- Rarely
- Never

(g) What security concerns, if any, do you have regarding the current authentication methods used by your university?

4. **Mobile Authentication**

(a) Have you ever had to use a separate device for the purpose of authenticating (i.e. YubiKey Phone, etc.)?

- Yes
- No

(b) How much did this retract from your ease of logging in?

- A great deal
- A lot
- A moderate amount
- A little
- Not at all

(c) How much do you feel this extra step of authentication increases your data's security?

- A great deal
- A lot
- A moderate amount
- A little
- Not at all

5. **Passkeys/FIDO2 Awareness**

(a) Are you familiar with FIDO2 or Passkeys?

- I am very familiar with FIDO2/Passkeys
- I have heard of FIDO2/Passkeys
- I have never heard of FIDO2/Passkeys

(b) Please provide a brief description of what you understand about FIDO2/Passkeys

6. **Passkeys/FIDO2**

(a) Passkeys are a new easy-to-use way to sign in to apps and websites, offering a safe and convenient alternative to passwords. Unlike passwords, they cannot be written down or guessed, helping to prevent the accidental sharing of a passkey with a bad actor. When a customer uses a passkey on their device, it proves they have their device and are able to unlock it. Customers no longer need to worry about remembering unique passwords or using easy-to-guess identifiers, like names or birthdays. Instead, a customer can use passkeys to sign in to apps and sites the same way they unlock their devices—with a fingerprint, face scan, or lock screen PIN. And passkeys are less susceptible to phishing attacks than passwords and one-time codes in text messages, making them a more secure option for our customers.
- Amazon in "Amazon is making it easier and safer for you to access your account with passwordless sign-in"

(b) Would you want your university to look into adopting FIDO2/Passkey authentication?
- I would want my university to look into adopting FIDO2/Passkey authentication
- I would want my university to be aware of the option of FIDO2/Passkey authentication
- I would not want my university to look into adopting FIDO2/Passkey authentication

(c) How comfortable would you be with using passkeys on your personal device for university related FIDO2/Passkey authentication?
- Extremely comfortable
- Somewhat comfortable
- Neither comfortable nor uncomfortable
- Somewhat uncomfortable
- Extremely uncomfortable

(d) Would you be comfortable using biometric authentication for university related FIDO2/Passkey authentication?
- Extremely comfortable
- Somewhat comfortable
- Neither comfortable nor uncomfortable
- Somewhat uncomfortable
- Extremely uncomfortable

(e) If someone was uncomfortable using a personal device for university related FIDO2/Passkey authentication, do you think the university should provide an alternative device?
- Yes
- No

(f) If somebody did not have access or the ability to use a personal device, do you think the university should provide an alternative device or method?
- No
- Yes

(g) If your university announced it planned to change it's authentication methods to use FIDO2/Passkeys, what concerns would you have?
- Increased risk to university security
- Cost of implementation
- Ease of use
- Personal privacy
- Access to authenticators
- other

(h) Please share any additional comments, thoughts, or questions you have regarding FIDO2/Passkey authentication for your university's campus.

B Appendix B: Team Contributions

- **Ibrahim Ammar**
  - Worked on PowerPoint Presentation
  - Worked on Abstract
  - Worked on Introduction
  - Worked on Related work
  - Worked on Methodology
  - Worked on Discussion
  - Worked on Future work
  - Worked on Conclusion
- **Armeet Chhina**
  - Researched Prior Work
  - Revised Survey Questions
  - Assisted in Distribution of Survey
  - Worked on Methodology
  - Worked on Results
  - Analyzed Data from Survey
  - Created Graphs from Survey
  - Created Tables from Survey
  - Worked on PowerPoint Presentation
- **Ryan Sauer**
  - Researched Prior Work
  - Designed Survey Sections
  - Wrote Survey Questions

- Assisted in Distribution of Survey
- Worked on Abstract
- Worked on Introduction
- Worked on Related work
- Worked on Methodology
- Worked on Discussion
- Worked on Future work
- Worked on Conclusion
- Appendix A