Security and Usability of the Windows Hello System

Brooks Tawil, Undergraduate Student, Human Computer Interactions Lab

***Abstract*—This paper sets out to demonstrate the weaknesses of the Microsoft Hello Authentication protocol. The Windows Hello protocol is a new way to sign in to your Windows 10 devices with just a look or a touch. It is a closed source protocol that aims at taking fingerprint and facial mapping data from users and create a login key for the user's Microsoft Account. Security vulnerabilities that in the fingerprint and facial recognition will be tested for using methods from previous works. The usability of the interface will also be tested under varying conditions in the laboratory and live test users will also rate the system. Results from the experiments run show promising signs for the security of the protocol in commonly known methods for bypassing both fingerprint and facial recognition.**

I. Introduction

Technology has brought about the ability of using our own bodies as keys to lock information from those who wish to steal it. These are known as biometric keys and they consist of fingerprints, retina scans and even 3D mappings of facial structure. These innovations of bio-security have the potential to drastically change how a user may interact with their devices. Microsoft has announced a foray into the world of consumer and enterprise level bio metric keys with the introduction of its Windows Hello Authentication system which allows users to log in to their Windows 10 devices using either their fingerprint or face. The goal of this research study will be to test these systems for vulnerabilities as well as run usability tests to try and understand how a common user might better interface with these new keys.

Since the introduction of fingerprint scanners to the market at large thee have been numerous exploitations demonstrated by hacking groups across the globe. One of these attacks comes from the German hacker group known as the Chaos Computer Club, referred to as CCC. CCC was successful in demonstrating the potential for exploitation in Apples Touch ID protocol [1,2]. This attack and attacks like calls these systems into question and the vulnerability of any system released to the public should be well tested and exposed. Without holding these systems accountable the problem of easily exploitable devices will only continue to grow. Consumers will be in danger of losing their data to thieves of various motives. It is an essential that exploits are tested so that better, stronger systems can be built.

Throughout this paper the system that is being tested will be described as a Windows Hello Environment. Such an environment will consist of the following: A laptop capable of reading fingerprints and facial scans using a built in 3D infrared camera and a fully licensed version of Windows 10. No additional software or hardware is needed.

The key contributions of this paper are as follows:

- Describe methods of previous fingerprint spoofing methods that have been used to successfully bypass the fingerprint scanner of other devices. These same methods were tested in a laboratory environment and the results of such experiments will be presented. Previous works will be used to demonstrate the success or failure of these methods in other instances as they relate to a Windows Hello environment [1-7].
- Describe methods of spoofing facial recognition by citing previous works in this area. These methods have varying degrees of success and some could easily be applied to a Windows Hello environment. A small amount of experimentation was also done in the laboratory and results of such experimentation are presented[9-13].
- Define a protocol to run a usability test with users in a real setup scenario of the Windows Hello Environment. This protocol was constructed by following usability testing guidelines typical of an in-depth testing of real users [14]. The methodology, hypothesis and results of these usability tests will be presented.
- A conclusion which looks at the tests as a whole and delivers a verdict based on previous work and testing in regards to the security and user experience of the Hello Environment. In addition better ways of testing will be proposed in order to facilitate more research into this growing security protocol.

II. Fingerprint Security

With spoofing, an attacker can use an artificial finger to fake the sensor and gain access to the device. Faking fingerprints may be achieved by lifting fingerprints off of something the victim has touched, and subsequently copied by using special materials. This is similar to leaving a key to a safe out in the open, allowing any would be assailant to press the key, leave the original, and get a copy of it manufactured thus compromising the security of the safe. This gives the hacker complete access to the device without the user ever knowing how or when access was gained.

The threat of residual data can be exploited by hackers in a variety of cases, even teenagers trying to get out of class. In 2010 When teenagers used a hack discovered by a security researcher involving gummy candies on the fingerprint scanners in their Australian school to fool the roll call devices setup for senior year students [3]. Similar to the physical lock and key, residual templates are the digital equivalent of leaving your house key hanging outside on the lock.

B. Tawil is an undergraduate student at the Department of Electrical and Computer Engineering, Rutgers Engineering, New Brunsick, NJ 08854 USA e-mail: (bt238@scarletmail.rutgers.edu).

The main goal of finding various methods was to try and first establish some sort of baseline test where success could be easily met under certain conditions. After finding this baseline more complicated methods could be built upon until a real world scenario can be closely replicated. In a realistic attack the attacker should only need a few moments with the device before being able to successfully spoof the device.

A. Chaos Computer Club Method

When trying to establish a baseline for testing various methods of fingerprint spoofing attack the hacking group known as CCC was the first place to look. CCC had successfully created a mold that could spoof the fingerprint sensor on the newly released IPhone 5S [1]. This method was the first step in trying to find a suitable baseline as it involved relatively small amounts of materials and started a motivated foray into spoofing methods [4]. In short the CCC used graphite powder to get some sort of contrast on the prints and its surrounding surface. By taking a high resolution picture of the print they were able to successively print it out onto a sheet of film paper using a typical laser print. With this a mold could be easily set in using wood glue. Once the mold was set it could be used to spoof the Touch ID sensor on the IPhone.

An important aspect of the CCC method is for its reliance on the collection of what are known as Patent Fingerprints. Patent Fingerprints are what can easily be identified as a fingerprint with the naked eye. They are clear and often contrast nicely on the surface with no signs of smudging or damage. These stand in contrast to Latent Fingerprints which are what most attackers would work with in a real situation. Latent prints tend to be lifted off of rough surfaces with slight smudging in areas around the print and damage that has to be repaired later using photo editing software [5].

These tests followed the same methods as the CCC when lifting the prints and attempted to collect data on a number of prints. [4]. The steps used to make the mold are as follows:

1) With a fingerprint placed on the surface of the laptop use a sprinkling of Graphite powder and brush over the print.
2) Using a high definition camera, such as one found on a modern smartphone, take a clear picture of the print.
3) Use photo imaging software such as Photoshop or the freely available GIMP to clear out any defects. The print should be edited to have a high contrast between ridges and background.
4) With a dark fingerprint edited in front of a white background.
5) Print the edited image using a laser printer to form a set of ridges onto thin film paper.
6) Create a mold by spreading wood glue over the print to form a nice even coating.
7) After roughly 30 minutes of drying time, cut and peel the mold off of the paper.

A set of 10 fingerprints of the right index finger were collected from 10 different points on the laptop. 5 were collected from the trackpad while 5 were collected from resting area where the palm rests. There were 2 iterations of testing for a total of to 20 prints created using the above method.

The results of this testing shed some positive light on the security of the system. Through the 20 prints, none were able to spoof the sensor. When the system is met with a live print that does not match there are prompts that come up displaying how to better swiping the finger for verification as detailed later in the paper. Through these 20 prints only 7 prints were even received this feedback with the rest showing no feedback from the system. This 0% success rate was impressive and instigated a search into discovering new methods of exploitation.

Problems with the above described method arose from the sturdiness of the mold. In the sensors spoofed by CCC a single pressing of the finger was all that was required [1]. However the Windows Hello Environment has hardware that requires a quick swiping of the finger. This quick motion would often result in a tear or smudging of the print within a couple of tries. Prints were lifted off of multiple locations on the laptop and image editing will not pose a significant learning curve for even an amateur.

The most promising prints were often ones that were collected very carefully. The prints that were recognized as live would also tend to be thicker than the molds that failed. The success of this method should not be ignored and the possibility of perfecting this method still exists. However the skill and experience level needed to consistently create high quality molding may be left for the more determined of hackers.

B. Conductive Ink & Paper Method

Other methods used in the lab involve recent developments with conductive ink and paper. Recent studies have seen researchers being able to spoof the mobile fingerprint sensors on phones like the Samsung Galaxy S6 and the Huawei Honor which use similar sensors to the IPhone [6]. The procedure is rather simple as it involves taking Patent Prints and capturing them onto the conductive paper using conductive ink. Conductive materials are used so that the capacitive sensor will read the print as live.

The collection of the print form the CCC method is the same but the creation of the mold varies.

1) Follow steps 1) through 4) on the above described method.
2) If available print the fingerprints onto conductive paper using conductive ink.(If a printer cartridge is not available it is sufficient to spread the ink onto the finger and collected a patent print by rolling onto the conductive paper.)
3) Let the print dry and use a thin blade to cut the print from the paper.

In this attempt the same brand of ink and paper was used although on a much smaller scale and data set. Using 20 prints in the same manner as the CCC method but the prints were

rolled directly onto the paper. Once again the experiment was met with a 0% success rate with only 8 out of the 20 prints being read as live.

The failures of the conductive ink test point to a problem in the collection methods and the formation of a valid spoof. The steps used to lift the print have been demonstrated in previous works and scenarios to hold true [4]. However converting the collected print into a physical spoof presents difficulties when applied to the Windows Hello Environment. The hardware of the fingerprint sensor is most likely playing a big role with advances in sensors over the course of the past decade hampering spoofing attempts. But a possible cause may lie in the algorithms present in Windows Hello where Microsoft has written a comprehensive fingerprint recognition algorithm. The failures encountered in testing may very well be as much of a software problem as it is a hardware priblem. But the closed nature of the Windows Hello protocol leaves the question of a root cause for failure hanging in the air.

C. Untested Methods

The search for more methods brought up some more methods which are described below but due to time constraints on the rest of the project they were not able to be fully realized in the laboratory environment.

It may be worth it to look back to some of the earlier method of fingerprint spoofing. The use of gummy bears in spoofing fingerprints has been used in scenario more than a decade ago [7]. The use of gummy or variations of it to build upon the idea of using a gummy base to create a mold of the finger that can successively fool a Windows Hello Environment.

There is also a video detailed by CCC that shows a variation of their previously demonstrated method [8]. The video demonstrates printing a Patent Print onto a PCP board and getting the mold from its ridges on the board. This may provide a more defined print then a mold constructed from a laser printer and film paper.

D. Reasons for Failure

Throughout the testing of the fingerprint there was difficulty in establishing even a baseline case that could be built upon. None of the tests showed any signs of success and potential tests all suffered from common points of failure to those already tested.

The most pressing issue with the tests used is with the hardware of the Windows Hello Environment. Previous methods have been used on sensors that have a passive scan method of the finger. This can be seen as a more classical scanner where the user simply places their finger on a sensor and access is subsequently granted or denied. The Windows Hello Environment however is an active fingerprint sensor meaning a quick swiping motion is required. As such the methods that rely on wood glue molds are at a disadvantage as the mold can quickly break up and scratch after a single use. However

Fig. 1. The Hello Environment(left) uses an active scanner while the Apple TouchID(right) uses a passive scanner.

the overall body of work in the field of fingerprint spoofing leans heavily towards testing passive scanners.

More resources and access to better equipment and skills may also lead to a better result. A more experienced hacker might be able to come up with a more precise method of spoofing an active sensor without using a breakable mold.

III. 3D Camera Security

The technology that allows for facial recognition is also a ripe candidate for exploitation and spoofing. Since the public release of the Microsoft Kinect camera there has been a growing trend towards using 3D camera technology outside of the Games industry. Windows Hello represents a new direction for consumer level biometric authentication. However there are security exploits that have been demonstrated in various capacities that can easily fool these consumer grade products. In these instances of attack the attacker does not even need access to the device to get sensitive information ready for future attacks. The attacker merely needs to sample photos and videos on social media in order to construct the identity of the victim.

A. Laboratory Testing

The establishment of a baseline for the camera started off with the intent of getting the simplest information possible in order to facilitate an attack. For this a 2D photo of the users face was printed at a high resolution both in color and gray-scale. This 2D photo was both kept 2D and also wrapped around a 3D object to simulate a 3D surface. But through all attempts no recognition could even be made. So it stands to reason that the main algorithm relies heavily on depth and liveness of the user.

From here the next step involved finding the areas of the face that are used in the recognition algorithm. Once this information was found a proper minimum could be established and it would be possible to construct a proper baseline. In order to properly test where the face was used to setup the facial recognition while 1 of the 8 regions as shown in the figure above was obstructed.

The results of this experiment showed that when regions 1-4, 6 or 7 were obstructed the setup failed. It thus stands to reason that Windows Hello uses the central part of the face in order to determine the identity of the individual.

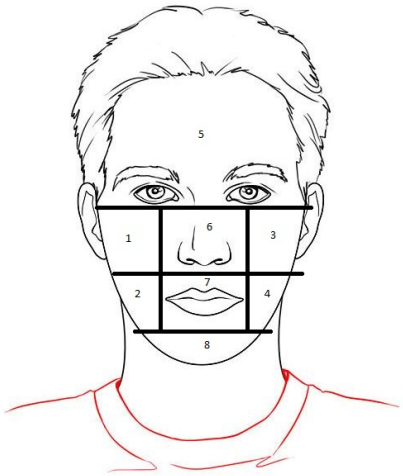

Fig. 2. The 8 regions used in the initial testing of obstructions.

B. Related Works

There have been many previous works that have set out to establish the security of 3D facial recognition systems. The possibility of taking a 2D image and wrapping across a 3D surface for spoofing is a difficult challenge that some have undertaken [9]. While this challenge that a normal hacker may not undertake it should still be noted that these systems are vulnerable to these methods. There has been research in this area as brought upon countermeasures that rely on a combination of liveness and facial structure, as it appears to be the case with the Hello Protocol [10]. The reliance of facial structure and positioning is at the core of the algorithms calculations as to whether the user is able to authenticate.

But there are still attacks on the Hello system that could not be carried out that show definite promise. The time old classic of wearing a mask to fool your friends may even be enough to fool Hello and other facial recognition protocols. Services like thatsmyface.com can turn a couple of head-shoot photographs of a face into a realistic mask [11]. There has already been work in this area to use this publicly available service to create masks for spoofing attacks [12]. The threat is magnified extremely when one takes into the account the increased availability of head-shoot and side-shoot photos of an individual due to the rise in use of social media platforms.

C. Implications on Hello

The more a user keeps his face out in public and on the Internet the less secure their face is an authentication factor. With these works and information in mind it is important to realize that the face should not be taken as an infallible and singular security measure like it is taken in the Windows Hello protocol.

IV. Usability

This section of the paper will seek to discover if Microsoft has built a good user interface and experience so that users could properly secure their devices using Windows Hello.

A. Interface

Windows Hello keeps the modern Metro style that Microsoft has thrust upon the Windows 10 Operating system. Prompts use simple language common amongst consumer level products with prompts using simple language and text. The setup for Windows Hello is in under the sign-in options in the settings menu and is easily search-able though the start menu.

B. Hardware Limitations Testing

In order to best gauge the typical Windows Hello Environment it would be optimal if a wide range of platforms using different sensors and cameras could be used. There were limitations in the resources and as such the experiments of the hardware were limited to the Lenovo E550 with its Intel RealSense F200 camera and fingerprint scanner. The first test was to see how the camera stacked up when presented with physical limitations such as lighting differences, facial accessories and variations in angle and orientation.

The lighting was an interesting test as the camera was able to authenticate regardless of the light level. Upon further investigation the camera uses infrared red light to measure the depth. It is possible that the Hello Protocol uses Infrared Light to measure the depth in a similar, or even exact, method as the Microsoft Kinect. The Kinect is able to do so by emitting a structured light and capturing the resulting light bouncing back [13]. This structured light is in essence a 2D grid being projected out of an infrared blaster. When that infrared hit an object it subsequently bounces backwards and using the infrared camera the distance can be calculated based off of the time of arrival. This represents an amazing use of computer vision but because of the closed source nature of Windows Hello and its algorithms it is impossible to determine how much of the Kinect is actually influencing Hello.

There was also the question of obstruction of the face due to common facial accessories such as glasses, hats or masks. The tests that followed were based very much on the previous facial obstruction tests as shown in section 3. In these tests the Hello profile was setup with variations of accessories 3 separate times between a hat, glasses and sunglasses for a total of 9 sign in attempts. The user was then tasked with signing in without any accessories on. It was hypothesized that only the sunglasses might pose an issue with the facial setup. In actuality none of the above accessories posed any difference in sign in attempts when the face was clear resulting in a 100% success rate.

This process was also reversed with setup being made using a clean face while sign-in was made with one of the accessories on. Again there were 3 accessories spread with 3 attempts each. The results showed that sunglasses presented some difficulty in the sign in one attempt leaving the tests with an 89% success rate.

The effects of angle and orientation were also tested against the camera. The face is able to be recognized at around a 30 degree angle with respect to the laptop's face. This also appears to be the point where the opposite side of the face

eclipses the cheek on the other side which accounts for the failure to authenticate.

V. Usability Test

To better establish a rating of the usability of the Hello Environment a group of 3 test users was brought in in an attempt to better understand what a typical user would do in this environment. The usability test is separated into 2 parts: (1) user tasks (2) interview questions.

A. Protocol

To better establish a rating of the usability of the Hello Environment a group of 3 test users was brought in in an attempt to better understand what a typical user would do in this environment. The usability test is separated into 2 parts: (1) Pre-screening (2) User tasks (3) Interview questions.To record the answers and data for the usability test a proctor would stand by the user to record the data and also make sure the test would run smoothly.

The first step was to establish the experience level and initial bias level of the user in regards to Windows, Hello and biometric security in general. If a user is more experienced in one or more of these aspects it may skew results and as such it is important to establish a standing of where users are [14]. The questions were specifically:

- Is Windows 10 your primary OS? If not how much experience do you have with it?
- Do you use fingerprint or facial identification on any device? If so, where?
- Based on current experience would you rather use a password you created or a fingerprint/facial scan?

The User Tasks consist of setting up the Windows Hello Environment for fingerprint and Facial Authentication from the desktop screen of Windows 10. These tasks were timed and rated with a binary response to questions Task Completed? and Task Difficult? User comments were also recorded down when significant. The users were encouraged to seek answers themselves without interference from the proctors. Letting the user figure out the interface for themselves allows for the continuity of the test [14].

After successful completion of the tasks the proctor would ask the user a series of interview questions to better gauge their experience and thoughts about the technology after the tests. The main goal of these questions is to establish a future outlook for the typical user after the setup. If the system has an inherent flaw that prevents users from continuing to use the Hello system in the future [14].

After successful completion of the tasks the proctor would ask the user a series of interview questions to better gauge their experience and thoughts about the technology after the tests. The main goal of these questions is to establish a future outlook for the typical user after the setup. If the system has an inherent flaw that prevents users from continuing to use the Hello system in the future [14].

Following the successful completion of the tasks, the user was then asked a series of interview questions to better measure issues and problems with the Hello Environments interface and experience. The series of questions asked were:

- Would you purchase a laptop like this and use the biometric sign in options?
- Would you want to use this technology for signing into a website or application in the future?
- How secure do you believe the system to be?
- How does this interface compare to other biometric security systems that you have used(TouchID)?
- Do you have any specific concerns with the interface?

Before the initial testing of the Hello Environment it was hypothesized that uses of the system was rather simple. The security interface of Hello appeared to be consumer driven from the start with simple on-screen prompts and a modern interface common of Windows 10 applications. In the worst case Hello was believed to be annoying and difficult to setup but only as much as a 2-3 minute inconvenience in trying to find the correct settings.

B. Demographics

Demographics wise the 3 test users tend to skew young as they were pulled from current undergraduate students ranging in the typical age of 18-24 years old. Of the 3 test users 2 identified as male while the third identified as female. No information regarding name, address or other personal forms of information was collected.

The test users will be referred to as U1, U2, and U3. U1 and U2 were the male test users with U3 being the lone female test user.

C. Screening Questions

Upon arrival of the test users the screening process revealed an interesting commonality amongst all participants. All three test users have used or currently use some form of biometric authentication on another device. U2 and U3 have experience with Apples TouchID feature on the Iphone while U1 has experience with the fingerprint capabilities of the Galaxy S6 although he is quoted as saying I never use it.

U2 and U3 also typically use MacOS as their primary operating system but are still familiar with the Windows 10 operating system. U1 list Windows 10 as his primary OS.

The use of fingerprint authentication covers a wide range amongst these 3 test users. As previously mentioned U1 does not currently use his fingerprint for authentication and prefers the use of a 4-digit PIN number. U2 is an active user of the TouchID feature on his IPhone and lists his fingerprint as the primary way of unlocking the device. U3 uses a mixture of security methods sometimes opting to use fingerprint instead of a PIN number the depending on the situation. These situations were quoted as if my other hand is busy then I will most likely opt for the fingerprint. As a summary U1 does not use biometric keys, U2 actively uses one and U3 uses it for convenience.

D. Testing Results

After completion of the screening questions the test users were given the task of setup. The times as well as binary results of completion are listed in the table below.

Test Results			
Test User	Time	Success?	Difficulty?
U1	0:42	Yes	No
U2	0:56	Yes	No
U3	3:15	Yes	Yes

Fig. 3. The table of results following the user tasks. Time is measured in Min:Sec with feedback on completion and difficulty.

U1 and U2 experienced little to no difficulty in setting up their fingerprints and face in the Windows Hello Environment. The majority of their time was spent following on screen prompts for setting up biometric keys. Both users expressed satisfaction with the interface for the on-screen dialogue.

U3 had a much more difficult time with the setup and spent a large amount of time attempting to setup fingerprint sign-in. Reaching the option through the menus did not take an appreciable amount of time, but upon being prompted by Windows Hello to scan her fingerprint there was confusion. The prompt, shown below, is signifying some sort of swiping motion to be made. U3 was quoted as saying Why is this fingerprint reader not working? U3 was simply placing her finger over the sensor without any swiping motion. To U3 the necessity to swipe across the reader was not apparent and protested on multiple occasions Its not telling me what to do! Eventually U3 did reach the conclusion of the test with a successful completion of the task but not after various expressions of frustration in the prompting system.

After inquiring further the reason for U3's confusion lies in a combination of prior knowledge and ambiguous prompting. None of the test users had used readers that require active motions up until that point. The prompt above was correctly interpreted by U1 and U2 as to mean some sort of swiping motion was needed. U3 however was unable to get this meaning at first and often criticized the interface.

E. Interview Questions

After completion of the tasks the interview question presented a more thorough perspective of the users about their experience with the Hello Environment. These questions were meant to capture user perception of Windows Hello and gauge how much they felt comfortable with it. These questions also attempt to understand the impact that Windows Hello made on their outlook on biometric security measures as they apply to consumer products. The following quotes and answers were gathered from the questions described above

All 3 users expressed that while they successfully setup the Windows Hello environment, they are not looking for a laptop with these capabilities. U2 was quoted as saying It seems cool but there really is not much of a reason to get it. Users U1 and U3 expressed similar feelings and showed a lack of enthusiasm

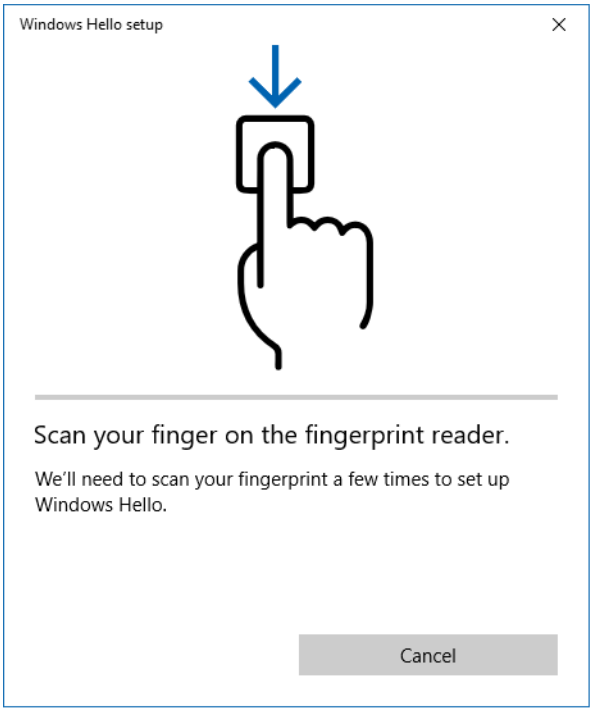

Fig. 4. The Windows Hello fingerprint scanning prompt.

for the prospect of getting a Windows Hello compatible laptop for themselves.

After asking whether this protocol would be more appealing if web and application sign-ins could be done using Windows Hello only U1 expressed interest. U1 expressed that such capabilities would be very interesting but I am not sure if I would use it for shopping online. U3 did not take much care to the prospect and brushed off the idea as not a big draw for me. U2 did show slight interest but wanted to see a full implementation before making judgements.

When asked about the relative security of the Hello system U2 and U3 believed that the use of fingerprints or facial recognition were both more secure than a password or PIN number system. U2 was rather stern in his belief that fingerprints are very secure and a much better alternative to passwords. U1 proposed an interesting prospect stating that while he believed they were secure he questioned Why isnt there a way of combining both the fingerprint and my face to unlock the laptop? After all I am sitting in front of it no matter what. This combination was an interesting proposition and one that has been discussed in previous works [15].

After the conclusion of the Interview questions and comments or concerns were addressed and an overall summary of their experience was asked for. U1 stated that while Windows Hello shows some promise it still does not present much advantage over a good password. A system that combines multiple metrics is promising but U1 still feels that Hello has a long way to go. U2 was also hopeful for the future of

biometrics but exclaimed It feels more natural on the phone. Using it on a laptop feels clunky and restricting, my phone works better. U3 was unsatisfied with the on-screen prompts and was the strongest opponent of the Hello system. According to U3 there should at least be some sort of animation or simple way of conveying the motion necessary. The chances of U3 using or recommending Hello are Basically zero.

VI. Conclusion

Through various testing and research of past works it is not explicitly apparent whether Hello is an improvement on previous iterations of biometric key protocols. The testing of fingerprints using previous methods shows a 0% success rate for spoofing attacks, but it may be a result of the hardware of the active fingerprint scanner rather than ny underlining algorithms. Future works and attempts should probably focus on how hardware played a difference in the fingerprint security and more experienced bio metric researchers may be needed to establish a baseline.

While the facial recognition security was tested as well the amount of available resources did not permit for the testing capabilities of previous works such as [12]. These methods described in prior works should be applied to Windows Hello to truly figure out how robust the underlining algorithms are.

The usability of the Hello system is promising based on the laboratory tests and user cases. The ability to use Hello's facial functionality with many combinations of accessories and in varying lighting scenarios speaks well for its camera technology. The fingerprints may experience issues with users who have had small amounts of experience with other fingerprint systems but a larger data set is needed to determine this. The test users revealed the perception that Hello does not add much to the security of the laptop and may even appear as an unnecessary annoyance. A combination of fingerprint and camera measures into a single key may help Hello out if implemented correctly.

Acknowledgment

I would like to thank my advisers Dr. Janne Lindqvist and Gradeigh D. Clark for their tremendous support throughout the course of this project.

References

[1] "Chaos computer club breaks apple TouchID," 2017. [Online]. Available: https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid.

[2] M.Rogers,2013.[Online]. Available: https://blog.lookout.com/blog/2013/09/23/why-i-hacked-apples-touchid-and-still-think-it-is-awesome/.

[3] Smith, G. 2013. iPhone Fingerprint Scanner Comes With A Catch http://www.huffingtonpost.com/2013/09/10/iphonefingerprint-scanner_n_3900529.html

[4] starbug, "How to fake fingerprints?," Chaos Computer Club e.V, 2004. [Online]. Availible: http://dasalte.ccc.de/biometrie/fingerabdruck_kopieren.en

[5] C. Marshall, Ed., Handbook of Bioinformatics. United States: Callisto Reference, 2015.

[6] K. Cao and A. Jain Hacking Mobile Phones Using 2D Printed Fingerprints, [Unpublished], February 19, 2016

[7] T. Matsumoto, H. Matsumoto, Impact of Artificial "Gummy" Fingers on Fingerprint Systems, Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, Thursday-Friday 24-25 January 2002

[8] Heise online, "The iPhone 5s touch ID hack in detail," YouTube, 2013. [Online]. Available: https://www.youtube.com/watch?v=bvRK7XDvTOk

[9] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using texture and local shape analysis," IET Biometrics, vol. 1, no. 1, p. 3, 2012.

[10] A. K. Singh, P. Joshi, and G. C. Nandi, "Face liveness detection through face structure analysis," International Journal of Applied Pattern Recognition, vol. 1, no. 4, p. 338, 2014.

[11] [Online]. Available: thatsmyface.com.

[12] N. Erdogmus and S. Marcel, "Spoofing face recognition with 3D masks," IEEE Transactions on Information Forensics and Security, vol. 9, no. 7, pp. 10841097, Jul. 2014.

[13] Z. Zhang, "Microsoft Kinect sensor and its effect," IEEE Multimedia, vol. 19, no. 2, pp. 410, Feb. 2012.

[14] J. Nielsen, Usability engineering (interactive technologies). San Diego: Morgan Kaufmann Publishers In, 1993.