

CSE 5349 – 001

SPECIAL TOPICS OF NETWORKING

PROFESSOR: VP Nguyen

TA: Abir Tasnim and Amir Radmehr

PROJECT REPORT

Problem Statement: How secure is your Faceprint?

BY

Sai Krishna Prateek Nam (1001880903)

Pratik Chavan (1001963580)

Parth Chodvadiya (1001865625)

Table of Contents

Introduction.....	1
Agenda.....	1
Case Study.....	4
Apple FaceID	4
Windows Hello	8
Government Policies	9
Analysis.....	11
Proposed Solution.....	12
Conclusion.....	12
Reference.....	13

Introduction

So how far do you think the companies go to protect your faceprint? Generally, most people blindly trust companies to keep their data secure by agreeing to accept the terms and conditions without even reading them.

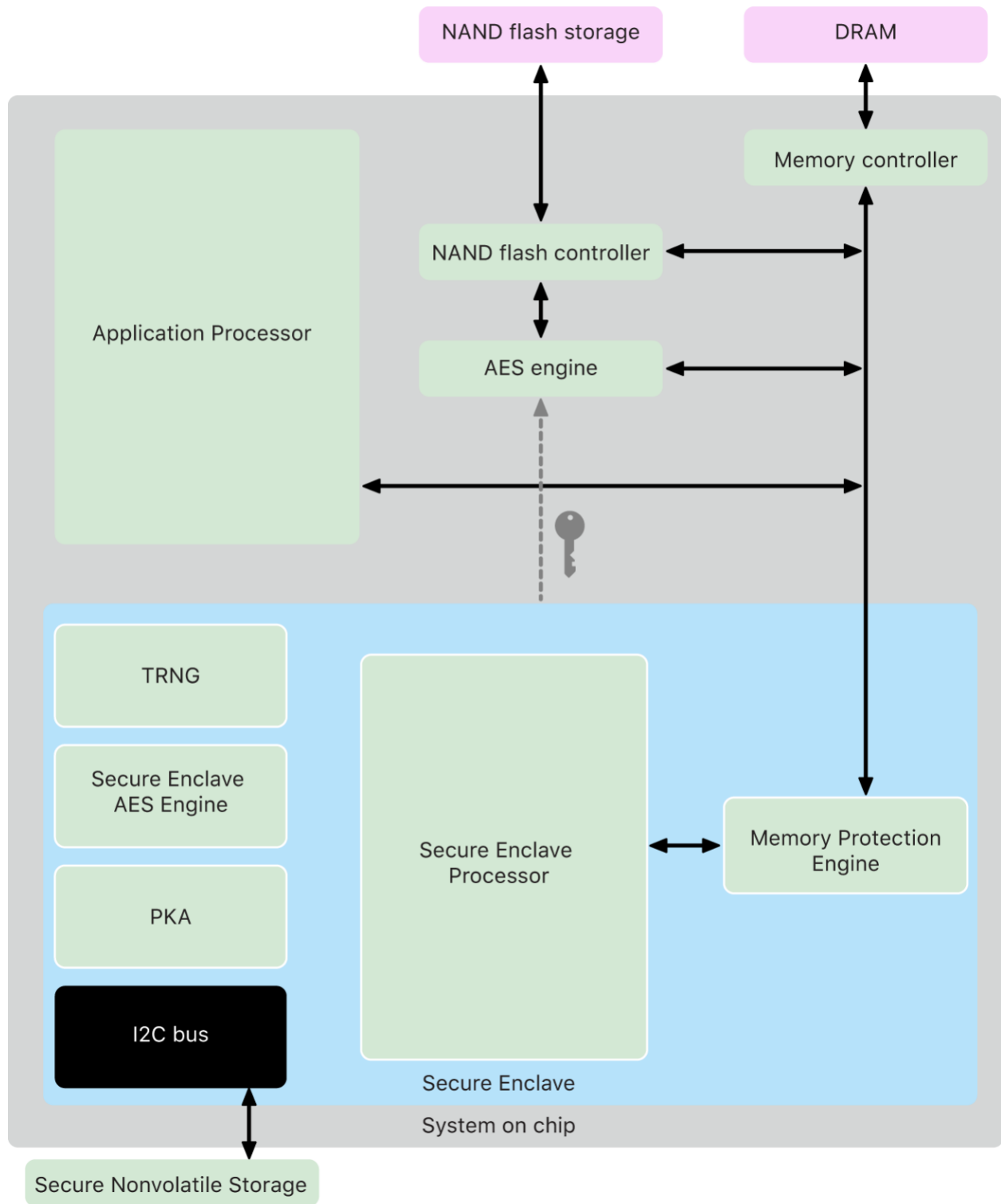
Modern AI has the capability to construct a 3D model of our face from our pictures. The constructed model can be used to unlock your smartphone and impersonate someone to gain unauthorized access. Lately, Apple has been compelled to use FaceID as means to secure your phone, payments, and security to applications. By exploiting FaceID which is the core authentication on our devices, bad actors can gain access to all the applications that use FaceID. Our facial data is not only limited to phones because we have freedom to use social media like Facebook, Instagram and TikTok where user uploads variety of photos and videos. Now a days there are very powerful and advance AI and ML models which can take those 2D image as an input and will give the 3D face model with sufficient accuracy from which bad actor can get the faceprint which later can be used to perform some unauthorized activities on behalf of the actual users. Generally, newbies or individual can use this kind of algorithm to get user's face then image what these big companies can do with all these data and their huge resourcing power. In that case how can one trust the social media companies and what if they misuse your data? As an ordinary user, we don't have that much power that we can oppose the company to do something, but government has that power. So, what are the prevention steps that could have taken which are them are implemented by the government?

Agenda

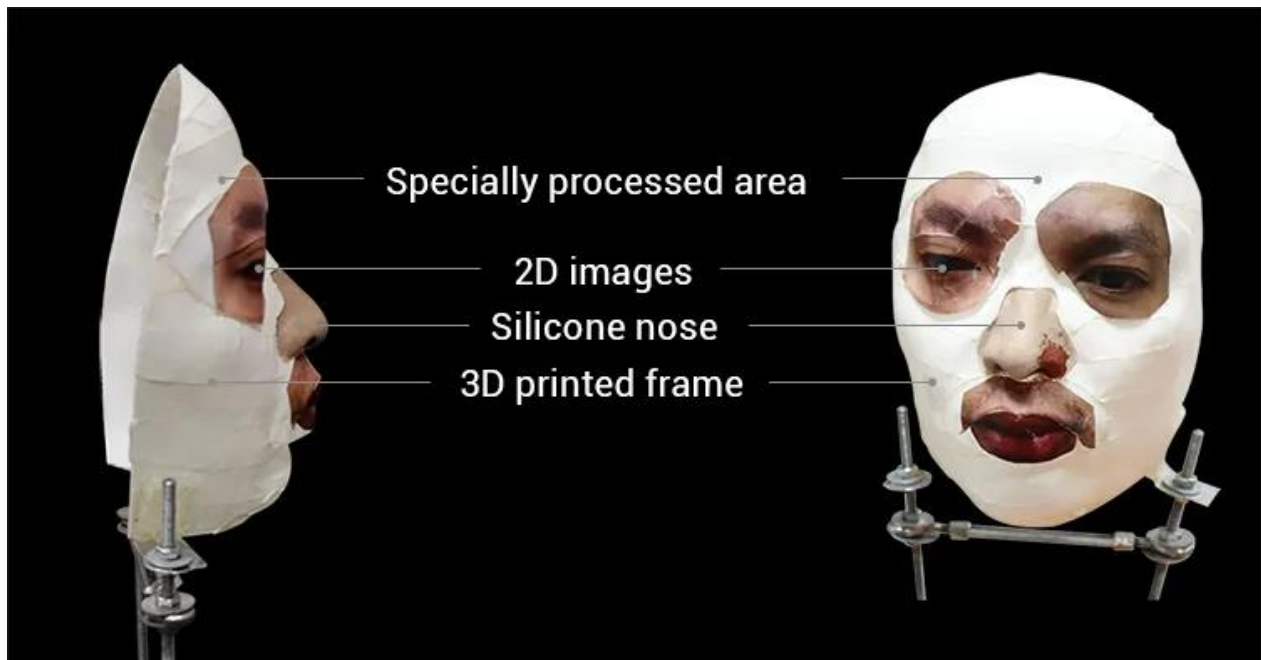
Our main goal is to compare current approaches implemented and different policies established by the companies and governments, leading to writing a brief report on how to improve the drawbacks that can be the way to protect their data or policies.

Case Study

Face ID: We know the popularity and efficiency of face ID, it's fast and secure then most of the FR locks. Apple claims that it's "face ID is intuitive and secure authentication enabled by the state-of-the-art TrueDepth camera system with advanced technologies to accurately map the geometry of your face." and "Face ID is less than 1 in 1,000,000 with a single enrolled appearance whether or not you're wearing a mask", so apple has added a special camera for capturing face and have a dedicated processor just to process the faceprint. The architecture is simple, the dedicated processor is called as secure enclave which doesn't have any connection to the application processor or with any other components except the memory protection engine. Memory protection engine a component which has multiple layers of protection and Along with the encrypted memory, the Memory Protection Engine saves the authentication tag. The Memory Protection Engine checks the authentication tag when the Secure Enclave reads the memory. The Memory Protection Engine decrypts the memory block if the authentication tag matches. The Memory Protection Engine alerts the Secure Enclave to an issue if the tag doesn't match. The Secure Enclave pauses accepting requests following a memory authentication error until the system is restarted. Supports the encryption and signature techniques RSA and ECC (Elliptic Curve Cryptography). The PKA is made to withstand timing and side-channel attacks like SPA and DPA that aim to leak information.



With this strong protection architecture, it's hard to crack the Face ID through hacking. But is it not still secure, software hacking is not the only threat to crack Face ID. In a blog post and video, the Vietnamese security company Bkav claimed that they had successfully circumvented Face ID using a composite mask made of 3-D-printed plastic, silicone, cosmetics, and plain paper cutouts. This mask fooled an iPhone X into unlocking. That demonstration, which other security researchers have not yet publicly corroborated, may compromise the pricey security of the iPhone X, especially because the researchers claim their mask only cost \$150 to manufacture.



In less than 120 seconds, the researchers were able to access the victim's iPhone by getting beyond FaceID user authentication. They required three items to accomplish this: a pair of glasses, some tape and an iPhone user who was dozing off or otherwise unconscious. The researchers discovered a bug in Apple's biometric authentication system's liveness detecting feature, which is used to unlock iPhones using FaceID. According to a report from Threat post, the researchers claimed that liveness detection has turned into the weak point in biometric authentication security because it must be checked to see if the biometric being taken comes from the authorized live person who is present at the time of capture.

The algorithm used by FaceID to determine liveness was found by the researchers to not fully collect 3D data from the region around the eye if it detects the wearer is donning glasses. Instead, it seeks a black area for the eye and a white point for the

iris on that location. Because of this, the researchers made a pair of glasses with a white tape frame and a black tape center. The "white spot" was visible to FaceID because of a gap in the black tape. This is sufficient to deceive FaceID and unlock the iPhone.

However, it's also the last time you can refer to the hack as "simple." Yes, the researchers demonstrated how they used "X-glasses" to put a "sleeping" victim in a locked iPhone to send money via mobile wallet. But in the actual world, you attempt to achieve that. It's not impossible by any means, but you need a sleeping or unconscious victim with an iPhone with FaceID protection who won't wake up when you put a set of glasses on their face.

Security safeguards

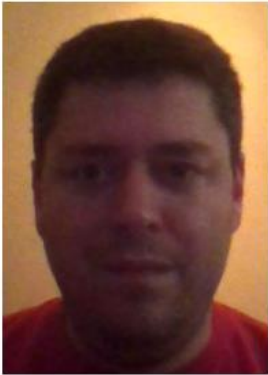



To use Face ID, you must set up a passcode on your device. You must enter your passcode for additional security validation when:

- The device has just been turned on or restarted.
- The device hasn't been unlocked for more than 48 hours.
- The passcode hasn't been used to unlock the device in the last six and a half days and Face ID hasn't unlocked the device in the last 4 hours.
- The device has received a remote lock command.
- After five unsuccessful attempts to match a face.
- After initiating power off / Emergency SOS by pressing and holding either volume button and the side button simultaneously for 2 seconds simultaneously.

Windows Hello face authentication:

Windows Hello is identity verification mechanism that is integrated into the windows 10/11. It uses an IR imaging to authenticate and unlock the device.

In primary scenario like Authentication windows hello algorithm takes less than 2 sec to unlock. Windows hello is so flexible that it can use external IR camera as primary input.

Scenario	Color Image from integrated Camera	IR Image from Microsoft Reference Sensor
Low light representative of watching TV or giving a PowerPoint presentation		
Side lighting when sitting near a window or desk lamp		

Source: <https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello-face-authentication>

Windows Hello requires user to have RGB sensor and IR sensor camera for detection.

How does the information from the sensor is made useful? There are basically 4 steps involved by the Windows facial recognition engine. First the algorithm detects the user's face in the camera and tries to find alignment point (like eyes, nose,

mouth). Next it will verify the alignment of the face so that it can make fair decision. It ensures that face is facing the camera and within +/- 15 degrees angle. Then using landmark location as anchor points, the algorithm takes thousands of samples from different areas of the face to build a representation. So basically, at the lowest level it is histogram representing the light and dark differences around specific points. Lastly for decision engine once the user is in front of the sensor it is compared with the representation of the enrolled user. Also, the matching should cross a certain threshold to accept it as a match.

How can this be exploited?

There are many attack surfaces in case of facial recognition systems, But the one that is easiest in case of windows is through use of external camera. The easy way is to replay the video of the enrolled person using a USB cable which will be pretending to be an IR camera. The windows Hello required the camera to be equipped with RGB sensor, but it does not use that as input. When performing this attack, the attacker sends the IR images of the Himself and RGB images of a cartoon SpongeBob SquarePants. The Video feed when played will open the device without causing any hassle or raising any alarms.

Government Policies: So far, we talked about how FaceID in Apple and windows works, what are the security safeguards in those mechanisms and how one can generate the mask from 2D to 3D and pretend to be someone else and tries to unlock the phone using masked face. This is not a new thing because people out there, they are interested in how things work and mostly how we can break down the things and brute forcing or trying to break down something has one positive side also. For example, we make the system open source so everyone can have access of it and more people will try to break down the things and many of them will succeed and they will report that issue to the company who developed the technology and can fix the loophole as soon as possible which prevent the company to suffering from zero-day attack.

There are variety of people outside and not everyone will report the issue to the company, but they can use to gain some finance out of it which become more dangerous. In case of facial data, one can easily get your picture from anywhere. For example, social medias like Facebook and Instagram, influencing became a job to most of the people and it is their main source of income and to make their pages more followed influencer generally uploads a lots of content like images and videos to their and mostly we can find the photos from all the angles plus from vides we

can easily get the face data. If there are multiple persons in the photos, then there is very high chance that the other person will be tagged in the post and from that information any malicious user as well as social media companies gets the facial data. The legal problem of new technologies removing our right to privacy is not a recent one. A young Boston based lawyer, Louis Brandeis in 1890 co-wrote a Harvard Review article saying that Privacy is the fundamental right of the public even it is not listed in US constitution. *“Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the house-tops.”*^[5]. To protect the use of collected facial data by these companies, facial recognition technology should be accompanied by policies and guidelines. No doubts that these data is very useful in some cases like to thwart potential terrorist attacks, to solve some sensitive crimes, to help finding and rescuing human trafficking and finding missing person etc. So, the policy should describe who is authorized to use the facial recognition system and under what circumstances and provide indication that human review is required.

To protect the data and privacy related to Facial Data, Illinois came with a Biometric Information Privacy Act (BIPA)^[6] in 2008. Under the BIPA, the government of Illinois ensures that individual is owner of their own data and tech companies can not collect that data unless they get the provide the user with information of what data is being collected and in which form, they are storing their data plus a written consent from the user. The BIPA remains the most stringent biometric privacy law in the country and is the only one of its kind to provide consumers with protection by enabling them to sue businesses that break the law in court. Main tech firms like Facebook, Google, TikTok has been sued by under the violation of BIPA and ended up giving settlement amount and changing their privacy policy regarding of collecting and using biometric data. After that there are some more states who acted against the use of Facial Recognition Techniques which are as follows.

- In 2021, New York passed a law to restrict the facial recognition in schools.
- Washington state passed the law that government agencies cannot use facial recognition unless they have warrant.
- New Hampshire passed the law to limit the government agencies to use biometric data to solve a crime case without warrant.^[7]
- Maryland restricted the employers for using facial recognition during interviews without consent.
- California passed a law to prohibit the use of facial recognition in on body cameras of police.

Below are some guardrails which got achieved by applying the above regulations:

- Permissible Use
 - Only actions that are compliant with constitutional safeguards for civil liberties and rights may be taken using FRT.
- Transparency
 - Choosing when and how to inform the public that FRT is being utilized is part of transparency.
- Consent and Authorization
 - Asking permission and consent even before collecting the data.
- Data Retention
 - Tells the users about how the data is captured and how data is being used.
- Autonomous Use
 - FRT can be autonomous when used for identity authentication, such as when gaining access to federal benefits or during border entrance and exit procedures, provided its use is transparent.
- Oversight and Auditing
 - Auditing like which data was used by whom for which purpose.

Analysis

- First thumb rule for any faceprint is that the data is always stored locally and in encrypted form. This reduces the attack surfaces and enforces reliability.
- There are 2 most practiced approaches when it comes facial recognition. One is through RGB sensor, and another is IR sensor.
- The IR sensor is more versatile since it can work in different environments with different illumination variable.
- Even though apple FaceID has vulnerabilities, but these were addressed and fixed in later version so regular security update will improve the experience.
- Unlike other companies, Apple has implemented their faceprint technology independent of other internal hardware makes it unique and robust.
- In New Hampshire, government passed the law than in case of criminal activities, police can use FRT without warrant which is not hard evidence to use FRT against the defendant. At least a warrant should be issued which can consider as hard evidence to violate the privacy of the defendant.

Proposed Solution

Increase transparency: One way to manage the facial data used by the companies and the government firms are to increase the transparency with their customers data. Meaning using the data where it is supposed to be consented about. The company should provide detailed information about how the data is captured, for which purpose the data is captured, how they are storing the data, and for how much time they are going to keep the data.

Smart Accessories: We can use our accessories as key to unlock our device. The Accessory can be smart watch, smart ring, Smart Glasses...etc. It will work similar to 2 factor authentication. The device doesn't even have to be powered. It can have a tag which will act as key. Tapping the tag on the device will complete the authentication device.

Conclusion:

Using your face as a key is not ideal since you are exposing your face every day to everyone, and it is only a matter of time before your face would turn against you. To keep our data/devices secured it is best that we use password as your savior.

References:

<https://www.wired.com/story/windows-hello-facial-recognition-bypass/>

<https://www.groovypost.com/unplugged/can-you-trick-windows-hello-with-a-photo/>

<https://epic.org/state-facial-recognition-policy/>

<https://support.apple.com/guide/security/secure-enclave-sec59b0b31ff/web>

<https://www.wired.com/story/hackers-say-broke-face-id-security/>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34466>

<https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello-face-authentication>

<https://www.buzzfeednews.com/article/daveyalba/these-documents-reveal-the-governments-detailed-plan-for>

<https://www.womblebonddickinson.com/us/insights/alerts/facial-recognition-new-trend-state-regulation#:~:text=Several%20states%20and%20municipalities%20are,use%20of%20biometric%20identification%20tools.>

⁵ https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

⁶ <https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa#:~:text=BIPA%20is%20currently%20the%20one,women%20and%20people%20of%20color.>

⁷ <https://legiscan.com/NH/text/HB312/id/1024501>

<https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape>