CNT5410 – Computer and Network Security

Face Unlock: Android's Flawed Biometric

Justin Tomlinson

Abstract

Android biometrics are convenient ways for users to unlock their device by using some feature that is unique to them with a guarantee of security. While they have all improved significantly over the years, Face Unlock is still very much insecure. The fatal flaw that Face Unlock employs is relying solely on visible light, a mistake that was also made by Android's fingerprint scanning. Given that we use visible light in almost every aspect of our life, it is quite easy to use it to bypass Face Unlock by just printing out a picture of the owner of the device. In this research, I examine various ways to attack Android biometrics that would require no real technical expertise by using digital images and videos and printed images in a variety of different settings. Through this, I was able to successfully bypass Face Unlock over 30% of the time with printed images. This unacceptably high success rate shows that Android Face Unlock is deeply flawed and needs to be corrected or removed entirely to ensure the user's security.

Introduction

Android Biometrics have been an important part of the operating system for most of its lifetime. Its convenience and security has made it very desirable for its users. However, it has not always been perfect and even today that remains true. Android has used four main biometrics in its lifetime: iris recognition, fingerprint scanning, Face Unlock, and voice recognition. Voice recognition was removed in Android 8.0 due to its insecurities; however, the others are still used widespread today.

Iris recognition is a very strong biometric and incredibly hard to bypass. Its use of visible and near-infrared light allows the device to map patterns from the user's irises in light that would not be visible otherwise. This means that a simple picture would not be an effective attack because the near-infrared features of the iris would not be visible to the device.

Fingerprint scanning used to use a simple camera to capture the user's fingerprint and create a map of the details of it. However, this could easily be spoofed by lifting the fingerprint of the owner off the device and using it against the fingerprint scanner. This failure led to the modern version which uses a grid of very small capacitors to map the user's fingerprint using the electricity from their body.

While fingerprint scanning stopped using visible light, that failure still resides in Face Unlock, which relies solely on the use of the device's front camera to recognize the user's face.

Architecture

To test the security of Face Unlock, there were three main types of attacks conducted on eight different subjects with ages ranging from 14 to 50. The three attacks were digital video attacks, digital images attacks, and physical image attacks. The digital attacks were recorded using a Logitech C920s webcam and the physical attack was captured using a Samsung Galaxy S8 front camera. Digital testing was performed on a 1920x1080 monitor at 60 Hz and physical testing was done using an HP Envy 4502 printer with plain paper.

Digital Video Attacks

To conduct a digital video attack, each subject was instructed to record a video from a close, medium, and far distance (roughly 10, 15, and 20 inches respectively). This was repeated for five different resolutions / framerates of 1920x1080 at 30 fps, 1280x720 at 60 fps 1280x720 at 30 fps, 640x480 at 60 fps, and 640x480 at 30 fps. All 15 videos were used to attempt to bypass Face Unlock five times, for a total of 75 trials per subject.

Success rates

	640x480 30 fps	640x480 60 fps	1280x720 30 fps	1280x720 60 fps	1920x1080 30 fps
Close	0.0%	0.0%	0.0%	2.5%	5.0%
Medium	0.0%	0.0%	0.0%	0.0%	2.5%
Far	0.0%	0.0%	0.0%	0.0%	0.0%

The higher resolution and closer distance does seem to have an impact, but overall, the success rates are low and mostly acceptable.

Digital Image Attacks

Digital image attacks were very similar to digital video attacks. They also used close, medium, and far distances from the camera, however, they were only taken in 1920x1080 resolution. Each distance was captured five times, for a total of 15 images per subject and, once again, each image was tested five times for a total of 75 trials per subject.

Success rates

Close	Medium	Far
3.5%	4.0%	5.5%

Interestingly, the opposite of the video attacks seems to be true, where the closer images have a lower success rate.

Physical Image Attacks

Physical image attacks were completed by having the subject take a picture of themselves at close, medium-close, medium-far, and far distances (roughly 20, 30, 40, and 50 centimeters).

Demonstration of the difference that distance makes using a wide-angle lens camera.

Each picture was printed and used to attempt to bypass Face Unlock 10 times each for a total of 40 trials per subject.

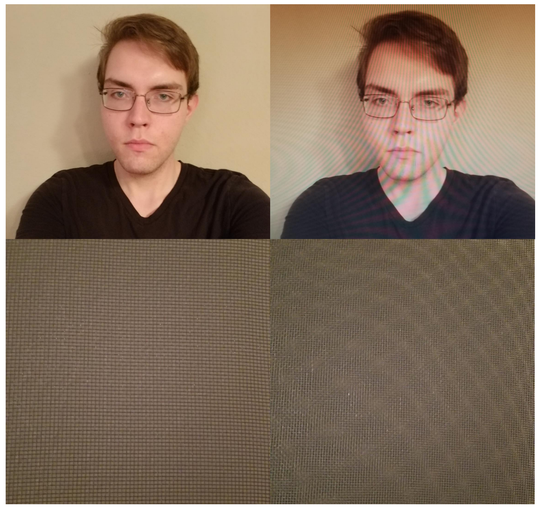
Success rates

Close	Medium-Close	Medium-Far	Far
35.0%	32.5%	32.5%	26.3%

Not surprisingly, the closer images have higher success rates. This is likely because people tend to unlock their device with their phone close to their face, and so the distortions caused by a wide-angle lens will be more like the mapping of the face that the device recognizes. These results show that a simple printed image of the owner can unlock their device around 30% of the time. These are incredibly high numbers for a very easy attack which requires no technical expertise. This is a massive flaw in Android biometrics and shows that Face Unlock is not secure and ultimately more research needs to be focused on improving the security of Face Unlock or it should just no longer be used in a similar manner to that of voice recognition.

Discussion

Physical image attacks showed significantly higher success rates then digital attacks. This is likely because of patterns that appear when using a camera to look at a computer monitor. A phenomenon called the Moiré pattern is often observed when someone tries to take a picture of something on their computer screen resulting in dark squiggly lines over their picture. This occurs because the grid of pixels in the computer monitor is not aligned with the grid of pixels in the camera's sensor. This effect is very easy to notice for computers but hard, if not impossible, to prevent by people. Using this as a prevention technique can be very effective but is only helps with digital attacks. The Moiré pattern will never be a factor with a printed image, and so the main flaw persists.



The top-left image shows a normal picture and the top-right shows the same picture of a computer screen to demonstrate the Moiré pattern. The bottom-left image shows a single wire mesh grid and the bottom-right image shows two overlapping wire mesh grids that also create the Moiré pattern.

Conclusion

If Android wishes to guarantee their users security with Android biometrics, then changes must be made with Face Unlock. Having the ability to bypass Face Unlock with over 30% success rate in some cases is not acceptable for the most widely used operating system on the planet. In a world dominated by social media, it is easier than it ever has been to find a picture of someone. If someone with malicious intentions wants to steal a phone and gain access to it, the combination of Face Unlock and social media makes it very easy for them.

Ultimately, Face Unlock fails because of its reliance on visible light. Future work on the subject should focus on the past failures of fingerprint scanning to build a better Face Unlock. Simply using the front camera of a device is too naïve and instead should incorporate some alternate way to recognize or confirm the face mapping like iris recognition's use of near-infrared light or fingerprint scanning's use of the body's electricity.

Future research on Android biometrics should have a heavy focus on Face Unlock because of this to produce a proper solution, and if one does not arise, then it may be necessary to simply remove Face Unlock from Android's list of biometrics.