Google Glass and Wearable Technology: A New Generation of Security Concerns

William Tucker Stone
william.stone@tufts.edu
Mentor: Ming Chow

Abstract

As new technologies such as the Google Glass are developed and released to the public, so too are new security problems and privacy apprehensions that must be acknowledged and accounted for. This paper examines the connotations of such abilities in the hands of everyday users, as well as the process through which your average programmer can deploy potentially insidious applications to a Google Glass unit. In addition, this piece will explore such topics as new social engineering apprehensions inherent with the release of a technology such as this and hardware vulnerabilities or exploits that have been discovered (as well as those that haven't). Already, dozens of Google Glass first-look users have found various ways to sabotage or subvert the device for other purposes, and these types of misuses are something every user and developer of this new technology must be aware of.

Introduction

The Google Glass is a small headband-like computer that puts a screen in front of the user's eye, allowing them to navigate the web, take pictures, and manage their various social media and communication. The device contains a wide-angle camera, retina sensor, microphone, and touch screen for device navigation. Users can easily shoot video clips or take pictures at the utterance of a command, and already there exists the ability to create custom applications for the device using Google's "Mirror-API", a web-based API that allows developers to interface with a Glass unit. The Google Glass is the latest and most cutting edge product developed by Google, and is the object of many a technology afficionado's desire. Already, hundreds of people have paid exorbitant amounts of money in order to participate in the Glass Discoverer program (a "beta" for the device), and interest in the headwear continues to increase as more people learn of the device and its capabilities. Because Google Glass is

targeted to be as affordable as a smartphone[1] and has caught the eye of so many tech-savvies, it is almost certain that these objects will become commonplace in our ever changing, ever upgrading society. As a result, it is of utmost importance that people be aware of the consequences of the use of such unprecedented hardware in order to protect our own personal information, privacy, and safety.

To The Community

In times such as these, with social media sites, portable technology, and cloud storage being prevalent in our daily lives, it becomes more and more difficult, if not impossible, to maintain a sense of privacy and security. The most effective way of counteracting those who would wish to subvert this technology and use it for their own purposes is to maintain a level of competency and knowledge that allows one to keep their data and themselves as safe as possible. This paper's main ambition is to enlighten its readers to the abilities and inner workings of the Google Glass, which has the potential to act as a subtle and mischievous medium.

Social Engineering

The Google Glass is among the first high-tech products developed that are intended to be worn on the user's person as an accessory. The concept of wearable technology has been developing for some time now, and although advanced wrist watches have been around for a while, nothing truly compares to a pair of pseudo-glasses interfacing with your surroundings and physical / auditory input. However, regardless of how the device actually works, wearable technology poses a serious risk to both the user of the device and those around them.

---

[1] Houghton, Stuart. "Google Glass: Release Date, News, and Features." November 2013, *TechRadar.* http://www.techradar.com/us/news/video/google-glass-what-you-need-to-know-1078114, Web Nov 2013.

Already, the majority of information loss can be attributed to the theft or loss of devices such as laptops[2], as opposed to actual technically advanced methods of malicious attacks. One can only imagine that this will become a prevalent problem for users of wearable technology, as valuable information is stored in an article notorious for being misplaced and left behind. In addition, the Glass is as of yet not secured with any sort of password, spoken or otherwise inputted, so a theft of the device results in complete information loss depending on what it has stored. On the flip side, those who have a Glass and have malicious intent can use the device's functionality to easily record a video or take a picture, without even communicating to those around them that they are doing so. For example, a Google Glass could be set up to take a picture whenever the user speaks aloud a specific word or phrase (something that can be easily set up). This would allow someone to easily snoop on and steal information from people using ATMs, typing in passwords on computers, etc. It is important to recognize that this technology implies that anything you can see could potentially be recorded and used for wicked purposes.

Action Items

Apart from the aforementioned Social Engineering risks of the Google Glass, there exist multiple other dangers when using a Google Glass. Google has released documentation and tutorials on the process of creating custom applications for the device, making it relatively simple (given basic knowledge of web development) to create a program that interfaces with a Glass device. The process of adding a new application to one's Glass is also very straightforward: register the application with your Google account (simultaneously adding it to your library and giving it permissions for various functionalities, from friend list access to

[2] Greenwald, Judy. "Personally Identifiable Data Most Frequently Exposed to Breaches: A Study." November 2013, *Business Insurance*. http://www.businessinsurance.com/article/20131101/NEWS07/131109979, Web Dec 2013.

account information), and look for it on your Glass' menu. All internet traffic that goes to the Glass travels first through Google's server, so when you ask the Glass for a menu of applications, it first checks with the Google servers to see which you are subscribed to and have activated. Any interaction goes from the Glass, to Google, to the server running the given application. Likewise, information sent from a server to the Glass must also go through the Google servers. This layer of security is essential in securing the traffic to a Glass; in this way, Google has ultimate control of what you get on your device. In order to display information on the Glass, applications must format responses into "cards" consisting purely of HTML and forward them the appropriate devices. Perhaps the most definitive and ultimate security measure that Google has taken with this device has been to forbid any and all JavaScript. This means that any script tags or other methods of attaching script to one of the HTML cards will be completely stripped before being forwarded on. However, already aspiring hackers have found ways around Google's security measures by loading Android apps onto the devices directly.[3] One recently developed SDK called WearScript allows native JavaScript on the device that can be programmed with ease. Brandyn White, a PhD candidate and faculty member at the University of Maryland and contributor to the WearScript library, says:

> *""We are putting significant effort into making the scripts easy to share. We regularly pass them around while we're working, [and] it takes a few seconds to try them out. There is a place for WearScript, Mirror, Android SDK/NDK, and eventually the GDK. All we're focused on now is making WearScript a great platform to hack on and show off what*

[3] Zheng, Song. "How to run Android apps on Google Glass." May 2013, *Quora*. http://songz.quora.com/How-to-run-Android-Apps-on-Google-Glass, Web Dec 2013.

Glass can do."[4]

As more and more developers get their hands on the hardware and source for a piece of new technology such as the Google Glass, it is inevitable that more and more workarounds and powerful tools become open source and available for all. With the integration of Javascript and Android SDK, a whole new wave of security concerns are on the board for this device, from XSS to facial recognition and covert recordings.

Supplementary Material

In order to help demonstrate how simple it is to create a pernicious program, I have provided with this paper an application built for the Google Glass. The application, built on the framework provided *by Google*, was made by the author of this paper and a few others from Tufts University[5] in just a few hours. The application, once loaded onto the malicious user's device, accepts name commands from a user and proceeds to query such social media sites as Facebook, LinkedIn, and Twitter for information on the given name. When provided with the user's own authentications for said sites, the results would become frighteningly accurate as the API queries utilize the connections between the user and the target, and allow the pernicious user to capitalize on pre existing privacy problems rampant in our modern social media culture.

What does this material demonstrate? The fact that, with no previous coding experience with the Google Glass, a small group of programmers were able to throw together a functioning, privacy invading application within a few hours. The Google Glass is meant to

---

[4] Claburn, Thomas. "Google Glass connects with JavaScript." October 2013, *InformationWeek*. http://www.informationweek.com/software/google-glass-connects-with-javascript/d/d-id/1111951, Web Dec 2013.

[5] Aaron Tietz, Caroline Marcks, Ethan Danahy, Rafi Yagudin

have private developers create custom apps, and as such has inherent privacy and security concerns because of the fact that not all developers are to be trusted.

Hardware and Hacking

Having presented the aforementioned points about malign application development and mischievous social engineering uses of the Google Glass, the most important thing to stress about these devices is that even with advanced touch inputs and augmented reality interfaces, they are still computers. And, like all other computers that are made with built in software and hardware, they have inherent security flaws and unforeseen vulnerabilities. Particularly with newer technologies, zero day exploits are rampant and potentially devastating for initial users of Glass. Already, a few exploits have been discovered that capitalize on certain aspects of the device's hardware in order to exploit users. For example, early on in the Glass' lifetime, it was discovered that QR codes viewed by the wearer were processed automatically. Malicious QR codes were then developed that caused the Google Glass to connect to a nearby wireless access point completely unbeknownst to the user, and from there all web traffic (including uploaded / downloaded pictures and video) could be monitored by the malign party. Finally, when this access was combined with an Android web vulnerability, the hacker could gain complete control over the glass device.[6]

Even with Google patching exploits such as these within weeks[7], without a doubt multiple new exploits are out there waiting to be taken advantage of. Without the use of QR codes, wireless impersonation and monitoring is still entirely possible and a legitimate concern for careless Glass users. We can't possible have found every abuse of a new system such as

---

[6] Souppouris, Aaron. "Google patches Glass exploit that allowed hackers full remote access." July 2013, *The Verge*. http://www.theverge.com/2013/7/17/4531186/google-glass-exploit-qr-code-patch, Web Nov 2013.

[7] Bell, Lee. "Google Glass Still vulnerable to Wifi Exploits, says Symantec." July 2013, *The Inquirer*. http://www.theinquirer.net/inquirer/news/2283687/google-glass-still-vulnerable-to-wifi-exploit-says-symantec, Web Nov 2013.

this, and possibilities grow more and more extensive as people discover how to do such things as install Ubuntu on their glass,[8] and unlock the bootloader on their devices.[9] Trusting sensitive and private data with the Google Glass is, simply put, not a wise decision. Those who believe their information to be completely safe are, in a way, deluding themselves in the face of these hacks and intrusions.

In Conclusion

As this paper has outlined, the release of a brand new technology in and of itself is reason to be suspicious of a device's security. This, paired with the fact that the Google Glass itself functions as a piece of apparel that can easily be taken off and forgotten, means that its users will need to take extreme precautions when utilizing it during its first few years of life. While the price tag motivates the Glass' users to handle their device with caution, it does not make the devices attacker proof in the slightest. In addition, our society will need to be extra careful about the concept of strapping a high definition, wide angle lens to our foreheads. Sensitive information put into the open will be almost assuredly captured by someone's camera, and looking over one's shoulder will never have been so potentially dangerous. Regardless of Google's security measures in preventing the device from being used past its intended purposes, hackers will without a doubt supersede those measures with their own nefarious tools. As laughable as privacy is in the modern era of technology and social media, more than ever those who use and associate with those who use new technology must be on their guard, stay suspicious and well informed, and know exactly what the capabilities of their devices are.

---

[8] Joire, Myriam. "Google Glass rooted and hacked to run Ubuntu live at Google I/O." June 2013, *Engadget*. http://www.engadget.com/2013/05/16/google-glass-rooted-and-hacked-to-run-ubuntu-live-at-google-i-o/ , Web Nov 2013.

[9] Freeman, Jay. "Exploiting a Bug In Google's Glass." June 2013, *Suarik's Blog*. http://www.saurik.com/id/16, Web Nov 2013.

References

1. Souppouris, Aaron. “Google patches Glass exploit that allowed hackers full remote access.” July 2013, *The Verge.* http://www.theverge.com/2013/7/17/4531186/google-glass-exploit-qr-code-patch, Web Nov 2013.

2. Bell, Lee. “Google Glass Still vulnerable to Wifi Exploits, says Symantec.” July 2013, *The Inquirer*. http://www.theinquirer.net/inquirer/news/2283687/google-glass-still-vulnerable-to-wifi-exploit-says-symantec, Web Nov 2013.

3. Joire, Myriam. “Google Glass rooted and hacked to run Ubuntu live at Google I/O.” June 2013, *Engadget.* http://www.engadget.com/2013/05/16/google-glass-rooted-and-hacked-to-run-ubuntu-live-at-google-i-o/ , Web Nov 2013.

4. Freeman, Jay. “Exploiting a Bug In Google’s Glass.” June 2013, *Suarik’s Blog.* http://www.saurik.com/id/16, Web Nov 2013.

5. Houghton, Stuart. “Google Glass: Release Date, News, and Features.” November 2013, *TechRadar.* http://www.techradar.com/us/news/video/google-glass-what-you-need-to-know-1078114, Web Nov 2013.

6. Greenwald, Judy. “Personally Identifiable Data Most Frequently Exposed to Breaches: A Study.” November 2013, *Business Insurance.* http://www.businessinsurance.com/article/20131101/NEWS07/131109979, Web Dec 2013.

7. Claburn, Thomas. “Google Glass connects with JavaScript.” October 2013, *InformationWeek*. http://www.informationweek.com/software/google-glass-connects-with-javascript/d/d-id/1111951 , Web Dec 2013.

8. Zheng, Song. “How to run Android apps on Google Glass.” May 2013, *Quora*. http://songz.quora.com/How-to-run-Android-Apps-on-Google-Glass, Web Dec 2013.