Brendan Voelz

Ming Chow

COMP-0116

13 December 2017

An Examination of AR/VR Security Concerns

Abstract

Years ago, the idea of mixed reality technology was a mere pipe dream. Today, developers are making great strides in exploring and experimenting with this frontier whose applications seem limitless. From the humble Google Cardboard to the groundbreaking HoloLens, augmented reality and virtual reality (AR/VR) technology have come a long way in the past few years, and it seems as though new improvements are always just around the corner. However, all of these advancements come at a cost. One must pose the following question: with the ever-looming cyber security threats in this day and age, how can developers be certain that AR/VR devices will be safe from malicious attackers? Research on this topic has revealed an ugly side of AR/VR technology: as consumers push for an untethered mixed reality experience, such technology faces serious security concerns surrounding privacy, monitoring, and botnets. This holds even greater weight in the scope of AR/VR, as these devices allow for new types of data to be captured, which raises concerns that consumers have never had to take into consideration before. For example, being able to access the data that tracks one's eye movement over a period of time could be exploited to create unlawful marketing strategies. Consequently, consumers and developers alike must push for a strong emphasis on securing these devices before getting too swept away by the hype.

Introduction

VR/AR, Data, and Security

With any new technology, the first thing that should be squared away is security. You might ask, *why is VR more dangerous than any other type of new technology?* Simply data. VR is feasible only because our computers and are so unfathomably powerful that they can process an enormous volume of data, enough data needed to make an entirely dynamic virtual world feel like reality, sometimes with only a smartphone needed to crunch all of the numbers. However, this comes at a cost: all of this data is not as innocent as you might think, and there are malicious attackers out there who dream of taking advantage of this wealth of data.

As Forbes puts it, "data becomes the differentiator for capitalizing on the power of VR and AR."[1] For one, being able to have headsets that log and respond to *where* the user is looking on the screen raises some concerns. Perhaps the hackers could sell the data to marketing companies that would be able to exploit in order to drive more successful ad campaigns. Or, hackers could take advantage of the fact that these VR/AR devices require you to give up so much of your privacy—location information, user data in general, etc.

In reality, the serious security issues surrounding VR/AR have not received enough attention in the media. So, I assert that we must place a higher importance upon security within the scope of VR/AR to ensure that these systems can improve our lives without putting us at greater risk of cyber attacks.

---

[1] Editors, Forbes Technology Council. "Mixed Reality: Where The Virtual World And IoT Collide."

To The Community

Why should we care about VR/AR technology?

Today, VR technology serves as a new frontier that has the ability to change the ways that we interact with the virtual world. However, one must always ask himself the following important question: *why do we care?* Many consumers write off anything VR as *not quite there yet*. It is certainly true that the technology behind VR is far from perfect, but the reality is that *VR/AR is already here*.

It has never before been so easy to develop VR applications without spending hundreds of thousands of dollars or going through a lengthy, expensive higher education program. Companies like Google and Facebook are developing software development kits (SDKs) that consumers can purchase – or in some cases download for free – to create VR applications.

The field of medicine has already begun taking advantage of the ways that VR can improve the way we diagnose and treat patients.

> *"[Stanford University has] a surgery simulator that even includes haptic feedback for those doing the training. Stanford's endoscopic sinus surgery simulation uses CT scans from patients to create 3D models for practice, and it's been in use since 2002. While this technology doesn't use a head mounted display, the groundwork that's been done could further the effectiveness of future virtual simulations"*[2]

Some other ways that VR has contributed to the field of medicine: improving certain methods of exposure therapy by creating controlled environments where patients can "deal with their fears of things like flying and claustrophobia" in a safe space and helping to teach social skills to children with autism.

---

[2] Carson, Eric. "10 Ways Virtual Reality Is Revolutionizing Medicine and Healthcare."

Consequences of Attacks on VR/AR

Scientists are already experimenting with systems that can perform live surgery by means of robotics and VR[3]. So, if this system were to be hacked, it is undeniable that the results could be catastrophic.

Systems that are built to help train soldiers and pilots could be modified to give the users false-positives. That is to say, hackers could modify the system in such a way that *teaches the user the wrong way to fly a plane*.

Even from a day-to-day consumer perspective where the products are more along the lines of Google Glass and Microsoft Hololens – two AR devices that allow users to interact with the world differently – you would not want any of your valuable data to be accessible to attackers. The eye-tracking data could be hacked and sold to marketing firms to target you with ads that are even smarter than the ones out there today, your location data could be exploited and monitored by anyone, and the list goes on and on.

Security Concerns

Privacy

Due to the immersive, all-encompassing experience that it offers, VR/AR presents some very serious security concerns in the scope of user privacy. When you download apps like *Pokemon Go,* you must realize that "your data is not solely in the hands of the

[3] "Cancer Surgery Broadcast Live in Virtual Reality." *BBC News*

vendor."[4] In the fine print of the terms and conditions – that we all sign upon download of these apps without reading – there are clauses that explicitly state that our data will be sold to third-party companies. And, since Facebook is already trying to start to find ways to integrate VR into social media, the company is likely already manipulating the data gathered from Oculus devices to strengthen its targeted ad campaigns and further other endeavors we don't know about. Is it morally right for these companies to be able to invade your privacy and sell all of your valuable data? Regardless of the answer, I think it is irresponsible for us as consumers to allow it to happen without at least trying to establish strict guidelines and legislation to ensure the security of VR/AR.

Monitoring

Plus, since these VR/AR companies are not focusing on security, we cannot ever be certain that these devices will be protected from attacks that could lead to hackers monitoring our activity without knowing it. Aaron Walker from G2 Crowd writes, "They can do more than sell the information to a marketing company or a product vendor. People could track your location, broadcast your feed or hack your network and steal your credit information. Hackers could also edit your environment."[5] Furthermore, it is no secret that government agencies like the FBI and NSA would love to use VR/AR to expand upon their surveillance methods, so it is important that we have this conversation about the role of security in VR/AR technology so that can maintain some level of control over the privacy that it seems so many people are willing to give away without the blink of an eye.

---

[4] Walker, Aaron. "Potential Security Threats with Virtual Reality Technology."
[5] Ibid.

A Lack of Attention

Ultimately, what most troubles me is the fact that we haven't really had much research or emphasis about the security of VR/AR yet, despite the fact that these products are already around us. It is irresponsible to use devices and technologies without understanding the potential risks you are taking when you sign the terms and conditions; and, as already highlighted in the previous section, it is clear that by using VR/AR devices you are taking non-negligible security risks in the realm of privacy and monitoring. So, where do we go from here? How do we even begin to start having proper discussions about these issues? I've identified three major items that consumers can uphold to improve the current state of security in VR/AR technology: vet manufacturers, become a cautious consumer, and change the perception of security.

Action Items

Vet Manufacturers

First off, we should not allow manufacturers to continue to get away with pushing insecure devices to the market. If big corporations want to ride the hype-train of VR/AR technology, we must enforce strict guidelines on security practices to ensure that company products hold up to proper security standards. It is sad to me that the lack of serious attention towards security is what has led to all of these DDoS attacks in recent years. And, until manufacturers start needing to play by the rules, these types of hacks are not going away. Plus, doubling back to the privacy concerns that already exist with apps like *Pokemon Go,* we cannot allow companies to have such unrestricted access to private

data since it is clear that they are selling our data. So, we must continue to put a lot of pressure on companies to put security first.

Become a Cautious Consumer

It is easy to get lost in the latest and greatest technology trends, but with VR/AR you must stop to consider the risks you are taking when purchasing devices that don't clearly emphasize security. Instead of jumping on the bandwagon of the hottest new VR headset, we should strive to be the most informed consumers possible. Roger Miller, an expert on the field of consumer technology, highlights, "technology-based products are likely to have the most defects when they are first available. No amount of testing can uncover every new 'bug' in a product… As a general rule of thumb, 'when in doubt, wait.'"[6]

Change the Perception of Security

What a lot of the discussion in this paper boils down to is the following: companies and consumers simply do not care that much about security. As a result, security too often gets put on the back burner behind innovation. However, those who truly understand technology know the reality that nothing matters if we have no security. Your iPhone is useless if a hacker can break into it and jam your calls, your computer is useless if it's too riddled with malware to load Gmail, and your smart refrigerator can't even keep your food cold if it's vulnerable to attacks that can disable its functionality. The point is, whether or not we consciously think of the role of security in our

[6] Miller, Roger LeRoy., and Alan D. Stafford. Economic Education for Consumers.

technological lives, it is absolutely essential to keeping everything running. So, we must we must develop products with the mindset of *security first*.

Conclusions

Indeed, VR/AR technology faces a great challenge in the realm of security: privacy and monitoring problems aren't going away any time soon, and we can only begin to solve these issues by openly addressing their existence. We must call out companies that try to slip data-logging clauses into the terms and conditions, and we must also stand up for our own privacy by not allowing anyone – government organizations, private companies, and hackers – to monitor what we are doing on these VR/AR devices. By shifting towards an attitude of "security first," we as consumers can feel more confident in the exciting products being offered to us. And, similarly, companies will enjoy more stability to further innovation, effectively setting the stage for VR/AR technology to safely change the ways in which we interact with the world.

Supporting Material

I have also put together a slide show that is publicly available for viewing that supplements this material at the following URL:

https://drive.google.com/open?id=1CaHzt5iZNlvVFjZetR7JqpycjIENeX1d

References

Works Cited

Bauer, Harold. “Security in the Internet of Things.” *McKinsey & Company*, May 2017, www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things.

“Cancer Surgery Broadcast Live in Virtual Reality.” *BBC News*, BBC, 14 Apr. 2016, www.bbc.com/news/av/technology-36046948/cancer-surgery-broadcast-live-in-virtual-reality.

Carson, Eric. “10 Ways Virtual Reality Is Revolutionizing Medicine and Healthcare.” *TechRepublic*, 8 Apr. 2015, www.techrepublic.com/article/10-ways-virtual-reality-is-revolutionizing-medicine-and-healthcare/.

Editors, Forbes Technology Council. “Mixed Reality: Where The Virtual World And IoT Collide.” *Forbes*, Forbes Magazine, 5 July 2017, www.forbes.com/sites/forbestechcouncil/2017/07/05/mixed-reality-where-the-virtual-world-and-iot-collide/#377dee96d3e3.

Gil, Paul. “What Exactly Is 'Telnet'? What Does Telnet Do?” *Lifewire*, 19 Sept. 2017, www.lifewire.com/what-does-telnet-do-2483642.

“History Of Virtual Reality.” *Virtual Reality Society*, www.vrs.org.uk/virtual-reality/history.html.

Leyden, John. “Sh... IoT Just Got Real: Mirai Botnet Attacks Targeting Multiple ISPs.” *The Register*, The Register, 2 Dec. 2016, www.theregister.co.uk/2016/12/02/broadband_mirai_takedown_analysis/.

Miller, Roger LeRoy., and Alan D. Stafford. *Economic Education for Consumers*. Thomson/South Western College Publishing, 2010.

Smith, Donald. "Another Good Reason to Stop Using Telnet." *InfoSec Handlers Diary Blog*, 13 Feb. 2007, isc.sans.edu/diary/%2A+Another+good+reason+to+stop+using+telnet/2220.

"VIRTUAL REALITY - History." *Expo/Theater/Virtual Environments*, NCSA Illinois, archive.ncsa.illinois.edu/Cyberia/VETopLevels/VR.History.html.

Walker, Aaron. "Potential Security Threats with Virtual Reality Technology." G2 Crowd, G2 Crowd, Inc., 11 Oct. 2017, www.g2crowd.com/blog/artificial intelligence/potential-security-threats-virtual-reality-technology/.

Woolf, Nicky. "DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say." *The Guardian*, Guardian News and Media, 26 Oct. 2016, www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.