Tracking Attacks on Virtual Reality Systems

Muhammad Usman Rafique and Sen-ching S. Cheung
University of Kentucky

***Abstract*—Virtual reality (VR) is a rapidly advancing technology with diverse applications. VR systems offer an immersive, life-like virtual experience by rendering interactive views on a head-mounted display. VR systems are vulnerable to various types of attacks, which could have dire consequences as they are designed to replace our perception of the physical world. However, there have been few studies on the security and integrity issues of the VR systems. We focus on the popular HTC Vive VR system and propose novel attack methods on blocking and manipulating its tracking subsystem. It is shown that simple attacks can jam or even manipulate the entire position and pose tracking process. Possible countermeasures are suggested to make VR systems safer and more secure.**

VIRTUAL REALITY (VR) SYSTEMS

The market of virtual and augmented reality systems is forecasted to be $1.8 billion by 2021,[1] with diverse applications ranging from entertainment, manufacturing to healthcare. There are many commercial VR systems available on the market. Oculus Rift, HTC Vive,[2] and PlayStation VR are the most commonly used room-scale VR systems. These systems require ground stations for tracking of the user. There are systems with limited tracking capability that do not use ground stations, such as Google Daydream view and Samsung Gear VR.

Digital Object Identifier 10.1109/MCE.2019.2953741
Date of current version 7 February 2020.

There is a strong need to ensure safe operations among VR systems as they alter or even replace our perception of the physical world. Security of cyber-physical systems goes beyond the traditional information technology as the physical parts and their respective inputs to the system need to be checked for veracity. A recent work by Trippe et al. showed that a malicious device can manipulate the accelerometers of phones and fitness trackers.[3] If the position and pose of the user can be deliberately manipulated, the feedback can be altered (i.e., what the user sees on the headset), and the result would have a direct impact on the user. Securing these systems is important, particularly for their emerging applications, such as health care,[4]

Published by the IEEE Consumer Electronics Society

medical visualization, therapy for psychological disorders,[5] management of in-flight anxiety.[6] Recent works such as by Menzies et al.[7] have begun investigating the effect of visual perturbation that may cause injury to a VR user. VR sickness and nausea caused by VR systems have been reported.[8] We highlight the security aspect of the VR system, a significant issue that will be incorporated into future standards of VR systems.[9]

However, to the best of our knowledge, there has been no study on integrity and security of VR systems. The research problem that we explore in this work is to analyze the security of VR systems by identifying vulnerabilities. We show how a malicious device based on commonly available IR LEDs can compromise the VR system by jamming or, even worse, manipulating the pose estimation. For concreteness, we focus our analysis and experiments on the HTC Vive system because, first, HTC Vive is the market leader with a slim lead over Oculus Rift[10] and, second, HTC Vive system provides better performance in terms of the working area.[11]

TRACKING SYSTEMS

In this section, we review the tracking mechanisms used in room-based VR systems. They can be categorized in two groups: first, active ground stations and passive headsets, and second, passive ground station and active headset.

Passive Ground Stations, Active Head-Mounted Display (HMD)

Pssive tracking system employed by Oculus Rift uses IR light emitters on the headset and controllers. The ground stations contain IR cameras that detect and localize the light emitted by the LEDs embedded in the headset and controllers. Each LED has a unique identity, conveyed by a distinctive lighting pattern. The frequency of LEDs and cameras is 60 Hz and cameras at different ground stations are synchronized by a pulse provided by the headset. Once enough number of LEDs have been seen and identified by the camera, the pose of the headset to the camera can be determined.

Active Ground Stations, Passive HMD

VR systems, like HTC Vive, use active ground stations, or lighthouses, that emit IR light signals. The headset and controllers have multiple IR diodes that detect these IR signals. Although the design of HTC Vive is not open-source, our descriptions here are based on information given by Nairol et al.[12–14] The HTC system has two lighthouses, labeled A and B. Both lighthouses emit light at a wavelength of 850 nm, modulated at a frequency of 1.84–2 MHz. There are different types of light signals: horizontal sweep, vertical sweep, and sync pulses. The horizontal and vertical sweeps are created by the two rotating lasers in each lighthouse. When the sweep hits IR diodes on the headset, it creates a pulse that lasts roughly 10 μs long, which is used to determine the distance between the lighthouse and the sensor. The sync pulse is a bright omnidirectional flash emitted from an array of IR LEDs to set a timing reference. The duration of the pulse varies from 62 to 135 μs. The first sync pulse, emitted by lighthouse A, and the second one by lighthouse B are always 400 μs apart. The four sweeps (vertical/horizontal, A/B) cycle through repeatedly and each occurrence is preceded by a sync pulse from each lighthouse.

The position and orientation calculation is based on the timing difference between sync pulses and the horizontal/vertical sweeps. HTC Vive also contains inertial sensors. Through experiments, we found out that attacks on the optical system alone can jam the system or add error in the position and orientation estimation.

DESIGN OF THE ATTACK DEVICE

The experimental setup, in a 10 m $\times$ 6 m area, is shown in Figure 1. The attacking device contains three IR photodiodes, 16 IR LEDs to create fake *sync pulses* and an on-board microcontroller, Teensy3.2. Figure 2 shows the functional block diagram of our attacking device. We adopted the design of sensors from Ashtuchkin.[13] The photodiode IR detector is based on BPV22NF and the high-pass filter is implemented using a resistor–capacitor combination of R = 47 $k\Omega$ and C =10 nF. Op-amp TLV2462IP is used for amplification and TLC59284LED driver powers VSLY3850 LEDs. Due to limited current rating of the LED driver, this

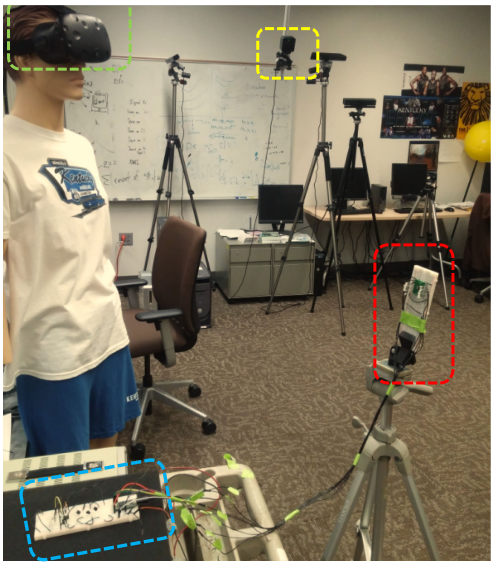

Figure 1. Physical setup for experimentation. The HMD is shown in green, Vive lighthouse in yellow, our sensor circuit in blue, and LED circuit with driver is shown in a red box.

system can interfere with a headset that is at most 2 m away. Using more drivers and IR LEDs in parallel can scale the range of attacks. To get the position and orientation data of the headset, we used SteamVR (version 1493337050) with Unity (version 5.4).

Controlled experiments were carried out to measure the true position (x, y, z), position during attack $(x,' y,' z')$, true orientation (α, β, γ), and orientation during attack $(\alpha,' \beta,' \gamma')$. Here, α, β, and γ are the roll, pitch, and yaw angles. The true position and orientation of the headset were first measured. Since the headset is always kept stationary, any change in the recorded measurements indicated error due to attack. Error in distance E_d is defined as

$$E_d = \sqrt{(x - x')^2 + (y - y')^2 + (z - z')^2}. \quad (1)$$

Similarly, error in angles E_a is defined as

$$E_a = \sqrt{(\Delta\alpha)^2 + (\Delta\beta)^2 + (\Delta\gamma)^2} \quad (2)$$

where the smaller angle is measured using

$$\Delta\theta = \min[(2\pi - |\theta - \theta'|), \quad |\theta - \theta'|]. \quad (3)$$

Here, θ can be α, β, or γ.

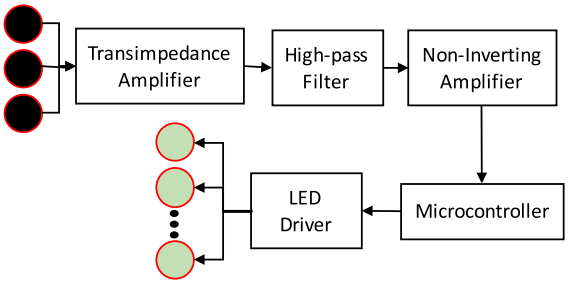

Figure 2. Design of the attacking device. A microcontroller coordinates the sensing part and the IR emitters.

JAMMING AND MANIPULATION OF TRACKING SYSTEM

Sync Pulse Attacks Without Sensing

In this attack, the on-time of attack pulses is randomly set between 62 and $135\,\mu$s while the off-time is set between 265 and $8000\,\mu$s. Even without any sensor, this method is capable of jamming the tracking system nearly half the time. The tracking usually stopped a few seconds after the attack—the host computer could still read the data but they were no longer changing, and the software display showed an error message, as shown in Figure 3. The system resumed tracking shortly after our attacking device was turned OFF. A key observation is that the system does not rely on the inertial sensors to provide motion estimates. On the contrary, we noted that the whole tracking process stopped once the attack was initiated, indicating that the inertial sensors were not used when the optical system failed. In summary, we show that an attack using only IR LEDs can jam the tracking system with roughly 50% success rate.

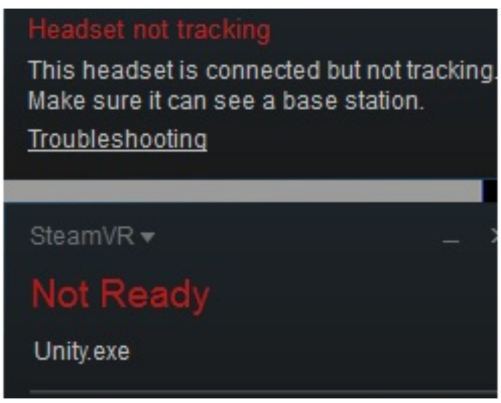

Figure 3. Error message displayed on the software after a jamming attack was launched.

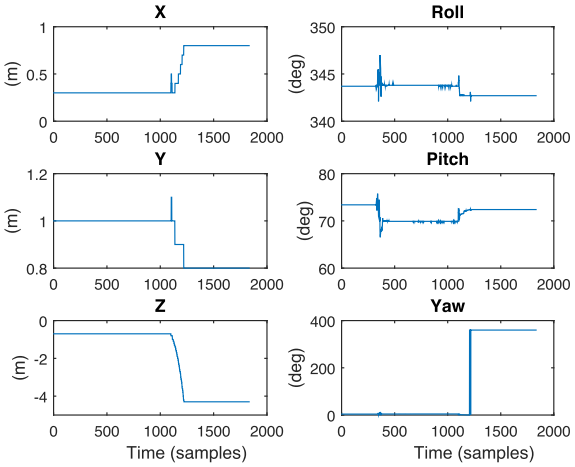

Figure 4. Measured positions and orientations during a manipulation attack. The horizontal axis shows samples collected over time. Since the headset was not moving, changes in position and pose correspond to the error due to attack.

Sync Pulse Attack With Sensing

Fake pulses could also be generated to modify the actual sync sequence by using sensors and microcontroller interrupts to detect the rising edges of the sync pulses. Since actual pulses vary from 62 to 135 μs, we use the pulse duration of 50 μs to ensure that the fake pulse interferes with the system. The detailed process is shown in Algorithm 1. Even though we did not differentiate whether a pulse is a sync flash or a rotating laser sweep, this attack was enough to jam the tracking system every time it was launched. We have shown that using a smart attacking device with sensors (IR detectors), an attacker can jam the VR tracking system with certainty.

Algorithm 1. Algorithm for Smart Jamming.

Input: Detection of the pulses (both rotating laser sweeps and sync pulses) of the actual system.
Output: A sequence of control signals provided to the IR LEDs that produce fake sync pulses.

1. **repeat forever**
2. Wait for start of any pulse of the actual system.
3. Generate a pulse with on-time of 50 μs.

Position and Orientation Manipulation

The last attack only jams the tracking system. However, it is possible to launch more sophisticated attacks to manipulate the pose estimation. When two consecutive real pulses are identified as sync pulses, start of a new cycle can be identified and we can now set our reference time with the actual system. We launched a position and orientation manipulation attack by generating a fake sync pulse before the start of actual pulse. This attack method is shown in Algorithm 2. We started the pulse at a time randomly sampled from 8200 to 8300 μs (the real one starts at 8333 s. The on-time of the pulse was 65 μs. The position and orientation during the attack are shown in Figure 4. Since the headset was set at a fixed position, any change is strictly due to the attack. Deviations from the true values, as defined in (1) and (2), are shown in Figure 5. As shown, this attack can induce error of more than 3.5 m in position and around 10° in orientation.

Algorithm 2. Algorithm to Manipulate the Position and Orientation Measurements.

Input: Detection of the pulses (both rotating laser sweeps and sync pulses) of the actual system.
Output: A sequence of control signals provided to the IR LEDs that produce fake sync pulses.
Initialize: synchronized ← false

1. **repeat forever**
2. **if** synchronized == false
3. $t_s \leftarrow$ start time of input pulse
4. **if** two consecutive sync pulses are detected
5. time reference $t_{ref} \leftarrow t_s$
6. synchronized ← true
7. **end if**
8. **else if** synchronized == true
9. $t_{nonce} \leftarrow$ a random number uniformly sampled from 8200 to 8300.
10. generate sync pulse at time $t_{ref} + t_{nonce}$ μs.
11. **end if**

COUNTERMEASURES

Intrusion Detection

A simple intrusion detection system can flag an attack if it detects any patterns different from the expected timing model. The detection of jamming signals is simple: if there are more than two IR light sources (i.e., more than two sync pulses), it implies there is a malicious device nearby. This is based on the fact that an unwanted lighthouse signal cannot cause harm

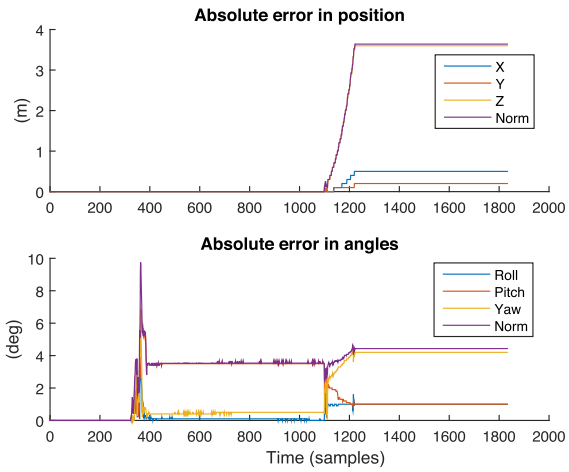

Figure 5. Error in position and orientation during the attack. The headset was fixed during the experiment and any change in position and orientation (shown in Figure 4) is error added by a successful attack. Error definition and measurement methods are discussed in the "Design of the Attack Device" section.

and the current system cannot synchronize with more than two IR signals. Second, it is easy to detect if the sync pulse arrives before the expected time by having a clock on the HMD. This simple countermeasure, however, will fail if a lighthouse is compromised. To deal with attacks that change the width of the sync pulses, data bits encoded in the sync pulses can be used to detect maliciously injected sync pulses.

Securing Timing Information

The optical signal is modulated at a high frequency. One way to make the system secure is by changing the modulation frequency and using a spread-spectrum modulation. Infrared communication using spread-spectrum techniques have been investigated in studies by Yin and Haas.[15] A private set of frequencies will allow the system to filter out adversaries who are not aware of these frequency sequences. Since lighthouses have Bluetooth modules, they can exchange keys to decode the frequency pattern. As spread-spectrum techniques can allow multiple parties to communicate without interference, multiple devices can simultaneously detect the modulated signals from multiple lighthouses concurrently, instead of having only one lighthouse transmitting at a time.

CONCLUSION AND DISCUSSION

We have discussed how the tracking system of HTC Vive VR system can be manipulated. We have shown the design of a simple and low-cost device that could be used to disrupt the service of the VR system. Different attacks, ranging from very simple jamming to relatively complex, well-timed attacks have been demonstrated. Our work resonates with other recently discovered cyber-physical attacks on consumer devices. To the best of our knowledge, this is the first work that shows the vulnerabilities in VR systems. We have outlined countermeasures, including intrusion detection and securing the communication, but we were not able to demonstrate their effectiveness due to the propriety implementation of the Vive system. While our experiments focus exclusively on the HTC Vive VR system, it is expected that other VR systems share similar vulnerabilities, making the development of appropriate countermeasures a top priority.

ACKNOWLEDGMENTS

The authors would like to thank S. Liaqat and P. Eberhart for their help with circuits, implementation, and debugging.

REFERENCES

1. "After mixed year, mobile AR to drive 108 billion VR/AR market by 2021." [Online]. Available: http://www.digi-capital.com/news/2017/01/after-mixed-year-mobile-ar-to-drive-108-billion-vrar-market-by-2021
2. "Vive—discover virtual reality beyond imagination." [Online]. Available: https://www:vive:com/us/
3. T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks," in *Proc. IEEE Eur. Symp. Secur. Privacy*, 2017, pp. 3–18.
4. B. K. Wiederhold, I. T. Miller, and M. D. Wiederhold, "Using virtual reality to mobilize health care: Mobile virtual reality technology for attenuation of anxiety and pain," *IEEE Consum. Electron. Mag.*, vol. 7, no. 1, pp. 106–109, Jan. 2018.
5. M. M. North and S. M. North, "Virtual reality therapy for treatment of psychological disorders," in *Career Paths in Telemental Health*. Berlin, Germany: Springer, 2017, pp. 263–268.
6. R. A. Cardoş, O. A. David, and D. O. David, "Virtual reality exposure therapy in flight anxiety: A quantitative meta-analysis," *Comput. Human Behav.*, vol. 72, pp. 371–380, 2017.

7. R. Menzies *et al.*, "An objective measure for the visual fidelity of virtual reality and the risks of falls in a virtual environment," *Virtual Reality*, vol. 20, no. 3, pp. 173–181, 2016.
8. N. Padmanaban, T. Ruban, V. Sitzmann, A. M. Norcia, and G. Wetzstein, "Towards a machine-learning approach for sickness prediction in 360 stereoscopic videos," *IEEE Trans. Vis. Comput. Graphics*, vol. 24, no. 4, pp. 1594–1603, Apr. 2018.
9. Y. Yuan, "Paving the road for virtual and augmented reality [standards]," *IEEE Consum. Electron. Mag.*, vol. 7, no. 1, pp. 117–128, Jan. 2018.
10. B. Lang, "Vive is hanging onto steam majority market share by a thread," Nov. 2017. [Online]. Available: http://www.roadtovr.com/vive-hanging-onto-steam-majority-market-share-thread/
11. A. Borrego, J. Latorre, M. Alcañiz, and R. Llorens, "Comparison of oculus rift and HTC vive: Feasibility for virtual reality-based exploration, navigation, exergaming, and rehabilitation," *Games Health J.*, vol. 7, pp. 151–156, 2018.
12. Nairol, "nairol/lighthouseredox," Jun. 2017. [Online]. Available: https://github.com/nairol/LighthouseRedox
13. Ashtuchkin, "ashtuchkin/vive-diy-position-sensor," May 2017. [Online]. Available: https://github.com/ashtuchkin/vive-diy-position-sensor
14. "Lighthouse tracking examined," May 2016. [Online]. Available: http://doc-ok.org/?p=1478
15. L. Yin and H. Haas, "Physical-layer security in multiuser visible light communication networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 1, pp. 162–174, Jan. 2018.

Muhammad Usman Rafique is currently working toward the Ph.D. degree at the University of Kentucky, Lexington, KY, USA. His research interests include security, privacy, computer vision, machine learning, and robotics. Contact him at usman.rafique@uky.edu.

Sen-ching S. Cheung is currently a Professor of Electrical and Computer Engineering and Director of Multimedia Information Analysis Laboratory, University of Kentucky, Lexington, KY, USA. His research interests include security, analysis, and communication of multimedia information. Contact him at sccheung@ieee.org.