

# Razvoj aplikacije u virtualnoj stvarnosti za simuliranje kibernetičkog napada

---

**Petak, Borna**

**Undergraduate thesis / Završni rad**

**2024**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **University of Zagreb, Faculty of Electrical Engineering and Computing / Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva**

*Permanent link / Trajna poveznica:* <https://urn.nsk.hr/urn:nbn:hr:168:252558>

*Rights / Prava:* [In copyright](#)/[Zaštićeno autorskim pravom.](#)

*Download date / Datum preuzimanja:* **2025-03-21**



*Repository / Repozitorij:*

[FER Repository - University of Zagreb Faculty of Electrical Engineering and Computing repozitory](#)



SVEUČILIŠTE U ZAGREBU  
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 1561

**RAZVOJ APLIKACIJE U VIRTUALNOJ STVARNOSTI ZA  
SIMULIRANJE KIBERNETIČKOG NAPADA**

Borna Petak

Zagreb, lipanj 2024.

SVEUČILIŠTE U ZAGREBU  
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 1561

**RAZVOJ APLIKACIJE U VIRTUALNOJ STVARNOSTI ZA  
SIMULIRANJE KIBERNETIČKOG NAPADA**

Borna Petak

Zagreb, lipanj 2024.

## ZAVRŠNI ZADATAK br. 1561

Pristupnik: **Borna Petak (0036535558)**  
Studij: Elektrotehnika i informacijska tehnologija i Računarstvo  
Modul: Računarstvo  
Mentorica: prof. dr. sc. Lea Skorin-Kapov

Zadatak: **Razvoj aplikacije u virtualnoj stvarnosti za simuliranje kibernetičkog napada**

### Opis zadatka:

Suvremeni komercijalni sustavi za virtualnu stvarnost (engl. Virtual Reality, skr. VR) temelje se na tehnologiji koja omogućuje praćenje korisnikovih pokreta u šest stupnjeva slobode te služe kao poticaj razvijateljima usluga i igara za razvoj kreativnih metoda interakcije s virtualnim svijetom. Tehnologija VR primjenjuje se u obrazovanju i treningu kao alat za stvaranje interaktivnog i vizualno privlačnog sadržaja radi stjecanja novog znanja. Kibernetička sigurnost je jedna od ključnih tema suvremenog društva te je vrlo važno educirati ljude o ovoj temi. Korištenje virtualne stvarnosti za učenje o kibernetičkim napadima pruža interaktivno iskustvo u kojem korisnici mogu praktično isprobati različite scenarije i razumjeti kako kibernetički napadi funkcioniraju u stvarnom svijetu te kako reagirati na napade i primijeniti sigurnosne mjere. Vaš zadatak je razviti aplikaciju u virtualnoj stvarnosti koja će simulirati odabrani kibernetički napad. Aplikacija bi trebala biti interaktivna, omogućujući korisnicima da prate napredak napada, identificiraju ranjivosti te primijene odgovarajuće sigurnosne mjere za obranu.

Rok za predaju rada: 14. lipnja 2024.



# Sadržaj

<b>1. Uvod</b>	<b>3</b>
<b>2. Virtualna stvarnost</b>	<b>5</b>
2.1. Povijest VR-a	5
2.2. Tehnologija	6
<b>3. Kibernetička sigurnost</b>	<b>8</b>
3.1. Kibernetički prostor	8
3.2. Napadi	8
3.3. Motivacija za napade	10
3.4. Obrane	10
<b>4. Opis aplikacije</b>	<b>12</b>
4.1. Motivacija	12
4.2. Dizajn aplikacije Office Defence	13
<b>5. Implementacija</b>	<b>15</b>
5.1. Korištene tehnologije	15
5.1.1. Unity	15
5.1.2. Visual Studio Code	15
5.1.3. Oculus Quest 2	16
5.1.4. XR Interaction Toolkit	16
5.1.5. Unity Asset Store i Skechfab	16
5.2. Ekran izbornika	17
5.3. Dizajn prostorija	18
5.3.1. Dizalo	18

5.3.2. Hodnik . . . . .	19
5.3.3. Ured . . . . .	19
5.4. Računala . . . . .	20
5.5. Zaraza računala . . . . .	21
5.6. Mehanizam igrača . . . . .	22
5.7. Mehanizam širenja virusa . . . . .	22
5.8. Spašavanje računala . . . . .	26
5.9. Proces bodovanja . . . . .	28
5.10. Nedostaci i mogućnost proširenja igre . . . . .	28
<b>6. Zaključak . . . . .</b>	<b>30</b>
<b>Literatura . . . . .</b>	<b>31</b>
<b>Popis slika . . . . .</b>	<b>33</b>
<b>Sažetak . . . . .</b>	<b>34</b>
<b>Abstract . . . . .</b>	<b>35</b>

# 1. Uvod

U današnjem digitalnom svijetu gdje je sve povezano, kibernetička sigurnost postaje sve kritičniji aspekt velikih kompanija, ali i pojedinaca. Rastom kibernetičkog prostora, broj kibernetičkih prijetnji se neprestano povećava, a samim time raste i potreba za učinkovitim treninzima koji mogu pripremiti stručnjake i korisnike za suočavanje s ovim izazovima. Svakodnevno se u svijetu ljudi suočavaju s prijetnjama poput phishing napada, napada ucjenjivačkim zloćudnim kodom (*engl. Ransomware*), napada uskraćivanjem resursa (*engl. distributed denial-of-service attack, skr. DDoS*) i drugih oblika kibernetičkih napada koji mogu nanijeti ogromne štete pojedincima i organizacijama [1]. Teoretska predavanja i laboratorijske vježbe često ne mogu u potpunosti replicirati stres i nepredvidljivost stvarnih napada.

Neka od rješenja za taj problem su simulatori, kao na primjer Cyber Conflict Simulator (*skr. CCS*) koji pokušavaju postaviti što realniji izgled cijelog sustava i simulirati napade koji su mogući na sustav [2]. Osim 2D simulatora, danas se koriste i imerzivne tehnologije kako bi poboljšale doživljaj samih napada [3]. Korištenjem imerzivnih tehnologija za trening kibernetičke sigurnosti, moguće je simulirati stvarne prijetnje i scenarije u kontroliranom okruženju, omogućavajući korisnicima da razviju praktične vještine i brzinu reakcije bez rizika od stvarne štete. Imerzivne tehnologije, poput virtualne stvarnosti (*engl. Virtual Reality, skr. VR*) i proširene stvarnosti (*engl. Augmented Reality, skr. AR*), donose nekoliko ključnih prednosti u kontekstu kibernetičkog treninga: povećana angažiranost korisnika kroz potpunu uronjenost u simulirani scenarij, realistična simulacija kompleksnih napada koja uključuje nepredvidive elemente, sigurno okruženje za učenje bez stvarnih posljedica, prilagodljivost scenarija za različite vrste prijetnji, te povratne informacije u stvarnom vremenu koje omogućavaju korisnicima da odmah isprave greške i unaprijede svoje vještine. Ove tehnologije omogućuju realistične simulacije i pružaju



priliku korisnicima da razviju praktične vještine u sigurnom i kontroliranom okruženju, čime se poboljšava njihova spremnost na stvarne prijetnje.

Ovaj rad se fokusira na razvoj aplikacije za kibernetički trening u VR-u, s ciljem poboljšanja učinkovitosti i angažiranosti korisnika. Rad pokušava simulirati odabranu vrstu napada unutar ureda neke kompanije i tako prikazati scenarij u kojem se osoba suočava sa stresom, brzinom i ozbiljnošću pravovremenih reakcija.

Rad je podijeljen u 7 poglavlja. Nakon uvoda opisani su pojmovi virtualne stvarnosti, ukratko povijest i koja se tehnologija koristi. Zatim u trećem poglavlju je dan uvid u kibernetičku sigurnost, koje su prijetnje i kako se sprječavaju. U četvrtom poglavlju opisana je problematika i zadatak. Peto poglavlje je rezervirano za opis tehnologija i programa koji su korišteni pri izradi igre Office Defence i dan je opis rješenja problematike. Na kraju je cijeli rad sažet u zaključak kao šesto poglavlje.

## 2. Virtualna stvarnost

Virtualna stvarnost je računalna simulacija izvedena uz pomoć posebnih računalnih periferija i programa, gdje je korisniku omogućen privid kretanja, opažanja i boravka [4]. Korištenjem posebnih uređaja kao što su VR naočale ili zaslone koji se montiraju na glavu (*engl. Head Mounted Device, skr. HMD*), korisnici mogu doživjeti realistična iskustva koja obuhvaćaju vizualne, zvučne, pa čak i haptičke podražaje. Ova tehnologija pruža visoku razinu uronjenosti, stvarajući osjećaj prisutnosti u virtualnom svijetu koji je usporediv s boravkom u stvarnom svijetu. Važni parametri koji utječu na stupanj uronjenosti uključuju širinu vidnog polja, broj osjetila koje sustav stimulira, kvalitetu slike i kašnjenje prikaza [5]. Stupanj uronjenosti je objektivno svojstvo sustava koje se može mjeriti neovisno o iskustvu koje stvara. Prisutnost je ljudska subjektivna reakcija na sustav, a definira se kao osjećaj da se tjelesno nalazimo u virtualnom okruženju, a ne na mjestu u stvarnom svijetu [5]. Tehnologija virtualne stvarnosti nalazi primjenu u raznim područjima, uključujući igre, medicinu, obrazovanje, arhitekturu i vojnu obuku.

### 2.1. Povijest VR-a

Usprkos vjerovanjima da je virtualna stvarnost nova stvar koja je započela razvojem grafike, njena povijest službeno započinje u 19. stoljeću. Već 1838. godine Charles Wheatstone demonstrira kako mozak procesira dvije dvodimenzionalne slike i time postavlja temelje za virtualnu stvarnost [6]. U pedesetim godinama dvadesetog stoljeća pojavljuje se Sensorama, stroj koji je simulirao sva osjetila, a ne samo vid i sluh. Nakon toga u šezdesetim godinama dvadesetog stoljeća se pojavljuju prvi primjeri zaslona na glavi. Nakon toga razvoj uređaja za VR bio je namijenjen uglavnom za razne treninge i simulacije.

Veća upotreba VR-a u javnosti počela je devedesetih godina dvadesetog stoljeća kada

se oprema počela koristiti u industriji video igara [6]. Tek početkom ovog stoljeća se oprema za virtualnu stvarnost počela koristiti komercijalno. Nakon što je 2010. godine Palmer Luckey, osnivač tvrtke Oculus VR, dizajnirao prototip za prvi Oculus, krenuo je značajni rast proizvođača naočala i opreme za VR. Danas je VR oprema česta pojava i velike tvrtke se natječu kako bi napravili što bolji i što jeftiniji proizvod kako bi bio dostupan što većoj javnosti za kupnju. VR oprema je dodatno promijenjena unatrag godinu dana kada je tvrtka Apple najavila svoj proizvod, Apple Vision Pro. Trenutno, među najboljim uređajima imerzivne tehnologije valja istaknuti, osim Apple Vision Pro, Meta Quest 2, Meta Quest 3 i Meta Quest Pro, tvrtke Meta koji su i dalje najdostupniji uređaji [7].

## 2.2. Tehnologija

Kako bi se stvorio osjećaj uronjenosti u virtualni svijet potrebni su posebni uređaji. Glavna komponenta su naočale koje prikazuju dvije slike iz različitih perspektiva kako bi ljudski mozak to procesuirao kao stvarnu sliku. Također, današnje moderne naočale imaju u sebi uređaj za praćenje pokreta glave (*engl. head tracking*) koji igraju ključnu ulogu u povećanju osjećaja uronjenosti, omogućavajući korisniku da se osvrće oko sebe u virtualnom okruženju.

Također, ako želimo interakciju s virtualnim svijetom potrebni su nam neki uređaji za interakciju. Najčešći uređaji su upravljači pokreta. Upravljači (*engl. controllers*) obično koriste optičke sustave praćenja (prvenstveno infracrvene kamere) za lociranje i navigaciju, tako da se korisnik može slobodno kretati bez ožičenja. Razlika između žičnog i bežičnog povezivanja također igra važnu ulogu u doživljaju uronjenosti. Žični uređaji obično pružaju stabilniju i bržu vezu, što može rezultirati manjim kašnjenjem u prijenosu podataka. Međutim, oni ograničavaju slobodu kretanja korisnika zbog fizičkih kablova. S druge strane, bežični uređaji omogućuju veću slobodu kretanja, ali mogu imati više kašnjenja i ponekad nižu stabilnost veze što je napredak u tehnologiji značajno smanjio.

Također, većem stupnju uronjenosti doprinose haptički povratni uređaji, poput rukavica ili odijela, koje mogu pružiti taktilne povratne informacije [8]. Navedeni uređaji svojom kvalitetom prijenosa informacija određuju stupanj uronjenosti i prisutnosti u sustavu. Postoji i nekoliko vrsta senzora koji se koriste za praćenje korisnika u virtualnom

okruženju. To uključuje akcelerometre i žiroskope koji prate orijentaciju i kretanje glave i tijela. Uz senzore, sustavi praćenja mogu uključivati i tehnologije kao što su ultrazvuk i tehnologije svjetlosnog zamjećivanja i klasifikacije (*engl. Light Detection and Ranging, skr. LiDAR*), za poboljšanje preciznosti i pouzdanosti praćenja. Ovi sustavi kontinuirano prate položaj i orijentaciju korisnika te prilagođavaju prikaz u virtualnom okruženju u stvarnom vremenu, što dodatno pojačava osjećaj prisutnosti i stupanj uronjenosti.

Gotovo savršeno virtualno okruženje ima visoku kvalitetu i visoku rezoluciju informacija koje se prenose korisniku, konzistentni prikaz i okolinu u kojoj korisnik može koristiti sva svoja osjetila [9]. Na slici 2.1. je VR set koji sadrži naočale s kamerom i dva upravljača pokreta.



**Slika 2.1.** Slika VR opreme, preuzeto iz [10]

## **3. Kibernetička sigurnost**

Kibernetika se u hrvatskom jeziku definira kao skupni naziv niza teorijskih disciplina i praktičnih postupaka koji se primjenjuju pri upravljanju i vođenju složenih sustava [11]. Model sustava koji se pritom razmatra (kibernetički sustav) sastoji se od triju cjelina: podsustava osjetila kojima se prikupljaju informacije o trenutačnom stanju sustava, podsustava u kojem se iz prikupljenih informacija trenutačno stanje uspoređuje sa željenim stanjem i tako utvrđuje razlika (pogreška) i podsustava koji utječe na ponašanje sustava tako što smanjuje nastale razlike [11].

### **3.1. Kibernetički prostor**

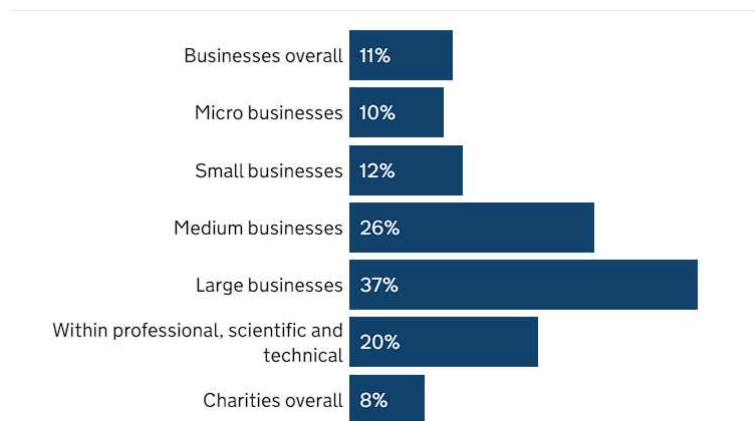
Danas se sve više i više stvari digitalizira i sve smo više ovisni o Internetu. Informacijski prostor koji se ostvaruje globalnim umrežavanjem računala nazivamo kibernetički prostor [11]. Nažalost, kako se cijeli sustav širi tako se šire i mogućnosti sigurnosnih propusta. Svaki sigurnosni propust je ranjivost koja se može realizirati potencijalnim napadom. Ranjivosti mogu biti rezultat slabih točaka u softveru, hardveru, mrežnoj arhitekturi, pa čak i u ljudskim faktorima, kao što su nepažnja ili nedostatak svijesti o sigurnosti.

### **3.2. Napadi**

Kibernetički napadi nisu nova pojava. Od samih početaka Interneta i mrežnog povezivanja postoje opasnosti različitih razmjera. Svaki pokušaj onemogućavanja, manipulacije ili dobivanja neovlaštenog pristupa računalnom sustavu, mreži ili uređaju smatra se kibernetičkim napadom. Kibernetički kriminal iz godine u godinu raste, te je 2023. samo u Ujedinjenom kraljevstvu prijavljeno više od 2.3 milijuna napada, gdje je prosječna dobit napadača iznosila 3230 funti [12]. Najpoznatiji i najčešći su napadi virusima, Phishing,

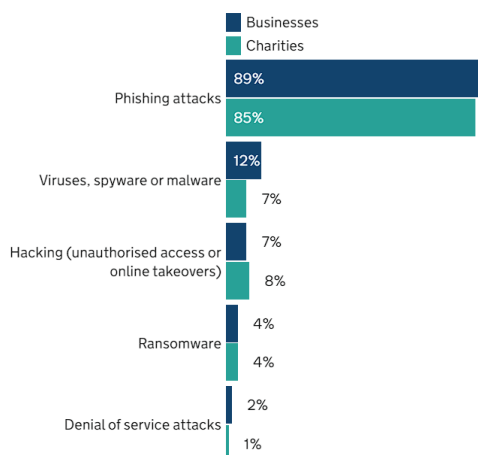
napad uskraćivanja usluge (DDoS), napadi ucjenjivačkim kodom (engl. Ransomware) i napad ranjivosti nultog dana.

U 2023. godini Odjel za znanost, inovacije i tehnologiju Ujedinjenog Kraljevstva proveo je istraživanje na 5985 tvrtki, kako bi pokazali koja je razina zaštite i broj napada unazad godinu dana [12]. Prikazano na slici 3.1. su rezultati koji pokazuju postotak tvrtki koje su pretrpjele neki od napada u razdoblju od 12 mjeseci prije provođenja istraživanja, koji je novčano oštetio tvrtku.



**Slika 3.1.** Postotak tvrtki koje su iskusile kibernetički napad, preuzeto iz [12]

Slika 3.2. prikazuje postotak pojedinih vrsta napada, te se može zaključiti kako se većina napada svodi na Phishing napad. Jedan od glavnih problema zašto se to događa jesu radnici u tvrtkama koji nisu dovoljno dobro upoznati sa sigurnosnim smjernicama.



**Slika 3.2.** Vrste napada u postotku, preuzeto iz [12]

### 3.3. Motivacija za napade

Grupe napadača dijele se prema određenim parametrima. Ovisno o tome koliko resursa posjeduju, koliko su odlučni o cilju, koliko znanje imaju i koje metode koriste, možemo ih razvrstati u ovih pet kategorija [1]:

- Napredne ustrajne prijetnje (*engl. advanced persistent threats*)
- Kibernetički kriminalci (*engl. cyber criminals*)
- Haktivisti (*engl. hactivists*)
- Pojedinačni napadači
- Automatizirane probe.

Iako se neke kategorije mogu još razdvajati, granice između njih su neprecizne i teško se odrede pa ih se može svrstati u jednu grupu [1]. Za označavanje jačine opasnosti koriste se nivoi od 1 do 4 [1]. Prijetnjom prvog nivoa se smatraju automatizirane probe, jer su danas sustavi zaštićeni od njih, a prijetnjom četvrtog nivoa se smatraju napredne ustrajne prijetnje, poput na primjer tajnih agencija Sjedinjenih Američkih Država ili Kine. Motivacije određenih grupa su različite, od zarade, do pronalaska skrivenih tajni. Jedna stvar koja je napadačima zajednička je ilegalni načini ostvarivanja motivacije.

Današnji sustavi sadrže puno mehanizama za zaštitu podataka. Kroz godine, kako su se otkrivali novi načini napada, tako se povećavala potreba za sigurnosnim mehanizmima [13]. Današnji sustavi imaju osiguranu zaštitu memorije i koriste se algoritmi kriptiranja koji su gotovo sigurni. Usprkos svim sigurnosnim mehanizmima napadači i dalje uspijevaju pronaći ranjivosti na sustavima i iskoristiti ih.

### 3.4. Obrane

Temeljni zahtjevi koje je važno ostvariti su povjerljivost (*engl. confidentiality*), cjelovitost (*engl. integrity*) i raspoloživost (*engl. availability*). Postoje još dva zahtjeva koji se dodaju temeljnim zahtjevima, a to su autentičnost (*engl. authenticity*) i neporecivost (*engl. non-repudiation*) [1]. Prema temeljnim zahtjevima sigurnosti moramo osigurati da su podaci dostupni samo ovlaštenim osobama (povjerljivost), da su podaci u izvornom

i nepromijenjenom obliku (cjelovitost) i da su podaci cijelo vrijeme dostupni (raspoloživost). Osiguravanjem tih zahtjeva dobivamo sigurni sustav. Temeljni izvor problema u sustavu je čovjek i ljudska sklonost rađanju pogrešaka [1].

Pogreške se mogu uvesti u bilo kojem dijelu razvoja sustava, što namjerno, što slučajno [1]. Kako bi se spriječila mogućnost ranjivosti, potrebno je od inicijalnog trenutka voditi računa o sigurnosti. Temeljni mehanizam koji se koristi za ispravni dizajn sustava je modeliranje prijetnji. Zadaća modeliranja prijetnji je utvrditi koje su sve opasnosti i potencijalne prijetnje koje mogu narušiti sigurnost sustava prije nego se uopće krene programirati sustav. Kasnije u daljnjim koracima razvoja je puno teže otkriti i ispraviti ranjivost sustava. Kako bi se smanjila mogućnost ranjivosti, potrebno je testirati kod, raditi reviziju koda, statičke i dinamičke analize koda i kao najvažnija točka, educirati programere.

Organizacija MITRE ATT&CK slaže baze taktika i procedura korištenih u napadima. Uz pomoć navedene baze razvijaju se modeli prijetnji i koriste se metode zaštita koje pokrivaju i najnovije vrste napada [14]. Slika 3.3. prikazuje tablicu koja se nalazi na početnoj stranici organizacije MITRE ATT&CK i dostupna je svima za pregled. Tablica kategorizira kibernetičke napade u 14 kategorija prema strategiji napada. Trenutno se u tablici nalazi 235 različitih tehnika, od kojih većina ima po nekoliko potkategorija. Odabirom određene tehnike otvara se stranica na kojoj je detaljno raspisano kako napad funkcionira i kako ga se prepoznaje.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (8)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (3)	Boot or Logon Autostart Execution (14)	Build Image on Host	Debugger Evasion	Cloud Infrastructure Discovery	Cloud Service Dashboard	Automated Collection	Content Injection
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (3)	Debugger Evasion	Exploitation for Credential Access	Cloud Service Discovery	Cloud Storage Discovery	Remote Service Session Hijacking (2)	Data Encoding (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Boot or Logon Initialization Scripts (3)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Storage Object Discovery	Cloud Storage Object Discovery	Remote Services (8)	Data Obfuscation
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Create or Modify System Process (5)	Deploy Container	Forge Web Credentials (2)	Container and Resource Discovery	Container and Resource Discovery	Replication Through Removable Media	Data from Cloud Storage
Search Open Technical Databases (3)	Stage Capabilities (3)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Domain or Tenant Policy Modification (2)	Direct Volume Access	Input Capture (4)	Debugger Evasion	Device Driver Discovery	Data from Configuration Repository (2)	Encrypted Channel (2)
Search Open Websites/Domains (3)	Trusted Relationship	Valid Accounts (4)	Serverless Execution	Create or Modify System Process (5)	Domain or Tenant Policy Modification (2)	Domain or Tenant Policy Modification (2)	Modify Authentication Process (2)	Device Driver Discovery	Domain Trust Discovery	Data from Information Repository (3)	Fallback Channels
Search Victim-Owned Websites	Valid Accounts (4)	Shared Modules	Software Deployment Tools	Event Triggered Execution (16)	Event Triggered Execution (16)	Execution Guardrails (1)	Multi-Factor Authentication Interception	File and Directory Discovery	File and Directory Discovery	Data from Local System	Ingress Tool Transfer
		System Services (2)	System Services (2)	Event Triggered Execution (16)	Event Triggered Execution (16)	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	Group Policy Discovery	Group Policy Discovery	Data from Network Shared Drive	Multi-Stage Channels
		User Execution (1)	User Execution (1)	Event Triggered Execution (16)	Event Triggered Execution (16)	Hide Artifacts (12)	Network Service Discovery	Log Enumeration	Log Enumeration	Data from Non-Application	Non-Application

Slika 3.3. MITRE ATT&CK baza, slika zaslona iz [14]



## 4. Opis aplikacije

U okviru ovog rada osmišljena je i implementirana aplikacija Office Defence. Navedena aplikacija je zamišljena kao edukativna igra unutar virtualne stvarnosti. U ovom poglavlju je opisana motivacija za izradu navedene aplikacije i kako je aplikacija zamišljena.

### 4.1. Motivacija

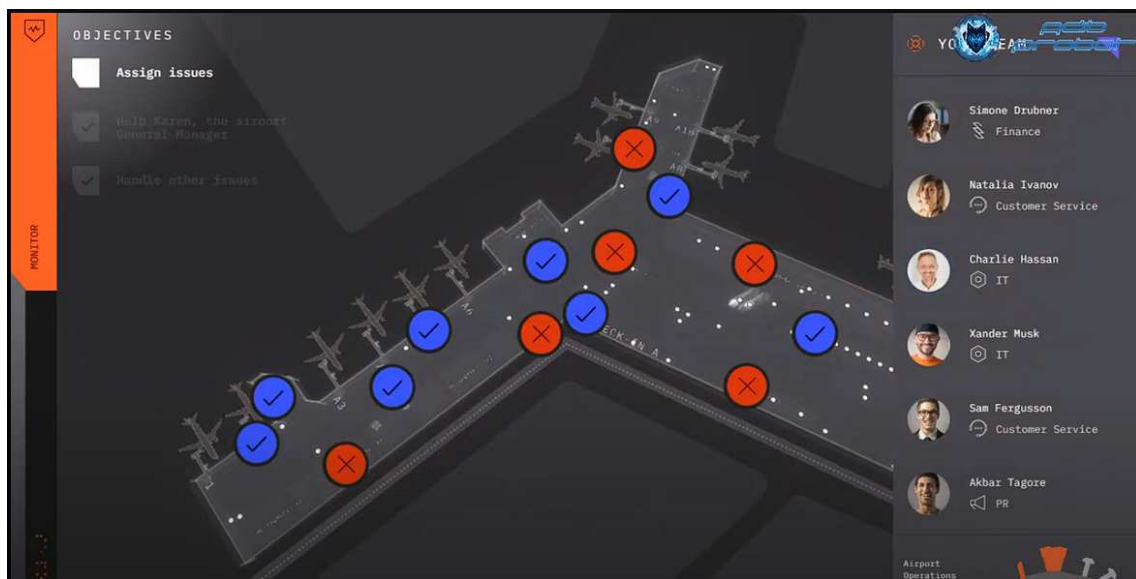
Ideja za aplikaciju dolazi iz dvije postojeće aplikacije. Prva aplikacija je CCS, simulator kibernetičkog napada koji je razvila tvrtka Utilis [2]. Simulator trenira zaposlenike firmi na stvarnoj postavi njihove mreže s realnim scenarijima kako bi bili kompetentniji u rješavanju napada i kako bi smanjili gubitke firme.



Slika 4.1. Sučelje CCS-a, preuzeto iz [2]

Druga aplikacija, Cyber Simulator OPS Terminal, aplikacija koju je razvio tim tvrtke

IBM, simulira napad na zračnu luku. Aplikacija je verzija IBM-ovog Cyber Range simulatora koja omogućava igračima da osjete stres i nevolju napada i da se nakon treninga znaju nositi s njom [15]. Glavna značajka igre je realni scenarij. Igra koristi detaljno izrađene scenarije koji simuliraju stvarne napade na zračnu luku. To uključuje različite vrste napada kao što su DDoS napadi, phishing, Ransomware napadi i unutarnje prijetnje. Korisnici mogu interaktivno komunicirati s različitim elementima unutar simulacije, uključujući sustave za nadzor, sigurnosne alate i mrežne resurse. Na slici 4.2. nalazi se sučelje u kojem se vidi skup interakcija na aerodromu.



**Slika 4.2.** Sučelje igre Terminal Ops, slika zaslona iz [16]

Obje aplikacije simuliraju slučajeve napada u 2D prostoru i prikazuju simulaciju napada. Ideja ovog rada je da se simulira napad, ali u 3D prostoru, kako bi ljudi dobili uvid kako to otprilike izgleda oko njih kad se događa.

## 4.2. Dizajn aplikacije Office Defence

Simulacija započinje unutar lifta i igrač dobiva upute kako se kreće i što mora napraviti. Lift je povezan na hodnik iz kojeg se ulazi u ured. Unutrašnjost ureda se sastoji od proizvoljnog broja računala i poslužitelj (*engl. server*) sobe koji su važni za simulaciju. Svako računalo i poslužitelji imaju iznad sebe indikator. Igrač pokretanjem simulacije aktivira nasumični indikator koji mijenja boju, dajući do znanja igraču da je to računalo zaraženo. Zatim nasumično kreće širenje po računalnoj mreži u uredu. Svako računalo

u uredu ima interaktivnu tipkovnicu na kojoj se mogu pisati naredbe za zaustavljanje širenja virusa i mogućnost gašenja računala kako bi ga se uklonilo s aktivne mreže. Igrač može započeti igru na slijepo ili može prikazati mrežu ureda koju je moguće paliti i gasiti na određenu interakciju. Igrač dobiva upute kako riješiti širenje virusa. Igrač pokušava unutar vremena zaštititi sva računala u uredu i taj postupak mu donosi bodove. Igra je zamišljena da na kraju prikupi bodove ovisno o potezima igrača i tako mu da povratnu informaciju koliko je bio uspješan.

## 5. Implementacija

Unutar ovog poglavlja opisane su tehnologije koje su se koristile za razvoj aplikacije Office Defence. Također, detaljno je opisan dizajne scena i proces razvoja igre. Kako igra funkcionira na principu bodovanja, dan je i pregled u bodove koji se mogu ostvariti tijekom igre.

### 5.1. Korištene tehnologije

#### 5.1.1. Unity

Unity je jedan od vodećih razvojnih alata za izradu interaktivnih 2D i 3D sadržaja, uključujući igre, simulacije i vizualizacije [17]. Unity je razvila tvrtka Unity Technologies i u lipnju 2005. predstavila na Worldwide Developers konferenciji tvrtke Apple kao Mac OS X softver za razvoj igara. Unity omogućava pisanje koda u jeziku C koristeći Mono, .NET razvojni okvir. Prethodno jeziku C, Unity je podržavao UnityScript, jezik koji je bio implementacija jezika JavaScript bazirana na jeziku Boo, te je bio korišten sve do verzije Unity 5 [18]. Unity nudi dva moderna kanala za renderiranje: High Definition Render Pipeline (HDRP) i Universal Render Pipeline (URP, ranije poznat kao Lightweight Render Pipeline ili LWRP). Uz njih, još uvijek postoji i naslijeđeni ugrađeni renderni sustav. Unity je podržan na sustavima Windows, Mac i Linux, a podržava izradu igara za više od 19 različitih platformi [17].

#### 5.1.2. Visual Studio Code

Visual Studio Code (*skr.* VSC) je uređivač koda razvijen od strane tvrtke Microsoft [19]. Ovaj alat je poznat po svojoj brzini, fleksibilnosti i širokom spektru značajki. Visual Studio Code podržava veliki broj programskih jezika i dolazi s integriranom podrškom za Git, što olakšava upravljanje verzijama koda. Jedna od najistaknutijih značajki Visual

Studio Codea je njegova ekstenzibilnost. Kroz bogatu biblioteku ekstenzija, korisnici mogu proširiti funkcionalnost uređivača prema svojim specifičnim potrebama.

### **5.1.3. Oculus Quest 2**

Meta Quest 2, ranije poznat kao Oculus Quest 2 je uređaj koji je razvila tvrtka Meta, prethodno poznata kao Facebook, 2020. godine [20]. Uređaj je opremljen s Qualcomm Snapdragon XR2 platformom i 6 GB RAM-a. Meta Quest 2 omogućuje glatko i brzo VR iskustvo. Uređaj ima dva LCD zaslona s ukupnom rezolucijom od 1832x1920 piksela po oku, što pruža oštru i jasnu sliku. Nadalje, podržava osvježavanje do 90 Hz, što doprinosi fluidnosti prikaza i smanjuje osjećaj mučnine kod korisnika.

### **5.1.4. XR Interaction Toolkit**

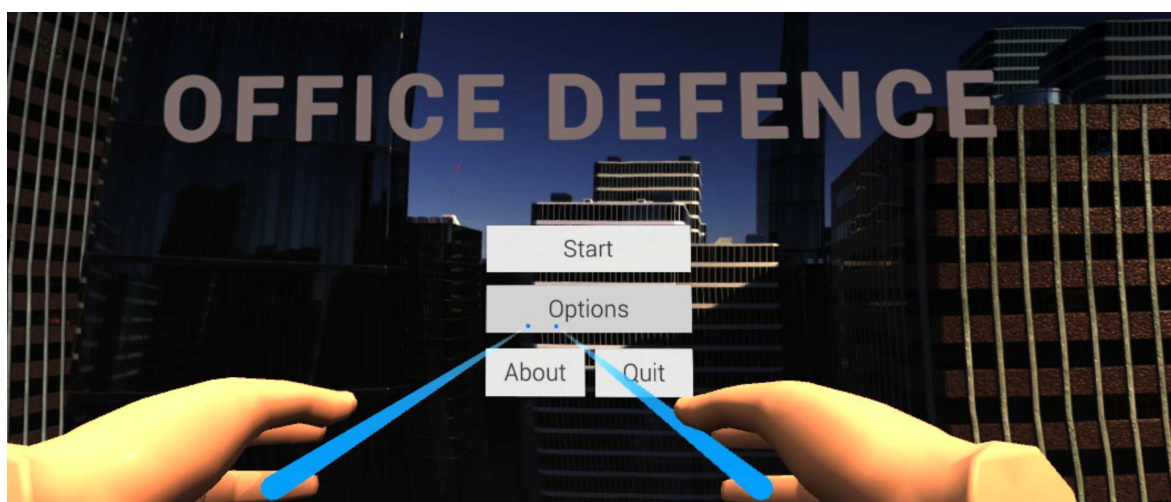
XR Interaction Toolkit je skup alata i komponenti razvijenih od strane tvrtke Unity za olakšavanje razvoja interaktivnih aplikacija u proširenoj (AR), virtualnoj (VR), i mješovitoj stvarnosti (MR) [21]. *XR Interaction Toolkit* se sastoji od nekoliko ključnih komponenti koje omogućavaju lako postavljanje i upravljanje interakcijama. Neke od korisnih komponenti koje se često koriste su *XR Controller*, *XR Interactable* i *XR Ray Interactor*. Komponente se koriste za povezivanje programa i hardvera ili za povezivanje interakcija unutar samog programa.

### **5.1.5. Unity Asset Store i Skechfab**

Unity Asset Store i Skechfab su stranice koje omogućuju dijeljenje 3D i 2D modela, zvukova i materijala kako bi olakšali i ubrzali proces razvoja aplikacija u Unityju. Obje virtualne trgovine nude raznovrsni spektar grafičkih elemenata, 3D modela i zvukova, kako bi olakšali kreiranje igara. Korisnici tamo mogu kupiti modele ili u nekim slučajevima i za besplatno preuzeti i koristiti. Obje stranice zahtijevaju od osobe da se registrira prije nego može kupovati i spremati dostupne resurse. Sučelje obje stranice je jako intuitivno i može se kao proširenje dodati u Unity Editor kako bi se koristilo bez prelaska u Internet preglednik.

## 5.2. Ekran izbornika

Pokretanjem igre, osobi se prikazuje početni ekran na kojem je izbornik. Osoba je smještena na zgradi i ispred nje se nalazi glavni izbornik. Okolina je izvedena s pomoću 360° slike koja je postavljena na unutarnji dio sfere i sama scena je smještena unutar sfere. Unutar scene izbornika igrač na obje ruke ima omogućenu komponentu *XR Ray Interactor* koja mu omogućava da odabere jednu od opcija na izborniku. Unutar kartice "opcije" (engl. *Options*) i kartice "o igri" (engl. *About*) korisnik može vidjeti neke podatke o igri. Opcija "izlaz" (engl. *Exit*) gasi aplikaciju, a opcija "početak" (engl. *Start*) prebacuje scenu na početak igre. Slika 5.1. prikazuje dizajn početnog izbornika i mogućnosti odabira.



**Slika 5.1.** Slika početnog ekrana

Početak i ulazak u igru napravljen je kao tranzicija između scena. Scena početnog izbornika nestane s pomoću efekta, prebaci se scena za igru i slika se prikaže s pomoću efekta pojavljivanja. Funkcija prima index scene za parametar i ima postavljen brojač, koji određuje duljinu nestanka i prikaza scene.

```

1
2 IEnumerator GoToSceneAsyncRoutine(int sceneIndex)
3     {
4         fadeScreen.FadeOut();
5         AsyncOperation operation = SceneManager.
6             LoadSceneAsync(sceneIndex);
7         operation.allowSceneActivation = false;
8
9         float timer = 0;
10        while(timer <= fadeScreen.fadeDuration && !
11            operation.isDone)
12        {
13            timer += Time.deltaTime;
14            yield return null;
15        }
16        operation.allowSceneActivation = true;
17    }

```

**Listing 5.1:** Funkcija za mijenje scene

## 5.3. Dizajn prostorija

### 5.3.1. Dizalo

Igrač započinje unutar dizala. Otvaraju se vrata i igrač može stupiti u hodnik. Dizalo je napravljeno s pomoću dva asseta<sup>1 2</sup>. Jedan predstavlja zidove i osvjetljenje u dizalu, a drugi predstavlja vrata dizala. Napravljena je animacija otvaranja i zatvaranja vrata dizala koja se može pokrenuti pritiskom na gumb. Animacija je napravljena tako da igrač može rukom proći (*engl. Hover*) preko određenog dijela dizala i vrata se otvore, čime je postignut efekt pritiska na gumb koji poziva dizalo.

<sup>1</sup><https://sketchfab.com/3d-models/elevator-building-c720d61408e8424289ffeb6ebef694e1>

<sup>2</sup><https://sketchfab.com/3d-models/elevators-8cf806c0b2d84871bac9d4f203ae3b1f>

### 5.3.2. Hodnik

Hodnik je napravljen uz pomoć ploči koje predstavljaju zidove i ploči s prozirnim materijalom koji predstavlja prozore. U hodniku se može ponovno stisnuti gumb za dizalo i ući u dizalo ili proći kroz vrata koja vode u ured.

Vrata u igri su napravljena uz pomoć besplatnog asseta<sup>3</sup> koji nudi mogućnost postavljanja kuta na rubu vrata, te tako simulira šarke na vratima. Osim toga, uz pomoć skripte i nevidljivog objekta postavljenog na kvaku vrata, napravljena je mogućnost da se vrata otvaraju uz pomoć animacije hvatanja. Objekt ima komponentu *XR Grab Interactable*, koja omogućava interakciju igrača s tim objektom, a skripta prima element *Rigidbody* vrata i mijenja poziciju vrata s obzirom koliko je nevidljivo tijelo pomaknuto. Na slici 5.2. nalaze se lijevo prozori, u sredini dizala i desno vrata od ureda.



Slika 5.2. Slika hodnika

### 5.3.3. Ured

Dio ureda je preuzet kao besplatni asset<sup>4</sup> sa SkechFab-a, te je nadograđen kako bi odgovarao potrebama igre. Prolaskom kroz vrata iz hodnika se ulazi u ured. Prva vrata nakon ulaza s lijeve strane vode u prostoriju s poslužiteljima. Nakon prostorije s poslužiteljima ulazi se u veliki prostor u kojem su raspoređena računala. Ured sadrži jedanaest računala raspoređenih na 3 seta stolova. Ured još sadrži sobu za sastanke i dva toaleta.

<sup>3</sup><https://assetstore.unity.com/packages/3d/props/interior/door-free-pack-aferar-148411>

<sup>4</sup><https://sketchfab.com/3d-models/mersus-office-8714be387bcd406898b2615f7dae3a47>



## 5.4. Računala

Računala su glavni objekt ove igre. Svako računalo sastoji se od mrežnog čvora, tipkovnice, računalnog kućišta i zaslona(*engl. monitor*) koji prikazuje prozor naredbenog retka (*engl. Command Prompt Window*). Igrač ima pristup tipkovnici na kojoj je omogućeno tipkanje prstima ili interakcija zrakom iz ruke. Kućište računala ima interaktivni gumb koji igrač može pritisnuti. Slika 5.3. prikazuje kako izgleda računalo. Crvena kugla iznad tipkovnice predstavlja mrežni čvor računala.



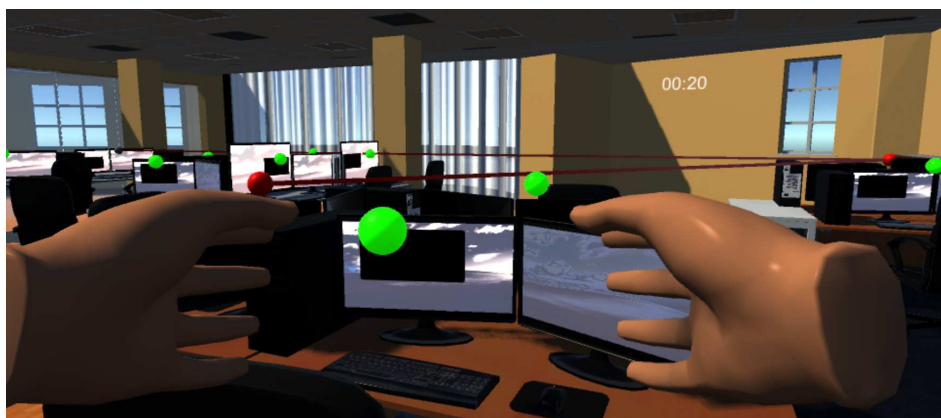
**Slika 5.3.** Slika računala

## 5.5. Zaraza računala

Glavni cilj igre je spasiti računala od zaraze virusom. Na početku igre jedno računalo je zaraženo i od njega se širi zaraza prema ostalim računalima koja su povezana. Čvorovi mreže su primarno nevidljivi igraču, te ih on može prikazati pritiskom na gumb upravljača. Mrežni čvorovi su obojeni u boje koje predstavljaju stanja računala. Primarno su svi čvorovi zelene boje, što simbolizira nezaraženo računalo. Crvena boja mrežnog čvora predstavlja računalo u opasnosti. Na početku je zaraženi čvor postavljen na crveno i svaki sljedeći na koji se pokuša spojiti indicira opasnost crvenom bojom. Plava i siva boja rezervirane su za prikaz nakon pokušaja zaraze računala. Plava kuglica signalizira uspješno spašeno računalo, a siva signalizira računalo koje je isključeno iz mreže, tj. zaraženo. Igrač kad je spreman započne napad.

Zaraženo računalo počinje širiti virus kroz mrežu i igrač može, ako upali mrežne čvorove, točno vidjeti prema kojem računalu se zaraza širi. Kako bi igrač zaštitio računala od širenja mora poduzeti jednu od tri radnje. Prva radnja je da isključi računalo na pritisak gumba na kućištu i time deaktivira računalo s mreže. Drugi i treći način su da u prozor komandne linije upiše jednu od naredbi koja će ili pokušati nadograditi zaštitu na računalu ili gasi računalu pristup mreži.

Uspije li igrač na bilo koji od navedena tri načina spasiti računalo od zaraze, virus pokuša nakon nekog vremena napasti neko drugo računalo. Igra traje dok virus ima računala koja su na mreži dostupna. Na slici 5.4. prikazano je širenje po mreži. Desno računalo je inicijalno zaraženo i crvenim linijama je prikazano koje računalo pokušava zaraziti.



**Slika 5.4.** Slika širenja virusa

Računala su u Unityju objekti koji se sastoje od:

- mrežnog čvora, prikazanog s pomoću objekta sfere
- tipkovnice i prozora naredbenog retka
- kućišta računala.

Tipkovnica je skriptom povezana s naredbenim retkom koji je napravljen s pomoću objekta tipa *Canvas* koji sadrži objekt tipa *TextArea*. Unutar alata *XR Interaction Toolkit* dostupne su različite točke ruku. Vrh kažiprsta je namješten da radi interakciju pri dodiru tipke na tipkovnici i time je postignut efekt tipkanja po tipkovnici. Također, tipkanje tipkovnicom je omogućeno i zrakom koja ide iz ruke.

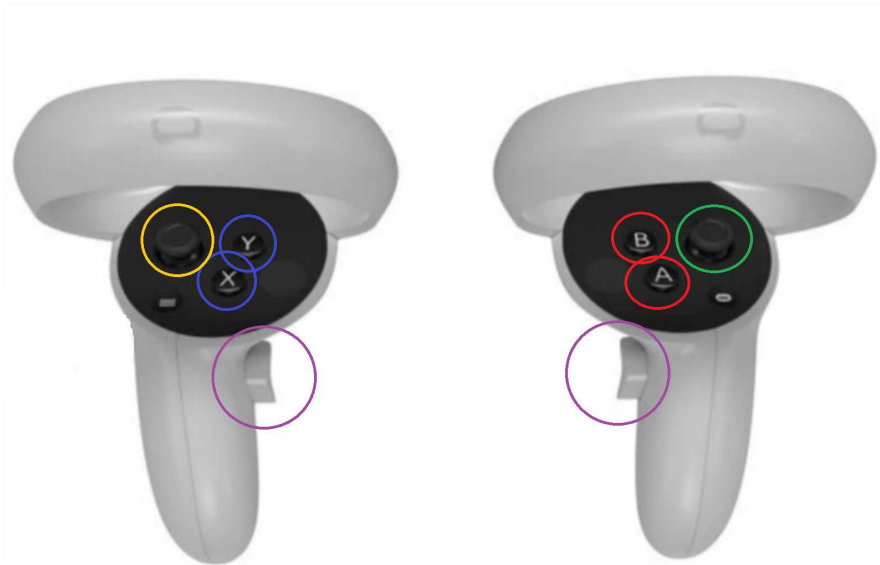
Kućište računala izvedeno je slično kao mehanizam otvaranja vrata na dizalu. Prelaskom prsta preko gumba na računalu pokreće se skripta koja gasi računalo.

## 5.6. Mehanizam igrača

Igrač je napravljen tako da se može kretati u prostoru, rotirati ili uz pomoć upravljača ili uz pomoć okretanja glave. Osim toga, igraču su dodane mogućnosti hvatanja stvari i ispućavanja zrake u smjeru ruke. Dodatno, igrač na upravljačima ima gumbе kojima su pridijeljene određene radnje. Na slici 5.5. zaokruženo žutom i zelenom bojom su gljivice kojima se igrač kreće i okreće. Crveno zaokružanim gumbima igrač može prikazivati i skrivati čvorove mreže i poveznice kojima se virus pokušava širiti. Ostali gumbi koriste se radnje hvatanja i ispaljivanja zrake s pojedinom rukom. Usprkos tome što većina igri u virtualnoj stvarnosti ima mogućnost teleportiranja, zbog kompaktnog prostora i poante realističnog kretanja, ovdje je onemogućena.

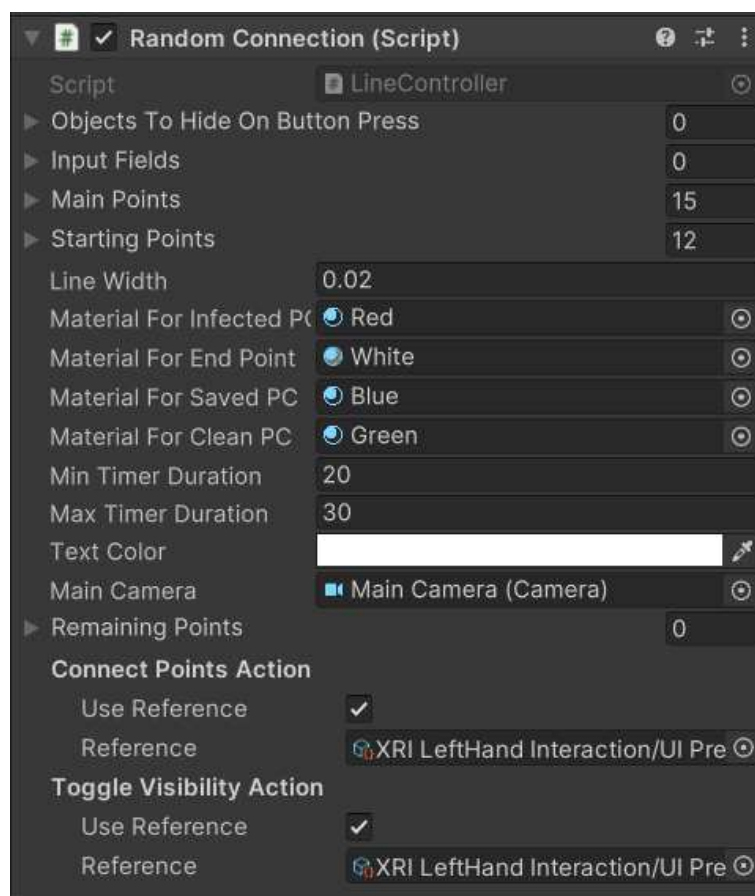
## 5.7. Mehanizam širenja virusa

Širenje virusa napravljen je skriptom. Koristi se dvije liste točaka, jedna sadrži sva računala koja mogu biti inicijalno zaražena, a druga sadrži sva računala u mreži. Pri pokretanju igre, nasumično se izabire računalo iz liste računala koja mogu inicijalno biti zaražena i to se postavlja kao početna točka programa. Zaraženo računalo od ostalih se



**Slika 5.5.** Slika kontrolera

razlikuje po boji. Slika 5.6. prikazuje komponentu koja sadrži skriptu za povezivanje čvorova u mreži.



**Slika 5.6.** Slika komponente za mrežu računala

Implementiran je i brojač koji broji vrijeme potrebno za zarazu računala. Funkcija *UpdateTimer* računa vrijeme i zapisuje ga u obliku "mm:ss" i poziva se unutar funkcije *Update()* koja se poziva svaki okvir vremena. Brojač određuje duljinu trajanja igre i pomaže igraču odrediti koji mu je najbolji potez za napraviti. Za iscrtavanje linije je korištena komponenta *LineRenderer* koja služi za iscrtavanje linije između dviju točaka.

```
1 void UpdateTimer()
2     {
3         if (!stopConnection)
4         {
5             currentTimer -= Time.deltaTime;
6             currentTimer = Mathf.Max(0f, currentTimer);
7             if (currentTextMesh != null)
8             {
9                 int minutes = Mathf.FloorToInt(currentTimer
10                    / 60.0f);
11                 int seconds = Mathf.FloorToInt(currentTimer
12                    % 60.0f);
13                 currentTextMesh.text = string.Format("
14                    {0:00}:{1:00}", minutes, seconds);
15             }
16         }
17     }
```

**Listing 5.2:** Funkcija za brojač

Računalo koje je odabrano kao inicijalno računalo miče se iz liste računala koja se mogu zaraziti. Ostala računala se nasumično biraju iz te liste. Odabrano računalo šalje su u funkciju za crtanje linije, odabire se nasumično vrijeme brojača i započinje simulacija pokušaja širenja na drugo računalo. Kako bi se istovremeno mijenjao brojač i spajale linije koristi se mehanizam korutine. Unity koristi taj mehanizam na način da može pauzirati izvođenje metode u određenom trenutku i prepustiti izvođenje Unityju, ali po završetku Unityjevog zadatka nastavi izvršavanje metode na mjestu gdje je stala. Iako se čini kao da su korutine različit dretve, to nije tako. Korutine se sve izvode na istoj dretvi sinkrono.

```
1     private void OnConnectPointsPressed (InputAction .
      CallbackContext context)
2     {
3         if (!connectOnKeyPress)
4         {
5             StartCoroutine (ConnectPoints ());
6             connectOnKeyPress = true;
7         }
8     }
```

**Listing 5.3:** Funkcija za pokretanje simulacije

```
1     public void StopConnectionOnTouch ()
2     {
3         stopConnection = true;
4         StopCoroutine (ConnectPoints ());
5     }
```

**Listing 5.4:** Funkcija za pokretanje simulacije

Dvije navedene funkcije koriste se za pokretanje i zaustavljanje simulacije. U slučajevima kada igrač uspije zaštititi računalo koristi se funkcija *StopConnectionOnTouch()* kojom se prekida spajanje čvorova. Taj mehanizam koristi se kako bi se uklonio čvor iz liste i premjestio u listu spašenih računala. Nakon toga postavlja se odgoda brojača kojom igrač dobiva vremena da pogleda koje će sljedeće računalo biti zaraženo. Nakon

isteka brojača ponovno se pokreće korutina kako bi se spojile dvije linije i pustio brojač da odbrojava preostalo vrijeme.

Na početku igre čvorovi mreže nisu vidljivi, ali što više vremena prolazi i što se više čvorova spoji to postaje teže za snalaziti se po uredu. Mehanizam paljenja i gašenja čvorova služi osobi u isto vrijeme da vidi mrežu, ali isto može poslužiti i da ugasi mrežu da mu ne smeta. Funkcija je napravljena na način da se mijenja vrijednost bool varijable i postiže efekt paljenja i gašenja mreže. Svi čvorovi se na početku igre dodaju u listu *objectsToHideOnButtonPress*, a poveznice između čvorova se dodaju kako se generiraju.

```
1 public void ToggleObjectsVisibility()
2 {
3     visible = !visible;
4     foreach (GameObject obj in
5         objectsToHideOnButtonPress)
6     {
7         obj.SetActive(!obj.activeSelf);
8     }
9 }
```

**Listing 5..5:** Funkcija za vidljivost mreže

## 5.8. Spašavanje računala

Igrač kada vidi koje računalo je u opasnosti prvo mora doći do njega. Ovisno o vremenu koje mu je ostalo ima tri opcije:

- Isključiti računalo
- Upisati naredbu `updateSecurity.exe`
- Upisati naredbu `run.exe`.

Opcija isključivanja je napravljena tako da kada osoba pređe prstom preko gumba za gašenje, pošalje se signal koji pokrene funkciju zaustavljanja korutine. Prethodno već objašnjeno, funkcija zaustavljanja korutine označi čvor kao spašen i pokrene brojač

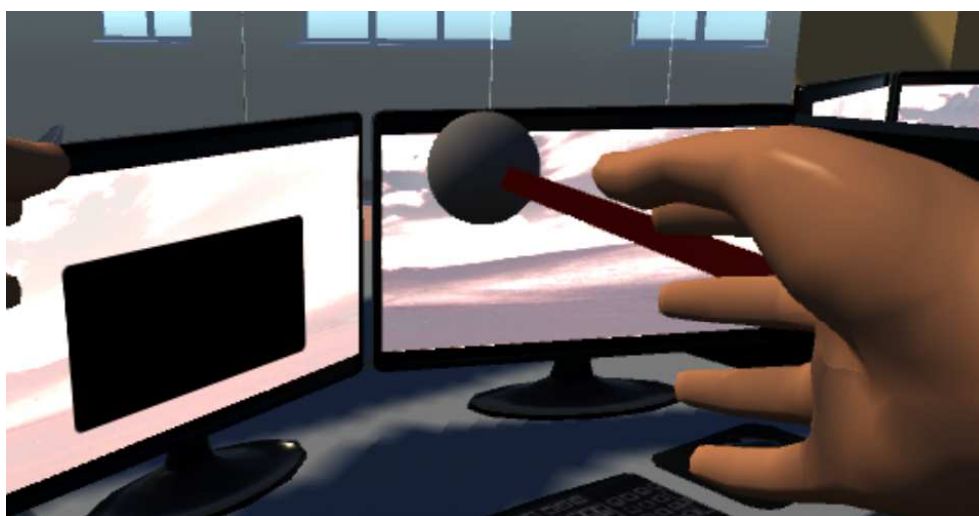
odgode između napada.

Opcije upisivanja naredbi se izvršavaju s pomoću tipkovnice. Interaktivna tipkovnica je inicijalno nevidljiva, odnosno deaktivirana. Pritiskom ruke na prozor naredbenog retka otvara se interaktivna tipkovnica i igrač može u nju napisati naredbe. Uspije li igrač na vrijeme upisati točnu naredbu pozvat će se funkcija zaustavljanja korutine. Slika 5.7. prikazuje promjenu boje na čvoru mreže koji je uspješno zaštićen na vrijeme.



**Slika 5.7.** Slika spašenog čvora

U slučajevima gdje igrač ne uspije upisati točne naredbe ili ne uspije isključiti računalo na vrijeme čvor će se isključiti iz mreže i računalo će biti zaraženo, te će se napad automatski nastaviti na drugo računalo. Slika 5.8. prikazuje promjenu boje na čvoru koji nije na vrijeme zaštićen.



**Slika 5.8.** Slika zaraženog čvora



## 5.9. Proces bodovanja

Igra je zamišljena da ima sustav bodovanja koji ovisi o akcijama koje igrač odigra. Svaka komponenta u uredu vrijedi određeni broj bodova. Pošto su u uredu poslužitelji i obična računala, poslužitelji vrijede više bodova. Svaka akcija donosi određeni broj bodova. Pošto je akcija upisivanja naredbe za nadogradnju systemske zaštite najdulja ta akcija će donositi najviše bodova. Sljedeća po redu je akcija za odspajanja računala s mreže koja će donositi drugi najveći broj bodova, a najmanje bodova je predviđeno za najlakšu i najbržu akciju, gašenje računala.

Osim pozitivnih bodova, svaki puta kada igrač ne uspije na vrijeme zaštititi računalo dobiva negativne bodove. Kako igrač vremenski ima drugačije intervale između dvaju računala koja simulacija pokušava zaraziti, tako je i broj negativnih bodova proporcionalan tome. U tablici 5.1. prikazan je broj bodova dodijeljen akcijama.

<b>Akcija</b>	<b>Broj bodova</b>	<b>Bonus bodovi za vrijeme</b>
Gašenje računala na gumb	0	0
Upisivanje naredbe za isključivanje s mreže	2	1
Upisivanje naredbe za nadogradnju sustava	3	2
Neuspjelo spašavanje računala	-2	-
Neuspjelo spašavanje poslužitelja	-4	-

Tablica 5.1. Tablica bodova

## 5.10. Nedostaci i mogućnost proširenja igre

Igra je zamišljena kako bi igrač imao više mogućih scenarija i više mogućih napada. Trenutna verzija igre ima donekle različite scenarije pošto se početna točka svaki puta bira nasumično, brojač između dva računala se bira nasumično i točke koje se spajaju se biraju nasumično.

Također, kao jedna vrsta proširenja je mogućnost dodavanja proizvoljnog broja računala i poslužitelja, te dodavanja različitih soba ili ureda. Ako bi osoba uspješno spasila sva računala unutar manjeg ureda, mogla bi odabrati veći ured s manje vremena između napada, čime se povećava težina igre i izazovnost za igrača. Osim toga, postoji mogućnost dodavanja novih akcija koje bi ovisile o vrsti napada. Kako nisu svi napadi isti, ako bi se dodalo više scenarija različitih napada bilo bi potrebno napraviti dodatne akcije koje

igrač može odigrati kako bi spriječio napad.

Kroz igru bi se također mogla uvesti mehanika upravljanja resursima, gdje bi igrač morao balansirati između različitih aspekata sigurnosti, poput alokacije proračuna za sigurnosne alate i održavanje sustava. Ovaj aspekt igre povećao bi dubinu i složenost, omogućujući igračima da razvijaju strategije i prioritiziraju aktivnosti prema specifičnim prijetnjama i resursima na raspolaganju. Daljnje proširenje igre moglo bi uključivati dinamične scenarije koji se prilagođavaju na temelju igračevih odluka i performansi.

## 6. Zaključak

Povećanjem kibernetičkog prostora i povećanjem sigurnosnih mjera za sustave i dalje ne možemo reći da su sigurni. Prema podacima iz 2023. godine vidljivo je da su kibernetički napadi i dalje česta pojava. Iako je danas jako teško zaobići zaštite sustava i programa, čovjek, svojim neznanjem i nepažnjom, je i dalje lagana meta napada. Postoje simulatori koje firme koriste kako bi bolje obrazovale svoje zaposlenike u području kibernetičke sigurnosti, kao što je na primjer IBM Cyber Range, a isto tako postoje i simulatori koji podučavaju timove koji reagiraju tijekom napada i pokušavaju smanjiti ili potpuno otkloniti štetu, kao na primjer CCS.

Ubrzani rast imerzivnih tehnologija unazad dvadeset godina znatno doprinosi dostupnosti uređaja za te tehnologije. Virtualna stvarnost, kao jedan od predstavnika imerzivnih tehnologija, koristan je alat u simulacijama. Postavljanje ljudi u 3D prostor, znatno se doprinosi povećanju realnosti slučaja. Tehnologija virtualne stvarnosti tako se može iskoristiti za simulaciju treninga kibernetičke sigurnosti.

U okviru ovog rada, miješanjem virtualne stvarnosti i simulatora kibernetičkog treninga odrađen je jedan scenarij kibernetičkog napada na ured. Cilj igre je da igrač pokuša unutar zadanog vremena obraniti što više računala od napadača koji pokušava zaraziti sva računala. Igrač prikazivanjem mreže ureda saznaje koja su računala zaražena i kako se zaraza širi. Na kraju simulacije povratnu informaciju dobiva u obliku bodova koji su zbroj njegovih akcija.

Igra ima mogućnosti proširenja, ako bi se išlo u daljnje razvijanje. Proširenja igre mogu biti u broju računala, veličini ureda i u broju scenarija. Različite vrste napada dovode do novih akcija koje su potrebne za obranu.

## Literatura

- [1] P. C. van Oorschot, “Tools and jewels from malware to bitcoin”, u *Computer Security and the Internet*, 2021., str. 2–28.
- [2] <https://ccs.utilis.biz/>, [mrežno; stranica posjećena: 29.5.2024.].
- [3] A. Nagarajan, J. M. Allbeck, A. Sood, i T. L. Janssen, “Exploring game design for cybersecurity training”, u *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, 2012., str. 256–262.  
<https://doi.org/10.1109/CYBER.2012.6392562>
- [4] Leksikografski zavod Miroslav Krleža, “Virtualna stvarnost”, Hrvatska enciklopedija, mrežno izdanje, 2013–2024., [Mrežno; pristupljeno 28.5.2024.]. [Mrežno].  
Adresa: <https://www.enciklopedija.hr/clanak/virtualna-stvarnost>
- [5] M. V. Sanchez-Vives i M. Slater, “From presence to consciousness through virtual reality”, *Nature Reviews Neuroscience*, sv. 6, str. 332–339, 2005.  
<https://doi.org/10.1038/nrn1651>
- [6] V. R. Society. (2024) The history of virtual reality. Pristupljeno: 29.5.2024. [Mrežno].  
Adresa: <https://www.vrs.org.uk/virtual-reality/history.html>
- [7] <https://www.cnet.com/tech/gaming/best-vr-headset/>, [mrežno; stranica posjećena: 10.6.2024.].
- [8] <https://www.sensortips.com/featured/what-sensors-are-used-in-ar-vr-systems-faq/>, [mrežno; stranica posjećena: 10.6.2024.].
- [9] M. Slater, M. Usoh, i A. Steed, “Depth of presence in immersive virtual environments”, *Teleoperators and Virtual Environments - Presence*, sv. 3, 01 1994.

- [10] <https://virtualspeech.com/blog/history-of-vr>, [mrežno; stranica posjećena: 9.6.2024.].
- [11] Leksikografski zavod Miroslav Krleža, “Virtualna stvarnost”, Hrvatska enciklopedija, mrežno izdanje, 2013–2024., [Mrežno; pristupljeno 28.5.2024.]. [Mrežno]. Adresa: <https://www.enciklopedija.hr/clanak/kibernetika>
- [12] Emma Johns, Maddy Ell, <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023>, [mrežno; stranica posjećena: svibanj 2024.].
- [13] P. C. van Oorschot, “Tools and jewels from malware to bitcoin”, u *Computer Security and the Internet*, 2021., str. 127–154.
- [14] <https://attack.mitre.org/>, [mrežno; stranica posjećena: 3.6.2024.].
- [15] <https://www.northkingdom.com/case/ibm-terminal>, [mrežno; stranica posjećena: 29.5.2024.].
- [16] <https://www.youtube.com/watch?v=Pv4Wjzsj1M4>, minuta videa: 13:00.
- [17] [https://en.wikipedia.org/wiki/unity\\_\(game\\_engine\)](https://en.wikipedia.org/wiki/unity_(game_engine)), [mrežno; stranica posjećena: 29.5.2024.].
- [18] <https://web.archive.org/web/20171017210326/https://unity3d.com/unity/whats-new/unity-5.0>), [mrežno; stranica posjećena: 29.5.2024.].
- [19] <https://code.visualstudio.com/docs>, [mrežno; stranica posjećena: 3.6.2024.].
- [20] <https://www.meta.com/quest/>, [mrežno; stranica posjećena: 3.6.2024.].
- [21] <https://docs.unity3d.com/Packages/com.unity.xr.interaction.toolkit@3.0/manual/index.html>, [mrežno; stranica posjećena: 30.6.2024.].

## Popis slika

2.1. Slika VR opreme, preuzeto iz [10] . . . . .	7
3.1. Postotak tvrtki koje su iskusile kibernetički napad, preuzeto iz [12] . . . . .	9
3.2. Vrste napada u postotku, preuzeto iz [12] . . . . .	9
3.3. MITRE ATT&CK baza, slika zaslona iz [14] . . . . .	11
4.1. Sučelje CCS-a, preuzeto iz [2] . . . . .	12
4.2. Sučelje igre Terminal Ops, slika zaslona iz [16] . . . . .	13
5.1. Slika početnog ekrana . . . . .	17
5.2. Slika hodnika . . . . .	19
5.3. Slika računala . . . . .	20
5.4. Slika širenja virusa . . . . .	21
5.5. Slika kontrolera . . . . .	23
5.6. Slika komponente za mrežu računala . . . . .	23
5.7. Slika spašenog čvora . . . . .	27
5.8. Slika zaraženog čvora . . . . .	27

# Sažetak

## Razvoj aplikacije u virtualnoj stvarnosti za simuliranje kibernetičkog napada

Borna Petak

Rad daje kratak uvod u virtualnu stvarnost, gdje i kako se koristi. Također, opisana je i povijest razvoja virtualne stvarnosti i tehnologije koje se koriste u razvoju aplikacija za virtualnu stvarnost. Potom je dan kratak uvod u kibernetičku stvarnost i opisano je što je kibernetički prostor. Nadalje, objašnjeni su napadi i koje su motivacije za njih, te kako se brani od njih. U nastavku rada dan je pregled aplikacija koje su bile motivacija za rad i opisano je kako je zamišljena aplikacija. Popisane su i ukratko opisane korištene tehnologije u radu. Na kraju slijedi opis kako je igra postignuta i na koji način se igra.

**Ključne riječi:** Virtualna stvarnost; Kibernetička sigurnost; Kibernetički napadi; Unity

# **Abstract**

## **Development of a Virtual Reality-Based Application for Simulating a Cyber Attack**

Borna Petak

This paper provides a brief introduction to virtual reality, where and how it is used. Also, The history of development of virtual reality and technologies used in development of virtual reality applications are described. Then a short introduction to cyber reality is given and is described what cyberspace is. Within that chapter, attacks are explained, what are the motivations for them, and how to defend against them. Technologies used in the work are listed and briefly described. Description of the application gives an overview of the applications that were motivation for the work and describes how the idea for application was born. At the end follows a description of how the game was achieved and how it is played.

**Keywords:** Virtual reality; Cyber security; Cyber attacks; Unity