Memoriu științific

Subsemnatul Prof.univ.dr. **Dorin-Mircea POPOVICI**, în calitate de conducător de doctorat al doctorandei **Rebecca ACHEAMPONG**, autor al tezei de doctorat cu titlul "**Addressing Cybersecurity Concerns in Virtual Reality Applications**", în urma studierii tezei de doctorat am constatat următoarele:

1. Aspecte generale referitoare la teză. Actualitatea tematicii

Digitalizarea tot mai mare a societății și integrarea pe scară largă a tehnologiilor avansate în viața de zi cu zi au extins semnificativ peisajul amenințărilor de securitate cibernetică. Printre aceste tehnologii, Realitatea Virtuală (RV) a evoluat rapid de la un concept de nișă într-un mediu transformator, remodelând sectoare precum jocurile, educația, asistența medicală, colaborarea între întreprinderi și introducând noi vulnerabilități care sunt fundamental diferite de cele ale mediilor de calcul tradiționale. Acestea includ amenințări care decurg din interacțiunile în timp real, calculul spațial, datele senzorilor, integrarea biometrică și ingineria socială în medii imersive.

Teza intitulată "Addressing Cybersecurity Concerns in Virtual Reality Applications" ("Abordarea preocupărilor de securitate cibernetică în aplicațiile de realitate virtuală") își propune investigarea peisajului unic de amenințări al sistemelor de RV și propunând soluții de securitate robuste, practice și centrate pe utilizator.

În acest sens, a fost introdusă o taxonomie structurată a amenințărilor, care clasifică riscurile utilizând triada CIA (Confidentiality, Integrity, and Availability / Confidențialitate, Integritate și Disponibilitate) și vectori de atac obișnuiți, cum ar fi exploit-uri hardware, vulnerabilități software, atacuri bazate pe rețea și tactici de inginerie socială. În plus, au fost efectuate mai multe studii de caz în lumea reală, inclusiv evaluarea unei vulnerabilități API (CWE-359) pe o platformă de jocuri de RV, precum și testarea de penetrare pe dispozitivele Oculus Quest 2. Aceste explorări practice au evidențiat puncte slabe critice, cum ar fi expunerea datelor, execuția APK rău intenționată, abuzul excesiv de permisiuni și gradul de conștientizare slab al utilizatorilor.

Pe baza acestor constatări, cercetarea a dezvoltat și validat strategii de atenuare a securității integrate direct în sistemele imersive. În plus, teza investighează și echilibrul dintre

utilizabilitate, experiență (a utilizatorului), confidențialitate și securitate, efectuând un studiu al utilizatorului pentru a explora modul în care mecanismele de securitate pot fi integrate perfect, fără a perturba imersiunea.

2. Aprecierea con inutului tezei

Prezenta teză este organizată sub forma a 6 (șase) capitole conținând 75 de figuri și 11 tabele, concluzii, o bibliografie ce cumulează 236 de titluri, fără a socoti și contribuțiile doctorandei, și 8 (opt) anexe după cum urmează.

Capitolul 1: **Introduction** - prezintă argumentele și motivația cercetării, subliniind riscurile de securitate inerente în tehnologiile de realitate virtuală și importanța abordării acestora. Autoarea identifică punctele slabe în cercetare și articulează scopurile și obiectivele care-i ghidează prezentul demers și anume *O1 – Identificarea și analiza vulnerabilităților de securitate cibernetică în sistemele de realitate virtuală*; *O2 – Evaluarea cadrelor de securitate cibernetică existente și limitările acestora*; *O3 – Realizarea de studii de caz în lumea reală și evaluarea riscurilor; O4 – Evaluarea echilibrului dintre utilizabilitate, securitate și confidențialitate în VR; O5 – Implementarea și validarea atenuărilor de securitate în mediile de RV*.

Capitolul 2: **Cybersecurity Concerns and Mitigation Strategies** - oferă o analiză cuprinzătoare a amenințărilor de securitate cibernetică în RV, prezintă o revizuire aprofundată a strategiilor de atenuare de ultimă generație, subliniind progresele actuale în securizarea spațiilor digitale imersive și include un studiu de caz al simulărilor de amenințări din lumea reală, efectuând o evaluare a riscurilor pentru a valida constatările și a consolida peisajul de securitate în mediile de RV.

Capitolul următor - **Balancing Usability, User Experience, Security, and Privacy in VR Systems** - explorează relația dintre utilizabilitate, experiența utilizatorului, securitate și confidențialitate în realitate virtuală, dezvoltând un model pentru a aborda acești factori conflictuali, evidențiind modul în care securitatea centrată pe utilizator și designul incluziv pot îmbunătăți securitatea aplicațiilor de RV.

Capitolul 4: **Enhancing Security and Authenticity in Immersive Environments** - propune integrarea semnăturilor digitale criptografice folosind RSA-2048 și SHA-256 pentru a asigura autenticitatea și integritatea artefactelor virtuale în medii imersive.

Integrarea unui cadru de securitate cu mai multe straturi pentru protejarea mecanismelor de autentificare, managementul sesiunilor și sistemele backend în timp real pe platforma GENSAVR este realizată în capitolul 5: **Security Integration and Enhancement in the GENSAVR Platform**. Îmbunătățirile de securitate includ: Nakama pentru autentificare sigură, Kubescape pentru scanarea de securitate Kubernetes și ARMO pentru monitorizarea securității.

Deoarece tehnologiile imersive implică colectarea de date multimodale (urmărirea mișcării, urmărirea privirii, recunoașterea biometrică, etc.), acest lucru generează noi provocări în ceea ce privește confidențialitatea. Capitolul - **Real-Time Adaptive Security for Privacy and Compliance in Immersive Applications** – explorează un model de securitate adaptiv în timp real conceput pentru a impune conformitatea și confidențialitatea datelor în aplicațiile imersive în funcție de locația utilizatorului, asigurând menținerea drepturilor de confidențialitate ale utilizatorilor în spațiile digitale și atenuând riscurile de securitate în Metaverse.

In - **Final Conclusions, Original Contributions, and Future Directions** – autoarea rezumă rezultatele cercetării, evidențiind contribuțiile sale originale, prezentând modalitățile de diseminare a cercetării, discutând despre posibilele aplicații din lumea reală, pericolele și limitările actuale, dar și despre direcțiile viitoare de cercetare care vor duce la creșterea eficienței cadrelor de securitate cibernetică în RV.

După o bibliografie impresionantă, teza se încheie cu 8(opt) anexe (Annex 1.1-Annex 1.8) ce conțin scurte descrieri ale modulelor software implementate de autoare.

3. Evaluarea contribu iilor originale

Prezenta teză aduce câteva contribuții originale în domeniul securității cibernetice la nivelul aplicațiilor de realitate virtuală, abordând clasificarea amenințărilor, evaluarea riscurilor, implementarea securității, cadrele de conformitate și considerații de utilizabilitate ale medii imersive. Contribuțiile originale ale prezentei teze sunt enumerate în cele ce urmează:

A. Categorizarea cuprinzătoare a amenințărilor la securitatea cibernetică în realitate virtuală

1. A dezvoltat un model de clasificare dublă, care clasifică amenințările bazate pe Triada CIA și vectori de atac.

2. A realizat o analiză sistematică a amenințărilor emergente, inclusiv atacuri însoțitoare, umane atacuri cu joystick, atacuri inițiale și atacuri MITR, contextualizând impactul acestora în medii de RV.

B. Studii de caz empirice și evaluarea riscurilor amenințărilor în realitate virtuală

1. A realizat simulări de amenințări din lumea reală pentru a evalua vulnerabilitățile practice în aplicațiile imersive.
2. A dezvoltat un cadru de evaluare a riscurilor pentru a cuantifica impactul potențial al atacurilor asupra utilizatorilor realităților extinse, confidențialității datelor și securității sistemului.
3. A efectuat o Evaluare a Vulnerabilității la Expunerea PII utilizând OWASP ZAP, analizând răspunsuri API configurate greșit pe o platformă de jocuri RV care a expus date financiare sensibile (CWE-359: Expunerea informațiilor sensibile).

C. Implementarea semnăturilor digitale criptografice pentru integritatea bunurilor virtuale

1. A proiectat și implementat un mecanism de semnătură criptografică folosind RSA-2048 și SHA-256 pentru a asigura autenticitatea și integritatea bunurilor digitale în mediile de realitate virtuală.
2. A dezvoltat un proces intuitiv de semnare și verificare care îmbunătățește securitatea respectând gradul de utilizabilitate.
3. A realizat evaluări de performanță, ce au demonstrat o latență scăzută în semnare (17,3 ms) și o verificare instantanee, făcând soluția scalabilă pentru aplicații de realitate virtuală în timp real.

D. Dezvoltarea unui cadru de securitate adaptabil pentru confidențialitate și conformitate

1. A propus și integrat un model de securitate adaptiv în timp real care ajustează dinamic colectarea datelor, politici de confidențialitate și protocoale de securitate bazate pe locația utilizatorului și cerințele de conformitate ale acestuia.
2. Utilizarea detectării geolocalizării (IPInfo API, urmărire prin GPS) pentru a aplica reglementările transfrontaliere de protecție a datelor, abordând problemele legate de confidențialitate în aplicațiile Metaverse și de RV globale.

E. Îmbunătățirea securității platformei GENSAVR

1. A integrat Nakama pentru autentificare, Kubescape pentru scanarea de securitate Kubernetes și ARMO pentru monitorizarea securității pentru a securiza platforma de realitate virtuala GENSAVR.

2. A efectuat scanări de conformitate NSA și evaluări ale vulnerabilităților pentru a identifica și a atenua riscurile de securitate în implementările volumului de lucru, configurațiile RBAC și lacunele de securitate ale rețelei.
3. A implementat protocoalele securizate de gestionare a sesiunii, asigurând o autentificare fără întreruperi și persistentă, prevenind în același timp deturnarea sesiunii și accesul neautorizat.

F. Reducerea decalajului dintre securitate, utilizare și experiența utilizatorului în realitate virtuală

1. A dezvoltat un model de securitate centrat pe utilizator care echilibrează gradul de utilizare, UX, securitate și confidențialitate, asigurându-se că măsurile de securitate nu perturbă imersiunea.
2. A efectuat studii empirice UX pentru a evalua modul în care mecanismele de securitate pot fi integrate perfect în aplicațiile imersive.

4. Diseminarea rezultatelor

În demersul său, candidata a reușit să publice și să comunice 12 articole cu impact internațional, după cum urmează: 7 - articole in jurnale/conferinte ISI (din care 4 ca prim autor) si 5 in diverse conferințe internaționale BDI sau in curs de indexare.

5. Concluzii

Teza intitulată „Addressing Cybersecurity Concerns in Virtual Reality", deschide calea pentru studii viitoare privind cadrele de securitate pentru a aborda provocările în evoluție de securitate și confidențialitate în realitate virtuală. Pe parcursul acestei teze, au fost efectuate simulări de amenințări pentru a identifica și analiza vulnerabilitățile sistemelor de RV. În plus, cercetarea explorează echilibrul dintre securitate și experiența utilizatorului, asigurând integrarea perfectă a măsurilor de securitate fără a compromite utilizabilitatea sistemelor.

Întrucât con inutul acestei teze de doctorat corespunde exigen elor din domeniul de doctorat CALCULATOARE ȘI TEHNOLOGIA INFORMAȚIEI, ce respectă standardele de etică profesională, potrivit prevederilor legale în vigoare și în totală concordanță cu contractul de studii doctorale (96/01.10.2021) art. 4, par 3.1, (lit. d[1]), sunt de acord cu susținerea publică a tezei.

[1] [Obligatie] De a publica in reviste de specialitate (ISI/BDI) si proceedings de conferinte internationale lucrari in domeniul tezei de doctorat, numarul minim de publicatii, pe domenii de doctorat, fiind stabillit in baza OMEN nr 5110/2018 privind aprobarea standardelor nationale minimale pentru acordarea titlului de doctor.

Data,

17.07.2025

Conducător de doctorat,

Prof.univ.dr. POPOVICI DORIN-MIRCEA