MINISTERUL EDUCAȚIEI ȘI CERCETĂRII

UNIVERSITATEA TEHNICĂ
DIN CLUJ-NAPOCA

Domeniul fundamental: Inginerie
Domeniul de specialitate: Calculatoare și tehnologia informației

# TEZĂ DE ABILITARE

## – REZUMAT –

# Ingineria securității cibernetice în era Inteligenței Artificiale

**Conf. Dr. Ing. Ciprian-Pavel OPRIȘA**
**Facultatea de Automatică și Calculatoare**
**Universitatea Tehnică din Cluj-Napoca**

**– Cluj-Napoca –**
**2025**

str. Memorandumului nr. 28, 400114 Cluj-Napoca, România
tel. +40-264-401200, fax +40-264-592055, secretariat tel. +40-264-202209, fax +40-264-202280
www.utcluj.ro

Securitatea cibernetică și inteligența artificială sunt două dintre cele mai importante domenii de cercetare din prezent, ambele având implicații profunde în societate. În timp ce securitatea cibernetică necesită rezultate exacte și determinism, inteligența artificială aduce raționamente probabilistice, aproximări și elemente de aleatoriu. Cu toate acestea, problemele moderne din securitatea cibernetică au nevoie de instrumente moderne, iar inteligența artificială este o componentă importantă a acestor instrumente.

Această teză de abilitare prezintă principalele mele realizări științifice, profesionale și academice după obținerea titlului de doctor (în 2016) și până în prezent. Cariera mea s-a desfășurat pe două planuri, atât în mediul academic la Universitatea Tehnică din Cluj-Napoca, cât și în industrie, la compania Bitdefender. Această perspectivă bilaterală m-a ajutat să dobândesc abilități utile atât în cercetarea academică, cât și în cercetarea și dezvoltarea de soluții industriale.

Cercetarea mea, atât înainte, cât și după susținerea tezei de doctorat, a fost centrată pe securitatea cibernetică, dezvoltând instrumente și soluții bazate pe inteligența artificială, care asigură securitatea cibernetică sau facilitează activitatea de analiză a securității.

Primul subdomeniu în care mi-am adus contribuția este analiza și clasificarea programelor malițioase, o continuare a cercetării pe care am efectuat-o în timpul doctoratului. Mai multe articole la care am contribuit descriu soluții eficiente pentru indexarea colecțiilor masive de fișiere, pentru regăsirea eficientă a programelor înrudite sau similare. Am evidențiat de asemenea importanța înțelegerii profunde a amenințărilor detectate, propunând soluții de asociere automată a atacurilor cu tehnici MITRE și soluții de reducere a numărului de detecții Fals Pozitive. Detecția de malware se poate face și pe date criptate homomorfic, unde entropia Shannon, o trăsătură importantă pentru detecția codului compactat poate fi calculată în mod eficient. Malware-ul este prezent pe mai multe platforme, inclusiv pe dispozitive din Internetul Lucrurilor (IoT). Un articol recent prezintă o modalitate de reprezentare semantică a codului binar, agnostică față de tipul de procesor pentru care a fost compilat.

Al doilea subiect de cercetare abordat se referă la securitatea rețelelor și a dispozitivelor IoT, a căror securitate trebuie asigurată la nivel de rețea. A fost propus un cadru (framework) de detonare a programelor suspecte, cu accent pe simularea și monitorizarea activității la nivel de rețea. Atacurile studiate au fost prezentate într-un alt articol, unde a fost realizată o taxonomie a atacurilor web împotriva dispozitivelor IoT. Am propus mai multe metode de protecție împotriva acestor atacuri prin detectarea anomaliilor. O provocare majoră a detecției de anomalii este reducerea alarmelor fals pozitive, obiectiv realizat prin analiza minuțioasă a URL-urilor detectate ca anomalii. Pentru a facilita această analiză am propus un algoritm de clustering optimizat pentru procesarea colecțiilor mari de URL-uri detectate prin anomalii. Am propus și o soluție pentru detecția domeniilor generate algoritmic (DGA), prin care malware-ul își ascunde serverul de comandă și control. Metoda de detecție, bazată pe învățarea automată, folosește un clasificator capabil să ruleze chiar și pe routere cu putere de calcul redusă.

Al treilea subdomeniu vizează detecția fraudelor prin analiza semantică a textului. Cercetarea mea în acest domeniu a avut ca scop identificarea unui echilibru între metodele moderne, mai precise, dar în același timp mai lente și metodele clasice, mai rapide, dar uneori mai puțin precise. Un pas important în detecția știrilor false este identificarea sursei inițiale, pentru care

este necesară o metrică de similaritate între două articole de știri. Am propus două soluții, una textuală, bazată pe n-grame extrase din text, iar una semantică, bazată pe modelul BERT. Deși a doua soluție este mai precisă, cea textuală obține rezultate rezonabile într-un timp semnificativ mai mic. Un alt rezultat în domeniul analizei articolelor de știri propune o soluție pentru detecția titlurilor înșelătoare (clickbait), analizând atât elemente din titlu precum și potrivirea dintre acesta și conținutul articolului. Analiza textului este utilă și pentru detecția e-mail-urilor de tip phishing. Modelele lingvistice mari (LLM) pot analiza textul unui mesaj și pot răspunde la întrebări privind autoritatea, urgența, familiaritatea, reciprocitatea sau consistența unui text.

Ultimul subdomeniu abordat este securitatea ofensivă. De multe ori, pentru analiza securității unui sistem informatic este necesar să gândim ca un atacator, chiar dacă scopul final este unul defensiv. Într-unul dintre articolele publicate am propus o metodă bazată pe învățarea automată, pentru automatizarea procesului de pentesting prin selectarea celui mai potrivit exploit. Un alt articol publicat oferă o soluție ofensivă pentru echipele roșii, sub forma unei infrastructuri complete pentru un malware specializat pentru containere orchestrate prin tehnologia Kubernetes.

După obținerea titlului de doctor, am publicat:

- o carte, un suport de curs și două îndrumătoare de laborator;
- două articole în jurnale, ambele indexate în WoS în zonele Q1/Q2;
- 18 articole în cadrul unor conferințe internaționale, dintre care 12 indexate în WoS și 6 indexate în baze de date internaționale.

Am participat și la șase proiecte de cercetare, fiind responsabil partener la trei dintre acestea.

Cariera mea profesională a început în iunie 2010, când am fost angajat ca Malware Researcher la compania Bitdefender. În prezent ocup rolul de Principal Security Researcher Lead în cadrul laboratorului Cyber Threats Intelligence din aceeași companie. În februarie 2017, după obținerea titlului de doctor, m-am angajat ca Șef Lucrări la Universitatea Tehnică din Cluj-Napoca, unde în prezent sunt Conferențiar, în cadrul Departamentului Calculatoare. Am desfășurat activități didactice la Universitatea Tehnică din Cluj-Napoca, în regim de plată cu ora, încă din octombrie 2011.

De-a lungul timpului am predat cursuri, seminarii și laboratoare la șase discipline de la licență și patru materii de la master. În prezent predau „Sisteme de Operare”, „Algoritmi Fundamentali” și „Administrarea Sistemelor de Operare” la nivel de licență, „Mobile Security” și „Big Data and Machine Learning for Cybersecurity” la masterul „Cybersecurity Engineering”, respectiv „Introduction to Big Data” și „Algorithms” în cadrul programului de master „Data Science”. La fiecare materie predată mi-am adus contribuția fie prin realizarea de noi materiale de curs sau laborator, fie prin îmbunătățirea celor existente.

Pe lângă activitățile de predare mai coordonez studenți pentru realizarea lucrărilor de licență și a disertațiilor, având peste 100 de lucrări finalizate cu succes. Sunt implicat și în organizarea concursului ACM ICPC, sunt membru în comisia de evaluare a lucrărilor de licență și secretar de comisie la finalizarea studiilor de masterat.

Ca planuri de dezvoltare academică, îmi propun să îmi adaptez metodele de evaluare la prezența inteligenței artificiale generative, să îmi actualizez permanent cursurile predate cu

materiale moderne și relevante, să formez competențe transversale prin colaborarea cu colegii care predau concepte înrudite și să scriu cărți acolo unde cursurile pe care le predau nu se bazează deja pe cărți consacrate. De asemenea, doresc să mă implic în continuare în organizarea concursului ACM ICPC și să cresc interesul studenților pentru acesta.

Din punct de vedere științific, îmi propun să extind grupul de cercetare CYDAR, din care fac parte, coordonând doctoranzi în domeniul securității cibernetice și participând la proiecte de cercetare. Îmi voi extinde domeniile de cercetare către inteligența artificială agentică și asupra sinergiei dintre modelele mari și mici de inteligență artificială, pe care le consider importante atât din punct de vedere al cercetării fundamentale cât și din punct de vedere industrial. Îmi propun de asemenea să utilizez reprezentarea semantică a datelor (embedding-uri) pentru a îmbunătăți soluțiile de detecție a plagiatului.

Prin urmărirea obiectivele propuse, consider că voi putea aduce contribuții importante în cercetare, oferind noi instrumente și soluții inovatoare pentru securitatea cibernetică și pregătind o nouă generație de cercetători, alături de care voi explora problemele de securitate din viitor. Din punct de vedere educațional, voi face trecerea la noua paradigmă, în care inteligența artificială este parte a contextului, valorificând avantajele și atenuând dezavantajele aduse de aceasta, pentru a menține un standard ridicat de calitate.