

RASOUL REZVANIJALAL

Email: rasoulrezvanijal@gmail.com

LinkedIn: <https://www.linkedin.com/in/rasoul-rezvani-80725721a/>

Github: <https://github.com/Rasoul-RezvaniJalal>

Phone: 0098-9055452916

EDUCATION

- MSc** Iran University of Science and Technology, Computer Engineering, Sep 2021 – Sep 2024
Software Engineering, Tehran, Iran
Grade: 18.11 / 20
- Master's Thesis**, Iran University of Science and Technology, Tehran, Iran April 2023 – Sep 2024
Supervisor: Dr. Saeed Parsa
Title: "Predicting the importance and type of damage in non-executable malicious complex files"
- BS** Bu-Ali Sina University, Computer Engineering, Software Engineering Sep 2014 – July 2019
Hamedan, Iran
Grade: 13.40 / 20

RESEARCH EXPERIENCE

Under review

Paper

June 2023 – April 2024

Rezvani-Jalal, Rasoul and Zakeri-Nasrabadi, Morteza and parsa, saeed and Hasan-Zarei, Amin, Enhancing Malware Detection Reliability in Non-Executable Files Using Confidence Score Prediction. Journal of Information security and applications. Available at SSRN: <https://ssrn.com/abstract=4823193>.

Under preparation

Paper

Dec 2024 – Present

Rezvani-Jalal, Rasoul and Zakeri-Nasrabadi, Morteza and Parsa, Saeed, Detecting the behavior of non-executable complex malwares using clustering technique.

Article

Rezvani-Jalal, Rasoul, Understanding the Architecture of an Antivirus System. Medium. Available at <https://medium.com/@rasoulrezvanijal/understanding-the-architecture-of-an-antivirus-system-7dd0cc6060e1>

TEACHING EXPERIENCE

Teaching Assistant

Oct 2022 - Jan 2023

Computer Engineering Department, Iran University of Science and Technology, Tehran, Iran

Professor: Dr. Saeed Parsa

- Compiler Design

Teaching Assistant

Oct 2023 – February 2024

Computer Engineering Department, Iran University of Science and Technology, Tehran, Iran

Professor: Dr. Hossein Rahmani

- Data Mining

Teaching Assistant

April 2024 – July 2024

Computer Engineering Department, Iran University of Science and Technology, Tehran, Iran

Professor: Dr. Ahmad Akbari-Azirani

- Advanced network security

PROFESSIONAL AFFILIATIONS

Full-time

Graph Company, Tehran, Iran

December 2023 – Now

Threat Analyst, EDR Project

- Analyze malicious files
- Create signature for malwares with YARA
- Implement famous process injection attacks like thread execution hijacking as test cases
- Cyber threat intelligence
- System calls monitoring in Linux OS with eBPF
- Signature validation
- Develop Intelligent malware detection mechanism

Full-time

Amnpardaz Software Co, Tehran, Iran

April 2019 - Mar 2020

Malware Analyst, Padvish Project

- Analyze malicious file
- Create signature based for them
- Develop cleaner for each type of malwares
- Configure Virtual-Box in order to detect malicious behaviors

Full-time

Amel System, Hamedan, Iran

April 2018 - Mar 2019

Noc Specialist

- Data Center Maintenance
- Network Monitoring
- Attending in BMS Course

Internship

Tolu Ideh Amn, Hamedan, Iran

Jun 2018 – Feb 2019

Cybersecurity

- Learning about malwares
- Learning about Data Center

PROJECTS

- Implementing a Python program using ANTLR to extract Control Flow Graph (CFG) of C++ programs which is important for many aspects of cybersecurity such as program analysis and code obfuscation.
- Implementing a Java program for encrypted communication between two side using socket-programming and also RAFT algorithm, all related to distributed systems.

- Implementing various Python programs to preprocess dataset, learn, postprocess and illustrate different diagrams for multiple contexts like Network Intrusion Detection, all related to data science.
- Implementing Python program using Selenium to crawl across different parts of a financial webpage in order to gather various data and report it as a csv file for further predictions.
- PfSense configuration and set all systems DNS on PfSense in order to monitor network traffic and also setting Suricata rules on PfSense machine to detect network intrusions.
- Implementing Python program to detect XSS vulnerability detection in a webpage.
- Implementing Python program using set-trace library to perform statistical fault localization which is a well-known technique in software testing.
- Conducting various cryptographic-related activities using relevant tools such as CrypTool and OpenSSL.
- Designing test sets for PID controllers using Python scripts and employing reinforcement technique to evaluate the performance of the controllers.
- Working with ROS v2 in CARLA simulator project. In included gathering information between client and server, and analyze it in ROS framework.

RESEARCH INTERESTS

- Malware Detection
- Malware Analysis
- Computer Security
- Machine Learning
- Cybersecurity for AI
- AI for Cybersecurity
- Program Analysis
- System Programming
- Software Testing
- Fuzzing
- Cyber Threat Intelligence
- Detecting Adversarial Attacks
- Trojan Neural Network

HONORS AND AWARDS

- | | |
|--|---------------------|
| • Ranked 4 th among 25 master's students | <i>June 2023</i> |
| • Participation in the Elite Foundation plan | Jan 2023 - Sep 2023 |
| • Ranked 3 rd in Mobile application competition marathon held in Bu-Ali Sina University | Sep 2017 |
| • Ranked 2 nd in Handball competitions for students of the west of the country | Dec 2016 |
| • Ranked 4 th in National table tennis tournaments | July 2009 |

LANGUAGES

English: IELTS overall band score 7 (C1). Listening: 8, Speaking: 7, Writing: 6.5, Reading: 6.5.

Persian: Native Language

COMPUTER SKILLS

Programming Languages	Malware Analysis Tools	UI/UX Design Technologies
VBA C++ Python Powershell Bash scripting	OllyDbg IDA Pro Process Monitor Process Explorer API Monitor Cuckoo Sandbox VMWare Workstation WireShark eBPF Yara	HTML JavaScript
General Technologies	Python Libraries	Other Tools
PID Controller Reinforcement learning Fixed-size-candidate-set ART Metamorphic Testing	TensorFlow Scikit-learn Keras Pandas Numpy Matplotlib Selenium Yara-python VirusTotal-python	Pycharm GitHub Jupyter Notebook Linux Visual Studio ANTLR

HOBBIES

- Going to the gym
- Listening to Music
- Playing Ping-Pong
- Playing Handball

REFERENCES

Dr. Saeed Parsa (Associate professor)

Faculty member
Computer Engineering Department
Iran University of Science and Technology
Tehran, Iran
Email: parsa@iust.ac.ir

Dr. Morteza Zakeri (Assistant professor)

Faculty member
Computer Engineering Department
Amirkabir University of Technology
Tehran, Iran
Email: zakeri@aut.ac.ir

Dr. Ahmad Akbari-Azirani (Associate professor)

Faculty member

Computer Engineering Department

Iran University of Science and Technology

Tehran, Iran

Email: akbari@iust.ac.ir