europass

Răzvan-Constantin Stoleriu

Date of birth:

Nationality: Romanian

Gender: Male

CONTACT

Iasi, Romania **(Work)**

ABOUT ME

Main objectives: - Participation in various projects in which to come up with ideas that make a significant contribution - Discovering optimal and efficient solutions - Improving knowledge in the cybersecurity and software development fields

WORK EXPERIENCE

01/09/2022 – CURRENT Iasi, Romania

Threat Analyst CrowdStrike

1. Malware analysis
2. Threat detection
3. Incident handling

01/12/2021 – 01/09/2022 Piatra-Neamț, Romania

IT Specialist Public Ministry

1. Informatic systems administration
2. Database administration

01/08/2019 – 01/12/2021 Bucharest, Romania

Cyber Security Analyst Cyberint National Center

- Security operations
- Threat hunting
- Intrusion detection
- Incident analysis
- Incident handling and log analysis
- Network/Endpoint anomalies detection
- Reviewing raw log files, data correlation, and analysis
- Creating mechanisms for detecting security incidents (e.g. rules, dashboards)

13.04-16.04 2021: Participation in the international cyber defense exercise LOCKED SHIELDS 2021
30.09-02.10 2019: Participation in CyDEx19

EDUCATION AND TRAINING

01/10/2021 – CURRENT Bucharest, Romania

Ph.D. student University Politehnica of Bucharest

Field of study Computers and Information Technology (CIT) | **Thesis** Advanced Cyber Security Attacks Management in Future Generation Computer Systems

01/10/2019 – 03/03/2021 Bucharest, Romania

Master's degree - specialization in Security of Information Technology "Ferdinand I" Military Technical Academy

24.11.2020: **Participation in the Threat Hunting Workshop organized by CISCO Romania**
11-12.10.2019: **Participation in the "Military Culture and War Experience" conference in Sofia, Bulgaria**

Final grade 10 | **Thesis** Thesis - Adaptive Solution for Cyberattacks Detection

01/10/2015 – 31/07/2019 Bucharest, Romania

Bachelor's degree - specialization in Computers and informatic systems for defense and national security "Ferdinand I" Military Technical Academy

2018-2019: **Special prize at the "CERC" International Student Conference, organized by the "Ferdinand I" Military Technical Academy**
2018-2019: **Creating a cross-platform application (iOS & Android), written in Flutter for Euro Atlantic Diplomacy Society**
2018-2019: **First Prize at the NATO Mobile App Hackathon, organized by TOTALSOFT and Euro Atlantic Diplomacy Society**
2017-2018: **Development of an Android recruitment application for the Ministry of National Defense**
2017-2018: **Participation in the International Conference of Students "CERC" organized by "Mircea cel Batran" Naval Forces Academy from Constanța**
2017-2018: **Participation in the International Conference of "CERC" Students organized by "Henri Coandă" Air Force Academy in Brașov**
2017-2018: **Qualification and participation in the "HackITAll hackathon" organized by Avira**
2016-2017: **Participation in "Data Assimilation Summer School 2017", Sibiu**
2016-2017: **Second Prize at the "CERC" International Student Conference organized by "Ferdinand I" Military Technical Academy**
2016-2017: **Erasmus grant for one semester at the Ecole Spéciale Militaire de Saint-Cyr academy in France**
2015-2016: **Participation in the National Mathematics Student Competition "TRAIAN LALESCU"**

Final grade 8.65 | **Thesis** Thesis - Android Security Application Based on Facial Recognition

15/09/2011 – 30/06/2015 Botoșani, Romania

Graduation diploma - specialization Mathematics-Computer Science, intensive English A.T.Laurian National College

LANGUAGE SKILLS

MOTHER TONGUE(S): Romanian

Other language(s):

English

Listening	Reading	Spoken production	Spoken interaction	Writing
B2	B2	B2	B2	B2

French

Listening	Reading	Spoken production	Spoken interaction	Writing
B1	B1	B1	B1	B1

Levels: A1 and A2: Basic user; B1 and B2: Independent user; C1 and C2: Proficient user

DIGITAL SKILLS

Security Operations | Threat Hunting | Intrusion Detection | Incident Handling and Log Analysis | Network/ Endpoint Anomalies Detection | Cyber Defence Content | Malware Analysis | Web Applications | Desktop Application Development | Android Studio | Object Oriented Design | Spring Framework | SQL | Android SDK | Networking | Flutter | ArcSight | SIEM | Java | Scripting | ELK Stack (Elasticsearch, Logstash, Kibana)

ADDITIONAL INFORMATION

Publications

Malicious Short URLs Detection Technique 2023

The paper has been accepted at ***2023 RoEduNet Conference: Networking in Education and Research***, and it will be submitted to ISI Web of Science, THOMSON REUTERS SCOPUS, GOOGLE SCHOLAR, etc.
The other co-authors are Bogdan-Costel Mocanu, Cătălin Negru and Florin Pop.

Modern Cyber Security Attacks, Detection Strategies, and Countermeasures Procedures 2023

R. Stoleriu, C. Negru and D. Rădulescu, "Modern Cyber Security Attacks, Detection Strategies, and Countermeasures Procedures," 2023 24th International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 2023, pp. 198-205, doi: 10.1109/CSCS59211.2023.00039.

Cyber Attacks Detection Using Open Source ELK Stack 2021

R. Stoleriu, A. Puncioiu and I. Bica, "Cyber Attacks Detection Using Open Source ELK Stack," 2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2021, pp. 1-6, doi: 10.1109/ECAI52376.2021.9515120.

A Secure Screen and App Lock System for Android Smart Phones Using Face Recognition 2020

R. Stoleriu and M. Togan, "A Secure Screen and App Lock System for Android Smart Phones Using Face Recognition," 2020 13th International Conference on Communications (COMM), Bucharest, Romania, 2020, pp. 133-138, doi: 10.1109/COMM48946.2020.9142008.

Driving Licence

Driving Licence: B

Projects

15/02/2020 – 30/10/2020

Adaptive Solution for Cyberattacks Detection Based on the model presented by Mandiant, I performed a series of APT-specific attacks, which were detected using the Elasticsearch stack. Each step in this model (e.g. Initial Compromise, Establish Foothold, Escalate Privileges) was performed using techniques from the MITRE ATT&CK matrix (e.g. Spearphishing Link, Scheduled Task, Domain Accounts). To determine if the files involved in security incidents contain malware, Elasticsearch has been integrated with VirusTotal. Moreover, data from network logs have been enriched with geolocation information via the GeoIP processor in Logstash. One fact that I consider to be of particular importance is the integration of the ELK stack with MISP. This allows us to perform real-time searches for certain compromise indicators reported by OSINT organizations as belonging to malware campaigns. Last but not least, I used Machine Learning algorithms from Elasticsearch to identify anomalies both in network traffic (data leakage through DNS and HTTP, respectively) and at workstations (suspicious login activities, running in the system of randomly named processes).

Technologies used: ELK stack, ELK Beats, Machine Learning, Sysmon, auditd, MISP, VirusTotal, MITRE ATT&CK, Cyber Kill Chain

This project was my master's degree thesis and based on it, I wrote a scientific article that I published at ECAI 2021 conference (see the reference in the *Publications* section)

01/04/2018 – 30/06/2019

Android Security Application Based on Facial Recognition - AppLock The main objective of this project is the implementation of a security application based on facial recognition intended for owners of mobile devices with the Android operating system. Its most important tasks are both restricting access to user-selected applications on the phone and blocking the screen. Restriction methods use facial recognition, PIN, or pattern. In addition to the methods listed above, when locking the screen the user also has available the drag-and-drop and unlock buttons. Moreover, an administrator can have via a web platform, an overview of all applications to which the access was restricted. In addition to the passive part that consists of just viewing the locked/unlocked applications, the administrator also can block or unlock other applications he or she wants. It should be noted that the change will occur in users' phones after a few minutes. The application can have as scope the corporate environment. Employees receive business phones in which access to some applications is restricted (Facebook, Instagram, etc.), and their manager wants to know if they use those applications. Thus, the application provides the administrator with the situation from the employees' phones, and he or she can block or unlock other applications in addition.

Technologies used: Android Studio, Java Spring, XAMPP, IntelliJ IDEA, MySQL Workbench, Volley library, OpenCV

This project was my bachelor's degree thesis and based on it, I wrote a scientific article that I published at COMM 2020 conference (see the reference in the *Publications* section)

01/07/2018 – 01/09/2018

Android Recruiting Application I have developed an Android application to facilitate the process of recruiting new candidates for the educational institutions of the Ministry of National Defense. In addition to the mobile application component, the project also includes a web application for staff employed by the Ministry of National Defense, which is responsible for recruiting candidates.

Technologies used: Android Studio, Volley library, Java-Spring