SIMA BAGHERI

Email: sima.bagheri@concordia.ca Website LinkedIn Google Scholar

EDUCATION

Master of Applied Science in Information Systems Security — *Fall 2020-Dec 2023*
Concordia University, Montreal, Canada — ***GPA:*** *3.53/4*

Master of Science in Information Technology Engineering-Enterprise Architecture — *2017-2019*
Shahid Beheshti University, Tehran, Iran — ***GPA:*** *17.83/20*

Bachelor of Science in Computer Engineering-Software — *2013-2017*
Shahid Beheshti University, Tehran, Iran — ***GPA:*** *17.56/20*

RESEARCH EXPERIENCE

Research Assistant, ARC lab, Concordia University — *Sep 2020-Dec 2023*

- Proactive Security Policy Compliance and Enforcement in Cloud
- Proactive and Non-disruptive Attack Mitigation in Cloud

Research Assistant, CloudSec lab, Shahid Beheshti University — *Dec 2016-Sep 2019*

- Dynamic Firewall Decomposition and Composition in the Cloud
- Software Project Cost/Effort Estimation using Improved Use Case Point: A Risk-based Approach

TEACHING EXPERIENCE

Teaching Assistant, Concordia University

- SOEN 321 (Information Systems Security): Tutor, Programmer on Duty (POD) — Winter 2022
- INSE 6130 (Operating System Security): Marker — Fall 2022

Teaching Assistant, Shahid Beheshti University

- Software Engineering I/II: Head TA (assignments, and project designer) — Fall 2017, Winter 2018
- Computer Networks: Head TA (assignments, and mini projects designer) — Winter 2018

INDUSTRIAL EXPERIENCE

Research Assistant, Ericsson/NSERC Industrial Research Chair — *2020-2023*

Project: Design and Implementation of AI-aided Security Solution for Cloud (Kubernetes)

- Research progress delivery to Ericsson representative
- Presenting at quarterly steering meetings with Ericsson Security team at Montreal and Sweden

Software Engineering Intern, Jooya Informatics group (JIG)[1] — *March-Sep 2016*

Project: Design and Implementation of a Web-based Android Application for JIG Internal Warehouse

- Requirement analysis and use case design
- Conducting user research and interviews with end users
- Design and implementation of web-based inventory application

[1] http://jooya.com

- Integration with Personal Device Assistant (PDA) scanner API

RESEARCH PUBLICATIONS

1. **ACE-WARP: A Cost-Effective Approach to Proactive and Non-disruptive Attack Mitigation in Kubernetes Clusters** *Aug 2023*
   Sima Bagheri, Hugo Kermabon-Bobinnec, Mohammad Ekramul Kabir,
   Suryadipta Majumdar, Yosr Jarraya, Lingyu Wang, Makan Pourzandi **[Under Review]**
   Journal of IEEE Transactions on Information Forensics & Security (TIFS)

2. **PerfSPEC: Performance Profiling-based Proactive Security Policy Enforcement for Containers** *Feb 2023*
   Hugo Kermabon-Bobinnec, Sima Bagheri, Suryadipta Majumdar, Yosr Jarraya,
   Lingyu Wang, Makan Pourzandi **[Under Review]**
   Journal of IEEE Transactions on Dependable and Secure Computing (TDSC)

3. **Warping the Defence Timeline: Non-disruptive Proactive Attack Mitigation for Kubernetes Clusters** *2023*
   Sima Bagheri, Hugo Kermabon-Bobinnec, Suryadipta Majumdar, Yosr Jarraya,
   Lingyu Wang, Makan Pourzandi
   IEEE International Conference on Communications (ICC 2023)

4. **ProSPEC: Proactive Security Policy Enforcement for Containers** *2022*
   Hugo Kermabon-Bobinnec, Mahmood Gholipourchoubeh, Sima Bagheri,
   Suryadipta Majumdar, Yosr Jarraya, Makan Pourzandi, Lingyu Wang
   ACM Conference on Data and Application Security and Privacy (CODASPY 2022)

5. **Dynamic Firewall Decomposition and Composition in the Cloud** *2020*
   Sima Bagheri, Alireza Shameli-Sendi
   Journal of IEEE Transactions on Information Forensics & Security (TIFS)

6. **Software Project Estimation using Improved Use Case Point** *2018*
   Sima Bagheri, Alireza Shameli-Sendi
   IEEE/ACIS International Conference on Software Engineering Research, Management and Applications (SERA 2018)

SKILLS

Programming: Proficient in Python, Keras, Numpy, linear programming, SQL, Learning R
Security: Attack simulation, Traffic analysis, *iptables* Firewall
Cloud Computing Platform: Docker, Kubernetes, OpenStack
Cloud Computing Service Model: Oracle Cloud Infrastructure Foundations, Google Cloud
Research Methodologies: Quantitative methodologies, interviews and survey design, user research

NOTABLE PROJECTS

1- Advanced Persistent Threats (APT) Attacks Simulation
Eight APT attacks and CVEs are investigated through their documentations, attack steps are derived in the form of MITRE ATT&CK tactics, and simulated using the autonomous adversary emulation tool, Caldera v4.0. in a Kubernetes protected environment.

2- Building First Dataset of Falco Alerts Dataset
Simulating eight APT attacks and CVEs during the normal operation of the cluster, and collecting the associated Falco alerts. Data normalization and scaling resulting in the first labeled dataset of Falco alerts (231K alerts) consisting attack alerts as 1% of the total.

3- Attacker Tactic Prediction
Building a Bayesian network, and a LSTM predictive model upon our dataset for predicting the attacker's next move using pgmpy v0.1.14, and keras v2.4.3.

4- Optimal Kubernetes Node Selection for Pods Live Migration
Modeling a multi-objective optimization problem for optimal Pods migration in Kubernetes cluster, and proving its NP-hardness. Implementing a dynamic-programming based heuristic algorithm to efficiently achieve a high level of cluster threat reduction with minimal imposed delay to 5G services running in the cluster. Results compared with genetic algorithm, implemented using geneticalgorithm2 6.8.5 library.

5- Dynamic Firewall Composition and Decomposition in the Cloud
Implementing a heuristic algorithm for automatic scaling of iptable firewall rules at network edge and solving the NP-Complete Firewall rule ordering problem. Using *Wireshark*,*GNS3*, and *Qemo*.

6- Empirical Risk Assessment in Software Projects Cost/Effort Estimation
Designing a risk based Use Case Points method (RUCP) for cost/effort estimation in software projects. Deriving software risks parameters using evaluation of 60 industrial projects. Transforming the conventional environmental and technical factors with software risks. Case study: Interviewing and data analysis of Five Iranian software companies.

ENGLISH LANGUAGE PROFICIENCY

TOEFL iBT: 112/120
Reading 29/30, Listening 29/30, Speaking 27/30, Writing 27/30, **Test Date:** 16 November 2019

French: A2 level

SERVICE

- **External Reviewer:** Computers & Security Journal, ESORICS'21, WWW (security, privacy, and trust track)'23
- **Technical Program Committee:** International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP'24)
- **Conference and Workshop Organizer:** Iranian Conference on Advances in Enterprise Architecture (ICAEA'18), Workshop on Enterprise Architecture Development in South Korea (ICAEA'18)

HONORS AND AWARDS

- Concordia university travel award *2023*
- Concordia university graduate student association (GSA) conference funding *2023*
- Concordia university tuition award of excellence *2020*
- Ranked **1** among M.Sc. program students, SBU, Tehran, Iran *2019*
- Admitted as exceptional talent to M.Sc. program (exempted from national M.Sc. entrance exam- Concour), SBU, Tehran, Iran *2017*
- Best B.Sc. Student with research paper[2], CloudSec Lab, SBU, Tehran, Iran *2017*

[2]https://cloudsec.sbu.ac.ir/researchteam/