Contact Information

03.03, Mercator 1, Toernooiveld 212, 6525 EC Nijmegen, The Netherlands.

Phone: +31 24 36
Cell No: +31 625440813
Email: hamid.bostani@ru.nl

Research Interests

- **Adversarial Machine Learning**
- **Machine Learning**
- **Deep Learning**
- **Malware Detection**
- **Intrusion Detection Systems**
- **Internet of Things**

Education

Radboud University, Nijmegen, The Netherlands. Oct. 2020-Present
Ph.D. Candidate in the Digital Security group, Institute for Computing and Information Sciences.
Ph.d. Research: **Improving the Adversarial Robustness of Machine Learning-based Malware Detection against Real-World Threat Models** (Supervisors: Dr. Veelasha Moonsamy and Prof. Erik Poll)

Islamic Azad University (IAU), South Tehran Branch, Tehran, Iran. 2012-2015
M. Sc. in Computer Engineering (Software Engineering), GPA: 17.55/20.
Thesis: **Intrusion Detection and Identification of Attacks on the Internet of Things (IoT) Using a Combination of Machine Learning Methods** (Supervisor: Prof. Mansour Sheikhan)
Master Seminar: **Using Collaborative Filtering in Recommender Systems** (Advisor: Prof. Ali Moeini)

Islamic Azad University (IAU), Shiraz Branch, Shiraz, Iran. 2004-2008
B. Sc. in Computer Engineering (Software Engineering), GPA: 16.73/20, Major GPA: 18.53/20.
Project: "**Developing E-Commerce Systems (a Case Study in a Mobile Phone Store)**" (Supervisor: Dr. Mostafa Fakhrahmad)

Honors and Awards

- **Fully-Funded Fellowship** (Radboud University, Oct. 2020).
- **Best Employee Award** (NOET, Nov. 2019).
- **Certificate of Appreciation (**NOET, Feb. 2018).
- **Research Funding** (Iran National Science Foundation, Feb. 2018).
- **Outstanding Researcher Award** (IAU, South Tehran Branch, Dec. 2017).
- **Best Thesis Award** (the 5th Research, Scientific & Technological National Festival of IAU, May 2017).
- **Certificate of Appreciation** (IAU, South Tehran Branch, May 2017).
- **Outstanding Paper Award** (ICSPIS'2016).
- **Selected Paper** (IST'2016).

Publications

Bibliographic indicators (Google Scholar January 2024) Citations: 517, h-index: 6.

Pre-print:

1. **H. Bostani**, Z. Zhao, Z. Liu, and V. Moonsamy. "Level Up with RealAEs: Leveraging Domain Constraints in Feature Space to Strengthen Robustness of Android Malware Detection," arXiv preprint arXiv:2205.15128 (2022).

Journals:

2. **H. Bostani** and V. Moonsamy, "EvadeDroid: A practical evasion attack on machine learning for black-box android malware detection," Computers & Security, In Press, Journal Pre-proof (2023). DOI: 10.1016/j.cose.2023.103676, Impact Factor (2023) = 5.6 (Q1)

3. **H. Bostani**, M. Sheikhan, B. Mahboobi, "A Strong Coreset Algorithm to Accelerate OPF as a Graph-based Machine Learning in Large-Scale Problems," *Information Sciences*, vol. 555 (2021), pp. 424-441. DOI: 10.1016/j.ins.2020.10.009, Impact Factor (2020) = 5.91 (Q1)

4. **H. Bostani**, M. Sheikhan, “Hybrid of Anomaly-Based and Specification-Based IDS for Internet of Things Using Unsupervised OPF based on Map-Reduce Approach,” *Computer Communications*, Elsevier, vol. 98 (2017), pp. 52-71. DOI: 10.1016/j.comcom.2016.12.001, Impact Factor (2016) = 3.338 (Q1)

5. **H. Bostani**, M. Sheikhan, “Modifying Supervised Optimum-Path Forest in Intrusion Detection Systems Using Social Network Approaches and Unsupervised Learning,” *Pattern Recognition*, Elsevier, vol. 62 (2017), pp. 56-72.DOI: 10.1016/j.patcog.2016.08.027, Impact Factor (2016) = 4.582 (Q1)

6. **H. Bostani**, M. Sheikhan, “Hybrid of Binary Gravitational Search Algorithm and Mutual Information for Feature Selection in Intrusion Detection Systems,” *Soft Computing*, Springer, vol. 21 (2017), no. 9, pp. 2307-2324.DOI: 10.1007/s00500-015-1942-8, Impact Factor (2016) = 2.472 (Q2)

7. M. Sheikhan, **H. Bostani**, “A Security Mechanism for Detecting Intrusions in Internet of Things Using Selected Features Based on MI-BGSA,” *International Journal of Information & Communication Technology Research*, Iran Telecommunication Research Center (ITRC), vol. 9 (2017), no. 2, pp. 53-62. http://journal.itrc.ac.ir/article-1-42-en.html

Book Chapter:

8. M. Sheikhan and **H. Bostani**, “Hybrid and modified OPFs for intrusion detection systems and large-scale problems,” in Optimum-Path Forest (pp. 109-136). Academic Press, 2022. https://doi.org/10.1016/B978-0-12-822688-9.00013-X

9. M. Sheikhan, **H. Bostani**, “Binary Gravitational Search Algorithm (BGSA): Improved Efficiency,” *in Encyclopedia of Information Assurance,* Taylor & Francis, 2016. https://www.taylorfrancis.com/books/9781351235808

Conferences:

10. Z. Moti, A. Senol, **H. Bostani**, F.Z. Borgesius, V. Moonsamy, A. Mathur, G. Acar, “Targeted and Troublesome: Tracking and Advertising on Children's Websites,” *In Proceedings of the 45th IEEE Symposium on Security and Privacy (**IEEE S&P 2024**).*
11. **H. Bostani**, M. Sheikhan, B. Mahboobi, “Developing a Fast Supervised Optimum-path Forest Based on Coreset,” *In Proceedings of 19th International Symposium on Artificial Intelligence and Signal Processing* (***AISP’2017***), pp. 172-177, 2017. DOI: 10.1109/AISP.2017.8324076

12. **H. Bostani**, M. Sheikhan, “Modification of Optimum-Path Forest using Markov Cluster Process Algorithm,” *In Proceedings of 2nd of International Conference on Signal Processing and Intelligent Systems (**ICSPIS’2016**)*, pp. 1-5, 2016. (***Winner of the Outstanding Paper Award***) DOI: 10.1109/ICSPIS.2016.7869874

13. M. Sheikhan, **H. Bostani**, “A Hybrid Intrusion Detection Architecture for Internet of Things,” *In Proceedings of 8th International Symposium on Telecommunication (**IST’2016**)*, pp. 601-606, 2016. (***Selected as one of the Best Papers***) DOI: 10.1109/ISTEL.2016.7881893

ORAL/POSTER PRESENTATIONS

- “Adversarial Machine Learning: Challenges and Solutions in Malware Detection,” **38th Webinar, Iranian Society of Cryptology, December 2023.**
- “Improving Robustness of Machine Learning-based Android Malware Detection against Realizable Adversarial Examples,” **ICT.OPEN’23, Utrecht, the Netherlands, April 2023.**
- “Improving Robustness of Machine Learning-based Malware Detection against Realizable Android Adversarial Examples,” **Lunch Colloquium, Digital Security Group, Radboud University, June 2022.**

- "A Novel Problem-space Evasion Attack for Black-box based Android Malware Detection," **Lunch Colloquium, Digital Security Group, Radboud University, Sep. 2020.**
- "AI for Intrusion Detection," **Lunch Colloquium, Digital Security Group, Radboud University, Oct. 2020.**
- "Developing a Fast Supervised Optimum-path Forest Based on Coreset," **AISP'2017, Shiraz University, Shiraz, Iran, 25-27 Oct. 2017**.
- "Modification of Optimum-Path Forest using Markov Cluster Process Algorithm," **ICSPIS'2016, Amirkabir University of Technology, Tehran, Iran, 14-15 Dec. 2016**.
- "A Hybrid Intrusion Detection Architecture for Internet of Things," **IST'2016, Iranian Research Institute for Information Science and Technology, Tehran, Iran, 27-28 Sept. 2016**.

OUTSTANDING RESEARCH AND PROJECTS

- **Project Manager** in Developing an Integrated Cloud Infrastructure for NOET to Deliver Online Services Associated with NOET's Mission. January 2020–Sept. 2020
- **Senior Researcher** in Developing a New Generation of Optimum-path Forest (OPF) as a Graph-based Machine Learning in Order to Achieve an Efficient Pattern Recognition Tool for Using on Massive Data sets. March 2017–Nov. 2019
- **Senior Developer** in Developing a Knowledge-based System based on the Current Legacy Information Systems of the Iranian University Entrance Exams in order to Facilitate Decision-Making May 2013–Nov 2018
- **Senior Developer** in Developing an Event-based WSN Simulator Based on RPL (the routing protocol for 6LoWPAN). April– June 2015
- **Senior Researcher** in Standardizing Software Testing at NOET. May- August 2013
- **Senior Researcher** in Presenting a Collaborative Filtering Recommender System to Offering the Favorite Major Fields to Students. Dec. 2012–February 2013

RESEARCH AND WORK EXPERIENCES

- **Visiting Scholar** Oct. 2023–Present
  Cybersecurity Group, King's College University
- **Visiting Scholar** Oct. 2023–Present
  Systems Security Lab, University College London
- **Research Assistant** August 2017–Sept. 2020
  Young Researchers and Elite Club of IAU, South Tehran Branch.
- **Research Assistant** August 2016–March 2017
  Research Center of Modeling and Optimization in Science and Engineering, IAU, South Tehran Branch.
- **Full-Stack Developer** Sep. 2012– Sep. 2020
  Strategic Analysis and Information Security Group, Department of New Communications, NOET, Tehran, Iran.
- **Software Expert** April–August 2012
  Software Systems Group, Department of Information and Communication Technology, Bank Hekmat Iranian, Tehran, Iran.

SKILLS AND CERTIFICATIONS

Professional National Certifications:

- **SQL Server Query Tuning and Optimization**, Faratar As Danesh Institute, Tehran, Iran (2018).
- **SQL Server 2016 – Design & Implementation**, Faratar As Danesh Institute, Tehran, Iran (2018).
- **Professional SCRUM Master**, Faratar As Danesh Institute, Tehran, Iran (2016).
- **MCSD Web Pack 2012**, Kahkeshane Noor Institute, Tehran, Iran (2016).
- **ETL (SSIS) and Data Mining (SSAS) 2012**, Faratar As Danesh Institute, Tehran, Iran (2014).
- **Data Warehousing & OLAP using SSAS 2012**, Faratar As Danesh Institute, Tehran, Iran (2014).

- **Win Application (C# & intro ADO.NET)**, South Industrial Management Institute, Shiraz, Iran (2008).

Computer Knowledge:

- **Programming and Scripting:** C/C++, C#, SQL, Java, JavaScript, HTLM & CSS, MATLAB, Python.
- **Frameworks, Tools, and IDEs:** PyTorch, MATLAB Optimization, Fuzzy, and Neural Net Tools, Microsoft Visual Studio, SQL Server Management Studio, Visual Paradigm, Microsoft Office, Azure Boards.
- **Software Development Technologies:** C#.Net Windows Form, ASP.Net Web Form, APS.Net MVC, WCF Service, jQuery & AngularJS, ADO.NET Entity Framework, Java 2 Platform Micro Edition (J2ME), Microsoft BI Technologies (Data Quality, Integrated, Analysis, and Reporting Services).
- **Databases and Dataflow Systems:** SQL Server (programming).
- **Software Development Methodologies:** RUP, EUP, SCRUM.
- **OS:** Windows

Language Skills:

- **Persian (Farsi):** Native language
- **English:** Fluent, TOEFL (Dec 2019) Internet-Based Test: 84/120 (Reading: 21/30, Listening: 22/30, Speaking: 21/30, Writing: 20/30)

REFERENCES

Dr. Veelasha Moonsamy, Tenured Research Faculty at Systems Security Chair, Ruhr University Bochum, Bochum, Germany
Email: email@veelasha.org

Dr. Erik Poll, Associate Professor in the Digital Security group, Institute for Computing and Information Sciences, Faculty of Science, Radboud University, Nijmegen, The Netherlands.
Email: erikpoll@cs.ru.nl

Dr. Mansour Sheikhan, Full Professor of Electrical Engineering, Faculty of Technical and Engineering, Islamic Azad University, South Tehran Branch, Tehran, Iran
Phone: +98 21 88215046
Cell No: +98 9121163132
Email: msheikhn@azad.ac.ir

Dr. Fabio Pierazzi, Associate Professor in Cybersecurity at the Department of Informatics of King's College London (KCL)
Email: fabio.pierazzi@kcl.ac.uk

Dr. Lorenzo Cavallaro, Full Professor of Computer Science, Department of Computer Science, University College London (UCL), UK.
Email: l.cavallaro@ucl.ac.uk