Sepideh Asadi

Ph.D. Student
Faculty of Informatics , University of Lugano

Date of Birth: April 13th 1986
Address: Informatics Building, Office 200 (Level 2)
Via Buffi 13, 6904 Lugano, Switzerland.
Email: sepideh.a65@gmail.com / sepideh.asadi@usi.ch
Website: http://www.inf.usi.ch/phd/asadi

Major Interests:

- Interpolation-based Model Checking
- Formal Verification of Software and Hardware
- SAT/SMT solving
- Information Security

Education:

- Ph.D. Candidate in Computer Science,
  University of Lugano, Lugano, Switzerland (3/2016 - present)
  - Thesis: **Guiding SMT-Based Interpolation for Program Verification.**
    Advisor: Prof. Natasha Sharygina

- M.Sc in Information Technology/ Secure Communications,
  Iran University of Science & Technology (IUST), Tehran, Iran, 9/2010-1/2013.
  - Thesis: "Formal Analysis of Security Properties of Network Management Protocol SNMPv3 and Verification using ProVerif", Score: 19.75/20.
    Total GPA: 17.27/20.

- B.Sc Electrical Engineering/ Electronics,
  Zanjan University, Zanjan, Iran, 9/2004-10/2008.
  - Thesis: Design and Implementation of a logic circuit using Low-Power Techniques.
    Total GPA: 14.48/20.

- Mathematics and Physics Diploma, Hekmat School, National Organization for Development of Exceptional Talents (NODET), Mianeh, Iran, 2000-2004.
  Total GPA: 19/20.

Technical and Research Experience:

- **Senior Researcher**, research group of PKI & Security, Matiran Co., 2/2014 – 9/2015.
- eNID (electronic National ID)
- Our research group is focusing on Issues including integrating PKI components with existing applications such as e-banking, e-commerce, e-health, and e-learning. Our team in collaboration with the most respected and recognized international digital security companies such as OpenTrust, Gemalto, and SafeNet is trying to offer trusted and convenient digital services to the country.

- **Researcher,** Cyber Space Research Institute (**CSRI**), 1/2013 - 6/2013.
  - Teamwork R&D project on:
    "IT Consultant Services and Security Issues for National Information Network based on Enterprise Service Bus (ESB) and G-Cloud" under supervision of Dr. M. Fasanghari.

- **Research Associate,** Iran Telecommunication Research Center (**ITRC**),Tehran, Iran, 7/2011-12/2012.
  - Knowledge Base and Technical Annex for Security of Network Management
  - Formal evaluation and security assurance of network management protocols.

- Under supervision of Professors: H. Shahhosseini, M. Azgomi, M. Naderi, and S. Pourazin.

- Vice-President of research group of "Network Security" in **SSG** (Student Study Group) Association, IT organization of Iran, Tehran, 2011-2012.
- Head of the research group of "Formal Methods in Security" in Student Group Association, IT organization of Iran, Tehran, 2012-2014.
- **Technical Consulter** in Electrical and Communications Engineering, NEDA Industries Co. 9/2008- 9/2009.
  - In-depth understanding of AMR, AMM and AMI concepts, modules and network topology.
  - security requirements for 3 Advanced Metering Infrastructure (AMI).
  - Familiarity with metering protocol: DLMS/COSEM.

Teaching Experience:

- Lecturer at **workshop**, *Approaches to formal verification of security protocols*, Iran Telecommunication Research Center (**ITRC**), Fall 2012.
- Lecturer at **workshop**, *Approaches to E-Voting protocols*, Iran Telecommunication Research Center (**ITRC**), summer 2015.
- Teaching Assistant of Prof. A. Shayestehfard for *Electronics (II)*, Electrical Engineering Department, Zanjan University, Spring 2006.
- Introductory Class to Security+, Matiran Co., Fall 2014.
- Introductory Classes to ProVerif, Iran University of Science & Technology, 2015.

Publications:

Conference & Journal Papers:

- S. Asadi, H. Shahhoseini. **Formal Security Analysis of Authentication in SNMPv3 Protocol by An Automated Tool,** Sixth International Symposium on Telecommunications (IST), pp.1060-1064, 2012. available at http://IEEEXplore.ieee.org/xpls/abs_all.jsp?arnumber=6483143

- S. Asadi, H. Shahhoseini. **Formal Analysis of Privacy in SNMPv3 Protocol by ProVerif,** In 9th International ISC Conference on Information Security and Cryptology (ISCISC'12), 2012.
  available at: http://www.researchgate.net/publication/283072412_Formal_Analysis_of_Privacy_in_SNMPv3_Protocol_by_ProVerif

- S. Asadi, etal. "Formal Analysis of RFID Authentication Protocol using ProVerif " 7th Iranian conference on Electrical Engineering, ICEE, May 2015; (In Persian).

- S. Asadi, H. Shahhoseini. **Automated Formal Verification of Security Properties of SNMPv3 Protocol over User-Based Security Model**". (Submitted to Journal of Security and Communication Networks 2015).

Books:

- S. Asadi, M. Safkhani, et al. **Technical Annex for Security of Network Management**, In: Iran Telecommunication Research Center (ITRC), Tehran, Iran, Dept. of Communications and Information Technology, 2013.
- M. Fasanghari, S. Asadi, H.S Cheragchi. **Security Requirements of Enterprise Service Bus (ESB) based on ITU-T Recommendation X.805**, *ITRC*, 2015.

Honors and Awards:

- Awarded ITRC Research Grant to my M.Sc. Thesis, 2013.
- Awarded "class A" rating for the research project with an honor by Iran Telecommunication Research Center, 2012.

- Ranked among the top 1% of the participants of both undergraduate and graduate university entrance exams.
- Ranked first among the students at the exhibition held for extracurricular activities at Hekmat High school with a digital calculator, 2000.
- Ranked 9th among 800 students of National Organization for Development of Exceptional Talents (NODET) in a general exam, 1996.
- Selected as the best student in Young Mathematicians Contest in Mianeh, 1996.

Programming and Technical skills:

- **Languages:** C/C++, Visual Basic, Verilog, HTML.
- **Tools:** HSPICE, PSPICE, MATLAB, MAX+II, Modelsim, Proteus, CodeVision AVR, ORCAD.
- **Hardware proficiency:** PLCs (S5 & S7)
- **Analyzing Security Protocols Tools:** ProVerif, AVISPA.
- **Microsoft Products:** Microsoft Windows Server 2008 R2.
- **Web Servers:** Apache 2.x, IIS 6.0/7.0.
- **Security and Digital Certificate:** PKI (OpenSSL & Microsoft Certificate Services).
- **Standards and protocols:** TCP/IP, SNMP, SSH, SSL/TLS, HTTP, DNS, FTP, X.509/PKIX and FIPS201, NIST SP 800-157 and related standards.

Invited Talks:

- Survey on Electronic Voting Protocols with a focus on cryptographic aspects, IT organization of Iran, September 2015.
- Formal Analysis of Security Properties of SNMPv3 and Verification using ProVerif, Iran Telecommunication Research Center, January 2013.
- Security in the internet, Security study group, IT organization of Iran, Tehran, February 2011.
- Formal Verification of Security Protocols, Security study group, IT organization of Iran, Tehran, February 2011.
- RFID Security, Security study group, IT organization of Iran, Tehran, 2011.

Memberships:

- Member of IEEE (Graduate Student Membership).
- Member of the research team in Super Computing and Networking (SCaN) laboratory, Electronic Research Center, Iran University of Science and Technology.
- Member of Network Security Group, Iranian Telecommunications Research Center (ITRC).
- Member of Student Branch of Iranian Society of Cryptology at Iran University of Science & Technology, Tehran, Iran.
- The Iranian Construction Engineering Organization, Tabriz, Iran.
- Young Researchers Club, Azad University Mianeh branch, 2000-2004.

Languages:

- English (TOEFL & GRE), Persian, Azeri, Turkish (fair), Arabic (fair).

Extracurricular Activities & Hobbies:

- Psychological Books, Painting, Playing piano, Films, Musics, Plant breeding.
- Sports specially Swimming, volleyball and mountain climbing.

---

* References available upon request.