Amir Naseredini

Secure Systems Group, IAIK, TU Graz, Graz, Austria
FoSS Group, University of Sussex, Brighton, UK
sahnaseredini@gmail.com https://sahnaseredini.github.io

Teaching and Research Interests

- Formal Security
- Programming Languages
- Pi-Calculus & Applied Pi-calculus
- Lambda-calculus
- Vulnerability Analysis
- Microarchitectural Attacks
- Security Protocols
- Cryptographic Hash Functions

Education

University of Sussex, Brighton, UK

Ph.D. in Informatics (Computer Science), Sep. 2018 - present

- Research student at FoSS Group at the University of Sussex

Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran

M.S. in Information Security, Sep. 2015 - Feb. 2018

- Master's Thesis: "Algebraic Cryptanalysis of ARX-Design Hash Functions", (Ranked 3rd among 10 classmates)

University of Kurdistan, Sanandaj, Iran

B.S. in Information Technology, Sep. 2011 - July 2015

- Overall GPA: 18.47/20 - 3.9/4.0 (142 units)
- Main and Technical modules GPA: 18.97/20 - 4.0/4.0 (90 units)
- 1st Student Award, in Computer Eng. and Information Technology Department

Honors and Awards

- Awarded with the School of Engineering and Informatics' Fully-Funded Scholarship by University of Sussex, September 2018
- Selected as a Talented Student, two times (University of Kurdistan): Dec 2013 to Dec 2015.
- Ranked #27 in the PhD National Entrance Test of Iran (Among 1093 persons).
- Ranked #2 in the M.S. National Entrance Test of Iran, With Respect to my B.S. GPA.
- Ranked #6 in Lahijan ACM Contest, on site, March 2014.

Teaching Experience

University of Sussex, Brighton, UK

- **Associate Tutor, Sep. 2018 - present**
  - Assisted Dr. B. Reus in "Further Programming" module, ran weekly lab sessions
  - Assisted Dr. G. Parisis in "Operating Systems" module, ran weekly lab sessions
  - Assisted Dr. B. Reus in "Limits of Computation" module, ran weekly lab sessions

- Assisted Dr. I. Khan in “Introduction to Computer Security” module, ran weekly lab sessions (2018-20)
- Assisted Dr. I. Mackie in “Comparative Programming” module, ran weekly lab sessions (2019-20)
- Assisted Dr. N. De Beaudrap in “Compilers and Computer Architecture” module
- Assisted Dr. D. Dmitrenko in “Programming for Engineers” module (graduate module)
- Assisted Prof. I. Wakeman in “Further Programming” module
- Delivered a lecture about "Rowhammer attack" and "Penetration Testing" to “Introduction to Computer Security” class (139 third-year undergraduate students), 21 November 2019
- Delivered a lecture about "Penetration Testing" to “Introduction to Computer Security” class (144 third-year undergraduate students), 7 December 2018

Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran

- **Lecturer, 2016 - 2017**
  - Taught “Operating Systems Laboratory” module, lectured, and administered all grades
  - Taught “Computer Workshop” module, lectured, and administered all grades
- **Teaching Assistant, 2016 - 2017**
  - Assisted Dr. B. Sadeghiyan in “Applied Cryptography” module (graduate module)
  - Assisted Professor M. Dehghan TakhtFooladi in “Data Structures” module
  - Assisted Dr. E. Nazerfard in “Fundamental of Programming” module

University of Kurdistan, Sanandaj, Iran

- **Teaching Assistant, 2012 - 2015**
  - Assisted Dr. P. Moradi in “Programming in C/C++” module
  - Assisted Dr. P. Moradi in “Data Structures” module
  - Assisted Dr. A. Khorramian in “Data Structures” module
  - Assisted Dr. A. Abdollahpouri in “Programming in Java” module
  - Assisted Dr. A. Abdollahpouri in “Design and Analysis of Algorithms” module

Research Experience (Notable Projects)

TU Graz, Graz, Austria

- **Researcher, Sep. 2020 - present**
  - Conduct research on “Microarchitecture Attacks” under the supervision of Dr. D. Gruss.

University of Sussex, Brighton, UK

- **Researcher, Sep. 2018 - present**
  - Conduct research on “Formal Security” under the supervision of Dr. M. Berger.

Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran

- **Researcher, Feb. 2017 - Sep. 2018**
  - Researched on “Computer Security Assessment” and “Smart phone and Computer forensics” under the supervision of Dr. B. Sadeghiyan and Dr. S. Niksefat
- **Researcher, Sep. 2015 - Feb. 2018**
  - Conducted research on Algebraic Cryptanalysis under the supervision of Dr. B. Sadeghiyan at Data Security Research laboratory (DSRLab)
- **Researcher, 2017**

    - Researched and administered research on “SMC and OT Protocols” under the supervision of Dr. S. Niksefat
- **Researcher, 2016**
    - Researched and implemented “Analysis and Verify KryptoKnight Protocol using CASPA Tool” under the supervision of Dr. B. Sadeghiyan

Publications and Presentations

- A. Naseredini, B. Sadeghiyan, "Security Assessment of ARX-Design Hash Functions against Algebraic Cryptanalysis ", 26th Iranian Conference on Electrical Engineering (ICEE2018), May 2018
- “Cryptographic Hash Functions: Definition, History and Cryptanalysis”. Presented at CE department, Amirkabir University of Technology (Tehran Polytechnic), Iran, May 2017.

Skills

Programming Language

- Haskell
- Python
- Java
- C/C++ & C#

Information Security Tools

- Metasploit
- Nmap
- Wireshark
- Tenable Nessus
- Netsparker

Operating Systems

- Linux (Ubuntu, Kali, Fedora)
- Windows (all kinds)
- Android
- iOS

Membership and Service

- Student Volunteer at PLDI 2020
- Student Volunteer at ECOOP and Curry On 2019
- ACM Membership: May 2013 to Apr 2016
- IEEE Membership: 01-Jan-2012 to 31-Dec-2012
- IEEE Computer Society Membership: 01-Jan-2012 to 31-Dec-2012
- IT association Chairman and primary member, University of Kurdistan: Sep 2013 to Sep 2014

Languages

- Kurdish: Native proficiency
- Persian: Native proficiency
- English: Full Professional proficiency
- Arabic: Elementary proficiency

References

University of Sussex, Brighton, UK

Department of Informatics

- Dr. Martin Berger
  E-Mail: M.F.Berger@sussex.ac.uk
- Dr. Ian Mackie
  E-Mail: i.mackie@sussex.ac.uk

TU Graz, Graz, Austria

IAIK - Institute of Applied Information Processing and Communications

- Dr. Daniel Gruss
  E-Mail: daniel.gruss@iaik.tugraz.at

Please feel free to contact any one of them if you should require more information.