Alireza Toroghi Haghighat

Email: toroghi@aut.ac.ir
Homepage: ce.sharif.edu/~toroghi
Cell-Phone: +98 (912) 820 9474

Education

Ph.D. Candidate IT Engineering, Information Security and E-Commerce Lab (ISEC), Computer Engineering and Information Technology Department, Amirkabir University of Technology, 2013-present.
Adviser: Dr. Mehdi Shajari
Current GPA: 18.12
Comprehensive Exam: Passed
Thesis Title: Service Integrity Assurance for Distributed Computation Outsourcing
Major Subjects: E-Payment Systems (19.7/20), E-Commerce Security (19/20), Cryptographic Protocols (17/20), Game Theory (16.5/20)

M. Sc. Student IT Engineering, Data and Network Security Lab (DNSL), Computer Engineering Department, Sharif University of Technology, 2011-2013.
Adviser: Dr. Rasool Jalili
Thesis Title: "Analysis of Security Properties of E-Voting Protocols: A Provable-Security Approach".
Overall GPA: 18.31
Major Subjects: Advanced Computer Networks (19/20), Computer Networks Management (19/20), Cryptography Theory (17.6/20), Databases Security (18.3/20)

B. Sc. Computer Engineering, Computer Engineering Department, Sharif University of Technology, 2007–2011.
Thesis Title: "A Survey of Zero Knowledge Models".
Overall GPA: 16.05
Major Subjects: Network Security (17.5/20), Operating Systems (17.6/20), Advanced Topics in Computer Engineering (18/20), Logic Circuits (19.5/20), Advanced Programming (18.9/20), Programming Fundamental (18.5/20), Computer Workshop (20/20)

Research Interests

- Security
- Applied Cryptography
- Cryptocurrencies
- Blockchain
- Cloud Security

Publications

- A. T. Haghighat and M. Shajari, "Service Integrity Assurance for Distributed Computation Outsourcing," IEEE Transactions on Services Computing, 2017.
- H. Gasemi, A. T. Haghighat, S. Sharifian, and M. Razazi, "Pervasive Privacy: A Practical Context-Aware System to Preserve Privacy on Android Smartphones," in 7th International Conference on Information and Knowledge Technology (IKT 2015).
- A. T. Haghighat, M. S. Dousti, and R. Jalili, "An efficient and provably-secure coercion-resistant e-voting protocol," in Eleventh Annual International Conference on Privacy, Security and Trust (PST). IEEE, 2013, pp. 161-168.
- A. T. Haghighat, M. A. Kargar, M. S. Dousti, and R. Jalili, "Minimal assumptions to achieve privacy in e-voting protocols," in 10th International ISC Conference on Information Security and Cryptology (ISCISC). IEEE, 2013.

Honors

- Ranked 225th in "Nationwide University Entrance Exam" over more than 270,000 participants, 2007.
- Ranked 11th in "Nationwide Entrance Exam for M.Sc. Studies in IT Engineering major" over more than 20,000 participants, 2011

Academic Experiences

- **Teaching, Sharif University of Technology**,
  - Fundamentals of Programming (Python) (Fall 2015, Spring 2016)
- **Teaching, University of Tehran, Farabi Campus**,
  - Fundamentals of Programming (C++) (Fall 2014, Fall 2015)
  - Advanced Programming (Java) (Spring 2016)
  - Advanced Databases (Fall 2014)
  - Analysis and Design of Information Systems and Databases (Fall 2014)
- **Teaching Assistant (*Selective list*),**
  - E-Payment Systems, By Dr. Shajari, Amirkabir University of Technology, Spring 2016
  - Secure Software Development, by Dr. Jalili, Sharif University of Technology, Spring 2013
  - Data and Network Security, by Dr. Amini, Sharif University of Technology, Fall 2011
  - Advanced Programming, by S. H. Yeganeh, Sharif University of Technology, Spring 2009

Computer Skills

- **Operating Systems:** Linux Family (Ubuntu, Debian, Fedora), BSD Family (FreeBSD), Windows Family
- **Programming Languages:** C, C++, Java, Python, PHP, Prolog
- **Mobile Programming:** Android
- **Web Technologies:** HTML, CSS, Javascript, JQuery, Ajax, Symphony, Django
- **Object Oriented Programming**
- **Modeling Languages & Tools:** UML, Enterprise Architect, Visual Paradigm, Open Model Sphere
- **Hardware Description Languages:** Verilog

- **Databases:** MySQL, PostgreSQL, SQLite
- **Revision Control:** SVN, Git, Mercurial
- **Network and Network Security:** Iptables, Pfsense, Snort, tcpdump, Wireshark, Nmap, Ns–2
- **Assembly Languages:** 8086 family, IBM360
- **Smart Card Programming:** Java Card Programming