Curriculum Vitae

Postal Code: 7618455745
Phone: +989369767942
Email: r.jahanshahi@aut.ac.ir
Date of Birth: 22 Sep 1991
LinkedIn Profile:
https://goo.gl/3FoLCC
Homepage:
http://ceit.aut.ac.ir/~rjahanshahi

Rasoul Jahanshahi

Master of Amirkabir University of Technology

RESEARCH INTEREST

- Secure Multi-Party Computing
- Cloud Computing
- Network
- Authentication Protocols
- Watermarking and Steganography
- Privacy Preserving
- Distributed system
- Authorization Protocols
- Image Processing
- Image Encryption

EDUCATION

M. Sc. Computer Engineering / Information Security
Amirkabir University of Technology, Tehran-Iran, Since 2013
Thesis Title: Privacy Preserving Genetic Algorithm
Supervisor: Dr. Babak Sadeghian
GPA: 15.88/20 till now

B. Sc. Computer Engineering / Software Engineering
Isfahan University of Technology, Isfahan-Iran, 2009-2013
Thesis Title: Improving Watermarking with NSGA II
Supervisor: Dr. Nader Karimi
GPA: 17.43/20

PUBLICATION

S.Karami, B.Sadeghian, R.Jahanshahi, "secure outsourcing of neural computation over distributed data". *On review*

HONORS AND ACHIEVEMENTS

- Ranked in the upper 0.01% among more than 400,000 applicants in the Iranian nationwide university entrance exam, summer 2009.
- Ranked 4th among computer engineering students in Isfahan University of Technology, 2013.
- Ranked 4th among software engineering students in Isfahan University of Technology, 2013.
- Received scholarship for the graduate studies in the school of computer engineering, Isfahan University of Technology, 2013.
- Received scholarship for the graduate studies in the school of computer engineering, Amirkabir University of Technology, 2011.

SEMINARS AND RESEARCH EXPERIENCE

Data warehouse Security, Discussed topics which bind OLAP Technology and Data warehouse including their characteristic, their needs for security and different approaches for enforcing security like Data masking techniques and access control models; Department of Computer Engineering and Information Technology, Amirkabir University of Technology 2014.
Key Recovery Attack on AES, discussed one of the most powerful cryptosystem and one way to perform key recovery attack on this cryptosystem; Department of Computer Engineering and Information Technology, Amirkabir University of Technology 2013.
Privacy Preserving Evolutionary Algorithm, discussed evolutionary algorithm and issues that bring preserving privacy for parties who are involved, and how they can be solved; Department

of Computer Engineering and Information Technology, Amirkabir University of Technology 2014.

Non-Interference in Kernel OS, discussed Non-Interference, Non-Influence and Kernel OS and their binds with each other; introducing one approach to enforce Non-Interference in Kernel OS by defining their data type and system model; Department of Computer Engineering and Information Technology, Amirkabir University of Technology 2014.

Coin flipping with major dishonesty, talked about their definition and their usage in cryptography; discussed their weakness for bias and some papers for resolving this issue; Department of Computer Engineering and Information Technology, Amirkabir University of Technology 2014.

Poly1305-AES, Discussed one of MAC systems, its parts and requirements and how they act in this MAC system, Department of Computer Engineering and Information Technology, Amirkabir University of Technology 2015.

SELECTED PROJECTS

Improvement in Digital Watermarking by Multi-Objective Genetic Algorithm NSGA II; B.Sc. Thesis. ECE Dept. Isfahan University of Technology 2013

Differential Cryptanalysis of DES Cryptosystem; Final Project of "Cryptography" course: Dr. B.Sadeghian, CEIT Dept. Amirkabir University of Technology, 2013

Twofish Cryptosystem Analysis, Implement Twofish Cryptosystem and analysis its avalanche Properties and randomness; Final project of "Cryptography" course: Dr. B.Sadeghian, CEIT Dept. Amirkabir University of Technology, 2013

Implementation and Analysis of Crammer's Voting Protocol, Final Project of "Security Protocols" course: Dr. B.Sadeghian, CEIT Dept. Amirkabir University of Technology, 2014

Configuring Oracle Database with all Security Features, Final Project of "Database Security", CEIT Dept. Amirkabir University of Technology, 2014.

Preventing Information Flow via SELinux, Implementing the principle of least privilege, Preventing access to high risk programs and data, by compromised programs, Final Project of "Secure Computing Systems" course: Dr. shajari CEIT Dept. Amirkabir University of Technology, 2013

Penetration Test of Saman bank's Desktop application, Cert Division of Amirkabir University of Technology, 2015

Penetration Test of Refah bank's Android Application, Cert Division of Amirkabir University of Technology, 2015

ACADEMIC POSITIONS

Amirkabir University of Technology, Iran
Research Assistant
Research on Privacy Preserving of Genetic Algorithms.
  ▪ Data Security Research Lab (Supervised by Dr. Babak Sadeghian). Since October 2013
Teaching Assistant
Head teaching assistant. Duties included giving lectures, fielding of all students' inquiries, and oversight student teaching assistants and graders.
  ▪ Undergraduate Course, Discrete Mathematics: Dr. M.Fallah, fall 2015
Teaching Assistant
Co-Teacher assistant of graduate level course for the Master of Science in Computer
Engineering Program. Responsibility included for lectures, exams, homework assignments, defining projects and grades.
  ▪ Graduate Course, Secure Protocols, instructor: Dr. B.Sadeghian, fall 2015
Cert Division of Amirkabir University of Technology, Iran
Instructor
Teacher of graduate level course for the Master of Science in Computer Engineering Program. Responsibility included for lecture, exam, and grade.
  ▪ Penetration Test Course, fall 2015

Isfahan University of Technology, Iran
Instructor

Teacher of Undergraduate level course for the Bachelor of Science in Computer Engineering Program. Responsibility for lectures, exams, homework assignments, and grades.

- Operating Systems Laboratory, summer 2013

Teaching Assistant

- C Programming, Instructor: Dr. Ali Sharifipour, Fall 2012

WORK EXPERIENCE

Amirkabir University of Technology Cert Lab, Researcher in Incident Response Team, Tehran, Iran, Since July 2015
Security Specialist
Job-content: Penetration Test of Desktop, Android or iPhone Applications, Penetration Test of Websites and Servers, Administration and Hardening of ESXi Server

PROFESSIONAL SKILLS

Programming Language: C, C++, Java, MATLAB, Python, Qt
DBMS: MySQL, PostgreSQL, Oracle
Operating Systems: Windows, Linux
Security Tools: Metasploit, Nessus, Nmap, Cain & Abel, Acunetix
Web Technologies: Vmware, ESXi servers, vSphere, HTML, CSS
Networking Tools: Wireshark, Familiar with: GNS3
Reverse Engineering Tools: IDA Pro, DJ Java Decomplier
Other Libraries and Tools: OpenCV, Android Programming, Eclipse IDE, Visual Paradigm, MS visual Studio
Familiar with: Machine Learning, Swarm Intelligence, Decision Tree, PHP, ASP.NET, GWT Framework, Django Framework

CERTIFIACTES

- Certificate of Attendance in Introductory Course on Penetration Testing, Amirkabir University of Technology APA (Cert) Laboratory (Placed First Team in the Competition), 2013
- Certificate of Attendance in Cryptography Online Course in Coursera Website, 2012 [link]

LANGUAGE SKILLS

Farsi: Native Speaker
English: Fluent
  TOEFL iBT Score: 102/120 (Reading: 28, Listening: 29, Speaking: 20, Writing: 25)
  GRE Score: 312/340 (Verbal: 145, Quantitive: 167)

REFERENECES

Official certificates, documents and other references are available upon request.

Dr. Babak Sadeghian
Faculty of CEIT Department, Amirkabir University of Technology, Tehran, Iran
Email: ba.sadegh@aut.ac.ir

Dr. Nader Karimi
Faculty of ECE Department, Isfahan University of Technology, Isfahan, Iran
Faculty of ECE Department, Isfahan University of Technology, Isfahan, Iran
Email: nader.karimi@cc.iut.ac.ir

Dr. Salman Niksefat
Faculty of APA Research Lab, Amirkabir University of Technology, Tehran, Iran
Email: s.niksefat@aut.ac.ir