

SeyedMohammadMehdi Ahmadpanah

Formal Security Lab., Computer Eng. and IT Dept., Amirkabir University of Tech. (AUT), 424 Hafez Ave., Tehran, Iran
Email: smahmadpanah@aut.ac.ir and smahmadpanah@gmail.com
Home-Page: <http://ceit.aut.ac.ir/~ahmadpanah>
Cell Phone: +98 939 036 1303

RESEARCH INTERESTS

- Language-based Security
- Formal Methods of Information Security
- Programming Languages
- Compiler Design

EDUCATION

- **Amirkabir University of Technology** (Tehran Polytechnic), Tehran, Iran
Ph.D. Student, Computer Engineering, Software
September 2017 - now
GPA: **TBA** / 20
- **Amirkabir University of Technology** (Tehran Polytechnic), Tehran, Iran
M.Sc., Information Technology, Information Security
September 2015 - September 2017
GPA: **17.89** / 20
- **Amirkabir University of Technology** (Tehran Polytechnic), Tehran, Iran
B.Sc., Computer Engineering, Software
September 2011 - September 2015
GPA: **17.69** / 20
- **Refah High School**, Semnan, Iran
Diploma in Mathematics and Physics
September 2007 - June 2011
GPA: High School **19.26** / 20 , Pre-University **19.52** / 20

HONORS AND AWARDS

- The **Youngest** Lecturer (at age 22) and Lab. Instructor (at age 20), Amirkabir University of Technology, Tehran, Iran.
- Honored as the **Best Teaching Assistant** of Computer Engineering and IT Department according to students evaluation for *Discrete Mathematics (Spring 2017)* and *Data Structures (Fall 2017)* course, Amirkabir University of Technology, Tehran, Iran.
- Offered for **Direct Admission** to graduate school (**Ph.D.**) in Computer Engineering - Software, **University of Tehran** and **Amirkabir University of Technology**, without taking the national entrance exam for graduate schools as a reward of academic records and achievements, Tehran, Iran, 2017.
- Ranked **1st** and **2nd** among all Laboratory Instructors in different topics of Computer Engineering and IT Department according to students evaluation for teaching *Computer Lab.* and *Operating Systems Lab.*, respectively, Amirkabir University of Technology, Tehran, Iran, Fall 2016.
- Awarded as the **Outstanding Student** and Achieved **1st** place among 2015-beginner graduate students in Information Security major, Amirkabir University of Technology, Tehran, Iran, 2016 and 2017.

- **Outstanding Graduate Student Fellowship**, Amirkabir University of Technology, Tehran, Iran, 2016.
- Admitted to **Tarbiat-Modares University** and Achieved **43rd** place among all applicants for the M.Sc. University Entrance Nationwide Exam in Information Technology, Iran, 2015.
- Honored as an Active Member of **Student Scientific Association of Computer Engineering and IT Department** (Announced as The best Student Scientific Association of the University), Amirkabir University of Technology, Tehran, Iran, 2015.
- Qualified to **Direct Admission** to graduate school (**M.Sc.**) of Computer Engineering and IT Department, Amirkabir University of Technology, without taking the national entrance exam for graduate schools as a reward of academic records and achievements, Tehran, Iran, 2014.
- Selected as a member of **National Scientific Olympiad** in Computer Engineering team of Amirkabir University of Technology as a result of outstanding performance (3rd place among undergraduate students), Tehran, Iran, 2014.
- Achieved top **2%** place among all applicants for the University Entrance Nationwide Exam (Approximately 260000 applicants) in Math. and Eng., Iran, 2011.
- Achieved top **1.5%** place among all applicants for the University Entrance Nationwide Exam (Approximately 108000 applicants) in Foreign Languages (English), Iran, 2011.
- Skipped **Three** grades of elementary school en masse as an exceptional talent, Tehran, Iran, 2002.

RESEARCH EXPERIENCES

- **Research Assistant**, *January 2015 - present*
Formal Security Lab.

Improving Multi-Execution-based Mechanisms for Enforcing Information Flow Policies, - M.Sc. Project *November 2015 - present*

Recently, much progress has been made on achieving information flow security via Secure Multi-Execution (SME). SME as an elegant dynamic technique enforces security by running one execution of the program per security level, and reinterpreting input/output operations w.r.t their associated security level. Improving its transparency and precision with relaxing the assumptions and adding features to the mechanism is our research goal.

A Tool for Rewriting-Based Enforcement of Noninterference in While Programs - B.Sc. Project, *March 2015 - September 2015*

Program rewriting has recently been suggested as a means of enforcing security policies and proven more powerful than execution monitoring and static analysis. In this project, we implemented a novel, sound and transparent rewriting mechanism to enforce progress-sensitive and -insensitive noninterference information flow policies in programs with observable intermediate values using program dependence graphs. More info: <http://ceit.aut.ac.ir/formalsecurity/rewriter/tool>

- **Static Analysis of Unsafe Use of Variables in Java**, *Spring 2014*
Reviewing the notion of unsafe use of variables, a dependency safety property violation pattern, due to exception occurrences. Also, studying a static approach using control flow graph and data flow analysis to automatically detect this kind of patterns that may introduce potential bugs in Java programs. The research has been done for Research Method and Technical Report Writings course (Technical Report, Oral Presentation, and Poster).

TEACHING EXPERIENCES

- **Lecturer, Advanced Programming, CEIT, AUT** *Spring 2018*
- **Teaching Assistant, Design of Programming Languages,** *Fall 2014, Fall 2015, Fall 2016, Fall 2017*
Under supervision of Prof. Fallah
Team coordinator + Holding classes + Grading assignments (30, 44, 27, 43 Students)
- **Teaching Assistant, Data Structures,** *Fall 2013, Fall 2014, Fall 2016, Fall 2017*
Under supervision of Prof. Dehghan Takht Fooladi
Team coordinator + Holding classes + Design and grading assignments and projects + Revising Syllabus (120-150 Students per semester)
- **Teaching Assistant, Discrete Mathematics,** *Spring 2014, Spring 2016, Spring 2017*
Under supervision of Prof. Fallah
Team coordinator + Holding classes + Grading assignments (114, 108, 151 Students)
- **Teaching Assistant, Principles of Compiler Design,** *Spring 2016, Fall 2016, Spring 2017*
Under supervision of Prof. Razzazi
Holding classes + Grading exams + Design and grading project (28, 40, 22 Students)
- **Instructor, Operating Systems Lab.,** *Spring 2016 [evaluation: 18.90/20], Fall 2016 [evaluation: 19.58/20]*
Under supervision of Prof. Bakhshi
Holding classes + Design and grading assignments and exams (13, 12 Students)
- **Instructor, Computer Lab.,** *Fall 2016 [evaluation: 18.99 and 19.62/20]*
Under supervision of Prof. NickAbadi
Holding two group classes + Design and grading assignments and exams + Revising Syllabus (23, 20 Students)
- **Teaching Assistant , Advanced Programming,** *Spring 2013, Spring 2014, Spring 2015*
Under supervision of Prof. Noorhosseini
Team coordinator + Holding classes + Design and grading assignments and exams + Revising Syllabus (126, 68, 55 Students)
- **Teaching Assistant, Computer Networks II,** *Spring 2015*
Under supervision of Prof. Sabaei
Design and grading assignments (60 Students)
- **Teaching Assistant, Information Storage and Retrieval,** *Spring 2015*
Under supervision of Prof. NickAbadi
Design and grading project (53 Students)
- **Teaching Assistant, Software Engineering I,** *Fall 2014*
Under supervision of Prof. Pourvatan
Holding classes + Design and grading assignments and projects (92 Students)
- **Teaching Assistant , Computer Architecture,** *Spring 2014*
Under supervision of Prof. Zarandi
Team coordinator + Design and grading assignments and projects (102 Students)

PUBLICATIONS AND TECHNICAL REPORTS

- **S.M.M. Ahmadpanah** “*Dynamic Enforcement of Security Hyperproperties*” - report for Seminar course (In Persian), AUT, Tehran, Iran, 2016.
- **S.M.M. Ahmadpanah** “*End-to-End Verifiable Elections*” - seminar report for Security Protocols course (In Persian), AUT, Tehran, Iran, 2016.
- **S.M.M. Ahmadpanah**, E. Edalat “*Formal Analysis of Kerberos v5*” - project report for Security Protocols course (In Persian), AUT, Tehran, Iran, 2016.
- **S.M.M. Ahmadpanah**, S.A.H. Nasereddini “*MSSQL Security: Overview, Mechanisms and Best Practices*” - project report for Secure Computer Systems course (In Persian), AUT, Tehran, Iran, 2016.
- **S.M.M. Ahmadpanah** “*Meet-in-the-Middle Attacks on Feistel Constructions*” - seminar report for Applied Cryptology course (In Persian), AUT, Tehran, Iran, 2016.
- **S.M.M. Ahmadpanah**, S.A.H. Nasereddini “*TwoFish Cryptosystem: A New 256-bit Expansion*” - project report for Applied Cryptology course (In Persian), AUT, Tehran, Iran, 2016.
- **S.M.M. Ahmadpanah**, S.A.H. Nasereddini “*TwoFish Linear and Differential Cryptanalysis*” - project report for Applied Cryptology course (In Persian), AUT, Tehran, Iran, 2016.
- **S.M.M. Ahmadpanah**, “*A Tool for Rewriting-Based Enforcement of Noninterference in While Programs*” - B.Sc. Thesis (In Persian), AUT, Tehran, Iran, 2015.
- **S.M.M. Ahmadpanah**, “*An Introduction to Artificial Bee Colony*” - project report for Artificial Intelligence course (In Persian), AUT, Tehran, Iran, 2015.
- **S.M.M. Ahmadpanah** “*An Introduction to Lambda Calculus*” (In Persian), Hamgaam Magazine, Tehran, Iran, 2014.
- **S.M.M. Ahmadpanah**, “*Static Analysis of Unsafe Use of Variables in Java*” - technical report for Research Method and Technical Report Writings course (In Persian), AUT, Tehran, Iran, 2014.
- **S.M.M. Ahmadpanah**, H.R. Ramezani, “*An Introduction To Adders*” - project report for Computer Architecture course (In Persian), AUT, Tehran, Iran, 2013.

TALKS

- **S.M.M. Ahmadpanah** “*Monitoring-Oriented Programming*” - GradTalk (In Persian), Computer Engineering and IT Department, Amirkabir University of Technology, Tehran, Iran, 2017.
- **S.M.M. Ahmadpanah** “*Monitoring-Oriented Programming*” - Oral presentation for seminar of Software Systems Security course (In Persian), AUT, Tehran, Iran, 2017.
- **S.M.M. Ahmadpanah** “*Dynamic Enforcement of Security Hyperproperties*” - Oral presentation for Seminar course (In Persian), AUT, Tehran, Iran, 2016.
- **S.M.M. Ahmadpanah** “*Probabilistic Noninterference*” - Oral presentation for seminar of Formal Models and Information Security course (In Persian), AUT, Tehran, Iran, 2016.
- **S.M.M. Ahmadpanah** “*End-to-End Verifiable Elections*” - Oral presentation for seminar of Security Protocols course (In Persian), AUT, Tehran, Iran, 2016.
- **S.M.M. Ahmadpanah** “*Explainable Security for Relational Database*” - Oral presentation for seminar of Database Security course (In Persian), AUT, Tehran, Iran, 2016.

	<ul style="list-style-type: none"> • S.M.M. Ahmadpanah “<i>Meet-in-the-Middle Attacks on Feistel Constructions</i>” - Oral presentation of seminar for Applied Cryptology course (In Persian), AUT, Tehran, Iran, 2016. • S.M.M. Ahmadpanah, “<i>Static Analysis of Unsafe Use of Variables in Java</i>” - Oral presentation for Research Method and Technical Report Writings course (In Persian), AUT, Tehran, Iran, 2014.
WORK EXPERIENCES	<ul style="list-style-type: none"> • Amirkabir University of Tech. CERT Lab. (A.P.A.), <i>Summer 2015</i> <i>Software Tester and Developer</i> • Rayan Pardazan Nikro Emertat (RAPNA), <i>Summer 2014</i> <i>Software Engineer and Web Developer (PHP server-side for an Android application) - Summer Internship.</i> • Sharif University of Technology Research Center, <i>May 2012 - present</i> <i>Question Designer and Checker of several Employment Exams</i>
AUDITED COURSES	<ul style="list-style-type: none"> • Formal Methods in Information Security, <i>Spring 2015</i> <i>By Prof. Fallah, Amirkabir University of Technology</i> • Advanced Programming Languages, <i>Fall 2015</i> <i>By Prof. Fallah, Amirkabir University of Technology</i> • Game Theory, <i>Spring 2014</i> <i>By Prof. Fallah, Amirkabir University of Technology</i>
TOP ACADEMIC COURSE PROJECTS	<ul style="list-style-type: none"> • Software Systems Security, <i>Threat Modeling and Bug Filing of a File Integrity Checker</i> • Network Security, <i>Security Mechanisms and Defense Techniques in different layers of Computer Networks</i> • Database Security, <i>Security in Oracle including User Management, Roles, VPD and Auditing</i> • Security Protocols, <i>Formal Analysis of Kerberos v5 Protocol with MaudePSL</i> • Secure Computer Systems, <i>BufferOverflow in SELinux and MSSQL Security Survey</i> • Cryptology, <i>TwoFish Cryptosystem: 256-bit Expansion and, Linear and Differential Analysis</i> • Microprocessor, <i>Simulating a Greenhouse in Proteus with ATmega16</i> • Compiler Design, <i>Implementing a front-end compiler for a programming language using flex and bison. This project was done using Java and C in two versions.</i> • Information Technology Strategic Planning, <i>Evaluation and Analysis of Transportation Organization of Tehran Municipality.</i> • Information Storage and Retrieval, <i>Amirkabir Search Engine 1.0: Implementing a static search engine using both traditional tf-idf method and semantic hashing for content-based document retrieval. This project was done using Java.</i>

- **Internet Engineering (Web Programming),**
Implementing an HTTP Analyzer (by Java), a webpage like www.macrumors.com (by XHTML and CSS), a weblog publishing tool (by JavaScript, PHP, HTML and CSS).
- **Project Management & Control,**
Evaluation and Analysis of creation and setup of data center services in Khuzestan province project.
- **Operating System Lab.,**
Implementing a calculator. This project was done using Fedora shell scripting.
- **Software Engineering II,**
Analysis and Design of a bookstore WebApp project by UML.
- **Software Engineering I,**
Analysis of a website project by UML.
- **Database Systems,**
Implementing a system like iTunes. Our database was MongoDB. This project was done mainly using Java.
- **Programming Languages,**
Developing an interpreter using ML language. This project was done using lex, yacc, and other abilities of OCaml.
- **Computer Networks I,**
Implementing an FTP client. This project was done mainly using Java.
- **Design of Algorithms,**
Implementing L-Tiling algorithm and Ford-Fulkerson algorithm. These projects was done mainly using Java.
- **Machine Language,**
Developing a previously dominant algorithm for the encryption of electronic data called DES. This project was done using Mips assembly language.
- **Data Structures,**
Implementing search files application with Inverted-Index algorithm. This project was done mainly using Java.
- **Logic Circuits,**
Design and Implementation of mastermind circuit. This project was done mainly using Proteus.
- **Advanced Programming,**
Developing JTank (a game like NormalTanks), JDM (a download manager like IDM) and JCalculator (a calculator). These project was done mainly using Java.
- **Principles of Programming,**
Developing Paint, Snake, Tetris, Editor(English and Persian) and Calculator(+ drawing diagram). These project was done mainly using C.

OTHER ACTIVITIES

- Founder and Coordinator of **Grad Talks**, Computer Engineering and IT Department, Amirkabir University of Technology, *Jan. 2017 - present.*
- Participant and Staff Member of **German-Austrian-Iranian Workshop on Digital Security and Privacy**, Amirkabir University of Technology, *Oct. 2016.*
- Member of **Computer Society of Iran**, *Jun. 2016 - present.*

- Executive Director and Website Administrator of **Formal Security Lab.**, Computer Engineering and IT Department, Amirkabir University of Technology, *Oct. 2015 - present.*
- Founder and Coordinator of **Graduate Students Learning Group**, Computer Engineering and IT Department, Amirkabir University of Technology, *Oct. 2015 - July 2016.*

In this group, we talk and discuss about any fresh topics and review computer science subjects. The members are the best students of graduate school of all M.Sc. majors.

- Head of visiting of IranOpen Robotics Festival for Computer Engineering and IT students (more than 20 students), Amirkabir University of Technology, *April 2016.*
- Assistant Coordinator of **National Scientific Olympiad** of Computer Engineering team, Computer Engineering and IT Department, Amirkabir University of Technology, *2016.*
- Management Board Member and Chief of Informatics of **Student Scientific Association** of Computer Engineering and IT Department (Elected by the votes of the students), Amirkabir University of Technology, *Jan. 2014 - Feb. 2015.*
- Staff Member of **2nd Ideas and Programming competitions for Smart Devices (IranMobiCode 2014+)** at Computer Engineering and IT Department, Amirkabir University of Technology, *Dec. 2014.*
- Staff Member of **1st IdeasBazaar Event** at Computer Engineering and IT Department, Amirkabir University of Technology, *Dec. 2014.*
- Staff member of **14th collegiate ACM contest** at Computer Engineering and IT Department, Amirkabir University of Technology, *Nov. 2014.*
- Staff member of **6th Linux Festival** at Computer Engineering and IT Department, Amirkabir University of Technology, *May. 2014.*
- Staff Member of **1st Ideas and Programming competitions for Android (IranMobiCode 2014)** at Computer Engineering and IT Department, Amirkabir University of Technology, *Mar. 2014.*
- Staff Member and official poster designer of **13th collegiate ACM contest** at Computer Engineering and IT Department, Amirkabir University of Technology, *Nov. 2013.*
- Staff Member and official poster designer of **1st National student ACM contest** at Computer Engineering and IT Department, Amirkabir University of Technology, *Mar. 2013.*
- Staff Member and official poster designer of **1st AUT AI programming contest** at Computer Engineering and IT Department, Amirkabir University of Technology, *Apr. 2013.*
- Participant and official poster designer of **12th collegiate ACM contest** at Computer Engineering and IT Department, Amirkabir University of Technology, *Nov. 2012.*
- Cooperation with **Pouyesh Magazine**, The publication of Guild Council at Computer Engineering and IT Department, Amirkabir University of Technology, *Sep. 2012 - present.*
- Chosen as **The Best Owner of Idea** at Technology Ideation competition (IPTEC), Semnan, Iran, *2009.*

TECHNICAL SKILLS

- Announced as **The Best Book Reader** of Public Libraries, Semnan, Iran, *2010*.
- **Programming Languages:**
Expert in: Java, C/C++
Familiar with: Mips, ML, OCaml, Lisp, Racket, Shell Scripting.
- **Database Systems:**
Expert in: MySQL
Familiar with: MongoDB.
- **Operating System:**
Windows, Linux (Ubuntu, Fedora and Kali).
- **Web Development:**
HTML (XHTML and HTML 5), CSS, Java Script, jQuery, PHP, XML, XSLT, J2EE.
- **Other:**
MS Threat Modeling Tool, PRefast, GNS3, MaudePSL, SELinux, UML, Flex and Bison, Boson NetSim, Cisco Packet Tracer, MS Project, VHDL, Verilog, Orcad Pspice, Proteus.

LANGUAGES

- **Persian** (Farsi) : *Mother tongue (Native)*
- **English** : *Professional working proficiency*

REFERENCES

- **Mehran S. Fallah, Associate Professor**
Computer Engineering and IT Department, Amirkabir University of Technology
Email: msfallah@aut.ac.ir
- **MohammadReza Razzazi, Professor**
Computer Engineering and IT Department, Amirkabir University of Technology
Email: razzazi@aut.ac.ir
- **Mehdi Dehghan TakhtFooladi, Professor**
Computer Engineering and IT Department, Amirkabir University of Technology
Email: dehghan@aut.ac.ir
- **Seyed Majid Noorhosseini, Assistant Professor**
Computer Engineering and IT Department, Amirkabir University of Technology
Email: majidnh@aut.ac.ir
- **Masoud Sabaei, Associate Professor**
Computer Engineering and IT Department, Amirkabir University of Technology
Email: sabaei@aut.ac.ir
- **HamidReza Zarandi, Associate Professor**
Computer Engineering and IT Department, Amirkabir University of Technology
Email: h_zarandi@aut.ac.ir
- **Bahador Bakhshi, Assistant Professor**
Computer Engineering and IT Department, Amirkabir University of Technology
Email: bbakhshi@aut.ac.ir
- **Ahmad NickAbadi, Assistant Professor**
Computer Engineering and IT Department, Amirkabir University of Technology
Email: nickabadi@aut.ac.ir

Last Update: Jan. 2018