# MOHSEN AHMADI

## Security Researcher

@ pwnslinger@asu.edu  +1 (480)-280-7998  1655 E University Dr, Apt #CD-2068  Tempe, Arizona  @pwnslinger
in linkedin.com/in/pwnslinger/  github.com/pwnslinger

## EDUCATION

### MS in Computer Science (Cyber Security)

**Arizona State University**

2017 – 2020  Tempe, AZ  3.57

### B.S in Information Technology (IT)

**University of Isfahan**

2013 – 2017  Isfahan, Iran  3.74

## PROJECTS

**Contributions**

- ***cuckoo* sandbox**: auto generating customizable VMs for large-scale Malware analysis under VBox, VMWare, Xen, Hyper-v, ESXi backends
- ***angr* framework**: Empowering angr with a new lifter engine (PyTCG) which supports more architectures than VEX IR
- **HoneyNet Project**: Enhancing the feasibility of interaction with Honeypot sensors for the community
- **USBlocker**: Introducing new capabilities to the HIDS engine driver for the USB traffic monitoring

**Course**

- Graduate Final Project: “Uncovering news ways to overwrite the firmware of the USB peripherals”
- Applying cryptographic best practices in designing AES from scratch in C, including considering attacks like Side-channels
- Bypassing Fight-Back Mechanism of OSPF Routing Protocol

## PUBLICATIONS

- M. Ahmadi and B. S. Ghahfarokhi, *"Preserving privacy in location based mobile coupon systems using anonymous authentication scheme,"* in Information Security and Cryptology (ISCISC), 2016 13th International Iranian Society of Cryptology Conference on, 2016, pp. 60-65.
- Protocol Structure and Semantic Extraction using Automated Binary Reverse-Engineering Technique ISCISC2016 – M.ahmadi, N.Momenian, B.Tork Ladani

## HONORS AND AWARDS

- Won the 1st Place in Nullcon HackIM CTF 2014
- Iranian National Olympiad in Informatics (INOI’19) Finalist
- Ranked the 3rd Place in Sharif University of Technology 2014
- PicoCTF Letter of Appreciation from CMU CyLab
- Playing at Finals DEFCON 26 CTF under Shellphish

## TEACHING ASSISTANTSHIP

### CSE 545 (Software Security)

**Prof. Fish Wang**

Aug 2018 – Dec 2018  Arizona State University, US

## WORK EXPERIENCE

### Research Assistant (Full-time Employee)

**SEFCOM**

Aug 2017 – May 2019  Tempe, Arizona

- Andriller: Fuzz-testing android services using AFL + angr
- Skynet: Automatically Detecting Root-cause of Vulnerabilities
- PyTCG: FFI-based Python Wrapper for QEMU TCG IR
- Epsilon: Using Symbolic Execution to Find Side-channels
- Developing a Fuzzer based on AFL Methodology

### Windows HIDS Engine Developer

**Payam Pardaz**

May 2016 – Aug 2017  Isfahan, Iran

- Ravin-HIDS: Developing Kernel-mode Drivers to Monitor and Detect Malicious Activities

### Web/Mobile Application Security Assessor

**Amngostar Payam Pardaz**

Oct 2014 – Aug 2017  Tehran, Iran

- Automating Penetration Test on Various Different Platforms
- Responsible Bug Reporting to Different Organizations

### Vulnerability Researcher and Malware Analyzer

**KNSecure**

Dec 2014 – Nov 2015  Tehran, Iran

- Software Security Verification in Windows Platform

### SOC Head of Red Team

**IRISACO**

Dec 2013 – Aug 2015  Isfahan, Iran

- Designing Labs for Testing the Effectiveness of SOC in Detecting Multi-stage Attacks

## TECHNICAL SKILLS

**C/C++, Python, Bash, PHP (Symfony)**
**MVC, Makefile, Javascript, Java**
**Matlab, Git, SVN, Travis CI, Ansible**

## SOFTWARE SKILLS

- IDA Pro, WinDBG, OllyDBG, BinDiff, angr, S2E, PANDA
- Linux OS (Fedora/Ubuntu/CentOS), Vim, Visual Studio

## VOLUNTEER ACTIVITIES AND TALKS

### Head of Student Branch of ISC (SBISC)

**Iranian Society of Cryptology (ISC)**

2015 – 2017  University of Isfahan, IR

- Leading UI-CERT CTF Team and Participating in National and International competitions
- Managing the SBISC organization for two years, getting the first place among other universities

### Invited Talk: angr and future of binary analysis

**OffsecConf’19**

- Designing Challenges and Organizing six in-class Attack-and-Defense CTFs

### Advanced Malware Analysis and Tracking

**Prof. Behrouz Tork Ladani**

Jan 2015 – Jul 2015 University of Isfahan, IR

- Designing Challenges and Organizing the MalCTF