Omid Setayeshfar

Email: omid.s@uga.edu linkedin.com/in/omidsetayeshfar/ notsomeh.me

Qualification Summary

- Experienced in problem solving specially in the field of enterprise software, industrial problems and security.
- Proficient with many programming languages and software development platforms in web based and client side programming as well as embedded systems, including Java, Microsoft.Net, JavaScript and C; broadly experienced in different areas of system and network security; I also have a history of team and project management using various methodologies including RUP and SCRUM.
- Efficient at flexibility and team work especially in teams where different majors come together.

Honors

- Ranked Second in HomeDepot CodeAthlon *Atlanta 2018*
- Elected as CS Graduate Student Association's president *UGA, 2018-2019*
- Ranked Second in Computer Science Research Week Poster competition. *UGA, 2017*
- Ranked Best for designing a gas type determination device using sound waves *Khawrazmi Fest. 2006*
- Awards won for more than 20 designs including "a food suggestion algorithm based on family preference and afford" *Khawrazmi Fest. 2004-2007*
- Won NODET Idea Design Challenges twice *NODET, 2006,2007*
- Honorary Member of Iranian Young Mathematicians Society *Iran– 2003*

Skills

Programming Languages: Python, Java, C, HTML5, ASP.NET, Code Vision, Assembly, C#, Objective-C, R
Software: Neo4J, MySQL, MS Projects, MS SharePoint, SQL Server, SQL Profiler, Log Stash, Log Agent, Log Agent, HEKA
Other: Windows WMI and WQL, Machine Learning, Deep Learning, Big-Data, Distributed System Design, Business Development and Analysis, Project Management, Web and IP Crawling, GPU Computing (CUDA), Embedded Systems

Education

University of Georgia, Department of Computer Science *Aug 2015- Aug 2020(expected)*
PhD, Computer Science *Athens, GA, USA*

Shahid Chamran University *Sep 2007- May 2012*
Bachelor of Science, Computer Software Engineering (first of Class) *Ahvaz, Iran*

National Organization for Development of Exceptional Talents (NODET) *Sep 1999- June 2006*
Diploma, Math and Physics *Dezful, Iran*

Relevant Experience

Intern Researcher, NEC Labs America., Princeton, NJ, USA *May 2017-Aug 2018*

- Developed multiple modules for Automated Security Intelligence system.
- Done research in the field of Systems Security which have resulted in 2 patents and 2 under writing research papers.

Research Assistant, The University of Georgia., Athens, GA, USA *Aug 2015 -Current*

- As Research Assistant to Dr. Kyu H. Lee, I have done numerous feasibility studies and worked on many government and industry funded projects, including projects mentioned in the projects sections.

Department Manager, Samix Co., Tehran, Iran *Jun 2014 - Aug 2015*

- Managed and assessed more than **10** projects of more than 100K$s of worth
- As "Mobile Solutions Committee Member" participated in Mobile Software business line development.
- As "CIO & New business development consultant to the CEO" helped analyzing and utilizing new technologies which resulted in lunching 1 new business line and 3 new startups.

Software Developer/ Analyzer, Samix Co., Tehran, Iran *Nov 2013 - Aug 2015*

- I analyzed and designed numerous software for big companies and banks including ***The Central Bank***
- I Programed several network distributed automated systems using integration of Active Directory, FTP and other network services.
- Also I utilized artificial intelligence approaches and basic data mining principals to some enterprise problems including banking transactions, help desk requests, road traffics and routes.

Some Projects

Research Projects

- **Cyber Deception,** formulating the computer security as a multi agent game playing problem between the attacker and defender we aim to deceive the attacker to learn their intent.
- **IoTDog: An Smart Home Privacy Evaluation,** we evaluated traffic coming from main stream smart home devices to evaluate them against a set of new attacks.
- **Microsoft Malware Classification Challenge (Kaggle),** we classified malware samples into groups of malware families based on malware binaries using, DeepLearing network implemented in Keras and TensorFlow.
- **Google Landmark Prediction Challenge (Kaggle),** finished in top 100, we tried to classify landmarks seen in images into 15K classes.
- **Cilia Segmentation,** using DeepLearning frameworks and optical flow we segmented out parts of cells.
- **Cyber Deception,** Funded by US Mil. We are trying to develop a game theory framework that deceives attackers in a cyber security incident into traps where their behavior will be analyzed and automated actions will be taken against them.
- **Log dependency graph visualizer,** reads and visualizes the system log entries into dependency and causal graphs highlighting resources and access types as well as a simple language to query them. published under our ASIACCS17 paper
- **TRACE,** in this project supported by DARPA we are tackling APT-Advanced Persistent Threats-. I have helped analyze and convert -mostly system call- forensics logs to key value pairs. Also I helped with analysis of more than 1TB of log containing crafted APT attacks as well as normal user behavior.
- **FastLog,** as part of our TRACE project research, this is a very high-performance log processor and string matching algorithm (beating the state of the art -DFC- by 35%, almost 5 times faster of that used in SNORT IDS).
- **GPU-based High-Performance Log Analysis, and the APT detection in (near) real-time,** under support of NVIDIA GPU Grant, we are utilizing GPU computing to speed up the large scale log processing as well as broadening our previous work's bandwidth.
- **Traffic Video Prediction,** we successfully leveraged *Deep Learning* and *RNNs* to predict video frames in traffic videos leveraging GPU computing for higher performance.
- **141.ir,** an advanced nationwide data gathering and reporting system with crowd sourcing navigation system suggesting routes and road state reporting with online hazard alert capabilities; Iranian Road Maintenance Ministry, I participated in algorithm designs for routing and data gathering; also I was one of the system architects on this project; deployed since 2013 this system has an average of 1000 concurrent users and peaks at several more.
- **Banking Surplus System,** analyzing the enormously huge banking transactions over an international Iranian bank's network to calculate surplus as well as profit/loss and visualize them; deployed since mid 2014 this system processes multiple Tera bytes of data each week to extract the weekly reports.

Mobile Development

- **141 App, iOS development**, available on iTunes store is a navigation app with more than 100K active users; it has just been ranked #90 in free navigation apps on iTunes market by third party market watches.

Publications

- **DroidForensics: Accurate Reconstruction of Android Attacks via Multi-Layer Forensic Logging,** X. Yuan, **O. Setayeshfar**, H. Yan, P. Panage, X. Wei, K. H. Lee –ASIACCS17
- **GrAALF: Supporting Graphical Analysis of Audit Logs for Forensics, O. Setayeshfar,** C. Adkins, M. Jones, K.H. Lee, P. Doshi – arxiv.org

Posters

- **FastPP: A very fast log preprocessing and aggregation tool,** Omid Setayeshfar, Kyu H. Lee , SEC Security Conference, Auburn, AL 2018

Patents

- **Automated Software Safeness Categorization with Hybrid Information Sources,** Pending, NEC Labs America
- **Path Based Program Lineage Inference Analysis,** Pending, NEC Labs America