Kiavash Satvat
PhD Student
University of Illinois at Chicago
205-862-0701 | ksatva2@uic.edu
LinkedIn: https://goo.gl/Be4VtC

Education.

Ph.D. in Computer Science, University of Illinois at Chicago, United States. **2018 - present**

- Research on the application of Natural language processing (NLP) and deep learning in threat detection.
- Detection of lateral movement between various hosts using similarity metrics adopted from NLP techniques.
- Developed a deep learning model using LSTM-CRF to extract the named entities from vulnerability reports (CVE-NVD) for automated exploit generation.

M.Sc. Computer Security and Resilience, Newcastle University, United Kingdom. **2011 - 2012**

- Introduced privacy vulnerabilities in Private Modes in the most popular web browsers.
- Developed extensions for Chrome, Safari, and Firefox to log the users' activities during web browsing.
- Developed and delivered numerous projects in a variety of fields such as HCI, system security, and cryptography.

B.Sc. Information Technology Engineering, PIAU University, Tehran, Iran. **2003 - 2008**

- Developed numerous websites using PHP and MySQL and open source applications.
- Delivered presentations and numerous projects on various topics such as Networking and web development.

Work Experiences.

Enterprise Infrastructure Specialist, MTN Group Telecom, Irancell, Tehran, Iran. **Dec 2015 - Aug 2016**

- Designed and planned infrastructure solutions to host business applications considering geo-redundancy.
- Worked closely with the Network group and IP teams to ensure infrastructure stability and network capacity.
- Designed Infrastructure architecture to cater for future system capacity and any Data Centre expansions.

EUS Team Lead, MTN Group Telecom, Irancell, Tehran, Iran. **Aug 2014 - Dec 2015**

- Monitored the periodical scanning of the systems and network elements to make sure they meet security standards.
- Managed and implemented Data Loss Prevention (DLP) strategies for Enterprise Network.
- Managed and implemented client Backup strategies and disaster recoveries.
- Managed and implemented Enterprise Endpoint Protection software systems.
- Involved in data leakage incidents investigation and mitigation programs carried out with involved teams.

Application Security Specialist, MTN Group Telecom, Irancell, Tehran, Iran. **Nov 2012 - Aug 2014**

- Performed regular vulnerability testing and follow up till fixation and provided related reports.
- Supported the implementation and administration of Vulnerability and Patch management solutions.
- Experienced in designing policies and procedures.
- Analyzed the effectiveness of information security functions and provide recommendations and reports to ITS Security Managers.
- Monitored vendors' advisories and vulnerability news groups to capture new vulnerabilities.
- Experienced in designing policies and procedures.

Software Engineer Specialist, System Groups Corporation, Tehran, Iran. **Oct 2004 - Nov 2010**

- Reviewed OS, database and application accesses and cleanup unneeded and dormant accesses.
- Reviewed user and password settings on systems to check access control policies compliance.
- Performed regular review of firewall ACLs and VPN accesses.
- Implemented role-based access management for the company's divisions.

Academic Experiences.

Research Assistant, University of Illinois at Chicago, United States. **May 2018 - present**

Teaching / Research Assistant, University of Alabama at Birmingham, United States. **Sep 2016 - Apr 2018**

- Teaching Assistant: Investigating Online Crimes, Malware Analysis, Big Data Programming, Advance Algorithm Programming Languages, and Introduction to Cyber Security.

Guest Lecturer at Azad University of Parand, Tehran, Iran. **Sep 2013 - Jul 2014**

- Software Engineering and Fundamental of Web Development.

Technical Skills.

- **Programming:** Python, C, Javascript, PHP.
- **Databases.** MySQL, MSSQL, PostgreSQL.
- **Operating System:** Windows, Linux: Centos, Ubuntu, Kali Linux.
- **Machine Learning and Statistical Analysis:** Allennlp, StanfordNLP, Scikit-learn, Keras, NLTK, Numpy, Matplotlib, R, Weka, Matlab, SPSS.
- **Other tools:** A wide range of security analysis tools, fNIRS devices and EEG headsets, Neo4j, and graph DBs.

Research Projects.

- **Provenance graph extraction using Semantic Role Labeling (SRL).** Utilized various NLP and deep learning techniques to extract the semantics from the unstructured blog post. This project aims to utilize the available knowledge presented in the technical blogs for threat detection. In more detail, I scraped over 40K technical blog posts, aiming to automatically process them and extracting meaning full semantic which can be processed by state of the art toolkits to prevent complex attacks(i.e., APT). I extracted data in the form of ontology's RDFs (triplets) and representing them as typed provenance graph. As a part of this project, we use a wide range of machine learning and

NLP techniques and tools such as text classification, Semantic Role Labeling (SRL), Dependency Parsing, Constituency Parsing, Neural-coref and Recursive Neural Networks (RNN) such as Allennlp, and N-ref.

- **Domain-Specific Named Entity Recognition.** Implemented a deep learning technique to extract the relevant cyber-security entities, such as vulnerability type, application name, version, file name, etc. from unstructured natural language and generate their corresponding exploits using the novel exploit generation tools. Timely discovery of information on newly published vulnerabilities and generating their corresponding exploits requires an automated system to extract information from the Web unstructured text. In this paper we implemented a neural architecture based on bidirectional LSTMs and conditional random fields (CRF) which shows the state of the art accuracy on NER data sets.
- **Cyber-security text-Classification and document clustering.** Worked on CTI and malware reports to extract possible intelligence from the text. I employed machine learning techniques to classify sentences and also used various clustering methods including LSH and Minhash to cluster nearly duplicate documents.
- **Enhanced Crash Reporting System.** Proposed a hotfix to enhance users' privacy and security in Automatic Crash Reporting Systems by detecting and removing sensitive data from the crash report prior to submission of the report to the server. We employed deep learning and NER techniques to detect comments, which contain private data like username, password, address, etc. We also further categorize comments based on the information they hold and cluster them in highly technical reports, and non-technical reports.
- **BCI demographic and age Inference.** We demonstrated the possibility of obtaining users' demographic information including age and gender through the Brain-Computer Interfaces (BCI) devices. We designed a machine learning technique to identify the user age group and gender by analyzing the innocuous brainwave signals leaked online in response to users' viewing of simple images or watching videos. Our study shows that we can predict the aging condition with 94% accuracy.
- **Credit Card Fraud Detection.** Employed different machine learning models to detect credit card fraud transactions in imbalanced data. Explored and summarized a wide body of work in the literature on credit card fraud detection using machine learning techniques, and provided a demonstration of Ridge Classifier, Logistic Regression, SVM, Neural Networks, AdaBoost, and Random Forest for this task (Python, R).
- **Secure File Sharing.** The current cloud architectures demand customers' trust in the integrity of providers. In this work, we introduced a practical system to boost the security assurance delivered by the current cloud architecture without requiring any changes on the cloud service providers, allowing users to securely and efficiently store and access their files stored on public cloud storage. Using a fast and light-weight XOR secret sharing scheme, we secret-shares users' files and distributes them among n publicly available cloud platforms (namely, Google Drive, Box, and Dropbox).

Publications.

1. **Kiavash Satvat**, Rigel Gjomemo and V.N Venkatakrishnan. "Extractor: Extracting Attack Behavior from Threat Reports", 2021 IEEE European Symposium on Security and Privacy (EuroS&P) IEEE, 2021.
2. **Kiavash Satvat**, Maliheh Shirvanian and Nitesh Saxena. "PASSAT: Single Password Authenticated Secret-Shared Intrusion-Tolerant Storage with Server Transparency." arXiv preprint arXiv:2102.13607, 2021.
3. **Kiavash Satvat**, Maliheh Shirvanian, Mahshid Hosseini, and Nitesh Saxena. (2020, March). CREPE: A Privacy-Enhanced Crash Reporting System. In Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy (pp. 295-306).
4. Shrestha, P., Saxena, N., Neupane, A., & **Kiavash Satvat**. (2019, November). CATCHA: When Cats Track Your Movements Online. In International Conference on Information Security Practice and Experience (pp. 172-193). Springer, Cham.
5. Ajaya Neupane, **Kiavash Satvat**, Mahshid Hosseini, Nitesh Saxena, "Brain Hemorrhage: When Brainwaves Leak Sensitive Medical Conditions and Personal Information", 17th International Conference on Privacy, Security and Trust (PST), 2019.
6. Yasser Karim, **Kiavash Satvat**, Mahshid Hosseini, Ragib Hasan, "PurgeMEM: Towards Building A Memory Safe Cloud," In proceedings of IEEE SoutheastCon, 2019.
7. **Kiavash Satvat,** Mahshid Hosseini and Maliheh Shirvanian, "*Camouflaged with Size: A Case Study of Espionage Using Acquirable Single-Board Computers*", 10th International Conference on Networks & Communications, 2018.
8. Ajaya Neupane, **Kiavash Satvat**, Nitesh Saxena, Despina Stavrinos and Haley J. Bishop, "*Do Social Disorders Facilitate Social Engineering? A Case Study of Autism and Phishing Attacks"*, Annual Computer Security Applications (ACSAC), 2018.
9. **Kiavash Satvat** and Nitesh Saxena, "*Crashing Privacy: An Autopsy of a Web Browser's Leaked Crash Reports",* arXiv preprint arXiv:1808.01718 (2018).
10. **Kiavash Satvat,** Matthew Forshaw, Feng Hao and Ehsan Toreini, *"On the Privacy of Private Browsing - A Forensic Approach"*, 8th International Workshop on DPM'14, 2014.
11. **Kiavash Satvat,** Matthew Forshaw, Feng Hao and Ehsan Toreini, *"On the Privacy of Private Browsing",* Journal of Information Security and Applications, Elsevier, 2014.

Awards and Honors.

1. Peter and Deborah Wexler Graduate Student Scholarship, University of Illinois at Chicago, 2018.
2. Member of the Honor Society of Phi Kappa Phi (for the outstanding academic performance), 2017.
3. Member of Golden Key International Honor Society, 2017.
4. BusyBee Award for the most hard-working employee in the ITS division in MTNIrancell, 2015.
5. Passed M.Sc. In computer Security and Resilience with Distinction Award, 2012.
6. The prize winner for the best project, School of Computing Science, NCL, 2012.

Public Services.

Reviewer/Sub reviewer: WPES 2016, IFIPSEC 2017, ESORICS 2017, WPES 2017, WWW 2018, CCS 2018, ISI 2018, NETCOM 2018, ICISS 2018, DPSC2019, DPSC2020.

References are available on request.