Eric Nunes

CONTACT INFORMATION

699 S. Mill Avenue
Arizona State University
Tempe, AZ 85281 USA

Voice: (315) 439-3089
E-mail: **enunes1@asu.edu**
website: **efnunes.github.io**

EDUCATION

Arizona State University, Tempe, Arizona USA

Ph.D. Computer Engineering (GPA: 4.0/4.0), August 2014 - Present

- Dissertation Topic: "Reasoning about Cyber Threat Actors"
- Advisor: Paulo Shakarian
- Ph.D. Candidate - May 2017

Syracuse University, Syracuse, New York USA

M.S. Electrical Engineering, May 2012

University of Mumbai, Mumbai, India

B.S. Electronics and Telecommunication, June 2010

HONORS AND AWARDS

- IEEE/ACM International Symposium on Foundations of Open Source Intelligence and Security Informatics (FOSINT-SI), 2016 **Best Paper Award** for "Argumentation Models for Cyber Attribution".
- "Systems and Methods for Data Driven Malware Task Identification"– Selected for TechConnect 2016 Innovation Showcase.
- Business Category - Most commercial potential winner (Idea: Weight Estimation from Anthropometric features), Medical Center of The Americas Foundation, 2014 ($1000).
- Graduate Scholarship to pursue M.S. at Syracuse University (2010 - 2012)

ACADEMIC EXPERIENCE

Arizona State University, Tempe, Arizona USA
Graduate Research Assistant (CySIS Lab) **August, 2014 - present**
Tools: Python, Spark, PostgreSQL, Prolog, tcpflow.

1. **Proactive Cyber-threat Intelligence**
   - Developed an operational system for cyber threat intelligence gathering from darknet and deepnet sites.
   - The system employs data mining and machine learning techniques to collect information from hacker forum discussions and marketplaces offering products and services focusing on malicious hacking.
   - Currently, this system collects high-quality cyber threat warnings each week. These threat warnings include information on newly developed malware and exploits.
   - Developed data analysis tools to gather meaningful insights from this data to aid security experts for better threat analysis.
   - *Relevant publications:* [B-1, J-1, C-10, C-9, C-7]
2. **Reasoning framework for Cyber-attribution**
   - Proposed a knowledge representation - machine learning (KR-ML) framework to reason about threat actors.

- The framework combines an argumentation model based on DeLP (Defeasible Logic Programming) and machine learning classifiers to evaluate evidence and reason about actors responsible for an attack.
- The framework was evaluated by building a dataset from the capture-the-flag event held at DEFCON – 10 million network attacks.
- Achieved higher precision than previously reported approaches (evaluated on the same dataset) that rely on machine learning classifiers alone—a jump from 37% to 64.5%.
- *Relevant publications:* [B-2, J-3, C-3, C-5, C-6, C-8, BC-1]

3. **Malware task identification**
   - Developed a novel cognitive learning model to identify tasks (e.g. logging keystrokes, recording video, establishing remote access, etc.) that the malware was designed to perform.
   - The proposed model was tested on different malware collections - including mutated and encrypted malware samples.
   - The model outperformed standard machine learning approaches in identifying the tasks.
   - *Relevant publications:* [J-2, C-1, C-2, C-4]

Dartmouth College, Hanover, New Hampshire USA
Research Associate (Brain Engineering Lab) **June, 2012 - July, 2014**
Tools: MATLAB, C++, OpenCV.

- Learning representations for Object recognition and localization from image and video datasets using biologically inspired algorithms.
- Proposed a supervised object recognition algorithm that achieves corresponding classification rates in comparison with standard machine learning approaches - at a fraction of the time and space costs.

SUNY Upstate Medical University, Syracuse, New York USA
Research Assistant **May, 2011 - June, 2012**
Tools: MATLAB, C++.
Registering Multi-Spectral Retinal images to find features and points of interest to estimate the abundance of Oxygen saturation in the blood vessels in retinal images to diagnose retinal disorders.

Patents

- "Systems and Methods for Data Driven Malware Task Identification."
  U.S. Provisional Patent: 62/182,006, Submitted (Non-provisional), 2016.
- "Intelligent darkweb crawling infrastructure for cyber threat intelligence collection."
  U.S. Provisional Patent: 62/409,291, Licensed by CYR3CON, 2016.

Publications

***B** - *Book*, ***J** - *Journal*, ***C** - *Conference*, ***BC** - *Book Chapter*

- [**B-2**] **E. Nunes**, P. Shakarian, G. Simari, A. Ruef "Artificial Intelligence Tools for Cyber Attribution", *Under Preparation*, 2017.
- [**B-1**] J. Robertson, A. Diab, E. Marin, **E. Nunes**, V. Paliath, J. Shakarian, P. Shakarian "Darkweb Cyber Threat Intelligence Mining", Cambridge University Press, 2017.
- [**J-3**] **E. Nunes**, P. Shakarian, G. Simari, A. Ruef "Hybrid Structured Argumentation Models for Cyber Attribution: An Empirical Study on Identifying Threat Actors" *submitted (under review)*, 2017.
- [**J-2**] **E. Nunes**, C. Buto, P. Shakarian, C. Lebiere, S. Bennati, R. Thomson "Cognitively-Inspired Inference for Malware Task Identification" *submitted (under review)*, 2017.

- [**J-1**] J. Robertson, A. Diab, E. Marin, **E. Nunes**, V. Paliath, J. Shakarian, P. Shakarian "Darknet Mining and Game Theory for Enhanced Cyber Threat Intelligence" The Cyber Defense Review, 2016.
- [**C-10**] M. Almukaynizi, A. Grimm, **E. Nunes**, J. Shakarian, P. Shakarian "Predicting Cyber Threats through User Connectivity in Darkweb and Deepweb Forums" ACM Computational Social Science (CSS), 2017.
- [**C-9**] M. Almukaynizi, **E. Nunes**, K. Dharaiya, M. Senguttuvan, J. Shakarian, P. Shakarian "Proactive Identification of Exploits in the Wild Through Vulnerability Mentions Online" International Conference on Cyber Conflict (CyCon-US), 2017.
- [**C-8**] A. Ruef, **E. Nunes**, G. Simari, P. Shakarian "Measuring Cyber Attribution In Games" IEEE APWG Symposium on Electronic Crime Research (eCrime), 2017.
- [**C-7**] **E. Nunes**, A. Diab, A. Gunn, E. Marin, V. Mishra, V. Paliath, J. Robertson, J. Shakarian, A. Thart, P. Shakarian "Darknet and Deepnet Mining for Proactive Cybersecurity Threat Intelligence" IEEE Conference on Intelligence and Security Informatics (ISI), 2016.
- [**C-6**] **E. Nunes**, P. Shakarian, G. Simari, A. Ruef "Argumentation Models for Cyber Attribution" IEEE/ACM International Symposium on Foundations of Open Source Intelligence and Security Informatics (FOSINT-SI), 2016 – **Best Paper Award**.
- [**C-5**] **E. Nunes**, P. Shakarian, G. Simari "Toward Argumentation-Based Cyber Attribution" AAAI Workshop on Artificial Intelligence and Cyber security (AICS), 2016.
- [**BC-1**] **E. Nunes**, N. Kulkarni, P. Shakarian, A Ruef, J. Little "Cyber-Deception and Attribution in Capture-the-Flag Exercises" (extended version) in Cyber Deception: Building the Scientific Foundation (editors: S. Jajodia, V.S. Subrahmanian, V. Swarup, C. Wang) Springer, 2016.
- [**C-4**] **E. Nunes**, C. Buto, P. Shakarian, C. Lebiere, S. Bennati, R. Thomson, H. Jaenisch "Malware Task Identification: A Data Driven Approach" IEEE/ACM International Symposium on Foundations of Open Source Intelligence and Security Informatics (FOSINT-SI), 2015.
- [**C-3**] **E. Nunes**, N. Kulkarni, P. Shakarian, A Ruef, J. Little "Cyber-Deception and Attribution in Capture-the-Flag Exercises" IEEE/ACM International Symposium on Foundations of Open Source Intelligence and Security Informatics (FOSINT-SI), 2015.
- [**C-2**] C. Lebiere, S. Bennati, R. Thomson, P. Shakarian, **E. Nunes** "Functional Cognitive Models of Malware Identification" 13th International Conference on Cognitive Modeling (ICCM), 2015.
- [**C-1**] R. Thomson, C. Lebiere, S. Bennati, P. Shakarian, **E. Nunes** "Malware Identification Using Cognitively-Inspired Inference" 24th Conference on Behavior Representation in Modeling and Simulation (BRiMS), 2015.

Invited talks

- **Cyber-Deception and Attribution in Capture-the-Flag Exercises**
  The International Information System Security Certification Consortium (ISC2), Phoenix chapter, October, 2016.
  Army Research Office's Cyber Deception Workshop, Washington, July 2015.
- **Automatic identification of malware tasks**
  Cactus-Con, Tempe, Arizona, March, 2015.

Professional Experience

Data Scientist, **Cyber Reconnaissance Inc. (CYR3CON)** **August, 2016 - Present**

- Developed data analysis tools for threat intelligence to draw meaningful insights from data mined from darknet and deepnet markets /forums (including detection of 0-day exploits, identifying exploits targeting specific vulnerabilities, trend analytics in cyber threat landscape etc.) for customer specific requirements. In particular, built learning models for predicting likelihood of exploitation of a vulnerability, named-entity recognition using RNN/LSTM seq2seq models.

- Consulted for SiteLock to improve their malicious web script detection model using machine learning techniques to make it more robust and less susceptible to false alarms

Security Automation Intern (Data Science), PayPal **May, 2017 - August, 2017**

- Analyzed user login activity using Akamai logs and enriched it with other data feeds such as threat intelligence, merchant data, credential dumps.
- Implemented operational Anomaly detection models to detect Account Takeover (ATO) attacks to raise alerts for automated mitigation.
- Visualized ATO attacks in real time on a dashboard in Splunk.

Research Consultant, CYR3CON (Client: SiteLock) **June 2016 - August 2016**

- Analyzed large dataset of malicious web scripts (PHP/HTML) to generate features indicative of malicious activity.
- Developed classification models to classify web scripts as malicious or not using the generated features in Python.
- Visualized the performance of the trained model overtime and analyzed the classification errors for further improvement through Plotly dashboard.
- **Achieved malicious web script detection rate of >90%.**

Technical Skills

- **Machine Learning:** Classification, regression, clustering, anomaly detection, feature engineering, online learning, Experience with deep learning.
- **Programming Languages:** Python, MATLAB, C++, Prolog, HTML, LaTeX. Familiar with C, PHP, LISP, R.
- **Libraries:** scikit-learn, Weka, Pandas, OpenCV, Theano, Caffe.
- **Databases:** SQL, PostgreSQL, MYSQL, Familiar with MongoDB.
- **Operating System:** Windows, Linux, Mac OS X.
- **Tools:** Eclipse, MS Visual Studio, PyCharm.
- **Big Data and Cloud:** Splunk, Familiar with Big Data Processing Platforms: Hadoop, Spark and Cloud tools: Amazon S3.

Press

- Hacking the hackers, ASU now: Access, Excellence, Impact. September 7, 2016.
- Arizona State Builds Darknet Mining Model, Finds 16 Zero Days, Cisco Continuum. August 18, 2016.
- Over 300 new cyber threats pop up on underground markets each week, HelpNetSecurity. August 10, 2016.
- Machine Learning Goes Dark And Deep To Find Zero-Day Exploits Before Day Zero, Forbes. August 8, 2016.
- Machine-Learning Algorithm Combs the Darknet for Zero Day Exploits, and Finds Them, MIT Tech Review. August 5, 2016. ACM TechNews. August 5, 2016.

Service

Journal Reviewer:

- Social Network Analysis and Mining (SNAM), 2017.
- Sustainability, 2017.

Conference Reviewer:

- ACM SIGKDD Conferences on Knowledge Discovery and Data Mining (KDD), 2015, 2016.
- AAAI Conference on Artificial Intelligence (AAAI), 2016.
- International Conference on Autonomous Agents and Multiagent Systems, 2015.

References

Available on request