Shoufu Luo

luoshoufu@gmail.com

Austin, TX
Revised on 2018.01.08

Work Experience

Security Researcher, Data Science at Trend Micro Inc., Austin, TX, 07/2016 -
Research in data-driven intelligent solutions for network security, Python and C/C++

- Led setup infrastructure for data collecting and cleaning, large-scale log analysis;
- Developed statistical models for detecting exploit kits with low false positives, including a FPGA-assisted implementation for real time inline blocking (patent pending);
- Beaconing detection using periodogram analysis and Gaussian Mixture Model, and designed a path finding algorithm for a noise-resilient and more reliable approach (patent pending) using Spark, MariaDB, Vertica etc.

Software Engineer (Intern) at Citrix Systems Inc., Jersey City, NJ, 2013/2015
Online Conferencing Audio Platform, C++ and JavaScript

- Initiated unit tests for audio platform using Google Test framework and developed a flexible SIP testing framework for unit testing of the platform (2013 summer);
- Re-factored components of conference management for automated unit testing, including using boost state machine to re-implement the conference flow and designing an adapter for a-synchronization interaction with 3rd-party library (2015 summer);

Security Engineer (Intern) at E8 Security Inc., Palo Alto, CA, 2014 Summer
Threat Modeling/Data Science Team, Cybersecurity on Big Data, Python, Pig, Hadoop

- Time-series security data analysis and threats modeling using learning techniques; Contributed to security assessment report for customers;
- Prototype a user-agent anomaly detector using *frequent itemsets*, as a component to E8 core platform

Sr. Software Engineer at Wyse (DELL) Technology Inc., Beijing, 2005-2011
System Security, software development for a BSD-based event-driven embedded OS, C/C++

- Maintained overall security of the embedded system, integrating and maintaining 3rd-party SSL/crypto libraries, and developing security features; supervised several projects related to security, e.g. agent for Citrix CSG;
- Implemented power management to reduce half power consumption; Led the wireless project and successfully delivered four device drivers for 802.11g/n, a native WPA/2 client and 802.1X for wired;
- Troubleshooting in memory management, TCP/IP stack and process scheduling, video and network device drivers, and remote desktop applications, RDP/ICA/VNC etc.

Technical Skills

- Expert in C/C++, proficient in Python and Java, familiar with SQL, JavaScript, Bash, Objective-C
- Proficient in machine learning algorithms such as linear regression, decision trees, SVM, K-Means, PCA, GMM, neural networks etc.; familiar with python machine learning packages and pySpark etc.; hand on experience in natural language processing; working knowledge in big data techniques, such as Spark, Hadoop, basic pig programming etc.
- Proficient in IDS/IPS, firewalls, anti-virus, PKI, network application protocols including HTTP/S, FTP, TCP/IP, SIP, SSL, EAP, and routing protocols like BGP, RIP, OSPF, etc.; good knowledge in cryptography foundations, system security, attacks and web security risks; familiar with security tools like Bro, Tcpdump, Snort, Nmap etc.
- Good knowledge in OS kernel and virtualization techniques; advanced user of Linux, OpenBSD and Windows 2003; proficient in Cisco networks (CCNA-equivalent); working knowledge in proxies, load balancers, cloud computing; an amateur developer of Php and iOS applications; brief experience in web application development using J2EE/Struts/JDBC, AngularJS/Php/MongoDB

Education

Ph.D. in Computer Science, **City University of New York**, U.S. (In progress)

- Research interests: system security, machine learning-based network defense systems

Master in Computer Science, **Stevens Institute of Technology**, U.S., 2014

- Gpa: 3.94/4.0 | Ph.D. Candidate | System Security | Advisor: Dr. Sven Dietrich
- Thesis: *"Characterizing Encrypted Botnet C&C using Entropy Measures"*

Bachelor of Science in Administration (Management of Information Systems)

- Gpa: 88/100 | **Beijing Information Technology Institute**, CHINA, 2005
- Thesis: *"Role-based Access Control System for J2EE Applications"*

Academic Experience

Research Assistant at City University of New York, 2014-2016
Botnet Detection, Targeted Attacks, System Security

- Applied machine learning, data mining and artificial intelligence for network security

Research Assistant at Stevens Institute of Technology, Hoboken, 2011-2014
Botnet Detection and Malware Analysis, System Security

- Malware analysis and Botnet detection; security analysis of IoT devices

Adjunct Lecturer at John Jay College of Criminal Justice, CUNY, 2014-2016

- Teaching CSci 375 Operating Systems, CSci 376 Database Systems and Data mining

Reviewer, the 17th European Symposium on Research in Computer Security, 2012
Reviewer, the 28th Annual Computer Security Applications Conference (ACSAC), 2012
Reviewer, the 10th International Conference, DIMVA 2013

Scholarship & Awards

2014-2015	Science Fellowship at The Graduate Center, CUNY ($50,270)
2014-2019	Five-year Tuition Fellowship at The Graduate Center, CUNY
May 2013	Student Travel Grant for IEEE Symposium on Security and Privacy, CA

Publications & Patents

- **Fingerprinting Cryptographic Protocols with Key Exchange using an Entropy Measure**, Shoufu Luo and Sven Dietrich, https://arxiv.org/abs/1712.05908
- **Examining Customer Responses to Fake Online Reviews: The Role of Suspicion and Product Knowledge**, Jie Ren, Pinar Ozturk and Shoufu Luo, WeB 2016, Volume 296 of the Lecture Notes in Business Information Processing (LNBIP)
- **Using global and local feature extraction contexts for machine learning model application on real-time network flow data**, Josiah Hagen, Jonathan Andersson, Shoufu Luo, Brandon Niemczyk, Leslie Zsohar, Craig Botkin, Pete, Andriukaitis, US Patent (Pending)
- **C&C Beaconing Detection using Path Finding Algorithm**, Shoufu Luo, Jonathan Andersson, Josiah Hagen, US Patent (Pending)