Kulsoom Abdullah, PhD

US Citizen kulsoom@gatech.edu
https://www.linkedin.com/in/kulsoomabdullah - https://github.com/kulsoom-abdullah - http://kulsoom.net/

INTERESTS

Applied Machine Learning, Information Networks & Security, Security Visualization, HCI, Applied Humanitarian Research

SKILLS

Computer Languages & Tools: Python (Numpy/Scipy/Matplotlib/Pandas, Jupyter/IPython, Hadoop/MapReduce, Sklearn), Spark (PySpark and Scala), Hive SQL, GitHub, SQLITE, Java, Wiki, JOGL (Java OpenGL extensions), HTML, C, Hping/Tcl, Sockets LaTeX 2e. Proficiency in: R, D3.js
Software: VIM, Tableau, Wireshark, Snort IDS, Qualnet, OPNET
Foreign Languages: Pashto (basic proficiency), Urdu & Arabic (limited proficiency)

SELECTED EXPERIENCE

Data Scientist, ADP Ventures — Atlanta, GA — March 2016 - Current

- Part of the small team leading and pioneering the Real Income product - aggregating and anonymizing ADP's payroll data of 30 million US employees.
    - Collaborated with peers, Sr Leadership and product owners to deliver initial products and iterated as needed with an aggressive sales team, resulting with reprioritization of deliverables. Diligently worked to support challenging goals.
    - Flexibly worked with new technical owners to continue to refine the product based on updated requirements.
    - Continuing to use ADP and external data, task sizing coding standards and other research to recommend views that will benefit the product and ADP Open Data Science.
- Supporting ADP Open Data science initiatives by researching and prototyping projects, questioning existing processes, updating and documenting findings, and educating peers, interns, business owners and third party vendors.

Mentor, Anidata — Atlanta, GA — Jan 2016 - Current

- Mentor future data scientists by guiding them on data projects that improve and benefit the community.

Research Scientist, Damballa, Inc. — Atlanta, GA — Jun 2014-Aug 2015

- Analyzed malware botnet command & control (c2) domain and malware network traffic using machine learning of big data amounts, domain attribution and classification to identify those that are malicious.
- Examined client query behavior by independently designing and coding experiments to test hypothesis. Used the results to come up with statistical features to classify clients that are following malicious domains specific to malware campaigns deployed by botnet operators.

Visiting Scholar, Georgia Tech - CAP Group — Atlanta, GA — July 2009-Sep 2015

Visualizing Domain Reputation & Attribution — Feb 2014-May 2014

- Leveraged DNS agility, used by malware command-and-control (C2) system, for reputation & attribution. Clustered domains on their network features and relationships, then visualize the most important relationships. A security company's passive DNS database was used to retrieve historic domain and IP information, sci-kit learn to perform clustering. My contributions involved using python, sqlite, querying a whois database to extract part of the features, and d3.js (JSON input) for the visualization.

Parallel 3D Coordinate System — Jan 2013**-**Apr 2014

- Research & development in network security stereoscopic 3D visualization, machine learning for new/inexperienced users (command/navigation recommendation based on expert users), and user evaluation. HPING/TCL to simulate network traffic activity using Wireshark to capture the traffic data, then filtered background & "noisy" packet data. The final data was test input for the visualization tool.
  More details in the publications.

Consultant, Georgia State University — Atlanta, GA — Dec 2012-Apr 2013

- Research in the Internet's role in Commercial Sexual Exploitation of Minors (CSEM), mostly self-supported. Collaborated with Dr. Mary Finn at Georgia State University
- Educated & trained investigators & research assistants about the current communication technologies & how they interface, assist with technology content-related questions in qualitative interview, assist with the collection & analysis of web data.
- Scraped web forum discussion data HTML pages of over one year from 3 boards. Tokenized each post & parameters (parent & child posts, userid, subject, date, time, message) from each HTML page using Python into MongoDB.
- Performed tf-idf using Sci-kit learn & presented top tfidf value words on all posts for all words. E.g. Atlanta forum was 39,436 posts by 113,214 unique words. Used cluster analysis for classification results, along with professor's feedback, to help reduce the dictionary.

Engineer III, Scientific Research Corporation — Atlanta, GA — Jan 2008-Jun 2009

- **Software Defined Radios**: Assisted in developing an adaptive power control algorithm in Qualnet, validating a thorough network testing plan & tested SRC's revised Mobile Route (MANET software).
- **AMF JTRS Router Trade Study**: Researched RFCs & COTS router specifications of the top router vendors, & finalized router choice in the AMF JTRS system.

- **JTRS Training Network Analysis**: Assessed the network loading for FCS training & potential for JTRS radios & waveforms to carry this load. Researched current methods to mathematically analyze unicast & geocast traffic for the system & developed equations to calculate the load.
- **SPAWAR SATCOM Analysis**: Wrote functions generating VTRPE input files for varying frequencies, wind speed, sea conditions, for multiple prime number seeds. Analyzed path loss vs. distance, difference & average for varying altitudes to derive a general channel model to test Reliable Link Protocol (RLP) performance over the sea.

Graduate Research Assistant, Georgia Tech Atlanta, GA Aug 2001-May 2006

- Researched topics in wireless communications, network security, & visualization.
  - Information visualization, designing GUIs, & performing user study surveys.
    - Dealt with general visualization & HCI issues of network security data – massive amount of data, scaling 65535 TCP & UDP ports & 4 billion possible IPv4 addresses, time scales for various activity detection.
    - Visualized IDS data output (anomalous activity alerts) from the IDS s/w used on the Georgia Tech campus based on the security analysts tasks, goals & challenges (Java OpenGL).
  - Wireless LAN (802.11) performance & security issues.
  - General network security topics: scanning, virus & worm propagation, intrusion detection Honeynet/Honeypots, network monitoring.

EDUCATION

Georgia Institute of Technology Atlanta, Georgia

PhD in Electrical & Computer Engineering Spring 2006; GPA 3.61/4.0

- Dissertation title: "Scaling and Visualizing Network Data to Facilitate in Intrusion Detection Tasks"
- Developed two systems that visualize packet header & IDS data. Visualization improved the efficiency at which attacks & anomalies are identified by the network security analyst.

Masters of Science in Electrical Engineering May 2000; GPA 3.57/4.0

University of Central Florida Orlando, Florida

Bachelors of Science in Computer Engineering May 1998; GPA 3.8/4.0

SELECTED PUBLICATIONS (12 TOTAL)

T. Nunnally, **K. Abdullah**, A. S. Uluagac, J. A. Copeland & R. A. Beyah, "InterSec: An Interaction System for Network Security Applications", *IEEE Symposium on Information Visualization's Workshop on Visualization for Computer Security (VizSEC)* 2014. http://bit.ly/1P58Hpd

T. Nunnally, **K. Abdullah**, A. S. Uluagac, & R. A. Beyah, "NAVSEC: A Recommender System for 3D Network Security Visualizations", To appear in the *IEEE Symposium on Information Visualization's Workshop on Visualization for Computer Security (VizSEC)*, Atlanta, GA, USA, October 2013. http://bit.ly/1PwX6cD

T. Nunnally, P. Chi, **K. Abdullah**, A. S. Uluagac, & R. A. Beyah, "P3D: A Parallel 3D Coordinate System for Advanced Network Scans", IEEE International Conference on Communications (ICC), Budapest, Hungary, September 2013. http://bit.ly/1Snre0m

K. Abdullah, G. Conti & E. Sobiesk. "Self-monitoring of Web-based Information Disclosure;" Workshop on Privacy in the Electronic Society (WPES); October 2007. http://bit.ly/1WfUB3L Cited in: G. Conti; Googling Security, Addison Wesley; November 2008. http://amzn.to/1NcestF

K. Abdullah & J. A. Copeland. "High alarm count issues in IDS RainStorm;" VizSec; ACM Conference on Computer and Communications Security's Workshop on Visualization and Data Mining for Computer Security (VizSEC); November 2006. http://bit.ly/1KioKbz

G. Conti, **K. Abdullah**, J. Grizzard, J. Stasko, J. A. Copeland, M. Ahamad, H. Owen, & C. Lee. *"Countering Security Analyst and Network Administrator Overload Through Alert and Packet Visualization;"* Special Issue of IEEE CG&A Visualization journal for Cyber Security, March/April 2006. http://bit.ly/1ZqpgeD

K. Abdullah, C. Lee, G. Conti, J. Copeland & J. Stasko; "*IDS RainStorm: Visualizing IDS Alarms*;" IEEE Symposium on Information Visualization's Workshop on Visualization for Computer Security (VizSEC); October 2005. http://bit.ly/1n1Heb8- Cited in: G. Conti; Security Data Visualization, No Starch Press; September 2007. http://amzn.to/1UVZPjY

BIO SUMMARY

Kulsoom Abdullah is a Pakistani-American competitive Olympic Weightlifter and was Crossfit [http://bit.ly/1n1SrIA] Level I certified. She attended the University of Central Florida and received her doctorate in electrical/computer engineering at the Georgia Institute of Technology.

Her website, LiftingCovered.com and Facebook page [http://on.fb.me/205IeJH] documents her experiences weightlifting in an effort to compete at U.S. national competitions. She advocated to compete in clothing that adheres to religious codes, opening the door for women from cultures around the world to compete and move beyond preconceived notions of gender, race, and religion. Her athletic feats and determination culminated in an invitation to deliver remarks following Secretary of State Hillary Clinton [http://bit.ly/1JQ5vLK] at the U.S. State Department's Eid ul Fitr reception 2011. She represented Pakistan as the first female at the international level to compete wearing hijab at the 2011 World Weightlifting Championships. She resides in Atlanta, GA and is currently taking a break from major competitions but continues to train. She continues the cycle of empowerment by helping others and supporting relevant causes. In 2014 she was one of four women in The Pakistan Four [http://on.fb.me/1Nckvyg] short documentary - redefining what it means to be a Pakistani Muslim female, one of the recipients of the Georgia Influential Muslim Award and spoke on a panel at the Religion Newswriters Association. In 2015, she was also presented in a 2015 calendar of female South Asian American role models, "Saris to Suits Empowered", and she was on Team Shirzanan [http://on.fb.me/1PwYjRp] (Persian for "female heroes") as a spokesperson and role model. The team participated at RAGBRAI 2015 (The Register's Annual Bike Ride Across Iowa) to celebrate our Right to Ride.