Qian Cui

cuibuaa.github.io / cuibuaa@gmail.com / +1 (613) 322-0629 / Ottawa, ON, Canada

EDUCATION

2016/01 - Now
PhD of Computer Science
University of Ottawa

2007/09 - 2009/12
Master of Computer Science
Beihang University

2003/09 - 2007/07
Bachelor of Computer Science
Beihang University

SKILL

Python, C, Java, Verilog
Linux, Windows
Mongodb, MySQL

TOOL

Tensorflow, Sklearn
Pandas, Numpy

HONORS

Outstanding Research Project
Rewarded by IBM Canada
University of Ottawa, 2017

Excellent Master's Thesis
Beihang University, 2010

PATENTS

2015
CN 102708012 B (*in Chinese*)
Translated by Google

2014
CN 103678206 A (*in Chinese*)
Translated by Google

2012
CN 102361460 A (*in Chinese*)
Translated by Google

2011
CN 101969358 A (*in Chinese*)
Translated by Google

RESEARCH

2017 →Now **Phishing Attack Detection with Machine Learning and Cognitive Computing**
The University of Ottawa

This research is to automate the detection of not only the known attacks, but also unknown attacks. Apply the machine learning algorithm to extract phishing signature, and make evolutions on the system by using cognitive computing to predict possible attack variation in future

Contribution

- Applied a CNN framework to identify phishing attacks only relying on screenshot, and achieved 86.7% accuracy with only 1% false positive.
- Proposed a new clustering algorithm based on cognitive computing, improved 10% performance of previous research (published paper in WWW'17), and also gave a short talk "Phishing Clustering Based on MST" in the CASCON 2017 conference.

2016 →2017 **Monitoring and Behavior Analysis of Phishing Attacks** The University of Ottawa

The goal of this research is to create a data collecting and monitoring system to track phishing attacks. Apply the clustering and similarity comparison techniques to explore the correlation between phishing attacks, and find the attackers' behavior pattern and common attacking method

Contribution

- Developed a large-scale phishing data collecting and monitoring system, which is gathering the relevant information behind the phishing attack, including geographic info, network info (IP history, domain history, whois history), behavior info (redirection path, attack fingerprint), 10,000+ lines python code. Up to Jan, 2018, more than 60,000 phishing attacks with refined profile were collected.
- First published paper (on WWW'17) uses the similarity comparison to detect phishing attacks, covering more than 90% attacks
- Generated a phishing connection graph which disclosed the small group of community hidden in a mass of phishing attacks
- Developed a code similarity comparison system to analyze the phishers' programming style, and outlined attackers' programming fingerprint.

WORK EXPERIENCE

2013 →2015 **Samsung Electronics** Beijing, China
Senior Embedded Engineer

- Designed Linux wireless driver and software architecture of firmware for Samsung high-speed Wifi chip, and successfully solved bottleneck of data transfer, increased 150% performance Links for the project

2010 →2013 **Space Star Co. Ltd** Beijing, China
Parallel Computing FPGA Engineer (IC)

- Designed parallel encode/decode modules and increased 400% performance (two patents)
- Developed high-speed transfer circuit board applied in multiple core products, and contributed more than 200,000$ annual benefit

PUBLICATION

Tracking Phishing Attacks Over Time
Qian Cui, Guy-Vincent Jourdan, Gregor v. Bochmann, Russell Couturier, Iosif-Viorel Onut.
26th International World Wide Web Conference (WWW '17), Perth, 2017