Weilin Xu 许伟林

xuweilin@virginia.edu

https://xuweilin.org/

Education

2013.8 – present	*University of Virginia,* U.S. Ph.D. student in Computer Science. Co-Advisors: Prof. David Evans, Prof. Yanjun (Jane) Qi
2008.9 – 2012.6	*Beijing University of Posts and Telecommunications* (BUPT), China B.E, Computer Science and Technology (Rank: 27/316)

Positions

2014.5 – present	Research Assistant in Security Research Group and Machine Learning Group, UVa
Fall 2016	TA, CS6316: Machine Learning, Prof. Yanjun Qi, University of Virginia
Spring 2014	TA, CS4414: Operating Systems, Prof. David Evans, University of Virginia
Fall 2013	TA, CS4414: Operating Systems, Prof. David Evans, University of Virginia
2012.7 – 2013.8	Engineer, Network and Information Security Lab, Tsinghua University

Research Interests

- Adversarial Machine Learning

Research Experience

2014.5 – present   Security Research Group and Machine Learning Group, UVa   **Research Assistant**

- Leading research on Feature Squeezing and Genetic Evasion.
- Project website: http://EvadeML.org

2012.7 – 2013.8   Network and Information Security Lab, Tsinghua University.   **Engineer**

Distributed Honeynet Project

- Leaded a team constructing a nationwide distributed honeynet system, MongoDB database, HPfeeds publish/subscribe protocol, SNMP and Django.
- Honeypots included Dionaea, Kippo, Glastopf and 6Guard.

2012.5 – 2012.8   Google Summer of Code 2012, Google, Inc.   **Developer**

The Honeynet Project   Mentor: Ryan W. Smith

- Designed and developed 6Guard, an efficient and economic IPv6 attack detector.
- Based on signature and honeypot techniques, mainly aiming at THC-IPv6 and Nmap.
- 6Guard was deployed in CNGI-CERNET2 to detect and capture informal traffics.
- The code repository is at https://github.com/mzweilin/ipv6-attack-detector/.

2011.5 - 2011.8   Google Summer of Code 2011, Google, Inc.   **IPv6 Expert**

Nmap Security Scanner Project   Mentor: David Fifield

- Worked as an IPv6 Expert (research oriented) aiming at improving IPv6 support of Nmap, and developing new host discovery methods on IPv6 network.
- Made contributions to some essential IPv6-related features, such as IPv6 raw packet scans, IPv6 host discovery, and advanced IPv6 link-local host discovery.
- The code repository is at https://svn.nmap.org/nmap/.

2010.4 - 2011.4   Innovation Laboratory for Students, BUPT   **Team Leader**
IPv6-to-IPv6 NAT Router Project:
- Founded NAPT66, an open source project of stateful IPv6-to-IPv6 NAT, implemented on Linux kernel.
- The code repository is at http://code.google.com/p/napt66/.
- Invented '802.1X Relay', a client-side method for supporting various proprietary 802.1X-based protocols.
- Developed an embedded IPv6/IPv4 Dual Stack NAT router based on the OpenWrt router OS.
- A project video is available at http://v.youku.com/v_show/id_XMjY4NTAwMTc2.html.

2009.10 - 2010.1   State Key Lab of Networking and Switching, BUPT   **Research Assistant**
Transparent Data Encryption on Android:
- Evaluated related works, such as the FiST maintained by Prof. Zadok of Stony Brook University.
- Invented a new technique based on Linux Kernel VFS layer and implemented a demo.

Publications

- **Weilin Xu**, David Evans, Yanjun Qi. *Feature Squeezing: Detecting Adversarial Examples in Deep Neural Networks*. To appear in Network and Distributed System Security Symposium (NDSS), 2018.
- **Weilin Xu**, Yanjun Qi, David Evans. *Automatically Evading Classifiers: A Case Study on PDF Malware Classifiers.* In Network and Distributed System Security Symposium (NDSS), 2016.

Patents

- Guanglin Xu, **Weilin Xu**, Wushao Wen, Xiaojing Xie. *Method based on packet forwarding for supporting proprietary 802.1X-based protocols in NAT router*, Patent No. CN 201010518735.5.

Honors

- First Prize of Creativity Award of BUPT, 2011
  (The highest academic award for graduates and undergraduates in BUPT.)
- National Scholarship for Encouragement of China, 2010, 2011
  (The highest award for outstanding and inspirational undergraduates.)
- Third-class College Scholarship of BUPT, 2009

Academic Services

- External Reviewer of IEEE S&P (Oakland) 2015, 2017
- External Reviewer of USENIX Security 2016
- External Reviewer of AsiaCCS 2016
- External Reviewer of NDSS 2017
- External Reviewer of CCS 2017
- Program Committee of NIPS Machine Learning and Computer Security Workshop (MLSec) 2017

References

Professor David Evans, Ph.D.   evans@virginia.edu
Computer Science department, University of Virginia
Charlottesville, VA 22904

Assistant Professor Yanjun (Jane) Qi, Ph.D.   yanjun@virginia.edu
Computer Science department, University of Virginia
Charlottesville, VA 22904