YUCHEN ZHOU

yz8ra@virginia.edu

5505 Seminary Rd #418, Falls Church, VA 22041 434-466-3448 (mobile)

Homepage: http://www.yuchenzhou.info/

EDUCATION

Ph.D. in Computer Engineering **University of Virginia,** Charlottesville, VA

GPA: 3.98 *Aug 2009-May 2015*

Relevant courses: Design and Analysis of Algorithms, Programming Language, Operating Systems, Theory of Computation, Computer Architecture, Computer Security, Probability and Stochastic Process, Game theory.

B.Eng., Department of Electronic and Information Engineering **Tsinghua University**, Beijing, China

GPA: 82.6/100 *Aug 2005-Jul 2009*

Relevant courses: Digital/Analog/RF circuit design; calculus, linear algebra, stochastic process; signal processing, communication theory, computer networks; Data structure, C++ programming, etc.

RESEARCH EXPERIENCE

Security Researcher *Aug 2009-Present*

Internet Security Research Group Palo Alto Networks, Santa Clara, CA

- Since joining Palo Alto Networks as a researcher I participated in various projects involving detecting malicious domain, URL, IP, JavaScript, and various other web-based threats. My main focus is on building a browser honeypot to analyze malicious website behavior and capture potential threat before the harm is widespread. I work with my supervisor Dr. Wei Xu.

Graduate Research Assistant *Aug 2009-Present*

Security research group, Department of Computer Science University of Virginia, Charlottesville, VA

- Working with my advisor Prof. David Evans, I have done various research projects on improving the security, privacy and integrity of third-party service integrations. These projects have resulted in multiple publications and posters which I presented at various major security conferences and industry research centers.

Research Intern *May 2012-Aug 2012*

Internet Services Research Center (ISRC) Microsoft Research, Redmond, WA

- Under the supervision of Dr. Shuo Chen, I did a security field study of Single Sign-On service and built a system that automatically checks for hidden assumptions in the developer guide. Our work was published at USENIX Security Symposium and I presented the work in August of 2013.

Undergraduate Research Assistant *Sep 2008-May 2009*

Center for Intelligent Image and Document Information Processing Tsinghua University, Beijing, China

- Under the guidance of Prof. Shengjin Wang, I studied various feature extraction/classification techniques and applied them to eye detection algorithm to assist drowsy drivers.

Research Intern *Jul 2008-Aug 2008*

Center of Information Security and Cryptography, Department of Computer Science Hong Kong University, China

- I led a three-people team and completed the motion detection module on a multi-core DSP board in parallel fashion. Our work was published at a major security magazine in China.

Student Research Trainee *Mar 2008-July 2008*

Lab of New Generation Network Technology and Application Tsinghua University, Beijing, China

- I participated in the optional student research training (SRT) program in my third year undergraduate and developed a search engine that focuses on removing duplicate query result. My work was published in the Journal of Information and Computational Science.

PUBLICATIONS

Understanding and Monitoring Embedded Web Scripts, **Yuchen Zhou** and David Evans, in proceedings of the 35th IEEE Symposium on Security and Privacy (Oakland), May 2015.
Project homepage: http://scriptinspector.org/

SSOScan: Automated Testing of Web Applications for Single Sign-On Vulnerabilities, **Yuchen Zhou** and David Evans, in proceedings of the 23rd USENIX Security Symposium, Aug, 2014.
Project homepage: http://yuchenzhou.info/research_ssoscan

Explicating SDKs: Uncovering Assumptions Underlying Secure Authentication and Authorization, **Rui Wang**, **Yuchen Zhou (co-first authors)**, Shuo Chen, Shaz Qadeer, David Evans and Yuri Gurevich, in proceedings of the 22nd USENIX Security Symposium, Aug, 2013.
Project homepage: http://yuchenzhou.info/research_explication

Protecting Private Web Content from Embedded Scripts, **Yuchen Zhou** and David Evans, in proceedings of the 16th European Symposium on Research in Computer Security (ESORICS), Sep, 2011.
Project homepage: http://yuchenzhou.info/research_esorics

Why Aren't HTTP-only Cookies more widely deployed, **Yuchen Zhou** and David Evans, appeared in the 4th workshop on Web 2.0 Security and Privacy, IEEE Security and Privacy Symposium, Mar, 2010.

Improved Fuzzy Set Information Retrieval Approach on duplicate webpage detection, **Yuchen Zhou**, Zuoda Liu, Beixing Deng, Xing Li, in proceedings of Journal of Information and Computational Science, May, 2009.

Implementation of motion detection algorithm on multi data lane DSP processor, **Yuchen Zhou**, Meilin Wang, Zheng Zhang, 2008.11, ISSN1673-7873,appeared in the China Security & Protection magazine, Sep, 2008.

PATENTS

Identifying Implicit Assumptions Associated with a Software Product, with Microsoft Research, approved in Sept 2014.

POSTERS

RedactDOM: Preventing Sensitive Data Leaking through Embedded Scripts, Longze Chen, **Yuchen Zhou** and David Evans, presented at the poster session of the 34th IEEE Symposium on Security and Privacy, May, 2013.
Unifying Data Policies across the Client and Server, Jonathan Burket, Jenny Cha, Austin DeVinney, Casey Mihaloew, **Yuchen Zhou**, David Evans, presented at the poster session of the 20th USENIX Security Symposium, Aug, 2011.

GRANTS AND PROPOSALS

Securing Single Sign-On Applications, Google Research Grant. PI: Prof. David Evans, Total amount: $59,000, Aug 2013.

- (**Primary Author**) I proposed to extend the explication approach for third-party service SDKs to apply to additional platforms and services, and build automated vulnerability scanners for integrated applications.

Automated Security Testing for Applications Integrating Third-Party Services, NSF Grant. PI: Prof. David Evans, Total amount: $500,000, Aug 2014.

- (**Primary Author**) I presented the automated vulnerability scanning results for single sign-on integrations, and proposed to further improve the scanning success rate and speed by server- and client-side optimizations.

AWARDS

Louis T. Rader Research Award, School of Engineering and Applied Science, University of Virginia. May, 2014

Student Travel Grant, USENIX Security Symposium. Aug, 2013

ACADEMIC SERVICES

- Program committee for EISIC 2015, ASIACCS 2016;
- External Reviewers for
  - IEEE Security & Privacy (Oakland), 2012, 2013, 2015
  - USENIX Security Symposium, 2011,2012,2013,2014,2015
  - Network and Distributed System Security Symposium (NDSS), 2011, 2012, 2016
  - ACM Conference on Computer and Communication Security (CCS), 2015
  - Annual Computer Security Applications Conference (ACSAC), 2015
  - USENIX Security Symposium, workshop on Cyber Security Experimentation and Test (CSET), 2015
  - International Conference on Distributed Computing and Networking (ICDCN), 2015

IMPORTANT IMPLEMENTATIONS (sorted in reverse chronological order)

- Modified Mozilla Firefox (C/C++/JavaScript) to support security-critical API call interceptions and policy checking functionality.
- Implemented an automated vulnerability scanner (JavaScript/Ruby) for web applications powered with Facebook Single Sign-On.
- Studied and modeled Facebook and Microsoft Single Sign-On systems (C++/PHP/JavaScript/Boogie) to discover implicit security-critical assumptions, common developer pitfalls and SDK vulnerabilities.
- Modified Google Chromium Browser (C/C++) to enable fine-grained access control policy enforcement on DOM APIs and JavaScript execution contexts.
- Designed and implemented 2-Player West Virginia bot/3-player Texas Hold'em robot (C/C++) for poker AI competition.
- Used TPM (Trusted Platform Module) to encrypt cookies in network traffic (C/C++/JavaScript) to prevent cookie stealing and cross-site scripting attacks.
- Used TPM to attest all processes running on the linux OS (C/C++) to provide proof of binary integrity to a remote challenger.
- Implemented a customized version of Adaboost and special image filter (C/C++) to detect drowsy drivers using video cameras mounted on the car dashboard.
- Implemented a handwriting recognition algorithm (Matlab) by applying Kernel PCA method.

PROGRAMMING SKILLS

Most proficient: Python, JavaScript, C/C++, Ruby.

Prior Experience: Java, PHP, Perl, Matlab, R, Linux Shell, OCAML, VHDL/Verilog and MySQL/MongoDB.

Familiar with HTML5/CSS, various libraries and frameworks in aforementioned languages (e.g. OpenCV, Rails, jQuery).

REFERENCES

Wei Xu (Palo Alto Networks manager), Principle Engineer, Internet Security Research Group, Palo Alto Networks, Santa Clara, CA, Phone: (814) 777-0147, Email: wei.xu@paloaltonetworks.com

David Evans (Ph.D. advisor), Full Professor, Department of Computer Science, School of Engineering, University of Virginia, Phone: (434) 409-5443, Email: evans@cs.virginia.edu

Shuo Chen (Microsoft research mentor, Ph.D. dissertation committee member), Ph.D., Researcher, Internet Service

Research Center, Microsoft Research Redmond, Phone: (425) 444-9436, Email: shuochen@microsoft.com
Westley Weimer (Ph.D. dissertation committee member), Associate Professor, Department of Computer Science, School of Engineering, University of Virginia, Phone: (434) 924-1021, Email: weimer@virginia.edu