

Yan Shoshitaishvili

Makes a good pumpkin pie.

yans@yancomm.net
(520) 305-9267
@Zardus

Education

- PhD* 2017 PhD in Computer Science from the University of California, Santa Barbara.
Advisors: Giovanni Vigna and Christopher Kruegel
Dissertation: Building a Base for Cyber-autonomy
- Undergraduate* 2006 BS in Computer Science from Rensselaer Polytechnic Institute.

Professional Appointments

- 2017 - Present Assistant Professor, Arizona State University.

Research Funding

- MITRE 2020-2021 LATCH: Live Binary Analysis and Patching, \$150,000, PI.
- DARPA 2020-2024 VOLT: A Viscous, Orchestrated Lifting and Translation Framework, \$6,678,767, co-PI (w/ Fish Wang, Adam Doupe, Tiffany Bao, Stephanie Forrest, Sandeep Gupta, Georgios Fainekos), \$1,001,815 share.
- DoD 2019-2020 Human-Assisted Cyber Reasoning Systems and Oppositional Human Factors, \$2,298,441.00, PI.
- DARPA 2019-2022 CHESS: CHECRS – Cognitive Human Extensions for Cyber Reasoning Systems, \$11,730,557, co-PI (w/ Fish Wang, Adam Doupe, Tiffany Bao, Chitta Baral, Stephanie Forrest), \$1,707,216 share.
- DARPA 2018-2022 HACCS: Puppeteer – Achieving Remote Control Over Complex Systems, \$7,474,245, PI.
- ONR 2017-2022 Binary Trimming for Improved Security, \$1,990,042, co-PI (w/ Giovanni Vigna, Christopher Kruegel), \$653,464 share.

Selected Academic Publications

- Jayakrishna Menon Vadayath, Moritz Eckert, Kyle Zeng, Nicolaas Weideman, Gokulkrishna Praveen Menon, Yanick Fratantonio, Davide Balzarotti, Adam Doupé, Tiffany Bao, Ruoyu Wang, Christophe Hauser, Yan Shoshitaishvili. *Arbiter: Bridging the Static and Dynamic Divide in Vulnerability Discovery on Binary Programs*, **USENIX Security** 2021.
- Zhibo Sun, Adam Oest, Penghui Zhang, Carlos Rubio-Medrano, Tiffany Bao, Ruoyu Wang, Ziming Zhao, Yan Shoshitaishvili, Adam Doupe, Gail-Joon Ahn. *Having Your Cake and Eating It: An Analysis of Concession-Abuse-as-a-Service*, **USENIX Security** 2021.
- Penghui Zhang, Adam Oest, Haehyun Cho, Zhibo Sun, RC Johnson, Brad Wardman, Shaown Sarker, Alexandros Kapravelos, Tiffany Bao, Ruoyu Wang, Yan Shoshitaishvili, Adam Doupé, Gail-Joon Ahn. *CrawlPhish: Large-scale Analysis of Client-side Cloaking Techniques in Phishing*. **IEEE Security and Privacy** 2021.
- Sung Ta Dinh, Haehyun Cho, Kyle Martin, Adam Oest, Kyle Zeng, Alexandros Kapravelos, Gail-Joon Ahn, Tiffany Bao, Ruoyu Wang, Adam Doupé, Yan Shoshitaishvili. *Favocado: Fuzzing the Binding Code of JavaScript Engines Using Semantically Correct Test Cases*, **NDSS** 2021.
- Pradeep Kumar Duraisamy Soundrapandian, Tiffany Bao, Jaejong Baek, Yan Shoshitaishvili, Adam Doupé, Ruoyu Wang, Gail-Joon Ahn. *MuTent: Dynamic Android Intent Protection with Ownership-Based Key Distribution and Security Contracts*. **HICCS** 2021.
- Mauricio Gutierrez, Ziming Zhao, Adam Doupé, Yan Shoshitaishvili, Gail-Joon Ahn. *Mitigating the CACHEKIT Attack*. **Frontiers in Hardware Security and Trust: Theory, Design and Practice** 2020.
- Efren Lopez-Morales, Carlos E. Rubio-Medrano, Tiffany Bao, Adam Doupe, Yan Shoshitaishvili, Ruoyu Wang, Gail-Joon Ahn. *HoneyPLC: A Next-Generation Honey-pot for Industrial Control Systems*. **ACM CCS** 2020.
- Christophe Hauser, Jayakrishna Menon, Yan Shoshitaishvili, Ruoyu Wang, Giovanni Vigna, Christopher Kruegel. *Sleak: Automating Address Space Layout Derandomization*. **ACSAC** 2020.
- Haehyun Cho, Jinbum Park, Joonwon Kang, Tiffany Bao, Ruoyu Wang, Yan Shoshitaishvili, Adam Doupe, Gail-Joon Ahn. *Exploiting Uses of Uninitialized Stack Variables in Linux Kernels to Leak Kernel Pointers*. **USENIX Woot** 2020.
- Adam Oest, Yeganeh Safaei, Penghui Zhang, Brad Wardman, Kevin Tyers, Yan Shoshitaishvili, Adam Doupé, Gail-Joon Ahn. *PhishTime: Continuous Longitudinal Measurement of the Effectiveness of Anti-phishing Blacklists*. **USENIX Security** 2020.
- Haehyun Cho, Jinbum Park, Donguk Kim, Ziming Zhao, Yan Shoshitaishvili, Adam Doupe, Gail-Joon Ahn. *SmokeBomb: Effective Mitigation Against Cache Side-channel Attacks on the*

ARM Architecture, **ACM MobiSys** 2020.

- Nilo Redini, Aravind Machiry, Ruoyu Wang, Chad Spensky, Andrea Continella, Yan Shoshitaishvili, Giovanni Vigna, Christopher Kruegel. *KARONTE: Detecting Insecure Multi-binary Interactions in Embedded Firmware*, **IEEE Security and Privacy** 2020.
- Faris Kokulu, Ananta Soneji, Tiffany Bao, Yan Shoshitaishvili, Ziming Zhao, Adam Doupé, Gail-Joon Ahn. *Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues*, **ACM CCS** 2019.
- Nilo Redini, Yan Shoshitaishvili, Ruoyu Wang, Aravind Machiry, Yan Shoshitaishvili, Giovanni Vigna, Christopher Kruegel. *BinTrimmer: Towards Static Binary Debloating Through Abstract Interpretation*, **DIMVA** 2019.
- Ronny Chevalier, Stefano Cristalli, Christophe Hauser, Yan Shoshitaishvili, Ruoyu Wang, Christopher Kruegel, Giovanni Vigna, Danilo Bruschi, Andrea Lanzi. *BootKeeper: Validating Software Integrity Properties on Boot Firmware Images*, **ACM CodaSpy** 2019.
- Vaibhav Dixit, Sukwha Kyung, Ziming Zhao, Adam Doupé, Yan Shoshitaishvili, Gail-Joon Ahn. *AIM-SDN: Attacking Information Mismanagement in SDN-datastores*, **ACM CCS** 2018.
- Jaejong Baek, Sukwha Kyung, Haehyun Cho, Ziming Zhao, Yan Shoshitaishvili, Adam Doupé, Gail-Joon Ahn. *Wi Not Calling: Practical Privacy and Availability Attacks in Wi-Fi Calling*, **ACSAC** 2018.
- Mauricio Gutierrez, Ziming Zhao, Adam Doupé, Yan Shoshitaishvili, Gail-Joon Ahn. *CacheLight: Defeating the CacheKit Attack*, **ACM ASHES** 2018.
- Jayakrishna Menon, Christophe Hauser, Yan Shoshitaishvili, Stephen Schwab. *A binary analysis approach to retrofit security in input parsing routines*. **IEEE LangSec** 2018.
- Moritz Eckert, Antonio Bianchi, Ruoyu Wang, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna. *Heaphopper: bringing bounded model checking to heap implementation security*, **Usenix Security** 2018.
- Hui Peng, Yan Shoshitaishvili, Mathias Payer. *T-Fuzz: fuzzing by program transformation*. **IEEE Security and Privacy** 2018.
- Yan Shoshitaishvili, Antonio Bianchi, Kevin Borgolte, Amat Cama, Jacopo Corbetta, Francesco Disperati, Audrey Dutcher, John Grosen, Paul Grosen, Aravind Machiry, Chris Salls, Nick Stephens, Ruoyu Wang, Giovanni Vigna. *Mechanical Phish: Resilient Autonomous Hacking*. **IEEE Security and Privacy Magazine** 2018.
- Vaibhav Hemant Dixit, Sukwha Kyung, Ziming Zhao, Adam Doupé, Yan Shoshitaishvili and Gail-Joon Ahn. *Challenges and Preparedness of SDN-based Firewalls*. **SDN-NFV** 2018.
- Yan Shoshitaishvili, Michael Weissbacher, Lukas Dresel, Christopher Salls, Ruoyu Wang,

Christopher Kruegel, Giovanni Vigna. *Rise of the HaCRS: Augmenting Automated Cyber Reasoning Systems with Human Assistance*. **ACM CCS** 2017.

- Jacob Corina, Aravind Machiry, Christopher Salls, Yan Shoshitaishvili, Shuang Hao, Christopher Kruegel, Giovanni Vigna. *DIFUZE: Interface Aware Fuzzing for Kernel Drivers*. **ACM CCS** 2017.
- Nilo Redini, Aravind Machiry, Dipanjan Das, Yanick Fratantonio, Antonio Bianchi, Eric Gustafson, Yan Shoshitaishvili, Christopher Kruegel, and Giovanni Vigna. *BootStomp: On the Security of Bootloaders in Mobile Devices*. **Usenix Security** 2017.
- Tiffany Bao, Ruoyu Wang, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna, David Brumley. *How Shall We Play a Game? A Game-Theoretical Model for Cyber-warfare Games*. **IEEE Computer Security Foundations Symposium** 2017.
- Tiffany Bao, Ruoyu Wang, Yan Shoshitaishvili, David Brumley. *Your Exploit is Mine: Automatic Shellcode Transplant for Remote Exploits*. **IEEE Security and Privacy** 2017.
- Yan Shoshitaishvili, et al. *Cyber Grand Shellphish*. **Phrack** 2017.
- Ruoyu Wang, Yan Shoshitaishvili, Antonio Bianchi, Aravind Machiry, John Grosen, Paul Grosen, Christopher Kruegel, Giovanni Vigna. *Ramblr: Making Binaries Great Again*. **NDSS** 2017 - Distinguished Paper Award.
- Marius Muench, Fabio Pagani, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna, Davide Balzarotti. *Taming Transactions: Towards Hardware-Assisted Control Flow Integrity using Transactional Memory*. **RAID** 2016.
- Yan Shoshitaishvili, Ruoyu Wang, Chris Salls, Nick Stephens, Mario Polino, Audrey Dutcher, John Grosen, Siji Feng, Christophe Hauser, Christopher Kruegel, Giovanni Vigna. *SoK: (State of the) Art of War: Offensive Techniques in Binary Analysis*. **IEEE Security and Privacy** 2016.
- Nick Stephens, John Grosen, Chris Salls, Audrey Dutcher, Ruoyu Wang, Jacopo Corbetta, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna. *Driller: Augmenting Fuzzing Through Symbolic Execution*. **NDSS** 2016.
- Alessandro Di Federico, Amat Cama, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna. *How the ELF Ruined Christmas*. **Usenix Security** 2015.
- Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna. *Portrait of a Privacy Invasion - Detecting Relationships Through Large-scale Photo Analysis*. **PETS** 2015.
- Yan Shoshitaishvili, Ruoyu Wang, Christophe Hauser, Christopher Kruegel, Giovanni Vigna. *Firmalice: Detecting Authentication Bypass Vulnerabilities in Embedded Devices*. **NDSS** 2015.
- Giovanni Vigna, Kevin Borgolte, Jacopo Corbetta, Adam Doupe, Yanick Fratantonio, Luca

Invernizzi, Dhilung Kirat, Yan Shoshitaishvili. *Ten Years of iCTF: The Good, The Bad, and The Ugly*. **Usenix 3GSE** 2014.

- Yan Shoshitaishvili, Luca Invernizzi, Adam Doupe, Christopher Kruegel, Giovanni Vigna. *Do You Feel Lucky? A Large-Scale Analysis of Risk-Reward Trade-Offs in Cyber Security*. **ACM SAC** 2014.
- Yinzhi Cao, Yan Shoshitaishvili, Kevin Borgolte, Christopher Kruegel, Giovanni Vigna, Yan Chen. *Protecting Web-based Single Sign-on Protocols against Relying Party Impersonation Attacks through a Dedicated Bi-directional Authenticated Secure Channel*. **RAID** 2014.
- Giancarlo De Mayo, Alexandros Kapravelos, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna. *PExy: The other side of Exploit Kits*. **DIMVA** 2014.
- Ruoyu Wang, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna. *Steal this Movie - Automatically Bypassing DRM Protection in Streaming Media Services*. **Usenix Security** 2013.
- Alexandros Kapravelos, Yan Shoshitaishvili, Marco Cova, Christopher Kruegel, Giovanni Vigna. *Revolver: An Automated Approach to the Detection of Evasive Web-based Malware*. **Usenix Security** 2013.
- Antonio Bianchi, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna. *Blacksheep: Detecting Compromised Hosts in Homogeneous Crowds*. **ACM CCS** 2012.

Awards

- Our paper, *How Shall We Play a Game?*, won the 2018 NSA Cybersecurity paper competition.
- I received the UC Santa Barbara Computer Science Department's Outstanding Dissertation Award for my graduate studies.
- We received a Distinguished Paper award for our paper, *Ramblr*, at NDSS 2017.
- I led my team, Shellphish, to a 3rd place victory (and another \$750,000 prize) in the DARPA Cyber Grand Challenge.
- I led Shellphish to qualify for the DARPA Cyber Grand Challenge (and win a \$750,000 prize). 7 teams qualified out of more than 100 entrants.
- Before passing on the mantle, I led Shellphish through a number of CTF victories and other finalist finishes in many competitions around the world, over the course of most of a decade.

Open Source Contributions

angr.io I led the design and development of **angr**, a next-generation binary analysis

framework developed at UC Santa Barbara, and oversaw its open source release. I also managed the details of many sub-projects using and supporting angr.

pwn.college I created **pwn college**, a curated, comprehensive cybersecurity education platform, upon which I built my security courses at ASU. Pwn College is based on the concept of "practice makes perfect" along with a new style of "walkthrough" CTF challenges.

github.com/o-o-overflow As one of the leaders of the Order of the Overflow, I organize the DEF CON CTF, the "world championship" of cybersecurity competitions. The challenges and infrastructure we open source end up here.

github.com/shellphish With the rest of my hacking team, Shellphish, I released various tools and educational materials relating to security. For example, **how2heap**, a set of heap exploitation tutorials, is one of our popular projects.

github.com/mechaphish My hacking team, Shellphish, open-sourced our CRS, the **Mechanical Phish**, which won third place at the DARPA Cyber Grand Challenge.

openglad.org I co-led the effort to port and improve a game called Gladiator for modern platforms under the name **Openglad**. This has involved releases on every major OS and Android.

github.com/zardus I enjoy solving problems in original ways. When I solve an interesting problem or just create something nice, I open source it. There's a fair bit of useful security software here: **preeny**, **ctf-tools**, **memcurses**, **idalink**, **kuboid**, and others.

Invited Talks and Presentations

Keynote. Potential of CTF as Educational Opportunity / Teaching Material for Information Security. **SECCON** 2020.

Invited Talk. pwn.college: The Cybersecurity Dojo for Binary Analysis. **CODE BLUE** 2020.

Panelist. Talent Cultivation, the post-pandemic talent cultivation challenges and opportunity. **HITCON** 2020.

Invited Lecture. Cyber Autonomy: Theory to Practice. **QualComm** 2020.

Invited Talk. Theory to Practice: Applying Academic Program Analysis Advances in the Real World. **Disclosure** 2020.

Keynote. Wax on, wax off: educating the next generation of hackers! **HITCON** 2019.

Panelist. Panel on Cybersecurity Education. **HITCON** 2019.

Keynote. The Dangers of the Subconscious Mind (of Cyber Reasoning Systems). **Artificial Intelligence and Cybersecurity Workshop** 2019.

Invited Talk. Master and Automation in Cybersecurity. **Tsinghua Inforsec Workshop** 2019.

Invited Seminar. How to Train Your Dragon: The Quest Toward Master and Automation in Cybersecurity. **Rensselaer Polytechnic Institute** 2019.

Invited Talk. The Rise, Tribulations, and Promises of the HaCRS. **NSA Research** 2018.

Distinguished Seminar. The Long Road to Cyber Autonomy. **CMU Cylab** 2018.

Keynote. All our Powers Combined: Connecting Academics, Engineers, and Hackers. **HITCON** 2017.

Panelist. Panel on International Cybersecurity. **HITCON** 2017.

Invited Talk. The Long Road to Cyber Autonomy. **Cyberchess** 2017.

Keynote. Reaching for Cyber Autonomy - From the Cradle to the Server Room. **Samsung Security Forum** 2017.

Panelist. Panel on Shifting the Balance in the Attack-Defend Cycle. **HotSoS** 2017.

Blue-team member. Workshop on Dangers of AI. **ASU Origins** 2017.

Panelist. Panel on National Privacy Research Strategy. **ACSAC** 2016.

Tutorial Instructor. ACSAC Tutorial - angr. **ACSAC** 2016.

Invited Talk. *Through the Cyber Grand Challenge and Beyond.* **DHS/SRI Infosec Technology Transition Council Meeting** 2016.

Invited Seminar. *From the Lab to the Cyber Grand Challenge.* **ASU Center for Cybersecurity and Digital Forensics Seminar Series** 2016.

Invited Talk. *Cyber Grand Shellphish.* **DEFCON** 2016.

Invited Talk. *Letting angr drive your actions.* **OCON** 2016.

Invited Talk. *Towards the DARPA Cyber Grand Challenge: A Dozen Years of Shellphish.* **SECCON** 2015.

Keynote. *Binary Analysis in the Wild West.* **ACSAC PPREW** 2015.

Invited Talk. *A Dozen Years of Shellphish - From Defcon to the DARPA Cyber Grand Challenge.* **HITCON CMT** 2015.

Invited Talk. *Angry Hacking - The Next Generation of Binary Analysis.* **DEFCON** 2015.

Invited Talk. *Dark Side of the ELF - Leveraging Dynamic Loading to pwn noobs.* **DEFCON** 2015.

Invited Talk. *Using Static Binary Analysis to Find Vulnerabilities and Backdoors in Firmware.* **Blackhat** 2015.

Tool Presentation. *CTF Tools - Taking the Headache out of Security Tool Installation.* **Blackhat Arsenal** 2015.

Tool Presentation. *Preeny - LD_PRELOAD for Security Analysis.* **Blackhat Arsenal** 2015.

Service

DEF CON CTF organizer. 2018-present.

Graduate Program Committee Chair. ASU 2019-2020.

Faculty Search Committee Chair. ASU 2019.

Program Committee. ACM CCS 2020.

Program Committee. IEEE Security and Privacy 2020, 2021.

Program Committee. ACM AsiaCCS 2020.

Steering Committee. NDSS Workshop on Binary Analysis Research 2017-present..

Program Committee. NDSS Workshop on Binary Analysis Research 2017-present.

Program Committee. ACM Workshop on Automotive Cybersecurity 2018.

Program Committee. ACM CCS Workshop on Forming an Ecosystem Around Software Transformation 2018-2019.

Program Committee Chair. ACM CCS Workshop on Forming an Ecosystem Around Software Transformation 2018.

Faculty Search Committee - Cybersecurity. ASU 2018.

Faculty Search Committee - Biodesign. ASU 2018.

NSF SaTC Panel Reviewer. 2018-2019.

Program Committee Chair. NDSS Workshop on Binary Analysis Research 2018.

Program Committee. DIMVA 2018.

Track Lead. SCORE C3E 2017.

Program Committee. ISSTA TECPS 2017.

Faculty Search Committee - Biodesign. ASU 2017.

Program Committee, Session Chair. Usenix Enigma 2017.

Mentorship

PhD Committee Chair. Zachary Wimer (expected graduation Fall 2023).

PhD Committee Chair. Arvind Raj (expected graduation Spring 2024).

PhD Committee Chair. Jay Menon (expected graduation Fall 2024).

PhD Committee Chair. HuiJun Tay (expected graduation Fall 2024).

PhD Committee. Fangzhou Dong.

PhD Committee. Ananta Soneji.

PhD Committee. Gokul Menon.

PhD Committee. Kyle Zheng.

PhD Committee. Siyu Liu.

PhD Committee. Sukwha Kyung.

PhD Committee. Zhibo Sun.

PhD Committee. Sana Habib.

PhD Committee. Erik Trickel.

PhD Committee. Faezeh Kalantari.

PhD Committee. Haehyun Cho.

PhD Committee. Mehrnoosh Zaeifi.

PhD Committee. Penghui Zhang.

PhD Committee. Yeganeh Ladwig.

PhD Committee. Connor Nelson.

PhD Committee. Maxfield Lehman.

PhD Committee. Adam Oest.

PhD Committee. Faris Kokulu.

MS Thesis Committee Co-Chair. Jaswant Pakki.

MS Thesis Committee Co-Chair. Ashwin Sudhir.

MS Thesis Committee Co-Chair. William Gibbs (**graduated**).

MS Thesis Committee Co-Chair. Connor Nelson (**graduated**).

MS Thesis Committee Co-Chair. Vaibhav Dixit (**graduated**).

MS Thesis Committee Co-Chair. Zachary Crosley (**graduated**).

Undergraduate Advisor. Kevin Stevens (**graduated**).

Undergraduate Co-Advisor. Jaswant Pakki (**graduated**).

Undergraduate Co-Advisor. William Gibbs (**graduated**).

Apprenticeship Mentor. Akshay Ajayan.

Apprenticeship Mentor. John Andrews.

Apprenticeship Mentor. Salah Baddou.

Apprenticeship Mentor. Xingman Chen.

Apprenticeship Mentor. Osi Ikharebha.

Apprenticeship Mentor. Xavier Maso.

Apprenticeship Mentor. Rana Pourmohamad.

Apprenticeship Mentor. Pradeep Soundrapandian (completed 2020).

Apprenticeship Mentor. Chien-Yuan Wang (completed 2019).

Apprenticeship Mentor. Ryo Ichikawa (completed 2018).

Apprenticeship Mentor. Jack Phillips (completed 2018).

Apprenticeship Mentor. Ange Andries (completed 2019).

Apprenticeship Mentor. Gokul Menon (completed 2019).

Apprenticeship Mentor. Jay Menon (completed 2019).

Apprenticeship Mentor. Sung Ta (completed 2019).

Apprenticeship Mentor. Zhenpeng Lin (completed 2019).

Apprenticeship Mentor. Nipun Gupta (completed 2019).

Apprenticeship Mentor. Fangzhou Dong (completed 2019).

Apprenticeship Mentor. Aaron Branch (completed 2019).

Apprenticeship Mentor. Bader AlBassam (completed 2019).

Teaching

Fall 2019, **CSE 466: Computer Systems Security**.

Fall 2018, **CSE 466: Computer Systems Security (fully redeveloped)**.

Spring 2017, **CSE 591: Automated Binary Code Analysis (newly developed)**.

Endeavors

- I am a leader of the Order of the Overflow, the current organizers of the DEF CON CTF, the world championship of cybersecurity competitions.
- I was the captain for Shellphish's participation in the DARPA Cyber Grand Challenge. We finished in 3rd place, of 7 finalists (out of over 100 teams). We were the top-placing "unfunded" team, the top-placing academic team, and the only team to open-source our

Cyber Reasoning System.

- I have competed on the UCSB Security Lab team (team Shellphish) at the DEFCON CTF from 2009 through 2017, leading it from 2011 through 2017. In 2015, our team ranked 4th worldwide.
- I have been a leading or core member of the organization team behind the 2011 through 2016 UCSB iCTF Computer Security competitions.
- I organized and taught at the UCSB Hacking Club meetings from 2011 to 2017.
- I danced Ballroom Dance competitively through college, and continue to dance West Coast Swing.
- I hold a black belt in Taekwondo from two studios.