Yan Shoshitaishvili

Striving to make the world more secure.

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

Education

Graduate PhD in Computer Security at University of California, Santa Barbara.

Undergraduate BS in Computer Science at Rensselaer Polytechnic Institute.

Work Experience

Aug 2017 - Present As an **Assistant Professor** at **Arizona State University**, I lead research into novel binary analysis techniques and their real-world applications. A secondary field of research (and personal interest) is educational cyber-security competitions.

Sept 2010 - Aug 2017 I worked on a diverse range of projects as a **Graduate Student Researcher at UC Santa Barbara's Computer Security Lab**. Among these were rootkit detection, protection of binary applications, tracking of the evolution of malicious web pages, identification of drawbacks in DRM techniques, privacy compromisation techniques in social networks, analysis of binary software, and creation of unique cybersecurity competitions. Among other accomplishments, I published over a dozen academic papers, started the angr binary analysis engine project, and led my team to a third-place finish in the DARPA Cyber Grand Challenge.

Academic Publications

- 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, Andrew 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, Andrew 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

- ➔ 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.
- ➔ I led Shellphish to a first place victory (out of 447 teams) in the 2016 Nuit Du Hack Cybersecurity Competition, along with 23 other top-5 finishes over the last 5 years.
- ➔ I received a Blackhat Student Scholarship for Blackhat 2014 and 2015.

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.
github.com/shellphish	With the rest of my hacking team, Shellphish, I release 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**, and others.

Invited Talks and Presentations

- **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.
- **Distinguished Lecture,** *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*. **0CON** 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

- ➔ **Track Lead.** SCORE C3E 2017.
- ➔ **Program Committee.** ISSTA TECPS 2017.
- ➔ **Program Committee, Session Chair.** Usenix Enigma 2017.

Endeavors

- ➔ I was the team leader 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 2016. In 2015, our team ranked 4th worldwide.
- ➔ I have been a leading or core member of the organization team behind the 2011 through 2015 UCSB iCTF Computer Security competitions.
- ➔ I organized and taught at the UCSB Hacking Club meetings for four years, 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.