Yan Shoshitaishvili

Security researcher seeking interesting opportunities and great challenges.

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

Education

Graduate PhD in Computer Security (in progress) at University of California, Santa Barbara with a 3.97 GPA.

Undergraduate BS in Computer Science at Rensselaer Polytechnic Institute with a 3.26 GPA.

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.

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.

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.

Work Experience

Sept 2010 - Present I work on a diverse range of projects as a **Graduate Student Researcher at UC Santa Barbara's Computer Security Lab**. Among these are 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 have published 13 academic papers, started the angr binary analysis engine project, and led my team to a third-place finish in the DARPA Cyber Grand Challenge.

July 2006 - As an **Information Security Engineer at Wells Fargo Bank**, I architected and deployed Wells Fargo's setup of the IBM Tivoli Identity Manager 4.6, 5.0, and 5.1 application stacks. This included IBM DB2 (an RDBMS), IBM ITDS (an LDAP server), IBM Websphere (a Java EE application server), and IBM TIM (an identity management solution). I also led support, troubleshooting, and vendor interaction efforts for this software and developed user-requested features and various tools to ensure availability, reliability, and a good user experience.

Sept 2004 - Dec 2004 During my internship as a **System Administrator at the Molecularium Project at RPI** (http://www.molecularium.com), I maintained a 24-node Linux cluster which was used for rendering the Molecularium's "Riding Snowflakes" production. The project required me to write a lot of utility applications to facilitate the management and distribution of rendered frames and to ensure the availability and security of the cluster.

June 2002 - Aug 2005 I undertook many projects in my duties as a **System Programmer and Network Administrator for the University of Arizona's Office of Institutional Research and Evaluation**. To improve the security of the department, I designed a properly-firewalled network setup in time to prevent the Slammer worm from infecting our database servers. I also developed and deployed a flexible and reliable backup system to facilitate cross-platform backups. Unfortunately, licensing issues prevented it from becoming an open-source project. Finally, I deployed VPN solutions to allow employees to work from home, led and assisted in network and computer troubleshooting, and maintained the security of the department network.

June 2001 - May 2003 In my duties as a **Web Developer at St. Gregory College Preparatory School**, I developed web applications to assist in school administration (such as event scheduling) and assisted in maintenance of network security. During the school year, as a **Technology Assistant**, I assisted in setup and maintenance of the school network, helped with computer assembly and repair, set up and maintained servers and computer lab workstations, and assisted teachers and students with computer problems.

June 2001 - July 2001 I spent the summer as a **Student Summer Assistant at the Pima County Department of Transportation**. To assist DOT software developers, I

maintained and updated several database applications to ease management of DOT employees and invoices. To assist the IT helpdesk, I carried out upgrades and rebuilds of DOT employee workstations.

Jan 2001 - Dec 2001 As a **Web Developer for NBWRPG**, an online roleplaying game, I developed and hosted a web site for the Neo Beast Wars RPG (http://nbwrpg.com, since defunct), including a Perl backend to provide social user interaction.

Academic Publications

- Antonio Bianchi, **Yan Shoshitaishvili**, Christopher Kruegel, Giovanni Vigna. *Blacksheep: Detecting Compromised Hosts in Homogeneous Crowds*. **ACM CCS** 2012.
- 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.
- Ruoyu Wang, **Yan Shoshitaishvili**, Christopher Kruegel, Giovanni Vigna. *Steal this Movie - Automatically Bypassing DRM Protection in Streaming Media Services*. **Usenix Security** 2013.
- Giancarlo De Mayo, Alexandros Kapravelos, **Yan Shoshitaishvili**, Christopher Kruegel, Giovanni Vigna. *PExy: The other side of Exploit Kits*. **DIMVA** 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.
- **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.
- 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**, Ruoyu Wang, Christophe Hauser, Christopher Kruegel, Giovanni Vigna. *Firmalice: Detecting Authentication Bypass Vulnerabilities in Embedded Devices.* **NDSS** 2015.
- **Yan Shoshitaishvili**, Christopher Kruegel, Giovanni Vigna. *Portrait of a Privacy Invasion - Detecting Relationships Through Large-scale Photo Analysis.* **PETS** 2015.
- Alessandro Di Federico, Amat Cama, **Yan Shoshitaishvili**, Christopher Kruegel, Giovanni Vigna. *How the ELF Ruined Christmas*. **Usenix Security** 2015.
- 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** 2015.

- **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.
- 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.

Invited Talks and Industry Presentations

- *Preeny - LD_PRELOAD for Security Analysis*. **Blackhat Arsenal** 2015.
- *CTF Tools - Taking the Headache out of Security Tool Installation*. **Blackhat Arsenal** 2015.
- *Using Static Binary Analysis to Find Vulnerabilities and Backdoors in Firmware*. **Blackhat Briefings** 2015.
- *Dark Side of the ELF - Leveraging Dynamic Loading to pwn noobs*. **DEFCON** 2015.
- *Angry Hacking - The Next Generation of Binary Analysis*. **DEFCON** 2015.
- *A Dozen Years of Shellphish - From Defcon to the DARPA Cyber Grand Challenge*. **HITCON CMT** 2015.
- *Binary Analysis in the Wild West.* Keynote for **ACSAC PPREW** 2015.
- *Towards the DARPA Cyber Grand Challenge: A Dozen Years of Shellphish*. **SECCON** 2015.
- *Letting angr drive your actions*. **0CON** 2016.

  Cyber Grand Shellphish. **DEFCON** 2016.

Endeavors

- I was the team leader for Shellphish's participation in the DARPA Cyber Grand Challenge. We finished in 3rd place, of the 7 finalists. 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 2016. I have led the organization and DEFCON preparation process of the team for the last five of those years. 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 taught at the UCSB Hacking Club meetings for four years, from 2011 to 2015.
- ➔ I used to organize and host most of the Super Smash Bros Brawl tournaments in Phoenix, AZ in 2009 and 2010.
- ➔ I danced Ballroom Dance competitively through college, and continue to dance West Coast Swing.
- ➔ I hold a black belt in Taekwondo from two studios.
- ➔ I was the president of the St. Gregory Computer Club in my Senior year of high school.
- ➔ I get awards sometimes:
    - Blackhat Student Scholarship
    - Dean's List at RPI
    - National Honor Roll
    - Robert Byrd Achievement Award
    - Arizona Daily Stars Senior Achievement Award
    - St. Gregory College Preparatory School Science and Technology Diploma
    - Sue and Dickson Potter Cup for Distinguished Citizenship from St. Gregory College Preparatory School
    - Science and Technology Medal from RPI
    - Certificate of Distinction from the American Mathematics Contests