DAVID SOLODUKHIN

U.S. CITIZEN | 914-564-8872 | DAVID.SOLODUKHIN@GATECH.EDU

EDUCATION

Georgia Institute of Technology - Atlanta, GA **Graduating Dec 2019**
Candidate for B.S. in Computer Science
GPA: 3.96/4.0
Courses: Information Security Lab, Systems and Networks, Advanced O.S. Development, HPC & Distributed Systems
Orgs: Grey Hat Security CTF team: web exploit lead, HackTheBox(Top 10%: S18); Linux Users Group; Phi Kappa Theta (ΓΤ) Fraternity– I.T. Chair

EXPERIENCE

Prudential Financial – Newark, NJ **May 2018 – August 2018**
Software Engineer Intern, Enterprise Services & Systems

- Modernized in-house Metadata Management System (TMS) web application, enabling lower query latency, a wider array of query protocols as well as reorganization into stable microservices.
  - Added frontend features using ReactJS (previously JSP) and rewrote Struts2 MVC functionality in Spring MVC(Web).
  - Using the Spring Framework, the application is now able to integrate with other middleware tools and provides microservices for metadata management. (Spring Web/Boot, JSP, Strut2, Maven, Gradle, Java 8, Javascript, Reactjs, ES6).
- Reduced daily build time of MMS system by several hours with multi-module Maven build scripts that automate building of Oracle ADF applications.
- Agile Methodology: paired programming, story writing, and extensive testing [TDD], including unit, integration, e2e, mutation, and performance (Junit, TestComplete, Jenkins)

Institute for Information Security and Privacy - Georgia Tech **October 2017 – February 2018**
Undergraduate Research Assistant – Dr. Taesoo Kim

- Designed and evaluated new anti-fuzzing techniques to slow down modern fuzzers and protect software (ELF binaries) from malicious fuzzing.
- Wrote LLVM passes in **C++** to implement anti-fuzzing techniques in existing Linux executables.
- Automated executable instrumentation, unit testing of anti-fuzzing methods as well as analysis and plotting of fuzzing statistics with **Python**.
- Revised and edited final paper which was submitted to USENIX and Black Hat.

Advise Technologies – New York City, NY **June 2016 – August 2016**
Software Engineer Intern, CI and QA Team

- Designed a continuous integration system for the development team that automatically pulled code from repositories, compiled projects, ran regression and unit tests and emailed results to team leads. (TestComplete, PowerShell, Java)
- Designed **Java** plugins for TeamCity CI server which added automation functionality such as email alerts and detailed logging.
- Scripted custom regression tests in Jscript using the TestComplete testing suite.

PROJECTS & CVES/BUGS– (GITHUB.COM/DAVID-SOLODUKHIN)

- **Linux Kernel Modules** (kernel v4.15.18): Developed a module which starts a UDP server process within the kernel for transmitting O.S. filesystem, process stats. Implemented a kernel module for network traffic artificial throttling and packet proxy. Modules were written in C.
- **Linux Kernel Hypervisor(KVM) Scheduler**: KVM management app that load balances up to 24 virtual machines on a multi core processor based on virtual CPU & memory load, leading to **~%10** speedup compared to native QEMU (C,C++)
- **(K)ASLR and PIE for xv6**: Implemented user-space ASLR and simple kernel ASLR for the xv6 operating system. Also added custom PIE support for xv6 binaries.
- **Wolfram Alpha Bug:** Found SSRF vulnerability in Wolfram Alpha's api giving access to premium features for free. Contacted WA team and exploit was patched.

SKILLS

Languages: Java, C, C++, Javascript, Python, (PL)SQL, Perl, PHP, x86/64 ISA (GAS, FASM)
Testing: Selenium, TeamCity, TestComplete, Junit
Libraries & Tools: Reactjs, Maven, Gradle, Node.js, JQuery, Android SDK, LLVM(Clang), Git, Mercurial, JSP, Oracle Weblogic, Struts2, Spring Web, KVM, QEMU, libvirt, Bash, Burp, IDA, Wireshark, Kali tools, Metasploit, PowerShell, Docker
Security: Reverse Engineering, Malware Analysis, Digital Forensics, Pentesting, Intrusion Detection & Prevention, exploit development, ROP, cryptography; concentration in AES, Linux Kernel Security, Windows/Linux privilege escalation, fuzzing, Netsec Architecture; Zero Trust, Active Directory; Kerberos, Oracle Server Administration; WebLogic, Wildfly, AWS
Foreign Language: Russian; Native Fluency