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, Distributed Systems, Advanced O.S. Development, Database Systems Design, Networking
Orgs: Grey Hat Security CTF team: web exploit engineer, Collegiate Cyber Defense Competition Team, 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 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.

Georgia Tech Database Research Group - Georgia Tech **Feb 2019 – Present**
Undergraduate Researcher– Dr. Joy Arulraj – Approximating Queries with Segment Trees

- Research is conducted with a team at the Georgia Tech Database Group. The team is evaluating new database 'cracking' architectures to enable fast concrete range query processing using statistical models and specialized indexes across multiple attributes. (C++)

College of Computing - Georgia Tech **January 2018 – Present**
Undergraduate Teaching Assistant – Design and Analysis of Operating Systems

- Responsibilities consist of hosting office hours to help students understand key operating systems and kernel programming concepts as well as grading.

Institute for Information Security and Privacy - Georgia Tech **October 2017 – October 2018**
Undergraduate Researcher – Dr. Taesoo Kim – Fuzzification: Anti-Fuzzing Techniques

- Designed and evaluated new anti-fuzzing techniques to slow down modern fuzzers and protect software from malicious fuzzing.
- Wrote LLVM passes in **C++** to implement anti-fuzzing techniques in existing Linux executables.
- Automated source-code 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 accepted in USENIX(2019) and Black Hat (pending).

PROJECTS, CVES, PAPERS– GITHUB.COM/DAVID-SOLODUKHIN

- Jinho Jung, Hong Hu, **David Solodukhin**, Daniel Pagan, Kyu Hyung Lee, and Taesoo Kim. **Fuzzification: Anti-Fuzzing Techniques** (to appear). *In Proceedings of the 28th USENIX Security Symposium (Security 2019)*, Santa Clara, CA, August 2019.
- **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 **~%5** more throughput compared to native KVM (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.
- **Map-Reduce GRPC Implementation:** Map-Reduce architecture using GRPC for rpc communication between cluster workers and master. Architecture includes separate worker and master applications written in C++ for Linux.
- **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)
Systems, Technologies/Tools: Reactjs, Maven, Gradle, Node.js, JQuery, Android SDK, LLVM(Clang), Git, Mercurial, JSP, Oracle Weblogic, Struts2, Spring Web, Dart, Flutter, KVM/QEMU, libvirt, Bash, Burp, IDA, Wireshark, Kali tools, Metasploit, PowerShell, Docker, DHT, Map-Reduce, Database Systems, OpenMP, MPI**,** Reverse Engineering, Digital Forensics, Pentesting, ROP, Linux Kernel-security, privilege escalation, fuzzing, WebLogic, Wildfly, AWS:LightSail/EC2, MS Exchange; Active Directory
Foreign Language: Russian; Native Fluency