

Mohammad Zaid Khaishagi

Phone: +1 4709092126 | Email: zaid960928@gmail.com or mkhaishagi3@gatech.edu

LinkedIn: <https://www.linkedin.com/in/zaid-khaishagi> | Github: <https://github.com/Zaxeli> | Website: <https://zaxeli.github.io/>

Education

Georgia Institute of Technology , Atlanta, GA Master of Science in Cybersecurity	<i>August 2020 - May 2022 (expected)</i>
Uttar Pradesh Technical University , Lucknow, India Bachelor of Technology in Computer Science Engineering	<i>August 2015 - June 2019</i>

Experience

Teaching Assistant	<i>2021</i>
<ul style="list-style-type: none">CS-6035: <i>Introduction to Information Security</i>, during Fall 2021CS-3251: <i>Computer Networks</i>, during Summer 2021CS-6035: <i>Introduction to Information Security</i>, during Spring 2021	
Freelance work	<i>2020</i>
<ul style="list-style-type: none"><i>Pandemic Modelling</i>, a project based on a research paper by Dirk Brockmann and Dirk Helbing published in 2013.<i>Genetic Algorithms</i>, used for solving optimisation problems.	

Research

NPM Package Manager Security	<i>Spring 2022</i>
<ul style="list-style-type: none">Developed a detection tool and mechanism for potential malicious packagesImplement alert system for malicious indicators in packagesAdditional package metadata analysis at package installationLook for possible typosquatting	
Survey on Symmetric Key Exchange	<i>Spring 2022</i>
<ul style="list-style-type: none">Reviewed multiple research papers dealing with Symmetric Key Exchange Protocols, including TLS 1.3 Handshake ProtocolDeveloped alterations on Sym Key Exchange protocol that achieves the same level of bounded gap and synchronisation robustness security.	

Browser Fingerprinting Techniques	<i>Summer 2021</i>
<ul style="list-style-type: none">Looked into fingerprinting techniques used by fingerprintjs.comAnalysed webRTC fingerprintingIdentified possible webRTC fingerprinting detection signatureProposed defences against fingerprintingAnalysed Google Privacy Sandbox	

Skills

Expertise: Information Security, Software development, Presentation skills	
Programming & Tools: C, C++, Java, Python, Solidity, Javascript, Node.js, HTML, SQL, Assembly, Ghidra, Pwndbg, GDB, Wireshark, nmap, Burp Suite, OWASP Zap, Cuckoo.	
Technical: Reverse engineering, Network forensics, Powershell, Registry analysis, Log analysis, Docker analysis, OSINT, Linux, Email analysis, XSS, CSRF, SQL Injection, OWASP, NIST Framework, HIPAA, PCI-DSS, Ethereum, Hyperledger, Loopback, Bootstrap, Java, Flask, Flask API, Wordpress, AWS, Webmail, MongoDB, SQLite, Google Apps.	
Course Concepts: Binary exploitation, Information Theory, Browser fingerprinting, Secure Comm Protocols, Distributed Systems and Consensus, Browser privacy, Information Security, Advanced Operating Systems, Cryptography, Network Security, Secure Computer Systems, Information Security Policies, Data Analysis, Blockchain, Shellcode Injection.	
Languages: English (fluent), Hindi (fluent), Arabic (beginner)	
Communication: Presentation, Articles, Project write-up, Research paper summaries, Lecture scribe.	

Course Projects

Secure Communication Protocols	<i>Spring 2022</i>
<ul style="list-style-type: none">Presentation on Cryptographic Analysis of TLS 1.3 Handshake ProtocolPresentation on Message Franking for abuse reporting in Facebook's end-to-end encryption	
Binary Exploitation	<i>Fall 2021</i>

- Exploited many binaries based on different techniques
- Techniques explored: Shellcode injection, buffer overflows, stack exploitation, ROP, Heap exploitation, Remote binary exploits, C64 debugging, remote binaries, fstring vulnerabilities
- Exploit scripts using Python

NSA Codebreaker Challenge

Fall 2021

- Malware Analysis on infected system
- Malicious email analysis and quarantining
- Network and computer forensics
- Powershell, registry analysis, docker analysis and reverse engineering

PAXOS consensus and Sharded KV Store

Fall 2021

- Implemented PAXOS consensus algorithm between servers
- Ensures consistency of operations performed across group of PAXOS servers
- Supports transactions across keys located in different shards and different groups
- Replication across multiple servers in each group to provide fault tolerance
- Supports reconfiguration of shards distributed over the groups with PAXOS in each group

Improved Authentication with Password Hardening

Spring 2021

- Implemented mechanism for stronger passwords using features from password typing
- Use of tokens to generate hardened passwords
- Password hash updated after each login

Memorandum for National Security

Spring 2021

- Evaluating possible responses for Solarwinds attack
- Considerations for escalation, deterrence and forward defence
- Recommendation for cybersecurity response to Russia

Memorandum analysing Federal Data Breach Notification Law

Spring 2021

- Analysis of benefits and drawbacks of Federal Data Breach Notification Law
- Proposed recommendations regarding supporting Law

Hypervisor Virtualization

Fall 2020

- Made use of qemu and libvirt to implement virtual CPU scheduler
- Implemented memory coordination between multiple virtual CPUs.

Map-reduce infrastructure using gRPC

Fall 2020

- Built map-reduce infrastructure for word counting over a set of input files.
- Implemented mapper and reducer phases with multiple functions in parallel at each phase

Intro to Infosec projects

Fall 2020

- **Malware Analysis using Cuckoo:** Analyse behaviour of malwares samples
- **Attack weak RSA keys:** Bad randomness source gave factorisable and weak RSA keys
- **Attack vulnerable RSA:** Used Chinese Remainder Theorem to attack weak RSA encryption

Publication and Presentation

Article explaining Cryptographic Hash function SHA-512

<https://medium.com/@zaid960928/cryptography-explaining-sha-512-ad896365a0c1>

Article explaining Blockchain

<https://medium.com/@zaid960928/introduction-to-blockchain-ad0ab0628c15>

Presentation on Blockchain delivered to undergraduate students

<https://www.slideshare.net/zaidkhaishagi/blockchain-introduction-99542456>

Activities/Participation

Country to Country (C2C) CTF

Spring 2022

- Performed challenges on: OSINT, Cryptography, Reverse Engg, Analysis
- Cleared qualifying rounds, finals to be held on 1st August 2022.

TKCTF Capture-the-flag event

Fall 2021

- Ranked 6th place among 15 teams in TKCTF event. (<https://ctf.gts3.org/>)
- 24-hour capture-the-flag event to exploit/hack binaries submitted by other teams
- Team submission of challenge binary with various defences implemented.

Greyhats Cybersecurity Club

2021-present

- Discussed security topics, attacks, and solve ctf challenges

- Participated in picoCTF 2022

- Over 95% completion in Binary Exploitation and Reverse Engineering