Mohammad Zaid Khaishagi

Phone: +1 4709092126 | Email: zaid960928@gmail.com or zaid.khaishagi@crimsonvista.com
LinkedIn:https://www.linkedin.com/in/zaid-khaishagi | Github: https://github.com/Zaxeli | Website: https://zaxeli.github.io/

Experience:

Cybersecurity Engineer @ Crimson Vista
August 2022 - Current

- **Engineering Analysis for Location Tracking and Privacy Issues**
  - Identify how location data is collected, stored and used based on internal documentations and communications.
  - Contribute to preparing a report analysing location data flow and related privacy issues.
  - Prepare diagrams visualising data flow between various internal components, services and data stores.
- **Patent Infringement Analysis: Firewalls and Network Filtering Gateways**
  - Microsoft Forefront TMG
    - Configure and setup the TMG Gateway
    - Filter traffic going between external and internal networks
    - Configure as firewall and application filtering
    - Analysing event logs produced
  - Sourcefire: Source code review of 3D Sensor appliances and set up
  - Source code review of Snort Engine including its packet processing
  - Checkpoint Gateway: Configuring and setting up the firewall and gateway and exploring its features
  - Networking physical devices and virtual machines
- **IperionX - Newsletter, Phishing analyses, Data Audit**
  - Weekly cybersecurity newsletter
    - Receiving and analysing phishing reports
    - Analysing new trends and techniques used in phishing campaigns
    - Explaining how to identify phishing emails based on reports
    - Analysing malicious links and attachments
  - Data Audit: Prepared draft for company data audit sheet
- **Android App Network Inspection and Capture: for Dryden Technology Group**
  - Investigate data transmitted while performing payments through one of the app's features.
  - Reverse engineering network communication of android application
  - Install application on android virtual device (AVD)
  - Rooting an emulated device
  - Generating and installing a system certificate on the AVD using elevated privileges, as opposed to a user certificate
  - Proxy to capture all device traffic in plaintext, bypassing TLS encryption
  - Capturing and analysing communication of application to its servers
  - Extracting information from specific payment-related flows and interactions
- **Editorial Board Member of Crypto Done Right**
  - Editing articles that give Cryptography advice
  - Content for website
- **Patent Infringement Analysis: Robotic Process Automation**
  - Exploring Robotic Process Automation features and functionalities
  - Investigating patent infringement
- **Dominion Voting Systems - Source code and systems security review**
  - Involved in the Fox News vs Dominion Voting Systems case as a member of the security review team
  - Performing source code review of voting systems to find evidence of vulnerabilities or bad coding practices
  - Evaluating security of live setup of voting systems
  - Exploring viability of exploiting these systems
  - Skills practised: Decompiling, reverse engineering and binary patching of application files
  - Reversing, analysing and modifying Dalvik Bytecode using Smali assembler/disassembler
- **Cybersecurity Investigation: Twitter**
  - Part of review team on behalf of Elon Musk in Elon Musk v. Twitter case, 2022
  - Investigating bot population on Twitter
  - Evaluating Twitter's internal bot detection techniques
  - Evaluating bot population using approaches outlined in academic papers
  - Comparing bot population results
- **Digital Radios investigation**
  - Reverse engineering digital radios

        - Deobfuscating firmware updates
        - Assisting with investigation of source code theft
        - Skills and tools: .NET reverse enginering, deobfuscation of binaries, firmware reverse engineering
        - Source code review
    - **Hashicorp Vault**
        - Worked on setting up a demo environment
        - Examining how the security fails when its security assumptions are broken
            - When attacker has code execution capability on the system hosting the vault server
            - When vault admin is an insider threat
            - Memory analysis of running vault to extract secrets
    - **Security evaluation of protocols**
        - Worked on evaluatiing security of Prime protocol.
        - Highlight security concerns and attacks againt the protocol
        - Worked on drafting a security analysis paper
    - **Offensive Security/CTF training**
        - Gave presentations to Crimson Vista explaining CTF participation and general overview
        - Demo'd several CTF chalenges on binary exploitation and reverse engineering and explained solution in a presentation
        - Give training on reverse engineering and using Ghidra

Graduate Teaching Assistant @ Georgia Tech
Spring 2021 - Spring 2022

- **CS 4235/6035: Intro to Information Security;** during Spring 2021, Fall 2021, Spring 2022
- **CS 3251: Computer Networks;** during Summer 2021
  Responsibilites:
    - Grading exams and projects
    - Giving project briefings and exam reviews in lecture format
    - Office Hours and answering on student forum
    - Drafting exam and quiz questions

Research:

Npm package manager security for developers using metadata analysis (report | code)
Mohammad Zaid Khaishagi
May 2022

Analysis of Symmetric Key Authenticated Key Exchange Protocols
Mohammad Zaid Khaishagi, Anderson Kunho Kim
May 2022

Analysis of Browser Fingerprinting by fingerprintjs.com
Mohammad Zaid Khaishagi, Frank Li
August 2021

- Review of public github codebase of fingerprintjs.com to identify fingerprinting techniques used
- Focused on analysing webRTC fingerprinting, with identification of feature that could potentially be used as detection signature
- Discussed defence techniques against fingerprinting
- Analysed and discusssed Google Privacy Sandbox proposal

Analysis and Implementation of Browser Fingerprinting Techniques and Defenses
Kevin Valakuzhy, Mohammad Zaid Khaishagi, Yoon Jae Lee, Shea Wells, Guoqiang Zhang
May 2021

CTFs:

NSA Codebreaker 2022

- Particpiating in NSA Codebreaker 2022 as alumni of Gorgia Tech

- Supported by Crimson Vista

WREK CTF

- CTF competition hosted by Greyhats Cybersecurity club @ Georgia Tech
- Participated solo, without a team
- Ranked 77th place among over 500 teams. (Scoreboard Name: Z_team)

Country to Country (C2C) CTF

- Participated in Finals held on 1s August 2022
- Placed 7th place before the scoreboard was closed
- Cleared the qualifier round earlier in 2022

---

corCTF
Participated in the CTF competition to solve challenges

DiceCTF @ HOPE
Participated in the CTF with GreyhatsGT team (Greyhats Cybersecurity club @ Georgia Tech)

PwnedNoMore Blockchain CTF
Participated in Blockchain CTF hosted by PwnedNoMore.

- Exploited vulnerability in smart contracts
- Focused on Ethereum smart contracts

NSA Codebreaker Challenge 2021
Participated on Georgia Tech team. We achieved 1st place in 2021.

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

---

TKCTF 2021
TKCTF competition organised at Georgia Tech.

PicoCTF
Participated in picoCTF competition.

TryHackMe
Solar, exploiting Log4j vulnerability: Solved this and also gave a demo on this.

Projects:
(code for some projects is not published to prevent copying)

Secure Communication Protocols
Spring 2022

- Presentation on Cryptographic Analysis of TLS 1.3 Handshake Protocol
- Presentation on Message Franking for abuse reporting in Facebook's end-to-end encryption

---

Cybersecurity Practicum
Spring 2022

- Advising on Android IDS Security project
- Advising project on Cryptocurrency regulation, tax and inheritance policy

Binary Exploitation
Fall 2021

- Weekly CTF challenges to solve
- Used a variety of exploit techniques including Buffer overflows, Stack exploitation, Heap exploits, Remote binary exploits, fstring vulnerabilities, Shellcode injection, Return-oriented-programming (ROP).

PAXOS Consensus
Fall 2021

- Implemented PAXOS consensus algorithm between server
- Ensures consistency of operations performed across group of PAXOS servers

Sharded Key-Value Store
Fall 2021

- 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
- PAXOS consensus used among servers in each group

Distributed Security - Secure Shared Store
Spring 2021

- Work on implementing distributed systems security for a service with multiple nodes that allows for storage and retrieval of docs by multiple users
- Access control policies specified by owners of documents
- Clients can check-in, checkout, delete files
- Use of certificates to ensure secure communication between clients and server, and to authenticate sources of requests
- Implement trusted Certificate Authority, client nodes, and server; used OpenSSL library for certificates

Password Hardening
Spring 2021

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

Memorandum for National Security
Spring 2021 | link

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

Analysis of Proposed Federal Data Breach Notification Law
Spring 2021 | link

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

Corporate Policy for Supply Chain Cybersecurity
Spring 2021 | link

- Drafted Supply Chain Cybersecurity Policy for Salesforce
- Policies for Technology, Processes and People

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

Barrier Synchronisation
Fall 2020 | link

- Implemented barrier synchronization algorithms across parallel threads and CPUs over a computer cluster.
- Analysed the performance of these algorithms by running experiments and reported findings
- Used OpenMP and MPI

Intro to Info Sec
Fall 2020 | link

- Malware Analysis using Cuckoo
- Attack weak RSA keys generated with bad randomness giving factorisable keys (based on this)
- Attack vulnerable broadcast RSA encryption using Chinese Remainder Theorem (Håstad's broadcast attack)

Ethereum State Channel game
2019 | link

- State channel tic-tac-toe game with escrow feature and conflict resolution
- Uses Ethereum chain; and has protocol diagram on Github

Blockchain projects
2018-19

- Hyperledger implementation of Glassdoor (link)
- DApp on NEM blockchain (link)
- DApp on Ethereum for storing tenancy records(link)
- Simple Blockhain application (link)

Articles:

- **Ghidra Tutorial Series**
  1. Ghidra Tutorial: Introduction
  2. Ghidra Tutorial: Usage
- Cryptographic Hash function SHA-512
- Intro to Blockchain

Activities:

- Greyhats Cybersecurity Club @ Georgia Tech
- Volunteering at Masjid Al-Farooq, Atlanta