HAMZA ALKOFAHI

Assistant Professor at Jordan University of Science & Technology

@ hoalkofahi@just.edu.jo +962 2 7201000 - Ex: 22481 Amman, Jordan linkedin.com/in/hkofahi github.com/hkof

EXPERIENCE

Assistant Professor - Software Engineering Department

Jordan University of Science & Technology

Sep 2020 – Present Irbid, Jordan

- **Teaching**: Software Security, Software Testing, Software Requirements Engineering (restructured the course), Object-oriented Programming, C/C++ Programming, Introduction to IT
- **Graduation Project Supervisor**: supervised more than five projects indifferent domains, such as Critical Infrastructure Protection, Resource Management, and Information System Management.

Graduate Research Assistant - College of Engineering

Auburn Cyber Research Center

Apr 2015 – Aug 2020 Auburn, Alabama

- Developed a novel approach to automate detecting business logic vulnerabilities from a black-box perspective.
- Designed a new approach to infer Business Rules from web applications only using its dynamic behavior.
- Reverse engineered Amazon Dash button to study the possibility of implanting permanent malware into its firmware.
- Taught a graduate-level course on **Software Reverse Engineering & Malware Analysis**. Received a **very good** in the student evaluation.
- Developed a Java-based framework for pentesting 3D printers, which I used to reverse engineer & attack Stratasys Dimension Elite 3DPrinter.
- Built the first open-source CMB file format decoder for Stratasys.printers.
- Designed an Arduino-based embedded system for automated car jamming detection.

Cyber Red Team Analyst - Office of Information Technology

Auburn University

Jan 2016 – Aug 2020 Auburn, Alabama

- Responsible for finding vulnerabilities in Auburn University web services. Detected several vulnerabilities ranging from critical to low and contributed to the patching process. Thanks for that; I got my Ph.D. expenses covered :D
- Lead a red team of grad & undergrad students responsible for finding vulnerabilities in Hexagon Safety & Infrastructure high-end solutions(used by governments and SPs across the globe).
- The team managed to detect different vulnerabilities, propose possible measures, and validate the security fixes.

Web Application Developer

DDAD for Information Technology

Jun 2013 – Sep 2013 Amman, Jordan

- Built links caching system for Zakzek servers.
- Implemented a fast content fetcher module to extract a content summary of web pages.
- Implemented and integrated new interface components.

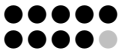
SKILLS

Unix/Linux | Android | Windows

Java | C/C++ | C# | Python | Assembly (ARM vs x86) | JS | SQL

Software Development | Web Development | Mobile Development | Reverse Engineering | Application Security | Vulnerability Assessment | Kernel Development | Problem Solving | GIT | OO Design | Design Patterns | Cryptography | Network Programming | Parallel Computing

Arabic
English



EDUCATION

Ph.D. in Software Engineering

Auburn University - GPA: 3.81

Jan 2017 – Summer 2020

Dissertation Topic: "**Towards Detecting Business Logic Vulnerability: Business Rules Mining through HTTP Traffic**"

M.Sc. in Software Engineering **Minor** in Information Assurance

Auburn University - GPA: 3.81

Jan 2015 – Dec 2016

B.Sc. in Software Engineering

Jordan University of Science & Technology - GPA: 3.7

Aug 2009 – May 2013

HONORS & AWARDS

- Departmental Award for the best project at AU Graduate Engineering Research Showcase 2016.
- Received Best Bachelor Graduation Project in the SE Dep. at JUST (2013).
- Achieved first place at NYUAD International Hackathon 2011.
- Achieved third place in Microsoft Jordan Imagine Cup Finals 2011.

PROJECTS

Towards Detecting Business Logic Vulnerability: Business Rules Mining through HTTP Traffic

Auburn University

Jan 2017 - Mar 2022

Business logic vulnerabilities can be considered one of the most challenging flaws to detect due to their nature and mainly the absence of any up-to-date business rules defining the system's expected behavior. My research focuses on automating the process of business rules extraction based on web applications' dynamic behavior. The proposed solution adapts process mining techniques and machine learning to extract candidate business rules and use them to automate detecting potential business logic vulnerabilities. **Technologies**: Process Mining, Machine Learning, Burp Suite Extender, Java, SQLite.

PCB Information Extraction from Kernal-Space for Android

Auburn University

May 2019 - May 2020

In this project, I modified the Android kernel for Google Pixel 2 to enable module insertion at run-time. I also built a kernel module to collect Process Control Block(PCB) information from a specific process, which can be determined from the user-space through virtual filesystems(/proc). **Technologies**: C, Linux, Kernel Development, Shell Script.

Security Framework for Testing 3D Printers Security

Auburn University

Jan 2016 – Ongoing

I implemented a Java-based framework for pentesting 3D printers, which I used to reverse engineer Stratasys Dimension Elite 3D printer and developed several exploits that take advantage of weaknesses in the design of the communication protocol. Allowing an attacker to silently steal, replace & sabotage 3D models on the fly. I also built the first open-source parser for **CMB** file format, which is a format Stratasys slicing software generates for their 3D printers. **Technologies**: Reverse Engineering, Shell Scripting, Java, Network Programming, Multi-Threading, MITMA, Wireshark.

Hacking Amazon Dash Button

Auburn University

May 2016 - Aug 2016

We managed to dump the dash firmware by exploiting a buffer overflow (discovered by Hunz) vulnerability in the dash audio configuration channel. Then we reverse-engineered it to study the possibility of permanently reprogramming it to simulate a permanent malware attack on IoT devices. **Technologies**: ARM Assemble, C, Reverse engineering, Hardware Hacking.

Automated Security Testing for Critical Infrastructure Website Vulnerabilities

Auburn University

Apr 2015 - May 2016

This system is designed to scan a large scale of critical infrastructure websites, looking for flaws in the HTTPS protocol and reporting the results. Also, a management system is integrated to keep track and manage all the websites under test. **Technologies**: Shell Scripting, C#, ASP.NET, PHP, HTML, JS, Python, Open Source tools, SQL.

PUBLICATIONS

Journal Articles

- Fraiwan, Mohammad, Natheer Khasawneh, Hosam Ershedat, Ibrahim Al-Alali, and Hamza Al-Kofahi (2015). "A Kinect-based system for Arabic sign language to speech translation". In: *International Journal of Computer Applications in Technology* 52.2-3, pp. 117–126.

Conference Proceedings

- Alkofahi, Hamza, David Umphress, and Heba Alawneh (2022a). "Discovering Authorization Business Rules toward Detecting Web Applications Logic Flaws". In: *2022 International Arab Conference on Information Technology (ACIT)*. IEEE, pp. 1–7.
- – (2022b). "Discovering Conditional Business Rules in Web Applications Using Process Mining". In: *Information Integration and Web Intelligence: 24th International Conference, iiWAS 2022, Virtual Event, November 28–30, 2022, Proceedings*. Springer, pp. 90–97.
- – (2022c). "Preparing HTTP traffic for process mining". In: *2022 13th International Conference on Information and Communication Systems (ICICS)*. IEEE, pp. 142–148.
- Fogel, Benjamin, Shane Farmer, Hamza Alkofahi, Anthony Skjellum, and Munawar Hafiz (2016). "POODLEs, more POODLEs, FREAK attacks too: how server administrators responded to three serious web vulnerabilities". In: *Engineering Secure Software and Systems: 8th International Symposium, ESSoS 2016, London, UK, April 6–8, 2016. Proceedings 8*. Springer, pp. 122–137.
- Ershaed, Hosam, Ibrahim Al-Alali, and Hamza AlKofahi (May 2011). "An arabic sign language computer interface using the xbox kinect". In: Annual Undergraduate Research Conf. on Applied Computing.

Presentations

- Hamza Alkofahi (Aug. 2019). *What You Print Is Not What You Get Anymore: Mitm Attack On 3D Printers Network Communications*. Defcon 27, Hardware Hacking Village. URL: `https://bit.ly/2kuF9ZQ`.

REFEREES

Prof. Anthony Skjellum
@ University of Tennessee at Chattanooga
tony-skjellum@utc.edu
Professor of Computer Science and Chair of Excellence