Nicolas Alhaddad

E-mail : nhaddad@bu.com Website: http://www.github.com/nicolas3355

Education

PhD in Computer Science Jan 2018 — Present

Boston University

Teaching Fellow: Introduction to Computing Systems (Spring 2018). Applied Cryptography (Spring 2019). Network-Security (Fall 2019).

Sub Reviews(2020): 1 paper in CSF, 2 papers in ICDCS, 1 paper in Oakland.

MS in Computer Science May 2016 — Jan 2018 (transferred)

American University of Beirut

BS in Computer Science Sep 2012 — May 2016

American University of Beirut

Work experience

Boston University Jan 2018 — Present

Research Fellow

-**Proactive security in the cloud**

I had the chance to work on this project with Professor Azer Bestavros, Professor Mayank Varia, and Professor Haibin Zhang from the University of Maryland. Imagine having a sensitive secret stored on the cloud. Such a secret may be vulnerable to three kinds of attacks: (1) A hacker may compromise the server/s used. (2) A malicious party may acquire a virtual machine (VM) running on the same hardware and use that VM to expose or attack the hypervisor or hardware of the host. (3) The cloud provider could attempt to steal your secret.

One possible way to fight these attacks would be to keep the secret distributed among many instances using Shamir's Secret Sharing. This approach can be combined with MTD by continuously requesting new VM instances while migrating and changing the shares between these instances. If such migrations happen frequently enough, the task of an attacker becomes significantly harder: not only does the attack need to identify and compromise all instances storing a share, but it also needs to do so in a short period of time before shares and instances change. I am currently working on an implementation of these ideas using OpenStack.

-**Conclave**: Secure Multi-Party Computation on Big Data

Secure multi-party computation (MPC) allows mutually distrusting parties to run joint computations without revealing any private data. Unfortunately, current MPC algorithms scale poorly with the size of the data, which makes MPC on "big data" prohibitively slow and inhibits many use cases.

Most analytics queries, however, can maintain the end-to-end security guarantee without running entirely under MPC's cryptographic techniques. Conclave is a query compiler that automatically accelerates such queries by transforming a relational query into a combination of scalable, local, cleartext processing and small, isolated MPC steps.

Working with Prof. Kfoury and Prof. Lapets, I formally defined the syntax and the semantics of the domain specific query language of conclave. I also worked on static execution cost analysis for statically reasoning about functional properties of conclave programs; with the goal of choosing the best conclave back-end based on message complexity performance.

Conclave Web allows multiple analysts/researchers to compute aggregate statistics over datasets uploaded to dataverse without revealing any private data to one another, except for what can be inferred from the output. Conclave web uses conclave to generate the appropriate mpc code and offload to it to containers that run the computation jointly. Conclave web uses openshift and kubernetes for that purpose. Conclave web is currently being deployed on the Massachusetts Open Cloud.

I worked with Prof. Mayank Varia on designing and implementing the key management system of conclave web.

American University of Beirut — Jan 2017 — Jan 2018

Research Assistant

I worked with Professor George Turkiyyah on High Performance Surgical Simulation. This project was in collaboration with faculty members from North Carolina University at Chapel Hill and Qatar Robotic Surgery Center.

Surgical simulation are an extremely challenging types of simulations. They require high performance and absolute robustness. Surgical simulators must be realistic and consistent both geometrically and mechanically. A single error regardless of its location and time may result in an incorrect and visually distracting simulation.

The long term aim of the project is to simulate surgical operations on bodily organs modeled as 3D tetrahedral meshes. This can be used for either procedure rehearsal or training. I worked with another researcher on the geometric model for cutting tetrahedral meshes efficiently. We defined a mathematical framework for representing, analyzing, and evaluating different nonlinear cuts on the mesh. We then implemented our ideas by creating a C++ library for that purpose.

Interactivelife — Aug 2015 — Jan 2017

Senior Full-Stack Software Engineer

I worked on the android platform side, building a highly customizable SDK that enables the build of various different applications with no time, coupled with automated scripts that creates/updates/builds all the different apps. Complex apps can extend behavior and customize the UI by attaching plugins or extending SDK modules. Customizations are registered in the SDK using dependency-injection, annotation processing and the builtin Manifest Merger.

The SDK provides generic implementations for chat, live-streaming, billing, triggering, push-notifications, server communication and generic UI animations. We were able to serve 30+ apps with our generic platform.

I also participated in the design and development of a dynamic system that manages and auto-generates database schemas, UI for matching forms for the mobile apps, and code for validity tests and consistency checks on the data as it gets stored in the database or migrates between different components.

I helped maintain, configure, deploy, and scale the servers providing services and API. During these tasks I worked with letsencrypt, NFS , Amazon EC2, load balancers, wrk, wowza streaming engine, git bare, openfire, postgreSQL.

I met with clients to discuss business ideas and requirements and worked closely with management to provide insight on development decisions that fit the client requirements best. I transformed business ideas and requirements into viable code while integrating work between different local and remote members of the team. I also helped interview and recruit developers into to the company. During my work, I was assigned the position mobile development team manager, and was tasked to lead that team.

Institute for War & Peace Reporting — Jul 2014 — Jan 2015

Digital Security Officer/Software Developer

Description of Services/Scope of Work:

- Coordinating and contributing to the development of digital security applications
- Keeping up to date with international developments in the field of digital security
- Monitoring of current developments related to digital security in the Arab world
- Preparing of training material on digital security
- Training journalists and activists on the subject of digital security
- Writing of digital security related articles in English or Arabic
- Supplying advice to journalists and activists in the field of digital security
- Managing and operating secure web services

- Installing, maintaining and operating server applications
- Analyzing digital threats (virus attacks, hacks, etc) and testing apps
- Research on Digital Security

Miscellaneous projects

Most of these projects can be found on my Github account.

- Simulation of a packet traveling inside a network written in c++ using Omnet++ framework.
- A basic Social Network where you can share pictures, send personal messages and get notifications.
- Tutor finder website written in Python flask, where students/tutors can schedule tutoring sessions.
- A basic Vehicle detection algorithm written in processing that counts cars, it was part of a bigger project to enhance traffic lights performance.
- Nasty blocker is an android application that blocks phone numbers by answering the incoming calls and hanging out really fast, making the caller loose money.
- CyberArabs is a cross platform app written in Html5 and Javascript that uses Cordova, the app is just an rss parser with push notifications and offline storage. The app was released on android google play.

Interests

- Cybersecurity, Applied Cryptography (includes multi-party computation), cryptocurrencies and smart contracts.
- Distributed Systems.
- Formal Verification.

Skills

- Languages: Bash, C/C++, Gallina(Coq), Java, Javascript, PHP, Python.
- Web and Mobile Development(Android).