

SAJJAD ARSHAD

(617) 390-3316 ◊ msarshadir@gmail.com ◊ <https://sajjadum.github.io/>

Google MTV, 1667 Plymouth Street, Mountain View, CA 94043

EDUCATION

Northeastern University	PhD in Cybersecurity	April 2019
Shahid Beheshti University	MS in Computer Engineering	January 2011
University of Tehran	BS in Computer Engineering	August 2008

TECHNICAL STRENGTHS

OS	Linux (Mint, Ubuntu, Debian, Fedora), Windows (XP, 7), QNX
Languages	C/C++, Python, Java, Shell/Bash Script, Go, Rust, Assembly, Ruby, Perl, C#
Web	HTML, JavaScript, CSS, Browser Extensions, PHP, NodeJS, J2EE, ASP.NET, JSP
Java	Maven, RMI, JDBC, Struts, Hibernate, Applet, SAX/DOM, Swing/AWT/SWT
Database	Oracle, MySQL, MS SQL Server, PostgreSQL, SQLite
Networking	nslookup, dig, Wireshark, tcpdump, netcat, (Raw) Socket Programming
Security	IDA Pro, Binary Ninja, Pwntools, AFL, GDB, NMap, Snort, Metasploit, Burp Suite
Big Data	Hadoop/MapReduce, Spark, Cassandra
ML	WEKA, SciPy, Scikit-Learn, R, MATLAB
SCM	Git, Subversion, Mercurial
Virtualization	VirtualBox, Docker, QEMU/KVM, VMware
IDE	vim, IntelliJ IDEA, Eclipse, Visual Studio

SUMMARY

My research is concerned with improving the security of computer systems through application of secure design principles and integration of defensive techniques such as attack detection, prevention, and recovery. Some domains I am active in are conducting web security & privacy measurement, static & dynamic program analysis, binary analysis (e.g, reverse engineering, exploit development), and malware detection (e.g., Botnet, Ransomware).

Specifically, my research focuses on large-scale web security measurement, primarily using browser instrumentation and distributed crawling. I am the founder of the DeepCrawling, an evolutionary crawling platform based on Chrome browser that provides a deeper look into the ecosystem of content inclusion on the Web. I have also participated in a number of CTF competitions, and have published several "technical" writeups. Thus far, I have published several peer-reviewed papers in major conference proceedings, including USENIX Security, NDSS, WWW, ACSAC, RAID, IMC, FC, and IEEE.

During my career, I have built an array of advanced technical skills, developed valuable skills in communication, management, and leadership, and gained good verbal and written communication skills that allow me to effectively present the information in a clear and concise manner.

SECURITY & NETWORKING EXPERIENCE

Google, Mountain View, CA <i>Security Software Engineer</i>	May 2019 - present
---	--------------------

· Fighting Android Malware.

Northeastern University, Boston, MA <i>Research Assistant</i>	September 2013 - April 2019
---	-----------------------------

- Evaluated the effectiveness of type-based and points-to analysis-based control flow integrity (CFI) techniques by focusing on grsecurity's Reuse Attack Protector (RAP) and LLVM-CFI.
- Developed a large-scale and distributed crawling platform based on Chrome debugging protocol.
- Developed a set of static and dynamic analysis (e.g., fuzzer) techniques for detection of algorithmic complexity vulnerabilities in Java programs by instrumenting JVM as well as using Java bytecode analysis framework such as ASM and Soot. This work resulted in [CVE-2018-1517](#).
- Conducted a large-scale measurement on Web Cache Deception attack on popular CDNs such as Akamai and Cloudflare.
- Used Amazon Web Services (AWS) for processing Common Crawl dataset for measurement of relative path overwrite (RPO) vulnerability in the wild.
- Modified Chromium code base (C++) to create an instrumented browser for multiple large-scale web security measurement studies including detection of malicious web pages/domains, advertisement injection by browser extensions, malvertising, and outdated JavaScript libraries.
- Conducted extensive research on ecosystem of online/web advertising and its related privacy/security issues (e.g., cookie matching, re-targeted ads).
- Conducted extensive research on security problems of web protocols and client-side technologies (e.g., JavaScript, CSS, HTML5, browser extensions).
- Built a malware analysis infrastructure based on Cuckoo sandbox and Windows for large-scale and automated detection of Ransomware.
- Designed and implemented a content distribution network (CDN) using DNS redirection, user-space threads in Linux, a file system using FUSE library in Linux, and a secure chat system using built-in Java security framework.
- Participated in a number of CTF competitions, and developed an array of advanced technical skills in binary exploitation, pwning, and reverse engineering (e.g., IDA Pro, Binary Ninja, GDB), and published detailed write ups.

Mozilla Corporation, Mountain View, CA
Security Research Intern

June 2017 - August 2017

- Designed and implemented a measurement study to analyze the adoption of TLS 1.3 protocol by middleboxes in enterprise networks. Basically, we developed a Firefox add-on (JavaScript), shipped it to a sample of Firefox users, and collected the experiment results in Telemetry platform (Spark) for further offline analysis.
- Modified Mozilla Firefox browser code base (C++) to enable flexible way for configuring TLS/HTTPS connections by developers.

Verisign Inc., Reston, VA
Security Research Intern

May 2016 - August 2016

- Built a system to analyze large amounts of HTTP traffic using machine learning techniques (e.g., clustering) to detect legitimate web clients in order to block DDoS attacks (R and Python's machine learning libraries).
- Gained a deep knowledge of DNS and related protocols (e.g., DNSSEC, Whois).

Amnafzar Co., Tehran, Iran
Senior Security Engineer

October 2011 - August 2013

- Designed and implemented a large-scale log management system (SIEM) using Java, MySQL, Hadoop, and MapReduce to collect and process large amounts of logs sent from various devices (e.g., Firewalls, IDSes/IPSes, Desktops, Servers) in an enterprise network.
- Worked on different components of Security Operation Center (SOC), Unified Threat Management (UTM), Firewall, and IDS/IPS.

Shahid Beheshti University, Tehran, Iran
Research Assistant

September 2008 - January 2011

- Conducted extensive research on security and performance evaluation of shared web hosting solutions for Apache web server in Linux installations.
- Designed and implemented a novel approach using machine learning techniques to detect Botnets by analyzing the network communications between the bot infected hosts and C&C servers. The whole system is implemented in C++, and WEKA tool is used for clustering purposes.
- Built a large-scale system for analyzing Pcap files to generate netflows for detecting attack patterns.

SOFTWARE & DATABASE EXPERIENCE

IT Center at University of Tehran, Tehran, Iran

March 2011 - September 2011

Senior Software Engineer

- Designed an integrated database schema for student and personnel information. In particular, a central database was built to integrate all the data scattered across databases (Oracle and MS SQL Server) of legacy systems.

Tejarat Bank, Tehran, Iran

March 2009 - September 2009

Software Engineer

- Designed a core banking system to integrate legacy banking systems (DB2, Oracle, MS SQL Server).

University of Tehran, Tehran, Iran

January 2007 - December 2008

Research Assistant

- Worked in different aspects of database including data warehousing, applications of data mining algorithms, classification and clustering techniques, and information retrieval.
- Developed multiple web applications during my course works using various technologies (e.g., PHP, J2EE, Struts, Hibernate, ASP.NET, MySQL, MS SQL Server).

Iran Khodro Industrial Group (IKCO), Tehran, Iran

January 2007 - December 2007

Software Engineer

- Designed a system based on multi-agent and expert systems to control car product line automatically.

Raydana Co., Tehran, Iran

June 2005 - March 2006

Software Engineer

- Designed and implemented a web-based ERP system using ASP.NET, C#, and MS SQL Server.

Mahkar System Engineers Co., Tehran, Iran

September 2004 - June 2005

Software Engineer

- Developed a centralized banking system for Maskan bank using Delphi and Oracle.

PUBLICATIONS

Cached and Confused: Web Cache Deception in the Wild

Seyed Ali Mirheidari, **Sajjad Arshad**, Kaan Onarlioglu, Bruno Crispo, Engin Kirda, William Robertson
USENIX Securit Symposium, 2020

A Longitudinal Analysis of the ads.txt Standard

Mohammad Ahmad Bashir, **Sajjad Arshad**, Engin Kirda, William Robertson, Christo Wilson
ACM Internet Measurement Conference (IMC), 2019

Understanding and Mitigating the Security Risks of Content Inclusion in Web Browsers

Doctor of Philosophy (PhD) Thesis

Khoury College of Computer Sciences, Northeastern University, 2019

On the Effectiveness of Type-based Control Flow Integrity

Reza Mirzazade, Saman Jafari, **Sajjad Arshad**, William Robertson, Engin Kirda, Hamed Okhravi
Annual Computer Security Applications Conference (ACSAC), 2018

How Tracking Companies Circumvented Ad Blockers Using WebSockets

Mohammad Ahmad Bashir, **Sajjad Arshad**, Engin Kirda, William Robertson, Christo Wilson
ACM Internet Measurement Conference (IMC), 2018

How Tracking Companies Circumvent Ad Blockers Using WebSockets

Muhammad Ahmad Bashir, **Sajjad Arshad**, Engin Kirda, William Robertson, Christo Wilson
IEEE S&P Workshop on Technology and Consumer Protection (ConPro), 2018

Large-Scale Analysis of Style Injection by Relative Path Overwrite.

Sajjad Arshad, Seyed Ali Mirheidari, Tobias Lauinger, Bruno Crispo, Engin Kirda, William Robertson
The Web Conference (WWW), 2018 (Honorable Mention)

Thou Shalt Not Depend on Me: Analysing the Use of Outdated JavaScript Libraries on the Web

Tobias Lauinger, Abdelberi Chaabane, **Sajjad Arshad**, William Robertson, Christo Wilson, Engin Kirda
Network and Distributed System Security Symposium (NDSS), 2017

Recommended For You: A First Look at Content Recommendation Networks

Mohammad Ahmad Bashir, **Sajjad Arshad**, Christo Wilson
ACM Internet Measurement Conference (IMC), 2016

Identifying Extension-based Ad Injection via Fine-grained Web Content Provenance

Sajjad Arshad, Amin Kharrazi, William Robertson
International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2016

Tracing Information Flows Between Ad Exchanges Using Retargeted Ads

Mohammad Ahmad Bashir, **Sajjad Arshad**, William Robertson, Christo Wilson
USENIX Security Symposium, 2016

UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware

Amin Kharraz, **Sajjad Arshad**, Collin Muliner, William Robertson, Engin Kirda
USENIX Security Symposium, 2016

Include Me Out: In-Browser Detection of Malicious Third-Party Content Inclusions

Sajjad Arshad, Amin Kharraz, William Robertson
International Conference on Financial Cryptography and Data Security (FC), 2016

Alert Correlation Algorithms: A Survey and Taxonomy

Seyed Ali Mirheidari, **Sajjad Arshad**, Rasool Jalili
Symposium on Cyberspace Safety and Security (CSS), 2013

A Comprehensive Approach to Abusing Locality in Shared Web Hosting Servers

Seyed Ali Mirheidari, **Sajjad Arshad**, Saeidreza Khoshkdahan, Rasool Jalili
IEEE Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2013

Comparison of Routing Protocols in Mobile Ad-Hoc Wireless Networks

Sajjad Arshad, Abbas Naderi
Journal of AWERProcedia Information Technology and Computer Science (ITCS), 2013

Two Novel Server-Side Attacks against Log File in Shared Web Hosting Servers

Seyed Ali Mirheidari, **Sajjad Arshad**, Saeidreza Khoshkdahan, Rasool Jalili
IEEE Conference for Internet Technology and Secured Transactions (ICITST), 2012

Performance Evaluation of Shared Hosting Security Methods

Seyed Ali Mirheidari, **Sajjad Arshad**, Saeidreza Khoshkdahan
IEEE Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2012

An Anomaly-based Botnet Detection Approach for Identifying Stealthy Botnets

Sajjad Arshad, Maghsoud Abbaspour, Mehdi Kharrazi, Hooman Sanatkar

IEEE Conference on Computer Applications and Industrial Electronics (ICCAIE), 2011

A Disk Scheduling Algorithm Based on ANT Colony Optimization

Hossein Rahmani, **Sajjad Arshad**, Mohsen Ebrahimi Moghaddam

ISCA Conference on Parallel and Distributed Computing and Communication Systems (PDCCS), 2009