Sajjad **Pourali**

Cyber Security Specialist

sajjad@pourali.com | www.pourali.com | SajjadPourali | sajjadpourali | Sajjad Pourali

Summary

Pragmatic cybersecurity specialist with over 10 years of hands-on experience identifying and analyzing software vulnerabilities across various platforms. Expert in privacy analysis, vulnerability detection, and malware analysis, focusing on Android, Linux, and Darwin operating systems. Experienced in penetration testing, security assessments, and implementing secure protocols such as TLS 1.3. Passionate open-source contributor, creator of **Narrowlink** (500+ GitHub stars), a remote access tool. Led Narrowlink's development while conducting practical research on Android security and privacy. Practical and adept at tooling and creating prototypes, demonstrated through research projects. Completing a PhD in cybersecurity, presented practical research at prestigious conferences, including ACM CCS and USENIX.

Experience

Concordia University

Montréal, Canada

Research Assistant — *Sep. 2020 - Present*

- Applied eBPF for network traffic attribution of Android apps and forced forwarding proxy-agnostic apps to an intermediate proxy server.
- Leveraged large language models (LLMs) to identify unknown PII leakages in Android app network traffic.
- Designed a fully automated large-scale Android app privacy analysis pipeline using Python, incorporating dynamic analysis (API hooking, network analysis), automatic login, and app interaction support to analyze over 15k apps.
- Created a deep packet inspection tool to extract PII from network traffic.
- Discovered a security issue in Android's default TLS library and analyzed over 9k top apps in the Android ecosystem to identify vulnerable apps.
- Created a fully automated dynamic analysis tool to identify privacy leakages in Android background services.
- Developed an automated framework to identify custom encryption on the Android platform (e.g., additional encryption on top of existing standard protocols like encryption over TLS).
- Created a custom version of Android AOSP to add kernel-level app tracing features.
- Conducted manual NDK and SDK static code analysis of various Android applications to identify privacy exposures.
- Applied LLM to identify unpredictable PII leakages in network traffic of Android apps.
- Created various Magisk modules to facilitate dynamic analysis on Android devices.
- Implemented a hybrid PHP analysis tool based on AST to detect phishing kit backdoors.
- Led a team of over 6 students, providing guidance and mentorship to help them achieve their research goals.

Ericsson

Montréal, Canada

Research Intern — *May. 2021 - Sep. 2023*

- Creating tools to measure performance of the client version of LURK (Rustls based SGX-based cryptography service.) (May. 2023 - Sep. 2023)
- Adapted the Rustls library to create a prototype of the Ericsson SGX-based cryptography service for TLS 1.3 client. (May. 2022 - Sep. 2022)
- Creating tools to measure performance of the server version of LURK (OpenSSL based SGX-based cryptography service.) (May. 2021 - Sep. 2021)

APA Center of Mashhad

Mashhad, Iran

Senior Application Security Specialist — *Nov. 2013 - Apr. 2021*

- Established and lead internal research groups.
  - Web application security auditing, mobile application security auditing, and reverse engineering (malware analysis)
- Consulted and performed penetration testing of more than 380 web applications based on OWASP ASVS.
- Consulted and performed penetration testing of about 35 mobile applications based on OWASP ASVS/MASVS.
- Analyzed highly obfuscated malware samples using dynamic and static analysis approaches.
  - Sandbox and API hooking methods for dynamic analysis. - Static code analysis using radare2 and Binary Ninja.
- Conducted nearly 24 emergency responses to various cyber-attacks.
- Performed Reverse engineering and security analysis of SIP-T22P Yealink firmware.
- Implemented MySQL Exception Monitoring tool for Fuzzing Web Applications.

Web Application Penetration Tester — *Apr. 2009 - Nov. 2013*

- Consulted and performed penetration testing of more than 60 web applications based on OWASP ASVS.
- Network security assessment of Ferdowsi University of Mashhad.
- Research in HTTP authentication downgrading.

Skills

Application Security	Vulnerability detection and exploitation based on OWASP ASVS/MASVS
Reverse Engineering	x86/ARM static and dynamic analysis (Linux, Android, Darwin) to identify vulnerabilities, and malware analysis
Network	Advanced socket programming, Various application layers (e.g., H1/2, TLS 1.3, QUIC), Linux kernel network
Forensics	Web application, Mobile application, Network, Memory, Linux
Programming	Rust, Python, Assembly (x86/Arm), C, JavaScript, PHP, SQL, Shell Scripting, Latex
Technologies	eBPF, AOSP, Intel SGX (Apache Teaclave), LLM

Select Open Source Projects

Narrowlink - Secure connectivity between devices across restricted networks *Homepage* *Github*

- Conceptualized and developed Narrowlink as a remote access tool, considering zero-trust network access principles.
- Engineered robust mechanisms for traversing NATs and firewalls, facilitating direct peer-to-peer communication using the QUIC protocol.
- Integrated advanced security features, including end-to-end encryption and authentication using XChaCha20-Poly1305 and HMAC-SHA256.
- Utilized Rust programming for its performance and safety benefits.
- Authored comprehensive user documentation and provided ongoing support to users.
- Actively engaged with the user community to gather feedback, prioritize feature requests, and incorporate improvements.
- Applied cutting-edge research in cyber security to enhance the security and performance of Narrowlink.

IpStack - Asynchronous lightweight userspace implementation of TCP/IP stack for Tun *Github*

- Implemented a userspace TCP/IP stack from scratch for the Rust programming language, integrating it with the TUN interface

Select Publications

Racing for TLS Certificate Validation: A Hijacker's Guide to the Android TLS Galaxy *Philadelphia, USA*

USENIX '24: 33rd USENIX Security Symposium *Aug 14-16. 2024*

Hidden in Plain Sight: Exploring Encrypted Channels in Android apps *Los Angeles, USA*

CCS '22: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security *Nov 7-11. 2022*

Education

Concordia University *Montréal, Canada*

Doctor of Philosophy in Information and Systems Engineering *Sep. 2020 - Dec. 2024 (Expected)*

- **Thesis**: Towards a Comprehensive Android Privacy Analysis with a Dynamic Analysis Approach (Ongoing)

ImamReza University *Mashhad, Iran*

Master of Science Programs in Secure Computation *Sep. 2017 - July. 2020*

- **Thesis**: Designing a Framework for Security Assessment in the Iot Application Layer

Khavaran Institute of Higher Education *Mashhad, Iran*

Bachelor of Software Engineering *Jan. 2014 - Nov. 2016*

- **Thesis**: Designed An Open-source Penetration Testing Framework With A Pipeline And Multi Thread Approach

Honors & Awards

Capture the flag competition

2019	**1st Place**, NSec 2019 Hacking Competition	*National,Iran*
2018	**4th Place**, ASIS CTF Finals 2018 Hacking Competition	*CTFtime*
2018	**4th Place**, SharifCTF 8 Hacking Competition	*CTFtime*
2018	**5th Place**, nullcom HackIM 2018 Hacking Competition	*CTFtime*
2018	**6th Place**, RITSEC CTF 2018 Hacking Competition	*CTFtime*
2016	**1st Place**, 7th international SharifCTF Hacking Competition	*CTFtime*
2016	**2nd Place**, Blaze CTF 2016 Hacking Competition	*CTFtime*

Select Discovered Vulnerabilities

2020	**CVE-2020-5188**, File upload vulnerability in DNN (DotNetNuke)	*NIST - Medium*
2020	**CVE-2020-5187**, Zip Slip vulnerability in DNN (DotNetNuke)	*NIST - Medium*
2020	**CVE-2020-5186**, Cross-site Scripting (XSS) vulnerability in DNN (DotNetNuke)	*NIST - Medium*
2014	**CVE-2014-4424**, SQL injection vulnerability in Wiki Server in Apple OS X Server	*Apple Apple Apple*
2013	**CVE-2013-5117**, SQL injection vulnerability in the ZLDNN DNN-Article module for DotNetNuke	*NIST - SecLists*
2013	**CVE-2013-4649**, Cross-site Scripting (XSS) vulnerability in DNN (DotNetNuke)	*NIST - PacketStorm*
2013	**CVE-2013-0722**, Stack-based buffer overflow in Ettercap	*NIST - RedHat*
2012	**CVE-2012-0389**, Cross-site Scripting (XSS) vulnerability in MailEnable	*NIST - Tenable*