

ROBERT MOONEY

email: rjmooney@gmail.com

web: <https://impetus.us/>

SEATTLE, WASHINGTON
UNITED STATES OF AMERICA

Seasoned engineer and security consultant with a penchant for design, assurance, rapid prototyping, and product development. Penetration tester, software developer, security analyst and researcher. Looking for a role which encompasses the aforementioned in which to build and offer services to protect critical assets. US Citizen.

RELEVANT WORK EXPERIENCE

Principal Technical Lead, Block 2023

Lead Security Software Engineer (L7) of InfraSec authorization infrastructure. Primary focus on architecture, planning, and design of an evolution of the zero-trust mesh infrastructure for both workforce and workload traffic. Simplified client access story. Emphasis on mentorship of junior engineers. Technologies include AWS AVP, Lattice, Envoy, and various client-side mesh tools including ghostunnel, curl, and proprietary tools and libraries. GoLang and C.

Principal Security Architect/Engineer/Manager, Coupang 2021-2022

Product Security team lead, architect, and engineer. Drove the Log4Shell vulnerability incident response company wide. Developed the application security bug bar. Co-created the vulnerability management program including ~90% of the in-use metrics and KPIs. Developed the product security incident response procedure. Static analysis rules composition and tuning. Designed, implemented (Bash, Python, Java, Groovy), and deployed SAST and container security tool integration across a diverse set of team-managed CI/CDs pipelines. Application security architecture design, threat modeling, and implementation/code reviews.

Principal Security Engineer, Casaba Security 2009-2021

Software and network security consultant responsible for the analysis, design, and testing of software and infrastructure security for various clients. Lead penetration tester. Co-author and project manager of patented intellectual property. Led development of a semantic analysis engine, developed a SAST/DAST orchestration system written in C#/PowerShell, led development of CAPTCHA system used by Bing Games on Microsoft Azure, contributor to a passive Web security analysis tool, developed custom fuzzers for protocols including TLS v1.3, security track speaker, multiple contributions to the Microsoft Security Development Lifecycle.

Software Security Engineer, Microsoft 2005-2008

Software engineer on the Forefront product suite. Responsible for the design and implementation of several client features including network discovery, threat metadata acquisition, and anti-malware scan scheduling. Windows services and other code written in C++ and C#. Engaged with Program Management early and often to influence design direction. Security subject matter expert, mentor, threat model development and review. Owned and shipped multiple products over multiple releases.

Research Software Engineer, Internet Security Systems 1997-2000

Member of the ISS X-Force. Developed and maintained the first commercial security vulnerability database on the Web. Performed security vulnerability research, implemented numerous network scanner and network IDS checks and signatures. Maintained website backend. Implemented the first mechanism to avoid TCP/IP stack fingerprinting.

WORK/LIFE BALANCE

Avid rower and backcountry snowboarder. Aspiring private pilot; aspiring RF and electrical engineer. Strong interest in security, networks, protocols, and software systems. Fascination with particle physics, business, finance, investing, and law. Licensed amateur radio operator.

TECHNOLOGIES

Python/Ruby
C/C++/GoLang
Bash
macOS
Linux
Windows
Microsoft Azure
Amazon Web Services (AWS)
Google Cloud Platform (GCP)

APPLICATIONS

vim, vscode
nmap, nessus, etc.
tcpdump, etc.
make, clang, etc.
git, docker, k8s
afl, afl+, peach
burp suite + various SAST/DAST tools

PROJECTS

Kernel-based TCP/IP stack fingerprint avoidance module in C; Digital audio extraction tool w/ CDDDB support for BSD in C; Web application firewall in C++; Contributions to multiple open-source projects including OpenBSD: ftp-proxy, identd; Packet construction and visualization tool for Windows written in C#; SSH file manager for Windows written in C++; SAX XML parser written in C++; High-port DCC send for BitchX IRC client; contact retrieval tool for Windows Mobile written in C++/DCOM; password brute-force tool written in Ruby; Various iterations of network discovery tools written in C, C++, Python, C#.

PATENTS

Principal Access Determination in an Environment - US 2017/0353453

Automated Threat Model Generation - US 2022/0207140

Licensing information, code samples, and FOSS commits/aliases available upon request.