Ayyappan Rajesh

Website | GitHub | arajesh@umassd.edu | LinkedIn | HackTheBox | +1(857) 437-9511

Summary:

An initiative-taking and talented cybersecurity researcher with extensive expertise in penetration testing, reverse engineering, and vulnerability research. Demonstrated ability to create and deliver impactful presentations and training sessions on automotive and IoT security, as well as effectively leading and managing teams. Noted for publishing several high-impact security vulnerabilities and committed to staying at the forefront of the ever-evolving cybersecurity landscape, continuously seeking out new challenges.

RELEVANT EXPERIENCE

ZScaler   Massachusetts

Offensive Security - Red Team Intern   *Feb 2024-current*
- Enhanced the security posture of ZScaler by conducting thorough red team operations and security assessments on the cloud, internal products, processes and facilities.

Cybastion   Washington DC
Cybersecurity Engineer Intern   *May 2023-July 2023*
- Conducted security assessments and designed testing plans for cybersecurity, forensics, and border surveillance solutions for West African governments.
- Evaluated and thoroughly tested open-source and commercial security tools for offensive and defensive operations.
- Conducted penetration tests, recommended and implemented cybersecurity and physical security policies within the company.

Northeastern University - Khoury College Signal Intelligence Lab

Research Assistant   *May 2023-December 2023*
- Researching wireless cybersecurity under Dr. Aanjhan Ranganathan
- Worked on projects relating to LoRa communication, Aviation, Unmanned Aircraft Systems security.

Car Hacking Village

Speaker, Organizer   *July 2022-Current*
- Created an in-person CTF for a Honda vehicle at DEFCON, the world's largest hacker conference which has over 30,000 attendees annually, to raise security awareness and demonstrate vulnerabilities in the automotive industry.
- Delivered a talk titled "Security like the '80s: How I stole your RF" on automotive security relating to CVE-2022-27254.
- Demonstrated the exploit to several DEFCON and BlackHat attendees, including the National Cyber Director, John C. Inglis and awarded the POTUS Office of the National Cyber Director challenge coin.
- Contributed toward the codebase for the Flipper Zero, allowing it to emulate certain vehicle key fobs.

Cyber Security Education Club at UMass Dartmouth   Massachusetts
President   *May 2022- current*
- In charge of organizing events for the CSEC (Cyber Security Education Club), a student-run organization at the University of Massachusetts Dartmouth, to raise cybersecurity awareness. Previously the Social Chair for CSEC.

Mass Cyber Center- Cybersecurity Mentorship Program   Massachusetts
Mentee   *March 2022-May 2022*
- Evaluated the Cyber Incident Response Plan for a large public research university using NIST.SP.800-61 and SIM3(Security Incident Management and Maturity model) framework, whilst being mentored by Mr. Sam Curry (CSO, Cybereason).
- Discovered and published a vulnerability in Honda vehicles which tracked as CVE-2022-27254 and interviewed on FOX11 News and ABC's Good Morning America show on key fob hacking.

NCIIPC (Govt. of India)   India-Remote
Cybersecurity Research & Development Intern   *September 2020-August 2021*
- Developed an easy-to-use framework/toolkit for security policy implementation and management of security risks in Linux Systems for Critical Information Infrastructure.
- Utilized open-source tools such as TripWire, Snort IDS, firejail, grapheneX, and SELinux and other proprietary tools to provide a comprehensive security solution, which decreased time to harden systems by 40%

SKILLS/INTERESTS

- **Programming Languages:** C++, C, C#, Objective C, Java, Bash, Python, Assembly
- **Technical skills:** Software Defined Radio, GNURadio, Penetration testing, Fuzzing, Reverse Engineering, Linux, CAN protocol, ESP32, Machine-to-Machine Communication(M2M)
- **Interests:** Automotive Cybersecurity, Wireless security and Signal Intelligence, IoT Security, CTFs (Capture the Flag), Secure -by-design engineering, Volunteering

---

Certificates – CompTIA Security+, (ISC)² CC, Intro to DFIR: The Divide and Conquer Process, LFS171x: Introduction to Hyperledger Blockchain Technologies, The Linux Foundation, Core Java NIIT, Programming in C++, Programming in C.

Achievements:

- 3 Published Critical CVE's
- Black Hat USA 2022 and 2023 Student Scholarship
- Top 50 on the HackTheBox Hall of Fame
- Top 14% in the DoE's CyberForce 2020

EDUCATION

University of Massachusetts Dartmouth   North Dartmouth, MA
College of Engineering   *Class of 2024*
Bachelor of Science in Computer Engineering with a concentration in Cyber Security

PROJECTS/ PRESENTATIONS

<u>AutoISAC Training</u>   Michigan
Feb 2024
Presented research and co-taught a course on SDR and Wireless security to over 20+ professionals working in the cybersecurity industry.

<u>United States Secret Service, Critical Systems Protection</u>   HQ, Washington DC
October 2023
Presented and provided training to 30+ special agents from the Critical System Protection Division's Cybersecurity Security Operations Center (CSOC) on Automotive, IoT and wireless security.

                                                                     Field Office, Boston, Massachusetts
May 2023
Presented research on emerging tools used to bypass physical access control systems and methods to detect and harden access control systems vulnerable to such attacks.

<u>CyberAuto 2023</u>   Warren, Michigan
October 2023
Delivered presentations and live demonstrations on automotive cybersecurity research, showcasing attacks to diverse audiences including students, OEMs, and government officials from law enforcement and national laboratories. Participated in an intensive weeklong training program, followed by a comprehensive 48-hour penetration test on vehicles to uncover potential vulnerabilities and zero-day exploits.

<u>Leetcon</u>   Bangladesh
May 2023
Presented automotive cybersecurity research to 500+ attendees at Bangladesh's first international cybersecurity conference.

<u>BlackHat MEA</u>   Riyadh, Saudi Arabia
November 2023
Led active attacks and demonstrations at the Car Hacking Village to 30,000 attendees and 200+ global information security influencers at the first BlackHat event in Saudi Arabia over the span of 3 days.

<u>Marist College</u>   *New York*
Capstone Guest Speaker   *October 2022*
Presented work on red teaming and physical penetration testing at Marist College for students graduating from their bachelor's Cybersecurity.

<u>ROOTCON 17</u>   *Philippines*
October 2022
Presented automotive cybersecurity research to attendees at Philippines's premier cybersecurity conference.

CVE-2022-27254   *March 2022*
Discovered vulnerability in Honda Remote Keyless Entry Systems which affect two generations of models worldwide and acknowledged by several individuals from the industry and govt.

CVE-2023-22906   *July 2023*
Acknowledged by the CTO and CERT-In for discovery of critical vulnerability in Hero Electronix Qubo IoT doorbell, one of the largest which allowed for an attacker to **remotely execute malicious code**, affecting user privacy and the ability to use the device in a botnet. Coordinated with the Indian Cyber Crime Coordination Center(I4C) to raise awareness amongst the industry to encourage secure by design approach.

CVE-2023-41442   *August 2023*
Discovered critical vulnerability and acknowledged by CERT-In which allowed an attacker **to remotely view and control** (through CAN injection**) 600+ connected vehicles** in India, which used the Tor IoT solution. Coordinated with I4C, Dept. of Telecommunications (DoT) and Center for Development of Telematics(C-DoT) to highlight the impact of end user privacy and importance of regulation for connected automotive and cyber physical systems.