General Motors
Vehicle Cybersecurity Testing Engineer

General Motors is hiring a full-time Vehicle Cybersecurity Testing Engineer. This position involves performing security research via vulnerability assessments, embedded penetration testing, reverse engineering, and product security testing on vehicle systems and components. For more information and to learn how to apply, please contact Stephanie at plum@vt.edu.

TASKS AND RESPONSIBILITIES:

- Perform security research against Automotive Electronic Control units, vehicle networks and their associated diagnostic and service tools to identify security vulnerabilities.
- Perform embedded security testing activities, both automated and manual, to identify and exploit vulnerabilities in embedded components, systems, applications, and network components in an effort to reduce risk and improve product security.
- Document technical and logical security findings identified during the security assessments, and report them in a timely manner.
- Make recommendations concerning the overall improvement of vehicle security posture through the proactive discovery of security weaknesses using penetration-testing techniques.
- Provide guidance on security controls and assist in troubleshooting problem areas as needed.
- Collaborate and share knowledge with team members via formal and informal methods on a regular basis.
- Perform testing using defined methodologies and a combination of automated and manual tools.
- Execute tests independently or work as part of a testing team, taking direction from team lead(s) and executing directives in a thorough and timely fashion.
- Demonstrate critical thinking and creative analysis techniques in distilling test results, eliminating false positives and providing actionable recommendations for mitigation.
- Perform additional incidental duties as assigned by management or job responsibilities.

REQUIRED SKILLS:

- Bachelor's degree (B.A. or B.S.) from four-year college or university; or equivalent training, education and experience.
- A hands-on self-starter with an innate aptitude for technology and is constantly looking to broaden their technical horizons.
- Very strong verbal and written communication skills.
- Ability to work collaboratively with individuals within both the technical community, IT leadership, and the business.
- Ability to work constructively as an individual or in groups with minimal supervision.
- Ability to work in a team environment with aggressive deadlines and multiple priorities while staying a team player.

PREFERRED SKILLS:

- Previous security research experience.
- Experience conducting reverse engineering to find security vulnerabilities in embedded devices and their associated firmware.
- Competence with security testing tools and procedures for information security.
- Extensive technical computer/network/vehicle knowledge and understanding of computer/vehicle hardware, software, networks, communications and connectivity.
- Experience with Software Defined Radios and RF Communications.
- Knowledge of the CAN serial data communication systems.
- Experience with and/or knowledge of technologies used to secure embedded systems.
- Proficiency in at least two of the following languages- C, C++, C#, Python, Ruby, Perl, shell scripting, Powershell.

Stephanie Plum  |  Program Coordinator, Outreach and Education
Hume Center for National Security and Technology  |  Virginia Polytechnic Institute and State University
1991 Kraft Drive, Suite 2019  |  Blacksburg, Virginia 24061  P: 540.231.8524