PROBLEM TITLE
Fuzz Better

CHALLENGE
MCTSSA Cybersecurity Engineers need to increase their ability to identify program vulnerabilities in order to improve the efficiency of cyber vulnerabilities testing.

BACKGROUND
Fuzzing, one of the first steps in identifying a system's cyber vulnerabilities, is the process of feeding malformed data to the program to trigger a fault, or unexpected behavior in that program. Two different forms of fuzzing exist: smart and dumb. Smart fuzzing requires a cybersecurity engineer to know the software well enough to understand how a program regularly communicates. The engineer can use that knowledge to feed targeted malformed data to exploit that communication channel. On the other hand, dumb fuzzing sends random data to try and exploit communication channels.

MCTSSA's cybersecurity engineers currently check Command and Control (C2) for cyber vulnerabilities using both dumb and smart fuzzing. While they attempt to conduct smart fuzzing, programs can run tens of thousands of embedded software. This makes it difficult for engineers to learn from source code and know-how to exploit it. Additionally, MCTSSA engineers only have about two or three weeks to test a program (although they may test a program up to twice a year).

Therefore, it is critical that cybersecurity engineers can conduct dumb fuzzing more efficiently. While the current process is manual, the department is considering autonomous tools to allow them to feed random data continuously in order to find as many vulnerabilities as possible. Once programs are tested, MCTSSA cybersecurity engineers send the vulnerability information back to program offices so that programs can be patched and protected from cyberattacks.

OPERATIONAL CONSTRAINTS
- Smart fuzzing cannot be done on all programs.

PROBLEM SPONSOR
Garrett Haley, Cybersecurity Engineer, Cyber Department, Marine Corps Tactical Systems Support Activity (garrett.haley@usmc.mil)

PROBLEM SPONSOR LOCATION
Camp Pendleton, California

SENIOR LEADER
Richard Domondon, Cybersecurity Engineer, Cyber Department, Marine Corps Tactical Systems Support Activity (richard.domondon@usmc.mil)

Do not exceed one page