1. PGFUZZ: Policy-Guided Fuzzing for Robotic Vehicles
   1. 时间：2022年2月19号
   2. 来源：NDSS-2021
   3. 文章概要：
      1. Motivation：
         1. RV面临着各种各样的威胁，包括

* 物理外部攻击，如传感器欺骗攻击,
* 由于浮点异常或内存损坏问题导致的软件崩溃
* 内部攻击
* 错误实施导致的安全和功能问题
  + - 1. 先前在fuzzing方面的努力已经引入了一些技术来解决(1)、(2)和(3)，但是(4)并没有得到太多的关注
      2. 安全违规行为可能会导致灾难性的后果, RV必须遵守安全和安保政策，以避免对其运营环境或自身造成物理损害.
    1. Challenge：
       1. 传统的fuzzing方法,他们地 bug oracles的设计理念不会检测不导致系统崩溃、内存访问冲突或物理不稳定的系统状态的输入。
       2. 传统fuzzing算法的变异引擎不能智能地生成RVs的输入。
    2. Approach
       1. 提出了一种基于行为的 Bug Oracle，通过 mtl 公式了解 rvs 的期望状态，并检测在fuzzing程序时是否违反了公式的测试方法
       2. 开发了Policy-Guided 突变引擎，将策略的每个条目与影响 rv 状态的输入联系起来的映射; 测量车辆当前状态与策略违反之间“距离”的距离度量。
    3. Contribution
       1. 提出了一种测试RV逻辑bug的新颖的方法
          1. 定义系统装填的mtl 公式，基于行为测试 Bug Oracle
       2. 开发了Policy-Guided 突变引擎
       3. 发现了156个 RV控制程序的bugs