1. ICS3Fuzzer: A Framework for Discovering Protocol Implementation Bugs in ICS Supervisory Software by Fuzzing
   1. 时间：2022年3月26号
   2. 来源：ACSAC-2021
   3. 文章概要：
      1. Motivation：
         1. 监控软件可能成为攻击者的目标
         2. 尽管 PLC 设备的监控软件在指定的、受到良好保护的计算机上运行，​​但它与 PLC 的交互并未受到严格保护。
         3. 关于 ICS 中的 fuzzing 监控软件的研究很少，存在三个挑战：Challenge：
            1. 闭源、体量大
            2. 与GUI操作紧耦合
            3. 私有协议
      2. Approach
         1. 提出了ICS3Fuzzer一个可移植的、模块化的，能够自动化测试supervisory software的fuzzing框架。
         2. 没有直接分析提取协议实现，而是直接在同步控制GUI操作以及网络通信的情况下，直接运行和fuzz对应的supervisory software。
         3. 通过自动化地输入专门生成地有效地输入并到达不同的协议状态，来持续地驱动整个过程。并且提出了新的fuzzy策略，倾向于更有可能发生漏洞的状态。测试目标时是结合模拟测试与实际测试的优缺点。
      3. Contribution
         1. 设计实现了ICS3Fuzzer。
         2. 提出了新的fuzzing策略。
         3. 结果好，并开源。