FirmPot: A Framework for Intelligent-Interaction Honeypots Using Firmware of IoT Devices

20220318 王毓贞

物联网设备的固件通常嵌入网络应用程序，允许用户从互联网上检查设备的状态，嵌入式 Web 应用程序具有特定于供应商的实现。因此，通过静态或动态分析发现它们的漏洞具有挑战性，并且它们在没有任何安全措施的情况下使用。

基于此，提出了FirmPot，一个使用固件自动生成智能交互蜜罐的框架。该框架有一个针对蜜罐生成优化的固件模拟器，并通过机器学习来学习嵌入式应用程序的行为。生成的蜜罐通过一种机制继续与攻击者交互，该机制从对攻击请求的模拟响应中返回最佳响应，而不是错误响应。

在基于开源 OpenWrt 的无线路由器的嵌入式 Web 应用程序上进行了实验。结果，框架生成了模仿八家供应商和十种不同 CPU 架构的嵌入式 Web 应用程序的蜜罐。此外，与现有的相比，交互方法改进了与攻击者的会话长度。