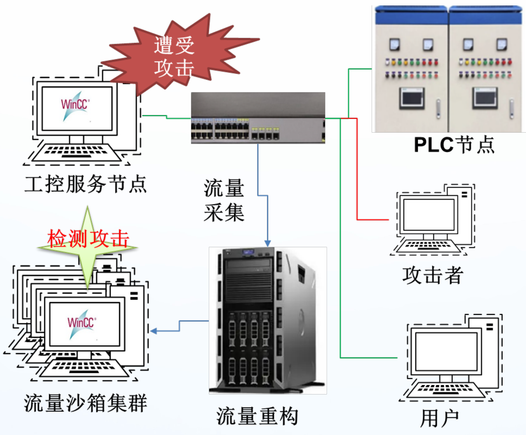
工控网络流量沙箱检测系统

闫佳、黄桦烽、苏璞睿、王梓博

联系方式：闫佳、13426264127、yanjia@iscas.ac.cn

总体介绍

工业控制网络下“闭源”、“对抗”、“无文件攻击”等特点对现有沙箱方案构成挑战。工控网络流量沙箱检测系统直接针对工控设备间“交互流量”进行沙箱检测，通过网络流量重构和重放，对流量驱动下的工控软件行为进行攻击检测，该系统具备数据包乱序修正、数据去冗余和还原等流量重构能力，实现了从“文件沙箱”升级到“流量沙箱”



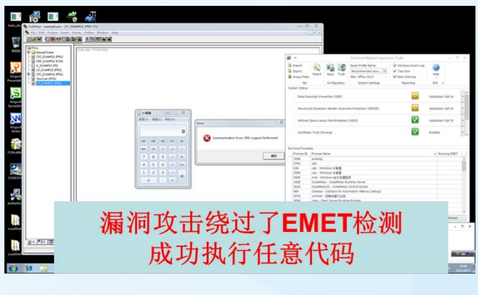
技术指标

- 支持西门子Step7、PLC WinNT、AutoCAD工控上位机软件的动态沙箱环境
- 支持47类对抗样本的检测，与谷歌Virus Total 平台部署的同类沙箱相比，对抗能力显著提升

典型应用

- 中标中国移动工业互联网安全项目，标前技术测试评分排名第一
- 中标某部车载安全设备采购项目

典型案例 - PLC WinNT的协议漏洞攻击



该攻击可绕过微软EMET的CFI防御机制，但可被流量沙箱检测