

# 工控网络流量沙箱检测系统

闫佳、黄桦烽、苏璞睿、王梓博

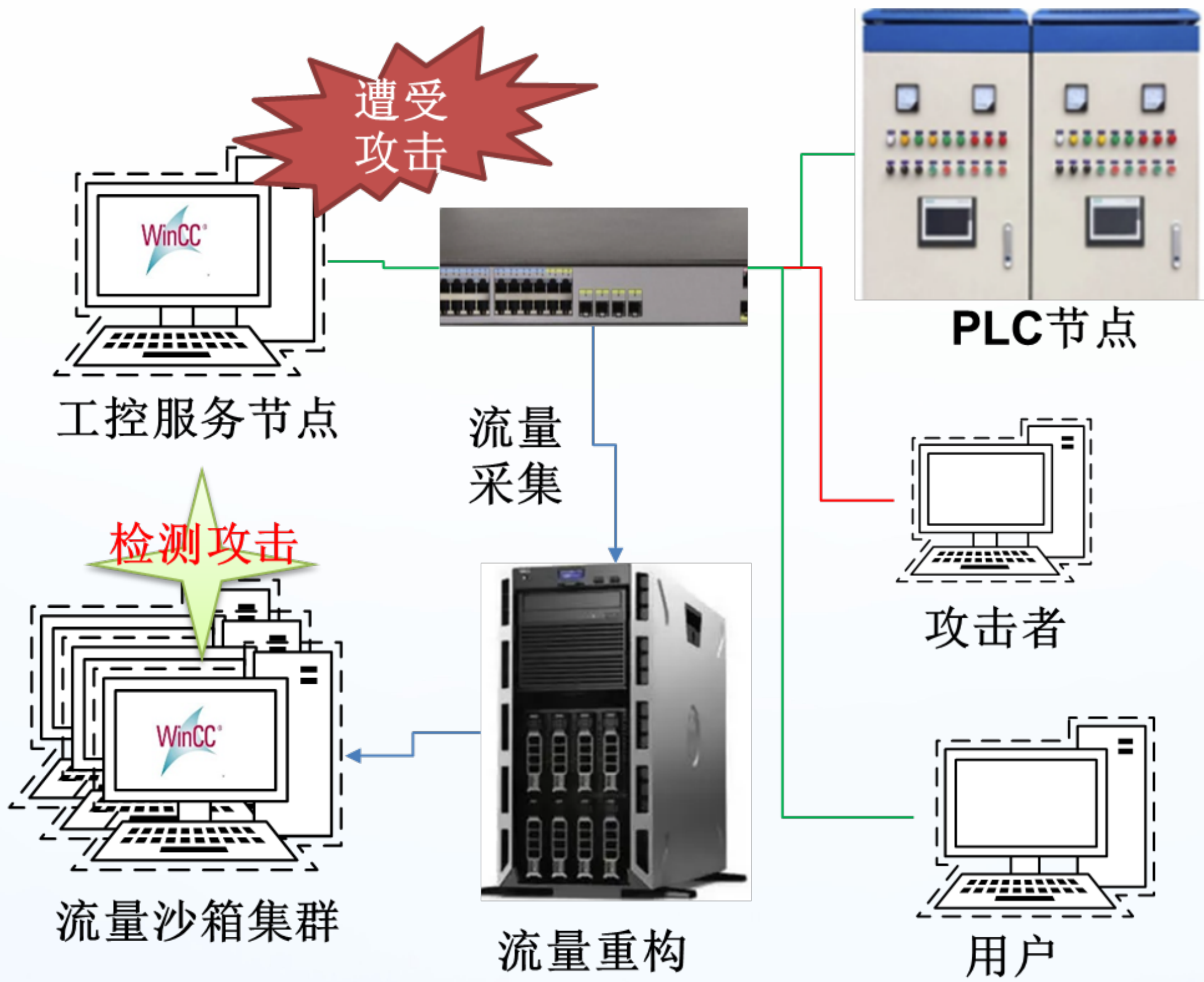
联系方式：闫佳、13426264127、yanjia@iscas.ac.cn

## 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



漏洞攻击绕过了EMET检测  
成功执行任意代码

动态行为类目	查看详细结果数据	异常代码片段	行为说明
进程开始执行	进程ID: 1256	被 (1256) 创建的进程开始执行	
读取文件	文件路径: Serial0	读取文件 Serial0	
接收本机网络数据包	接收到的数据包	收到本机的网络数据包	
发送网络数据包	发送的数据包	向本机发送网络数据包	
接收网络数据包	接收来自 192.168.4.10:35354 的数据包	接收来自 192.168.4.10:35354 的数据包	
发送网络数据包	发送的数据包	向 192.168.4.10:35354 (Unknown Host) 发送网络数据包	
检测测试环境	检测到的环境	检测测试环境，进程分析与查杀	
加载模块	加载的模块: HarddiskVolume1\WINDOWS\system32\faultrep.dll	加载模块 HarddiskVolume1\WINDOWS\system32\faultrep.dll	
读取系统文件	读取的文件: HarddiskVolume1\WINDOWS\system32\cmd.exe	读取文件 HarddiskVolume1\WINDOWS\system32\cmd.exe	
将进程内存读取	读取的内存地址	读取 cmd.exe 进程中的数据，窃取信息	
将进程内存写入	写入的内存地址	修改进程 cmd.exe 的内存数据	
创建进程线程	创建的线程	创建进程 cmd.exe 的线程	
添加系统用户	添加的用户名	添加注册后门账户的行为	
启动CPU程序	启动的CPU程序		
创建进程	创建的进程		
结束其他进程	结束的其他进程		

流量动态沙箱检测出了创建进程，  
添加注册后门账户的行为；

该攻击可绕过微软EMET的CFI防御机制，但可被流量沙箱检测