基于动态污点分析的工业控制系统协议自动逆向工程分析

麻荣宽[1]，郑豪[2]，王竟亦[2]，汪慕峰[2]，魏强[1]，王清贤[1]
[1]数学工程与先进计算国家重点实验室，中国郑州市，450001
[2]浙江大学NGICS平台，中国杭州市，310000

摘要：私有（或半私有）协议广泛应用于工业控制系统（ICS）。通过逆向工程推断协议格式对于许多网络安全应用（例如程序测试和入侵检测）具有重要意义。传统协议逆向工程方法耗时，繁琐、易出错。最近提出的自动化逆向协议方法既不能有效处理基于网络流量分析的二进制ICS协议，也不能从协议程序实现中准确提取协议字段。本文提出一个工业控制系统协议逆向工程框架（ICSPRF），旨在以更高准确度提取ICS协议字段。ICSPRF基于以下关键见解架构：消息中单个字段通常在同一执行上下文中处理，例如基本块（BBL）组。通过监视程序的执行，ICSPRF可以在执行跟踪中收集每个BBL组中处理的污染数据信息，并将它们聚类以得出协议格式。用6个开源ICS协议实现评估所提方法。结果表明，ICSPRF可以高精度地识别各个协议字段（平均匹配率为94.3％）。ICSPRF还具有较低粗粒度匹配率和过细粒度匹配率。对于同一指标，ICSPRF比Autoformat更准确（后者对于所有评估协议匹配率为88.5％，对二进制协议匹配率为80.0％）。

关键词：工业控制系统（ICS）；ICS协议逆向工程；动态污点分析；协议格式
https://doi.org/10.1631/FITEE.2000709