·体系结构与软件技术·　　文章编号：1000-3428(2019)08-0092-10　　文献标志码：A　　中图分类号：TP399

面向工业控制系统的渗透测试工具研究

周伟平[1]，杨维永[2]，王雪华[1]，茅　兵[1]

（1. 南京大学 计算机软件新技术国家重点实验室，南京 210023；
2. 南京南瑞信息通信科技有限公司，南京 210000）

摘　要：为提高对工业控制系统的渗透测试效率，保障其安全可靠性并提升系统安全防护能力，基于 shell 交互技术构建面向工控系统的渗透测试工具框架，并通过 Python 语言进行实现。设计具有层次结构的网络探测和系统探测模块，利用协议解析和逆向技术对工控协议进行脆弱性检测，同时研究基于工控环境的漏洞利用方式，通过模糊测试模块对测试目标进行漏洞挖掘和脆弱性检测。在此基础上，参考开源 Metasploit 软件，根据模板规则编写渗透攻击脚本。仿真结果表明，该设计可提高对工控系统的探测效率，降低协议脆弱性检测难度，并且具有结构简明、易于扩展的特点。

关键词：工业控制系统；漏洞；渗透测试；协议逆向；模糊测试

中文引用格式：周伟平，杨维永，王雪华，等. 面向工业控制系统的渗透测试工具研究[J]. 计算机工程，2019，45(8)：92-101.

英文引用格式：ZHOU Weiping, YANG Weiyong, WANG Xuehua, et al. Research on penetration testing tool for industrial control system[J]. Computer Engineering, 2019, 45(8): 92-101.

Research on Penetration Testing Tool for Industrial Control System

ZHOU Weiping[1], YANG Weiyong[2], WANG Xuehua[1], MAO Bing[1]

(1. State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210023, China;
2. Nanjing NARI Information and Communication Technology Co., Ltd., Nanjing 210000, China)

【Abstract】 In order to improve the penetration testing efficiency of an Industrial Control System (ICS), ensure its security and reliability and enhance the system security protection ability, this paper constructs a penetration testing tool framework for ICS based on shell interaction technology and implements it with the Python language. It designs a hierarchical network detection module and system detection module, and uses protocol parsing and reverse technology for vulnerability testing of industrial control protocols. It also researches vulnerability exploitation ways based on the industrial control environment and designs a fuzzy testing module for vulnerability mining and detection of testing targets. On this basis, a penetration attack script is written according to the template rules in reference to the open source software, Metasploit. Simulation results show that this design can improve the detection efficiency for ICS, reduce the difficulty of protocol vulnerability detection. Meanwhile, it has the characteristics of simple structure and easy extension.

【Key words】 Industrial Control System (ICS); vulnerability; penetration testing; protocol reverse; fuzzy testing

DOI: 10.19678/j.issn.1000-3428.0051265

0　概述

工业控制系统（Industrial Control System，ICS）是国家关键基础设施的重要组成部分，其被广泛应用在石油石化、水利、电力、食品加工和污水处理等工业领域，主要用于数据采集和生产控制等方面。早期的工控系统与互联网物理隔离，且多数采用专用软硬件，即使系统中存在安全隐患，外界也难以接触并展开研究。随着计算机技术在工业环境中的广泛应用，通用计算设备、通用操作系统开始用于工控系统的实现，工控协议也开始基于 TCP/IP 协议构建，打破了工业控制系统的封闭性和专有性，使得传统互联网系统所面临的威胁蔓延到工控系统环境中。根据对有关工控系统在线监测平台数据的统计[1]发现，越来越多的工控系统暴露在互联网上，黑客有目的地探测并锁定攻击目标变得更加容易，对

基金项目：国家自然科学基金(61272078)；国家电网公司科技项目(SGHE0000KXJS1700079)。

作者简介：周伟平(1992—)，男，硕士研究生，主研方向为工业控制系统；杨维永，正高级工程师；王雪华，硕士研究生；茅　兵，教授、博士生导师。

收稿日期：2018-04-18　　**修回日期：**2018-08-04　**E-mail：**zhouweipingcs@163.com

工控系统的入侵攻击已不再神秘。如 2015 年12 月,乌克兰电力系统遭黑客攻击,将远程访问并控制工控系统的 BlackEnergy 软件植入乌克兰电力部门,造成电网数据采集和监控系统崩溃,导致伊万诺-弗兰科夫斯克地区约一半家庭停电数小时。

近年来频繁发生的工控安全事件[2-3]暴露了工业控制系统在安全防护和安全监测预警上的不足,工业控制系统的安全脆弱性处于“先天不足,后天失养”的严峻行情。近年来工控安全事件的攻击策略主要利用工业以太网协议漏洞,向工业控制系统发送伪造或恶意的控制命令。工控系统安全事关经济发展、社会稳定和国家安全,因此,针对工业控制系统的安全研究[4-5]迫在眉睫,特别是对工业以太网协议的安全研究更刻不容缓。

针对目前关于工控系统的测试技术较少,而成熟渗透测试工具[6-7]又不适用的现状,本文设计一种面向工控系统的渗透测试工具框架,以解决探测效率低、协议脆弱性检测复杂和漏洞利用方式单一等问题。

1　相关背景

1.1　工控系统体系结构

在两化融合和工业 4.0 的趋势下,计算机全自动化采集展示现场数据的方式在工业控制领域中愈受欢迎,其优势在于便于合理集中地处理分散的现场数据,因此,设计适合工业现场复杂环境且可靠稳定的网络结构是工控系统研究的重要内容。随着信息技术的发展,工业控制系统从不可路由的现场总线发展到可路由的工业以太网,形成了新一代扁平化网络控制系统。图 1 所示为符合普渡参考模型的工业控制系统层次结构[8]。随着以太网在工控系统中的应用,控制系统与企业管理网络无缝衔接,为满足工业需求,工业以太网在部分继承传统以太网核心技术的基础上,针对实时性、安全性进行了相应改进和演化,图 2 所示为工业以太网协议的体系结构。

Modbus/TCP 协议将 Modbus 帧作为 OSI 通信参考模型中应用层报文进行传输,通过 502 端口进行请求应答模式,能够兼容标准以太网设备,成为工业以太网标准的既定事实标准。S7 通信协议由西门子公司基于某 ISO 协议实现,其中:会话层 TPKT 是一个传输服务协议,主要用来在 COTP 和 TCP 之间建立桥梁,包含用户协议的数据长度;表示层 COTP 的作用是定义数据传输的基本单位,而以 0x32 开始的 S7Comm 协议是西门子 S7 通信协议簇中的一种,可以完成对控制器信息的读取。

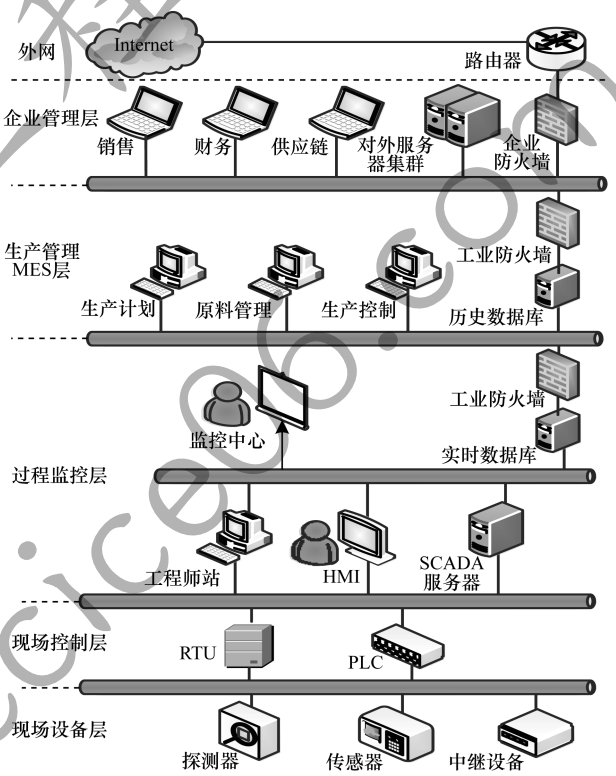

图 1　工业控制系统层次结构

OSI参考模型	标准以太网	Modbus/TCP	Ethernet/IP				S7	DNP3
应用层	HTTP/FTP	Modbus	行规 应用对象库 CIP				S7Comm	DNP3
表示层 会话层	无	无	无				COTP TPKT	无
传输层	TCP/UDP	TCP/UDP			TCP/UDP	留于扩展	TCP/UDP	TCP/UDP
网络层	IP	IP			IP		IP	IP
数据链路层	CSMA/CD	CSMA/CD	USMA/CD	CAN	CTDMA		CSMA/CD	CSMA/CD
物理层	以太网物理层	以太网物理层	以太网物理层				以太网物理层	以太网物理层

图 2　工业以太网协议的体系结构

1.2 工控协议安全性分析

随着工业以太网的广泛应用,其安全研究逐步成为业界的研究热点,由于工控环境早期处于隔离状态,追求实时性和可靠性的工控通信协议多数缺乏加密、认证等安全机制(如 Modbus 协议),因此网络黑客只需要获取总线的访问权限,就能对总线数据进行监听、篡改,实现对工业控制网络的破坏。文献[9]总结了此类协议所面临的安全威胁。文献[10]综述了工业以太网协议的脆弱性,其面临的主要风险有:大量协议数据明文传输,缺乏认证和加密,存在被窃听、伪装、篡改、抵赖和重放的攻击风险。文献[11]指出 Modbus/TCP 协议缺乏加密机制,网络攻击者能够识别通信设备,篡改数据分组,造成服务器恶意宕机。而文献[12]则将针对 Modbus 串行协议和 Modbus/TCP 的攻击做了相应的分类。Ethernet/IP 协议容易受以太网漏洞影响。研究指出 Ethernet/IP 协议缺乏时间戳和加密机制,可能遭受拒绝服务攻击。为降低工业以太网面临的重放攻击风险,西门子创建了需要使用口令才能与设备进行通信的授权指令,但安全研究人员发现可以通过访问项目文件直接从文件中提取出口令。此外,基于嗅探技术捕获的网络数据包,可以利用字典进行口令破解。DNP3 协议是由美国 IEEE 电力工程协议制定并推广的工业通信标准,在通信机制中添加了认证、加密、授权、完整性校验等安全手段,但仍然无法避免安全威胁。通过发送大量错误信息,会使协议栈缓冲区溢出,最终导致服务崩溃。

针对工业协议的脆弱性,业界主要从以下 3 个方面进行安全防护:

1)主动探测协议脆弱性,先于攻击者发现目标系统的风险因素,即科学检测目标系统的协议漏洞并及时更新补丁。ICS-CERT、CVE 等安全漏洞平台会实时发布针对工控协议的安全漏洞,企业用户可以配置扫描设备来检测资产设备的安全可靠性。

2)部署入侵检测系统和入侵防御系统等被动防护手段,即当攻击向量已经进入系统内部,通过检测手段或者防御机制使得攻击无法成功。

3)基于加密技术对当前工业协议的不安全机制进行改进。例如:文献[13]提出基于 ECC 加密体制的认证授权机制,实现用户与变电站智能设备的双向认证和访问控制;文献[14]提出一种基于 NTRU 公钥加密算法,实现 SCADA 系统端到端的安全传输。

鉴于工业控制系统的安全脆弱性很大程度上取决于工控通信协议的设计,因此必须对工业通信协议开展安全性研究,特别是针对测试目标的渗透测试。渗透测试通常指通过模拟恶意黑客的攻击行为,挫败目标系统安全控制措施,取得访问权,并发现具备业务影响后果安全隐患的一种针对计算机系统和网络安全的安全测试和评估方式。根据 PTES 标准,渗透测试包括前期交互、情报搜集、威胁建模、漏洞分析、渗透攻击、后渗透攻击和报告等7 个阶段,其涵盖内容广泛,因此渗透测试工具也丰富多样,如以 MSF 为代表的网络渗透集成工具和针对 Web 漏洞的 SQLmap。

目前发达国家已经开始部署工业控制系统模拟环境,并在渗透测试和风险研究等领域开展研究,制定了相关标准,而国内在工控安全领域的研究[15]缺乏针对工控系统环境的专业渗透工具,尽管绿盟科技在 2014 年发布产品 NSFOCUS ICSScan,针对工业控制系统中的特有设备进行漏洞扫描和脆弱性评估,但并没有公开其使用的扫描方法和包含的渗透脚本。

2 框架设计与实现

2.1 总体设计

从攻击者角度出发,假设工控系统的某个组件或应用至少存在一个已知或未知的安全脆弱性,攻击者能够利用这个脆弱性实施网络攻击,如拒绝服务或代码执行。更具体来说,攻击者首先需要对目标系统进行网络侦查,获取目标工控系统的指纹信息及各种服务的版本信息,利用工控专有漏洞库进行数据比对,探查该目标系统是否存在某已知的脆弱性,并根据脆弱性属性(时间、可利用性)来决定下一步的工作。如果攻击者没有发现任何可利用的公开漏洞,下一步工作则是根据已掌握的目标信息,利用模糊测试等脆弱性挖掘技术对目标系统中可能的脆弱点(通信协议、应用服务等)进行深入的脆弱性检测,试图挖掘 0-day 漏洞并开发利用。攻击操作模型(Offensive Operations Model,OOM)是 KSAJ 公司于 2004 年提出的一种模型框架,供设计、开发及测试人员在测试项目安全性的过程中使用,具有高扩展性和高伸缩性等特点。从实际使用角度出发,OOM 模型的流程符合一次模拟攻击的过程,可以作为脆弱性检测模型的基础。结合工业控制系统渗透测试特征,本文建立一种基于攻击操作模型的工控渗透测试模型,对其前三个阶段稍作修改,将后两个阶段替换为渗透测试过程。如图 3 所示,该模型是一种以网络探测为前期准备,以漏洞扫描和模糊测试为辅助手段,以渗透测试为核心,以脆弱性评估为最终目标的工控渗透测试模型。

根据工控渗透测试模型,从功能需求出发,本文系统采用层次结构和模块化设计,如图 4 所示,其总体架构集成了网络环境探测、工控系统探测、漏洞扫描与挖掘、工控协议模糊测试和渗透攻击等功能,由功能交互模块调用,基于不同测试目标和用户需求调用相应的功能模块,各功能模块间结构相互独立,可单独使用且方便单元测试。

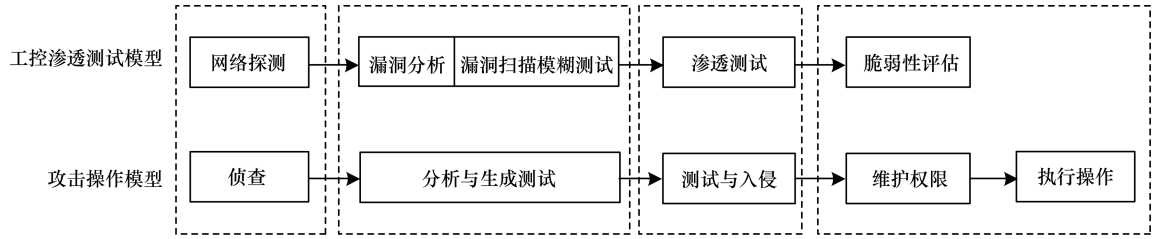

图 3　工控渗透测试模型与攻击操作模型的流程对比

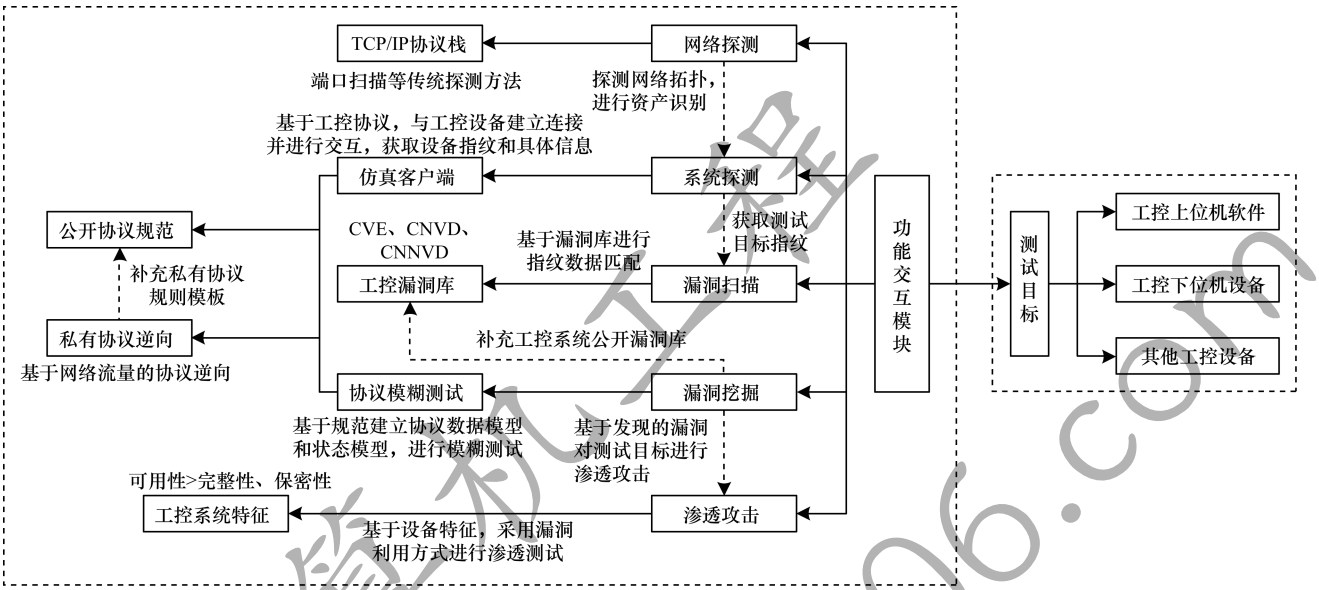

图 4　渗透测试工具架构

2.2　系统探测模块

对渗透测试而言,采用主动侦查的方式来探查渗透目标的网络访问范围、拓扑、运行服务、安全漏洞等全方位多类型的情报信息是前提条件,为后续的渗透攻击提供基础。系统探测和脆弱性检测框架如图 5 所示。

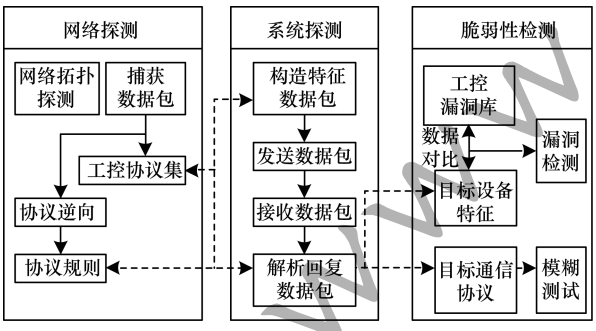

图 5　系统探测与脆弱性检测框架

网络探测模块主要承担针对工业控制系统的情报搜集、主机探测、端口扫描等任务,因为工业协议开始基于 TCP/IP 构建,所以该模块利用传统的网络探测手段对工控测试目标进行探测,为基于层次的系统探测提供信息支撑。此外,其利用工控设备具备周期性发送查询数据包的特性,捕获在工控环境中进行数据交互的网络数据包,为工控协议逆向提供数据支持。

鉴于工控系统的特殊性,传统的网络探测技术无法最大程度地收集到充分有效的信息(如工控设备的模块类型、固件版本),需要借助基于工控协议特征的系统探测方法[16]。网络探测模块在该渗透测试框架中起到重要作用,在网络探测的基础上对测试目标进行二次探测,承担获取工控设备的指纹信息的重要任务,为后续漏洞数据比对提供详细准确的指纹信息。

工控系统通信协议是为实现上位机和下位机之间相互通信而设计的,目的是工程师站下发控制指令给下位机程序,或主设备查询从设备状态和历史数据。因此,工控协议多数基于不同特征码来进行数据解析,以 Modbus/TCP 协议[17-18]为例,其特征码 1用于表示读取线圈状态,特征码 14 用于读取设备标识。因此,基于公开协议 Modbus/TCP 协议集和网络数据包解析,可以解析工程师站对 PLC 下发程序的流程,以及特殊命令的特征码。基于信息提取,可以得知工程师站所使用的编程软件在和 PLC 的通信中是否使用了一些非标准的功能码,用来实现一些特殊功能,比如终止 PLC CPU。这些二次探测得到的有效信息也对后期的渗透测试具有极大的帮助,例如,在缺乏验证机制的工控环境中可以进行数据包重放,造成严重的拒绝服务攻击。

此外,对于未知协议,利用协议逆向技术[19-20]推断状态机,可建立仿真客户端与其交互,发送基于模板构造的探测数据包获取测试目标的设备信息。

2.3 漏洞扫描与工控漏洞库

本框架从通用漏洞平台(CVE)、国家信息安全漏洞共享平台(CNVD)和中国国家信息安全漏洞库(CNNVD)等公开漏洞平台专门搜集工控系统相关的漏洞信息,组织包含指纹信息(如漏洞特征、受影响产品、版本信息、通信协议等)的工控漏洞库,并保持不断更新。

当基于层次的网络探测和系统探测模块扫描出测试目标的工控设备名称、型号、端口服务、固件版本等有效信息后,利用工控漏洞库中的工控设备具体信息和漏洞数据进行特征对比。如果查找成功,则发现测试目标的安全漏洞和脆弱性,并基于此进行后续的渗透攻击。如果查找失败,则进行特殊处理:

1)测试目标可能存在的漏洞未收录在本框架的工控漏洞库中,即漏洞库更新不及时。

2)漏洞特征库设计不完善,数据比对过程出现异常,则进行手工查找。

3)测试目标不存在公开已知漏洞,后续进行基于模糊测试的漏洞挖掘。

2.4 漏洞挖掘模块

随着工控协议基于 TCP/IP 构建,可将工控协议划分为底层协议和应用层协议,应用层协议又分为公开协议和私有协议。其公开协议结构清晰,可以基于说明文档提供的协议结构开发协议套件,提供给测试工具进行模糊测试[21],但生成的测试用例往往只能挖掘出协议实现的浅层漏洞,无法深入地对工控协议进行安全性测试。

为弥补基于公开工控漏洞库的漏洞扫描[22]的不足,同时进行完整性更高的渗透测试,本文根据协议模型建立样本树,以 Modbus/TCP 协议为例(如图 6 所示),利用功能函数 *ByteCount* 直观表明 *Length* 字段与其他字段的关联性,以避免协议描述模型中冗长的 BNF 表示[23]。

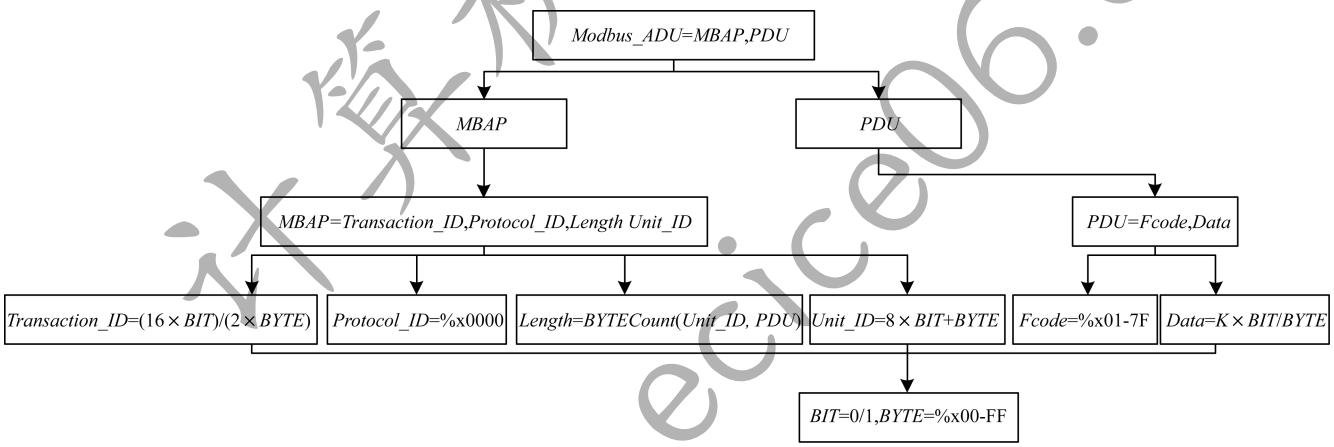

图 6 Modbus/TCP 协议样本树

首先对变异树进行深度优先遍历,得到变异树节点及其属性组成的集合,然后将节点集合逆序,根据该集合的顺序依次寻找未被测试的节点作为变异对象,同时将节点字段放入已测试集合中,避免在后续样本测试中对相同字段重复测试。此外,为了更好地提升模糊测试的效率,系统采用哈希算法和反馈机制来优化测试样例,避免发送低质量测试样例。

借助哈希值去重的设计思路,在生成测试用例的同时计算测试用例的哈希值,并保存测试用例的 ID 和哈希值。每当生成新的测试用例,首先计算测试用例的哈希值,然后根据哈希值在数据库里进行查询,如果没用此测试用例的哈希值,则生成测试用例,并将其编号和哈希值写入数据库。这样会大量减少重复的测试用例,避免对冗余的测试用例进行不必要的冗余的测试,以便节省测试时间,并使得模糊测试的效率得到提升。

基于工控通信协议的特征是利用功能码和异常码的反馈来调整测试用例的生成。例如,根据处理结果,Modbus/TCP 可以生成 2 类响应,正常响应的功能码和请求功能码一致,而异常响应功能码在请求功能码的基础上加上 0x80,目的是为客户机提供处理过程检测到的错误信息,并用异常码来表明出错原因,例如:异常码 0x01 表示非法的功能码,即服务器不支持此类功能码;0x02 表示非法的数据地址,表明请求数据包所要求访问的数据地址是非法的。而根据回应报文得到的反馈信息,可以知道当前变异的报文域是否跟代码分支有关,有利于调整测试样例的生成。

在传统的模糊测试中,异常监测的方法主要是调试器跟踪和日志分析。调试器跟踪需要在被测软件所在的平台上安装本地监视器,但工控系统的运行环境封闭,如 PLC 和 RTU 等组件属于嵌入式设备,难以安装本地监视工具,所以,该方法只适用于工控系统中的协议软件,无法应用于 PLC 和 RTU 等组件。所谓心跳报文,是指以单播或广播的方式发送 ICMP、ARP 命令和相关测试协议的诊断报文,通过测试目标的响应报文来判断测试目标是否处于正常运行状态。在本文所设计的模糊测试模块中,会话管理模块可以在发送相应的数据包之后调用心跳包构造模块,然后心跳包构造模块根据前序发送的命令和数据包,生成相应的心跳包,发送给测试目标。测试目标收到相应的心跳包之后,会根据心跳包的具体内容回送反馈信息,远程监视通信模块处理反馈信息包的具体内容,并根据其内容判断测试目标是否存在异常,进而判断漏洞的相应信息。

基于以上测试思路,本文渗透测试框架基于 Sulley 测试工具实现了针对工控协议的模糊测试模块,对测试目标进行漏洞挖掘和脆弱性检测。Sulley 作为模糊测试工具,实现了数据生成、测试用例执行、过程监控等模块的自动化,由 Python 语言构建,具备其方便移植、兼容性好、方便二次开发的特点。图 7 是基于 Sulley 改进的工控协议模糊测试流程,本文对用于生成测试样例的数据构造部分和监控代理进行了修改,沿用了其会话管理和异常报告模块。

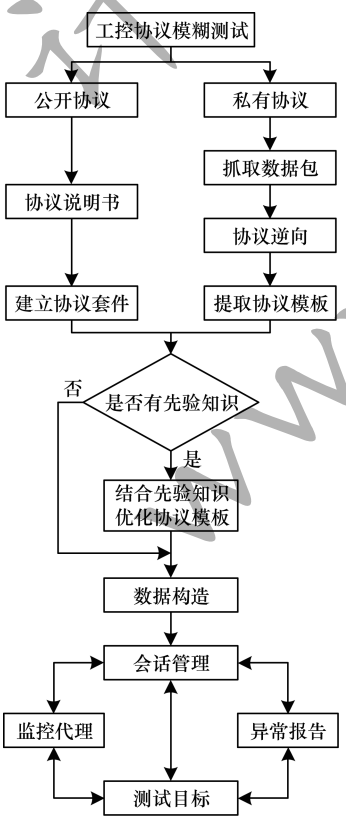

图 7　工控协议模糊测试流程

2.5　渗透攻击模块

渗透工具模块实现渗透框架的核心功能,即对漏洞利用脚本编写提供支持。传统的渗透测试工具往往简单地把渗透脚本集中到系统中,再使用工具分别进行调用,使得漏洞样本功能单一且不利扩展。本文框架仿造开源渗透测试框架软件 Metasploit,基于模板规则进行渗透攻击脚本的编写,既满足不同模板定义不同输入信息的特殊性,也具备扩展性,如 exploit 函数用于漏洞利用,option 结构用于设置脚本输入信息,info 结构用来描述该脚本所利用的漏洞信息(类型、CVE 编号、影响软件版本、危害等级等)。

针对工控环境的特殊性,需要基于策略机制选取漏洞利用方式,如图 8 所示。针对 SCADA 软件的缓冲区溢出攻击,脚本编写时不需要考虑随机化对 shellcode 布局的影响;针对 PLC 固件漏洞,要考虑其指令集对不同编码的支持度;针对工控协议的模糊测试,在没有完全逆向协议规范的情况下,基于特定功能码的数据包会造成由于协议栈资源管理错误的 DOS 攻击。因此,本文框架渗透攻击模块在考虑工控系统安全配置和环境特殊性的基础[24]上,所采用的漏洞利用方式能够解决目前通用渗透攻击针对工控系统漏洞利用单一的问题。

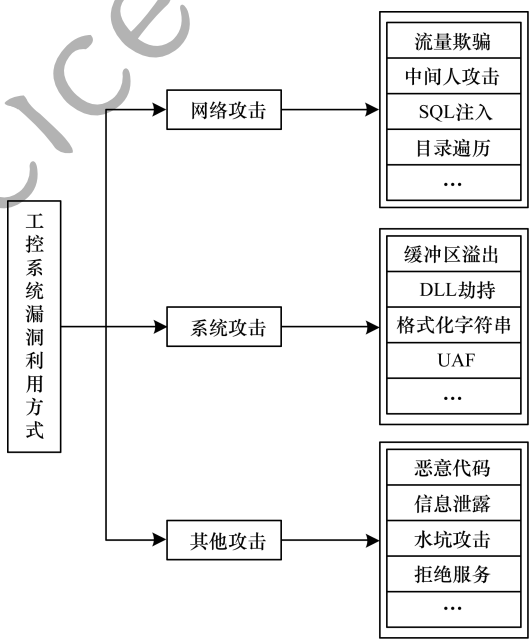

图 8　工控漏洞利用方式分类

2.6　功能交互模块

基于上述框架结构,本文利用 Python 语言实现一个基于 shell 交互的面向工业控制系统的渗透测试工具,其 CPS 功能交互界面如图 9 所示。本文设计将功能模块集中到 shell 交互模块,基于不同的测试目标和

测试需求调用相应功能模块,精简了框架结构以及开发、测试和用户使用流程,便于功能扩展。

图 9 CPS 功能交互界面

3 实验结果与分析

3.1 实验设计

为验证本文工具框架包含功能的有效性,利用如图 10 所示的工控仿真测试环境和 Shodan 引擎搜索得到的公开工业控制设备,对该渗透框架的功能进行测试,包括工控目标探测、基于数据包的协议逆向和针对工控系统的渗透测试。表 1 列出了仿真环境中测试设备的具体功能及其包含的安全脆弱性。

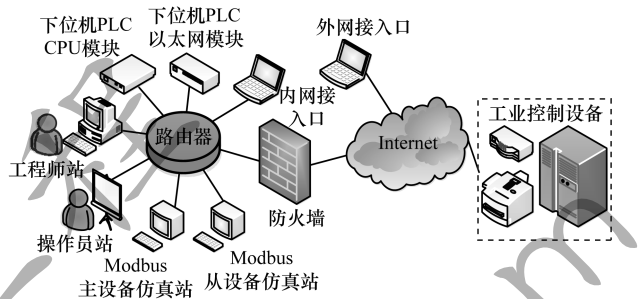

图 10 工控仿真测试环境拓扑

表 1 测试环境功能模块

测试设备名称	功能	脆弱性
Quantum PLC CPU 模块	运行 PLC 程序,并接收上位机信号	Web 漏洞
Quantum PLC 以太网模块	为 PLC 提供以太网服务	协议栈拒绝服务
Modbus 主/从设备仿真站	以 Modbus/TCP 通信协议进行数据交互	中间人劫持
工程师站	运行 PLC 编程软件,工程师编写 PLC 程序,并对下位机下发控制指令	数据包重放攻击
操作员站	运行 SCADA 软件,监测 PLC 运行状态,查询历史数据	缓冲区溢出
路由器、防火墙	仿真工控环境网络拓扑	不做测试
工业控制设备	为系统探测模块提供真实工控设备	不做脆弱性测试

3.2 结果分析

3.2.1 基于协议特征的工控目标探测

探测目标设置为互联网中的公开设备(shodan 引擎搜索结果),实验选择西门子、施耐德、罗德韦尔自动化、欧姆龙等主流工控厂商的工业设备进行目标探测。工控资产识别的结果如表 2 所示。从表中可知,利用扫描器 nmap 和工控相关的扫描脚本可以探测出主流工控设备的基本信息(如版本信息、设备型号等),而该渗透测试工具框架所提供的探测模块能够扫描出更具体的信息,如 PLC 的 CPU 型号、项目运行信息等,其原因是基于渐近性层次探测的思想,在网络探测的基础上,利用工控协议基于特征码的请求回应,基于协议规范构建的特殊请求数据包能够探测目标的具体信息。

表 2 工控设备资产识别结果

测试目标描述	Nmap(包括 nse)探测结果	CPS_Scan 探测结果
Wind Italy 组织提供的工控蜜罐,开放端口 102,运行 S7-300	版本、设备名、模块类型、序列号	版本、设备名、模块类型、序列号、CPU 型号、内存卡序列号
施耐德 BMX 型号 PLC,开放 502 端口支持 Modbus/TCP 协议 Unit ID:0 ~ 255	端口信息、设备型号、CPU 模块	设备型号、CPU 模块、内存卡型号、项目运行版本、项目上次修改时间
UPCnet 组织公开在互联网上的欧姆龙 PLC,开放端口 9600	控制器型号、版本、IOM 尺寸、DM 序列号	控制器型号、版本、IOM 尺寸、DM 序列号
AT&T Wireless 组织公开在互联网上的罗德韦尔的工控设备	产品名、供应商 ID、序列号、设备类型	产品名、供应商 ID、序列号、设备类型
俄罗斯工控厂商 Fastwel 设备,支持 Modbus 协议	端口信息	设备型号、CPU 模块、运行时间

以 Modbus/TCP 协议为例进行说明:

1)公共功能码保证唯一,如特征码 0x2b(43)可以读取设备标识,而特征码 0x11(17)用于报告从机标识。

2)用户定义功能码可能被用户使用为特殊功能的实现的,比如 Basecamp 项目中,功能码 0x5a(90)允许厂商实现 Modbus 协议原本没有的功能,比如终止 CPU 运行。

3)保留功能码一般留作内部作用或异常应答,如特征码 0x91(145)可以用来回应从设备发生的 ID 错误。

S7-300 PLC 的探测结果如图 11 所示。尽管 S7 通信协议是西门子基于某 ISO 协议实现的,该协议采用了比较严格的控制措施,但仍然可以根据协议从西门子设备中提取信息并进行响应分析,基于特征信息鉴别目标型号;而针对欧姆龙 PLC 的探测结果没有更进一步的信息,是因为其 9600 端口服务使用的是私有协议,协议解析出的模板特征不健全,构建的特征数据包不具备查询进一步信息的特殊功能;罗德韦尔厂商的工控设备使用的是公开协议 EtherNet/IP,框架的探测模块没有达到进一步探测目的,其原因是 EtherNet/IP 协议在常用 44818 端口之外还使用了 2222 端口,用于辅助客户端/服务端通信报文和 I/O 报文的发送,状态机的复杂程度超过了探测模块目前的支持范围。

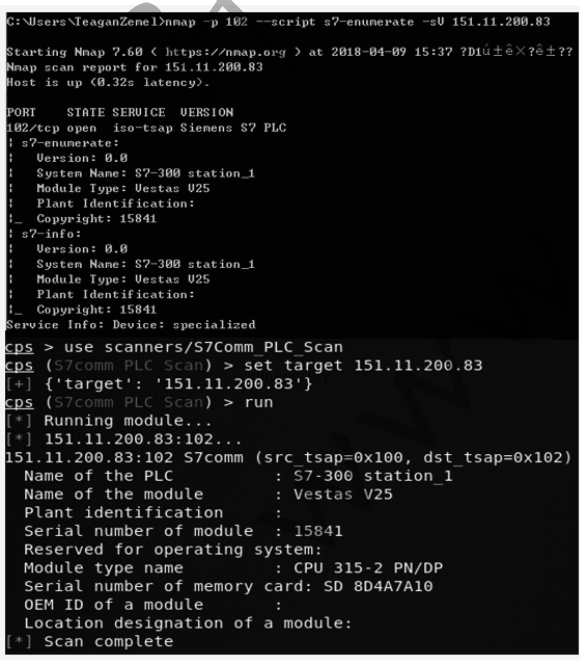

图 11　西门子 PLC 探测结果对比

表 2 和图 11 的结果对比表明,基于渐近性层次探测的思想,充分利用工控协议基于特征码的状态转移(请求与响应)构建特殊功能码的请求数据包,可以最大限度提高工控目标的探测效率。

3.2.2　工控通信协议模糊测试

基于本文提出的基于协议模型的模糊测试方法,选择基于 Modbus/TCP 协议的 PLC、上位机软件和相应的仿真软件作为待测目标对象,并根据得到异常将测试结果分为 3 类,如表 3 所示。其中,CPS 表示本文框架所设计的工具,A 类异常表示 RST 请求报文,B 类异常表示响应不符合协议规范,C 类异常为目标崩溃或者 Ping 不通。下位机硬件设备或模拟软件都存在 A 型异常,是因为从设备由于异常断掉了 TCP 连接,但由于工控通信协议对于可靠性的要求,在断掉连接后会有机制保活并重新连接,因此并没有崩溃。

表 3　协议模糊测试结果

测试目标	CPS			Sulley			Smod		
	A	B	C	A	B	C	A	B	C
Pymodbus	26	1 300	0	20	982	1	13	1 106	0
MOD_RSSIM	42	6 983	2	40	3 305	1	22	2 940	1
Modbus Slave	284	5 894	1	237	4 763	0	170	5 029	0
Modbus Poll	—	—	1	—	—	0	—	—	0
Unity Pro	—	—	2	—	—	1	—	—	0
TouchView	—	—	3	—	—	2	—	—	1
Quantum CPU	5	4	1	0	2	1	0	2	0
Quantum NOE	7	9	1	1	1	2	0	3	0

如图 12 所示,OR_mask 字段错误应该返回差错码 0x96 和异常码 0x02,但反馈的数据包显示的异常码为 0x01,B 类异常出现的原因根据测试对象的不同而不同,对于仿真软件如 Modbus/Slave 等而言,是因为开发者没有按照标准协议规范实现,完全由开发者自定义功能码的使用,所以导致数量巨大的 B 类异常;而对于施耐德厂商的专业设备,其存在的 B 类异常由内存错误导致。

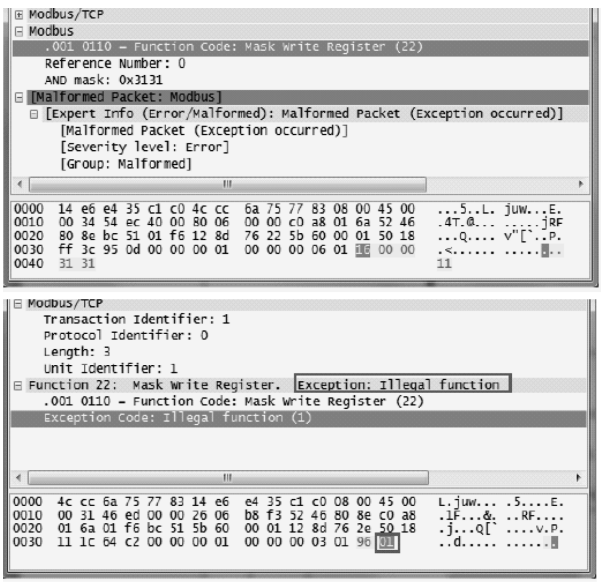

图 12　非法响应数据包示意图

对于 C 类异常,其中测试目标 Quantum CPU 挖掘出的协议漏洞经过验证为已知漏洞 CVE-2017-6017,即 Schneider PLC 中存在资源耗尽漏洞,攻击者发送精修编制的数据包导致设备无响应,导致拒绝服务;Quantum NOE 中挖掘出的 2 个漏洞:一个是以太网模块接收全部分段并重组报文时总长度超过 65 535 Byte,导致 NOE 模块出现内存分配错误,触发 TCP/IP 堆栈崩溃;另一个也是资源消耗型漏洞,会导致拒绝服务攻击。

为验证基于协议样本树的测试用例生成算法能够提升模糊测试的效率,本文对 Modbus/TCP 协议不同的功能码进行测试,结果如表 4 所示。其中:异常测试用例指报文格式错误,字段取值不符合协议标准或者不在去取值范围内,可能会触发目标对象异常响应;变异率则是异常测试样例数目在测试样例总数中所在比重,能够反映模糊测试工具在生成测试样例的随机性和针对性。Modbus/TCP 读系列功能码的报文格式固定,上下文关联性较小,CPS 的变异率为 69.36% ~75.28% 。Modbus/TCP 写系列功能码的报文负载字段取决于用户,上下文关联性大,CPS 变异率为 68.31% ~80.03% 。实验结果表明,无论是变异率的大小,还是变异率的稳定性,CPS 都高于基于随机策略的测试用例生成的 Sulley 工具。

表 4 Modbus 功能码测试结果

功能码	CPS			Sulley		
	测试用例总数	异常测试用例	变异率/%	测试用例总数	异常测试用例	变异率/%
0x01	1 538	1 085	70.55	1 428	690	48.31
0x02	940	652	69.36	1 022	507	49.61
0x03	1 800	1 355	75.28	1 690	948	56.09
0x04	2 054	1 492	72.64	2 230	1 008	45.20
0x05	2 048	1 403	68.31	1 802	1 139	63.21
0x06	3 058	2 148	70.24	2 450	1 393	56.86
0x0F	2 594	2 076	80.03	3 018	2 094	69.38
0x10	3 409	2 496	73.21	2 908	1 931	66.40

3.2.3 针对工控系统的渗透攻击

框架中渗透攻击脚本能够支持多种漏洞利用方式,如表 5 所示。基于图 10 所示的测试环境和漏洞挖掘模块所提供的指纹信息,对工控设备的脆弱性进行渗透测试。

表 5 CPS 工具部分漏洞利用脚本

漏洞类型	工控设备类型	工控厂商	漏洞编号
权限许可和访问控制	Quantum PLC 以太网模块	Schneider	CVE-2011-4861
堆缓冲区溢出	KingView SCADA	亚控科技	CVE-2011-0406
远程利用	S7-300/400 PLC	Siemens	CNVD-2016-05901
拒绝服务	Cisco IOS Common Industrial Protocol	Cisco	CVE-2016-6391
SQL 注入	Advantech SCADA WebAccess	Advantech	CVE-2012-0244

如图 13 所示,工程师站的编程软件是 Unity Pro,负责编写 PLC 程序并下发到下位机 Quantum PLC 中,其通过文件服务器进行固件的远程更新,通过流量分析,发现内置硬编码密钥,攻击者可通过该密码账户下载 PLC 的固件,以及对其进行恶意更新,注入 RootKit,造成严重后果。

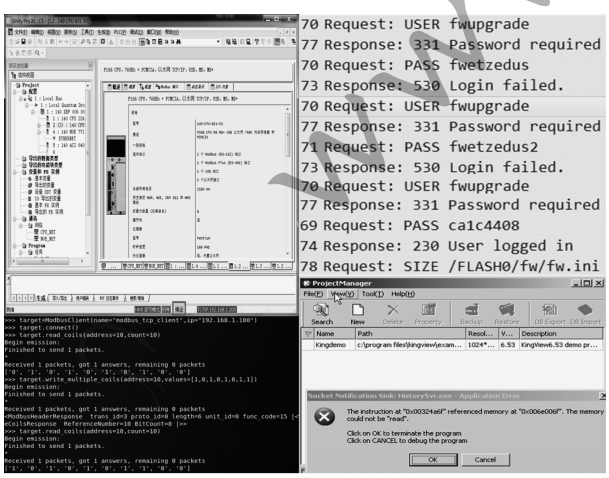

图 13 渗透测试效果

此外,该软件使用的通信协议是 Modbus/TCP,缺乏现代化的安全功能,容易遭受数据包重放攻击。操作员站使用的是亚控科技的 SCADA 软件,负责监控下位机 PLC 的运行状态,根据指纹比对,发现其服务组件存在已知的堆缓冲区溢出,发送特定的数据包可导致软件崩溃,甚至是达到代码执行的目的。

3.3 工具对比

将该渗透测试框架与 Nmap、MSF、Core Impact 等工具进行各方面的比较,结果如表 6 所示。可以看出:CPS 通过模块组合的方式进行渗透测试工具的开发,与成熟的渗透工具相比,其各功能模块耦合性低,可单独进行工作,易于扩展,其脚本开发受到的限制较少,灵活性高;在具体的功能模块方面,因为 CPS 为面向工业控制系统所设计并实现的,所以在系统探测和漏洞利用方面,在与现有通用工具的纵向比较下,其系统扫描覆盖面低,漏洞利用方式少,但基于工控系统的特殊性,既保留了传统的漏洞利用方式,又具有针对工控系统的渗透测试,因而针对性强;此外,根据工控系统注重稳定可靠性、版本

和补丁更新少的现状,CPS 还包括了基于协议模糊测试的漏洞挖掘功能,特别是基于协议描述模型和工控协议反馈特征的测试用例生成,可大幅提高渗透测试的效率。

表 6　渗透测试工具对比

指标	Nmap + MSF	Core Impact	CPS
模块耦合性	高	高	低
脚本开发周期	长	长	低
灵活性	低	低	高
覆盖面	广	广	窄
针对性	低	低	高

4　结束语

工业控制系统网络化和信息化的深度融合提高了生产效率,但同时又使系统面临信息安全问题。针对当前面向工控系统渗透测试研究较少的现状,本文设计一种渗透测试工具框架。实验结果表明其能针对工控系统进行有效的效率探测、协议脆弱性检测和渗透测试,且结构简明、易于扩展。但该渗透测试工具的功能还不够完善,如系统探测模块所支持的工控协议数量较少、模糊测试的效率还有待提升。鉴于工业控制系统信息安全的特殊性和复杂性,可以通过基于可信计算的工业以太网协议改进方案来提高其通信的安全可靠性[25],这将是下一步的研究方向。

参考文献

[1] 国家工业信息安全产业发展联盟. 工业信息安全态势白皮书(2017 年)[EB/OL]. [2018-03-10]. https://max.book118.com/html/2018/1007/5043141300001320.shtm.

[2] ZHU B,JOSEPH A,SASTRY S. A taxonomy of cyber attacks on SCADA systems[C]//Proceedings of 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing. Washington D.C.,USA:IEEE Press,2012:380-388.

[3] BODUNGEN C E,SINGER B L,SHBEEB A,等. 黑客大曝光:工业控制系统安全[M]. 戴超,张鹿,译. 北京:机械工业出版社,2017.

[4] 陶耀东,李宁,曾广圣. 工业控制系统安全综述[J]. 计算机工程与应用,2016,52(13):8-18.

[5] 彭勇,江常青,谢丰,等. 工业控制系统信息安全研究进展[J]. 清华大学学报(自然科学版),2012,52(10):1396-1408.

[6] 王炎,刘嘉勇,刘亮,等. 漏洞利用工具研发框架研究[J]. 计算机工程,2018,44(3):127-131.

[7] 严俊龙. 基于 Metasploit 框架自动化渗透测试研究[J]. 信息网络安全,2013(2):53-56.

[8] 姚宇,祝烈煌,武传坤. 工业控制网络安全技术与实践[M]. 北京:机械工业出版社,2017.

[9] 屈婉莹,魏为民,朱苏榕. 工业控制系统通信协议安全研究[C]//全国智能电网用户端能源管理学术年会. 上海:出版者不详,2015:220-224.

[10] 冯涛,鲁晔,方君丽. 工业以太网协议脆弱性与安全防护技术综述[J]. 通信学报,2017,38(增刊):185-196.

[11] SHAHZAD A,LEE M,LEE Y K,et al. Realtime MODBUS transmissions and cryptography security designs and enhancements of protocol sensitive information[J]. Symmetry,2015,7(3):1176-1210.

[12] HUITSING P,CHANDIA R,PAPA M,et al. Attack taxonomies for the Modbus protocols[J]. International Journal of Critical Infrastructure Protection,2008,1(1):37-44.

[13] VAIDYA B,MAKRAKIS D,MOUFTAH H T. Authentication and authorization mechanisms for substation automation in smart grid network[J]. IEEE Network,2013,27(1):5-11.

[14] PREMNATH A P,JO J Y,KIM Y. Application of NTRU cryptographic algorithm for SCADA security[C]// Proceedings of International Conference on Information Technology: New Generations. Washington D. C., USA: IEEE Press,2014:341-346.

[15] 张环宇,陈凯. 基于零动态的工控系统攻击检测识别安全模型[J]. 计算机工程,2017,43(10):98-103.

[16] FORMBY D,SRINIVASAN P,LEONARD A,et al. Who's in control of your control system? device fingerprinting for cyber-physical systems[C]//Proceedings of Network and Distributed System Security Symposium. San Diego, USA: IEICE,2016:1-15.

[17] 李伟. 基于 Modbus 协议的工控节点设计与实现[J]. 计算机工程,2010,36(16):226-228.

[18] 司马莉萍,贺贵明,陈明榜. 基于 Modbus/TCP 协议的工业控制通信[J]. 计算机应用,2005,25(z1):29-31.

[19] BOSSERT G, HIET G. Towards automated protocol reverse engineering using semantic information[C]// Proceedings of ACM Symposium on Information, Computer and Communications Security. New York, USA:ACM Press,2014:51-62.

[20] DUCHÊNE J,GUERNIC C L,ALATA E,et al. State of the art of network protocol reverse engineering tools[J]. Journal of Computer Virology and Hacking Techniques, 2017(2):1-16.

[21] ANTROBUS R,FREY S,GREEN B,et al. SimaticScan: towards a specialised vulnerability scanner for industrial control systems[C]//Proceedings of the 4th International Symposium on ICS and SCADA Cyber Security Research. Belfast,UK:[s. n.],2016:1-8.

[22] VOYIATZIS A G, KATSIGIANNIS K, KOUBIAS S. A Modbus/TCP fuzzer for testing Internet worked industrial systems[C]//Proceedings of IEEE Conference on Emerging Technologies and Factory Automation. Washington D.C.,USA: IEEE Press,2015:1-6.

[23] 张亚丰,洪征,吴礼发,等. 基于范式语法的工控协议 Fuzzing 测试技术[J]. 计算机应用研究,2016,33(8):2433-2439.

[24] VARGAS C,LANGFINGER M,VOGEL-HEUSER B. A tiered security analysis of industrial control system devices[C]// Proceedings of IEEE International Conference on Industrial Informatics. Washington D. C., USA: IEEE Press, 2017: 399-404.

[25] 詹静,杨静. 基于远程证明的可信 Modbus/TCP 协议研究[J]. 四川大学学报(工程科学版),2017,49(1):197-205.

编辑　金胡考