Journal of Computer Applications
计算机应用, 2020, 40(9): 2650 - 2656
ISSN 1001-9081
CODEN JYIIDU
2020-09-10
http://www.joca.cn

文章编号:1001-9081(2020)09-2650-07
DOI:10.11772/j.issn.1001-9081.2019122214

# 基于工控业务仿真的高交互可编程逻辑控制器蜜罐系统设计实现

赵国新[1],丁若凡[2,3],游建舟[3*],吕世超[3],彭　锋[1],李　菲[1],孙利民[3]
(1. 北京石油化工学院 信息工程学院,北京 102617; 2. 北京化工大学 信息科学与技术学院,北京 100020;
3. 中国科学院 信息工程研究所,北京 100089)
(*通信作者电子邮箱 youjianzhou@iie.ac.cn)

**摘　要**:工控蜜罐的诱捕能力受仿真程度显著影响,针对现有工控蜜罐缺乏业务逻辑仿真的问题,提出了一种基于工控业务仿真的高交互可编程逻辑控制器(PLC)蜜罐设计框架和搭建方法。首先,基于工控系统的交互层次提出了一种新的工控系统(ICS)蜜罐分类方法;然后,根据工控设备的不同仿真维度,将蜜罐诱捕过程分为过程仿真循环和服务仿真循环;最后,通过定制的数据转存模块将过程数据转换到服务仿真循环中,以实现业务逻辑数据的实时响应。实验以西门子S7-300 PLC设备为参考,结合典型工控蜜罐软件Conpot和建模仿真工具Matlab/Simulink,实现了信息服务仿真和控制过程仿真的协同工作。实验结果表明,相较于Conpot,高交互PLC蜜罐系统新增了11种西门子S7设备私有功能,其中读(04 Read功能码)写(05 Write功能码)操作实现了对PLC的I区7个通道的监测和Q区1个通道的控制。这种全新的蜜罐系统突破了现有交互层次和方式的局限,为工控蜜罐设计拓展了新方向。

**关键词**:蜜罐;工控系统;Conpot;高交互;S7comm私有功能
**中图分类号**:TP393.08　　**文献标志码**:A

# Design and implementation of high-interaction programmable logic controller honeypot system based on industrial control business simulation

ZHAO Guoxin[1], DING Ruofan[2,3], YOU Jianzhou[3*], LYU Shichao[3], PENG Feng[1], LI Fei[1], SUN Limin[3]
(1. *College of Information Engineering, Beijing Institute of Petrochemical Technology, Beijing* 102617, *China*;
2. *College of Information Science and Technology, Beijing University of Chemical Technology, Beijing* 100020, *China*;
3. *Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100089, *China*)

**Abstract:** The capability of entrapment is significantly influenced by the degree of simulation in industrial control honeypots. In view of the lack of business logic simulation of existing industrial control honeypots, the high-interaction Programmable Logic Controller (PLC) honeypot design framework and implementation method based on industrial control business simulation were proposed. First, based on the interaction level of industrial control system, a new classification method of Industrial Control System (ICS) honeypots was proposed. Then, according to different simulation dimensions of ICS devices, the entrapment process in honeypot was divided into a process simulation cycle and a service simulation cycle. Finally, in order to realize the real-time response to business logic data, the process data was transferred to the service simulation cycle through a customized data transfer module. Combining typical ICS honeypot software Conpot and the modeling simulation tool Matlab/Simulink, the experiments were carried out with Siemens S7-300 PLC device as the reference, and so as to realize the collaborative work of information service simulation and control process simulation. The experimental results show that compared with Conpot, the proposed PLC honeypot system newly adds 11 private functions of Siemens S7 devices. Especially, the operating read (function code 04 Read) and write (function code 05 Write) in the new functions realize 7 channel monitoring for I area data and 1 channel control for Q area data in PLC. This new honeypot system breaks through the limitations of existing interaction levels and methods and finds new directions for ICS honeypot design.

**Key words:** honeypot; Industrial Control System (ICS); Conpot; high-interaction; S7comm private function

**收稿日期**:2020-01-03;**修回日期**:2020-03-01;**录用日期**:2020-03-11。　**基金项目**:国家重点研发计划项目(2018YFC1201102);广东省重点研发计划项目(2019B010137004);国家电网公司总部科技项目(522722180007)。

**作者简介**:赵国新(1963—),男,辽宁铁岭人,教授,硕士,主要研究方向:智能控制、工控安全; 丁若凡(1995—),男,江苏扬州人,硕士研究生,主要研究方向:工控安全、蜜罐技术; 游建舟(1992—),男,福建龙岩人,博士研究生,主要研究方向:工控安全、物联网安全、蜜罐技术; 吕世超(1985—),男,河北保定人,助理研究员,博士研究生,主要研究方向:无线通信安全、工控安全; 彭锋(1993—),男,湖北黄冈人,硕士研究生,主要研究方向:智能控制、工控安全; 李菲(1994—),女,北京人,硕士研究生,主要研究方向:工控安全、故障诊断; 孙利民(1966—),男,河南淮阳人,研究员,博士,主要研究方向:工控安全、物联网安全。

## 0　引言

随着“中国制造2025”的推进,传统工业开始了信息化、数字化、智能化的产业升级。与此同时,随着大量工业设备不可避免地接入互联网,工业控制系统信息安全也面临着日益严重的挑战和威胁[1]。自2010年震网事件以来,工控信息安全问题一直备受国内外各界关注。从国家互联网应急中心[2]发布的《2017年中国互联网网络安全报告》可知,世界各国越来越重视工控网络信息安全。基于工控安全领域相关研究[3-4]表明,为了应对互联网中潜在的威胁,仅仅依靠被动防御是不够的,应用蜜罐技术进行主动防御是工控安全防护领域的杀手锏[5-6]。

蜜罐技术是一种安全威胁的主动检测技术,它通过设置诱饵性质的虚拟系统来吸引攻击者入侵并对其进行攻击捕获。蜜罐技术在近十几年内呈现交互能力由低到高、兼容功能由少到多的趋势。事实上,蜜罐的分类方式最常用的是按照其与外界的交互能力分为低、中、高交互蜜罐,其区别在于提供交互的空间是否覆盖完整的操作系统。

由于工控系统的设计封闭性和架构特殊性,上述以通用服务器为对象的分类标准难以评估工控的过程控制特性。因此,本文从架构特点出发,划分了工控设备的交互层次,提出一种新的工控蜜罐分类方法。低交互工控蜜罐具备网络层的基础协议栈的通信能力。中交互工控蜜罐具备操作系统层指令模拟能力,如开机关机、代码上传/下载等。高交互工控蜜罐具备生产现场业务过程控制的仿真能力。

基于上述分类标准,本文设计并实验验证了一种可编程逻辑控制器(Programmable Logic Controller, PLC)蜜罐框架,主要工作如下:

1)设计了基于工控业务仿真的PLC蜜罐系统框架,由工控业务模块、数据转存模块和信息服务模块三部分组成。

2)提出了工控私有协议的解析与模拟方法,实现了S7comm私有功能拓展。通过与西门子S7-300 PLC设备的交互实验结果,新增了11种S7comm私有功能。

3)提出了Simulink的工控业务实时仿真方法,其提供的仿真数据与S7comm私有功能相互协同,有效实现控制指令的执行与响应。在交互层次上贯穿了信息域和物理域,大大增强蜜罐的业务真实度和可靠性。

## 1　相关工作

国内外各信息安全领域的研究者一直致力于蜜罐技术的发展。2004年Cisco公司以honeyd[7]为基础首先实现了具有Modbus服务的工控蜜罐系统[8]。2011年Tamminen[9]提出的Kippo是一款基于Python并支持多操作系统的蜜罐工具。2013年Glastopf蜜网项目[10]发布了首个开源工控蜜罐框架Conpot,使用Python编写,主要实现了对Modbus、S7comm、简单网络管理协议(Simple Network Management Protocol, SNMP)、超文本传输协议(HyperText Transfer Protocol, HTTP)等多种工控协议和互联网协议的仿真。2014年Buza等[11]实现的CryPLH以S7comm服务为基础,扩展实现了SNMP、HTTP服务,增强了蜜罐的交互性。2015年实现的Cowrie[12]是Kippo的继承者,扩展了对安全拷贝协议(Secure Copy Protocol, SCP)、安全外壳协议(Secure SHell, SSH)文件传输协议(SSH File Transfer Protocol, SFTP)和Telnet协议的支持。2016年Lau等[13]提出的XPOT实现了对Nmap等系统指纹识别工具的欺骗,作者指出如果能结合工业过程模拟,会进一步提升蜜罐的交互性。同年Litchfield等[14]提出了HoneyPhy,该框架考虑了信息物理系统(Cyber-Physical System, CPS)过程和设备的行为,进行了简单的理论验证和实验。2017年Kyung等[15]提出一种基于软件定义网络(Software Defined Network, SDN)的蜜网系统HoneyProxy,支持低高交互蜜罐动态转换。而国内对蜜罐技术的研究起步较晚,北京大学计算机研究所“狩猎女神”项目组于2004年开始捕获并深入分析攻击案例。近年来,中国科学院信息工程研究所研究并实现了针对电力系统的IEC104规约蜜罐、人机接口(Human Machine Interface, HMI)电力调度系统蜜罐等与行业紧密结合的蜜罐。

从工控特有的分类看,上述工控蜜罐主要在信息域交互方面进行拓展和开发,或仅实现了理论设计,未实现有效的实验验证和应用部署。因此,现有工控蜜罐工作应当被归类为中交互工控蜜罐,主要缺乏物理域交互能力。

## 2　高交互PLC蜜罐系统架构设计

针对现有工控蜜罐存在无法与攻击者交互,或者有交互但数据、系统可信度低的问题,本文基于工控业务仿真的固有特征,设计了一种高交互PLC蜜罐系统架构,为蜜罐通信提供真实的实时生产数据和生产环境来欺骗攻击者,从而在全新领域实现了蜜罐的交互能力突破。

如图1所示,本文设计的高交互PLC蜜罐总体架构分为信息服务仿真模块、过程控制仿真模块和数据转存模块3个部分,数据流动分为服务仿真循环和过程仿真循环两条路线。

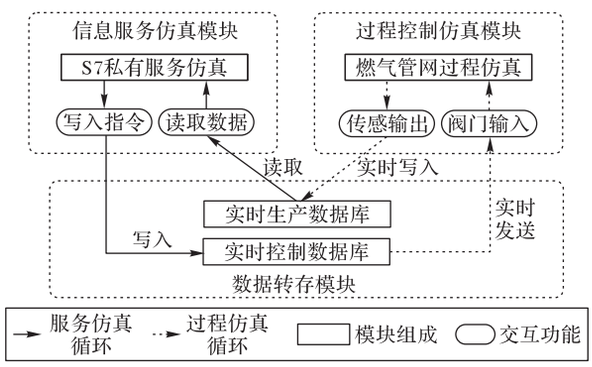


图1　高交互PLC蜜罐总体架构

Fig. 1　High-interaction PLC honeypot architecture

信息服务仿真模块通过部署Conpot蜜罐来仿真西门子S7-300PLC设备,使用Conpot内置的S7comm服务器与外界进行交互,并以此为基础开发实现了多种S7comm私有服务的仿真。S7comm私有服务仿真能够根据攻击者的请求,调用相应函数,通过读取数据转存模块中实时生产数据库里的数据并组入响应数据包,或者将攻击者提供的控制指令写入实时控制数据库,以满足交互需求。本模块与数据转存模块之间的数据流通构成了服务仿真循环。

过程控制仿真模块对燃气管网过程进行了仿真建模。通过在Simulink中运行该仿真模型,系统能够生成实时生产数据,并通过仿真传感器实时输出,最终写入到数据转存模块的实时生产数据库中;同时该系统具备仿真的阀门输入接口,会接收实时控制数据库实时发送的数据作为系统的控制信号。本模块与数据转存模块的数据流通构成了过程仿真循环。

数据转存模块是上述两个模块的交互中转站,也是两个数据仿真循环的核心。数据转存模块中建立了两个不同的数据库,分别为实时生产数据库和实时控制数据库,使用脚本程

序来实现一系列读取、存储和发送的功能。通过这里的数据存储、流通，信息服务仿真模块能够读取到过程控制仿真模块的实时生产数据，过程控制仿真模块也能够根据信息服务仿真模块下达的实时指令改变生产状态，以此实现了控制过程仿真运行状况的闭环逻辑。

## 3 关键技术

### 3.1 S7comm私有协议解析与实现方法

S7comm协议是西门子S7系列PLC内部集成的一种私有不公开协议，属于传输控制协议/网际协议（Transmission Control Protocol/Internet Protocol，TCP/IP）协议族的一种。它运行在应用层中，经过特殊优化，用于西门子设备之间或者与外界进行通信。S7comm协议常用的通信方式是基于以太网的客户端/服务端模式：PLC设备作为服务端，接收外界访问请求数据包并执行相应服务，返回响应数据包；外界访问者作为客户端，与PLC进行通信，发送请求数据包并接收响应数据包。本文针对Conpot的S7comm服务器进行了深度开发，从协议仿真的角度开发实现了更多S7comm私有服务功能，从而符合本文设计的PLC蜜罐系统的需求。

#### 3.1.1 S7私有协议的解析和模拟

S7comm协议不同设备间使用S7数据包进行通信。如图2所示，S7数据包使用了多种协议进行协议数据单元（Protocol Data Unit，PDU）封装，S7数据在经过面向连接的传输协议（Connection-Oriented Transport Protocol，COTP）协议和应用程数据传输协议（ISO transport services on top of the TCP，TPKT）协议打包后，由TCP/IP协议进行连接和输送。

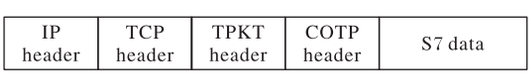


图2 S7comm协议包头格式

Fig. 2 S7comm protocol packet header format

如图3所示，S7comm协议服务端和客户端之间的通信流程分为三次握手。第一次握手是经过客户端和服务端COTP请求与应答，建立基于国际标准化组织传输协议（International Organization for Standardization_Transport Protocols，ISO_TP）的连接；第二次握手进行S7通信设置，建立S7comm连接；第三次握手进行S7comm服务的应答交互，最终服务端会生成基于特定S7comm私有功能的响应数据包返回给客户端。

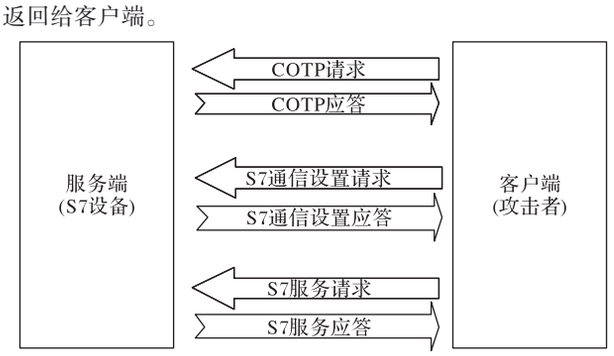


图3 S7comm协议通信流程

Fig. 3 S7comm protocol communication process

根据以上对S7comm协议通信三次握手原理的解析，Conpot通过对S7通信系统中服务端功能进行模拟，建立了S7comm服务器。如图4所示，其处理信息的流程主要分为以下几步：

1）S7comm服务器从Conpot获取执行流，与客户端建立连接。然后，进入会话处理流程，开始循环接收数据包，为客户端提供服务。

2）S7comm服务器会接收握手信息的前四个字节：如果接收的数据为空，S7comm服务器会结束本次会话；否则，会接收握手信息的剩余信息。然后，S7comm服务器会解析包头，提取出length参数，用于判定是否是非法的S7comm数据包请求。

3）S7comm服务器完成第一次握手，建立ISO_TP连接。ISO_TP握手信息的标识tpdu_type参数值为0xe0，只有通过本次握手，ISO_TP连接才能建立起来。

4）S7comm服务器完成第二次握手，建立S7comm连接。S7comm握手信息的标识tpdu_type参数值为0xf0，只有通过本次握手，S7comm连接才能建立起来。

5）S7comm服务器开始第三次握手，开始接收S7comm的数据循环。服务器解析TPKT和COTP层数据，当请求数据的tpdu_type参数值为0xf0时，表明该PDU是通信数据（而非握手信息），S7comm会解析此数据并据此生成响应数据包；然后，将响应数据包发送给客户端，完成第三次握手；最后，S7comm服务器会准备接收本次会话的下一个数据包。

S7comm服务器具备完整的信息交互机能，通过扮演PLC设备的角色来取信于外界攻击者。除此之外，S7comm服务器还集成了日志记录功能，研究者可以通过分析日志来获取攻击者信息、研究攻击模式、提升防护能力。

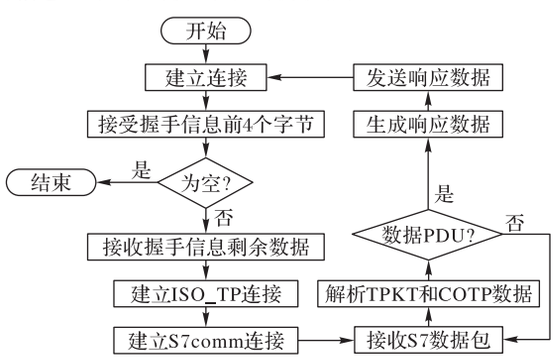


图4 Conpot中S7comm服务器工作流程

Fig. 4 Workflow of S7comm server in Conpot

#### 3.1.2 新增S7comm私有功能

S7功能码是S7comm协议数据包中用来标明自身所代表何种S7comm私有功能的数字码，每个功能码代表一种S7comm私有功能。在Conpot的S7comm服务器通信过程中，当客户端向服务端发送请求数据包时，数据包中S7Data包含的功能码将告诉服务端需要执行的是哪种服务。服务端会据此调用不同的功能码程序来产生特定数据。这些数据经过处理后会被组入响应数据包，最终返回给客户端。

Conpot虽然搭建了S7comm服务器的交互框架，却并没有广泛地实现S7comm协议内的诸多S7comm私有功能。目前为止，S7comm协议中解析了12种主功能码，20种次级功能码，而Conpot除了简单的次级功能“读取系统状态列表”外，其余功能码对应的S7comm私有功能均未实现，因此实际上无法正常进行S7通信，也就无法返回攻击者客户端正常的响应

数据包。

2019年游建舟等[16]关注并初步进行了S7comm私有功能的开发工作,本文在其基础上进行了进一步的方法整理和代码重构。如表1所示,通过与真实PLC设备做交互实验,在Conpot中新增了11种S7comm私有服务。

**表1　在Conpot中新增的S7comm服务器功能码**

Tab. 1　New S7comm function codes added in Conpot

| 功能码 | 功能名称 | 描述 |
|---|---|---|
| 0x04 | Read | 读取指定数据 |
| 0x05 | Write | 写入数据 |
| 0x1a | Request download | 请求下载程序 |
| 0x1b | Download block | 下载程序块 |
| 0x1c | Download end | 下载结束 |
| 0x1d | Upload start | 开始上传程序 |
| 0x1e | Upload | 上传程序 |
| 0x1f | Upload end | 上传结束 |
| 0x28 | PLC start | 启动PLC |
| 0x29 | PLC stop | 停止PLC |
| 0xf0 | Communication setup | 请求建立通信 |

S7comm私有功能扩展的开发流程如下:

1)主机PC连接西门子S7-300PLC。其中PC的IP要与PLC配置在同一网段内。

2)根据S7comm协议的握手机制向PLC发送包含待实现功能码的三段请求数据包,建立S7comm通信。

3)用wireshark抓取PLC设备的响应数据包。

4)分析Conpot源码中对S7数据包的解析过程,对执行程序进行修改和完善,确保其对新增S7comm私有功能的兼容性。

5)基于之前捕捉到的PLC的响应,在S7comm服务器中添加实现对应功能码的数据生成器。其任务是根据功能码对应的不同S7comm私有功能,输出特定parament值和data值,将其写入S7data,再交给S7comm客户端中其他模块进行进一步的协议封装。

在设置对应S7comm私有功能的功能码响应数据时,单纯的信息重放是不足以欺骗攻击者的,需要根据数据包字段结构来对响应数据包进行编辑。以Read功能码和Write功能码为例,通过上述流程,获得其响应数据包如下:

1)Read功能码。

0300003902f0803203000000050002001200000401ff04000000000000000000000000000000

2)Write功能码。

0300002402f080320100000009000e00050501120a10010001000083000029000300010 1

表2分别是其数据包字段解析示例,前者由服务端输出蜜罐能够提供给攻击者的信息,后者由客户端输入攻击者想要写入的信息。本文选择Read和Write功能码进行深度解析,为蜜罐系统建立了读取数据、控制数据的功能,不仅在S7comm私有服务方面具备功能协同性,也在现有系统框架下,将真实攻击者与PLC的通信逻辑纳入了物理域的信息交互之中。

**表2　Read和Write功能码响应数据包的字段解析**

Tab. 2　Field analysis of response package of Read and Write function code

| 功能码 | 数据字段 | 功能含义 |
|---|---|---|
| Read | 0300 | 报文头 |
| | 0039 | 总长度57 |
| | 02f08032 | S7固定字段 |
| | 03 | S7type,表示返回包 |
| | 00000005 | 序列号 |
| | 0002 | 固定字段 |
| | 0012 | 有效数字长度 |
| | 0000 | 固定字段 |
| | 04 | 功能码编号read |
| | 01 | 数据块个数:1 |
| | ff0400 | 数据前缀 |
| | 000000000000000 00000000000000 | 读取的数据 |
| Write | 0300 | 报文头 |
| | 0024 | 总长度36 |
| | 02f08032 | S7固定字段 |
| | 01 | S7type,表示请求包 |
| | 00000009 | 序列号 |
| | 000e | 固定字段 |
| | 0005 | 有效数字长度 |
| | 05 | 命令起始符 |
| | 01 | 数据块个数 |
| | 120a10 | 数据前缀 |
| | 01 | 按bit写入 |
| | 0001 | 写入数据个数 |
| | 0000 | 写入数据块编号 |
| | 83 | 写入哪种数据块 |
| | 000029 | 写入地址偏移量 |
| | 0003 | 写入方式 |
| | 0001 | bit个数 |
| | 01 | 写入的数据 |

### 3.2　基于Simulink的以太网通信与控制

为了提升信息服务仿真模块中S7comm私有服务仿真的真实性、在过程控制仿真模块里提供实时更新动态的生产数据,并在蜜罐系统内构建模拟真实生产现场PLC的工作过程,需要使用Matlab/Simulink来搭建实时仿真系统。Simulink是Matlab中的一种可视化仿真工具,自带种类繁多、功能强大的模块库,被广泛应用在系统建模、数据处理和业务仿真中。

仿真系统使用了多个关键组件,来实现过程业务仿真模块与其他模块的数据实时交互传输。

To Instrument组件用于将Simulink中的数据输出到外界设备中,在仿真系统中用于模拟传感器,将工业过程产生的各项实时数据发送到数据转存模块中的实时生产数据库。如表3第一部分所示,To Instrument支持对通信协议、地址、端口、数据类型、缓冲区大小、传输间隔、传输格式等进行设置以满足系统需求。

Query Instrument组件用于在Simulink中接收外界信号。在仿真系统中用于模拟系统总阀,控制系统紧急停车。如表3第二部分所示,与To Instrument组件类似,同样需要进行相应预先设置。

Real-time sync组件用于Simulink中仿真系统的实时化处理,通过引入此组件,Simulink系统的仿真运行速度会与外界

物理时间保持一致(而不是在几秒内运行完毕全部仿真流程),从而模拟工业现场实时产生数据并接收控制的过程,使得整个PLC蜜罐系统的数据流转更加真实。

**表3 To Instrument和Query Instrument组件设置**

Tab. 3 Settings of To Instrument and Query Instrument components

| 组件 | 设置 | 内容 |
|---|---|---|
| To Instrument | Timeout | 11 |
| | Buffer size | 64 |
| | Interface | TCPIP |
| | Remote host | '192. 168. 206. 133' |
| | Port | 1080 |
| | Output format | ASCII |
| | ASCII format string | '%7. 2f' |
| Query Instrument | Timeout | 11 |
| | Buffer size | 64 |
| | Interface | TCPIP |
| | Remote host | '192. 168. 206. 133' |
| | Port | 1090 |
| | Output format | ASCII |
| | ASCII format string | '%d' |

## 4 系统实现

本文构建的高交互PLC蜜罐系统以开源蜜罐Conpot和Simulink仿真器为基础,基于S7comm私有功能开发和工控业务仿真,采用信息服务仿真、数据转存、过程控制仿真三模块体系,通过模块间的信息交换,实现了具备高交互性和高仿真度的PLC蜜罐系统。

### 4.1 过程控制仿真模块

过程控制仿真模块使用Matlab/Simulink搭建了燃气管网仿真系统。燃气管网是一个由多过程组成的燃气输送控制系统,包括高压、中高压、低压三部分,通过监测并控制不同阶段的压强、流速、温度保持稳定预设值,最终输出标准状态的燃气到用户家中。

在Simulink中搭建的燃气管网仿真系统架构如图5所示。

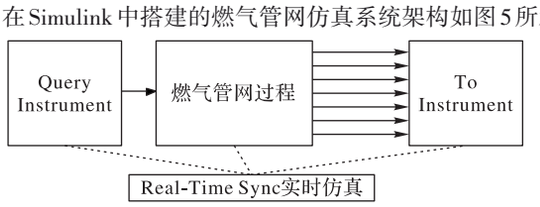


图5 燃气管网仿真系统架构

Fig. 5 Simulation system architecture of gas pipe network

通过不同组件之间的相互协作,结合过程模拟、通信交互、实时仿真三种功能,最终实现了接收实时控制信号、输出实时生产数据的功能。燃气管网过程组件内集成了燃气管网系统生产过程仿真的诸多物理特性,包括高中低压三部分传递函数构建、干扰量模拟、开关选择模拟等,当仿真系统运行正常时,该过程能够产生7个持续、实时输出的数据流,分别为运行过程中不同的流量、温度、压强值。To Instrument组件采集以上燃气管网系统产生的数据,并通过TCP/IP协议将其输出到数据转存模块的实时生产数据库中,实现了本模块系统传感器的功能。Query Instrument组件接收数据转存模块通过TCP/IP协议发送的实时控制指令流,然后将其输入到燃气管网过程中,只要控制指令不变,运行状态就不会变;一旦外部输入的控制指令流发生变化,燃气管网过程的运行状态和输出数据也会随之变化,其实现的是本模块系统总阀的功能。Real-time sync组件负责整体系统的实时化,这使得该工业过程的仿真和通信行为都是实时进行的,符合蜜罐系统的设计要求。

### 4.2 数据转存模块

数据转存模块的脚本使用python3语言编写,调用的核心库是Socket和MySQL,通过搭建、操作数据库并与其他模块进行通信,实现了接收、存储生产数据和调用、发送控制指令流的功能。

实时生产数据库存储着系统的实时生产数据,程序脚本会通过Socket库与过程控制仿真模块的To Instrument组件相连接,并接收其输出的生产数据;然后经过一定的格式化处理,通过SQL语句将其存入数据库内。由于数据的产生和传输是实时的,因此实时生产数据库中的数据是实时变化更新的最新数据。

实时控制数据库存储系统的实时控制指令。与实时更新数据的实时生产数据库不同,实时控制数据库的数据并非实时输入,而是实时输出。实时控制数据库会使用Socket脚本,对过程控制仿真模块中的Query Instrument组件实时发送内部存储的数据作为控制指令,从而为工业过程提供了持续的阀门信号。

### 4.3 信息服务仿真模块

在Ubuntu系统内以S7-300模板部署二次开发后的Conpot蜜罐,以此模拟西门子S7-300 PLC与外界攻击者进行通信,从而实现系统所需的信息服务。

在交互过程中,Conpot的S7comm服务器在执行Read功能码对应的S7comm私有服务时,预设的脚本函数会使用SQL语句读取数据转存模块中的实时生产数据数据库;同样,在执行Write功能码对应的服务时,预设的脚本函数会使用SQL语句来将数据转存模块中实时控制数据库的数覆盖为新的数,从而控制过程控制仿真模块。

## 5 实验测试与分析

### 5.1 实验环境

本文通过控制网仿真攻击来测试高交互PLC蜜罐系统的连通性和工作逻辑。如表4所示,实验设备分为蜜罐设备和测试设备,通过以太网进行通信。高交互蜜罐系统部署在蜜罐设备内,其中信息服务仿真模块和数据转存模块位于虚拟机,过程控制仿真模块位于宿主机。测试设备为同一IP段内的独立计算机。

**表4 实验环境配置**

Tab. 4 Configuration of experimental environment

| 序号 | 名称 | 硬件配置 | 操作系统 |
|---|---|---|---|
| 1 | 蜜罐设备 | Celeron J1900处理器<br>4 GB内存<br>128 GB工业级固态硬盘<br>工控主板 | Windows 10(宿主机)<br>Ubuntu14. 04<br>(虚拟机) |
| 2 | 测试设备 | Celeron J1900处理器<br>4 GB内存<br>128 GB工业级固态硬盘<br>工控主板 | Windows 10 |

### 5.2 控制网攻击测试

控制网攻击测试的主要目的是验证蜜罐系统的信息域交

互能力。将测试设备与蜜罐设备的以太网输入端口相连,利用Nmap探测脚本分别进行了设备操作系统指纹识别、系统探测。然后测试S7comm私有服务实现情况,以“0x28 PLC start”为例,向蜜罐设备发送基于真实设备反馈信息的数据包,如图6所示,蜜罐系统能够识别出数据包请求的S7comm私有服务为“28”并返回对应响应数据包。经完整测试,蜜罐系统支持表1中列举的全部11种S7comm私有服务。

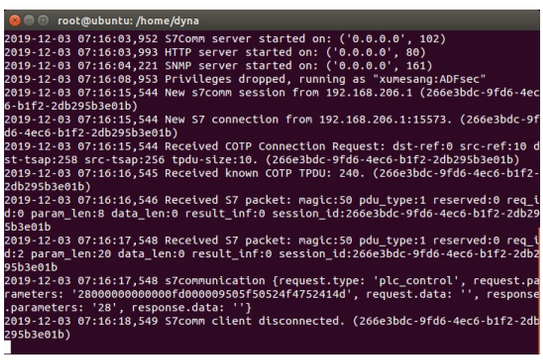


图6　蜜罐系统日志

Fig. 6　Log of honeypot system

### 5.3　业务逻辑测试

业务逻辑攻击测试的主要目的是验证蜜罐系统的物理域交互能力。在虚拟机内以S7-300模式部署定制版Conpot,运行信息服务仿真模块主程序和数据转存模块中主程序,在宿主机中运行Simulink实时仿真,开始更新实时数据。

如图7所示,测试设备对蜜罐系统进行了完整测试来验证其连接稳定性和功能协同性。考虑到过程控制仿真模块中信号的复杂多样,以总阀(图8)和管道压强值PT2的全过程状态(图9)为例展示蜜罐系统中的运行状态。

在716 s前,过程控制仿真模块持续正常运行。在此间,测试设备通过使用包含Read功能码的请求数据包Read_1向蜜罐系统发起第一次通信,请求读取PLC的I区实时数据,得到系统返回的响应数据包。响应数据包的实时数据来自过程控制仿真模块,在数据转存模块模拟真实PLC的I区7通道数据格式进行格式化组合,为28位7通道十六进制数“557931e12af52eec13dd2808244b”,这段正常I区数据作为S7data携带的PLC的I区数据的一部分被组入响应数据包。

在716 s时,测试设备使用包含Write功能码的数据包向蜜罐系统发起第二次通信,请求写入控制指令,得到写入成功的响应数据包,这表示攻击者已成功劫持了PLC输出。此时数据转存模块发送出去的控制指令也随攻击指令发生了变化,可见图8中过程控制仿真模块的总阀信号由0阶跃为1,阀门由开启转为关闭,过程控制仿真模块的生产状态立即发生变化,图9中PT2输出值发生突变,系统的正常运行遭到破坏,开始输出失常的实时数据,直至仿真结束。

在716 s后,再次使用包含Read功能码的数据包发起第三次通信,请求读数据,得到过程控制仿真模块生产瘫痪状态下系统返回的响应数据包,此时接收到的数据已变为失常I区数据“0000000000000000000000027c024e8”,可见其中末位2个通道值保持稳定(温度为室温不变),其余过程量归零,这表示系统传感器输出异常,攻击者据此可知生产过程遭到了破坏。


图7　高交互蜜罐系统测试流程

Fig. 7　Test process of high-interaction honeypot system

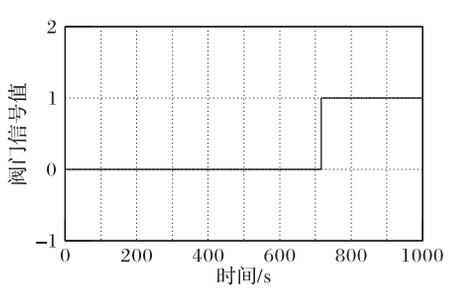


图8　仿真期间总阀信号状态图

Fig. 8　Signal state diagram of main valve during simulation

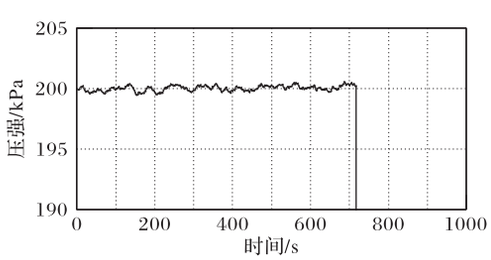


图9　仿真期间管道压强PT2信号状态图

Fig. 9　Signal state diagram of pipe pressure PT2 during simulation

通过以上测试可知,本文设计的高交互PLC蜜罐系统各模块能稳定工作,内部连接和对外交互运转正常,多次通信证

实了蜜罐系统实现的不同S7comm私有服务在迎合攻击者的行为方面配合默契,逻辑严密,具备良好的协同性。其仿真工业过程提供的实时生产数据和可供破坏的生产环境形成的物理域交互循环对只接触过信息域交互蜜罐的攻击者来说更具诱骗性。综上可得出结论,本文设计的高交互PLC蜜罐系统达到了引言中提出的高交互的指标。相较于以往的中低交互工控蜜罐,本文所设计的PLC蜜罐系统具有显著的突破性。

## 6 结语

蜜罐技术是对抗日益猖獗的互联网威胁建立的防御手段,由于传统工控蜜罐交互能力的局限和输出信息的随机化,不具备足够的真实性和欺骗性。本文针对此问题,提出了一种结合工控业务仿真的高交互PLC蜜罐系统搭建方法。当攻击者对基于工控业务仿真的高交互PLC蜜罐系统进行攻击时,其不仅能够获取到实时更新的生产数据,还能够控制PLC蜜罐输出对生产系统写入数据来造成生产停车,完成逻辑闭环的蜜罐系统也因此具备更高的诱骗性。相较于传统低交互、中交互蜜罐,本文提出的蜜罐系统发展了新的交互层次,在信息域交互的基础上不仅拓展了物理域的业务逻辑支持,交互形式也更加立体、丰富、真实。

本文的研究目标集中于Simulink仿真系统与定制Conpot蜜罐的数据交换框架、S7comm私有功能的扩展和S7comm协议数据包的字段解析上,没有针对PLC程序的控制、解析进行研究,此外由于使用了预设的攻击脚本,没有进行广泛的攻击行为描述,这是未来研究的方向。

**参考文献**(References)


[1] 范文斌. 工业控制协议安全防护分析[J]. 电子科学技术, 2015, 2(3): 334-337. (FAN W B. Analysis of security protection on industrial control protocol [J]. Electronic Science and Technology, 2015, 2(3): 334-337.)

[2] 国家计算机网络应急技术处理协调中心. 2011年中国互联网网络安全态势报告[J]. 信息网络安全, 2012, 12(4): 98-100. (National Computer Network Emergency Response Technical Team/Coordination Center of China. 2011 China Internet network security situation report[J]. Netinfo Security, 2012, 12(4): 98-100.)

[3] GUPTA J N D, SHARMA S K. Handbook of Research on Information Security and Assurance [M]. Hershey, PA: Information Science Reference, 2008: 527-532.

[4] NARUOKA H, MATSUTA M, MACHII W, et al. ICS honeypot system (CamouflageNet) based on attacker's human factors[J]. Procedia Manufacturing, 2015, 3: 1074-1081.

[5] SIMÕES P, CRUZ T, PROENÇA J, et al. Specialized honeypots for SCADA systems[M]// LEHTO M, NEITTAANMÄKI P. Cyber Security: Analytics, Technology and Automation, ISCA 78. Cham: Springer, 2015: 251-269.

[6] IRVENE C, FORMBY D, LITCHFIELD S, et al. HoneyBot: a honeypot for robotic systems[J]. Proceedings of the IEEE, 2018, 106(1): 61-70.

[7] PROVOS N. A virtual honeypot framework[C]// Proceedings of the 13th USENIX Security Symposium. Berkeley: USENIX Association, 2004: 1-14.

[8] POTHAMSETTY V, FRANZ M. SCADA HoneyNet project: building honeypots for industrial networks[EB/OL]. [2019-10-29]. http://scadahoneynet.sourceforge.net/.

[9] TAMMINEN U. Kippo - SSH honeypot[EB/OL]. [2019-10-29]. https://github.com/desaster/kippo.

[10] MushMush. Conpot: ICS/SCADA honeypot[EB/OL]. [2019-04-06]. https://github.com/mushorg/conpot.

[11] BUZA D I, JUHÁSZ F, MIRU G, et al. CryPLH: protecting smart energy systems from targeted attacks with a PLC honeypot [C]// Proceedings of the 2014 International Workshop on Smart Grid Security, LNCS 8448. Cham: Springer, 2014: 181-192.

[12] Cowrie Project. Cowrie SSH/Telnet honeypot[EB/OL]. [2019-10-29]. https://github.com/cowrie/cowrie.

[13] LAU S, KLICK J, ARNDT S, et al. POSTER: towards highly interactive honeypots for industrial control systems [C]// Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016: 1823-1825.

[14] LITCHFIELD S, FORMBY D, ROGERS J, et al. Rethinking the honeypot for cyber-physical systems [J]. IEEE Internet Computing, 2016, 20(5): 9-17.

[15] KYUNG S, HAN W, TIWARI N, et al. HoneyProxy: design and implementation of next-generation honeynet via SDN [C]// Proceedings of the 2017 IEEE Conference on Communications and Network Security. Piscataway: IEEE, 2017: 1-9.

[16] 游建舟,张悦阳,吕世超,等. 基于数据包分片的工控蜜罐识别方法[J]. 信息安全学报, 2019, 4(3): 83-92. (YOU J Z, ZHANG Y Y, LYU S C, et al. Method of ICS honeypot identification based on packet-sharding [J]. Journal of Cyber Security, 2019, 4(3): 83-92.)


This work is partially supported by the National Key Research and Development Program of China (2018YFC1201102), the Key Research and Development Program of Guangdong Province (2019B010137004), the Science and Technology Project of Headquarter of State Grid Corporation of China (522722180007).

**ZHAO Guoxin**, born in 1963, M. S., professor. His research interests include intelligent control, industrial control security.

**DING Ruofan**, born in 1995, M. S. candidate. His research interests include industrial control security, honeypot technology.

**YOU Jianzhou**, born in 1992, Ph. D. candidate. His research interests include industrial control security, IoT security, honeypot technology.

**LYU Shichao**, born in 1985, Ph. D. candidate, research assistant. His research interests include wireless communication security, industrial control security.

**PENG Feng**, born in 1993, M. S. candidate. His research interests include intelligent control, industrial control security.

**LI Fei**, born in 1994, M. S. candidate. Her research interests include industrial control safety, fault diagnosis.

**SUN Limin**, born in 1966, Ph. D., research fellow. His research interests include industrial control security, IoT security.