基于蜜罐的工控蜜网系统的设计与实现

李政达[1],周成胜[2]

(1.华北计算机系统工程研究所,北京 100083;2.中国信息通信研究院安全研究所,北京 100191)

摘 要:随着我国信息化和工业化融合不断深入,工业控制系统的网络安全就显得尤为重要。从主动防御现状、系统架构、实现方法等角度出发,介绍了针对工业控制系统设计的蜜网系统,并对其网络架构和关键技术进行了深入的分析,提出了适合在工控系统中使用的蜜网系统设计方案。通过设计符合工控行业实际情况的蜜网架构,在蜜网中部署传统蜜罐、PLC 蜜罐、真实 PLC 设备以及通过高仿真等关键技术做到攻击诱捕,改变网络攻防博弈不对称局面,使企业运维人员面对威胁早发现早预防。

关键词:工控安全;蜜网系统;蜜罐;网络安全

中图分类号:TP399 文献标识码:A DOI:10.19358/j.issn.2096-5133.2020.08.005

引用格式:李政达,周成胜. 基于蜜罐的工控蜜网系统的设计与实现[J].信息技术与网络安全,2020,39(8):21-26,32.

Design and implementation of honeynet based on honeypot for industrial control system

Li Zhengda[1], Zhou Chengsheng[2]

(1.National Computer System Engineering Research Institute of China, Beijing 100083, China;
2.Institute of Security, China Academy of Information and Communications Technology, Beijing 100191, China)

Abstract: With the deepening of the integration of information and industrialization in China, the network security of industrial control system is particularly important. This paper introduces the honeynet system designed for industrial control system from the perspectives of active defense status, system architecture and realization method, and deeply analyzes its network architecture and key technologies, proposes a honeynet system design scheme suitable for industrial control systems. By designing a honeynet architecture that conforms to the actual situation of the industrial control industry, deploying traditional honeypots, PLC honeypots, real PLC devices in honeynets and through key technologies such as high simulation to achieve attack and trap, the asymmetry situation of network offensive and defensive games can be changed, and the operation and maintenance personnel of enterprises can detect and prevent threats early.

Key words: industrial safety; honeynet system; honeypot; network security

0 引言

自 2010 年震网(Stuxnet)病毒被披露以后,工控安全问题开始引起世界范围的关注。全国人民代表大会常务委员会于 2016 年 11 月 7 日发布《中华人民共和国网络安全法》,网络安全上升到国家战略层面。目前的工业控制系统多以被动防御为主,无法及时应对新型未知的威胁。2019 年正式实施的等保 2.0 更加注重全方位主动防御、动态防御、整体防控和精准防护,并明确了工控行业的网络安全防护要求[1]。

本文介绍了一种针对工业控制系统设计的蜜网。蜜网是在蜜罐技术上发展起来的一个新的概念,又称为诱捕网络,是一种变被动为主动的网络安全技术[2]。蜜网通过在一个更具有欺骗性的网络架构中部署多个蜜罐以及相应的网络设备,通过模拟真实系统网络架构,达到主动防御、数据捕获的目的。

本系统通过部署蜜网网关、PLC(Programable Logic Controller)蜜罐、工程师站蜜罐等组成蜜网,搭建相应的网络架构,诱导攻击者对蜜网进行攻击,从而对入侵行为进行数据捕获并进行分析,以做到

主动性防御，面对未知威胁及时发现，及早研究应对措施。对收集到的数据进行分析，能够让安全运维人员了解所面对的网络安全威胁，通过蜜网系统与实际生产系统的对比发现系统弱点，以使用适当的技术手段及时弥补缺陷。

1 项目背景

从历史上看，工业自动化控制系统在很大程度上与传统的数字网络是隔离的。在需要连通性的地方，采用了分区架构和设备隔离来保护核心控制系统组件。随着我国信息化和工业化融合进程不断深入，现代信息技术在工控领域的应用越来越广泛，数字化控制、软件技术、网络技术都应用于大规模工业生产环境[3]。同时为了生产效率进一步提高，工控系统内部网络开始接入企业广域网甚至是互联网，这些新技术与传统工控网络的融合在提高了生产效率的同时，也导致了当前工控系统的网络安全面临严峻威胁，工业控制系统的“孤岛”模式被打破。近些年随着漏洞挖掘技术不断成熟，在工业控制系统中的漏洞被发现的数量明显增多，针对工业系统生产控制网攻击事件层出不穷[4]。

虽然大多数工控行业生产数据网为行业内网或内部局域网，但由于存在运维人员非法外联、安全分区不明确、网络边界控制不严格、设备管理不到位等因素，从而都会导致内部网络受到威胁。大部分企业对外部网络渗透的安全防御停留在使用防火墙、入侵检测系统(IDS)、入侵防御系统(IPS)等传统方式应对攻击的层面，这些方式需要设备定义已知的攻击模式，并主要通过模式匹配去阻断非法访问或恶意攻击，依赖于第三方资源库，这种防御方式的致命缺点在于不能主动地学习攻击方式。

2 现状与风险概述

当前的防御体系对新型的网络威胁捉襟见肘，存在网络攻防中信息不对称、博弈不对等。首先，网络中新型的威胁不易被发现，第三方资源库的更新需要一定的周期。当入侵者利用新型漏洞或使用新的隐匿手段入侵系统时，现有的防御体系是无法及时发现的，往往经过一段时间内网传播，有较多设备出现异常时才被运维人员发现。其次，当运维人员发现系统被入侵时，入侵者可能已删除相应的日志记录隐匿踪迹，即使发现被入侵也只能进行查杀、更新补丁进行加固，恢复正常业务，而很难进行攻击溯源，分析入侵者攻击方法、如何利用漏洞以及如何进行传播。

目前国内外针对工业网络的蜜网技术的研究仍处于起步阶段。由 Digital Bond 维护的 SCADA Honeynet 项目核心是 Honeyd[5]，它将创建的虚拟主机的网络流量从适当的端口路由到这些应用程序和脚本。然而，模拟服务提供的交互很少，无法吸引攻击者足够长的时间来分析攻击行为。江苏科技大学的丁晨鹏设计了一种船舶网络工业蜜罐[6]，使用虚拟化技术，以 Docker 容器为载体，开发了支持 S7 协议、SNMP 协议和 HTTP 协议的蜜罐，其定制化程度高，无法广泛应用。

本文通过构建工控蜜网系统，可做到提前与攻击者交互的效果，保障系统安全运行的同时也能更进一步对攻击行为进行捕捉并分析，了解攻击者入侵系统使用的技术与方法，并通过蜜罐资源尽量拖延入侵者，转移攻击目标以便给安全生产人员足够的反应时间来防御攻击，及时弥补漏洞，尽最大努力保护真实网络并降低损失[7]。

3 蜜网系统设计

3.1 系统架构

蜜网系统需要实现的核心功能为：数据捕获、数据分析、数据控制。总体而言，工控系统蜜网的整体构架在结合现有的互联网蜜网技术的情况下，同样要兼顾典型工业控制系统网络构架，只有做到两者相互融合，才能发挥出蜜网系统构架的优势。本文经过对工控蜜网系统的需求分析设计了如图 1 所示的功能模块图。

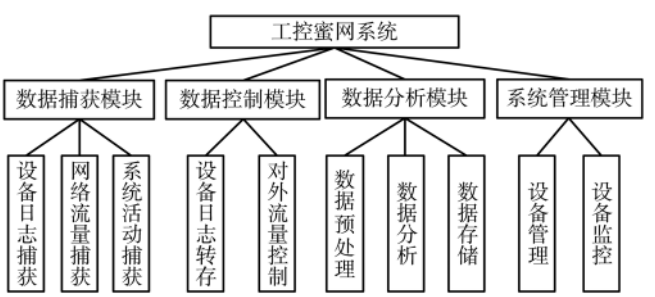

图 1 蜜网系统功能模块图

数据捕获模块：数据捕获的目的是记录入侵事件和恶意行为，以便日后进行处理与分析。它是一个强制性的功能，任何类型的蜜罐都必须有这个功能。该模块确定了对于要捕获的数据类型可以分为设备日志、网络流量和设备活动信息，这些数据都反映了入侵者在系统内的活动。本文蜜网系统由于

是模拟工控系统，那么其中必然需要模拟工控设备，同时需要对其数据流进行捕获。数据捕获的能力是评价一个蜜网的重要标准，蜜网能够收集的数据越全面，蜜网系统就越成功。

数据控制模块：由于工业控制系统对可用性的要求，在部署蜜网进行安全防护时不能对工控系统的可用性产生影响，所以蜜网系统必须控制从蜜网发出对其外部其他系统的访问。为了保护蜜网以外的其他系统，必须对出站的连接行为进行管控，但同时也要考虑仿真性，尽量不能被攻击者察觉。对内的流量控制功能用于控制入侵者从外部对蜜网内部的访问，蜜网内不是所有蜜罐都是高交互的[8]，这样就需要使用重定向技术，当低交互蜜罐无法处理入侵者的请求时，将请求转发到其他可以响应该请求的蜜罐中去，提高系统的仿真性。

数据分析模块：数据分析的目的是对收集到的数据进行分析来获取攻击的信息，以揭示攻击技术和对手的动机。因此，如果不能对数据进行分析，蜜罐系统的价值就会降低。经蜜网捕获到的数据需要经过处理，消除噪声，然后使用有效的数据进行分析展示，并持久化存储。

系统管理模块：系统管理需要提供设备管理功能和设备监控功能。设备管理功能要提供易于部署、配置的管理机制，并涵盖蜜罐生命周期的所有方面，从蜜罐节点建立到安全远程管理、安装服务配置最后到下线、删除。

3.2 网络架构

工控蜜网系统是针对典型的工业控制系统，将目前的蜜罐技术、虚拟化技术与工业系统进行融合，在具备典型工控系统架构的同时，又兼顾蜜网技术结构的一种新型技术架构。要想最大限度地获取新的漏洞信息以及攻击方法等数据，吸引入侵者，则需要将蜜网系统部署在一个有足够吸引力的工作网络里。

为了保证企业内部网络的安全，需要与蜜网系统划分在不同的网段，同时蜜网系统中蜜罐和数据分析主机也在不同的网段以保证安全。通过分析工控系统典型网络结构，最大程度保证蜜网系统的高仿真性，本文设计的蜜网系统中的蜜网网关是部署在工业控制网络的企业资源层和生产管理层中间的设备，蜜网系统的蜜罐网络向下模拟生产管理层、过程监控层和现场控制层的 PLC 设备。

如图 2 所示，工控蜜网系统的整体架构分为蜜罐网络与监控管理平台两个模块，外部访问经接入路由器进入内部网络，路由器连接网关的 eth0 接口，网关的 eth1 接口与数据分析网连接，eth2 接口与蜜网网络连接。其中 eth0 与 eth2 这两个接口使用桥接模式，且这两个接口使用同一网段，当数据包通过网关时 TTL 的值不会发生递减，并且也不需要提供网关自己的 MAC 地址。因此，蜜网网关对外部的攻击者是透明的，也就是在网络层面无法识别其攻击的网络是蜜网系统[9]。

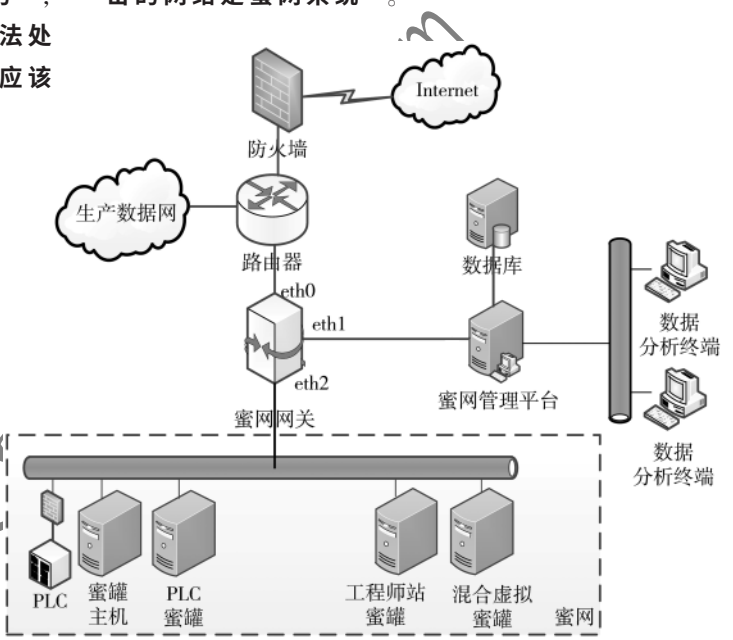

图 2 蜜网网络拓扑图

eht1 接口用来负责将蜜网中传输来的数据发送到蜜网管理平台中，同时 eth1 切断与 eth0 的数据转发。本系统不允许入侵者从路由器经网关直接进入数据分析网，因为这会使蜜网系统变得毫无价值。数据分析网的数据也不需要传输至外部网络，这样就避免了一旦入侵者通过蜜罐网络入侵数据分析网，将数据分析网作为跳板绕过蜜网的数据控制机制对外部网络进行攻击。

由于蜜网系统没有强制访问措施，无法强行要求他人访问或入侵，也就是无论蜜网系统多逼真，只要网络中还有真实企业网络，它就存在被攻击的可能性[10]。为了尽可能避免这种情况的发生，在接入路由器的配置中，采用白名单方式对允许访问的 IP

地址和 MAC 地址进行绑定，对于不在白名单中的IP地址发起的访问全部重定向到蜜网系统。这样提高了生产数据网的安全性，并且增加了入侵者掉入蜜网系统的可能性。

在传统的蜜罐结构基础上，本文系统中蜜罐根据企业所在行业进行设计，包含 PLC 蜜罐、工程师站蜜罐等。在整个平台中以真实主机与虚拟化技术结合的方式，一方面让工控蜜罐系统的逼真度尽可能地高，另一方面使用虚拟化技术，模拟一些不必要使用真实物理机的部分，进而节省成本。采用了灵活的构建方式，通过将实体机与虚拟机共同接入网络，实现了高交互与低交互并存的动态混合虚拟蜜网。蜜网系统包括真实的 PLC 设备、PLC 蜜罐、工程师站蜜罐和虚拟蜜罐等。虚拟 PLC 蜜罐和真实 PLC 设备同时与工程师站进行通信，这样就不仅仅是应对简单的扫描攻击，在入侵者看来，系统更加真实，取得的效果更好。

本文设计的工控蜜网系统是弹性可伸缩的，部署的企业可以根据实际情况，使用虚拟蜜罐替代真实物理机，在兼顾高仿真性的同时，达到节约成本的目的。

4 蜜网系统关键技术的实现方法

在设计蜜网系统时需要考虑蜜网的仿真性、功能性、安全性的结合。更真实地模仿真实的系统能够提高蜜罐的诱骗能力，从而吸引入侵者的注意力。蜜网系统的功能性，体现在蜜网的数据捕获能力，通过捕获有价值的数据以达到部署蜜网的目的。在工控系统中部署其他设备的安全性至关重要，需要通过数据控制技术实现入侵者无法在蜜网中对外发起攻击。

4.1 蜜网仿真技术

要想使蜜网具有高仿真性，则需要使用多种欺骗方法使蜜网系统更像一个真实的生产环境，从而引诱攻击者对其进行网络入侵。本系统主要使用以下方法。

4.1.1 网络流量仿真

产生仿真流量能够弥补虚拟蜜网中没有实时流量的缺陷，使入侵者不能使用分析网络流量的方法发现蜜网的仿真诱捕活动。在蜜罐主机中通过镜像的方式重现生产数据网的网络流量，这使得蜜网系统与真实的生产系统具有较高的相似性。为了进一步确保真实性，系统中部署了真实的西门子 PLC 设备，在蜜罐主机与 PLC 设备中运行真实的工艺流程和数据采集过程，完全真实地重现生产数据网中某些生产活动。同时，本系统使用管道技术将蜜罐网络模块中捕获的数据发送到监控管理平台。

4.1.2 重定向技术

地址转换技术能够将蜜网网络和真实网络分离开来，这样就可以使用真实的操作系统替换低可信度的诱骗方法，增加了隐蔽性的同时增强了仿真性。重定向技术使用重定向代理服务，由代理服务进行地址转换，本文网关选择使用 Ubuntu18.10 作为主机系统，防火墙 Netfilter 提供的目标网络地址转换功能实现静态重定向。

本文还使用了一种动态重定向的选择性机制，允许从蜜罐到互联网的连接自动和动态重定向。其目的是让攻击者产生一种错觉，即其可以从蜜罐连接到外部网络，而实际上，这些连接只是被重定向到另一个蜜罐。

如图 3 所示，本文使用两个 hook 函数，并将它们置于 Netfilter 组件 PREROUTING 链中的 conntrack 函数和 nat 函数之间。第一个 hook 函数负责提取数据包并将它们发送到用户空间中的 dialog_tracker，以便决定是否需要重定向它们。第二个 hook 函数负责为决定需要重新定向数据包添加标签。

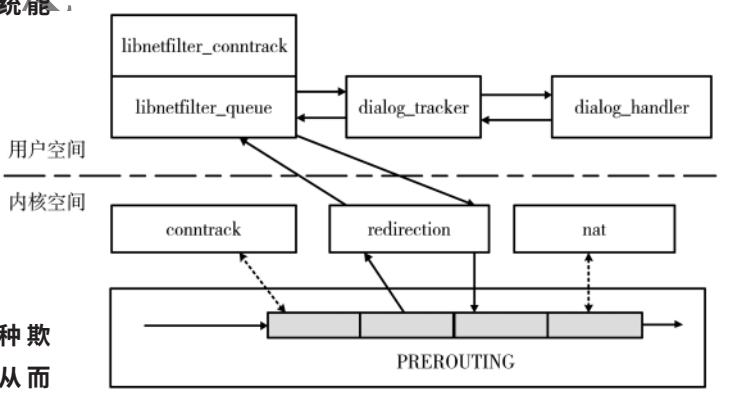

图 3 数据动态重定向实现方法

当一个数据包从外部进入网关设备的网卡的缓存区，首先进入 PREROUTING 链，当 conntrack 函数对数据包进行处理后，由 redirection 模块进行处理，将数据读取到用户空间，进入 libnetfilter_queue 队列，由重定向模块处理。对于每个连接，第一个 hook 函数只提取第一个包并将其发送到 dialog_tracker。然后，dialog_tracker 将数据包转发给 dialog_handler，由它决定这个数据包是否需要重定向或阻塞。做出决定时，dialog_tracker 通知内核模块进行重定向，然后

第二个 hook 函数为需要重定向的数据包添加标签，并将数据包重新发送给链表的下一个函数，数据包被重新注入到相应链表中。链表中下一个函数是 nat 函数，它需要通过将数据包的目标地址更改为系统内的一个蜜罐的地址，来实现动态重定向。

由于 Netfilter 的动态追踪机制，一个连接的重定向只需要重定向此连接的第一个数据包，其他数据包与第一个数据包一样自动处理。

4.2 数据捕获技术

数据捕获是蜜网的核心功能模块，其目标是获取攻击者从探测扫描到实施攻击再到最后离开蜜网过程中，入侵者使用的攻击方法、利用的漏洞及其目的。低交互度蜜罐大多使用静态数据，其中没有真实的流量，数据的捕获经常是通过日志记录，捕获能力有限[11]。与低交互蜜罐相比，高交互程度的蜜网系统的数据捕捉功能优势明显。如图 4 所示，本系统引入分层捕获的机制，做到攻击流量进入蜜网经过的每台设备都进行数据捕获，使用网络数据捕获和操作系统数据捕获两种方法。其中，使用 Iptables 和 Snort 进行网络数据捕获，由操作系统日志和 Sebek 模块组成操作系统层面的数据捕获机制。

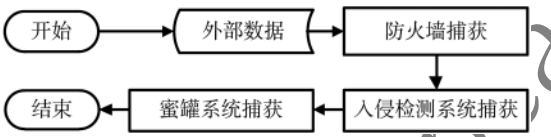

图 4 数据捕获处理流程

4.2.1 网络数据捕获

网关中的 Iptables 是分层捕获机制的第一层，在研究阶段，Iptables 的访问控制规则可以适当放宽，以此来吸引更多的入侵者对蜜网系统进行入侵。在实际部署阶段，Iptables 的访问策略应该与网络接入层的企业防火墙访问控制规则宽松程度持平或适当放宽，以起到保护真实系统的效果，并发现企业部署的防火墙的规则不合理之处，起到主动防御的效果。Snort 安装在网关中，起到捕获数据包并过滤的作用，当攻击流量信息与已有规则匹配时，Snort 会对其进行记录并丢弃。

蜜罐操作系统内部在网络层和应用层设置捕获点实现数据捕获。

网络层：对于每个协议，相关端口上的输入和输出流量，防火墙 Iptables 条目都会自动添加，以便使用 Netfilter 队列将原始流量重定向到驻留在应用程序级别的蜜罐软件。这里接收到的每个数据包都由回调函数处理，如果其他方法仍然需要该数据包，回调函数会将其存储在临时缓冲区中，或者直接将其发送到数据库组件中的关联缓冲区。在前者的情况下，在所有方法使用完捕获的包之后，最后一个方法将数据发送到数据库组件中的缓冲区，这种方法能够使用整个包的原始状态进行捕获和检查。

应用层：如果有通过协议实现的服务，每个模拟服务可以集成通过上述 Netfilter 队列重定向接收的原始数据并在内部使用。这种数据捕获机制的一个优点是，可以通过使用标准技术将诸如处理 TCP 连接之类的任务从蜜罐软件层面下放到操作系统上，从而提高性能。

4.2.2 Sebek 基于内核的数据捕获

虽然网络数据的捕获一般不会被入侵者察觉，但是随着入侵技术的发展，入侵者越来越多地使用加密工具来保护传输通道，如果目标机器没有安装加密服务，那么入侵者可能会自己安装如 SSH、加密的客户端程序等服务。如果没有密钥，基于网络的数据捕获工具就极难破译出被加密的数据的具体内容，为了解决这种情况，本文使用在内核中收集用户行为的工具 Sebek。

如图 5 所示，Sebek 客户端通过调用自己创建的系统调用函数 new_read 替换正常的系统调用函数，记录入侵者调用系统默认 read 函数的所有数据，并把记录的数据包载入缓存，之后对数据包进行封装。封装后的数据包包含了调用的内容信息、调用的进程描述、调用的时间和数据的大小。数据包封装之后直接发送给驱动设备，绕过套接字代码

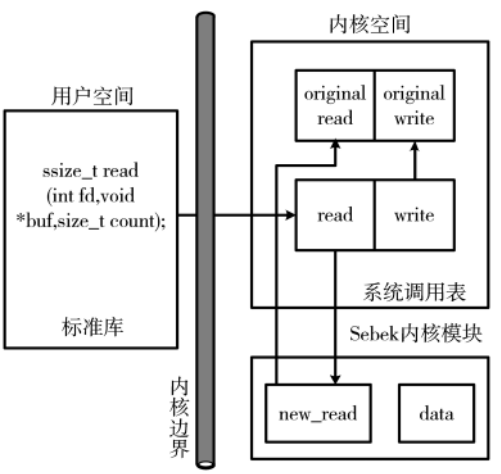

图 5 Sebek 捕获消息机制

和包过滤器，再把数据发送到 Sebek 服务器[12]。由于嗅探器一般是基于使用原始套接字接口的 libpcap 函数库的，因此嗅探器也就无法过滤到 Sebek 产生的数据包。数据在使用时一般是在解密情况下操作的，在进行操作时都会产生系统调用，在内核空间收集数据，这样就能截获这个系统调用的访问进程解密后还未处理的数据。

Sebek 客户端模块通过调用自己创建的 new_read 函数替换原来的函数本质就是改变系统调用表的函数指针。由于 Sebek 客户端模块挂载于内核中的一个单向链表，入侵者在对链表进行扫描时，能够发现 Sebek 客户端模块，这样攻击者可能会发现该主机是一台蜜罐主机[13]。为了防止这种情况发生，本文通过安装 cleaner 模块替代这个 Sebek 客户端模块，再通过 clearner 模块调用 Sebek 模块。这种方法有两方面效果：首先，入侵者通过遍历无法找到 Sebek 客户端模块起到了隐藏模块的效果；其次，入侵者无法从内核中删除客户端模块，进而保护了蜜罐主机的安全性。

4.3 数据控制技术

由于蜜网中的蜜罐是用来吸引攻击者，其本身会有一些故意预留的漏洞。如果蜜网系统中某些宿主机本身被黑客攻陷，那么某个蜜罐网系统可能已经被识破，蜜网系统可能被黑客利用，作为攻击其他系统的跳板。因此，既要防止蜜网内部的网络风暴，又要防止蜜罐主机被当成跳板机影响企业自身办公数据网乃至生产数据网。数据控制的挑战在于如何设置出站活动的阈值，攻击者在蜜网系统中的自由度越大，用户能捕获的数据就越全面。但是，攻击者被允许的行为越多，可能造成的威胁就越大，这需要控制允许出站活动的阈值。

蜜网系统会对外部连接蜜罐的访问控制做到适度宽松，但对从蜜网系统向外部网络的连接要进行严格管控，当蜜网系统中的真实物理机发起向外的连接时，很可能是黑客利用蜜网系统对外尝试发起的攻击。然而，数据控制不能轻松地阻断对外的全部连接，这样无疑是在告诉入侵者他可能处在蜜网之内。同时，单纯地阻断也无法获取入侵者对外连接的目的，而入侵者进入蜜网后的行为和目的是需要收集的。

本文蜜网系统数据控制的方法主要包括攻击包抑制和对外连接数限制两种手段，网关主机通过 Snort 实现该功能。入侵检测系统 Snort，经由 libipq 接收来自 Iptables 的数据包，并根据 Snort 的规则集对数据包进行检查，一旦发现恶意代码就对该数据包采取预先定义的策略，然后再将数据包传回给 Iptables 进行阻断[14]。对流出蜜网的数据包进行严格控制，以防黑客使用蜜网作为跳板向外部发起攻击，而对外连接数限制是用来控制黑客对其他网络系统发起的连接数量。开启 Snort 网络入侵检测模式，使用 Filters 过滤器，如果检测到含有恶意代码的数据包，则对其加以拦截并记录到日志文件中，使其不能对第三方网络构成危害。

5 结论

本文论述了为工控系统设计的蜜网系统，对传统蜜网无法对工业控制系统进行高仿真的问题提出了解决方法。系统使用半实物半仿真的方法，采用真实设备 PLC 与蜜罐主机交互的方式，实现了蜜网系统的网络流量高仿真，保证有效性的同时兼顾灵活性与部署成本。通过隐藏 Sebek 模块、模拟服务等方法做到操作系统高仿真。通过有效的捕获机制保证数据捕获的全面性，使用网关控制达到蜜网系统安全可控。后续研究需要更进一步探索其他蜜网高仿真方法，并丰富数据分析、数据展示功能，也可将有价值的威胁信息上报到漏洞发布平台。

参考文献

[1] 张宇翔，陶源.基于等级保护与可信计算构建我国关键信息基础设施保障体系[J].信息安全研究，2017，3(4)：375-381.

[2] 诸葛建伟，唐勇，韩心慧，等.蜜罐技术研究与应用进展[J].软件学报，2013，24(4)：825-842.

[3] 杨伟，周权.工业控制系统安全及对策[J].网络空间安全，2018，9(7)：60-63，73.

[4] 于长奇.工控设备漏洞挖掘技术研究[D].北京：北京邮电大学，2015.

[5] JICHA A，PATTON M，CHEN H.SCADA honeypots：an in-depth analysis of conpot[C].2016 IEEE Conference on Intelligence and Security Informatics，Tucson，AZ，USA，2016.

[6] 丁晨鹏.船舶网络蜜罐技术研究[D].镇江：江苏科技大学，2019.

[7] 刘风路.蜜罐技术研究与分析[D].长沙：国防科学技术大学，2006.

[8] 许建伟，郑康锋，钮心忻.高交互蜜网系统的分析、

(下转第 32 页)

[2] 甄海涛,王金玉,杨卓林.基于 Hadoop 大数据平台的数据安全研究[J].自动化技术与应用,2019,38(8):159-161.
[3] 谢林江,杭菲璐.大数据背景下数据治理的网络安全策略[J].科技资讯,2018,16(17):5-6.
[4] 陈保.大数据背景下计算机信息安全处理技术探究[J].南方农机,2019(3):169.
[5] 李妩可,黎元,颜宁.大数据技术在网络入侵检测的应用[J].科学技术创新,2018(26):79-80.
[6] 孟祥富.大数据技术在计算机信息系统中的应用研究[J].办公室业务,2017(24):190,192.
[7] 王小君.网络信息安全防范与 Web 数据挖掘系统的设计与研究[J].电子设计工程,2018,26(12):83-87.
[8] 赵卫东.基于移动设备的实训互动管理平台前端设计与实现[J].重庆科技学院学报(自然科学版),2019,21(3):100-103.
[9] 李刚,陈怡潇,黄沛烁,等.基于日志分析的信息通信网络安全预警研究[J].电力信息与通信技术,2018,16(12):1-8.
[10] 贾迪,黄河滔.对 Web 安全性测试技术的分析[J].信息安全与技术,2014,5(5):68-69.
[11] 吴翰清.白帽子讲 Web 安全[M].北京:电子工业出版社,2014.
[12] 吴兰.Web 应用系统的渗透测试研究[J].电脑编程技巧与维护,2013(6):111-112.
[13] 曲卓,周翰逊,耿天华.信息安全渗透测试流程的研究[J].北方交通,2015(12):112-114.
[14] 徐绍飞,龚家瑜,杨亚萍.医疗行业 Web 应用程序渗透测试实例研究[J].计算机与数字工程,2018,46(1):122-125.
[15] 郎智哲,封筱宇,董齐芬.浅谈 Web 渗透测试的信息收集[J].电子技术与软件工程,2017(8):13-16.

(收稿日期:2020-04-17)

作者简介:

张颢芳(1997-),女,硕士,主要研究方向:网络攻防。

康春颖(1976-),通信作者,女,硕士,教授,主要研究方向:网络攻防。E-mail:kangchunying@hlju.edu.cn。

张伟(1976-),男,硕士,高级工程师,主要研究方向:信息处理。

(上接第 26 页)

设计与实现[C].2009 年中国高校通信类院系学术研讨会论文集,2009.
[9] 张秀岭,万旻,骆建彬,等.Linux 下基于 Squid 的多能代理系统与透明网关解决方案[J].微计算机应用,2004(5):534-539,561.
[10] 杨晓丹.蜜网技术在军队网络安全中的应用研究[J].信息与电脑(理论版),2013(9):127-128.
[11] 谭琼玲.浅谈蜜罐系统的实现技术[J].中国科技信息,2010(7):80-82.
[12] 朱一帅,吴礼发.基于 Sebek 的蜜罐识别机制研究[J].信息技术,2009,33(1):83-86.
[13] BALAS E,TRAVIS G,VIECCO C.A dynamic filtering technique for Sebek system monitoring[C].IEEE Information Assurance Workshop.IEEE,2006.
[14] CHAMOTRA S,SEHGAL R K,ROR S,et al.Honeypot deployment in broadband networks[C].International Conference on Information Systems Security,2016:479-488.

(收稿日期:2020-04-07)

作者简介:

李政达(1994-),男,硕士研究生,主要研究方向:网络安全、工业互联网安全。

周成胜(1982-),男,硕士,工程师,主要研究方向:工业自动化、行业信息化、工业互联网安全。

版权声明