(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110351237 B
(45)授权公告日 2020.07.10

(21)申请号 201910435072.1

(22)申请日 2019.05.23

(65)同一申请的已公布的文献号
申请公布号 CN 110351237 A

(43)申请公布日 2019.10.18

(73)专利权人 中国科学院信息工程研究所
地址 100093 北京市海淀区闵庄路甲89号

(72)发明人 孙利民 栾世杰 吕世超 游建舟 石志强 李红

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 苗青盛 张睿

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 109639733 A,2019.04.16,
CN 105447385 A,2016.03.30,
CN 107566401 A,2018.01.09,
CN 106341819 A,2017.01.18,
CN 106973071 A,2017.07.21,
CN 107465702 A,2017.12.12,
郭骞.《基于沙盒技术的应用层蜜罐软件实现》.《中国优秀硕士学位论文全文数据库 程科技Ⅱ辑》.2019,第2019卷(第5期),C042-1049.

审查员 肖丽金

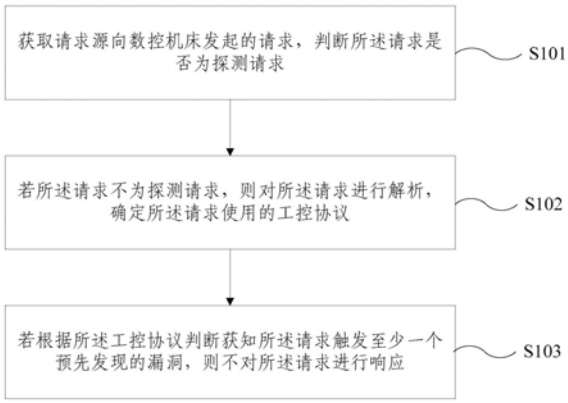
权利要求书2页 说明书10页 附图2页

(54)发明名称

用于数控机床的蜜罐方法及装置

(57)摘要

本发明实施例提供一种用于数控机床的蜜罐方法及装置。其中,方法包括:获取请求源向数控机床发起的请求,判断请求是否为探测请求;若请求不为探测请求,则对请求进行解析,确定请求使用的工控协议;若根据工控协议判断获知请求触发至少一个预先发现的漏洞,则不对请求进行响应。本发明实施例提供的用于数控机床的蜜罐方法及装置,通过模拟真实数控机床对请求的响应,能有效地诱导攻击者的非法访问,混淆攻击者的视听,能根据攻击者的攻击行为对数控机床进行有针对性的防护,能提高安全防护的可靠性。



CN 110351237 B

1.一种用于数控机床的蜜罐方法,其特征在于,包括:

获取请求源向数控机床发起的请求,判断所述请求是否为探测请求;

若所述请求不为探测请求,则对所述请求进行解析,确定所述请求使用的工控协议;

若根据所述工控协议判断获知所述请求触发至少一个预先发现的漏洞,则不对所述请求进行响应;

其中,所述判断所述请求是否为探测请求之后,还包括:

若所述请求为探测请求,则获取所述请求的探测类型,返回根据所述探测类型生成的响应;

所述确定所述请求使用的工控协议之后,还包括:

若根据所述工控协议判断获知所述请求未触发任一所述预先发现的漏洞,则基于所述工控协议获取所述请求所请求的服务,并返回所述服务的执行结果,作为对所述请求的响应;

所述对所述请求进行解析之后,还包括:

若未确定出所述请求使用的工控协议,则针对所述请求进行数据捕获;

所述确定所述请求使用的工控协议之后,还包括:

若根据所述工控协议判断获知所述请求触发至少一个所述预先发现的漏洞,则针对所述请求进行数据捕获;

所述判断所述请求是否为探测请求之后,还包括:

针对所述请求进行数据捕获。

2.根据权利要求1所述的用于数控机床的蜜罐方法,其特征在于,所述获取向数控机床发起的请求之后,还包括:

对所述请求进行日志记录。

3.一种用于数控机床的蜜罐装置,其特征在于,包括:

指纹模拟模块,用于获取请求源向数控机床发起的请求,判断所述请求是否为探测请求;

协议交互模块,用于若所述请求不为探测请求,则对所述请求进行解析,确定所述请求使用的工控协议;

漏洞部署模块,用于若根据所述工控协议判断获知所述请求触发至少一个预先发现的漏洞,则不对所述请求进行响应;

其中,所述蜜罐装置还用于,所述判断所述请求是否为探测请求之后,若所述请求为探测请求,则获取所述请求的探测类型,返回根据所述探测类型生成的响应;

所述确定所述请求使用的工控协议之后,若根据所述工控协议判断获知所述请求未触发任一所述预先发现的漏洞,则基于所述工控协议获取所述请求所请求的服务,并返回所述服务的执行结果,作为对所述请求的响应;

所述对所述请求进行解析之后,若未确定出所述请求使用的工控协议,则针对所述请求进行数据捕获;

所述确定所述请求使用的工控协议之后,若根据所述工控协议判断获知所述请求触发至少一个所述预先发现的漏洞,则针对所述请求进行数据捕获;

所述判断所述请求是否为探测请求之后,针对所述请求进行数据捕获。

4.一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现如权利要求1和权利要求2任一项所述的用于数控机床的蜜罐方法的步骤。

5.一种非暂态计算机可读存储介质，其上存储有计算机程序，其特征在于，该计算机程序被处理器执行时实现如权利要求1和权利要求2任一项所述的用于数控机床的蜜罐方法的步骤。

用于数控机床的蜜罐方法及装置

技术领域

[0001] 本发明涉及计算机技术领域，更具体地，涉及一种用于数控机床的蜜罐方法及装置。

背景技术

[0002] 近年来，随着智能制造的不断推进，工业制造和互联网深度融合，智能制造背后的网络安全问题不断凸显，其安全需求不断增强。

[0003] 数控机床在工控系统中扮演着非常重要的角色，是实现生产自动化的重要工控设备之一。但是，目前多数企业使用的是诸如发那科(也有译成法兰克，Fanuc)、西门子(Siemens)、三菱(Mitsubishi)及海德汉等国内外厂商生产的数控系统(数控机床上安装的操作系统)。这些数控系统对用户来说就是黑盒子，其是否存在安全后门或安全威胁，用户一无所知。因此，需要对数控机床进行安全防护。

[0004] 目前，对于数控机床的安全防护技术还停留在业务管理层面，主要包括在数控机床区域建立防火墙来监管出入流量的方法，及从结构安全、行为安全、本体安全和基因安全四个维度进行数控网络的安全防护设计的方法。但基于业务管理层面的安全防护方法，通过检测攻击行为进行防护，误报率很高，且无法针对数控机床自身进行安全防护，因而防护的可靠性较差。

发明内容

[0005] 本发明实施例提供一种用于数控机床的蜜罐方法及装置，用以解决或者至少部分地解决现有技术对数控机床进行防护的可靠性较差的缺陷。

[0006] 第一方面，本发明实施例提供一种用于数控机床的蜜罐方法，包括：

[0007] 获取请求源向数控机床发起的请求，判断所述请求是否为探测请求；

[0008] 若所述请求不为探测请求，则对所述请求进行解析，确定所述请求使用的工控协议；

[0009] 若根据所述工控协议判断获知所述请求触发至少一个预先发现的漏洞，则不对所述请求进行响应。

[0010] 优选地，所述判断所述请求是否为探测请求之后，还包括：

[0011] 若所述请求为探测请求，则获取所述请求的探测类型，返回根据所述探测类型生成的响应。

[0012] 优选地，所述确定所述请求使用的工控协议之后，还包括：

[0013] 若根据所述工控协议判断获知所述请求未触发任一所述预先发现的漏洞，则基于所述工控协议获取所述请求所请求的服务，并返回所述服务的执行结果，作为对所述请求的响应。

[0014] 优选地，所述对所述请求进行解析之后，还包括：

[0015] 若未确定出所述请求使用的工控协议，则针对所述请求进行数据捕获。

[0016] 优选地，所述确定所述请求使用的工控协议之后，还包括：

[0017] 若根据所述工控协议判断获知所述请求触发至少一个所述预先发现的漏洞，则针对所述请求进行数据捕获。

[0018] 优选地，所述判断所述请求是否为探测请求之后，还包括：

[0019] 针对所述请求进行数据捕获。

[0020] 优选地，所述获取向数控机床发起的请求之后，还包括：

[0021] 对所述请求进行日志记录。

[0022] 第二方面，本发明实施例提供一种用于数控机床的蜜罐装置，包括：

[0023] 指纹模拟模块，用于获取请求源向数控机床发起的请求，判断所述请求是否为探测请求；

[0024] 协议交互模块，用于若所述请求不为探测请求，则对所述请求进行解析，确定所述请求使用的工控协议；

[0025] 漏洞部署模块，用于若根据所述工控协议判断获知所述请求触发至少一个预先发现的漏洞，则不对所述请求进行响应。

[0026] 第三方面，本发明实施例提供一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，执行所述程序时实现如第一方面的各种可能的实现方式中任一种可能的实现方式所提供的用于数控机床的蜜罐方法的步骤。

[0027] 第四方面，本发明实施例提供一种非暂态计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现如第一方面的各种可能的实现方式中任一种可能的实现方式所提供的用于数控机床的蜜罐方法的步骤。

[0028] 本发明实施例提供的用于数控机床的蜜罐方法及装置，通过模拟真实数控机床对请求的响应，能有效地诱导攻击者的非法访问，混淆攻击者的视听，能根据攻击者的攻击行为对数控机床进行有针对性的防护，能提高安全防护的可靠性。

附图说明

[0029] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0030] 图1为根据本发明实施例提供的用于数控机床的蜜罐方法的流程示意图；

[0031] 图2为根据本发明实施例提供的用于数控机床的蜜罐装置的结构示意图；

[0032] 图3为根据本发明实施例提供的电子设备的实体结构示意图。

具体实施方式

[0033] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0034] 为了克服现有技术的上述问题，本发明实施例提供一种用于数控机床的蜜罐方法

及装置,其发明构思是,通过构建的用于数控机床的蜜罐装置实现蜜罐方法,该蜜罐装置可以有效地诱导攻击者的非法访问,混淆攻击者的视听,进而实现对真实数控机床的保护。

[0035] 图1为根据本发明实施例提供的用于数控机床的蜜罐方法的流程示意图。如图1所示,该方法包括:步骤S101、获取向数控机床发起的请求,判断请求是否为探测请求。

[0036] 需要说明的是,本发明实施例提供的用于数控机床的蜜罐方法的执行主体为预先构建的蜜罐装置。

[0037] 数控机床对外通过特定的端口提供TCP(Transmission Control Protocol,传输控制协议)连接服务,完成NC(Numerical Control,数字控制,简称数控)数据传送、远程控制等功能。特定的端口,与数控机床的数控系统有关。例如,Fanuc数控机床的数控系统,通过8193端口提供TCP连接服务。

[0038] 蜜罐装置通过预先选定的至少一个端口对外提供服务。提供的服务,可以包括搜索、读取、删除、导入NC程序,读取、写入PMC(ProgrammableMachineController,数控机床内置式PLC控制技术)参数,获取各轴坐标、运行时间、加工个数以及获取设备信息等中的至少一种。

[0039] 蜜罐装置用来充当诱饵,引诱攻击者前来攻击数控机床。攻击者实施攻击后,通过监测与分析,可以获知攻击者是如何对数控机床进行攻击的,随时了解针对数控机床发动的最新的攻击和漏洞,从而可以有针对性地对数控机床自身进行安全防护,防护的可靠性更高。

[0040] 蜜罐装置将所有请求的发起者均视为攻击者。

[0041] 攻击者向数控机床发起一个请求。请求是数据包。该请求用于触发数控机床执行数控系统中的某一项服务,数控机床根据该项服务的结果生成响应报文,返回给请求的发起者。攻击者可以为终端,如个人计算机,及智能手机、平板电脑等移动终端。

[0042] 蜜罐装置可以通过监听上述预先选定的各端口,获取该攻击者发起的该请求。

[0043] 蜜罐装置通过解析该请求并回复对应的响应报文,以此来仿真数控机床的基本功能,从而达到引诱攻击的目的。

[0044] 真正的攻击者可以通过安装的网络扫描和嗅探工具,例如Nmap(Network Mapper),发送请求。

[0045] 攻击者的请求可分为三种类型:探测请求、正常握手请求和工控协议请求。正常请求包括正常握手请求和工控协议请求。

[0046] 对攻击者发送的请求进行TCP报头和载荷分析,判断该请求是探测请求还是正常请求。

[0047] 如果该不是探测请求,而是正常请求,则执行后面的步骤S102。

[0048] 步骤S102、若请求不为探测请求,则对请求进行解析,确定请求使用的工控协议。

[0049] 需要说明的是,由于不同厂商的数控系统不同,相应地,不同的数控系统使用的工控协议也不同。

[0050] 例如,Fanuc数控机床使用的工控协议为FOCAS1/2协议,Fanuc Mate 0i-D型数控机床使用的工控协议为FOCAS2协议。

[0051] 当攻击者访问蜜罐装置时,蜜罐装置会根据请求源(即请求的发起者)来建立与该请求源之间的会话。

[0052] 蜜罐装置可以建立会话队列以方便管理与各攻击者之间的会话。当攻击者访问蜜罐装置时，蜜罐装置建立与该攻击者之间的会话，并插入到会话队列中；会话结束后，蜜罐装置将该会话移出会话队列。

[0053] 蜜罐装置可以包括协议分发器。

[0054] 协议分发器对该请求的应用层数据进行匹配，根据固定字段(例如可以将固定字段定义为type字段)将不同工控协议进行区分，从而可以确定该请求使用的工控协议。

[0055] 可以理解的是，蜜罐系统中预置了各种工控协议的基本协议格式，协议格式包括各字段。可以各种工控协议的基本协议格式，是预先对各种工控协议进行逆向得到的。

[0056] 步骤S103、若根据工控协议判断获知请求触发至少一个预先发现的漏洞，则不对请求作出响应。

[0057] 其中，漏洞为使用工控协议的数控系统中的漏洞。

[0058] 需要说明的是，对于每一种工控协议，可以预先获取使用该请求所使用的工控协议的数控系统中的至少一个漏洞，并将各数控系统的上述漏洞部署在蜜罐装置中。蜜罐装置可以模拟上述各漏洞，以便更好地欺骗攻击者。

[0059] 例如，预先发现Fanuc Mate 0i-D型数控机床存在三个拒绝服务漏洞(0Day漏洞)，漏洞编号分别为CNVD-2019-07658、CNVD-2019-07659和CNVD-2019-07660。

[0060] 判断该请求是否触发预先发现的该数控系统中的至少一个漏洞中的任意一个。该数控系统，为使用该请求所使用的工控协议的数控系统。

[0061] 当攻击者在扫描探测后通过发送伪装的正常请求进行尝试性攻击时，如果攻击的是上述至少一个漏洞中的一个，则会触发该漏洞。

[0062] 对于真实的数控机床，触发该漏洞会导致数控机床的宕机，数控机床停止工作，而对于蜜罐装置，蜜罐装置并没有停止工作，但不返回任何结果，不向攻击者发送响应报文，并停止对外提供连接TCP服务(即模拟数控机床上的数控系统切换到拒绝服务的状态，无响应)，以模拟数控机床宕机的情况。

[0063] 由于真实数控机床对该请求的响应为停止工作，停止工作则不会返回响应报文，因而蜜罐装置对该请求的响应为不向攻击者返回任何结果。

[0064] 进一步地，可以在判断获知请求触发至少一个预先发现的漏洞之后，经过预设的时长，蜜罐装置重新对外提供连接TCP服务。

[0065] 预设的时长可以设置为与数控机床重启的耗时接近，例如5分钟，从而可以使攻击者更加确信蜜罐装置是真实数控机床。

[0066] 对于预设的时长的具体值，本发明实施例不作限制。

[0067] 需要说明的是，蜜罐装置对于获取的每一个请求，均以完成响应为结束。无响应也是一种响应，除了无响应之外，其他的响应的形式均为响应报文。

[0068] 需要说明的是，蜜罐装置与攻击者之间的每个会话都是相互独立的。

[0069] 本发明实施例通过蜜罐装置模拟真实数控机床对请求的响应，能有效地诱导攻击者的非法访问，混淆攻击者的视听，能根据攻击者的攻击行为对数控机床进行有针对性的防护，能提高安全防护的可靠性。

[0070] 基于上述各实施例的内容，判断请求是否为探测请求之后，还包括：若请求为探测请求，则获取请求的探测类型，返回根据探测类型生成的响应。

[0071] 具体地,攻击者在信息收集阶段会对被攻击者(数控机床)进行探测扫描。探测类型包括序列号探测、控制报文协议请求探测、传输控制协议拥塞探测、传输控制协议详细探测和用户数据报协议探测中的至少一种。

[0072] 序列号探测可表示为sequence generation(SEQ/OPS/WIN/T1)。

[0073] 控制报文协议(Internet Control Message Protocol,ICMP)请求探测可表示为ICMP echo(IE)。

[0074] 传输控制协议(Transmission Control Protocol,TCP)拥塞探测表示为TCP explicit congestion notification(ECN)

[0075] 传输控制协议详细探测表示为TCP(T2-T7)

[0076] 用户数据报协议探测表示为UDP(U1)。

[0077] 如果确定攻击者所发送的请求为探测请求,要区分出该请求属于哪种协议,如IP、ICMP、TCP还是UDP,根据请求属于的协议确定该请求的探测类型,然后根据不同的探测类型进入不同的执行单元进行响应报文的生成,完成以上流程之后,将生成的响应报文返回至攻击者,实现指纹模拟,以欺骗攻击者。

[0078] 下面以攻击者通过Nmap工具对FANUC Mate 0i-D型数控机床的OS(操作系统,Operating System)的指纹扫描探测为例,说明蜜罐装置进行指纹模拟的实现过程。

[0079] 首先,通过对Nmap对操作系统的指纹探测的原理进行剖析,确定主要针对其发送的5类探测请求(探测类型包括序列号探测、控制报文协议请求探测、传输控制协议拥塞探测、传输控制协议详细探测和用户数据报协议探测)进行欺骗。

[0080] 确定上述5类探测请求之后,在实验环境下,用Nmap扫描FANUC Mate 0i-D型机床,抓取Nmap发送的5类探测请求以及机床给予的响应数据。

[0081] 由于数控机床的数控系统多为基于Linux的系统,可以利用Linux系统中的子系统netfilter,具体利用netfilter框架提供的5个hook中的Local_In点(这是提交协议栈处理之前的一个点,具体为hook2,在此截断,先进行处理),在网卡接收到数据并经协议栈处理前的过程中,将该请求转移至QUEUE(这是iptables的一个规则专用值,分别有DROP、ACCEPT、QUEUE,而QUEUE是用户空间,将所有的请求都转移至用户空间)中,在用户空间通过回调函数进行处理,利用gevent来进行自动切换,以便处理放置于队列的来自于不同请求源的请求。

[0082] 回调函数中,采用以下两种方式处理:

[0083] 若判断请求是否为探测请求的结果为是,则根据已获取的机床对5类探测请求给予的响应数据,模拟指纹的响应结果,即按照真实机床回应的方式修改IP层和TCP层各字段的值。

[0084] 若判断请求是否为探测请求的结果为否,则释放请求并交还给协议栈处理,进而由工控协议中的服务给予响应,生成响应结果。

[0085] 通过上述过程,黑客从系统指纹的角度也无法区分蜜罐装置与真实数控机床,能避免蜜罐装置被Shodan以及Nmap识别出不是真实数控机床。

[0086] 本发明实施例通过对各探测类型的响应数据的模拟,使得攻击者无法从系统指纹的角度识别出蜜罐装置,从而能更有效地诱导攻击者的非法访问,混淆攻击者的视听,能根据攻击者的攻击行为对数控机床进行有针对性的防护,能提高安全防护的可靠性。

[0087] 基于上述各实施例的内容，确定请求使用的工控协议之后，还包括：若根据工控协议判断获知请求未触发任一预先发现的漏洞，则基于工控协议获取请求所请求的服务，并返回服务的执行结果，作为对请求的响应。

[0088] 可以理解的是，攻击者发送的请求也可能并不全是攻击行为，攻击者也可能发送正常请求，以进行试探。

[0089] 具体地，判断该请求是否触发预先发现的使用该请求的工控协议的数控系统中至少一个漏洞中的任意一个之后，若判断结果为该请求未触发任一预先发现的漏洞，则基于该请求使用的工控协议，确定该请求所请求的服务，并模拟该服务的执行结果，作为该请求对应的响应数据。

[0090] 基于该请求使用的工控协议，确定该请求所请求的服务，并模拟该服务的执行结果，具体是通过预先对该工控协议进行逆向得到的该工控协议的基本协议格式实现的。

[0091] 可以理解的是，蜜罐装置中预置了预先对各种工控协议进行逆向得到的各种工控协议的基本协议格式。

[0092] 工控协议包括的服务主要有连接、NC程序搜索删除读取、获取轴信息、获取PMC参数信息等。

[0093] 执行结果为响应报文，生成响应报文之后，将生成的响应报文返回至攻击者。

[0094] 本发明实施例通过模拟正常请求的结果并返回对应的响应数据，能更有效地应对攻击者的试探，使得攻击者更难以识别出蜜罐装置，从而能更有效地诱导攻击者的非法访问，混淆攻击者的视听，能根据攻击者的攻击行为对数控机床进行有针对性的防护，能提高安全防护的可靠性。

[0095] 基于上述各实施例的内容，对请求进行解析之后，还包括：若未确定出请求使用的工控协议，则针对请求进行数据捕获。

[0096] 具体地，未确定出请求使用的工控协议，指解析请求的结果不符合预置的每一种工控协议的基本协议格式，此时，将该请求作为异常数据包。

[0097] 发现异常数据包之后，可以通过蜜罐装置包括的数据捕获模块对该请求的攻击数据进行捕获。

[0098] 数据捕获是蜜罐方法的重要步骤，数据捕获的目的是为了进行数据分析。可以使用Tcpdump来实现原始数据抓取和过滤，完成数据捕获。

[0099] 可以理解的是，对于未能解析的部分功能，本发明实施例将捕获的攻击数据存储于蜜罐装置的本地数据库中。

[0100] 对于捕获的攻击数据，可以进行分析，从而根据分析结果获知攻击者是如何对数控机床进行攻击的，获知针对数控机床发动的最新的攻击和漏洞，从而可以有针对性地对数控机床自身进行安全防护，防护的可靠性更高。

[0101] 本发明实施例针对异常数据包进行数据捕获，能对捕获的数据进行分析，从而能根据更有针对性地对数控机床自身进行安全防护，防护的可靠性更高。

[0102] 基于上述各实施例的内容，确定请求使用的工控协议之后，还包括：若根据工控协议判断获知请求触发至少一个预先发现的漏洞，则针对请求进行数据捕获。

[0103] 具体地，若请求触发了之前在蜜罐装置中部署好的、使用该请求的工控协议的数控系统中的任一漏洞，则可以通过蜜罐装置包括的数据捕获模块对该请求的攻击数据进行

捕获。

[0104] 可以理解的是,对于未能解析的部分功能,本发明实施例将捕获的攻击数据存储于蜜罐装置的本地数据库中。

[0105] 对于捕获的攻击数据,可以进行分析,从而根据分析结果获知攻击者是如何对数控机床进行攻击的,获知针对数控机床发动的最新的攻击和漏洞,从而可以有针对性地对数控机床自身进行安全防护,防护的可靠性更高。

[0106] 本发明实施例针对触发漏洞的请求进行数据捕获,能对捕获的数据进行分析,从而能根据更有针对性地对数控机床自身进行安全防护,防护的可靠性更高。

[0107] 基于上述各实施例的内容,判断请求是否为探测请求之后,还包括:针对请求进行数据捕获。

[0108] 具体地,若判断获知请求为探测请求,则可以通过蜜罐装置包括的数据捕获模块对该请求的攻击数据进行捕获。

[0109] 可以理解的是,对于未能解析的部分功能,本发明实施例将捕获的攻击数据存储于蜜罐装置的本地数据库中。

[0110] 对于捕获的攻击数据,可以进行分析,从而根据分析结果获知攻击者是如何对数控机床进行攻击的,获知针对数控机床发动的最新的攻击和漏洞,从而可以有针对性地对数控机床自身进行安全防护,防护的可靠性更高。

[0111] 本发明实施例针对探测请求进行数据捕获,能对捕获的数据进行分析,从而能根据更有针对性地对数控机床自身进行安全防护,防护的可靠性更高。

[0112] 基于上述各实施例的内容,获取向数控机床发起的请求之后,还包括:对请求进行日志记录。

[0113] 具体地,为了便于对请求的分析,在获取请求之后,蜜罐装置包括的日志记录模块可以根据对该请求的各处理步骤生成相应的日志,对该请求进行日志记录。

[0114] 蜜罐装置在攻击者请求相应的功能的同时,将其请求数据以日志和数据包的形式分别进行存储,日志由分析模块进行处理和展示,数据包则可以留给研究分析人员进行事后分析。

[0115] 日志记录是为了更方便地进行分析和展示。

[0116] 日志记录是可以采用三元组,即时间戳、等级(int型)、请求类别(int型)、详细信息(包括请求源、请求报文和返回报文)。为了更高效,可以通过蜜罐装置包括的日志模块提取应用层数据作为请求和返回报文信息。

[0117] 例如:日志格式如下

[0118] 时间戳:

[0119] 消息等级:0/1/2(值分别对应Normal/Medium/Serious)

[0120] 请求类别:0-32(分别对应32类功能)

[0121] 详细信息:{

[0122] 源:(ip、端口),

[0123] request_data:'a0a0a0a0..',

[0124] response_data:'a0a0a0a0..'

[0125] }

[0126] 可以以预设的时间周期(日每日)生成一个日志文件和一个pcap数据包,并以日期命名,日志交由ELK日志分析展示模块进行分析展示,pcap数据包则留给研究人员进一步提取攻击特征,在事后进行重放实验,验证其是否属于未发现的漏洞并及时上报。

[0127] pcap数据包,即针对该时间周期内获取的请求捕获的攻击数据。

[0128] 可以采用E(Elasticsearch)L(Logstash)K(Kibana)这三个开源软件建立集日志采集、分析和展示的一套解决方案,通过蜜罐装置包括的日志分析展示模块实现对日志的展示和分析。由于采用了E(Elasticsearch)L(Logstash)K(Kibana)这三个开源软件,日志分析展示模块还可以称为ELK日志分析展示模块。

[0129] 需要说明的是,对攻击者发起的非法访问的流量进行甄别分类之后,还可以对威胁性较大的请求以警报进行标记,在进行日志记录时,根据该标记及时发出警报,及时采取措施防止攻击者进一步的破坏。

[0130] 本发明实施例对请求进行日志记录,能对日志进行分析和展示,从而能更好得掌握该请求的情况,能根据更有针对性地对数控机床自身进行安全防护,防护的可靠性更高。

[0131] 图2为根据本发明实施例提供的用于数控机床的蜜罐装置的结构示意图。基于上述各实施例的内容,如图2所示,该装置包括指纹模拟模块201、协议交互模块202和漏洞部署模块203,其中:

[0132] 指纹模拟模块201,用于获取请求源向数控机床发起的请求,判断请求是否为探测请求;

[0133] 协议交互模块202,用于若请求不为探测请求,则对请求进行解析,确定请求使用的工控协议;

[0134] 漏洞部署模块203,用于若根据工控协议判断获知请求触发至少一个预先发现的漏洞,则不对请求进行响应。

[0135] 具体地,指纹模拟模块201通过监听上述预先选定的各端口,获取该攻击者发起的请求,并对该请求进行TCP报头和载荷分析,判断该请求是探测请求还是正常请求。

[0136] 协议交互模块202对该请求的应用层数据进行匹配,根据固定字段(例如可以将固定字段定义为type字段)将不同工控协议进行区分,从而可以确定该请求使用的工控协议。

[0137] 漏洞部署模块203根据工控协议判断该请求是否触发预先发现的使用该工控协议的数控系统中的至少一个漏洞中的任意一个,如果攻击的是上述至少一个漏洞中的一个,则会触发该漏洞,漏洞部署模块203不返回任何结果,不向攻击者发送响应报文,并停止对外提供连接TCP服务,以模拟数控机床宕机的情况。

[0138] 本发明实施例提供的用于数控机床的蜜罐装置,用于执行本发明上述各实施例提供的用于数控机床的蜜罐方法,该用于数控机床的蜜罐装置包括的各模块实现相应功能的具体方法和流程详见上述用于数控机床的蜜罐方法的实施例,此处不再赘述。

[0139] 该用于数控机床的蜜罐装置用于前述各实施例的用于数控机床的蜜罐方法。因此,在前述各实施例中的用于数控机床的蜜罐方法中的描述和定义,可以用于本发明实施例中各执行模块的理解。

[0140] 本发明实施例通过蜜罐装置模拟真实数控机床对请求的响应,能有效地诱导攻击者的非法访问,混淆攻击者的视听,能根据攻击者的攻击行为对数控机床进行有针对性的防护,能提高安全防护的可靠性。

[0141] 图3为根据本发明实施例提供的电子设备的结构框图。基于上述实施例的内容，如图3所示，该电子设备可以包括：处理器(processor)301、存储器(memory)302和总线303；其中，处理器301和存储器302通过总线303完成相互间的通信；处理器301用于调用存储在存储器302中并可在处理器301上运行的计算机程序指令，以执行上述各方法实施例所提供的用于数控机床的蜜罐方法，例如包括：获取请求源向数控机床发起的请求，判断请求是否为探测请求；若请求不为探测请求，则对请求进行解析，确定请求使用的工控协议；若根据工控协议判断获知请求触发至少一个预先发现的漏洞，则不对请求进行响应。

[0142] 本发明另一实施例公开一种计算机程序产品，计算机程序产品包括存储在非暂态计算机可读存储介质上的计算机程序，计算机程序包括程序指令，当程序指令被计算机执行时，计算机能够执行上述各方法实施例所提供的用于数控机床的蜜罐方法，例如包括：获取请求源向数控机床发起的请求，判断请求是否为探测请求；若请求不为探测请求，则对请求进行解析，确定请求使用的工控协议；若根据工控协议判断获知请求触发至少一个预先发现的漏洞，则不对请求进行响应。

[0143] 此外，上述的存储器302中的逻辑指令可以通过软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明实施例的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0144] 本发明另一实施例提供一种非暂态计算机可读存储介质，非暂态计算机可读存储介质存储计算机指令，计算机指令使计算机执行上述各方法实施例所提供的用于数控机床的蜜罐方法，例如包括：获取请求源向数控机床发起的请求，判断请求是否为探测请求；若请求不为探测请求，则对请求进行解析，确定请求使用的工控协议；若根据工控协议判断获知请求触发至少一个预先发现的漏洞，则不对请求进行响应。

[0145] 以上所描述的装置实施例仅仅是示意性的，其中作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下，即可以理解并实施。

[0146] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件。这样的理解，上述技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在计算机可读存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行上述各个实施例或者实施例的某些部分的方法。

[0147] 最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可

以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

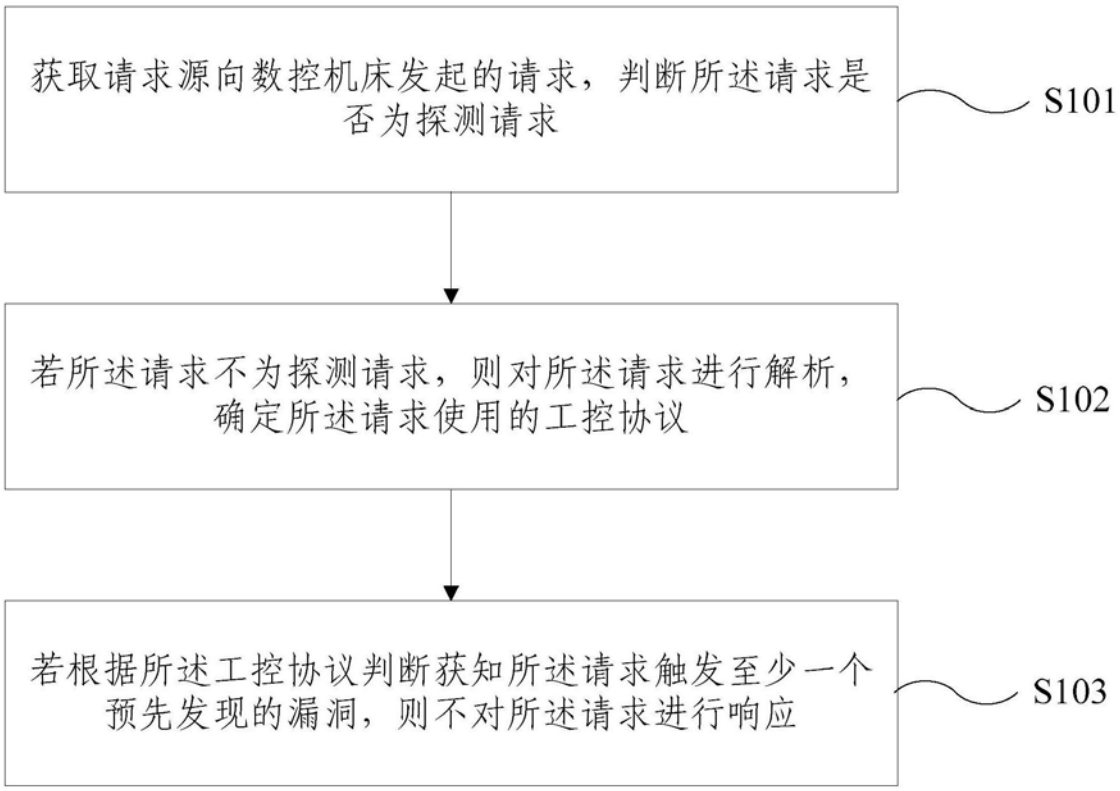

获取请求源向数控机床发起的请求，判断所述请求是否为探测请求
S101
若所述请求不为探测请求，则对所述请求进行解析，确定所述请求使用的工控协议
S102
若根据所述工控协议判断获知所述请求触发至少一个预先发现的漏洞，则不对所述请求进行响应
S103

图1

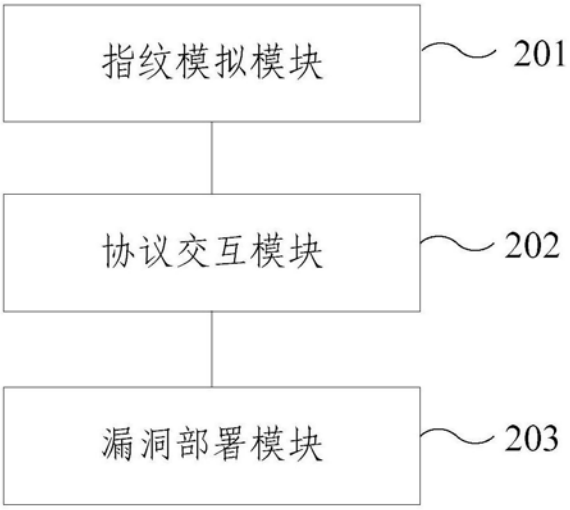

指纹模拟模块
201
协议交互模块
202
漏洞部署模块
203

图2

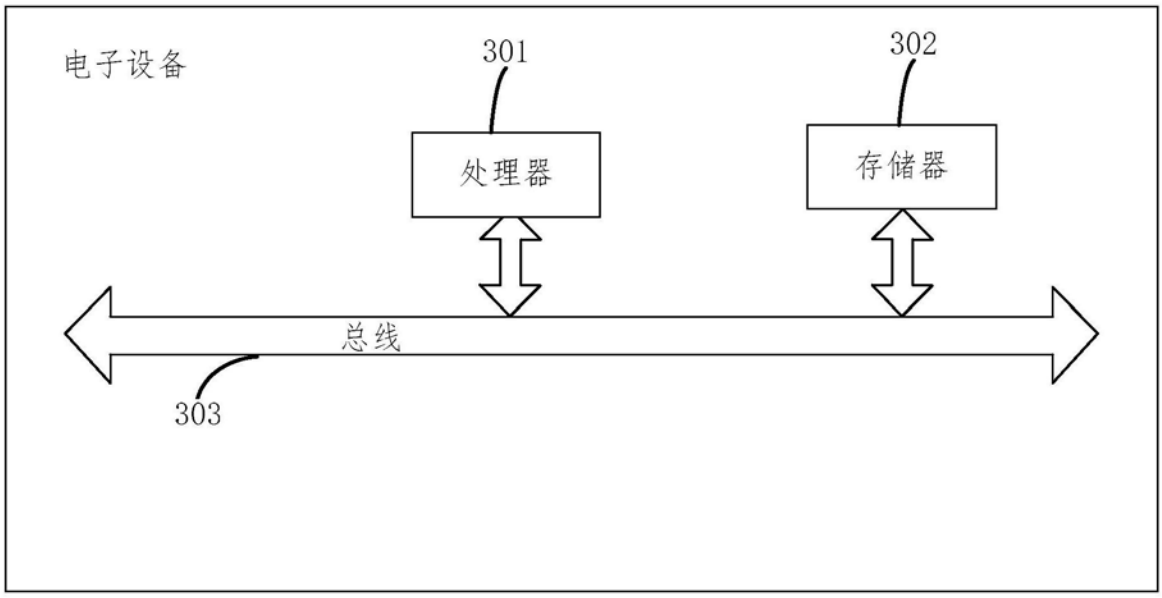


图3