新型网络空间防御体系的构建及效能评估

靳 骁 葛 慧 马 锐
(中国航天系统科学与工程研究院 北京 100048)

摘 要 当前的网络空间中,防御方往往在攻防博弈中处于被动地位,这种现状可以通过构建动态赋能的网络空间防御体系来改变。通过研究基于动态赋能的网络空间防御体系,从网络、软件、平台、数据 4 个方面梳理提升传统网络空间安全性的关键动态技术,以及构建动态赋能的网络空间的方法;通过结合攻防两方面对动态赋能网络进行安全效能评估,证明了动态赋能网络空间防御体系在提高系统安全防御能力方面的贡献。

关键词 网络空间,动态赋能,网络安全,效能评估
中图法分类号 TP393 **文献标识码** A

Construction and Effectiveness Evaluation of New Cyber Defense System

JIN Xiao GE Hui MA Rui
(China Aerospace Academy of Systems Science and Engineering, Beijing 100048, China)

Abstract In the current network space, the defender is in the passive position in the attack-and-defense game. This situation can be changed by constructing a dynamically-enabled cyber defense system. Through the research of the dynamically-enabled cyber defense system, critical danamic technology is given in four aspects (network, software, platform, data) for enhancing the security of the traditional cyber space, and a danamically-enapled cyber space method is constructed. By combining with the offensive and defensive in the face of dynamically-enabled cyber security effectiveness evaluation, the contribution of the dynamically-enabled cyberspace defense system in the safety of cyber space was proved.

Keywords Cyber space, Dynamically-enabled, Network security, Effectiveness evaluation

众所周知,当前的网络空间在构建时是静态的:安装固定的物理链路,配置固定的网络拓扑,部署固定的安全防御产品。这样部署后,网络空间将不再改变,防御方在面对攻击方的持续侦查和层出不穷的新型攻击方式时显得较为乏力。网络攻防的本质是双方不断采取不同手段的博弈,而防御方要改变当前"被动挨打"的现状,可以构建动态赋能[1]的网络空间防御体系,以实现防御体系甚至网络空间本身的不断变化,从而增强其防御能力。

1 动态赋能的网络空间

1.1 动态赋能的定义

"赋能"即赋予某种能力。动态赋能的网络空间防御是使网络空间具有动态变化的能力,通过动态变化隐藏、改变自身状态,直接或间接地增加网络空间的防御能力。

传统的静态网络安全防御体系是通过不同安全防御产品的部署、累积实现筑高墙式的安全防御,被动地应对攻击者不断变化的攻击手段。而动态赋能的网络空间通过部署和运行不确定、随机动态的网络和系统,改变被动防御的现状,使网络空间具备变化的能力,掌握防御主动权。它能有机地结合不同的动态防御技术系统并主动进行防御,使动态技术内生地存在于网络空间中。

1.2 动态攻击面

在网络系统的攻防中,攻击者可以利用系统程序(如 API)、通道(如套接字)和系统环境中出现的数据项(如输入输出字符串)攻击系统。我们将上述系统程序、通道、数据项统称为系统资源。攻击者利用这些系统资源对网络系统进行攻击。可以利用的系统资源的子集就被称为攻击面。通常情况下,网络系统一经部署将不再改变,其攻击面也相应固定,被称为静态攻击面。

在动态赋能的网络防御体系中,防御者通过不同的方式改变网络系统状态,进而带动攻击面发生变化,也就产生了动态攻击面。动态攻击面的出现使得整个网络系统的攻击面增大,但对于攻击者来说,其能利用的攻击面却未必比原有静态攻击面更大,而且是不断变化的,该变化使攻击者难以对攻击面进行利用,从而提高了攻击者的攻击难度并降低了受到的损失。因此,从攻击面的角度来说,具有动态攻击面的网络空间显然要比具有静态攻击面的网络空间的防御能力更强,对动态攻击面的度量研究也有助于我们更准确地评估动态赋能防御的效果。

1.3 动态防御技术的现状

随着人们对网络安全需求的提升,科研人员也逐渐意识到,对动态防御技术进行研究有助于改变防御方被动挨打的

本文受国家重点研发计划(2016YFB0800700)资助。

靳 骁(1992-),男,硕士生,主要研究方向为信息安全,E-mail:deprajin@163.com;葛 慧(1979-),女,硕士,主要研究方向为信息安全;马 锐(1978-),女,硕士,主要研究方向为信息安全。

现状。为此,科研人员在各自的领域进行研究,提出或实现了多种动态防御技术。

网络空间拟态防御[2](Cyber Mimic Defense,CMD)是国内研究团队首创的主动防御理论,为应对网络空间中不同领域相关应用层次上的未知漏洞、后门、病毒或木马等未知威胁提供了具有普适创新意义的防御理论和方法。受生物界基于拟态现象的伪装防御启迪,CMD 理论在可靠性领域非相似余度架构的基础上导入多维动态重构机制,造成视在功能不变条件下,目标对象内部的非相似余度构造元素始终在做数量或类型、时间或空间维度上的策略性变化或变换,用不确定防御原理来对抗网络空间的确定或不确定威胁。

基于 DHCP 的网络地址空间随机化分配技术(NASR)能够限制 DHCP 服务器分配地址的时间间隔到足够短,同时对原有的连续 IP 进行修改,使其对外呈现随机化特征。NASR 本质上是 IP 跳变技术,是一种典型的动态防御技术。

软件多态化技术主要用于将单一软件转变为功能相同、结构不同的软件实体,从而使攻击者无法用同一种方式迅速攻破大量设备。该技术将对编译器进行优化,通过多阶段插桩、程序分段和函数重排等技术实现为相同代码段生成不同软件实体的功能,面对功能相同、结构不同的大量软件,攻击者就无法使用相同的攻击手段进行广泛攻击,从而实现了空间层面上的动态防御。

2 基于动态赋能的网络空间防御体系的构建

归纳当前的动态防御技术不难发现,多数动态技术在本质上都是针对实体或实体的某部分,在时间、空间或时间+空间上使其得以发生规律性或可控的随机性或触发性的变化。而在实际操作中,可按信息系统中实体种类的不同,将动态赋能防御技术分为网络、软件、数据、平台 4 个层面,用具体的技术分别对这些层面进行动态化、统一调控,构建一个完整的基于动态赋能的网络空间防御体系。

2.1 网络动态防御技术

网络层面的动态防御技术是指在网络层面,针对网络的配置、设备、拓扑、资源等要素实施动态防御,通过随机化、动态化和虚拟化方法,提升攻击者对网络的探测难度和对内部节点的渗透难度,从而抵御针对网络的攻击。研究网络动态防御技术的目的,就是使原本静态的网络转变为不断进行随机改变的动态网络,从而阻止和迷惑攻击者。研究的重点在于网络架构、协议和服务的动态化,主要针对网络动态防御的本质、防御的目标和效果,包括网络拓扑动态变化、配置信息动态变化、虚拟网络覆盖技术等。

网络拓扑的动态变化是指动态改变网络的拓扑结构,在构建物理网络或对物理网络进行改进时应当充分考虑不同网络的形态特点,必要时配备冗余设备。网络拓扑的动态变化由于牵扯到物理链路的变动,不应轻易改变,因此可适当降低其变化频率。

如图 1 所示,网络拓扑由星状结构变化为环状结构,其中虚线表示有实际相连的物理链路但并未启用,变为环状结构后,原有的中心服务器可以成为冗余设备,也可以连入环状网;在不同拓扑结构的变换过程中,相应的诸如 IP 地址、网关服务器地址、DNS 等配置信息也随之变化,以适应不同的拓扑结构。

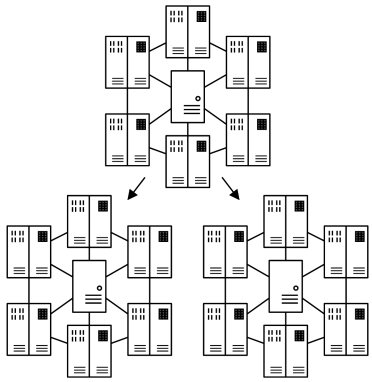


图 1 动态网络拓扑的变化

配置信息的动态变化包括动态网络地址转换技术、基于 DHCP 的网络地址空间随机化分配技术、基于同步的端信息跳变防护技术[3]等,随机化改变网络通信中的节点信息、地址信息甚至加密协议、通信协议,采用虚拟随机动态的网络地址、端口甚至协议,实现在时间+空间上的动态变化。

虚拟网络覆盖技术目前有针对 DDoS 攻击的覆盖网络防护技术,是一种构造网络的方法。覆盖网络建设在实际网络之上,是一种虚拟网络,是应用层软件借用不同物理链路达到相同网络状况从而进行通信的网络连接方法。

2.2 软件动态防御技术

软件动态防御技术是指应用随机化思想,动态更改应用程序自身及其执行环境的技术。运用密码技术、编译技术等处理软件程序,更改软件代码布局、执行时的内存分布等,实现随机化、软件多样化。从时间角度来看,主要包括指令集随机化技术、就地代码随机化技术,从空间角度则有软件多态化技术、地址空间布局随机化技术等。

指令集随机化技术(ISR)通过实现代码到指令过程中或指令本身的随机化来防御攻击,能够抵挡代码注入攻击。攻击者虽然能成功注入代码,但在翻译(或解释)的过程中,由于不识别目标指令集而无法正常运行。

地址空间布局随机化技术(ASLR)可以通过对堆、栈、共享库映射等线性区布局的随机化,以及增加攻击者预测目的地址的难度,防止攻击者直接定位攻击代码位置,可以应对缓冲区溢出攻击。

2.3 数据动态防御技术

数据动态防御技术的保护对象是内存中的数据以及应用程序中的协议语法和配置信息,动态更改数据格式、句法、编码或者表现形式,从而抵御攻击。数据的动态化应当不影响数据语义的表现,同时减少系统中的设计错误,防止代码注入攻击,规避漏洞。具有代表性的技术包括数据随机化[4]和 N 变体数据多样化。

数据随机化技术将写入内存的数据分类进行加密处理,任何进行读写操作的函数都只能对经过随机化或加密后随机化的数据进行操作,确保由一种类型溢出到另一种类型的数据是无效的,从而应对缓冲区溢出攻击。

N 变体数据多样化技术基于重新解释函数构造变体,对特定数据类型的数据进行多样化处理,实现数据层面对同样

语义数据的多变体设计,并设置监控器检测不同变体的执行情况,从而分析和发现攻击。

2.4　平台动态防御技术

平台动态防御技术的目的是动态改变应用运行的环境。平台是指应用运行时包括处理器、操作系统、开发环境等在内的软硬件环境。目前的应用运行平台大都版本统一,漏洞明显,易被攻破。而通过动态化,增强其随机变化,能够使攻击者难以对系统进行有效的侦察和探测,极大地增加了攻击难度。在动态构建多样化运行平台方面,主要有以下几种技术。

基于可重构计算的平台动态化技术借鉴了可重构计算中对可编程逻辑器件的复用,设计多个可执行文件和配置数据以供应用任务运行时进行随机变换,实现多样化软硬件任务的划分和差异化逻辑电路的设计,满足应用任务的运行需求,从而实现动态化。

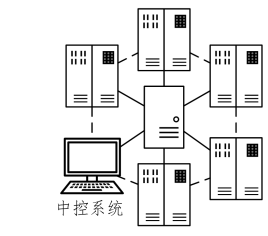
基于异构平台的应用热迁移技术利用操作系统级虚拟化和检查点编译技术创建多个虚拟运行环境,并在运行时保存应用状态用于迁移。该技术能够构造异构的多种系统平台,使应用在其中运行时随机迁移,增加了系统的随机性、多样性和不确定性。

Web 服务动态多样化是通过虚拟化技术,随机调用多个不同软件架构的虚拟服务器之一为客户端提供服务的,并且这些虚拟服务器以时间间隔或事件驱动在离线或在线状态间转换,从而提高防御能力。

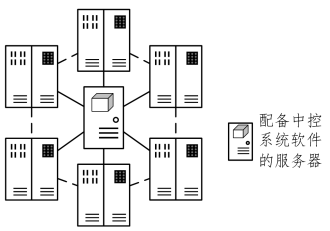
2.5　中控系统设计与动态赋能网络构建

根据上文不难发现,动态赋能的防御体系中应用的不同动态防御技术虽然实现了不同层面实体在时间或空间上的随机化,但细究到一定程度时又是相对静态的。因此,为了将上述不同层面、不同设计的动态防御技术与已有的传统静态防御体系结合起来,实现可控的随机变化,可以在网络系统中配备中控系统,从全局层面对不同的动态防御技术进行调整和调配,从而将各种动态防御技术与传统静态防御体系的优势充分结合。

中控系统的实现方式较为灵活,可设计为独立但接入网络空间的硬件设备,也可开发成相应软件部署到网络空间中,如图 2 所示。



(a)硬件实现中控系统配置



(b)软件实现中控系统配置

图 2　通过软硬件方式部署中控系统

通过统一调控网络、软件、数据、平台各层面的不同动态防御技术,可以实现诸如链路结构变化、配置信息更改、加密措施和通信端口的变化,并通过时间点(如固定时间间隔)或特殊事件(如入侵警报)触发上述改变,实现动态赋能。同时,配备中控系统后,不仅能够自动变化,还可以根据需要进行人工调整,更改其他配置。如图 3 所示,其中在中控系统针对不同层面的目标进行变化时,可以直接对网络空间进行改动,也可以在难以自动变化时提供操作说明供维护人员进行操作。

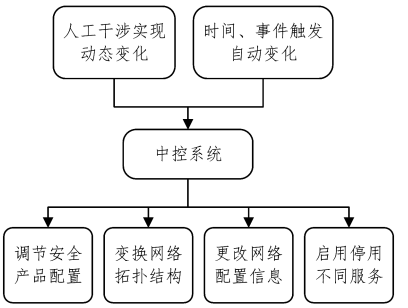


图 3　借助中控系统实现的动态变化

当前绝大多数的网络系统都是静态的,对其进行动态化改变的成本较高。为此,可以通过中控系统手工配置 3～5 套全局防御体系,为每种体系配备特有的防御技术和特定的配置信息,使其拥有不同的攻击面,并根据需要(时间或事件触发)进行调整,从而间接实现动态赋能。通常,攻击者需要一个较长的时间来对网络系统进行侦查和攻击尝试,只要调整的频率足够高,这样配置的网络体系对攻击者来说就是几乎不可探查、不可攻破的。具体部署方式如下。

首先,为已有的静态网络设计 3～5 种不同的网络架构,这些异构的网络架构应能实现相同的网络服务功能,并符合相应的安全、通信标准,每种网络架构都有诸如拓扑结构、IP 地址、DNS 等在内的一整套配置信息。维护人员定期或按事件对网络架构进行改变,更换配置文件或更改网络拓扑结构,从而实现“拟动态”。这种方法需要对网络设施进行一定程度的增加或修改,但其实现是具有极高可行性的。

其次,采取动态身份认证方式,通过动态密钥等形式实现用户身份认证和审查,以此改变当前依靠固定端口号、IP 地址和 Mac 地址来确定用户身份的现状,为实现 NASR 做铺垫。

最后,按照网络架构的不同,为防火墙、DNS 服务器、路由器等设置相应的配置文件,从而实现不同的防御目的和连通功能,以适应不同的网络架构。

3　基于动态赋能的网络空间安全效能评估

3.1　全面评估安全效能

在网络攻防博弈中,无论是攻击方还是防御方的行为和策略都是动态变化的,两者之间是一种此消彼长的零和游戏,仅仅根据防御方的防御能力和防御配置对其安全效能进行评估是非常片面的。因此,应当充分考虑攻击方可以利用的漏洞、攻击路径,以及防御方所防护对象的资产价值、配备的防御手段,从攻防两方面共同分析安全效能。

在攻击路径的分析方面,可以考虑通过建立攻击图、攻击树、Petri 网模型等方式对网络系统中的节点进行攻击路径分析,攻击者到达节点所需的路径越长,所要付出的代价也就越

高，间接表明节点的安全性越高。如图 4 所示，显然，攻击者要想攻破节点 7 所需要付出的代价要比攻破节点 1 大得多。

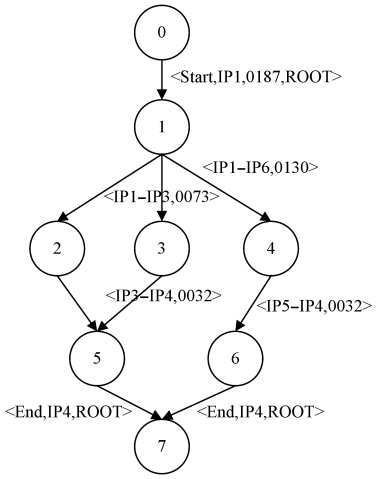


图 4 某网络攻击图模型

在漏洞利用方面，我们认为攻击者对漏洞的攻击能力与漏洞的严重程度成正相关，因此可以利用漏洞扫描工具对节点进行漏洞扫描，之后根据通用漏洞评分系统(Common Vulnerability Scoring System，CVSS)提供的漏洞重要程度对漏洞进行分析。

在资产价值评估方面，网络系统中的节点可能是存有绝密资料的服务器，也可能是不含任何信息的普通机器，节点的资产价值也就完全不同，将节点所存储、处理的信息的重要程度作为节点安全效能评估的一方面是非常必要的。

在防御能力方面，显然，充分配置安全产品的节点比未进行任何安全配置的节点的安全性要高，且防护能力更强。在考虑节点的防御能力时，应对其所配置的针对不同层面防御的安全产品进行评估，同时考虑动态赋能对网络系统的影响，充分考虑其防御能力。

3.2 动态变化因子

要在静态网络中进行效能评估以及上述攻防博弈，只需要汇总分析攻防两方面的各种现状即可。而要在动态赋能的网络系统中进行分析，需要考虑攻击者攻击手段的变化与动态赋能网络自身的变化。攻击者从开始侦查到发起攻击需要一定的时间，将在这个时间内动态赋能的网络状态发生变化的概率记为动态变化因子 α，该因子的主要作用是对下面两种情况发生的概率进行分析。

1)攻击者侦查到的网络状态在其发动攻击时并未改变，即网络在该时隙内处于相对静态；

2)攻击者侦查到的网络状态在其发动攻击时已经产生变化，即攻击者针对上一段时间的网络状态进行了攻击。

因此，定义 α 的大小与动态赋能的网络变化频率以及攻击者从侦查到发动攻击的时间间隔相关：α 的值越大，表示网络变化越频繁，或攻击者从侦查到发动攻击的时隙越长，攻击者越可能针对上一段时间的网络状态进行攻击；反之则亦。

3.3 安全效能评估

对于网络系统中的节点来说，自身具有的漏洞、所存储资产的价值都可能提高其受攻击且被攻破的概率，而节点所处网络攻击路径越长、自身的防御能力越强，则这种概率越低。因此将漏洞情况、资产价值归入攻击一方，将攻击路径、自身防御配置归入防御一方，据此对网络系统中节点的安全效能进行评估。

定义 l 表示攻击者利用某一攻击路径进行攻击的难易程度，其影响因素包括路径长度、中间节点的防御能力、漏洞情况等。路径越长、中间节点的防御能力越强、中间节点的漏洞越少或越难利用，则攻击者利用该路径进行攻击的难度就越大，l 也就越大。据此，对于 l，有：

$$l \rightarrow \varepsilon \frac{l_m d_m}{v_m} \tag{1}$$

其中，l_m，d_m，v_m 分别表示中间路径长度、防御能力强度、中间节点漏洞数量，ε 为系数。

定义 v 表示节点所具有的全部安全漏洞。对节点的安全漏洞进行汇总后，再汇总 CVSS 中对应漏洞的评分分值便得出 v 的值。显然，节点所含漏洞越多、程度越严重，v 也就越大。因此有：

$$v \rightarrow \mu \sum_{i=1}^{n} k_i \mu v_i \tag{2}$$

其中，k_i，v_i 为节点所含的不同漏洞的权重及其分值，μ 为系数。

定义 p 表示节点所存储数据的重要程度。以该节点所在的网络系统总数据的资产价值为整体，该节点所存储数据的价值占总资产价值的比重即为该节点的资产价值，将其量化后得到 p 的值。因此，节点所含的资产价值越高，则 p 越大，有：

$$p \rightarrow \delta \frac{p_c}{p_a} \tag{3}$$

其中，p_c 和 p_a 分别为网络系统总资产价值以及该节点所存储的资产价值，δ 为系数。

定义 d 表示节点防御能力的强弱，其影响因素包括节点所配置的全部静态防御产品以及其所在的动态赋能网络对节点安全性的影响。静态防御产品所覆盖节点的脆弱性越全面，则动态赋能网络越完善，节点的防御能力也就越强，d 也就越大，因此有：

$$d \rightarrow \sigma s m \tag{4}$$

其中，s 和 m 分别为静态防御产品的完善性以及动态赋能网络的防御能力，δ 为系数。

综合式(1)－式(4)，得出节点的安全效能 $f(x)$ 为：

$$f(x) \rightarrow (1-\alpha)\frac{\lambda_1 v_1 + \lambda_2 p_1}{\lambda_3 l_1 + \lambda_4 d_1} + \alpha \frac{\lambda_1' v_2 + \lambda_2' p_2}{\lambda_3' l_2 + \lambda_4' d_2)} \tag{5}$$

其中，λ_1 到 λ_4，λ_1'到λ_4'为系数，用于统一各参数的度量值；l_1，d_1，v_1，p_1 为当前网络状态下的各项指标；l_2，d_2，v_2，p_2 为下一时隙网络状态下的各项指标。

由此可见，减小漏洞风险、降低存储资产的价值、增加攻击路径长度、提高防御能力以及加快网络动态变化频率等方式，都能有效地提高网络空间的安全性，而基于动态赋能的网络空间正是通过动态变化实现上述一种或多种方式的改变。

结束语 动态赋能的网络空间与现有静态网络的不同之处主要在于其将动态变化融入网络空间的各个层面，改变了过去一经部署将不再改变的网络状态，通过不断改变自身，甚

至针对不同攻击做出相应变化来提升自身防御能力。但由于现有技术的局限等,目前对动态赋能的网络空间防御体系的构建还不完善,多数网络体系仅仅是逐步开始应用部分动态防御技术,构建出的网络多属于“伪动态”。

动态赋能防御体系目前尚处于研究中,经过完善的动态赋能防御应当实现无需人工操作的自行变化,且其应对攻击做出的反应也将更加准确、迅速,一个成熟的基于动态赋能的网络空间对攻击者来说应当是始终在变化、令其无从下手的。可以预见的是,随着动态赋能防御体系的完善,动态变化的网络也必将被广泛应用,未来的网络空间的安全性必将得到更大的提升。

参 考 文 献

[1] 杨林,于全.动态赋能网络空间防御[M].北京:人民邮电出版社,2016.

[2] 邬江兴.网络空间拟态安全防御[J].保密科学技术,2014(10):4-9.

[3] BADISHI G,HERZBERG A,KEIDAR I. Keeping Denial-of-Service Attackers in the Dark [J]. IEEE Transactions on Dependable & Secure Computing,2005,4(3):191-204.

[4] CADAR C,AKRITIDIS P,COSTA M,et al. Data Randomization[OL]. http://www. msr-waypoint. com/pubs/70626/tr-2008-120. pdf.

(上接第 368 页)

通过去中心化的方式维护了一个可靠的 RFID 大数据溯源数据库,是一个自带信任、防篡改以及能进行多签名复杂权限管理的分布式记录系统,可以采用 HADOOP 集群或云端实现。利用区块链可以集成不同数据库中的信息,创建互操作性,实现数据共享并能安全可靠地存储数据。区块链技术非常适合携带 RFID 标签的物品交易(流通)形成的大数据溯源。区块链的价值就体现在对数据构造出了某种程度的“唯一性”。将带有唯一标识的数据附于区块链上进行交易,很自然地解决了数据难以溯源的问题。通过区块链,用户可以明确区分数据流通产业链上的各个角色(拥有方、使用方、中介方等)。正在交易的数据究竟来自何方,究竟经过多少环节,究竟可能流向何处,都将不可辩驳地得以验证。再通过区块链的加密举证技术,用户可以实现对数据是否经过查阅、篡改、复制留存等内容的权威验证。倘若流通的每一环节都在区块链上规范进行,则对数据的复原、追溯,乃至整体统一规范,都将成为现实。建立 RFID 大数据的溯源区块链,可保障数据源提供者的权益,使数据在流动过程中可管、可控,加快数据交换和流通,是对数据交易模式的一种重要创新。物联网大数据溯源区块链的建立对数据交换过程中业务层面和控制层面的联系起到了关键作用,完善并细化其在整个数据交易流程中的作用,在数据提供者、中间商、用户等参与者间真正实现确权、许可、兑汇、核算的目标。

结束语　数据溯源描述了数据产生并随时间推移而演变的整个过程,它的应用领域很广,包括数据质量评价、数据核查、数据恢复和数据引用等。在物联网大数据环境下,数据溯源安全是目前迫切需要解决的问题。区块链在改善大数据溯源安全性方面可以发挥重要作用,其像链条一样构建记录数据的溯源记录,在不打乱整个连接的条件下是无法将之打破或重新排序的,从而可以保证 RFID 大数据溯源过程的安全性。

本文提出了一种基于区块链技术的 RFID 大数据溯源安全模型,并在 RFID 大数据的追踪溯源过程中应用区块链技术,形成多方参与且信息透明、共享、保真的溯源链,对携带 RFID 标签的溯源物品的生产、加工、销售等多个环节建立区块链账本,建立起 RFID 大数据的溯源全程链式路径,路径直达终端使用者,从而实现 RFID 大数据的溯源安全管理。

参 考 文 献

[1] 刘耀宗. RFID 数据流管理与挖掘若干关键技术研究[D]. 南京:南京理工大学,2016.

[2] 明华,张勇,符小辉. 数据溯源技术综述[J]. 小型微型计算机系统,2012,33(9):1917-1923.

[3] 魏亚东,李康. 一种基于物联网技术的大数据应用系统:CN205091639U[P]. 2016.

[4] 魏银珍,邓仲华. 云环境下科学工作流的溯源数据收集和查询框架研究[J]. 情报理论与实践,2015,38(7):115-118.

[5] NAKAMOTO S. Bitcoin:a peer-to-peer electronic cash system [OL]. https://bitcoin. org/bitcoin. pdf,2009.

[6] SWAN M. Blockchain:Blueprint for a New Economy [M]. USA : O0Reilly Media Inc. ,2015.

[7] 何蒲,于戈,张岩峰,等. 区块链技术与应用前瞻综述[J]. 计算机科学,2017,44(4):1-7.

[8] 朱岩,甘国华,邓迪,等. 区块链关键技术中的安全性研究[J]. 信息安全研究,2016,2(12):1090-1097.

[9] 谢雨来. 溯源的高效存储管理及在安全方面的应用研究[D]. 武汉:华中科技大学,2013.

[10] XIE Y,FENG D,TAN Z,et al. Design and evaluation of a provenance-based rebuild framework [J]. IEEE Transactions on Magnetics,2013,49(6):2805-2811.

[11] WIDOM J. Trio:A System for Integrated Management of Data, Accuracy, and Lineage[C]// Proceedings of the International Conference on Innovation Data Systems Research(CIDR). Asilomar,CA,January,2005:262-276.

[12] IKEDA R,WIDOM J. Panda:a system for provenance and data [C]// Proceedings for the 2nd Conference on Theory and Practice of Provenance. San Jose,CA,2010:1-4.

[13] LIANG X,SHETTY S,TOSH D,et al. Provchain:A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability[C]// Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. IEEE Press,2017:468-477.

[14] MCCONAGHY T,MARQUES R,MÜLLER,et al. Bigchain-DB:A Scalable Blockchain Database (DRAFT)[OL]. http://s3amazonaw5.com/arena-attachemnts/830378/db1ff2fb010d68e67dd5bfe1d20f5e33. pdf?1484096147.

[15] 梅海涛,刘洁. 区块链的产业现状、存在问题和政策建议[J]. 电信科学,2016(11):134-138.