

动态信任管理模型在农业科学数据安全领域的应用探索

吴定峰^{1,2}, 刘婷婷^{1,2*}, 王 剑¹, 胡 林^{1,2}

(1. 中国农业科学院 农业信息研究所, 北京 100081; 2. 国家农业科学数据中心, 北京 100081)

摘 要: [目的 / 意义] 为适应数据密集型农业科研范式的需要, 农业科学数据的安全防护亟需向着动态化、自适应的方向发展。信任管理是保障数据安全的核心手段之一, 其管理模型的动态化研究和应用探索具有十分重要的意义。[方法 / 过程] 本文梳理了动态信任管理模型的发展历程和理论框架, 分析了农业科学数据全生命周期的业务特点, 总结了农业科学数据信任管理的现实需求, 阐述了在农业科学数据安全领域实践动态信任管理模型的合理性和可行性。在此基础上, 结合农业科研本身的业务特征, 从用户信任、设备信任和应用信任 3 个层面探索了动态信任管理模型在农业科学数据安防领域的应用方法和要点。[结果 / 结论] 研究展望了动态信任管理模型的应用前景和未来的发展方向, 讨论了动态信任管理模型向动态流量管理和动态授权管理扩展以及和 SDP 相结合的可能性和必要性。

关键词: 动态信任管理; 数据安全; 农业; 科学数据

中图分类号: G250

文献标识码: A

文章编号: 1002-1248 (2020) 10-0016-09

引用本文: 吴定峰, 刘婷婷, 王剑, 胡林. 动态信任管理模型在农业科学数据安全领域的应用探索[J]. 农业图书情报学报, 2020, 32(10): 16-24.

Applications of Dynamic Trust Management Model in Agricultural Scientific Data Security

WU Dingfeng^{1,2}, LIU Tingting^{1,2*}, WANG Jian¹, HU Lin^{1,2}

(1. Agricultural Information Institute of CAAS, Beijing 100081; 2. National Agriculture Science Data Center, Beijing 100081)

Abstract: [Purpose/Significance] In order to meet the needs of intensive agricultural data research, the security protection of agricultural data needs to be developed in a dynamic and adaptive direction. Trust management is one of

收稿日期: 2020-06-02

基金项目: 科技部平台运行项目“农业科学数据在线服务系统建设”(2020PT002); 中国农业科学院创新工程项目(CAAS-ASTIP-2016-AII)

作者简介: 吴定峰 (ORCID: 0000-0001-7087-8538), 男, 博士, 副研究员, 研究方向为科学大数据管理系统等。王剑 (ORCID: 0000-0003-1765-824X), 男, 博士, 副研究员, 研究方向为科技资源共享理论等。胡林 (ORCID: 0000-0003-0699-0589), 男, 博士, 研究员, 研究方向为数据分析与可视化等

*通信作者: 刘婷婷 (ORCID: 0000-0003-2919-3101), 女, 硕士, 助理研究员, 研究方向为科学数据管理、科学数据共享等。E-mail: liutingting@caas.cn

the core means to ensure data security, the dynamic research and application exploration of its management model is of great significance. [Method/Process] This paper reviews the development process and theoretical framework of dynamic trust management model, analyzes the characteristics of the whole life cycle of agricultural data, summarizes the practical needs of trust management of agricultural data, and expounds the rationality and feasibility of practicing the dynamic trust management model in the field of agricultural data security. On the basis of the above research, combined with the business characteristics of agricultural research itself, this paper explores the application methods and key points of dynamic trust management model in the field of agricultural data security from the aspects of user trust, equipment trust and application trust. [Results/Conclusions] At the end of this paper, the application prospect and future development direction of dynamic trust management model are prospected. The possibility and necessity of expansion and development of a dynamic trust management model to dynamic traffic management and dynamic authorization management, as well as combining with SDP, are discussed.

Keywords: dynamic trust management; data security; agricultural; scientific data

1 引言

随着农业科学研究逐渐以数据密集型科研发现为主要研究范式, 农业科学数据的采集、处理和分析利用向着自动化、实时化的方向快速发展, 相关的业务系统开始呈现出集群化、高适应性、高弹性的显著特征, 系统边界变得模糊且难以准确定义, 安全实体随数据业务不断变化, 给农业科学数据的安全保障带来了极大的挑战。作为农业科学数据安全的核心内容之一, 农业科学数据的信任管理也亟需推陈出新, 满足实时动态变化的要求。近几年, 与零信任安全理念相结合后, 动态信任管理模型拥有了自适应、自成长的内生闭环特性, 获得了业界和学界的广泛关注, 其特性与农业科学数据信任管理的需求高度契合。因此探索动态信任模型在农业科学数据安全领域的应用对于提升农业科学数据应用质量, 保障农业科学数据安全都具有十分重要的意义。

2 动态信任管理模型介绍

2.1 信任管理模型的发展历程

在系统、网络和数据安全领域, 信任管理是非常

重要的安全保障手段。1996 年, BLAZE 首先提出了信任管理的概念, 将信任作为授权的首要因素从笼统的授权决策体系中脱离出来, 为信任管理作为一个单独的研究方向扫清了理论障碍^[1], BLAZE 将信任管理定义为一种描述和解释安全策略 (Security Policy)、安全凭证 (Security Credential) 并用来决策关键安全操作授权的信任关系 (Trust Relationship)^[2]。简单地说, 信任管理就是对信任取向的获取、评估和依据评估结果进行的反馈实施过程的集合^[3]。信任管理模型是信任管理的实施模型, 其一般规定了信任描述、信任度量、信任评估和信任反馈实施这一闭环过程中的标准和方法^[4]。

早期的信任管理模型完全基于信任凭证建立, 信任凭证是对实体信任度进行背书的有效凭证集合, 一般由 CA 等第三方信任机构发放, 其具有客观、精确、可定量描述和支持推理的特性。基于信任凭证, 早期的信任管理模型通过信任传递函数得出实体信任值, 根据实体信任值做出对实体安全行为的授权决策, 这类信任管理模型一般被称为客观信任管理模型, 可以准确地描述系统信任体系的初始状态, 对于实体接入管控有较好的效果, 客观信任管理模型的相关研究主要集中在 2000 年以前, 对当时功能单一, 结构相对独立的信息系统安全业务授权具有一定的支撑作用。然而, 信任不仅是客观描述^[5], 在很多实际场景中, 信任

更体现为一种主观和非理性的信念^[6]，因此，学者们从信任的主观性着手，在信任凭证的基础上加入实体间的主观信任度量结果用以实体信任值评估^[7,8]，实体间的主管信任度量往往以实体业务交互评估为基础，从而在客观上构成了随着业务演进的信任管理过程^[9]，这一类研究主要集中在 2005 年之前，随着复杂分布式系统的出现，这一类静态的信任管理模型已无法适应在弹性和适应性上都有较高要求的分布式系统权限管理需要。

动态性是信任的重要特性之一，信任的动态性由信任体系内实体的自然属性推导而来，如图 1 所示，知识、目标、能力等内因和行为、规则等外因共同决定了信任的动态性^[10]，信任的动态性决定了信任管理不应当是静态的。因此，时间因子和业务因子被纳入信任管理模型之中^[11,12]，以保证信任管理模型可以适应实体间随着业务发展和时间流逝而不断发生变化的相互信任关系。随着分布式系统和云计算的飞速发展，对于业务安全授权机制提出了高弹性和高适应性的要求，动态信任管理模型因其能快速反应全局信任变化的优势迅速成为研究热点，在信任度量标准、信任传递函数、信任评估方法、信任授权机制等方面不断创新发展^[13-16]。

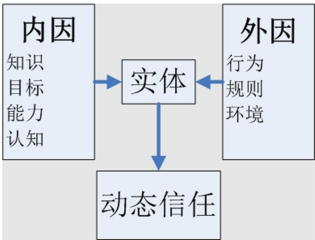


图 1 信任的动态特性

如图 2 所示，动态信任管理模型相比于静态信任管理模型具有扩展性好、能够动态适应系统软硬件组件变化的显著优点，近年来，甚至在信任管理实践中发展出自反馈闭环，具有了自成长特性（详见本文 1.2 节）。这种高度动态化的特性正是来源于其对于信任预期和信任证据的动态收集和管控，以及基于以上动态数据的信任评估和决策机制。

2010 年，JOHN K 提出了“从来不信任，始终在

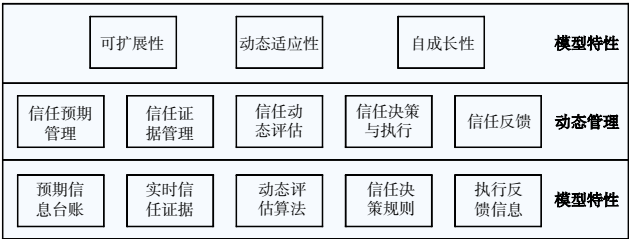


图 2 动态信任管理模型架构

认证”的零信任安全思想^[17]，零信任安全思想的提出极大地丰富了动态信任管理模型的内涵。在零信任安全思想提出前，信任管理模型往往局限于网络层和链路层的安全授权决策，缺少在应用层甚至应用程序内的场景实践。零信任思想将设备、应用程序、用户打包为网络代理概念进行统一的信任和授权管理^[18]，这一理论创新使得动态信任管理模型的涵盖范围由网络层、链路层向应用层扩展，在零信任安全框架下，动态信任管理的内容不但包括设备信任、流量信任，还进一步囊括了应用信任和用户信任，将综合的信任评估结果纳入网络代理的授权控制基础中^[19]。

2.2 动态信任管理模型闭环框架

在零信任安全思想下，动态信任管理模型发展为一个高弹性、多维度、自成长、自适应的闭环框架。如图 3 所示，动态信任管理模型根据信任数据对网络代理的信任值进行综合评估，基于评估结果做出信任决策，信任决策结果影响对于网络代理的安全业务授权结果，从而影响实际开展的安全业务。同时，安全业务运行过程中产生的信任数据被反馈给信任管理模块，从而形成可以独立成长的信任安全闭环。

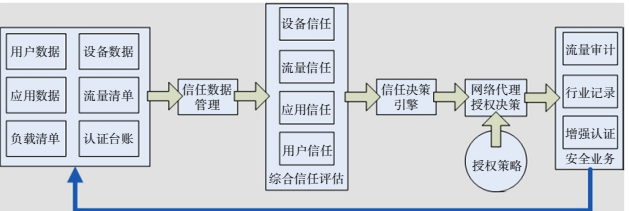


图 3 零信任思想下的动态信任管理闭环

信任数据管理是动态信任管理模型能够持续正常运行的基础。信任数据管理将用户数据、设备数据、

应用数据、流量清单、认证数据等用于信任评估的信任数据进行抽取、分类存储和管理。信任数据分为各实体的静态信任数据和系统的动态信任数据两类,静态信任数据包括各实体列表、实体静态属性、关联实体的初始信任传递数据等描述系统初始信任状态的数据,动态信任数据包括流量清单、认证数据、负载变化、实体行为数据、实体间信任传递变化数据等安全业务运行过程中产生的数据。信任数据管理模块通过建立和维护静态信任数据,抽取动态信任数据,将动态数据静态化等方式维护一个兼顾可用性和系统效率的信任数据库。

在信任数据支撑下,动态信任管理模型从设备、用户、应用和流量等多个方面分别进行信任评估,动态信任管理模型下的信任评估除了在信任评估函数中加入时间因子还在评估指标体系中加入了动态的业务影响指标^[20,21],以便使得评估结果可以反应系统一段运行周期之后的信任变化情况。

信任决策引擎对信任评估结果进行分析,预测网络代理在当前的信任度。通过引入上下文并对信任阈值进行动态配置^[22,23],信任决策将信任评估结果归一化为一系列离散的信任等级供授权决策引擎引用。

授权决策引擎则根据信任分析结果和授权策略库中的规则对网络流量和业务请求进行授权处理,针对

不同信任度的网络代理实施从行为监控、强制认证、信任续租到拒绝授权等一系列的安全操作,以保证系统内流量的安全性。这一系列安全业务的实时数据作为动态信任数据的来源经信任数据管理模块处理后存入信任数据库中,以保证后续的信任决策具备实时动态特性。

3 农业科学数据面临的安全信任管理危机

农业科学数据是指在农业知识指导下和农业科研生产背景下,用以描述农业科学研究活动的原始数据及其衍生数据^[24],其一般是对农业科学研究对象和过程抽象化后形成的事实记录^[25],是证实农业科学发现和科学观点的科学证据,是基于农业科研成果进行论证和推理的基础^[26]。农业科学数据的生命周期包含多个阶段,如图 4 所示,农业科学数据的生命周期包括计划、获取、存储、处理、共享与出版、分析与重用、归档与保存等多个阶段^[27,28]。在计划阶段对农业科学数据的获取时间和方式、加工内容和方法、存储格式和主体、共享途径和范围等内容进行规划,计划阶段所产生的数据属于农业科学数据的数据附件,是农业科学数据的重要组成部分^[29];获取阶段所产生

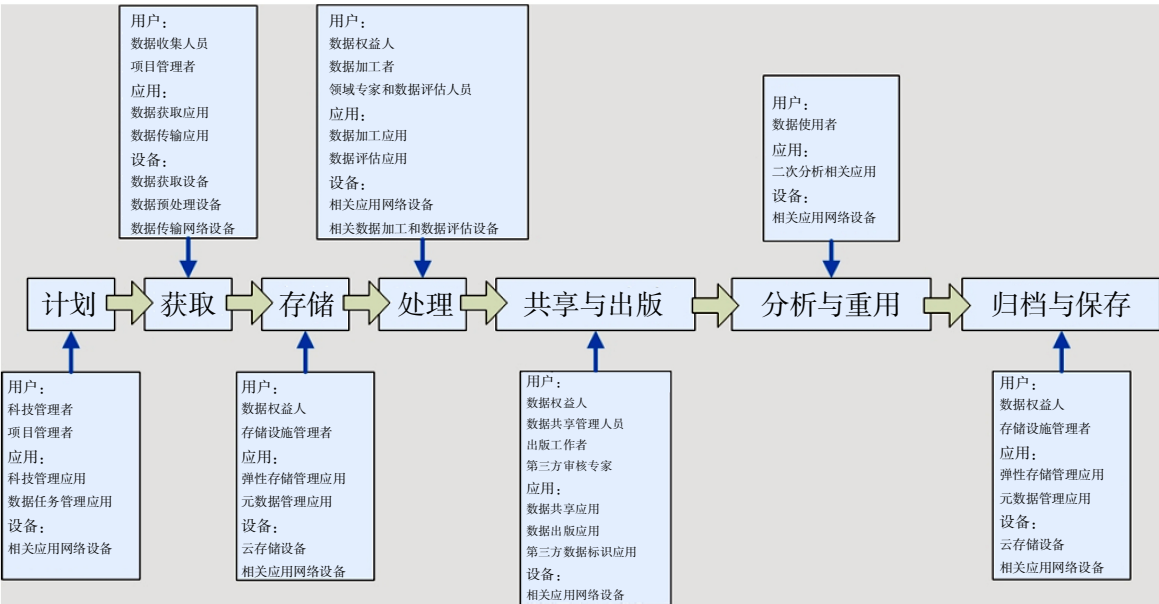


图 4 农业科学数据生命周期与各阶段的安全实体

的是未经加工的原始农业科学数据，数据虽然带有一定的组织结构，其中经常带有不宜公开的敏感信息或个人信息，需要进一步处理后才能作为农业科学数据产品加以分享和利用，原始农业科学数据在采集后需要及时持久化存储；原始的农业科学数据在处理阶段经过去标识化处理、脱敏处理、分级分类评估和进一步组织加工形成农业科学数据产品；加工形成的农业科学数据产品在共享与出版阶段以 Web 发布的方式或者以科学数据产品出版的方式向科研界发布并提供分享和利用的接口^[30]；发布后，其他科技工作者可以对农业科学数据产品进行二次整合分析，达成进一步的科学发现^[31]；农业科学数据发布后也需要进行持久化存储，完成对于数据的归档和长期储存。

在农业科学数据的全生命周期中涉及到各种不同的安全实体，不仅类型多样而且数量众多。从用户层面来看，涉及到 10 多类用户，而且数据搜集人员、第三方专家、数据使用者等用户实体不仅数量巨大而且缺乏稳定性和可控性^[32]，给用户的信任管理带来了很大的挑战；从应用层面来看，整个农业科学数据生命周期依赖大量第三方应用所提供的服务，且根据数据类型不同往往需要临时接入不同的第三方应用^[33]，这些应用的信任管理在很大程度上影响着农业科学数据的安全；从设备层面看，数据采集设备、第三方应用依赖的网络设备、低可控用户的接入设备都极有可能影响农业科学数据的安全，对这些设备进行有效的信任管理也是一大挑战。同时，农业科学数据进入大数据时代后，其业务处理往往依赖大量高弹性和高适应性的自动化系统完成，对信任管理的适应性、动态性和灵活性提出了更高的要求。

4 农业科学数据系统中实践动态信任管理模型

由于动态信任管理模型具有高弹性、多维度、自成长、自适应的特点，笔者认为将其应用于农业科学数据系统安防可以有效地应对农业科学数据所面临的信任管理挑战。下面将从用户信任、设备信任和应用

信任 3 个方面分别阐述在农业科学数据系统中应用动态信任管理模型的技术方案。

4.1 农业科学数据用户信任管理

动态信任管理模型的用户信任管理机制可以有效地识别恶意的用户行为和用户凭证遭到窃取的情况，通过对这些情况的用户信任进行评估并做出相应的针对性预防措施可以有效预防用户凭证泄露对农业科学数据带来的安全威胁。如图 5 所示，动态的用户信任管理包含用户信任初始化、用户目录动态维护、动态用户信任评估和动态身份认证 4 个相互联系的方面。

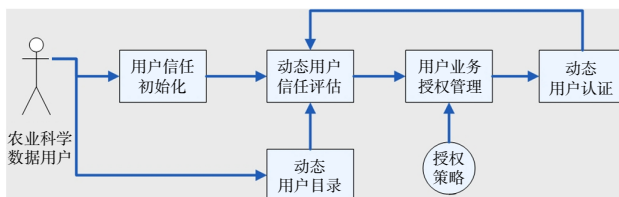


图 5 动态用户信任管理机制

在农业科学数据系统中，对数据安全造成威胁的往往是具有特殊权限的用户凭证泄露^[34]，这一类用户包括农业科学数据加工用户、评级用户、审核用户、数据权益用户以及农业科学数据生命周期各阶段的管理用户，这些用户初始化信任建立往往采取盲引或人工授信的方式进行^[35]，在初始信任建立时应加强用户预期信息的收集和确认，初始收集的用户预期信息是动态用户信任评估过程中重要的评估参照数据^[36]。动态用户信任管理模型注重用户目录的动态性，以保证模型具备高弹性特征，用户目录中除了普通用户的基本认证信息还支持存储 X.509 等数字用户凭证用以支持自动化系统的动态数字用户体系^[37]。在农业科学数据系统中，除了收集常规的用户预期信息外，还应考虑到农业的学科特点和知识组织结构收集相关信息以预测用户的合理数据访问范围。例如，植保专家拥有的数据审核账户其预期数据访问范围应集中于植保及相关学科。动态用户信任管理模型监控用户的安全行为，随着时间变化和用户安全行为的变化而对用户信任值进行动态评估。在农业科学数据业务背景下，应重点监控农业科学数据操作的相关安全行为，尤其

是跨任务、跨领域的农业科学数据访问和操作请求, 以及和科学数据访问权限相关的提权行为。这些行为往往和农业科学数据的泄露和不当使用关系密切。如农业科学数据共享环节常发生数据不当使用^[38], 为防止自己的数据被不当使用, 一些数据权益方会使用区块链等技术标记数据的获取者和其后续的使用行为^[39-41], 这些标记提供了十分重要的用户信任证据, 用户信任管理应当监控这些标记结果并和用户预期行为相对照, 确保及时将用户的不当使用行为纳入用户信任评估中。当用户信任值过低将触发授权策略中的强制信任续租策略, 执行动态用户认证, 通过密码、TOTP、证书续租、生物验证等多种认证方式对用户身份进行再认证^[42], 从而有效防范非法用户, 保障农业科学数据安全。

4.2 农业科学数据设备信任管理

动态信任管理模型中的设备信任管理机制可以有效地识别接入系统的设备身份, 并持续监控设备的信任信号发现设备异常状态, 结合设备度量信息进行设备信任评估, 在必要的时候通过触发设备的信任续租来控制该设备可能对系统安全造成的危害。

农业科学数据系统中相关设备的接入具备较明显的动态特性, 除了传统的网络设备和服务设备外, 农业科学数据获取、加工、评审、重用过程中经常会涉及到专用设备的接入^[43], 如田间的专用数据采集设备, 生化、农机和基因实验室内具备自动数据收集传输功能的实验仪器设备, 数据加工和审核人员可能配备的专用设备, 数据仿真等第三方系统接入的交互设备等。这些设备的初始信任建立可以采用数字证书的方式自动配置, 关键节点设备可以采用 TOTP 的方式引入人工认证^[44], 对于农业科学数据采集设备和第三方专家的评审设备等专用设备可以采用 HSM 或 TPM 等硬件设施来存储加密的身份证书^[45], 从而赋予其很高的初始可信度, 初始信任建立时, 动态信任管理模型会建立设备清单, 存储设备初始状态信息和预期信息。在农业科学数据业务范围内, 应根据业务范围和数据特性对设备的预期安全操作建立台账。设备接入系统后的运行过程中, 动态信任管理模型通过本地度量和远

程度量相结合的方式评估设备状态, 获取设备信任信号, 通过设备信任评估来决定是否执行设备的信任续租操作, 通过重镜像或重认证的方式来消除或限制设备威胁, 从而保障农业科学数据安全。设备信任信息还可以用以增强对用户信任信息的评估强度, 动态信任管理模型支持使用设备认证来进一步验证用户认证的可信度, 当设备预期信息和用户预期信息不符时, 可以发起进一步认证, 以发现威胁或重建预期。

结合农业科学数据相关业务信息可以有效获取设备的信任证据, 使得信任评估更加精准高效。在农业科学数据安全背景下, 设备信任评估应和农业科学数据的具体业务语境相结合, 农业科学数据的接入设备通常带有具体的工作环境特征, 其频率、时段等特性具有特定的模式, 其接入状态与相关业务的发展状态相吻合。在农业科学数据加工处理环节的设备信任管理就是一个很典型的案例, 数据加工者和数据评估者的工作设备往往属于临时接入的外围设备, 这些设备极易受到攻击者劫持, 是农业科学数据安全的一大隐患, 这些设备的接入状态必定和相关的加工和评估作业相一致, 如果监控到一台标注在某领域数据专家身上的接入设备在没有相关领域数据评估作业时异常接入, 就需要对该设备重新进行信任评估, 迫使其实施信任续租操作。

4.3 农业科学数据应用信任管理

动态信任管理模型从应用构建分发和应用执行两个阶段管理应用信任。在应用构建和分发阶段, 动态信任管理模型要求应用的构建和分发系统具有一定效力的第三方数字签名, 以保证应用真实性, 通过散列验证应用完整性^[46]。农业科学数据生命周期中依赖的第三方应用数量众多, 来源复杂, 有必要对其构建和分发体系执行有效的信用管理, 防止来历不明或经过篡改的第三方应用危害农业科学数据安全。在应用执行阶段, 动态信任管理模型会建立应用台账, 通过模糊扫描、端口扫描和漏洞扫描等主动监控方式确保应用的安全性。通过 TPM 引用和行为分析等手段达成应用集群内的相互监视, 主动监控和集群监视^[47]所获得

的信任型号会结合应用台账信息用以评估应用信任度,通过沙箱等方式确保较低信任度的应用无法危害到农业科学数据安全。

5 结论和展望

动态信任管理模型强调灵活动态的信任管理能力,从用户信任、设备信任、应用信任 3 个层面选择合适的实践技术,来具体实施动态的信任信号获取、评估和反馈,达成信任管理的闭环。笔者认为,将动态信用管理模型应用于农业科学数据安全领域,在未来有以下两个值得注意的发展趋势。

一是从动态信任管理向动态的权限管理、流量管理和认证管理扩展,最终达成全系统语境下的动态安全管理。信任管理是系统安全防护的重要基础,但信用管理并不能直接作用于系统安全行为,而是需要权限管理、流量管理、认证管理等一系列系统安全构件共同作用,来实现系统安全管控行为^[48]。在信用管理动态化的趋势下,权限管理、流量管理和认证管理也必然需要向动态化和自适应的方向发展。动态信任管理给了授权决策一个动态的证据源,但是其决策策略仍旧是静态化的,权限策略的动态化尝试已经成为权限管理研究的热点之一;现行的流量管理手段仍以静态技术为主,流量加密算法、密钥管理和流量监控指标管理以预先设定为主,一旦防护失败很难给予快速的响应补救,因此动态流量管控技术也已成为研究热点之一;现行的系统认证方式和响应情景都依赖于预先的静态设置,作为信用续租的重要方式,认证管理的动态化也是必然的趋势。在农业科学数据安全领域,由于农业科学数据系统的固有复杂性和高开放性,对于全系统域的安全管理技术需求更加迫切,因此需要对流量管理和认证管理的动态化研究进展加以关注和应用。

二是动态信任管理模型和 SDP 的有机结合。动态信任管理模型强调基于动态获取的信任证据进行信任赋值和信任评估,在农业科学数据系统这样高度复杂和高度开放的系统环境下,信任证据的监控和获取范

围往往需要动态扩展,这就容易导致系统攻击面的增加,成为潜在的系统风险点。攻击者可能利用这些攻击面欺骗信任管理系统,非法提升自身信任值,这也是动态信任管理模型的硬伤之一,因此,在实现动态信任管理的同时尽力缩小攻击面十分必要。作为一种全新发展起来的网络动态防御技术,SDP 的特征之一对于攻击面的保护和动态隐藏能力^[49,50],将动态信任管理和 SDP 相结合有助于缩小小攻击面,极有可能动态信任管理模型在未来的发展方向之一。

参考文献:

- [1] BLAZE M, FEIGENBAUM J, LACY J. Decentralized trust management[C]. Proceedings of the 17th symposium on security and privacy, Oakland: IEEE computer society press, 1996: 164-173.
- [2] BLAZE M, FEIGENBAUM J, IOANNIDIS J, et al. The role of trust management in distributed systems security[C]. Secure internet programming: issues for mobile and distributed objects, Berlin: Springer-Verlag, 1999: 185-210.
- [3] POVEY D. Developing electronic trust policies using a risk management model[C]. Proc. of the 1999 CQRE congress, 1999: 1-16.
- [4] 吴晓凌. 面向服务的动态信任模型和信任管理[D]. 武汉: 武汉大学, 2012.
- [5] GAMBETTA D. Can we trust trust?//Trust: Making and breaking cooperative relations[C]. Oxford: Basil Blackwell, 1990: 213-238.
- [6] ABDUL-RAHMAN A, HAILES S. A distributed trust model[C]. Proceedings of the 1997 workshop on new security paradigms, New York, USA: ACM Press, 1998: 48-60.
- [7] ABDUL-RAHMAN A, HAILES S. Using recommendations for managing trust in distributed systems[C]. Proc. of the IEEE Malaysia int'l conf. on communication'97, 1997.
- [8] 李承,汪为农. 分布式信任模型直接信任的模糊计算方法[J]. 计算机应用与软件, 2004(8): 84-86.
- [9] ABDUL-RAHMAN A, HAILES S. Supporting trust in virtual communities [C]. Proceedings of the 33rd Hawaii international conference on system sciences, Maui, Hawaii, 2000: 6007-6016.
- [10] CHANG E, THOMSON P, DILLON T, et al. The fuzzy and dynamic nature of trust[C]. LNCS 3592, Berlin: Springer-Verlag, 2005: 161-

- 174.
- [11] 常俊胜, 王怀民, 尹刚. DyTrust: 一种 P2P 系统中基于时间帧的动态信任模型[J]. 计算机学报, 2006, 29(8): 1301-1306.
- [12] 方群, 吉逸, 吴国新, 等. 一种基于行程编码的 P2P 网络动态信任模型[J]. 软件学报, 2009, 20(6): 1602-1616.
- [13] 郭磊涛, 杨寿保, 王菁, 等. P2P 网络中基于矢量空间的分布式信任模型[J]. 计算机研究与发展, 2006, 43(9): 1564-1570.
- [14] 梁军涛, 蒋晓原. 一种基于推荐的 Web 服务信任模型[J]. 计算机工程, 2007, 33(15): 52-54.
- [15] 李小勇, 桂小林. 可信网络中基于多维决策属性的信任量化模型[J]. 计算机学报, 2009, 32(3): 405-415.
- [16] 代战锋, 温巧燕, 李小标. P2P 网络环境下的推荐信任模型方案[J]. 北京邮电大学学报, 2009, 32(3): 69-72.
- [17] CONRAN M. Zero trust: Single packet authorization passive authorization[EB/OL]. (2019-06-18) [2020-03-05]. <https://network-insight.net/2019/06/zero-trust-single-packet-authorization-passive-authorization/>.
- [18] ROSE S, BORCHERT O, MITCHELL S, et al. NIST. SP. 800-207-draft2 zero trust architecture[S]. Gaithersburg: National institute of standards and technology special publication, Maryland, United States, 2020.
- [19] EVAN G, DOUG B. Zero trust networks: building secure systems in untrusted networks[B]. Sebastopol, CA: O'Reilly media, 2017.
- [20] ARIN G R, DAMIANI E, DIVIMERCATI D C, et al. Assessing efficiency of trust management in Peer-to-Peer systems[J]. IEEE, 2005, 20(13/15): 368-373.
- [21] SONG S, HWANG K, ZHOU R, et al. Trusted P2P transactions with fuzzy reputation aggregation[J]. IEEE internet computing, 2005, 9(6): 24-34.
- [22] SUN Y, YU W, HAN Z, et al. Information theoretic framework of trust modeling and evaluation for ad hoc networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 305-319.
- [23] 代战锋, 温巧燕, 李小标. P2P 网络环境下的推荐信任模型方案[J]. 北京邮电大学学报, 2009, 32(3): 69-72.
- [24] HEY T, TANSLEY S, TOLLE K M. The fourth paradigm: Data-intensive scientific discovery[J]. External research, Microsoft research, Redmond, 2011, 99(8): 24-32.
- [25] 毕达天, 曹冉, 杜小民. 科学数据共享研究现状与展望[J]. 图书情报工作, 2019, 63(24): 69-76.
- [26] OECD. OECD principles and guidelines for access to research data from public funding [EB/OL]. [2018-09-01]. <http://www.oecd.org/science/scitech/38500813.pdf>.
- [27] USGS. USGS Data Management Training Modules: USGS Science Data Lifecycle[EB/OL]. [2016-08-11]. <https://oedbreeze.cr.usgs.gov/dm-sdl/>.
- [28] 黎建辉, 沈志宏, 孟小峰. 科学大数据管理: 概念、技术与系统[J]. 计算机研究与发展, 2017, 54(2): 235-247.
- [29] MARK D W, MICHEL D, IJSBRAND J A, et al. Addendum: the FAIR guiding principles for scientific data management and stewardship[J]. Scientific data, 2019, 6(1).
- [30] 李成赞, 张丽丽, 侯艳飞, 等. 科学大数据开放共享: 模式与机制[J]. 情报理论与实践, 2017, 40(11): 45-51.
- [31] 李云婷, 温亮明, 张丽丽, 等. 科学数据共享系统的现状与趋势[J]. 农业大数据学报, 2019, 1(4): 86-97.
- [32] 陈明奇, 黎建辉, 郑晓欢, 等. 科学大数据的发展态势及建议[J]. 中国教育信息化, 2016(21): 5-9.
- [33] 程学旗, 靳小龙, 王元卓, 等. 大数据系统和分析技术综述[J]. 软件学报, 2014, 25(9): 1889-1908.
- [34] 王秉, 吴超. 基于安全大数据的安全科学创新发展探讨[J]. 科技管理研究, 2017, 37(1): 37-43.
- [35] 张丽丽, 黎建辉. 科研数据的开放: 进展、模式与新探索[J]. 大数据, 2016, 2(6): 25-33.
- [36] 赵刚. 大数据[M]. 北京: 电子工业出版社, 2016.
- [37] RACHEL K. Whitepaper: Practical challenges for researchers in data sharing: Review[J]. Learned publishing, 2018, 31(4): 417-419.
- [38] 温亮明, 张丽丽, 黎建辉. 大数据时代科学数据共享伦理问题研究[J]. 情报资料工作, 2019, 40(2): 38-44.
- [39] 苏震, 赵文彦. 基于区块链的智慧农业应用分析与设计[J]. 农业图书情报学报, 2020, 32(3): 44-53.
- [40] 杨明, 丁龙, 许艳. 基于区块链的医疗数据云存储共享方案[J]. 南京信息工程大学学报(自然科学版), 2019, 11(5): 590-595.
- [41] 丁伟, 王国成, 许爱东, 等. 能源区块链的关键技术及信息安全问题研究[J]. 中国电机工程学报, 2018, 38(4): 1026-1034, 1279.
- [42] MASSIMILIANO A, ALESSANDRA D E B, DOUGLAS D J, et al.

- Security and trust in cloud application life-cycle management[J]. Future generation computer systems, 2020, 111: 934-936.
- [43] 赵江华, 穆舒婷, 王学志, 等. 科学数据众包处理研究[J]. 计算机研究与发展, 2017, 54(2): 284-294.
- [44] MARTIN L, JITKA K. Big and open linked data analytics ecosystem: Theoretical background and essential elements[J]. Government information quarterly, 2019, 36(1).
- [45] 吴林, 吴超, 吴娥. 大数据视域下安全信息资源管理模式研究[J]. 科技管理研究, 2020, 40(9): 156-162.
- [46] WANG B, WU C, HUANG L, et al. Using data-driven safety decision-making to realize smart safety management in the era of big data: A theoretical perspective on basic questions and their answers [J]. Journal of Cleaner Production, 2019, 201: 1595-1604.
- [47] ZHOU Q Y, SUN W Y, ZHANG H C. A new simple model trust-region method with generalized barzilai-borwein parameter for large-scale optimization[J]. Science China(mathematics), 2016, 59(11): 2265-2280.
- [48] 蔡冉, 张晓兵. 零信任身份安全解决方案[J]. 信息技术与标准化, 2019(9): 46-49.
- [49] MATT C. Software defined perimeter (SDP): Creating a new network perimeter[EB/OL]. Network world (online). [2020-05-20]. <https://www.networkworld.com/article/3402258/software-defined-perimeter-sdp-creating-a-new-network-perimeter.html>.
- [50] MOUBAYED A, REFAEY A, SHAMI A. Software-defined perimeter (SDP): State of the art secure solution for modern networks[J]. IEEE network, 2019, 33(5): 226-233.