DOI:10.3969/j.issn.1009-6868.2016.01.005
网络出版地址:http://www.cnki.net/kcms/detail/34.1228.TN.20151117.1512.010.html

面向数据的安全体系结构初步研究

Data Oriented Security Architecture

苗放/ MIAO Fang
(成都大学 大数据研究院,四川 成都 610106)
(The Research Institute of Big Data, Chengdu University, Chengdu 610106, China)

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2016) 01-0019-004

摘要: 提出了一种以数据为核心和面向数据的信息安全解决方案,即面向数据的安全体系结构(DOSA)。DOSA将通过网络用户身份认证、数据所有权确立、数据注册、加密呈现、授权使用、水印记录、过程溯源、数据监管、安全应用等方法,建立一套开放环境下的数据安全体系,从数据的采集、管理、应用等层面上,最大限度地保护数据安全。在数据交易、数据存储、数据传输、数据应用、数据隐私保护等方面,具有较大的应用前景。

关键词: 面向数据的安全体系结构;数据所有权;加密呈现;数据安全

Abstract: System vulnerabilities and excess authority to access data are the main reasons for data divulgence. In this paper, a new data security solution called Data Oriented Security Architecture (DOSA) is proposed. DOSA is an open data security system to use a series of methods, including network user identity certification, data property rights, data register, data encryption present, data authority to use, data watermark log, data procedure tracing, data monitoring, and data safety application. DOSA protects data in data collecting, data management and data applications. It can be used in data transaction, data storage, data transfer, data application, data privacy safeguarding, etc.

Key words: data oriented security architecture; data property rights; encryption present; data security

1 信息安全面临的挑战

信息安全关乎国家安全、社会稳定、企业利益和个人隐私。随着环境的开放,数据的急剧扩张,人们对数据的依赖程度越来越高。由于数据集中存放、系统安全漏洞、数据越权访问等情况,使信息安全问题愈发突出。随着数据时代的到来,要求我们以新的数据体系结构去适应新的社会发展要求。

(1)开放环境下需要有新一代的数据安全解决方案

中国政府提出的"互联网+"行动计划,要将移动互联网、云计算、大数据、物联网等作为新时期经济发展的重要推力,信息系统或应用体系所面临的环境更为开放,对数据和信息安全的要求更高。

通常情况下,一个相对安全的信息系统或应用体系,是建立在一个相对封闭和安全的环境中,通过"门窗加固"等方式来保证这个封闭环境是安全的或可信的,更加强调的是网络空间安全、系统安全、环境安全和应用安全。虽然和外部交换信息时是通过数据加密或虚拟专用网络(VPN)通道来传输数据,但在这个相对"安全"的内部环境里,大多数数据却是处于"裸露"状态的。一旦有不速之客通过各种漏洞或非法获得权限进入到这个环境,裸露的数据就面临着极大的危险。

一些数据中心所涉及的数据安全,多是指利用数据备份、数据灾备等技术来保障数据不丢失、不被破坏,但仍存在着越权访问等危险行为,造成数据和信息泄露的隐患。

封闭环境下的安全方法在开放环境下的面临着极大的挑战,开放环境下的数据安全成为重要的研究课题。文献[1]提出了开放网络环境下数据的发布与管理,涉及了单向加密、新人凭证等属性概念;文献[2]较系统地了开放环境下敏感数据的安全问题;文献[3]提出了开放环境下敏感数据防泄露若干关键技术,其中主要涉及威胁模型、数据管理机制、可信执行、数据封装加密、秘钥保存等问题;文献[4]提出基于关系数据库上基于数据目的概念分层的隐私数据访问控制机制(R-PAACEE)模型的隐私分析算法,可以判断用户隐私,且该方法,对于结构化数据、日志数据、XML数据均有判断力,并且依据不同场景进行了实验分析。

在开放环境下,除了网络安全和系统安全保障之外,还需要在安全的

收稿日期:2015-11-10
网络出版时间:2015-11-17
基金项目:国家自然科学基金(61071121)

体系结构和安全的数据保护机制等方面有相应的举措。2012年，美国一些知名的数据管理领域的专家学者联合发布白皮书《Challenges and Opportunities with Big Data》，提出数据安全及系统架构问题的挑战[5]。

信息安全的核心就是数据的安全，开展面向数据和以数据为核心的数据安全体系研究是十分必要的。文献[6]在无线传感网络上的应用中对面向数据的安全模型进行过研究，但没有从面向数据的安全体系结构上开展研究。

因此，需要有一种新的安全体系结构，即面向数据的安全体系结构，来应对这个挑战。文章针对开放环境下数据安全性问题，进行了安全体系设计，引入了面向数据的技术架构，构建安全的数据访问机制。

（2）新时代下需要更底层的体系结构来保证数据安全和其应用

“互联网+”行动计划带给我们两点启示：一是以互联网为代表的信息技术集合由过去的行业性质，转变为了可以支撑其他行业发展的基础；二是只有“互联网+数据”，才能把传统行业加到互联网上去发展。

随着人类的发展，人们在地球上构建了不同的皮肤（见表1），让人类赖以生存、生活和发展，否则，就会被地球所淘汰。在由互联网构成的新皮肤上，承载着数据，使人的智慧得到提高，人类本身得到更好地发展。

人类经过漫长的文明发展之路，从物质文明进入到了非物质文明，亦即进入到目前以信息社会和数据时代为特征的非物质文明或文明3阶段，如表2所示。

由表2中可见，文明3的核心就是数据。从映射真实世界的虚拟世界，到信息、知识、智慧的根本，都是数据；从数据出发，才有信息、知识、智慧和决策；从网络连接传输的内容，到服务器、云主机、终端所存储、处理和展示的内容，也都是数据。数据是人类认识世界、沟通交流、获得知识、智慧决策的本源。一切技术、业务、功能、流程都是为了数据，并围绕数据而开展的。

▼表1 数据思维之地球皮肤概念

皮肤	皮肤类型	承载内容	作用
皮肤1	自然界	万物	世界上的生物通过阳光、空气、土地、水等生存
皮肤2	语言	人类	人类通过语言实现广泛交流
皮肤3	纸张	文字	文字通过纸张进行广泛传播和交流
皮肤4	交通	人类和物品	人类和物品通过陆地交通、水上交通、空中交通，快速到达地球上的任何地方
皮肤5	电力线	电	电通过电力线，给人们带来光明和动力
皮肤6	有线无线电波	电报、电话、广播、电视	电报、电话、广播、电视等信息内容，通过有线和无线电波，在更大范围、以更快速度传播信息到世界各地，从单向到双向
皮肤7	互联网	数据	各种以数据形式的媒体信息，通过互联网实现全球范围广泛和交互式地交流

▼表2 数据思维之人类文明演进轨迹

阶段	持续时间	社会	时代	技术手段	特征	征服事物
文明0	几万年	原始社会	蛮荒时代	自体能力	人类靠本能生存	蛮荒蒙昧，自食其力
文明1	几千年	农耕社会	庄园时代	农耕技术、畜牧技术	物质文明：人类开始征服生命物质	征服农作物和家畜家禽，利用生物为人类服务
文明2	几百年	工商社会	帝国时代	建筑技术、冶炼技术、机械技术、制造技术、电力技术等	物质文明：人类开始征服无生命物质	征服煤、石油、金属、非金属，利用非生物为人类服务
文明3	几十年	信息社会	数据时代	计算机、互联网、物联网、社交网、云计算、智能技术、大数据	非物质文明：人类开始征服思想、智慧，核心为数据	征服人类自己的思想世界、精神世界、意识世界，利用信息和数据为人类服务

数据在文明3和非物质文明中是至关重要的基本要素，因此以数据视角来看待文明3，就需要有面向数据的体系结构和安全体系结构，来支撑非物质文明的社会发展。为此，作者提出面向数据的体系结构（DOA）[7]，来构建数据时代的底层架构，并试图去解决数据所有权、信息共享、系统功能扩展、数据管理、大数据分析和挖掘支持、软件工程、信息安全、数据拥有者利益保障等问题。

2 面向数据的安全体系结构

面向数据的安全体系结构（DOSA）旨在从架构角度对未来的数据安全体系进行全方位设计，包括数据的管理和应用等。DOSA是在DOA基础之上，面向数据和以数据为核心的关于数据的安全体系结构，构建起从数据保护到授权应用的整套机制。

DOSA建立在云计算基础之上，以数据“天生加密、授权使用”为原则，对数据的属性进行注册和管理，实现数据的安全管理和安全的相关应用。

中国颁布的《电子签名法》，从法律和技术层面上，为面向数据的安全体系结构奠定了重要基础。《电子签名法》所依赖的用户认证中心（CA）和公共密钥基础设施（PKI）技术，是面向数据的安全体系结构的基本数学和技术保障。

作为非物质社会的基本元素，数据应满足以下的基本特征：具有广义数据的概念，并有生命和属性（具有身份属性、安全属性、时间以及空间属性）。

（1）广义数据：凡是能够被计算机注册和登记的任何事物都称之为数据。

（2）身份属性：数据权属，即数据

的主人(数据生产者和数据所有者)、朋友(数据使用者或被授权人)、陌生人(未授权和待授权人)和敌人(不授权人、黑名单)。

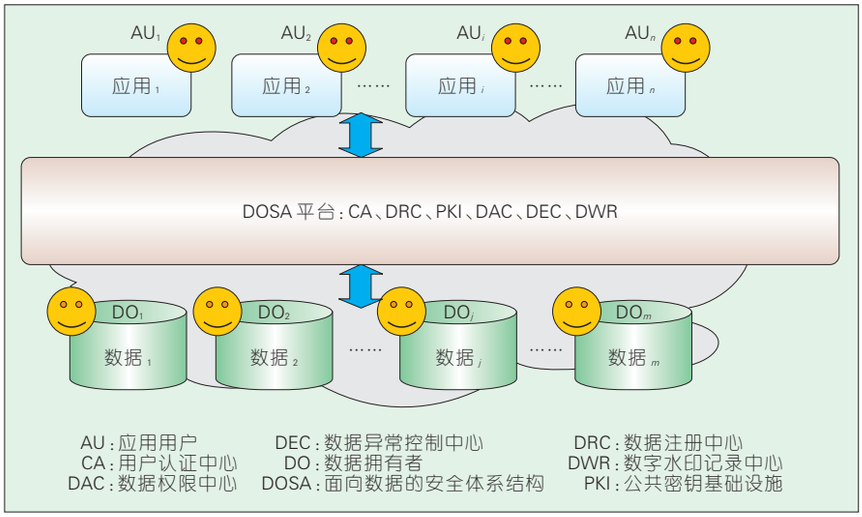
(3)安全属性:数据具有自保护功能,要“穿戴盔甲”,以加密方式呈现,具有不同的加密级别和深度,数据的使用要经过授权。

(4)时间和空间属性:数据的产生、授权以及使用等,都有时间和空间印记。

数据是应用的基础,不依赖于特定的硬件环境和软件环境,同一数据可以支撑不同的应用。

为便于管理,我们将数据分成存储和传输时保持加密的“数据”态和在应用中授权使用时解密的“应用态”。数据只有在应用态时是处于解密状态,一旦完成应用或离开了应用环境,或是由应用产生了新的数据,数据应立即变为加密的数据态,充分保证数据的安全及使用的授权。数据态的数据,既适合于封闭环境,也适合于较为开放环境,而应用态的数据,仅适合于相对来说比较封闭的环境[8-10]。

DOSA由以下主要部件构成:CA、数据注册中心(DRC)、PKI、数据权限中心(DAC)、数据异常控制中心(DEC)、数字水印记录中心(DWR)以及数据应用单元(DAUs)等,来构成面向数据的安全体系结构,从数据管理、数据安全保障到安全应用的全过程管理,如图1所示。



▲图1 DOSA平台与数据和应用之关系

2.1 CA用户认证

DOSA的一个核心理念是要确定数据与用户的关系,需要明确数据的所有权人。这就需要对参与网络活动的用户进行注册和身份确认。DRC要对所有用户进行登记注册,而用户身份则通过CA来进行认证。CA认证采用第三方CA认证中心,对网络用户颁发数字证书,即公钥和私钥。私钥以多种形式安全地发放到每位用户的手中,而公钥则存储在数据注册中心中。

2.2 DRC数据注册

DRC是DOSA的核心部件,用于注册各种数据的属性信息,包括数据的安全属性信息和数据权人信息等,并对数据的使用过程进行记录。DRC还要保留所有数据权人和应用用户的公钥。

DRC用来构建逻辑的数据资源池,通过建立索引和搜索引擎,实现数据和应用的管理和服务。一个DRC可以关联其他的DRC,从而实现广泛的数据共享。

2.3 PKI数据所有权与加密呈现

一旦数据产生了,DOSA平台就需要明确两件事情:一是要确定数据的生产者和数据的所有者;二是要对数据进行加密,防止他人窃取。一般情况下,数据的生产者就是数据的所有者。但在有些情况下,这两者是不一样的:数据的生产者不一定是数据的所有者。

确定数据的生产者,需要用数据生产者的私钥对数据进行加密(数字签名),标明数据的生产者身份。确定数据的所有者,则需要要用所有者的公钥加密来确定,同时实现数据的天生加密。对于体量较大的数据,可以采用对称密钥加密的办法,对对称密钥再进行公钥加密。不论数据是处于存储状态还是传输状态,都要保持加密呈现。

换句话说,用公钥加密,就确定了数据的所有者,并做到了数据加密呈现;用私钥加密,就确定了数据的生产者,数据生产者一般情况下就是数据所有者,但有些情况下不同。

2.4 DAC数据授权使用

DAC也是DOSA的关键部件,用于对数据进行授权管理。数据在生成、存储和传输时是加了密且不可使用的,而经过授权的用户在使用数据时才是解密和可访问的。数据授权,就是数据的权属变更,就是数据解密和加密的过程,即用数据所有者的私钥解密后再用数据使用者(被授权人)的公钥加密,授权过程[11]要通过水印和数据注册中心进行记录和管理。对于体量较大的数据,采取的是对称密钥加密方法,授权过程只是对对称密钥进行。

DOSA下的数据安全使用、记录,网络用户的认证等,可采用网络安全的验证、授权和记账(AAA)等技术。

2.5 DEC数据监管

DEC是DOSA的重要部件,用于

对数据资源进行自适应管理，保证数据的唯一性和一致性，监管和处置数据的各种异常行为。

2.6 DWR数字水印记录

DWR以水印的方式将数据所有者及授权使用过程记录下来，与原始数据一起进行加密管理，便于数据的溯源、记账和数据的非授权使用的取证。

2.7 DAUs数据安全应用

DAUs用于关联应用对数据的访问，并对各种应用提供支持。要确定数据安全应用的环境，一般考虑数据在内存中解密使用，要通过多种手段实现内存数据的安全保障和不被侵入窃取。

3 DOSA应用展望

DOSA作为一种数据安全理念和机制，就是要保证数据能够在数据和应用两个层面中都能做到安全、可靠，便于管理和使用，既可以在传统的封闭环境下应用，增强数据的安全保护，又可以在开放环境下保护数据的安全和不被越权访问[12-13]。

目前有关信息安全、数据安全的理论和方法体系，有关网络安全的AAA技术，有关CA技术、PKI技术、密钥体系、加解密技术，有关可信技术，以及不断发展的网络空间安全技术、系统安全技术、应用环境安全技术等，都能在DOSA框架下使用，但需要进一步从面向数据和以数据为核心的角度，进行重新梳理，从数据安全的理念、理论、方法和受保护数据的应用机制等方面，进行适应性和深入地研究，为进一步提高信息安全提供保障[14-15]。

基于DOSA，目前正在试点开展以下一些应用：

（1）数据交易（虚拟数字资产保护及交易）平台。在建立数据资产所有权的基础上，通过数据加密呈现、授权交易、过程记录、价值评估、记账计费管理、水印溯源等，保障数据安全交易和数据拥有者利益。

（2）数据隐私保护。通过分析数据和隐私的特征，进行数据脱敏、数据所有权确认、数据加密、数据授权应用、数据安全应用、数据过程记录和溯源等，进行一些数据的隐私保护研究。

4 结束语

开放环境下信息安全问题集中体现在数据的安全上。DOSA采用面向数据和以数据为核心的理念，建立数据与用户之间的权属关系，采用数据“天生加密，授权使用”方法，通过CA、DRC、DAC、DEC、PKI、DWR、DAUs等实现数据的安全管理和安全应用，建立从数据保护到授权应用的整套机制。

基于DOSA的初步应用表明：面向数据的安全体系结构能有效解决和应对开放环境下数据的安全、数据所有权、数据交易、数据共享、数据管理、数据隐私保护等问题和挑战。

致谢

本研究得到中国软件行业协会赵小凡理事长、北京邮电大学杨义先教授、四川省计算机学会宋昌元秘书长以及成都大学大数据研究院、成都理工大学空间信息技术研究所、成都灵云信息技术有限公司、成都五舟汉盛科技有限公司、四川红山世纪科技有限公司等的大力支持和帮助，谨致谢意！

参考文献

[1] 朱静波. 网络环境下敏感数据的发布和管理[D]. 杭州: 浙江大学, 2006
[2] 陈珂. 开放式环境下敏感数据安全的关键技术研究[D]. 杭州: 浙江大学, 2007
[3] 闫玺玺. 开放网络环境下敏感数据安全与防泄密关键技术研究[D]. 北京: 北京邮电大学, 2012
[4] 刘逸敏. 基于访问目的的隐私数据访问控制机制研究[D]. 上海: 复旦大学, 2012
[5] AGRAWAL D, BERNSTEIN P, BERTINO E, et al. Challenges and Opportunities with Big Data–A Community White Paper Developed by Leading Researchers Across the United States [EB/OL].[2012–10–02]. http://www.cra.org/ccc/files/docs/init/bigdatawhitepaper.pdf
[6] XIAO X R, SUN X M, WANG X B, et al. DOSM: A Data–Oriented Security Model Based on Information Hiding in WSNs [J]. Information Technology Journal, 2009, 8(5): 678–687
[7] 苗放.DOA（面向数据的体系结构）[EB/OL]. http://baike.baidu.com/subview/649092/12822804.htm#viewPageContent, 2014
[8] 尹建国. 美国网络信息安全治理机制及其对我国之启示[J]. 法商研究, 2013, (2): 138–146
[9] 赵勇. 大数据革命:理论、模式与技术创新[M]. 北京:电子工业出版社, 2014
[10] 王世伟. 论信息安全、网络安全、网络空间安全[J]. 中国图书馆学报, 2015, 41(2): 72–84. doi:10.13530/j.cnki.jlis.150009
[11] KRESIMIR S, HRVOJE O, MARIN G. The Information Systems' Security Level Assessment Model Based on An Ontology and Evidential Reasoning Approach [J]. Computers & Security, 2015, 55(6): 100–112.doi: doi:10.1016/j.cose.2015.08.004
[12] GEORGE S, VLADLENA B, JEAN N E, et al. Individual Information Security, User Behaviour and Cyber Victimisation: An Empirical Study of Social Networking Users [J]. Technological Forecasting and Social Change, 2015, (5): 320–330. doi:10.1016/j.techfore.2015.08.012
[13] GURPREET D, ROMILLA S, CRISTIANE P. Interpreting Information Security Culture: An Organizational Transformation Case Study [J]. Computers & Security, 2015, (4): 63–69.doi: 10.1016/j.cose.2015.10.001
[14] 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
[15] 孟小峰, 慈祥. 大数据管理:概念、技术与挑战[J]. 计算机研究与发展, 2013, (1): 146–169

作者简介

苗放，成都大学大数据研究院院长，成都理工大学空间信息研究所所长、教授、博士生导师；主要研究方向为空间信息技术及应用、大数据管理；先后主持国家自然科学基金项目、国家“863”、“973”计划子课题、部省项目20余项，成果获得部省级二等奖2项，三等奖2项；已发表论文160余篇，其中被EI检索20余篇。