



云计算差异化安全技术研究^{*}

李冬梅¹, 尹式钧², 陈剑勇²

(1. 中兴通讯股份有限公司技术战略部 深圳 518057; 2. 深圳大学计算机与软件学院 深圳 518060)

摘要: 云计算的部署和应用可以明显节约 IT 成本, 促进业务的创新和发展, 然而公有云将用户数据和业务处理环节交由独立第三方提供, 使用户数据和业务系统面临更多的安全威胁, 安全已经成为云计算发展的主要瓶颈。本文根据用户对云业务多样化的安全需求, 提出差异化安全技术框架, 在满足用户安全要求的前提下, 降低安全对云计算计算资源的消耗, 从而促进云计算的应用。

关键词: 云计算; 安全; 差异化安全

doi: 10.3969/j.issn.1000-0801.2013.03.012

Study on Differentiated Security Service Based on Cloud Computing

Li Dongmei¹, Yin Shijun², Chen Jianyong²

(1. Department of Technology Strategy, ZTE Corporation, Shenzhen 518057, China;

2. Department of Computer Science and Technology, Shenzhen University, Shenzhen 518060, China)

Abstract: Deployment and application of cloud computing can significantly save computing resource, and promote business innovation and development. However, if users' data is stored and processed in public cloud computing which is provided by an independent third party, more security threat will be faced than that of the traditional way. Security has become one of the most important obstacles for the development of cloud computing. Differentiated security architecture was proposed, according to the diversity of security requirements from different users. The consumption of computing resource from security service could be reduced and thus the development of cloud computing is benefited.

Key words: cloud computing, security, differentiated security

1 引言

云计算使内容提供商能够快速部署和扩展服务, 并通过低成本、付费使用的模式获利。与此同时, 用户能够充分地体验基于互联网运算的弹性。云计算一般表现为软件即服务(SaaS)、平台即服务(PaaS)、基础设施即服务(IaaS)的形式。成功运营云计算的企业包括亚马逊的 EC2/S3、

Google App 和 force.com 等。

然而, 由云计算提供的弹性和高效配置对安全提出更高要求^[1]。用户很难完全信任基于云计算的服务, 因为云计算对数据的存储和防护机制不能由用户完全控制, 所以会导致更多的安全风险。例如服务提供商将用户已经删除的数据进行恢复, 用于非法获利或者将用户的隐私信息非法卖给第三方等^[2]。

^{*} 国家自然科学基金资助项目(No.61170283), 深圳市基础研究计划基金资助项目(No. JC201005250045A)

当前的云安全研究仍然处于早期阶段,还没有一套通用的模式或技术出现。目前的一些研究方法包括隔离不同用户的业务和数据,防止用户间的安全风险互相渗透^[2];利用第三方审计平台确保用户数据的完整性^[3,4];研究基于数据属性和语义的访问控制机制^[5,6];采用多种安全策略来验证和管理用户的身份,从而保护数据不受未经授权的用户使用,例如针对访问用户数据和操作系统的事件,亚马逊通过日志进行详细审计^[6]。

以上对云计算安全的研究,都是应对某一具体的安全威胁,并没有在系统层面建立有效应对各种安全威胁的综合解决方案。而且,这些针对特定安全威胁的技术并没有反映云计算用户对安全需求的动态变化。例如有些服务涉及公共信息,只需要基础的安全。而一些重要的服务,如电子商务的交易过程,则需要有非常高的安全要求。可见,如果将传统安全解决方案所追求的安全性越高越好的策略用于设计云计算安全解决方案,将明显浪费云计算资源。

2 差异化安全需求

安全,本质意义上讲是对风险的有效控制。信息安全技术只能降低风险发生的概率,而不能完全避免事件的发生。因此,若不考虑安全的实施成本,用户对安全的需求是无止境的。从这个意义上讲,如何在成本可控的前提下,尽量减少安全风险,成为近年来网络安全解决方案发展的主要方向。差异化安全服务指系统为用户提供个性化安全防护能力,满足用户多样化的安全要求。差异化安全服务主要来源于以下安全需求^[7,8]。

(1) 业务日益丰富导致安全需求的多样性

云计算将大规模的计算承载在云端运行,客户终端可以通过轻量级的应用(如 Web 应用)来获取相应的数据。随着 IT 技术的进步和应用需求的扩展以及计算能力的不断增加,建立在云端的业务将会趋向多样化。

一方面,不同的业务有不同的安全需求,采用单一的安全机制无法适应业务多样化的需求。比如对于朋友之间日常聊天的话音业务,传输的信息资产对第三方来讲价值比较低,因此不需要有高等级的安全服务;但如果传输的信息是与金融业务相关的,如信用卡信息,就必须有高等级的安全服务来确保信息不被泄露。

另一方面,同一业务在不同场合以及面对不同使用者时,其业务的安全需求也可能不同。比如多媒体视频业务,当用于视频点播时,只需要低等级的安全防护;而用于商

业目的的视频会议,若传输的信息资产价值比较高,则需要高等级的安全防护。因此,从业务需求的角度分析,云计算需要从技术上提供机制,使具体的业务可以选择合适等级和技术的安全防护,而选择权既可以在终端,也可以在云端服务器,还可以是双方的平等协商。

(2) 只有分级的安全服务才能有效地利用资源

当服务商将业务搬到云计算平台上时,安全需求的差异性就阻碍了业务的部署。如果统一应用高等级的安全服务(如加密全部数据),会严重制约计算资源的合理使用。对信息价值不大的业务使用高等级安全意味着计算资源的浪费,从这个意义上讲,有必要根据信息资产价值的大小,适当进行分级处理。对于高安全需求的业务,采用较高级别的防护力度;对于低安全需求的业务,采用低级别的防护力度。从而能够建立资源有偿使用机制,有效利用资源。

(3) 安全服务需要持续的投入

将应用服务迁移到云平台是一个重要的发展趋势。安全的网络意味着网络提供商需要更多的投资,并且安全是相对的,不存在绝对安全的网络。安全防护力度和网络提供商对网络安全设施的投入多少紧密相关,这种投入至少包含网络安全管理、安全设备、更多的带宽消耗、计算资源消耗、对安全管理人员和用户的安全培训等费用。

将投入和产出联系起来,形成可持续发展的价值链,是实现网络安全良性发展的前提条件。因此客观上需要要有技术解决方案,提供将差异化安全服务转化为增值服务的途径,从而由运营商或服务商向用户提供按需所取的安全服务,并根据服务的代价进行合理收费。安全一旦成为一种增值业务,用户为高等级的安全服务支付费用,对低等级的安全服务免费或支付少量费用。这样一来,运营商既能够将安全的投入转化为可盈利的业务,又满足了用户对安全的差异化需求。

(4) 针对用户简单、高效的安全服务

安全服务内涵丰富,既包括基础安全服务,如加密、认证、抗抵赖、完整性保护等;也包括应用安全服务,如在线杀毒、入侵检测、安全预警、内容监控等。除了防止信息被非法获取外,还需要防范更广泛的安全威胁,如病毒的攻击、木马程序对信息的非法收集、用户欺骗等威胁,因此,安全解决方案越来越复杂。然而由于用户需要简单有效地使用各种业务,因此需要把复杂的安全服务以及相应的安全配置,尽量在网络侧解决,从而确保用户在没有安全专业知识的情况下,能够享受到安全的各种业务。



3 安全域的划分

业务数据流在云计算中一般处于传输、业务逻辑处理和存储3种状态中的一种。业务数据在一种状态下所面临的安全威胁基本相同,因此所需要的安全功能相同。为了便于安全中心通过安全策略控制云计算中的安全功能,笔者将云计算安全划分为传输安全域、业务逻辑安全域和存储安全域3个安全域,如图1所示。存储安全域和业务逻辑安全域通过传输安全域相互链接。安全中心控制每个安全域所属安全功能的运行。安全中心承担安全策略的管理功能,并通过安全策略驱动3个安全域所属的安全功能对用户业务数据实施差异化安全防护。

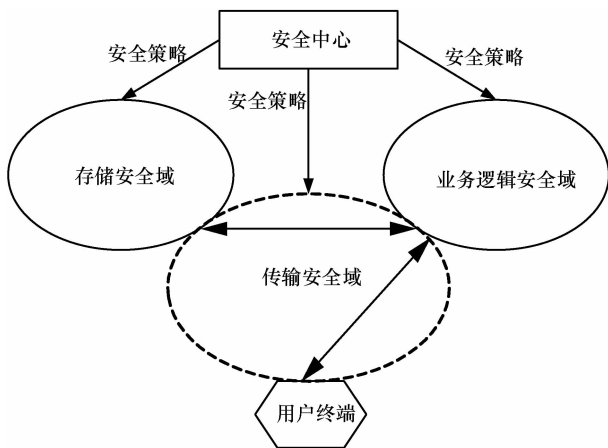


图1 安全中心、安全域与用户终端的相互关系

安全域划分的优点如下。

- 同一个安全域面临相似的安全威胁,这种划分有利于每一个安全域专注解决本域的安全问题。
- 尽管云计算解决方案有复杂的部署方式,但用户数据可以归结为由传输、业务逻辑处理和存储3种状态组成。这种功能域划分方式有助于从逻辑层面设计出有效的安全架构。
- 对云计算来说,传输、业务逻辑和存储3大功能域并没有必要由单一运营商提供,有可能分属不同的运营商运营。部分功能域也有可能属于私有云范畴,比如某集团企业,其传输用了电信运营商网络,业务平台用了第三方云服务提供商,而存储则直接放在公司的内部网。由此可见,云计算这3大功能域,是可以相互分离的,因此安全域的划分有必要以这3大功能域的划分为边界。

4 差异化安全框架

如图2所示,在3层的安全框架中,接入层负责接收用户指定的安全等级、接入网风险和服务类型3种输入参数;策略层根据以上输入参数,通过策略规则匹配,输出安全功能参数,用于驱动每个安全域的安全功能;安全功能层的安全功能根据安全功能参数,保护特定的业务数据。

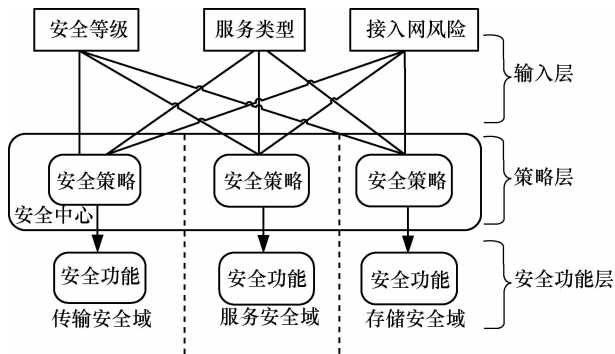


图2 差异化安全框架

(1) 输入层

安全等级参数:安全等级一般由用户提出,体现用户对业务数据的安全要求。一般来讲,业务数据价值越高,所需要的安全等级也越高。安全等级不同于安全强度,安全强度一般指安全功能对业务数据所能提供的防护力度。安全强度取决于安全等级和安全风险的综合作用。

服务类型参数:由于不同的服务类型需要不同的安全功能组合,因此该体系结构在输入层中包含了服务类型参数。例如,多媒体服务对时延比较敏感,一定程度上允许数据分组的丢失,无需完整的验证。而文件传输服务则刚好相反,完整性的验证是一项非常重要的保护机制。业务类型可以由云计算通过业务感知自动识别,无需用户设定。

接入网风险参数:用户可以通过3G、公共Wi-Fi或有线网络接入云计算平台,不同的接入网场景所面临的安全风险不同。例如公共Wi-Fi接入风险较高,而在办公场所通过有线宽带接入,则面临的风险较低。云计算可以通过用户终端或接入网设备识别接入网场景,从而能自动评估其所面临的风险,因此接入网参数无需用户设置。在安全等级相同的条件下,接入网安全风险越高,所需要的安全强度也越大。

(2)策略层

每个安全域的安全策略相对独立,各自接收来自输入层的3种参数,通过策略的规则匹配,输出安全功能参数。安全策略的主要作用是根据这些输入参数,经过策略匹配,输出合适的安全功能参数。

(3)安全功能层

每个安全域都有一组特定的安全功能,接受来自策略层的安全功能参数的驱动,对业务数据实施安全防护。例如传输安全域中的IPSec、业务逻辑安全域中的Honeypot、数据存储安全域中的加密/解密模块等。有些安全功能同时存在于多个安全域,并有不同的专业术语。例如,入侵检测在网络安全域中是基于网络的入侵检测,而在业务逻辑安全域中是基于主机的入侵检测。

业务数据通过特定标识(ID)在每个安全域中被识别,并获得相应的安全防护。如图3所示,在传输安全域中,业务数据的用户ID和业务ID被安全功能模块获取,安全功能模块由此确定该业务数据所需使用的安全功能参数,并对该业务数据实施相应的安全防护,如加密等。

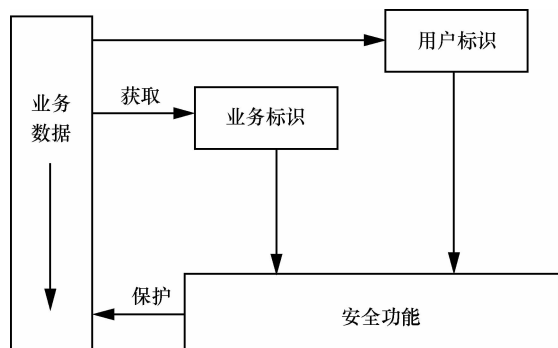


图3 传输安全域安全功能对数据的防护过程示意

5 结束语

本文首先分析了差异化安全需求,并在此基础上提出了差异化安全框架,该框架由输入层、策略层和安全功能层3部分组成,并作用在云计算的传输安全域、业务逻辑安全域和存储安全域。通过用户标识和业务标识,使业务数据在云计算不同安全域中获得差异化防护服务。该框架能够满足云计算差异化安全需求,有利于降低安全对云计算计算资源的消耗,促进云计算的应用。

参考文献

1 Takabi H, Joshi J B D, Ahn G J. Security and privacy

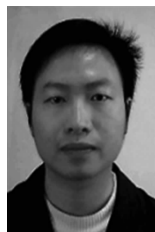
challenges in cloud computing environments. IEEE Computer Society, 2010, 8(6): 24~31

- 2 Subashini S, Kavitha V. A Survey on security issues in service delivery models of cloud computing. Network and Computer Applications, 2011, 34(1): 1~11
- 3 Wang C, Ren K, Lou W T, et al. Toward publicly auditable secure cloud data storage services. IEEE Network, 2010, 24(4): 19~24
- 4 Wang Q, Wang C, Li J, et al. Enabling public auditability and data dynamics for storage security in cloud computing. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(5): 847~859
- 5 Hu L K, Yi S, Jia X Y. A semantics-based approach for cross domain access control. Internet Technology, 2010, 11(2): 279~288
- 6 Pallis G. Cloud computing: the new frontier of internet computing. IEEE Internet Computing, 2010, 14(5): 70~73
- 7 ITU-T Recommendation. ITU-T X.1123 Differentiated Security Service for Secure Mobile End-to-End Data Communication, 2007
- 8 陈剑勇, 腾志猛, 刘利军等. YD/T 2037-2009 移动通信差异化安全服务, 2009

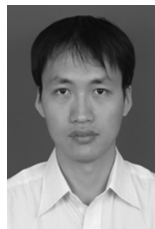
[作者简介]



李冬梅,女,中兴通讯股份有限公司技术战略部主任工程师,主要研究方向为网络通信标准。



尹式钧,男,深圳大学计算机与软件学院硕士研究生,主要研究方向为网络与信息安全。



陈剑勇,男,深圳大学计算机与软件学院教授,主要研究方向为网络与信息安全。

(收稿日期:2013-02-20)