云安全研究进展及技术解决方案发展趋势

陈　军　中国电信北京研究院网络运营支撑中心高级工程师
薄明霞　中国电信北京研究院网络运营支撑中心高级工程师
王渭清　中国电信北京研究院网络运营支撑中心工程师

摘要：针对横亘在云计算发展道路上的一个鸿沟——安全性，本文介绍了云安全的概念及其内涵，并对云安全研究的主要方向及云安全研究主流厂家技术解决方案的现状及发展趋势进行了详细阐述，这对我国云计算安全的发展具有一定的借鉴意义。
关键词：云安全，技术解决方案

Abstract：Security has become a critical issue in cloud computing. This article describes the concept and signification of cloud security, and introduces major topics in research and technology solutions from mainstream IT companies with regard to cloud security.
Key words: cloud computing, clouding security, solution

随着网络进入更加自由和灵活的 Web2.0 时代，云计算的概念风起云涌。所谓云计算，就是利用虚拟化技术建立统一的基础设施、服务、应用及信息的资源池，以分布式技术对各种基础设施资源池进行有效组织和运用的一种运行模式。

云计算的出现使得公众客户获得低成本、高性能、快速配置和海量化的计算服务成为可能。但正如一件新鲜事物在带给我们好处的同时，也会带来问题一样，云计算在带给我们规模经济、高应用可用性益处的同时，其核心技术特点（虚拟化、资源共享、分布式等）也决定了它在安全性上存在着天然隐患。例如，当数据、信息存储在物理位置不确定的“云端”，服务安全、数据安全与隐私安全如何保障？这些问题是否会威胁到个人、企业以至国家的信息安全？虚拟化模式下业务的可用性如何保证？为此，现阶段云安全研究成为云计算应用发展中最为重要的研究课题之一，得到越来越多的关注。

1　云安全的含义及研究方向

所谓云安全，主要包含两个方面的含义。第一是云自身的安全保护，也称为云计算安全，包括云计算应用系统安全、云计算应用服务安全、云计算用户信息安全

等，云计算安全是云计算技术健康可持续发展的基础；第二是使用云的形式提供和交付安全，也即云计算技术在安全领域的具体应用，也称为安全云计算，就是基于云计算的、通过采用云计算技术来提升安全系统的服务效能的安全解决方案，如基于云计算的防病毒技术、挂马检测技术等。

针对云安全，目前研究方向主要有三个。第一是云计算安全，主要研究如何保障云自身及其上的各种应用的安全，包括云计算平台系统安全、用户数据安全存贮与隔离、用户接入认证、信息传输安全、网络攻击防护、合规审计等；第二是安全基础设置的云化，主要研究如何采用云计算技术新建、整合安全基础设施资源、优化安全防护机制，包括通过云计算技术构建超大规模安全事件、信息采集与处理平台，实现对海量信息的采集、关联分析、提升全网安全态势把控及风险控制能力等；第三是云安全服务，主要研究各种基于云计算平台为客户提供的安全服务，如防病毒服务等。本文重点对云计算安全的研究进行及进行探讨。

2 云安全研究进展

目前，对云安全研究最为活跃的组织是云安全联盟（CSA：Cloud Security Alliance）。CSA 作为业界比较认可的云安全研究论坛，在 2009 年 12 月 17 日发布了一份云计算服务的安全实践手册——《云计算安全指南》，该指南总结了云计算的技术架构模型、安全控制模型以及相关合规模型之间的映射关系，如图 1。

根据 CSA 提出的云安全控制模型，“云”上的安全首先取决于云服务的分类，其次是“云”上部署的安全架构以及业务、监管和其它合规要求。对这两部分内容进行差距分析，就可以输出整个“云”的安全状态，以及如何与资产的保障要求相关联。

2010 年 3 月云安全联盟又发表了其在云安全领域的最新研究成果——云计算的七大安全威胁，获得了广泛的引用和认可，其主要内容如下：

·云计算的滥用、恶用、拒绝服务攻击
·不安全的接口和 API
·恶意的内部员工
·共享技术产生的问题
·数据泄漏
·账号和服务劫持
·未知的安全场景

依据 CSA 提出的技术观点，国际上一些组织和机构如 CAM （Common Assurance Metric Beyond the Cloud）、微软以及国内的绿盟科技等也在云安全领域进行了系列探索，如云计算安全技术体系框架研究、云安全技术解决方案研究等。关于云计算安全技术体系框架，目前比较获得认可的模型如图 2 所示。

从图 2 可以看出，对于不同的云服务模式（IaaS、PaaS、SaaS），安全关注点是不一样的。当然也有一些是这三种模式共有的，如数据安全、加密和密钥管理、身份识别和访问控制、安全事件管理、业务连续性等。

（1）IaaS 层安全

IaaS 涵盖从机房设备到硬件平台的所有基础设施资源层面，它包括将资源抽象化的能力，并交付里

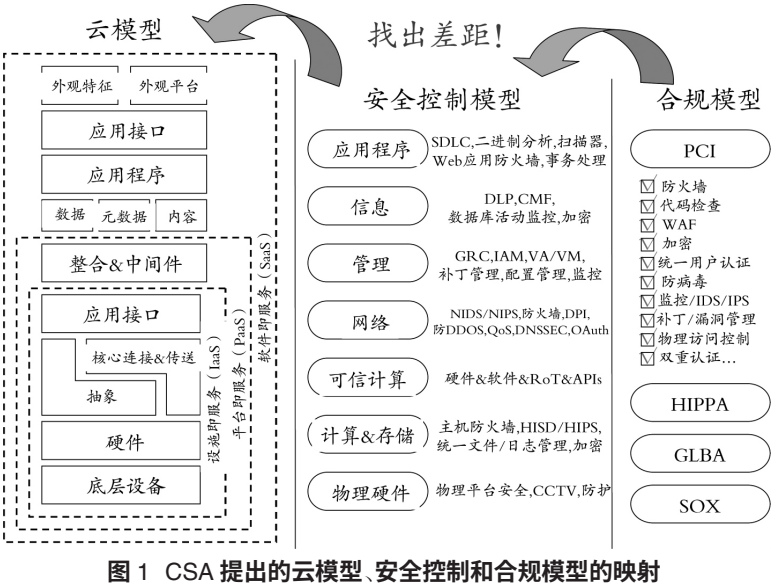

图 1 CSA 提出的云模型、安全控制和合规模型的映射

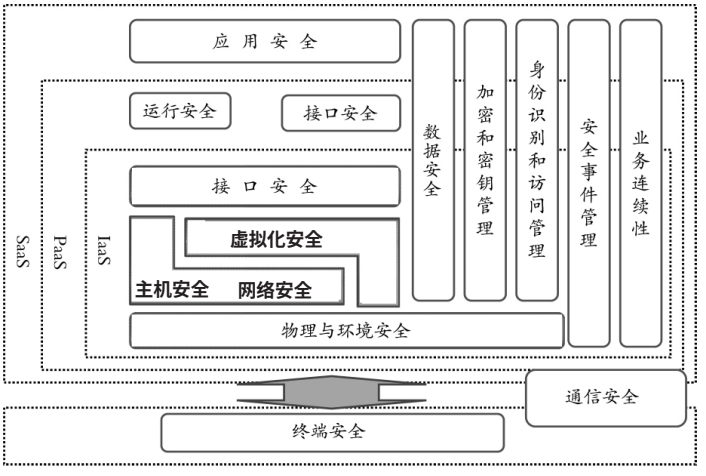

图 2 云计算安全技术体系框架

阿杰到这些资源的物理或逻辑网络连接，终极状态是 IaaS 提供商提供一组 API，允许用户管理基础设施资源以及进行其它形式的交互。IaaS 层安全主要包括物理安全、主机安全、网络安全、虚拟化安全、接口安全，以及数据安全、加密和密钥管理、身份识别和访问控制、安全事件管理、业务连续性等。

⑵ PaaS 层安全

PaaS 位于 IaaS 之上，它由 IaaS 增加了一个层面得来，用以与应用开发框架、中间件能力以及数据库、消息和队列等功能集成。PaaS 允许开发者在平台之上开发应用，开发的编程语言和工具由 PaaS 提供。PaaS 层的安全主要包括接口安全、运行安全以及数据安全、加密和密钥管理、身份识别和访问控制、安全事件管理、业务连续性等。

⑶ SaaS 层安全

SaaS 位于 IaaS 和 PaaS 之上，它能够提供独立的运行环境，用以交付完整的用户体验，包括内容、展现、应用和管理能力。SaaS 层的安全主要是应用安全，当然也包括数据安全、加密和密钥管理、身份识别和访问控制、安全事件管理、业务连续性等。

4 云安全技术解决方案发展趋势

以上对云安全研究的进展进行了阐述。从整体上来说，国际上关于云计算安全问题的研究也是刚刚起步，虽然很多的组织和机构都在积极地对云计算的安全问题进行分析和研究，但主要是 CSA 以及微软、谷歌、亚马逊等几个为数不多的组织和机构能够比较清晰地提出各自对云计算安全问题的基本认识以及关于云计算安全问题的初步解决方案。为此，现对主流企业云安全研究进展及技术解决方案进行阐述。

⑴ 微软

微软的云计算平台叫做 Windows Azure。在 Azure 上，微软通过采用强化底层安全技术性能、使用所提出的 Sydney 安全机制，以及在硬件层面上提升访问权限安全等系列技术措施为用户提供一个可信任的云，从私密性、数据删除、完整性、可用性和可靠性五个方面保证云安全。

·私密性：Windows Azure 通过身份和访问管理、SMAPI 身份验证、最少特权用户软件、内部控制通信量的 SSL 双向认证、证书和私有密钥管理、Windows Azure Storage 的访问控制机制保证用户数据的私密性。

·隔离：把不同的数据适当地进行隔离，作为一种保护方式。微软提供了管理程序，Root OS 和 Guest VMs 的隔离、Fabric Controllers 的隔离 、包过滤、VLAN 隔离、用户访问的隔离五种隔离方式给用户数据提供保护。

·加密：在存储和传输中对数据进行加密，确保数据的保密性和完整性。此外，针对关键的内部通信，使用 SSL 加密进行保护。作为用户的选择之一，Windows Azure SDK 扩展了核心.NET 类库以允许开发人员在 Windows Azure 中整合.NET 加密服务提供商（CSPs）；

·数据删除：Windows Azure 的所有的存储操作，包括删除操作被设计成即时一致的。一个成功执行的删除操作将删除所有相关数据项的引用使得它无法再通过存储 API 访问。所有被删除的数据项在之后被垃圾回收。正如一般的计算机物理设备一样，物理二进制数据在相应的存储数据块为了存储其他数据而被重用的时候会被覆盖掉。

·完整性：微软的云操作系统以多种方式来提供这一保证。对客户数据的完整性保护的首要机制是通过 Fabric VM 设计本身提供的。每个 VM 被连接到三个本地虚拟硬盘驱动（VHDs）：D 驱动器包含了多个版本的 Guest OS 中的一个，保证了最新的相关补丁，并能由用户自己选择；E 驱动器包含了一个被 FC 创建的映像，该映像是基于用户提供的程序包的；C 驱动器包含了配置信息，paging 文件和其他存储。另外存储在读 / 写 C:驱动中的配置文件是另一个主要的完整性控制器。至于 Windows Azure 存储，完整性是通过使用简单的访问控制模型来实现的。每个存储账户有两个存储账户密钥来控制所有对在存储账户中数据的访问，因此对存储密钥的访问提供了完全的对相应数据的控制。Fabric 自身的完整性在从引导程序到操作中都被精心管理。

·可用性：Windows Azure 提供了大量的冗余级别来提升最大化的用户数据可用性。数据在 Windows Azure 中被复制备份到 Fabric 中的三个不同的节点来最小化硬件故障带来的影响。用户可以通过创建第二个存储账户来利用 Windows Azure 基础设施的地理分布特性达到热失效备援功能。

·可靠性：Windows Azure 通过记录和报告来让用户了解这一点。监视代理（MA）从包括 FC 和 Root OS 在内的许多地方获取监视和诊断日志信息并写到日志文件中，最终将这些信息的子集推送到一个预先配置好的 Windows Azure 存储账户中。此外，监视数据分析服务（MDS）是一个独立的服务，能够读取多种监视和诊断日志数据并总结信息，将其写到集成化日志中。

⑵ 谷歌

在 2010 年，为使其安全措施、政策及涉及到谷歌应用程序套件的技术更透明，谷歌发布了一份白皮书，向当前和潜在的云计算客户保证强大而广泛的安全基础。此外，谷歌在云计算平台上还创建了一个特殊门户，供使用应用程序的用户了解其隐私政策和安全问题。

谷歌的云计算平台上主要从三个部分着手保障云安全。

·人员保证。谷歌雇佣一个全天候的顶级信息安全团队，负责公司周围的的防御系统并编写文件，实现谷歌的安全策略和标准。

·流程保证。应用要经过多次的安全检查。作为安全代码开发过程，应用开发环境是严格控制并认真调整到最大的安全性能。外部的安全审计也有规则的实施来提供额外的保障。

·技术保证。为降低开发风险，每个 Google 服务器只根据定制安装必需的软件组件，而且在需要的时候，均匀的服务器架构能够实现全网的快速升级和配置改变。数据被复制到多个数据中心，以获得冗余的和一致的可用性。在安全上，实现可信云安全产品管理、可信云安全合作伙伴管理、云计算合作伙伴自管理、可信云安全的接入服务管理、可信云安全企业自管理。在可信云安全系统技术动态 IDC 解决方案中，采取面向服务的接口设计、虚拟化服务、系统监控服务、配置管理服务、数据保护服务等方法，实现按需服务、资源池、高可扩展性、弹性服务、自服务、自动化和虚拟化、便捷网络访问、服务可度量等特点。

⑶ 亚马逊

亚马逊是互联网上最大的在线零售商，但是同时也为独立开发人员以及开发商提供云计算服务平台。亚马逊是最早提供远程云计算平台服务的公司，他们的云计算平台称为弹性计算云（Elastic Compute Cloud，EC2）。亚马逊从主机系统的操作系统、虚拟实例操作系统火客户操作系统、防火墙以及 API 呼叫多个层次为 EC2 提供安全，目的就是防止亚马逊 EC2 中的数据被未经认可的系统或用户拦截，并在不牺牲用户要求的配置灵活性的基础上提供最大限度的安全保障。EC2 系统主要包括以下组成部分。

·主机操作系统。具有进入管理面业务需要的管理员被要求使用多因子的认证以获得目标主机的接入。这些管理主机都被专门设计、建立、配置和加固，以保证云的管理面，所有的接入都被记录并审计。当一个员工不再具有这种进入管理面的业务需要时，

对这些主机和相关系统的接入和优先权被取消。

·客户操作系统：虚拟实例由用户完全控制，对账户、服务和应用具有完全的根访问和管理控制。AWS 对用户实例没有任何的接入权，并不能登录用户的操作系统。 AWS 建议一个最佳实践的安全基本集，包括不再允许只用密码访问他们的主机，而是利用一些多因子认证获得访问他们的例子。另外，用户需要采用一个能登录每个用户平台的特权升级机制。例如，如果用户的操作系统是 Linux，在加固他们的实例后，他们应当采用基于认证的 SSHv2 来接入虚拟实例，不允许远程登陆，使用命令行日志，并使用“sudo”进行特权升级。用户应生成他们的关键对，以保证他们独特性，不与其他用户或 AWS 共享。

·防火墙：亚马逊 EC2 提供了一个完整的防火墙解决方案。这个归本地的强制防火墙配置在一个默认的 deny- all 模式，亚马逊 EC2 顾客必须明确地打开允许对内通信的端口。通信可能受协议、服务端口以及附近的的源设定接口的网络逻辑地址的限制。防火墙可以配置在组中，允许不同等级的实例有不同的规则。

·实例隔离：运行在相同物理机器上的不同实例通过 Xen 程序相互隔离。另外，AWS 防火墙位于管理层，在物理网络接口和实例虚拟接口之间。所有的包必须经过这个层，从而一个实例的附近的实例与网上的其他主机相比，没有任何多余的接入方式，并可认为他们在单独的物理主机上。物理 RAM 也使用相同的机制进行隔离。 客户实例不能得到原始磁盘设备，而是提供虚拟磁盘。AWS 所有的的圆盘虚拟化层自动复位用户使用的每个存储块，以便用户的数据不会无意的暴露给另一用户。AWS 还建议用户在虚拟圆盘之上使用一个加密的文件系统，以进一步保护用户数据。

⑷ 中国电信

作为拥有全球最大固话网络和中文信息网络的基础电信运营商，中国电信一直高度关注云计算的发展。对于云安全，中国电信认为，云计算应用作为一项信息服务模式，其安全与 ASP（应用托管服务）等传统 IT 信息服务并无本质上的区别，只是由于云计算的应用模式及底层架构的特性，使得在具体安全技术及防护策略实现上会有所不同。为有效保障云计算应用的安全，需在采取基本的 IT 系统安全防护技术的基础上，结合云计算应用特点，进一步集成数据加密、VPN、身份认证、安全存储等综合安全技术手段，构建面向云计算应用的纵深安全防御体系，并重点解决如下问题。

·云计算底层技术架构安全：如虚拟化安全、分布式计算安全等。

·云计算基础设施安全：保障云计算系统稳定性及服务连续性。

·用户信息安全：保护用户信息的可用性、保密性和完整性。

·运营管理安全：加强运营管理，完善安全审计及溯源机制。

5 结语

随着云计算部署和实施规模的日益扩大，对“云”安全的研究及技术解决方案的探索将持续深入。微软、谷歌、亚马逊等 IT 巨头们以前所未有的速度和规模推动云计算的普及和发展，而云安全技术推出的时间不长，且网络威胁是动态变化的，所以云安全技术永远都处于不断研发、完善和前进的过程中。各大公司积极地应对云安全，为此，我们对云计算主流企业的云安全研究进展和解决方案进行分析和跟踪，对我国云计算安全事业的发展有一定的现实意义。 MSTT

参考文献

[1] Microsoft. Securing Microsoft’s Cloud Infrastructure , 2009, 5.
[2] Google. Security Whitepaper: Google Apps Messaging and Collaboration Products.2010.
[3] Amazon Web Services: Overview of Security Processes . http://d36cz9buwru1tt.cloudfront.net/pdf/AWS_Security_Whitepaper.pdf.
[4] CSA,Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. http://www.cloudsecurityalliance.org/csaguide.pdf.
[5] CSA,Top Threats to Cloud Computing V1.0.http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.
[6]Biggest Cloud Challenge:Secuity.http://cloudsecurity.org/blog/2008/10/14/biggest- cloud- challenge- security.html.