



云计算应用模式下移动互联网安全问题浅析^{*}

房秉毅¹, 张云勇¹, 吴俊², 徐雷¹

(1. 中国联通集团研究院 北京 100048; 2. 北京邮电大学 北京 100876)

摘要: 根据云计算模式下移动互联网的安全目标和层次结构, 在聚合网络系统中现有安全技术的基础上, 构建了云计算模式下的移动互联网安全保护体系, 并分析了其中关键的安全问题。

关键词: 云计算; 移动互联网; 安全

doi: 10.3969/j.issn.1000-0801.2013.03.009

Analysis on Mobile Internet Application Security Issues Based on the Cloud Computing Mode

Fang Bingyi¹, Zhang Yunyong¹, Wu Jun², Xu Lei¹

(1. China Unicom Research Institute, Beijing 100048, China;

2. Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: According to the safety objectives and the hierarchy of the cloud computing model of mobile internet, the security system was built and the key security problems were analyzed based on analysis of the existing security technologies in the network system.

Key words: cloud computing, mobile internet, security

1 引言

移动互联网是传统互联网与移动通信网络融合的产物, 越来越多的人正在或将会使用移动终端访问互联网。与传统互联网相比, 移动互联网具有随身性、可鉴权、可身份识别等独特优势, 但同时也存在移动终端处理能力弱、网络带宽相对较小的局限性。发展移动互联网, 绝不是简单的互联网移动化, 也不是简单的移动业务互联网化, 即简单地以互联网的模式运营移动业务。发展移动互联网, 要融合传统互联网上的优秀模式, 并结合移动互联网的特点, 寻找适合的业务模式和商业模式。

云计算是互联网领域的一个新热点, 已经受到各大

IT企业的关注。云计算将计算过程从用户终端集中到“云端”, 作为应用通过互联网提供给用户, 计算过程通过分布式计算等技术由多台计算机共同完成, 多台计算机组成的集合即所谓的“云”。用户只关心应用的功能, 而不关心应用的实现方式, 应用的实现和维护只由其提供商完成, 用户根据自己的需要选择相应的应用。云计算具有规模经济性, 应用通过互联网提供给多个外部客户, 多个客户共享同一个应用, 进而实现了计算在客户间的共享, 提高了处理器和存储设备的利用率, 也避免了用户对信息系统的重复建设。云计算不仅仅是一个工具、平台、网站或者架构, 更是一种计算的方式和创新性商业模式。

结合移动互联网和云计算的特点, 可以看出, 云计算

^{*} 国家自然科学基金资助项目(No.71172134), “新一代宽带无线移动通信网”国家科技重大专项基金资助项目(No.2012ZX03002001-002, No.2013ZX03002004-002, No.2013ZX03002003-005)



是适合移动互联网应用的一种模式。首先,云计算将应用的“计算”从终端转移到服务器端,从而弱化了对移动终端设备的处理需求。这样,移动终端主要承担与用户交互的功能,复杂的运算交由云端(服务器端)处理,终端不需要强大的运算能力即可响应用户操作,并将结果展现给用户,从而实现丰富的应用。其次,云计算降低了对网络的要求。比如,用户需要查看某个文件时,不需要将整个文件传送给用户,而只需发送用户需要查看的部分内容。最后由于终端不感知应用的具体实现,扩展应用变得更加容易,应用在强大的服务器端实现和部署,并以统一的方式(如通过浏览器)在终端实现与用户的交互。因此,云计算的大规模运算与存储资源集中共享的模式,给移动互联网的总体架构带来重大影响,使得移动互联网体系发生变化。

同时,云计算及其服务的安全,尤其是云计算的虚拟化、多租户和动态性等,为移动互联网引入了一系列新的安全问题,主要表现在数据安全、隐私保护、内容安全、运行环境安全、风险评估和安全监管等多个方面。围绕云计算应用模式下的移动互联网安全问题及关键安全技术展开研究,对完善移动互联网安全技术体系,保障移动互联网演进安全具有重要的意义。

2 移动互联网应用架构下云计算安全风险与安全体系

引入云计算的移动互联网应用架构发生极大改变,可将其分为“端”、“管”、“云”3个层面,如图1所示。“端”指的是用户接入“云”的移动终端设备,可以是笔记本电脑、PDA或手机等能够完成信息交互的终端;“管”指的是信息传输的网络通道,主要指电信运营商提供的通信网络;“云”指的是提供ICT资源或信息服务的基础设施中心、平台和应用服务器等,提供的服务类型包括基础设施、平台和应用等。云服务模式包含了3个层面:基础设施层面(IaaS),如各种服务器、数据库、存储设备、并行分布式计算系统等;平台层面(PaaS),由运营、支撑和开发3个平台组成;应用层面(SaaS),提供软件、数据和信息等各种应用。

通过对云计算应用模式下的移动互联网总体架构的分析以及对移动互联网安全风险问题的系统性研究,能够更准确地定义云计算应用模式下的移动互联网总体安全架构,如图2所示。根据在网络结构中部署位置的不同,可以将该总体安全架构分为3个部分:移动终端安全机制、网络安全机制和云端安全机制。

移动终端是指移动互联网的最终用户设备,包括手机、PDA、便携式电脑等;网络部分既包括接入网,也包括IP承载网或互联网。这两部分的安全风险都可以从物理安全、系统安全、应用安全和数据安全等方面进行分析。例如,移动终端安全机制包括硬件设备安全标准、CCC/SRRC/通信入网认证等,终端操作系统安全机制、防病毒、系统漏洞攻击等,数据安全及隐私保护机制、数据授权访问、加密等;网络安全机制包括网络设备的环境安全,操作系统、数据库等的访问控制及入侵防御机制,用户认证及数据加密机制A3/A8/ASE、Kasumi等。

云计算的引入给移动互联网带来的新的安全风险主要体现在云服务端。新的计算模式带来了传统业务模式的改造和新型业务服务的创新,在数据管理、应用部署、运行环境、服务模式等方面都引入了新的安全风险。因此,基于云端的安全机制,从数据保护、用户隐私、内容安全、运行环境安全、风险评估和安全监管等核心安全问题入手,构建移动互联网应用架构下的云计算安全技术体系框架,其框架如图3所示。

移动互联网应用架构下的云计算安全技术体系框架主要包括5大组成部分:数据安全和隐私保护、虚拟化运行环境安全、差异化移动云安全接入、基于SLA的动态云安全服务、风险评估及监管体系。其中,数据安全和隐私保护的方案贯穿安全技术体系的不同层次,而数据的所有权和管理权的分离正是云计算模式下最大的安全问题;虚拟化运行环境安全、差异化移动云安全接入、基于SLA的动态云安全服务分别是不同层次的安全问题研究点;风险评估及监管体系能够对来自不同层次的安全风险做出全面评估,并对其安全现状进行监控管理,反过来也能够促进安全技术体系的完善,从而形成整个安全体系的良性循环。

3 关键安全问题

云计算与移动互联网的结合,不仅仍要面临传统互联网技术以及移动通信网技术的双重安全风险威胁,而且将云计算中的安全风险引入移动互联网架构中。云计算及其服务的安全,尤其是云计算的虚拟化、多租户和动态性等为移动互联网引入了一系列新的安全问题,带来了一系列挑战,表现在数据安全、隐私保护、内容安全、运行环境安全、风险评估和安全监管等多个方面。

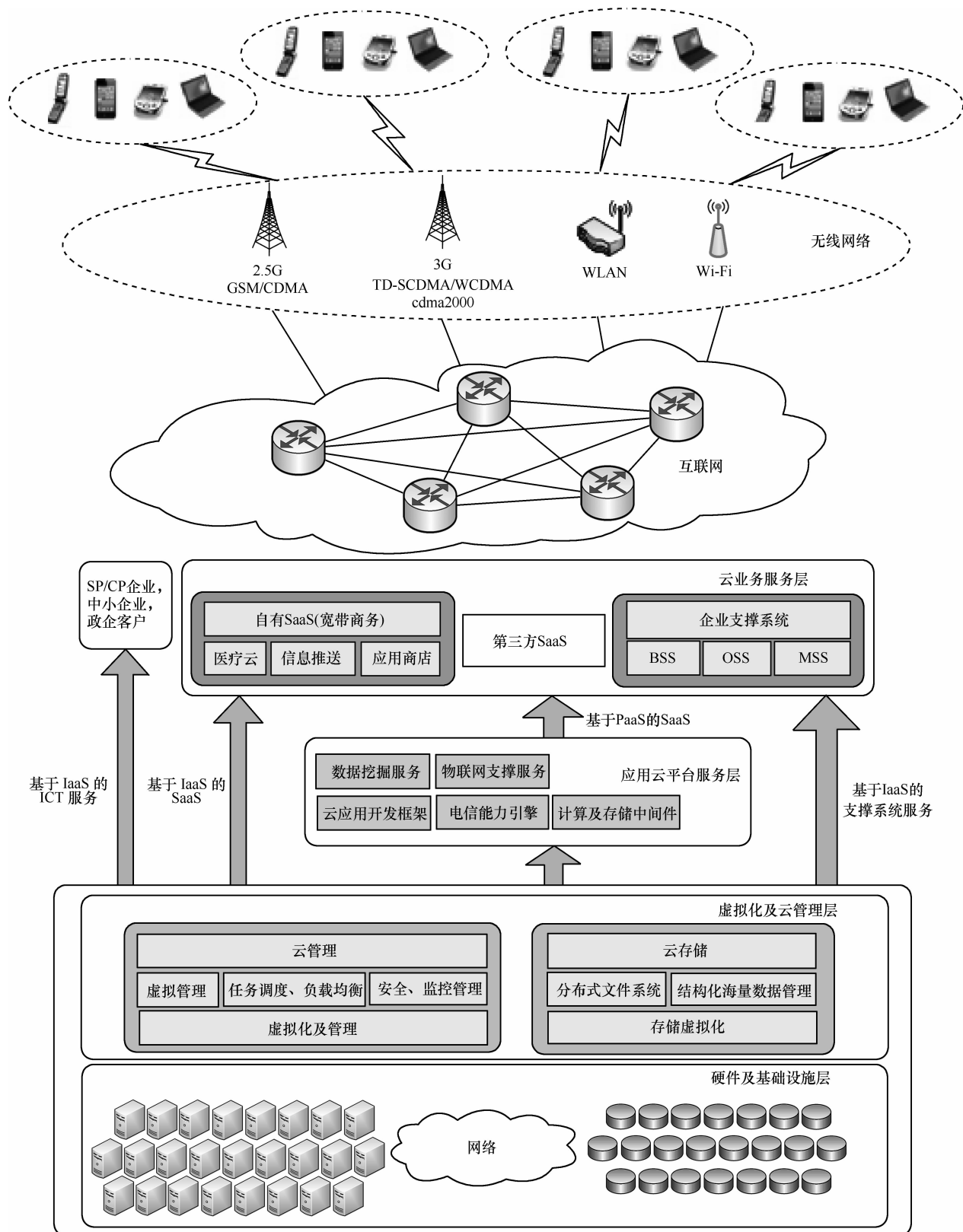


图 1 云计算应用模式下的移动互联网总体架构

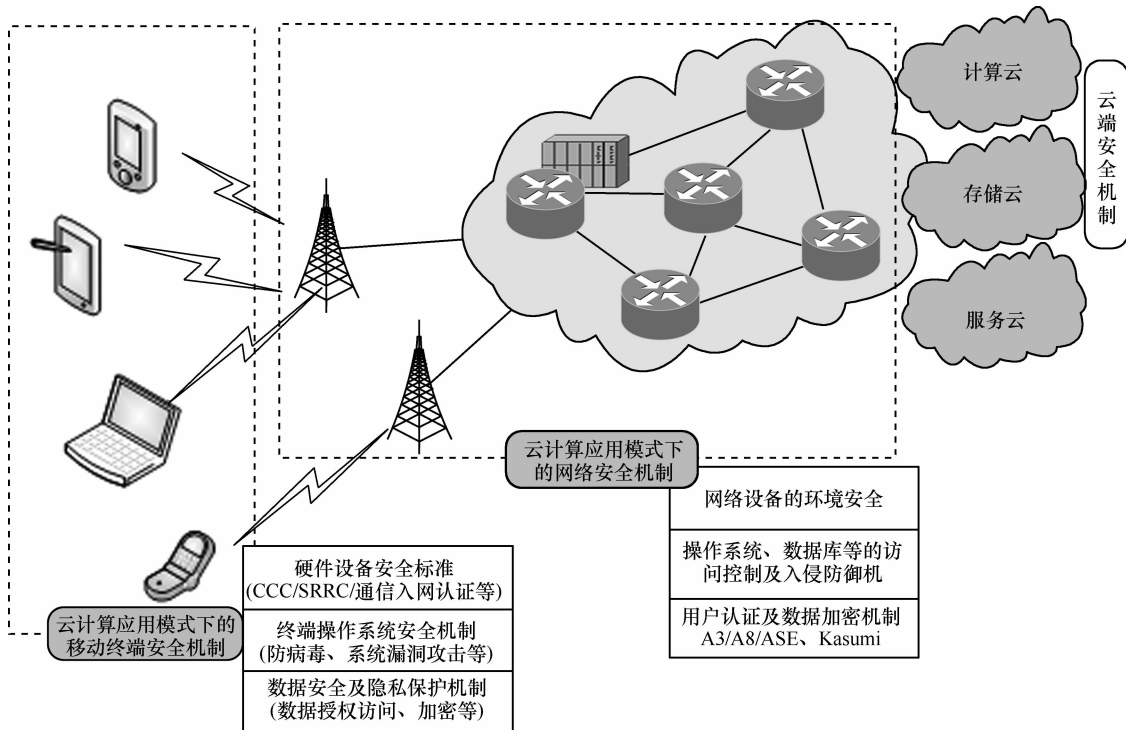


图2 云计算应用模式下的移动互联网总体安全架构

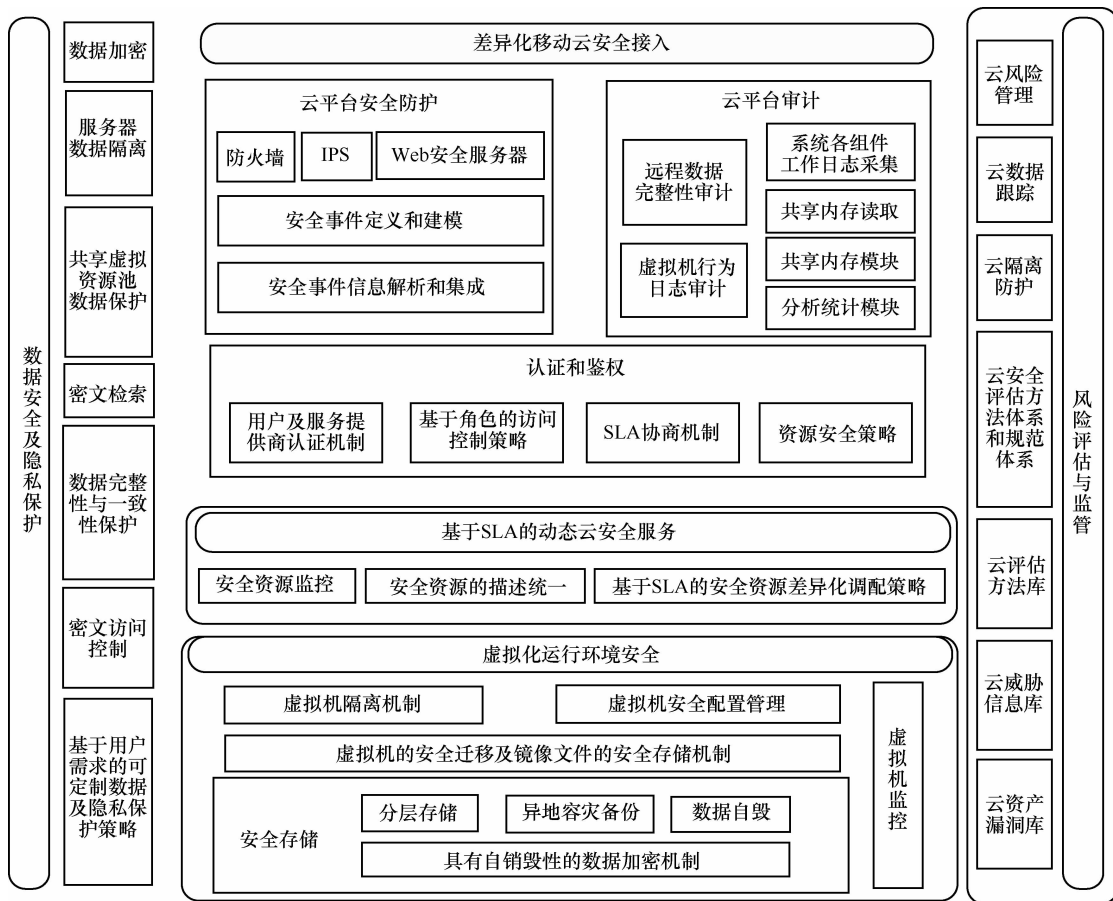


图3 移动互联网应用架构下的云计算安全技术体系框架

3.1 数据管理方式引发的安全问题

一方面,由于云计算模式下数据资产的所有权和管理权可能分离,客户将通过移动互联网对数据资产进行访问和使用,客户对数据资产安全的担忧成为重要的安全障碍。当用户或企业将所属的数据外包给云计算服务商或委托其运行所属的应用时,云计算服务商就获得了该数据或应用的优先访问权。事实证明,由于存在内部人员失职、黑客攻击及系统故障导致安全机制失效等多种风险,云服务商没有充足的证据让用户确信其数据被正确地使用。例如,用户数据没有被盗卖给其竞争对手;用户使用习惯、隐私没有被记录或分析;用户数据被正确存储在其指定的国家或区域,且不需要的数据已被彻底删除等。

另一方面,移动终端与用户的高黏合度导致数据的敏感度更高,信息泄露的危害更大。其永远在线(always-on)的特性会招致更多的窃听和监视问题,其“个性化”容易引发涉及隐私/金融等的恶意代码攻击;较PC用户,移动互联网用户缺乏安全意识,且其病毒传播途径多样化,如短信、彩信、互联网、蓝牙、存储卡等;较PC而言,移动终端对用户的重要性增加,已经如身份证一样不可或缺,因此使得攻击价值增大,危险度和严重性增加。固定互联网的业务复制是目前移动互联网业务发展的特点,而融合“移动”特征的业务创新则是移动互联网业务发展的方向,这类新业务中包含位置信息等隐私数据,不应被云服务提供商随意获取而用于挖掘分析谋取商业利益。

与固定互联网相比,移动互联网的恶意信息传播方式多样化,具有即时性、群组的精确性。移动互联网传播方式可以分为4种:通过短信/彩信进行群组消息传送;通过MMSC/SMSC服务器在SNS、BBS及微博客等进行信息发布,在指定的群组中进行消息散布;通过即时消息,Push Mail等交流沟通类业务在特定的群组中进行传播。引入云计算后,移动互联网的数据内容安全更加复杂化,而云计算的虚拟化、多租户和动态性等特点,使得恶意信息的传播途径和内容的监控管理难度更大。

3.2 虚拟化运行引发的安全问题

在典型的云计算服务平台中,资源以虚拟、租用的模式提供给用户,这些虚拟资源根据实际运行所需与物理资源绑定。由于在云计算中是多租户共享资源,因此,多个虚拟资源很多情况下会被绑定到相同的物理资源上。若云平台中的虚拟化软件中存在安全漏洞,则用户的数据就会被其他用户访问。例如,2009年5月,网络上曾经曝光

VMware虚拟化软件的Mac版本中存在一个严重的安全漏洞,黑客利用该漏洞通过Windows虚拟机在Mac主机上执行恶意代码。特别是,如果主机受到破坏,那么主机所管理的客户端服务器就有可能被攻克;如果虚拟网络受到破坏,那么客户端也会受到损害;如果主机有问题,那么所有的虚拟机都会产生问题。因此,如果云计算平台无法实现用户数据与其他企业用户数据的有效隔离,用户不知道自己的邻居是谁、有何企图,那么云服务商就无法说服用户相信自己的数据是安全的。

存储虚拟化是实现云存储的基本技术,通过将存储系统/子系统的内部功能从应用程序、计算服务器、网络资源中进行抽象、隐藏或隔离,实现其独立于应用程序、网络的存储与数据管理。存储虚拟化技术将底层存储设备进行抽象化统一管理,向服务器层屏蔽存储设备硬件的特殊性,而只保留其统一的逻辑特性,从而实现了存储系统集中、统一、方便的管理。采用虚拟化存储,磁盘利用率高达70%~90%,而且可以很好地进行负载均衡,把每一次数据访问所需的带宽合理地分配到各个存储模块上,提高了系统的整体访问带宽,改变了过度配置、冗余过多等问题。然而,PaaS和SaaS应用为了实现可扩展、可用性、管理以及运行效率等方面的“经济性”,基本都采用多租户模式,因此,被云计算应用所用的数据会和其他用户的数据混合存储(如Google的BigTable)。虽然云计算应用在设计之初已采用诸如“数据标记”等技术以防非法访问混合数据,但是通过应用程序的漏洞,非法访问还是会发生。在云计算环境中,数据残留更有可能无意泄露敏感信息,因此,云服务提供商应向云用户保证其鉴别信息所在的存储空间被释放或再分配给其他云用户前能够完全得到清除,无论这些信息是存放在硬盘上还是内存中。

3.3 服务模式引发的安全问题

云计算发展的趋势之一是IT服务专业化,即云服务商在对外提供服务的同时,自身也需要购买其他云服务商所提供的服务。因而用户所享用的云服务间接涉及多个服务提供商,多层转包极大地提高了问题的复杂性,进一步增加了安全风险。在提供云计算服务时要考虑到不同企业、不同应用的差异化安全需求,根据用户需求,结合移动互联网应用架构,提供动态差异化的云安全服务,为不同用户提供不同等级的安全保护服务。

3.4 风险评估方面的挑战

建立安全指导标准及其测评技术体系是实现移动互



联网云计算安全的另一个重要支柱。云计算安全标准是度量云用户安全目标与云服务商安全服务能力的尺度,也是安全服务提供商构建安全服务的重要参考。基于标准的“安全服务品质协议”,可以依据科学的测评方法检测与评估,在出现安全事故时快速实现责任认定,避免产生责任时互相推诿。建立云计算安全标准及其测评体系的挑战在于以下3点。

(1) 云计算安全标准应支持更广义的安全目标

云计算安全标准不仅应支持用户描述其数据安全保护目标,指定其所属资产安全保护的范围和程度;而且应支持用户,尤其是企业用户的安全管理需求,如分析查看日志信息、搜集信息、了解数据使用情况以及展开违法操作调查等。而这些信息的搜集可能会牵涉云计算服务商的数据中心或涉及其他用户的数据,带来一定安全隐患。云计算商业运作模式仍不是十分成熟,用户与云计算服务商之间的责任与权限界定得并不清晰,所以在管理范围与权限上可能存在冲突,因此,需要以标准形式将其确定下来,明确指出信息搜集的程度、范围、手段等,防止影响其他用户的权益。不仅如此,上述安全目标还应是可测量、可验证的,便于在相关规范中规定上述安全目标的标准化测量验证方法。

(2) 云计算安全标准应支持对灵活、复杂的云服务过程的安全评估

传统意义上对服务商能力的安全风险评估方式是,通过全面识别和分析系统架构下的威胁和弱点及其对资产的潜在影响,确定其抵抗安全风险的能力和水平,但在云计算环境下,云服务提供商可能租用其他服务商提供的基础设施服务或购买多个服务商的软件服务,根据系统状况动态选用。因此,标准应针对云计算中动态性与多方参与的特点,提供相应的云服务安全能力的计算和评估方法;同时,应支持云服务的安全水平等级化,便于用户直观理解与选择。

(3) 云计算安全标准应规定云服务安全目标验证的方法和程序

由于用户自身缺乏举证能力,因此,验证的核心是服务商提供正确执行的证据,如可信审计记录等。云计算安全标准应明确定义证据提取方法以及证据交付方法。

3.5 安全监管方面的挑战

云计算在带来巨大好处的同时,也带来了巨大的破坏性。而网络空间又是继领土权、领空权、领海权、太空权之

后的第五维国家主权,是任何主权国家必须自主掌控的重要资源。因此,应在发展云计算产业的同时大力发展云计算监控技术体系,牢牢掌握技术主动权,防止其被竞争对手控制与利用。与互联网监控管理体系相比,实现云计算监控管理必须解决以下3个问题。

(1) 实现基于云计算的安全攻击的快速识别、预警与防护

如果黑客攻入了云客户的主机,使其成为向云服务提供商发动DDoS攻击的工具,那么如果按照云计算对计算资源的付费方式,即根据实际使用进行付费,受控客户将在不知情的情况下为黑客发起的资源连线支付巨额费用。不仅如此,与以往DDoS攻击相比,基于云的攻击更容易组织,破坏性更大。而一旦攻击的对象是大型云服务提供商,势必影响大批用户,所造成的损失就更加难以估量。因此,需要及时识别与阻断这类攻击,防止重大的灾害性安全事件的发生。

(2) 实现云计算内容监控

云的高度动态性增加了网络内容监管的难度。首先,云计算所具有的动态性特征使得建立或关闭一个网站服务较以往更加容易,成本代价更低,因此,各种含有黄色内容或反动内容的网站将很容易以“打游击”的模式在网络上迁移,使得追踪管理难度加大,对内容的监管更加困难,内容监管时可能会涉及其他用户的隐私问题。其次,云服务提供商往往具有国际性的特点,数据存储平台也常跨越国界,将网络数据存储到云上可能会超出本地政府的监管范围或同属多地区、多国的管辖范围,而这些不同地域的监管法律和规则之间很有可能存在着严重的冲突,当出现安全问题时,难以给出公允的裁决。

(3) 识别并防止基于云计算的密码类犯罪活动

云计算的出现使得组织实施密码破译更加容易,原来只有资金雄厚的大型组织才能实施的密码破解任务,在云计算平台的支持下,普通用户也可以轻松实现,严重威胁了各类密码产品的安全。在云计算环境下,如何防止单个用户或者多个合谋用户购得足够规模的计算能力来破解安全算法,也是云计算安全监管中有待解决的问题之一。

4 结束语

在通过分析上述云计算模式下移动互联网面临的安

全威胁的基础上,建立云计算模式下移动互联网的安全保护体系和体系架构,研究多层次的云计算模式下移动互联网安全保障方法,提出相关安全技术标准与测评体系,解决移动终端安全、客户数据安全和隐私保护、虚拟化运行环境安全和风险评估及安全监管等问题,增强了云计算模式下移动互联网的机密性、完整性、可验证性和可用性,为基于云计算模式下的移动互联网业务发展提供了参考。

参考文献

- 1 中国通信标准化协会. 移动环境下云安全技术研究, 2012
- 2 张云勇, 陈清金, 潘松柏等. 云计算安全关键技术. 电信科学, 2010(8)

[作者简介]



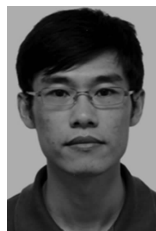
房秉毅,男,博士,中国联通集团研究院高级工程师,主要研究方向为云计算、核心网新技术,已发表论文 20 余篇。



张云勇,男,博士后,中国联通集团研究院平台与云计算研究中心主任、高级工程师,中国通信学会、电子学会、计算机学会高级会员,中国人工智能学会会员,主要研究方向为下一代开放网络、固定移动融合核心网、移动互联网及业务、公共运算,已出版中文论著 14 部、英文论著 1 部,已发表论文 58 篇。



吴俊,男,博士,北京邮电大学副教授,主要研究方向为移动互联网应用、云计算商业价值评价等。



徐雷,男,博士,中国联通集团研究院高级工程师,主要研究方向为云计算、移动互联网新技术。

(收稿日期:2013-02-20)

(上接第 40 页)

[作者简介]



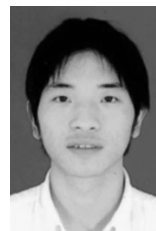
陈娜,女,硕士,中国电信股份有限公司广东研究院高级工程师,主要从事电信 IT 支撑系统的相关研究工作。



宋红兵,女,硕士,中国电信集团公司工程师,长期从事中国电信业务支撑运营管理和研究工作。



徐歆壹,男,学士,现就职于中国电信股份有限公司广东研究院,主要从事 BSS 领域的研究工作。



何毅,男,硕士,亚信联创集团股份有限公司工程师,主要从事电信 IT 支撑系统的设计和开发工作。

(收稿日期:2013-03-05)