



浅谈云计算的网络安全威胁与应对策略

姚 平,李 洪

(中国电信集团公司网络运行维护事业部 北京 100032)

摘 要:介绍了云计算的概念和类型。云计算是一个给用户提提供虚拟化资源的新概念,用户可以从云平台中获取各类服务、应用程序和解决方案,云平台能将大量的数据信息存储在云上的不同位置。随着云计算的不断普及,日益增长的安全风险已经成为一个大家讨论的热点话题。针对云计算的类型和网络安全威胁问题进行了细致讨论,提出了一些解决云计算中网络安全问题的应对策略方案。

关键词:云计算;网络问题;安全问题;应对策略

doi: 10.3969/j.issn.1000-0801.2013.08.015

Network Security Threats and Countermeasures on Cloud Computing

Yao Ping, Li Hong

(Network Operation & Maintenance Division, China Telecom Corporation, Beijing 100032, China)

Abstract: Cloud computing is a new concept of providing virtualized resources to the consumers. Consumers can request a cloud for services, applications, solution and can store large amount of data in different locations. But with the growing popularity of cloud computing, the increasing risk of security is becoming a main and top issue. The type of cloud computing and the network security issues were discussed. A backup plan required for overcoming the network security issues in cloud computing was proposed.

Keywords: cloud computing, network issue, security issue, countermeasure

1 引言

2007年10月,Google和IBM在美国大学校园开始尝试推广云计算计划,学生可以透过网络开发各项以大规模计算为基础的研究计划;随后,更多的IT巨头也开始往这方面发展。从此,云计算技术开始取代其他计算机技术成为IT业界的流行术语。所谓云计算,指的是一种模式,一个利用互联网和远程服务器来维护数据和应用程序的新概念。通过互联网,云计算能提供动态的虚拟化资源、带宽资源和定制软件给用户,并承诺在应用中为用户产生可观的经济效益。云计算可以帮助用户减少对硬件资源、软件

许可及系统维护的投入成本;通过互联网,用户可以方便地使用云平台上的各类应用服务。此外,通过云计算用户可以节约投资成本并可灵活地实现按需定制服务,云平台的按需定制服务可以快速地响应用户需求,并方便地将用户资源接入宽带网络。

本文针对云计算的类型和网络安全威胁问题进行了细致探讨。在网络风险方面,云计算主要面临着以下的威胁攻击:拒绝服务攻击、中间人攻击、网络嗅探、端口扫描、SQL注入和跨站脚本攻击;在安全风险方面,云计算面临的威胁主要是:XML签名包装、浏览器安全性、云恶意软件注入、洪流攻击、数据保护、数据删除不彻底和技术锁定。

2 云计算的相关概念

许多公司/机构经常需要对海量数据进行存储和检索,而云计算可以有效地以最小的成本、最短的时间和最大的灵活性来实施完成该项任务。利用云计算获取便利的同时,用户也要面临云计算中各种不同的安全风险问题,如必须要将云平台上不同用户的数据相隔离,要保证不同云用户数据的私密性、可靠性和完整性。此外,云服务提供商对云上的基础服务设施必须制定一套完善的风险管理控制方案,像服务提供商操纵或窃取程序代码的安全风险是时有出现的。

经常使用的互联网,通常也可以被看作一朵巨大的云。通过互联网,云计算被看作一个应用和服务呈现给用户。它的出现迅速将旧的计算机技术整合,然后转变为一项新技术。目前互联网提供了不同的服务给不同的用户群体,提供这些服务并不需要什么特殊的设备或软件。因此,云计算最起码包含几个特性:“云是一个大型资源池,可以轻松获取虚拟化资源(如硬件、开发平台或服务)。这些资源可以动态地重新配置和灵活整合,达到一个最佳的资源利用率。云服务提供商通过定制服务水平协议,提供基础设施服务并按付费的模式来管理维护这种资源池。”

云计算不是一个单一产品,它提供了不同的服务模式,主要包括以下 3 种:软件即服务(SaaS)、平台即服务(PaaS)和基础设施即服务(IaaS)。

SaaS 是一种通过互联网来提供软件的服务模式,用户无需购买软件,而是向云服务提供商租用基于 Web 的软件来管理企业经营活动。

PaaS 是把计算环境、开发环境等平台作为一种服务提供的商业模式。云计算服务提供商可以将操作系统、应

用开发环境等平台级产品通过 Web 以服务的方式提供给用户。通过 PaaS,软件开发人员可以在不购买服务器的情况下开发新的应用程序。

IaaS 是把数据中心、基础设施硬件资源(如存储、硬件、服务器、网络)通过 Web 分配给用户使用的商业模式。这些资源由云服务提供商进行操作、维护和管理。

根据美国国家标准技术研究院(NIST)的定义,云计算有 4 种部署模式,分别是:公共云、私有云、混合云和社区云,如图 1 所示。

公共云:它面向大众提供资源、Web 应用和其他服务等,任何用户都可以通过互联网从云服务商处获取这些服务。公共云上的基础设施由公用的企业机构进行建设及管理。

私有云:这种云基础设施专门为一个企业服务,该企业内的任何用户都可以从云设施处获取数据、服务和 Web 应用,但企业外部的用户则不能访问云。私有云上的基础设施完全由企业自身管理,并维护公共数据。

混合云:混合云是两种或两种以上的云计算模式的综合体,如公有云和私有云混合。它们相互独立,但在云的内部又相互结合,可以发挥出所混合的多种云计算模型各自的优势。

社区云:这种模式是建立在一个特定的小组里多个目标相似的公司之间的,其共享一套基础设施,所产生的成本共同承担。因此,其所能实现的成本节约效果也并不很明显。社区云的成员都可以登入云中获取信息和使用应用程序。

3 云计算的网络问题

云计算环境中存在着多种网络安全威胁问题,现将其

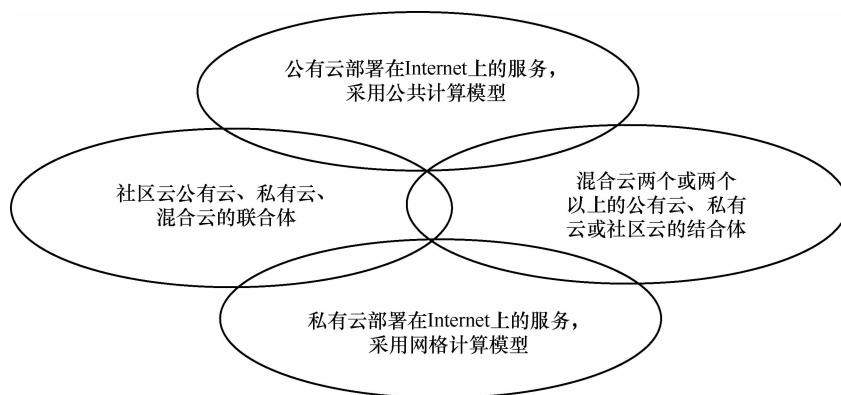


图 1 云计算的类型



中一些主要的网络问题进行探讨分析。

3.1 拒绝服务攻击

拒绝服务攻击指攻击者想办法让目标服务器停止提供服务甚至主机死机。如攻击者频繁地向服务器发起访问请求,造成网络带宽的消耗或者应用服务器的缓冲区满溢;该攻击使得服务器无法接收新的服务请求,其中包括了合法客户端的访问请求。例如,一个黑客劫持了 Web 服务器,使其应用服务停止运行,导致服务器不能提供 Web 服务。在云计算中,黑客对服务器开展拒绝服务攻击时,会发起成千上万次的访问请求到服务器,导致服务器无法正常工作,无法响应客户端的合法访问请求。针对这种攻击,可以采用的应对策略是减少连接到服务器的用户的权限,这将有助于降低拒绝服务攻击的影响。

3.2 中间人攻击

中间人攻击是另一种网络攻击手段。攻击者通过拦截正常的网络通信数据,并进行数据篡改和嗅探,而通信的双方却毫不知情。在网络通信中,如果安全套接字层(SSL)没有正确配置,那么这个风险问题就有可能发生。例如,如果通信双方正在进行信息交互,而 SSL 没有正确地安装,那么所有双方之间的数据通信,都有可能被黑客侵入获取。针对这种攻击手段,可以采用的应对措施是正确地安装配置 SSL,而且使用通信前应由第三方权威机构对 SSL 的安装配置进行检查确认。

3.3 网络嗅探

网络嗅探原先是网络管理员用来查找网络漏洞和检测网络性能的一种工具,但是到了黑客手中,它变成了一种网络攻击手段,造成了一个更为严峻的网络安全问题。例如,在通信过程中,由于数据密码设置过于简单或未设置,导致被黑客破解,那么未加密的数据便被黑客通过网络攻击获取。如果通信双方没有使用加密技术来保护数据安全性,那么攻击者作为第三方便可以在通信双方的数据传输过程中窃取到数据信息。针对这种攻击手段,可以采用的应对策略是通信各方使用加密技术及方法,确保数据在传输过程中安全。

3.4 端口扫描

端口扫描也是一种常见的网络攻击方法,攻击者通过向目标服务器发送一组端口扫描消息,并从返回的消息结果中探寻攻击的弱点。应用服务器总是开放各类端口应用,例如 80 端口(HTTP)是为了给用户提供 Web 应用服务,再如 21 端口(FTP)是为了给用户提供 FTP 应用服务

的。这些端口总是一直处于打开状态,应该在需要的时候打开,并且应该对端口进行加密。针对此类攻击,可以启用防火墙来保护数据信息免遭端口攻击。

3.5 SQL 注入攻击

SQL 注入是一种安全漏洞,利用这个安全漏洞,攻击者可以向网络表格输入框中添加 SQL 代码以获得访问权。在这种攻击中,攻击者可以操纵基于 Web 界面的网站,迫使数据库执行不良 SQL 代码,获取用户数据信息。针对这种攻击,应定期使用安全扫描工具对服务器的 Web 应用进行渗透扫描,这样可以提前发现服务器上的 SQL 注入漏洞,并进行加固处理;另外,针对数据库 SQL 注入攻击,应尽量避免使用单引号标识,同时限制那些执行 Web 应用程序代码的账户权限,减少或消除调试信息。

3.6 跨站脚本攻击

跨站脚本攻击指攻击者利用网站漏洞恶意盗取用户信息。用户在浏览网站内容时,一般会点击网站中的链接,攻击者在链接中植入恶意代码,用户点击该链接就会执行该恶意代码,将用户重定向到一个攻击者定制好的页面中,并盗取用户 cookie 等敏感数据。跨站点脚本攻击可以提供缓冲溢出、DoS 攻击和恶意软件植入 Web 浏览器等方式来盗取用户信息。对付此类攻击,最主要的应对策略是编写安全的代码,避免恶意数据被浏览器解析;另外,可以在客户端进行防御,如把安全级别设高,只允许信任的站点运行脚本、Java、flash 等小程序。

跨站脚本攻击示意如图 2 所示。

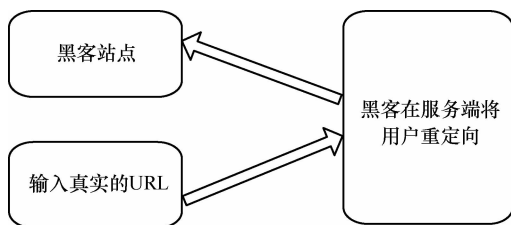


图 2 跨站脚本攻击示意

4 云计算的安全问题

根据调查统计,云计算主要面临以下 7 种安全问题,下面逐一进行探讨分析。

4.1 XML 签名包装

XML 签名包装是常见的 Web 服务攻击漏洞,XML 签名元素包装原本是用于防止组件名、属性和值的非法访问,但它无法隐蔽自己在公文中的位置。攻击者通过 SOAP

(simple object access protocol,简单对象访问协议)消息携带内容攻击组件。对付此类攻击的策略是使用类似证书颁发机构这样的第三方授权的数字证书(如 X.509)和 WS-Security 的 XML 签名组件。具备组件列表的 XML 就可以拒绝有恶意文件的消息以及客户端的非法消息。

4.2 浏览器安全性

当用户通过 Web 浏览器向服务器发送请求时,浏览器必须使用 SSL 来加密授权以认证用户,SSL 支持点对点通信,这就意味着如果有第三方,中介主机就可以对数据解密。如果黑客在中介主机上安装窥探包,就可能获取用户的认证信息并且使用这些认证信息在云系统中成为一个合法的用户。应对这类攻击的策略是卖方在 Web 浏览器上使用 WS-security 策略。因为 WS-security 工作在消息层,可使用 XML 的加密策略对 SOAP 消息进行连续加密,而且并不需要在中间传递的主机上进行解密。

4.3 云恶意软件注入攻击

云恶意软件注入攻击试图破坏一个恶意的服务、应用程序或虚拟机。闯入者恶意地强行生成个人对应用程序、服务或虚拟机的请求,并把它放到云架构中。一旦这样的恶意软件进入了云架构里,攻击者对这些恶意软件的关注就成为合法的需求。如果用户成功地向恶意服务发出申请,那么恶意软件就可以执行。攻击者向云架构上传病毒程序,一旦云架构将这些程序视为合法的服务,病毒就得以执行,进而破坏云架构安全。在这种情况下,硬件的破坏和攻击的主要目标是用户。一旦用户对恶意程序发送请求,云平台将通过互联网向客户传送病毒。客户端的机器将会感染病毒。攻击者一般使用散列函数存储请求文件的原始图像,并将其与所有即将到来的服务请求进行散列值比较,以此来建立一个合法的散列值与云平台进行对话或进入云平台。因此对付这种攻击的主要策略是检查收到消息的真实有效性。

4.4 洪流攻击

攻击者公开攻击云系统。云系统最显著的特征是能够提供强大的、可扩展的资源。当有更多的客户请求时,云系统就会持续增加其规模,云系统会初始化新的服务以满足客户的需求。洪流攻击主要是向中央服务器发送数量巨大的无意义的服务请求。一旦攻击者发送大量的请求,云系统将会认为有过多的资源请求而暂时拒绝一些资源请求,最终系统将资源耗尽而不能对正常的请求提供服务。DoS 攻击导致客户使用资源产生额外的费用,在这种情况下,

服务的所有者还必须对此赔付额外的费用。应对这种攻击的策略不是简单地阻止 DoS 攻击,而是要停止服务的攻击。可以通过部署入侵检测系统来过滤恶意请求,并通过防火墙进行拦截。但是,有时入侵检测系统会提供假警报,可能会对管理员产生误导。

4.5 数据保护

云计算中的数据保护是一个非常重要的安全问题。由于用户数据保存在云端,云服务商管理人员有可能不小心泄露数据或者“监守自盗”,给用户造成较大损失。因此,需要有效地管控云服务提供商的操作行为。针对此类安全风险,需使用加密技术对用户数据进行加密处理,这样可以解决云端的数据隔离问题,即使用户数据外泄,也能保证其内容信息无法被查看。另外,可以考虑引入第三方的云安全审计系统,它可以详细记录各种数据操作行为记录,对云服务提供商也起到监督管理作用。

4.6 数据删除不彻底

数据删除不彻底问题在云计算中是有极大风险的,数据删除不彻底的主要原因是数据副本已经被放置在其他服务器上。例如,当云用户申请删除一个云资源时,由于该资源的存放位置可能涉及多个虚拟机系统,而部分虚拟机可能在当时不可用,所以用户数据无法彻底删除。针对该类安全问题,应该采用虚拟化的私有网络来应用于保护数据,并通过查询工具来确保用户数据已从主机和备机上完全删除。

4.7 技术锁定

技术锁定是云计算中一个令人担心的问题。在云计算领域,被技术锁定是有较大风险的,万一云服务提供商倒闭了,那么用户的基础设施也会跟着消失。为应对此风险,用户可以选择以应用程序为主(或至少要 VM-centric)的管理工具或服务,万一出现意外状况,可以把数据或应用程序带走,以备不时之需。

参考文献

- 1 沈昌祥.云计算安全.信息安全与通信保密,2010(12):12~15
- 2 党卫红.云计算的安全防护策略分析与研究.读与写杂志,2010(5):79
- 3 黄志宏,巫莉莉,张波.基于云计算的网络安全威胁及防范.重庆理工大学学报,2012(8):26
- 4 李虹,李昊.可信云安全的关键技术与实现.北京:人民邮电出版社,2010

(收稿日期:2013-08-05)