doi :10.3969/j.issn.1671-1122.2010.02.026

“云”计算环境的信息安全问题

蒋建春[1]，文伟平[2]
（1. 中国科学院软件研究所，北京 100190；
2. 北京大学 软件与微电子学院软件技术系，北京 102600）

摘 要：“云”计算是当前IT工业界、学术界的关注热点问题。本文首先简单介绍“云”计算的概念以及实现机制。然后分析“云”计算下的安全威胁以及表现方式，最后文章归纳了十个关于当前“云”计算信息安全问题。

关键词：云计算；安全风险；信息安全
中图分类号：TP393.08 **文献标识码：**A

1“云”计算概念

在传统计算模式下，当用户完成一个计算任务时候，需要用户自己做大量繁杂的工作，例如安装所需要的计算软件包，设置软件配置，甚至编写复杂的软件。随着互联网技术发展，人们实际上希望一种简捷计算环境，就如同通过自来水管获取水、通过电线获取电源、通过银行来储蓄。“云”计算就是在这样的需求驱动下而产生的一种计算模式。所谓“云”计算就是一种计算平台或者应用模式，在“云”中，集聚大量服务器或应用软件，或者存储设备，用户通过访问这些“云”，就可以方便获取自己所需要的服务，如数据访问、特定计算服务[1-4]。

2“云”计算实现机制

目前，实现“云”计算实现机制各不相同，本文在文献[2]基础上，对下面“云”计算实现方式分别进行分析。

2.1 基于软件即服务（SaaS）“云”计算

在“云”计算下，传统软件形式将逐渐发生新的变化，软件变成一种服务形式，即软件即服务(SaaS)，特别是应用软件的形式打包装成虚拟应用(Virtual appliances)，通过这种形式用户可以无需要安装软件，就可以使用这种软件服务，就如同购买某种器具，购买就可使用。如图1所示，图中展示的是NC state大学的虚拟计算实验室VCL，用户无需安装自己应用软件，通过Internet就可以获取到所需要的软件服务。

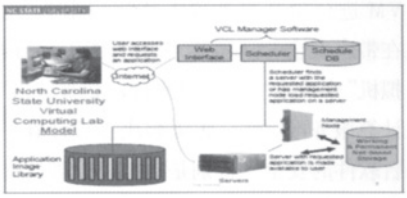

图1 美国NC State大学的VCL结构图

2.2 基于效用计算（Utility computing）“云”计算

效用计算的想法是提供一种服务，能够按需满足用户的计算要求。目前Amazon.com、Sun、IBM等公司按需提供存储和虚拟服务器访问服务。Amazong公司通过EC2计算云，可以让客户通过WEB Service方式租用计算机来运行自己的应用程序[11]。

2.3 基于WEB服务“云”计算

同SaaS类似，服务提供者利用Web服务，通过Internet给软件开发者提供API应用接口，而不是整个应用程序。当前，国外一些公司开始建立基于Web 服务的云服务，如Amazon公司、Strike Iron公司。如图2所示，Strike Iron公司提供一种Web服务，企业用户可以集成到自己的应用中。

2.4 基于平台服务（Platform as a service）“云”计算

与SaaS 不同的，这种“云”计算形式把开发环境或者运行平台也作为一种服务给用户提供。用户可以把自己的应用运行在提供者的基础设施中，例如Salesforce.com、Yahoo Pipes等公司提供这种形式的服务。

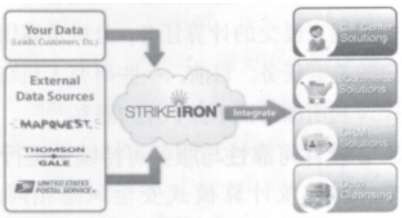

图2 Strike Iron的Web服务应用示意图

2.5 基于管理服务MSP (managed service providers) “云”计算

MSP管理服务就是通常所说的IT外包管理服务，服务者提供可以通过安全网络给用户提供MSP服务，例如桌面管理服务。

2.6 基于商业服务“云”计算

这种“云”计算服务混合SaaS 和MSP服务，这种服务实际上是通过设置一个服务中心，用户可以通过这个服务中心进行商业计算服务，同时也获取管理服务。

3“云”计算安全风险分析与信息安全问题

美国公司Gartner于2008年发布了一份关于“云”计算安全风险分析，其

中列举七项安全风险。其中，这些安全风险包括特权管理、数据位置、数据隔离、数据恢复、审计与法律调查、服务延续性等[12]。本节从技术安全的角度，分析“云”计算所带来安全风险，以及“云”计算对传统信息安全防御机制的影响。

3.1 系统软件安全与用户隐私保护

软件系统安全仍然是一个挑战性难题。在“云”计算环境下，如果所使用的商业操作系统不是安全操作系统，那么系统管理员拥有过高的权限，一旦这些权限失控，获得这些权限的人都可以访问用户的个人信息。因此，将会直接影响到用户的个人数据隐私。同时，与传统计算模式不同的是，“云”计算利用虚拟计算技术，用户个人数据可能分散在各个虚拟的数据中心，而不是在同一个物理位置，也许跨越国境，此时，数据隐私保护面临不同法律体系争议。另一方面，用户在使用云计算服务时候，有可能泄露用户隐藏信息。攻击者可以根据用户提交的计算任务，分析透露用户的关键任务。目前，一些研究人员在探讨利用加密技术保护用户隐私[7]。

3.2 软件可靠性与服务可持续性运行

同传统计算模式安全风险相同，“云”计算仍然需要解决服务可靠性问题，但不同的是，在“云”计算形式下，用户对服务提供者依赖性更高，“云”计算的服务由各种软件模块或者各种Web Services来集成实现，一旦软件安全事件出现将会产生巨大的影响。例如，云计算服务者系统软件漏洞被利用，造成攻击者可以进行拒绝服务攻击，用户将无法远程访问到“云”服务。

3.3 服务协议符合性与软件服务可信证明

在“云”计算下，有可能存在一些恶意的服务者，这些服务者所提供的服务内容不一定能够满足服务协议[5,6]。例如，如图3所示，数据拥有者Alice将数据库外包给Bob，但Bob不是恶意服务者，Bob只选择性执行Alice查询任务，或者说，给Alice查询服务结果不完整。

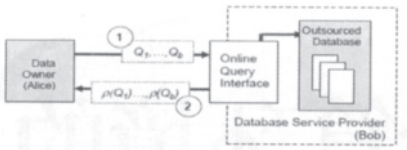

图3 数据库外包查询示意图

3.4 虚拟计算平台安全与“云”计算服务可信

“云”计算服务可信性依赖于计算平台的安全性。目前，服务者通过新型的虚拟计算(Virtual Computing)技术来实现“云”计算模式。在“云”计算下，服务者利用XEN、VMWare等技术，将一台高性能的物理机器运行多个虚拟机(VM)以满足用户的需求[8]，如图4所示。

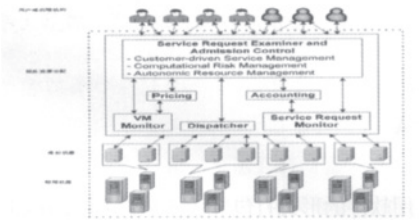

图4 基于VM的“云”计算结构示意图

例如，Amazon公司的EC2。这种计算组织形式，可以让不同虚拟机运行互不干扰，但是前提是虚拟机的管理控制软件Hypervisor是可信的，而且由于各虚拟机共享物理内存，用户的机密数据有可能通过内存泄漏，或者黑客利用VM进行拒绝服务攻击[9-10]。同时，潜在带来安全的问题是，黑客可能租用“虚拟机”来攻击“云”计算平台。 因此，“云”计算服务可信性，必须解决虚拟计算平台软件的安全，特别是虚拟机管理软件Hypervisor。

3.5 应用虚拟映像与软件安全管理

与传统的软件发布模式不同的是，在“云”计算环境下，软件开发商通过将应用软件预安装，同操作系统打包形成不同类型的虚拟机文件格式VA(virtual appliances)。用户即可以在Hypervisor支持下，自行运行VA，或者通过租用“云”计算服务提供者的计算机运行。虽然这种软件部署模式对终端用户简单，但是软件安全维护将会变得复杂，目前漏洞和补丁管理系统尚不支持对VA有效管理。通常VA文件比较大，用户使用传统杀毒方式，检测速度比较缓慢。同时，VA实际上是一台虚拟机，只是未运行，但是如何测试VA安全配置将是一个软件安全管理难题。

3.6 基于VM 恶意代码与病毒检测软件变革

随着各种应用VM Image文件发布而传播，恶意代码有可能伪装一个特殊的VM。当用户运行VM时候，就激活恶意代码VM，但是传统的计算机病毒检测软件无法监测到，因为恶意代码和现有杀毒软件不在同一台计算机[13]。给出一个利用VMM技术构造的恶意代码SubVirt，如图5所示。

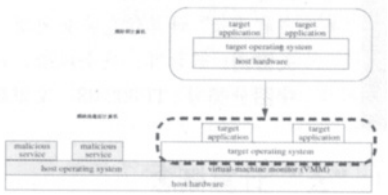

图5 SubVirt工作原理图

3.7 虚拟机与僵尸网络

僵尸网络控制者可能利用“云”计算资源，将僵尸代码以虚拟机形式传播，这些僵尸代码虚拟机运行在受害用户的计算机中，用户难以察觉。同时，僵尸网络控制者还可能利用租用的虚拟机隐藏自己的真实身份。

3.8 虚拟计算与网络内容安全

在“云”计算环境下，有害信息网站利用虚拟计算技术，将信息隐藏在虚拟机中，然后发布，这些基于虚拟机网站部署简单，可以随时动态运行，传统网络内容安全机制有可能无法察觉。

3.9 “云”计算与网络安全控制

黑客有可能利用“云”计算开放环境，匿名租用各种虚拟机，然后发起各种攻击。例如，黑客可以租用虚拟机，绕开网络安全机制(如防火墙)。

3.10 网络犯罪与计算机取证

在“云”计算环境下，网络犯罪人员利用租用的虚拟机以隐藏犯罪行为。当关闭虚拟机运行，虚拟机状态信息可能随着用户使用后消失，因此网络犯罪

在虚拟机上的证据就可能消失。因此，获取虚拟机犯罪证据成为新的难题。

4 结束语

本文首先简单介绍“云”计算的概念以及实现机制。在“云”计算环境下，传统安全威胁将会利用“云”计算资源，改变威胁途径，使得安全威胁更具有隐蔽性。同时，新的安全问题随之产生，如外包数据安全保护、软件服务可信证明、大规模虚拟映像文件安全管理。（责编 杨晨）

参考文献：

[1] Cloud computing. http://en.wikipedia.org/wiki/Cloud_computing.

[2] Galen Gruman. What is cloud computing? http://www.infoage.idg.com.au/index.php/id;909486215;fp;4;fpid;1051515815.

[3] Mladen Vouk, Sam Averitt etc. Powered by VCL – Using Virtual Computing Laboratory (VCL).Proc. 2nd International Conference on Virtual Computing (ICVCI), 15–16 May, 2008, RTP, NC, pp 1–10. May 16, 2008.

[4] Patrick DREHERa, Mladen A. VOUK, Eric SILLS, Sam AVERITT. Cost Effective Cloud Computing Using VCL. http://vcl.ncsu.edu/papers–publications.

[5] Radu Sion.Query Execution Assurance for Outsourced Databases. International Conference on Very Large Data Bases (VLDB), 2005.

[6] Min Xie, Haixun Wang, Jian Yin and Xiaofeng Meng. Integrity Auditing of Outsourced Data by, International Conference on Very Large Data Bases (VLDB), 2007.

[7] Balakrishna R. Iyer, Chen Li, Sharad Mehrotra . Executing SQL over encrypted data in the database–service–provider model by Hakan Hacigumus. ACM SIGMOD Conference on Management of Data, 2002.

[8] Rajkumar Buyya etc. Market–Oriented Cloud Computing:Vision, Hype, and Reality for Delivering IT Services as Computing Utilities.

[9] Tal Garfinkel etc.When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments.

[10] Jenni Susan Reuben. A Survey on Virtual Machine .http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdf.

[11] http://en.wikipedia.org/wiki/Amazon_Elastic_Compute_Cloud.

[12] J. Brodkin. “Gartner: Seven cloud–computing security risks” http://www.networkworld.com/news/2008/070208–cloud.html, 2008.

[13] Samuel T. King etc. SubVirt: Implementing malware with virtual machines” . http://www.eecs.umich.edu/~pmchen/papers/king06.pdf.

作者简介：蒋建春（1971–），男，副研究员，博士，主要研究方向：信息对抗理论、网络入侵检测、恶意代码分析、信息系统安全风险评估、安全操作系统与可信计算；文伟平 (1976–)，男，副教授，博士，主要研究方向：网络攻击与防范、恶意代码研究、信息系统逆向工程和可信计算技术等。

上接第 50 页

WebmailInfo，写入数据库的内容包括账号、IP 地址、MAC 地址、Webmail 登录时间，其中登录时间为向数据库写入信息时获取本机系统时间。

3 实验及结果

3.1 系统部署及实验方法

系统部署拓扑结构如图 5 所示：Webmail 监控系统安装在交换机的镜像端口上，采用的操作系统为 Linux 2.6，用两台安装了 Windows XP 的 PC 机模拟受控机。实验中，我们在在两台受控 PC 机上用 IE、遨游、搜狗浏览器使用不同类型的 Webmail，实验结果记录在数据库中。

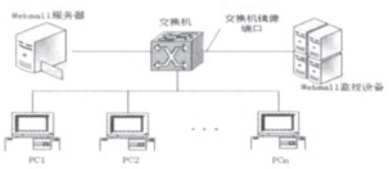

图5 Webmail监控系统框图

3.2 实验结果展示

运行监控系统，用几种常见的 Webmail 登录服务器和发送邮件，Oracle 数据库中记录如表 2、表 3 所示：

表 2 记录了监控网络中 Webmail 登录的账号、登录时间、登录者 IP 及 MAC 信息；表 3 中记录了监控网络中 Webmail 发件人账号、收件人账号、发送时间、发件人 IP 及 MAC 信息。

表2 Webmail登录情况记录

表3 邮件发送记录

4 结束语

本文实现了一个以 Linux 为开发平台的 Webmail 监控系统，系统部署在大型骨干网或企业内网出口处，功能是监控网络中的 Webmail 活动情况。考虑到骨干网或内网出口处数据流量很大，所以采用零拷贝技术提高数据包捕获能力，通过减少数据在内存中的拷贝次数，极大的提高了系统的整体性能。针对 Webmail 格式经常变化的情况，作为本文核心，提出了建立动态 Webmail 特征库的思想。当要监控新的 Webmail 或原有 Webmail 特征库因升级而发生变化时，只要在特征库中加入新的特征或更新特征库中相应的项可方便实现系统的后期维护，这样大大的提高了系统的灵活性和可扩展性。

通过实际的测试，本设计的不足之处在于 TCP 重组时，需要在内存中维护大量的 TCP 链接信息，这样对监控设备的内存、处理速度等提供了较高的要求，这正是本设计下一步重点需要改进的工作。（责编 岳逍远）

参考文献：

[1] Richard W. Stevens. TCP/IP 详解（卷 1：协议）[M] . 北京：机械工业出版社 ,2000.

[2] 张诚，郝东白，龙海，黄皓 . 基于正则表达式的 Webmail 监控与审计 [J]. 计算机工程与设计，2007，(2)：14–17.

[3] 马博，袁丁 . Linux 下的高流量数据包监听技术 [J]. 计算机应用，2009，(5):1244–1250

[4] 郭世泽，何韶军，牛伟 . . 基于 Hash 表和 SYN 计算的 TCP 包重组方法 [J]. 信息安全与通信保密，2006，(2):18–22.

[5] 张晋，于磊 . 局域网电子邮件监控系统的设计与实现 [J]. 信息技术，2007，(6):14–17

[6] Alexander Budanitsky，Graeme Himt. Evaluating WordNet–based Measures of Lexical Semantic Relatedness[J]. Computational Linguisfics, 2006, 32(l):13–7.

作者简介：朱鸿旭（1984 –），男，硕士研究生，主要研究方向：信息安全理论与应用；刘嘉勇（1962 –），男，教授，硕士生导师，主要研究方向：信息安全理论与应用，网络信息处理与信息安全。