浅析云安全技术及实现

张春明

(辽宁对外经贸学院，辽宁 大连 116052)

摘 要：云计算具有巨大商机，但同时也面临着潜在的巨大风险，云安全问题是云计算发展的重要障碍。应用云安全技术识别和查杀病毒不再仅仅依靠本地硬盘中的病毒库，而是依靠庞大的网络服务，实时采集、分析和处理。文章着重从查杀病毒和木马的角度来阐述有关云安全的技术以及实现，探讨了云安全问题的概念和所涉及到的技术问题，研究了资源池的建立及杀毒产品对云安全策略的各种解决方案。

关键词：云安全；云计算；资源池；病毒库

中图分类号：TP391 **文献标志码**：A **文章编号**：1006-8228(2012)10-04-03

Technology and implementationon of cloud security

Zhang Chunming

(*Liaoning university of international business and economics, Dalian, Liaoning 116052, China*)

Abstract: Cloud computing has great business opportunities, but also faces potential risks. Cloud security technology is a crucial impetus for the development of cloud computing. Recognizing and killing the virus by cloud security technology will no longer rely on the virus database in the local hard disk, but on a vast network service to realize real-time collection, analysis and processing. The technology and implementation of cloud security are introduced from the perspective of killing viruses and Trojans. The concept of cloud security issues and the relevant technical problems are discussed. The solutions to establishing resources pool and antivirus products are studied.

Key words: c1oud security; cloud computing; resources pool; virus database

0 引言

众所周知，云计算有着巨大商机，与此同时，也存在着巨大的安全风险。云计算发展中存在着隔离失败风险、合规风险、管理界面损害风险、数据删除不彻底风险、内部威胁风险等众多运营和使用风险，但这些都只是一般性风险，而不是主要风险。云计算当前最重要、最核心的风险是国家安全风险和企业经济信息失控风险。就国家安全风险而言，前哥伦比亚电视台新闻频道总裁在其撰写的报告中已明确指出："随着世界的变化，美国的未来也需重新定位，不过云计算是美国可以重申其全球经济和技术带头人地位的重要领域"。应该说，"云计算"的提出和快速发展，正好为美国提供了新的机会。就经济信息安全而言，发展云计算以后，企业和行业的大量经济信息，竞争信息将进入信息运营商的资源池中，其"海涵"的大型数据中心和强劲服务器，担当着软件开发的信息"调度师"和流程"监控员"。

在当前全球经济一体化的背景下，企业只有掌握竞争情报，并注意保护好自己的商业秘密，才能在激烈的市场竞争中处于主动地位。

本文将着重从查杀病毒和木马的角度来阐述有关云安全的问题。

1 云安全

1.1 云安全产生

云安全(C1oud Security)紧随云计算之后出现，它是网络时代信息安全的最新体现，它融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，并发送到服务器端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。未来杀毒软件将无法有效地处理日益增多的恶意程序。来自互联网的主要威胁正在由电脑病毒转向恶意程序及木马，在这样的情况下，原有的特征库判别法显然已经过时。云安全技术应用后，识别和查杀病毒不再仅仅依靠本地硬盘中的病毒库，而是依靠庞大的网络服务，实时进行采集、分析以及处理。

最早提出云安全这一概念的是趋势科技，2008年5月，趋势科技在美国正式推出了云安全技术。云安全的概念早期曾经引起过不小争议，现在已经被普遍接受。值得一提的是，中国网络安全企业在云安全的技术应用上走到了世界前列。

云安全的策略构想是：整个互联网就是一个巨大的"杀毒

收稿日期：2012-7-30

作者简介：张春明(1977-)，女，黑龙江人，硕士，副教授，主要研究方向：计算机应用。

软件”，参与者越多，每个参与者就越安全，整个互联网就会更安全。因为如此庞大的用户群，足以覆盖互联网的每个角落，只要某个网站被挂马或某个新木马病毒出现，就会立刻被截获。

1.2 云安全概念

云安全（Cloud security），《著云台》的分析师团队结合云发展的理论总结认为，是指基于云计算商业模式应用的安全软件，硬件，用户，机构，安全云平台的总称。

1.3 云安全技术

云安全是云计算技术的重要分支，已经在反病毒领域当中获得了广泛应用。云安全通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，推送到服务端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。整个互联网，变成了一个超级大的杀毒软件，这就是云安全计划的宏伟目标。未来本地杀毒软件将无法有效地处理日益增多的恶意程序。来自互联网的主要威胁正在由电脑病毒转向恶意程序及木马，在这样的情况下，采用的特征库判别法显然已经过时。云安全技术应用后，识别和查杀病毒不再仅仅依靠本地硬盘中的病毒库，而是依靠庞大的网络服务，实时进行采集、分析以及处理。

2 云安全技术应用

2.1 资源池的建立

构建一个合理的资源池，是实现从传统的“烟囱式IT”迈向云计算基础架构的第一步。在传统的“烟囱式IT”基础架构中，应用和专门的资源捆绑在一起，为了应对少量的峰值负载，往往会过度配置计算资源，导致资源利用率低下，据统计，在传统的数据中心里，IT资源的平均利用率不到20%。

构建资源池也就是通过虚拟化的方式将服务器、存储、网络等资源全面形成一个巨大的资源池。云计算就是基于这样的资源池，通过分布式的算法进行资源的分配，从而消除物理边界，提升资源利用率，统一资源池分配。作为云计算的第一步，资源池的构建在实现云计算基础架构的过程中显得尤为重要，只有构建合理的资源池，才能实现云计算的最终目的——按需动态分配资源。要搭建虚拟资源池，首先需要具备物理的资源，然后通过虚拟化的方式形成资源池。一个物理服务器可以虚拟出几个甚至是几十个虚拟的服务器，每一个虚拟机都可以运行不同的应用和任务。资源池应能提供对不同平台工作负载的兼容，企业应用类型多样化要求系统平台的多样化，一个企业可能既有基于Linux的应用，又有基于Windows的应用，甚至是基于Unix的应用，如何使得原有的应用都能够在资源池上运行，而不需要对应用进行重新编写。随着企业业务的增长，应用所需要的IT资源不断增加，应用的类型也不断增多，这就要求现有的资源池需要有充分的扩展能力，并根据应用的需求动态添加应用所需要的资源。同时，当现有的资源不足以支撑当前的业务时，资源池需要能够具有充分扩展能力，随时进行IT资源的扩容。

在云资源池中，应确保其客户的保密/敏感数据不能在使用、储存、传输过程中，或在没有任何补偿控制的情况下与其他客户数据混合或被他人获取。其云数据备份和云恢复计划，必须落实到位，以防止数据丢失和意外破坏。

2.2 现阶段云安全解决方案

金山毒霸云安全是为了解决木马商业化之后的互联网严峻的安全形势应运而生的一种全网防御的安全体系结构。它包括智能化客户端、集群式服务端和开放的平台三个层次。金山毒霸2011采用的“可信云安全平台”里的三项核心技术为：①可信云安全——云端人工智能自动鉴定，一分钟识别95%未知样本。金山倡导的可信云安全体系包含互联网可信认证；人工智能自动分析；样本的极速匹配算法；在客户端每天上亿次查询请求时，能够瞬间响应。金山毒霸2011的“可信云安全平台”，是由一系列收集、鉴定、发布等技术体系组成。②蓝芯II云引擎—实现精准快速查杀。蓝芯II云引擎，是将金山毒霸蓝芯II引擎和云安全紧密结合的版本。在引入可信云安全技术之后，将客户端非正常文件的微特征发送到云安全服务器查询，服务器瞬间返回查询结果（响应时间以毫秒计）。采用蓝芯II云引擎技术，能大大提升病毒扫描的性能。据网友实际测试，联网时进行病毒扫描的速度大约是断网扫描的两倍。③白名单优先技术—传统杀毒软件都是以识别文件是不是病毒为出发点，这种传统的病毒识别方法难免会出现误报（将正常文件报告为病毒）和漏报。识别正常文件，因为对一个普通的电脑用户来说，系统一旦配置好，再安装新软件的机会并不是很多，99%用户电脑上的正常文件是可以被完全收集到的，只有正常文件之外的其他程序才会真的对系统有威胁。简单的逻辑分析可以得出一个结论，这种白名单优先的鉴定方法可以将危险程序100%排除。

趋势科技云安全利用行为分析的“相关性技术”把威胁活动综合联系起来，确定其是否属于恶意行为。Web威胁的单一活动似乎没有什么害处，但是如果同时进行多项活动，那么就可能会导致恶意结果。因此需要按照启发式观点来判断是否实际存在威胁，可以检查潜在威胁不同组件之间的相互关系。通过把威胁的不同部分关联起来并不断更新其威胁数据库，使得趋势科技获得了突出的优势，即能够实时做出响应，针对电子邮件和Web威胁提供及时、自动的保护。趋势科技广泛的全球自动反馈机制的功能很像现在很多社区采用的“邻里监督”方式，实现实时探测和及时的“共同智能”保护，将有助于确立全面的最新威胁指数。

卡巴斯基的全功能安全防护旨在为互联网信息搭建一个无缝透明的安全体系，针对互联网环境中类型多样的信息安全威胁，卡巴斯基实验室以反恶意程序引擎为核心，以技术集成为基础，实现了信息安全软件的功能平台化。系统安全、在线安全、内容过滤和反恶意程序等核心功能可以在全功能安全软件的平台上实现统一、有序和立体的安全防御。

瑞星云安全计划：将用户和瑞星技术平台通过互联网紧密相连，组成一个庞大的木马/恶意软件监测、查杀网络，每个“瑞星卡卡6.0”用户都为云安全计划贡献一份力量，同时分享其他所有用户的安全成果。 “瑞星卡卡6.0”的“自动在线诊断”模块，是云安全计划的核心之一，每当用户启动电脑，该模块都会自动检测并提取电脑中的可疑木马样本，并上传到瑞星“木马/恶意软件自动分析系统”（简称RsAMA），整个过程只需要几秒

钟。随后RsAMA将把分析结果反馈给用户，查杀木马病毒，并通过“瑞星安全资料库”(简称RsSD)，分享给其他所有“瑞星卡卡6.0”用户。由于此过程全部通过互联网并经程序自动控制，可以在最大程度上提高用户对木马和病毒的防范能力。理想状态下，从一个盗号木马从攻击某台电脑，到整个云安全网络对其拥有免疫、查杀能力，仅需几秒的时间。

2.3 尚待解决问题

云安全联盟与惠普公司共同列出了云计算的七宗罪，主要是基于对29家企业、技术供应商和咨询公司的调查结果而得出的结论。

⑴ 数据丢失/泄漏。云计算中对数据的安全控制力度并不是十分理想，API访问权限控制以及密钥生成、存储和管理方面的不足都可能造成数据泄漏，并且还可能缺乏必要的数据销毁政策。

⑵ 共享技术漏洞。在云计算中，简单的错误配置都可能造成严重影响，因为云计算环境中的很多虚拟服务器共享着相同的配置，所以必须为网络和服务器配置执行服务水平协议(SLA)，以确保及时安装修复程序，以及实施最佳处理。

⑶ 内奸。云计算服务供应商对工作人员的背景调查力度可能与企业数据访问权限的控制力度有所不同，很多供应商在这方面做得还不错，但并不够，企业需要对供应商进行评估并提出如何筛选员工的方案。

⑷ 帐户、服务和通信劫持。很多数据、应用程序和资源都集中在云计算中，而云计算的身份验证机制如果很薄弱的话，入侵者就可以轻松获取用户帐号并登录客户的虚拟机，因此建议主动监控这种威胁，并采用双因素身份验证机制。

⑸ 不安全的应用程序接口。在开发应用程序方面，企业必须将云计算看作是新的平台，而不是外包。在应用程序的生命周期中，必须部署严格的审核过程，开发者可以运用某些准则来处理身份验证、访问权限控制和加密。

⑹ 没有正确运用云计算。在运用技术方面，黑客可能比技术人员进步更快，黑客通常能够迅速部署新的攻击技术而在云计算中自由穿行。

⑺ 未知的风险。透明度问题一直困扰着云服务供应商，帐户用户仅使用前端界面，他们不知道他们的供应商使用的是哪种平台及他们的修复水平。

3 结束语

云安全并不是一种纯粹的反病毒技术，我们可以将其理解为一种反病毒理念，一种安全互联网化的思路，一个互联网化的安全防御体系，也就是杀毒软件的互联网化。利用云安全体系，杀毒软件能够更快地收集病毒样本，更快地对病毒进行处理，并能在网络威胁到达用户计算机前就对其进行阻止，反病毒的效率大大提升，而且将更为智能化，带来更完善的用户体验，最终达到让互联网时代的用户都能得到更快、更全面的安全保护的目的。

参考文献：

[1] 余媚娟.浅析“云安全”技术[J].计算机安全,2011.9.
[2] 方志.浅谈云安全[J].信息系统工程,2009.8.
[3] 蓝调.构建云计算资源池必须考虑五个问题,http://www.cnw.com.cn/cloud-computing/htm2012/20120615_248781.shtml.
[4] 王汝林.发展“云计算”必须高度重视“云安全”[J].中国信息界,2011.1.
[5] 欧阳中辉.“云安全”在计算机防病毒应用中的问题研究[J].计算机与现代化,2010.12.

(上接第3页)

机工程与应用,2011.47(18):45-47
[13] 张治俊,罗辞勇,张帆,卢斌.采用振荡参数策略的粒子群优化算法[J].重庆大学学报,2011.34(6):36-41
[14] 刘进,覃洁萍.带极值抖动的变尺度粒子群优化算法[J].计算机工程与应用,2011.47(30):53-57
[15] Shi Y,Eberhart R C.A modified particle swarm optimization[C]. Proceedings of the IEEE Congress on Evolutionary Computa-tion, 1998:303-308
[16] Shi Y, Eberhart R C. Empirical study of particle swarm optimiza-tion[C]. Proceedings of the IEEE Congress on Evolutionary Computation,1999:1945-1950
[17] 梁昔明,董淑华,龙文,肖晓芳.动态惯性权重向量和雅变异的粒子群优化算法[J].计算机工程与应用,2011.47(5):29-31
[18] 高立群,李若平,邹德.全局粒子群优化算法[J].东北大学学报(自然科学版),2011.32(11):1538-1541
[19] 周敏,李太勇.粒子群优化算法中的惯性权值非线性调整策略[J].计算机工程,2011.37(5):204-206
[20] Holden N, Freitas A A. A hybrid particle swatm/ant colonyalgorithm for the classification of hierarchical biologicaldata//Proc of the IEEE Swarm Intelligence Sympo-sium: NewDelhi, India, 2005L100-107.
[21] Angeline P J. Using selection to improve particle swarmopti-mization//Proc of the IEEE International Conference onEvo-lutionary Computation. Anchorage,USA,1998:84-89
[22] Senthil A M, Chandramohan A, Rao M V C. Competitiveap-proaches to pso algorithms via new acceleration co-efficient variant with mutation operators// Proc of the 6m Interna-tionalConference on Computational Intelligence and Multime-dia Applications. Las Vagas,USA,2005:225-230
[23] 李勇,王建君,曹丽华.基于繁殖粒子群算法的火电厂负荷优化分配[J].电力自动化设备,2012.32(4):80-83
[24] 齐学梅,罗永龙,赵诚.求解流水车间调度问题的混合粒子群算法[J].计算机工程与应用,2012.48(9):33-36
[25] 彭力,王茂海.基于前馈扰动的粒子群改进算法[J].控制工程,2012.19(1):102-105
[26] 陶新民,杨立标.一种自适应指导的文化粒子群算法[J].计算机工程与应用,2011.47(14):37-41
[27] 朱冰,齐名军.混合粒子群优化算法[J].计算机工程与应用,2012.48(9):47-50
[28] Alireza Alfi, Mohammad-Mehdi Fateh. Parameter Identification Based on a Modified PSO Applied to Suspension System. J. Software Engineering &Applications,2010.3:221-229