



军事云信息安全保障体系架构

郭保平¹, 程建¹, 刘维平²

(1. 空军工程大学 西安 710077; 2. 宝鸡市公安局网络安全支队 宝鸡 721000)

摘要:云计算架构以其强大的信息处理能力、按需弹性的服务模式、增强的安全性等优势,已成为军事信息系统的的发展方向。首先探讨了军事云计算安全的概念及特点,对军事云安全领域研究及应用的现状进行了分析。在此基础上,提出了军事云信息安全保障体系构建的目标,构建了军事云信息安全保障体系架构,并对其包含的主要模块进行了深入分析,最后给出了需要解决的关键技术问题。

关键词:云计算;军事云;信息安全保障;安全体系架构

doi: 10.11959/j.issn.1000-0801.2015299

Information Assurance Framework of Military Cloud

Guo Baoping¹, Cheng Jian¹, Liu Weiping²

(1. Air Force Engineering University, Xi'an 710077, China;

2. Baoji Municipal Public Security Bureau Network Security Detachment, Baoji 721000, China)

Abstract: Due to the powerful capacity of information processing, on-demand and elastic service model, and enhanced security, cloud computing has become the future of military information system. At first, the conception and feature of cloud computing security was discussed. The current situation of research and application in military cloud security was analyzed. The objective of information assurance with military cloud was proposed on this foundation, then the architecture of information assurance with military cloud was structured, and the main modules of this architecture were analyzed in-depth. Lastly some key research opportunities were listed.

Key words: cloud computing, military cloud, information assurance, security framework

1 引言

随着军队信息化建设的深入推进,云计算架构因其强大的信息处理能力和良好的信息服务能力,已成为军事信息系统的发展方向。但从当前云计算研究和应用的现状来看,安全问题已成为影响云计算深化应用的关键问题。军事信息系统是基于信息系统体系作战的关键依

托,涉密程度高、使用环境复杂恶劣、应用类型多样,对于安全性有着比民用信息系统更高的要求。随着信息技术的发展,军事信息系统的安全问题已经从通信安全保密、计算机主机及信息系统的安全防护,发展到面向云计算架构的信息安全保障的阶段^[1]。深入研究军事云计算的信息安全保障问题,有利于加速推动云计算架构在军事信息系统中的应用。

收稿日期:2015-06-22;修回日期:2015-10-31

基金项目:全军军事类研究生资助课题(No.2013JY507)

Foundation Item: PLA Military Graduate Funded Project (No.2013JY507)

论文引用格式:郭保平,程建,刘维平.军事云信息安全保障体系架构.电信科学,2015299

Guo B P, Cheng J, Liu W P. Information assurance framework of military cloud. Telecommunications Science, 2015299

2 军事云计算安全的概念及特点

军事云计算,简称军事云,就是应用云计算相关的关键技术,建设军事云数据中心等硬件基础设施体系,开发军事领域相关应用服务等软件体系,依托军事信息网络,向军队的单位或个人用户提供云计算服务。军事云计算安全是指与军事云计算相关的安全问题,包括数据安全、服务安全、安全法规标准等构成的完整的军事云信息安全保障体系。

军事云计算具有不同于民用云计算的特点,其工作于复杂电磁环境和强网络对抗的环境之下,对于信息安全保密具有极高的要求,主要应用目标服务于军事效能和战斗力的提升。在安全性方面,军事云计算与民用云计算的具体对比见表 1。

表 1 民用云计算与军事云计算在安全性方面的对比

比较项目	民用云计算	军事云计算
应用目标	经济效益和生产力的提升	军事效能和战斗力的提升
应用环境	互联网	军事独立网络
安保要求	一般	严格
联网对象	低敏感	高敏感
器件要求	指标低	指标高
关键技术	共性关键技术	共性关键技术、军事专用关键技术
标准协议	市场成熟商用	国产自主产权

相比传统军事信息系统安全及民用云计算安全,军事云计算安全具有以下主要特点。

(1)军事云安全边界相对模糊

传统的军事信息系统具有封闭性的特点,通过物理和逻辑上的安全域定义,可以清楚地保护设备及用户^[2]。军事云计算环境下,必将对原有的许多封闭系统进行整合,大量的用户及数据存储在军事云数据中心的云端,流动性增强,使得安全边界变得模糊,对传统的基于边界防护的军事信息系统安全防护策略构成了挑战。

(2)军事云服务面临可用性的挑战

传统的军事信息系统大量采用客户端/服务器(C/S)的服务模式,虽然也向网络中心的方向发展,但仍有大量的数据及应用运行在军事信息网络各个位置的客户端之上。泛在的网络连接是云计算的基本特征之一,随着大量移动计算设备的部署,关键数据及核心服务部署在云端,导致军事云对军事信息网络基础设施的依赖性增强。战术网络环境下,网络时断时续或带宽受限,还面临着敌方硬摧毁的

威胁,这些都会对军事云服务的可用性造成较大的影响。

(3)军事云对安全保密性的要求更高

军事云工作于复杂电磁环境和高强度网络对抗的环境之下,其主要目标是获得军事效能和战斗力的提升。相比民用云计算以经济效益为目标,军事云对安全保密的要求更高。在安全方面,民用云计算主要联网对象具有较低的敏感度,对于器件指标要求低,主要采用市场上共性的关键技术和成熟商用的标准协议;而对于军事云计算,因为联网对象通常具有较高的敏感度,对安全器件的指标要求高,必须发展军事专用关键技术和具有自主知识产权的标准协议。

3 军事云信息安全研究及应用现状

在全球范围内,美军、印军等都将云计算作为军事领域一项极具发展潜力的技术,研究将其应用到军事信息系统中的方法,其中美军在军事云计算的研究及应用方面处于领先地位^[3]。自 2008 年云计算技术开始发展以来,美军就和 IT 领域的跨国公司,如 IBM、亚马逊、惠普等展开合作,研发了多个军事云计算项目,主要包括全球信息栅格内容分发服务(GIG content delivery service, GCDS)、快速访问计算环境(rapid access computing environment, RACE)、Forge.mil 开发平台工具、海军私有安全云等^[4]。美军的国防部企业云环境计划在非密网络、保密网络以及绝密网络 3 类网络中各自独立实现,并在各自网络中进行数据交换^[5]。

随着军事云计算应用的深入,安全问题开始凸显,逐渐得到美军的高度重视。美军将军事云的安全问题作为军事云应用时优先考虑的战略问题,这在美军各种信息技术相关规划中得到了显著体现。美军于 2012 年 7 月在美国《联邦政府云计算战略》的基础上,制定了美国国防部云计算战略,各军种也相继发布了各自的云计算战略或规划^[6]。美军在国防部云计算战略中指出“使云计算成为最具创新性、最高效和最安全的信息和 IT 服务交付平台”,分析了向云计算环境迁移时面临的安全挑战,明确将安全性作为国防部云计算的主要目标之一^[7]。美军在向云计算环境迁移时,提出了统一的安全体系结构。该架构不同于各军种现有的标准纵深防御,而是构建一种陆海空三军共用的企业级的体系机构,最终实现随时随地、安全、按需的情报及数据共享^[8]。

军事云与民用云计算不同,其具有特有的安全问题。



对于这些军事领域特有的问题,美军展开了自主的研究。在美国国防部,主要由先进研究项目局(DoD Advanced Research Program Agency,DARPA)和信息系统局(DoD Information System Agency,DISA)结合联合信息环境(joint information environment,JIE)的构建,负责军事云安全问题的研究工作。美国国防科学委员会在2013年1月发布的报告《数字云中的网络安全》中,从军事云硬件安全、军事云软件安全、军事云数据中心的安全运行、军事云安全评估等方面,将军事云安全问题作为一个重要的研究方面进行了深入研究,并给出了相关的对策建议及后续的技术研究方向^[9]。DARPA研究的面向任务的弹性云计划,通过检测、诊断、响应云中的攻击,有效地构建云计算的社区健康系统;加密数据计算计划主要通过同态加密的方法,在不解密数据的情况下对加密数据直接进行操作,但这种技术目前还未进入实用阶段^[10]。美国海军研究生院的Noemi基于信息安全职业资格认证的视角,从10个领域对国防部云计算安全问题进行了研究^[11]。此外,针对军事云安全特有的理论及技术问题,美军还从安全管理架构、风险管理、安全评估、网络防御等方面自主展开了较为深入的研究^[12,13]。

4 军事云信息安全保障体系构建

4.1 军事云信息安全保障体系构建的目标

军事云信息安全保障体系构建的总体目标是保证军

事云中的数据及应用程序的机密性、完整性、可用性,同时确保基于云计算架构的军事信息系统安全、可靠地运行,从而支撑基于信息系统的体系作战效能的提升。军事云安全体系的构建,不应该以牺牲业务系统的运行效率为代价。同时,安全目标必须具体且具有针对性,以使其有效并且易于实现。具体目标包含以下3个方面:一是保护军事云中数据及软件计算的机密性和完整性,这是军事云信息安全保障体系所要完成的基本目标,也是实现其他目标的基础。二是确保军事云运行的可用性、可靠性、可预测性及弹性。确保军事云服务运行的可用性,主要是要保证战术环境下军事信息网络的可用性,同时还要避免军事云中应用软件的单点故障。三是对军事云进行不间断的故障检测及安全评估,这也是指军事云的安全态势感知,需要对军事云数据中心的所有操作和行为进行审计和取证。当系统发生故障时进行故障检测、收集信息,进行不间断的安全评估,才能快速地检测入侵,并对其后果进行快速彻底的补救。

4.2 军事云信息安全保障体系架构

军事云信息安全保障体系架构如图1所示,在军事云的使命任务和安全需求的引领下,主要包含两大功能:一是对军事云自身的保护,即军事云安全防护体系,包括对军事云数据中心、云用户端及两者之间交互的军事信息网络基础设施的防护,类似于对传统的网络化军事信息系统

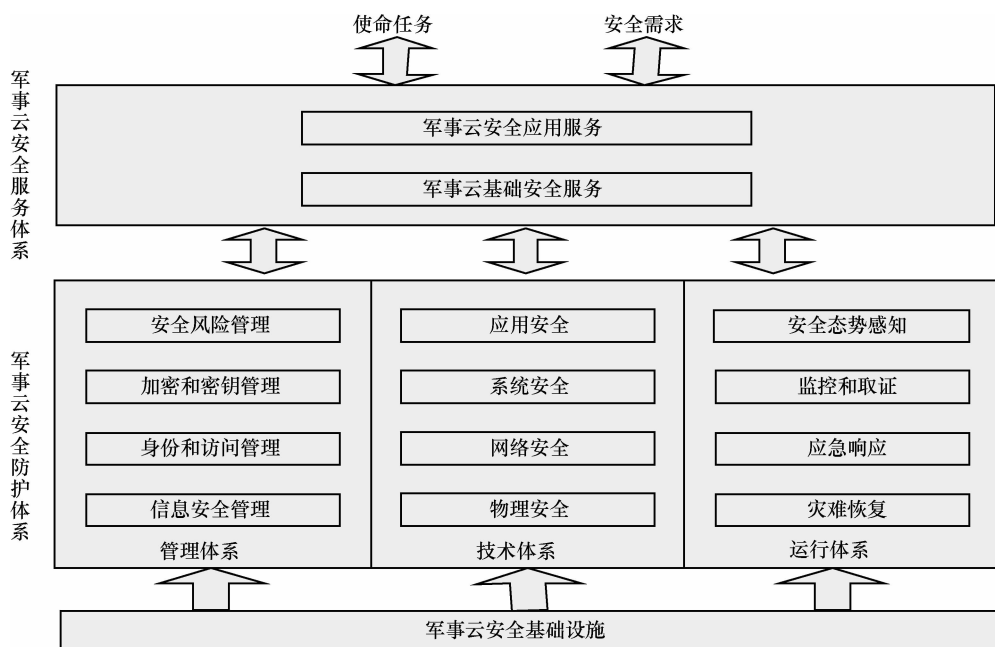


图1 军事云信息安全保障体系架构

的保护;另外一大功能是在军事云安全防护体系的基础上,构建军事云安全服务体系,由军事云数据中心将安全作为一种服务向云用户提供。军事云安全防护体系和安全服务体系均建立在军事云安全基础设施的基础之上,相互之间进行安全信息的交换,并和用户进行交互。

4.2.1 军事云安全防护体系

军事云安全防护体系包含技术体系、管理体系及运行体系3个部分。技术体系是军事云安全防护体系的支撑,通过先进和有效的技术手段保证军事云的安全运行。按照防护对象的层次,技术体系可划分为物理安全、网络安全、系统安全和应用安全4个部分。其中每个部分不仅包含现有军事信息系统的安全技术,还包括军事云特有的安全技术,如虚拟化安全、云计算体系架构安全性分析等。

管理体系在军事云安全防护体系中位于较高的层次,作用至关重要。按照管理对象的不同,可分为信息安全管理、安全技术管理、人事安全管理和安全法规标准管理等。军事云的安全管理体系由功能组件和过程组件两部分组成,在安全管理员的统一管理下,通过接口与技术体系和运行体系进行交互。功能组件包括身份管理、证书管理、属性管理、特权管理、数字政策管理、安全配置管理、元数据管理、密钥管理及审计管理等,过程组件包含云服务实例管理、账户管理、认证和授权管理、客户管理、外部供应商管理及内部管理等^[14]。

运行体系体现了军事云安全防护体系动态安全防护的特征,贯穿于整个信息安全生命周期。运行体系包括军事云安全态势感知、全程安全监控和取证、应急响应和灾难备份及恢复等部分。各部分在统一的军事云安全防护策略的指导下构成一个有机整体,协调工作,共同维护军事云数据中心的安全运行。

军事云安全防护体系中的技术体系、管理体系和运行体系3个部分相辅相成、互为补充,共同构筑稳固的军事云安全防护系统。其中,管理体系是军事云安全防护系统的基础,先进的军事云安全技术只有在科学管理体系的基础上才能发挥其应有的防护作用;技术体系是军事云安全防护的支撑,针对军事云出现的各种新的安全威胁,需要研发先进的安全技术手段予以解决和应对;运行体系是军事云安全防护的核心,其在安全防护策略的指导下,需要综合运用技术和管理手段,实现军事云的动态安全运行。

4.2.2 军事云安全服务体系

军事云安全服务体系提供的服务包含军事云基础安全服务、军事云安全应用服务以及军事云服务安全等级评估。军事云基础安全服务将一些基础的安全功能作为云服务提供,包括云认证服务、云授权服务、云加密服务及云审计服务等。军事云安全应用服务在军事云基础安全服务的层次之上,提供云反病毒服务、云网络安全监控服务、云垃圾邮件处置服务及分布式拒绝服务攻击告警服务等^[15]。军事云服务安全等级评估依据等级保护的思想,将军事云服务按照所处理信息的密级,进行定性结合定量的安全评估,并划分等级,由此确定军事云服务的安全等级。

5 军事云安全需要突破的关键技术

军事云信息安全保障体系的建立,需要大量安全技术的支撑。其中有些利用传统的安全技术就可以实现,但还有一些军事云特有的安全问题,需要研发相应的先进技术予以解决。军事云安全需要突破的关键技术主要有以下几种。

5.1 同态加密技术

军事云用户将大量的数据存储于军事云数据中心,为了保证数据的机密性,加密技术起着重要的作用。同态加密技术是指对加密状态的数据进行各种功能的操作,而不需要对其进行解密^[16]。同态加密中一项关键的挑战是降低计算的复杂度。现有技术已经具备了简单操作(比如加法和乘法)的能力,然而,现有技术计算复杂度过高。同态加密技术的进步,将使得高安全的效用计算和跨越多种安全层次的数据密集型计算成为可能。这项技术也可以提供态势感知和聚合统计,而不用牺牲原始数据源的敏感性。现在已经有相关的研究对云中的加密数据、保留数据的机密性进行类似于数据库的操作。

5.2 云可信计算技术

可信计算技术是解决信息安全问题的一个重要研究方向,其核心思想是通过硬件的支持,实现系统行为的可预期和可验证。云计算因为其面向服务体系架构固有的安全缺陷,其基于软件技术的安全防护措施有极大可能性被破解和利用。云可信计算技术通过在云计算数据中心服务器、指挥终端等硬件上加装符合可信平台模块标准的安全芯片,从硬件上阻断非法用户对系统资源的访问^[17]。目前的可信计算技术主要结合传统的服务器、终端等展开研



究,对于军事云还应该结合军事云安全及应用的特点,研究适合军事应用环境的云可信计算技术。

5.3 虚拟化安全技术

虚拟化技术在云计算中的大量应用使得虚拟化安全成为云计算安全不可回避的问题。虚拟化技术有其安全上的优点,但也存在潜在的风险和挑战。服务器虚拟化中的内存虚拟化,共享的物理内存有数据泄露的风险;存储虚拟化中不同用户、不同安全等级的数据共用物理存储设备,其中数据隔离问题是影响虚拟化安全的关键问题;网络虚拟化使得虚拟机之间的网络流量只需要在物理机器内部交换而不需要通过交换机,基于网络设备的安全监控难以实施^[8]。因此,发展虚拟化安全技术、解决这些由虚拟化带来的安全挑战,就成为军事云安全一项重要的研究领域。

5.4 安全事件大数据分析

现有的网络流分析,不管是检测网络安全事件或者是对大数据分析,经常是对于大数据进行相对简单的计算或者是对于其中一小部分进行复杂的计算。然而,为了解决军事云安全采集的大数据带来的挑战,对大数据进行复杂的分析是必需的。也就是说,在缺少先验知识的情况下,以一种高效和限时的方式从多源情报或多源数据中集中检测微弱的安全信号及事件^[9]。军事云安全事件大数据分析的主要挑战集中在数据表示、开发创新的算法等方面。这些算法主要用于从全局的角度检测统计学的异常事件,警告分析人员或者其他的算法层。这种方法将从根本上改变现有基于人工的安全事件分析和处理流程,提高安全事件自动化处理的水平。

6 结束语

军事云计算在军队信息化建设中的应用已经开始起步,军事云安全作为军事云应用的关键问题,其相关理论及技术还需要结合军事云的实践进行深入研究和探索。对军事云安全建立相应的安全模型,进行定性结合定量的安全评估,制定适合军事云安全需求的安全防护策略、安全法规及标准等,都是后续需要研究的课题。

参考文献

- 1 王古宣,左琳琳.美军信息保障浅析.现代军事,2008(6): 64~66
Wang G X, Zuo L L. Information assurance analysis of US

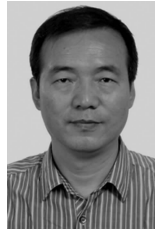
- army. Modern Military, 2008(6): 64~66
- 2 张慧,邢培振.云计算环境下信息安全分析.计算机技术与发展,2011,21(12): 164~166
Zhang H, Xing P Z. Information security analysis in cloud computing environment. Computer Technology and Development, 2011, 21(12): 164~166
- 3 Dallas A P. The military applications of cloud computing technologies (master dissertation). Kansas: United States Army Command and General Staff College, 2013
- 4 郑全弟,张文,李成海等.云计算在美军事领域的应用与展望.飞航导弹,2013(1): 53~56
Zheng Q D, Zhang W, Li C H, et al. Cloud computing applications and prospect in US army. Aerodynamic Missile Journal, 2013(1): 53~56
- 5 韩星晔,李新明.云计算军事应用研究.装备指挥技术学院学报,2011,22(2): 103~107
Han X Y, Li X M. Research on military application of cloud computing. Journal of the Academy of Equipment Command & Technology, 2011, 22(2): 103~107
- 6 HQMC C4 Strategy and Vision Division. Marine corps private cloud computing environment strategy. <http://www.defense.gov/news/Marine-Corps-PrivateCloud.pdf>, 2012
- 7 Department of Defense Chief Information Officer. Cloud computing strategy, <http://www.defense.gov/news/DoDCloudComputingS-strategy.pdf>, 2014
- 8 李成,李明桂,向敏.联合信息环境JIE及其安全研究.通信技术,2015,48(1): 46~50
Li C, Li M G, Xiang M. Joint information environment and its security. Communications Technology, 2015, 48(1): 46~50
- 9 The Defense Science Board. Cyber Security and Reliability in a Digital Cloud. Washington DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2013: 29~40
- 10 任福乐,朱志祥,王雄.基于全同态加密的云计算数据安全方案.西安邮电大学学报,2013,18(3): 92~95
Ren F L, Zhu Z X, Wang X. A cloud computing security solution based on fully homomorphic encryption. Journal of Xi'an University of Posts and Telecommunications, 2013, 18(3): 92~95
- 11 Noemi A. Optimizing security of cloud computing within the DOD (master dissertation). Monterey: Naval Postgraduate School, 2010
- 12 Kris E B, Jeffrey W H, Robert F M. A case for DoD application of public cloud computing services. Proceedings of the 2011 Military Communications Conference, Maryland, USA, 2011: 1888~1893
- 13 Timothy K B. A strategic approach to network defense: framing the cloud. Parameters, 2011(3): 43~58

- 14 Kretzschmar M, Knuepfer M. Reference security management architecture-guiding governmental and military inter-cloud initiatives. Proceedings of 2011 Military Communications and Information Systems Conference, Canberra, Australia, 2011: 391~397
- 15 冯登国, 张敏, 张妍等. 云计算安全研究. 软件学报, 2011, 22(1): 71~83
Feng D G, Zhang M, Zhang Y, *et al.* Study on cloud computing security. Journal of Software, 2011, 22(1): 71~83
- 16 李美云, 李剑, 黄超. 基于同态加密的可信云存储平台. 信息网络安全, 2012, 12(9): 35~40
Li M Y, Li J, Huang C. A credible cloud storage platform based on homomorphic encryption. Netinfo Security, 2012, 12(9): 35~40
- 17 孙晶晶, 蔡勉, 赵阳. 基于可信计算的云用户安全模型. 计算机安全, 2012, 12(4): 19~24
Sun J J, Cai M, Zhao Y. Based on trusted computing user security model for cloud computing. Computer Security, 2012, 12(4): 19~24
- 18 房晶, 吴昊, 白松林. 云计算的虚拟化安全问题. 电信科学, 2012, 28(4): 135~140
Fang J, Wu H, Bai S L. Virtualization security issues in cloud computing. Telecommunications Science, 2012, 28(4): 135~140
- 19 李明桂, 肖毅, 陈剑锋等. 基于大数据的安全事件挖掘框架. 通信技术, 2015, 48(3): 346~350
Li M G, Xiao Y, Chen J F, *et al.* Big data-based framework for security event mining. Communications Technology, 2015, 48(3): 346~350

[作者简介]



郭保平,男,空军工程大学博士生,主要研究方向为军事云计算及其安全问题。



程建,男,博士,空军工程大学教授、博士生导师,主要研究方向为信息化作战与建设。



刘维平,男,宝鸡市公安局网络安全支队高级工程师、四级警长,主要研究方向为网络安全。