新型入侵检测机制①

汪 鑫，黄廷磊

(桂林电子科技大学 计算机与控制学院，桂林 541004)

摘 要：入侵检测作为一项重要计算机网络安全技术日益受到人们的重视，而现在的入侵检测技术还存在许多尚未解决的问题，如因为网络速度传输加快，网络流量大导致检测的实时性和有效性的降低，无法检测复杂多样的入侵行为等。研究设计出一种基于云计算框架下的新型入侵检测机制，该机制使用一种全局策略可弥补传统入侵检测系统的不足，并具有极大的可扩展性。

关键词：入侵检测；网络安全技术；云计算；数据采集；数据分析；安全评估

A New Type of Intrusion Detection Mechanism

WANG Xin, HUANG Ting-Lei

(Computer and Control Institute, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract: People are paying more attention on Intrusion detection which is an important computer network security technolog. However there are still many unresolved issues in Intrusion Detection, for instance, the rapid speed of network transmission and network high traffic flow lead to real-time and effectiveness detection going down, and can not detect complex and diverse intrusion. We are developing a new intrusion detection mechanism based on cloud computing. This mechanism uses a global view which can make up for the deficiency of traditional intrusion detection, and proved to be great scalable.

Keywords: intrusion detection; network security technology; cloud computing; data collection; data analysis; security assessment

近年来，在入侵检测技术取得到了快速发展，国外很多实验室和公司在从事入侵检测系统的研究和开发工作，已经完成了原形系统和产品的开发，国内的研究机构和从事网络安全产品生产的公司也进行了相关的研究开发。但是当前入侵检测系统在技术上仍然存在着许多有待解决的问题，如低检出率，误报率高等。

本文根据入侵检测发展趋势研究设计出一种基于云计算框架下的入侵检测机制。在该机制下，网络站点的检测引擎分析来自云计算中心收集的数据，判断发现入侵路径，然后将所产生的警告由全局数据分析器处理，全局数据分析器利用全局视野来监控网络安全。

1 云计算

1.1 云计算的概念

中国云计算专委会认为，云计算最基本的概念是：通过整合、管理、调配分布在网络各处的计算资源，并以统一的界面同时向大量用户提供服务[1]。云计算是并行计算、分布式计算和网格计算的融合和发展，也是虚拟化、效用计算、面向服务架构等概念混合演进的结果。从研究现状上看，云计算具有以下特点：

1) 超大规模。“云”能赋予用户前所未有的计算能力。GOOGLE 云计算已经拥有 100 多万台服务器，亚马逊、微软等公司的“云”均拥有几十万台服务器。

2) 虚拟化。“云”中所请求的资源不是固定有形

① 基金项目:广西自然基金(桂科自 0640169)
收稿时间:2010-08-30;收到修改稿时间:2010-10-02

实体，而且用户无需知道应用运行的具体位置，可以在任何位置、使用各种终端获取服务。

3) 高可扩展性。“云”的资源规模可动态伸缩，满足用户规模和应用增长的需要。

4) 通用性。在“云”的支撑下可以构造出千变万化的应用。

5) 高可靠性。“云”使用了数据多副本容错、计算节点同构可互换等措施来保障服务，使用云计算比使用本地计算机更加可靠。

6) 按需服务。“云”是一个庞大的资源池，用户按需购买，像自来水、煤气那样计费。

7) 低成本。“云”的特殊容错措施使得可以采用及其廉价的节点构成云，云的自动化管理使数据中心管理成本大幅降低，云的公用性和通用性使资源的利用率大幅提升，云设施可以建在电力资源丰富的地区从而降低能源成本。GOOGLE 中国区前总裁李开复称，GOOGLE 每年投入约 16 亿美元建云计算数据中心，所获得的能力相当于使用传统技术投入 640 亿美元，节省了 40 倍的成本。

1.2 云计算的实现机制

由于云计算分为 IaaS、PaaS 和 SaaS 三种类型，不同厂家又提供不同的解决方案，本文综合不同厂家方案，构造了一个供参考的云计算体系结构。

云计算技术体系结构分为四层[2]:物理资源池、资源池层、管理中间件层和 SOA 构建层。物理资源池层包括计算机、存储器、网络设施、数据库和软件等。资源池层是把大量相同类型的资源构成同构或接近同构的资源池，如计算机资源池、数据资源池等。SOA 构建层将云计算能力封装成标准的 WEB SERVICES 服务，并纳入到 SOA 体系进行管理使用，包括服务接口、服务注册、服务访问等。管理中间件层负责资源管理、任务管理、用户安全管理等工作。

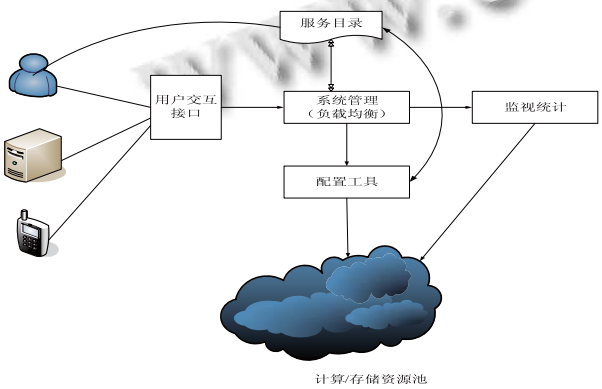

图 1　云计算的实现机制

基于上述体系结构，以 IaaS 云计算为例，简述云计算的实现机制[2]。如图 1。

用户交互接口向应用以 Web Services 方式提供访问接口获取用户需求。服务目录是用户可以访问的服务清单。系统管理模块负责管理和分配所有可用资源，其核心是负载均衡。配置工具负责在分配的节点上准备任务运行环境。监视统计模块负责监视节点运行状态并完成用户使用节点情况统计。执行过程是用户交互接口允许用户从目录中选取并调用一个服务，该请求传递给系统管理模块后，它将为用户分配恰当的资源，然后调用配置工具为用户准备运行环境。

2 基于云计算框架下的入侵检测机制

为了克服传统 IDS 的不足，本文设计了一种基于云计算框架下的入侵检测机制(intrusion detection mechanism based on cloud computing)，简称 IDCC。

2.1 IDCC 体系结构

IDCC 体系结构是基于公共入侵检测框架(CIDF)设计构建出的，由四部分组成：本地站点数据采集器[3]、本地站点分析器[3]、远程站点数据采集器[3]、云计算数据中心(CCDC)。整体结构如图 2。

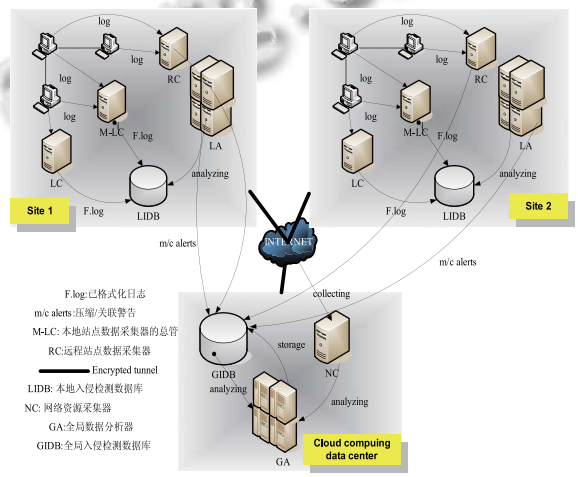

图 2　IDCC 体系结构图

1) 本地站点数据采集器

本地站点数据采集器采集的日志信息来自位于同

一网段的传感器，这些传感器可以是主机、服务器。防火墙、或 IDS 等，我们这个采集器的优点在于无需在传感器上安装任何软件。采集器将所收集的信息日志格式化，然后将其传送到本地站点入侵数据库。在每个站点我们都设置一个或多个采集器作为主管采集器，主管采集器平时采集数据，还负责同一站点所有采集器的管理，当其中的采集器发生故障时，主管采集器进行调度协调。

2) 本地站点分析器

本地站点分析器是入侵检测的关键，它分析本地站点入侵数据库里已格式化的日志信息，若判断是入侵行为则产生警告提示，然后关联警告以便发现更复杂的入侵。本地站点分析器将产生的所有警告打包压缩传送到云计算数据中心的全局入侵检测数据库。

3) 远程站点数据采集器

远程站点数据采集器是个特殊的数据采集器，它所采集的日志来自一些关键的传感器和安装在传感器上的安全工具，然后分析这些日志，实时产生相关站点的近似安全级别，同时将这些日志传送给云计算数据中心的全局入侵检测数据库。当危险入侵介入时，即使黑客搽除被感染的传感器上的信息，远程数据采集器也能实时发现，并同时在瘫痪站点充当故障排查员的身份。

4) 云计算数据中心

云计算数据中心[6]有三个主要的功能部件：全局数据分析器[4]，网络资源采集器，全局入侵检测数据库。如图 3。

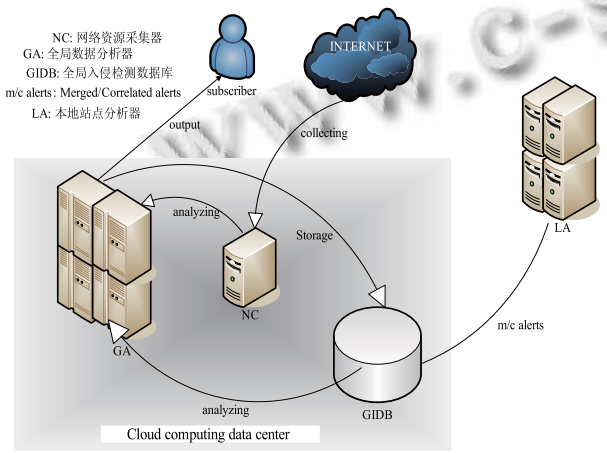

图 3 云计算数据中心体系结构图

(a) 全局数据分析器控制和管理本地站点分析器，它是本地站点分析器的主管者，负责在网络中监控全局的入侵检测。它的工作流程是提取网络资源采集器中已格式化的网络数据信息，综合参考来自全局入侵检测数据库的警告，解析信息，判断是否有入侵行为，然后产生相应警告提示，最后将所有产生的警告关联起来反馈用户，同时还将其警告存入全局入侵检测数据库以便下次的快速检测查询。全局数据分析器的内部结构图 4。

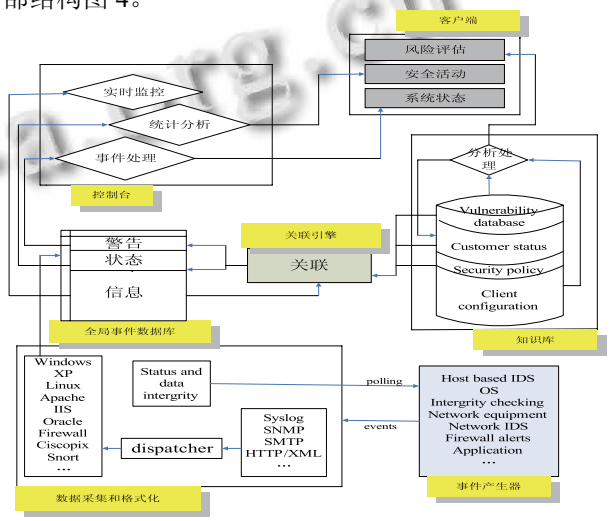

图 4 全局数据分析器内部结构图

(b) 网络资源采集器是个特殊的本地站点数据采集器，因为它所采集的所有数据信息来自整个网络，然后将其采集信息格式化并发送给全局数据分析器。

(c) 全局入侵检测数据库是个拥有巨大容量的数据库，它存储来自本地站点分析器和全局数据分析器产生的警告。

2.2 入侵检测的数据采集

一般来说，来自异构数据源的数据采集使用传输协议[5]，例如 snmp、smtp 等。在 IDCC 机制中的数据采集是使用两种代理机制[5],一种是协议代理，另一种是应用程序代理。前者是采集来自传感器的数据信息，后者是解析数据将其转化成“伪标准”格式(IDCC 机制中定义的格式如图 5)，而调度分配器负责将其两种代理模块联接。

1) 协议代理。协议代理的功能是接收来自特定的传输协议(如 syslog,snmp 等)的数据信息，它们作为服务器端应用程序，不仅监听由传感器传入连接的网络

数据，同时还将监听收集的可疑数据传送给调度分配器。

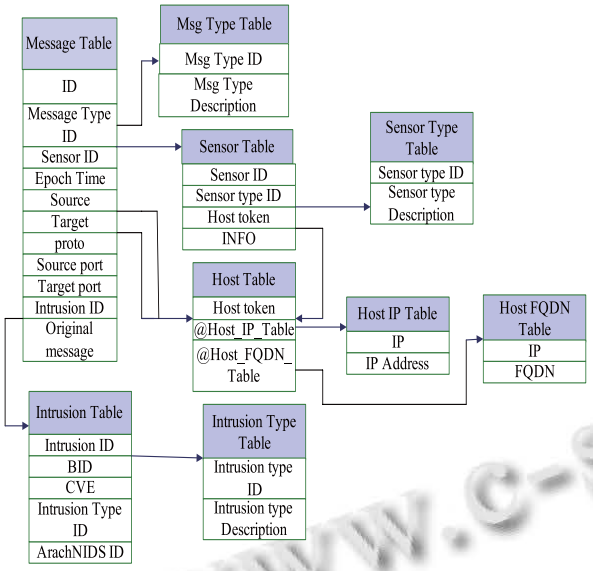

图 5　“伪标准”数据格式

2) 调度分配器。调度分配器的功能是首先确定接受的数据信息类型，然后将其数据分配给合适的应用程序代理处理。

3) 应用程序代理。应用程序代理按照 IDCC 机制中规定的“伪标准”格式，将调度分配器分配的数据信息格式化，以方便 IDCC 中的下步检测操作。

2.3 入侵检测的数据分析

数据分析是入侵检测中关键的步骤之一，所需要进行的操作如下：数据关联性分析[3]，数据结构化分析[3]，入侵路径分析[3]和入侵行为分析[3]等操作。

a.数据关联性分析是个独立的操作，它的功能是分析复杂的事件数据，寻找其中的序列规律，将其转换成简单精确的事件，为下一步分析是否有入侵意图的数据分析工作打下坚实基础。

b.数据结构化分析在于确定是否有入侵意图，管理上下文的静止和终止状态。简而言之，数据结构化分析是由独立模块控制的一组操作，每个模块由特定信息驱动激活，而模块使用自定义的“标准”语义进行分析，最后分析模块的输出结果是几种逻辑运算的和。

c.入侵路径分析提供是否有入侵企图的依据，通过路径分析，进行路径绑定，对入侵源进行封锁查找。

d.入侵行为分析根据安全策略，结合以上步骤所有结论，综合得出结论并发送反馈信息

2.4 入侵检测的安全评估

前文所介绍的远处站点数据采集器除了拥有数据采集这个功能外，还能产生安全级别，可以保障多站点网络的安全活动。操作如下：

在每个本地站点，远程站点数据采集器收集数据来自本地站点数据采集器和一些特殊的传感器，然后将这些数据传输到云计算数据中心的全局入侵检测数据库。

全局数据分析器分析判断接收到的数据，并产生警告提示，最终在本地站点产生近似安全级别。

本地站点数据分析器分析判断来自本地站点数据采集器收集的数据，匹配入侵特征模式，检测是否存在可疑行为，最终在本地站点产生真实安全级别。

全局数据分析器将近似安全级别和真实安全级别进行比较，当两种安全级别之间发生显著差异时，则产生可疑行为的警告提示，最后将其警告送到安全管理器进行更进一步调查。

3　小结

该文所提的基于云计算框架下的入侵检测机制与传统的入侵检测机制相比较，有以下优点：

1) 提高入侵检测系统的检测速度，以适应网络通信的要求。在入侵检测系统中，截获网络中的每一个数据包，进行分析、匹配是否具有某种攻击的特征需要花费大量的时间和系统资源。而现在的分析匹配等功能完成都只需要在云计算数据中心完成即可，大大提高了检测速度。

2) 快速感知，捕获新的威胁，减少入侵检测系统的漏报和误报，提高其安全性和准确度[7]。与传统信息安全模式的“一个人战斗”相比，云计算的客户数据中心凝聚了互联网的力量，整合了所有可能参与的人，效率大大提高，并且云计算数据中心能即时更新面对着每天都有新的攻击方法产生和新漏洞发布，并且主机代理的相互协作功能能有效检测网络范围的入侵行为，极大的提高安全性和准确度。

3) 提高入侵检测系统的互动性能，从而提高整个系统的安全性能。在大型网络中，网络的不同部分可能使用了多种入侵检测系统，甚至还有防火墙、漏洞扫描等其他类别的安全设备，而在云计算数据中心使

（下转第 91 页）

80%以上，其中最高的识别率可以达到 93.02%(高兴识别率：88.89%，平静识别率：94.74%，愤怒识别率：90.20%，悲伤识别率 100%)。这主要是由于 SVM 算法将问题转化为凸二次优化问题，得到的解为全局最优解，而基于 BP 算法的 ACON 网络和 OCON 网络得到的可能是局部最优解，而并非是全局最优解。

5 小结

本文采用 SVM 作为分类器实现了基于语音信号的四种情感(高兴、愤怒、平静、悲伤)识别，达到了 86.36%的平均识别率。对比 ACON 网络、OCON 网络，SVM 方法识别正确率分别提升了 7.06 %和 7.21 %。通过对比试验可知用 SVM 作为情感识别的分类器非常有效。但仍存在不足，比如高兴情感相对其他三种情感的识别率显得较低，主要是将高兴情感误判为愤怒情感。这可能是由于本文计算的情感特征对于区分高兴情感并不一定是最有效的。如从能量特征这方面来讲，高兴情感和愤怒情感的语音信号能量都比较大，这就不利于高兴情感和愤怒情感的区分。因此，提取有效的情感特征是情感识别正确的前提和基础，这有待于以后进一步研究。

参考文献

1 张石清,赵知劲,戴育良,杨广映,等.支持向量机应用于语音情感识别的研究.声学技术,2008,27(1):88–90.

2 Schroder M. Experimental study of affect bursts. Speech Communication, 2003,40(1-2):99–116.

3 韩纪庆,邵艳秋.基于语音信号的情感处理研究进展.语音技术,2006,5:58–62.

4 林奕琳,韦岗,杨康才.语音情感识别的研究进展.电路与系统学报,2007,12(1):90–98.

5 尤鸣宇.语音情感识别的关键技术研究[博士学位论文].杭州:浙江大学,2007.

6 Khanchandani KB, Hussain MA. Emotion recognition using multilayer perceptron and gengealized feed forward neural network. Journal of Scientific & Industrial Research, 2009, 68:367–371.

7 赵力.语音信号处理.北京:机械工业出版社,2008.36-80.

8 姜晓庆,田岚,崔国辉.多语种情感语音的韵律特征分析和情感识别研究.声学学报,2006,31(3):217–221.

9 边肇祺,张学工.模式识别.第 2 版.北京:清华大学出版社,2000.296–303.

10 Wang ZP, Zhao L, Zou CR.Support vector machines for emotion recognition in chinese speech. Journal of Southeast University, 2003,19(4):307–310.

11 Burkhardt F, Kienast M, Paeschke A, Weiss B. Berlin Database of Emotional Speech (Technical University, Institute for Speech and Communication, Department of Communication Science, Berlin). http://pascal.kgw.tu-berlin.de/emodb/

（上接第 68 页）

用了通用安全用户接口，使得这些入侵检测系统之间以及入侵检测系统和其他安全组件之间如何交换信息，共同协作来发现攻击、作出响应并阻止攻击。

4) 较低的成本[8]。基于云计算框架下的入侵检测系统通过云计算数据中心进行控制检测，并不需要在各种各样的主机上进行安装，大大减少了安全和管理的复杂性。

参考文献

1 张为民,唐剑峰.云计算深刻改变未来.北京:科学出版社,2010.30–31.

2 王鹏.云计算.北京:电子工业出版社,2010.5–6.

3 Ganame AK, Bourgeois J, Bidou R, Spies F. A global security architecture for intrusion detection on computer networks. Computers & Security, March 2008, 27: 30–47.

4 Liu XL. Research and application on Hierarchical Intrusion Detection [MS Thesis]. Shanghai Jiaotong University. January, 2008.

5 Sun Y, Huang Hao. Hybrid network intrusion detection system. Computer Engineering, 2008, 34(9).

6 Zhang LJ, Zhou Q. CCOA: Cloud Computing Open Architecture. IBM T.J. Watson Research Center, New York, USA, 2009 IEEE International Conference on Web Services, November 2009.

7 Muttik I, Barton C. Cloud security technologies. information security technical report. 2009 Elsevier Ltd All rights reserved. April 2009.

8 Christodorescu M, Sailer R, Schales DL. Cloud Security Is Not(Just) Virtualization Security. IBMT. J. Watson Research, September 2009.