浅析“云安全”病毒防范技术的架构与原理

赵 伟
(燕山大学里仁学院 河北 秦皇岛 066004)

[摘 要]随着网络技术的发展和信息交换的日益频繁,信息安全技术的研究变得越来越重要。近来,国际和国内的安全专家和厂商纷纷提出了“云安全”的概念和基于“云安全”的计算机安全解决方案。文中用通俗的语言讲解了“云安全”的概念、技术、应用及展望

[关键词]云安全 病毒 木马 网络信息安全
中图分类号:V353 文献标识码:A 文章编号:1009-914X(2010)31-0089-01

“云安全”是计算机信息安全界最热门的词语,国际和国内的计算机安全专家为了应对计算机信息安全正在受到前所未有的挑战,把计算机安全也由单台的计算机各自为政的防御局面提升为整个网络层面来考虑,统一协调各方面资源,充分发挥网络资源的优势,提出了全新的“云安全”概念。那么“云安全”到底是什么?

1 云安全的概念

中国企业创造的“云安全”概念,在国际云计算领域独树一帜。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。

2 发展趋势

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,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。整个互联网就是一个巨大的“杀毒软件”,参与者越多,每个参与者就越安全,整个互联网就会更安全。

云安全的概念提出后,曾引起了广泛的争议,许多人认为它是伪命题。但事实胜于雄辩,云安全的发展像一阵风,瑞星、趋势、卡巴斯基、MCAFEE、SYMANTEC、江民科技、PANDA、金山、360安全卫士等都推出了云安全解决方案。瑞星基于云安全策略开发的2009新品,每天拦截数百万次木马攻击,其中1月8日更是达到了765万余次。趋势科技云安全已经在全球建立了5大数据中心,几万部在线服务器。据悉,云安全可以支持平均每天55亿条点击查询,每天收集分析2.5亿个样本,资料库第一次命中率就可以达到99%。借助云安全,趋势科技现在每天阻断的病毒感染最高达1000万次。

3 思想来源

云安全技术是P2P技术、网格技术、云计算技术等分布式计算技术混合发展、自然演化的结果。为此,可以建立一个分布式统计和学习平台,以大规模用户的协同计算来过滤垃圾邮件:

首先,用户安装客户端,为收到的每一封邮件计算出一个唯一的“指纹”,通过比对“指纹”可以统计相似邮件的副本数,当副本数达到一定数量,就可以判定邮件是垃圾邮件;

其次,由于互联网上多台计算机比一台计算机掌握的信息更多,因而可以采用分布式贝叶斯学习算法,在成百上千的客户端机器上实现协同学习过程,收集、分析并共享最新的信息。

反垃圾邮件网格体现了真正的网格思想,每个加入系统的用户既是服务的对象,也是完成分布式统计功能的一个信息节点,随着系统规模的不断扩大,系统过滤垃圾邮件的准确性也会随之提高。用大规模统计方法来过滤垃圾邮件的做法比用人工智能的方法更成熟,不容易出现误判假阳性的情况,实用性很强。反垃圾邮件网格就是利用分布互联网里的千百万台主机的协同工作,来构建一道拦截垃圾邮件的“天网”。 反垃圾邮件网格思想提出后,被IEEE Cluster 2003国际会议选为杰出网格项目在香港作了现场演示,在2004年网格计算国际研讨会上作了专题报告和现场演示,引起较为广泛的关注。

4 难点问题

要想建立“云安全”系统,并使之正常运行,需要解决四大问题:

第一,需要海量的客户端(云安全探针);

第二,需要专业的反病毒技术和经验;

第三,需要大量的资金和技术投入;

第四,必须是开放的系统,而且需要大量合作伙伴的加入。

第一、需要海量的客户端(云安全探针)。只有拥有海量的客户端,才能对互联网上出现的病毒、木马、挂马网站有最灵敏的感知能力。目前瑞星有超过一亿的自有客户端,如果加上迅雷、久游等合作伙伴的客户端,则能够完全覆盖国内的所有网民,无论哪个网民中毒、访问挂马网页,都能在第一时间做出反应。

第二、需要专业的反病毒技术和经验。瑞星拥有将近20年的反病毒技术积累,有数百名工程师组成的研发队伍,近年来连续获得国际级技术认证,技术实力稳居世界前列。这些都使瑞星“云安全”系统的技术水平国内首创,国际领先。大量专利技术、虚拟机、智能主动防御、大规模并行运算等技术的综合运用,使得瑞星的“云安全”系统能够及时处理海量的上报信息,将处理结果共享给“云安全”系统的每个成员。

第三、需要大量的资金和技术投入。目前瑞星“云安全”系统单单在服务器、带宽等硬件上的投入已经超过1亿元,而相应的顶尖技术团队、未来数年持续的研究花费将数倍于硬件投资,这样的投入规模是非专业厂商无法做到的。

第四、必须是开放的系统,而且需要大量合作伙伴的加入。瑞星“云安全”是个开放性的系统,其“探针”与所有软件完全兼容,即使用户使用其他杀毒软件,也可以安装瑞星卡卡助手等带有“探针”功能的软件,享受“云安全”系统带来的成果。而久游、迅雷等数百家重量级厂商的加入,也大大加强了“云安全”系统的覆盖能力。

5 云安全展望

“云安全”是一种趋势,它让“云计算”应用到网络信息安全领域,将会为网络信息安全领域带来巨大的变化。“云安全”的发展给网络信息安全要求提供了更大的可能性,但是“云安全”本身也存在很多问题,这就需要不断的完善和改进。因此,对“云安全”的进一步研究显得尤为重要,相信未来它的发展必为网络信息安全界带来飞跃。

参考文献

[1] 薛质编著. 信息安全技术基础和安全策略[M]. 清华大学出版社,2007.

[2] 王雷,房倩. 对“云安全”的初探. 实验室科学,2009(5).

[3] 趋势科技Secure Cloud云安全网站:http://219.234.88.31/edm/TrendMicro/TMweb/page_ya_1_1.html.

[4] CSDN官方网站:http://www.Csdn.net.

---

u(- λ) 紫外可见分光光度计的测量重复性0.037nm
uc(Δλ) 镨钕滤光片波长定值不确定度 0.2nm
合成不确定度uc(△λ)= nm=0.203nm
标准的执行能力 k取2时
扩展不确定度为U=0.203×2=0.41nm

7、干涉滤光片:

采用同样方法对干涉滤光片进行评定,输入量的标准不确定度汇总见下表:

标准不确定度汇总表

标准不确定度分量u(Xi)	不确定度来源	标准不确定度
u(- λ)	紫外可见分光光度计的测量重复性	0.036nm
uc(Δλ)	干涉滤光片波长定值不确定度	0.5nm

合成不确定度uc(△λ)= nm=0.501nm
标准的执行能力k 取2时
扩展不确定度为U=0.501×2=1.0nm

注:以上分析主要针对中低档仪器测量结果不确定度评定。

作者简介:侯会杰 1965年3月出生 男 汉族 籍贯:河南省辉县市
学位:专科 职称:中级工程师 主要研究方向:计量检定。