

基于私有云泄漏的攻击方法研究

张 伟,解争龙

(咸阳师范学院 信息工程学院,陕西 咸阳 712000)

摘 要:为了解决云计算框架所面临的威胁,提出了针对私有云间隐私泄漏攻击的最优攻击选择算法。该方法根据最优攻击选择算法选择攻击对象,然后发起攻击,攻击造成私有云间的路径发生拥塞,迫使私有云改变路径;与此同时发起对其他路径的攻击,进而控制其他路径,从而实现对私有云间通信的控制,通过对被控制路径的监听完成隐私窃取,最后对攻击方法进行了实现。实验结果表明,该方法能够有效地控制私有云间的通信,从而达到对私有云侦测的目的,为保护私有云间信息的攻击提供参考。

关键词:私有云;云计算;隐私泄漏;攻击算法

中图分类号:TP309.2

文献标识码:A

文章编号:1673-629X(2015)06-0124-04

doi:10.3969/j.issn.1673-629X.2015.06.027

Research on Attack Method Based on Private Cloud Leak

ZHANG Wei, XIE Zheng-long

(School of Information Engineering, Xianyang Normal University, Xianyang 712000, China)

Abstract: In order to solve the threats in cloud computing framework, the algorithm of optimal selection attacking on private clouds privacy leaking is proposed. Using the optimal selection algorithm to choose attacked object and attack, causing the path congestion between the private clouds, forcing the clouds to change another communication path. Simultaneously, attack the other paths, and then control the other paths, so as to realize the control of communication between the private clouds, completing privacy stealing by monitoring the controlled paths. Finally, the attack method is realized. The experimental results show that this method can effectively control the communication between private clouds, so as to achieve the aim of the private cloud detection, providing an reference for protecting the information between private cloud to be attacked.

Key words: private clouds; cloud computing; privacy leak; attack algorithm

0 引言

现代计算服务的架构采用层次化网络架构难以满足企业对信息日益增长的需求,然而在对计算需求日益增长的同时,所面临的安全问题也在不断增多。云计算^[1]的出现一定程度上解决了计算对资源的需求,但云计算框架^[2-3]本身同样也面临着来自云内部和云外部的各种威胁,而这些威胁会直接或间接地影响云体系自身的整体安全。如何降低由于内外部威胁造成的损失,成为目前研究的主要问题。云计算框架的应用,所产生的安全威胁主要有两类:一类是云内部的安全威胁,另一类是云外部的安全威胁。针对这些威胁,目前采取的主要防范措施是将传统安全防护措施变相应用到云计算的框架中,这在一定程度上能够缓解目前所面临的诸多问题,如云内部间相互攻击、云

与外部协同攻击等。

文中针对在云计算框架下所面临的系统安全问题,提出并实现针对私有云间隐私泄漏的攻击方法和最优攻击选择算法。

1 私有云漏洞检测的主要技术

私有云漏洞检测技术主要有系统漏洞静态分析技术、系统漏洞模糊分析技术、系统渗透测试分析技术、系统漏洞发现模型等。下面主要对这四类技术的主要特征进行分析研究。

1.1 系统漏洞静态分析技术

静态分析方法^[4]通过对系统的形式、结构、内容或者文档等的评价,以得出相应的评估结果。静态分析不在程序执行时进行。其主要形式有:

收稿日期:2014-07-17

修回日期:2014-10-23

网络出版时间:2015-05-06

基金项目:国家自然科学基金资助项目(61102018);咸阳师范学院专项科研基金项目(14XSYK039)

作者简介:张 伟(1981-),男,副教授,硕士,研究方向为嵌入式系统、可信计算、并行计算;解争龙,教授,硕士,研究方向为网络安全。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20150506.1630.025.html>

(1)人工检查方式。该方式由相关人员对系统整体安全性进行评价。该方式的优点为:①对系统漏洞识别的准确度较高;②能够发现潜在的错误。缺点为:①人工方式花费的时间较多,人工的效率受到多方面因素的影响;②对相关实施人员的专业素质要求较高。

(2)自动检查方式。由计算机根据相关标准、规则和算法识别系统的漏洞。该方式的优点为:①相较于人工方式减少了时间的开销,工作效率得到提高;②对相关实施人员专业素质要求不高。缺点为:①自动化程度不高,部分工作流程还需要借助人工完成;②对系统漏洞的识别依赖于前期的标准和规则的建立,效率和准确率受限于识别算法和规则等。

系统漏洞静态分析技术的主要方式^[5]:模式匹配技术、词法分析技术、注解分析技术、语法树分析技术、数据信息流分析技术等。

1.2 系统漏洞模糊分析技术

系统漏洞模糊分析^[6-7]的概念在目前尚没有统一的定义。模糊分析是一种高度自动化测试,该测试覆盖大多数边界用例,测试用例参考使用了一些无效数据作为应用的输入,使得结果更加具有代表性。文中结合不同观点,对模糊分析提出如下的概念:首先,数据的产生来自于随机性;其次,将产生的随机性数据交由目标系统进行处理;最后,分析处理结果。综上所述,即一种不完全由人工执行、选择,且测试规范的分析方法。

1.3 系统渗透测试分析技术

系统渗透测试^[8]分析技术是通过模拟可能的攻击来评估系统整体安全的一种方法。该过程包括对系统的不足、缺陷或漏洞的分析,即从一个攻击者的角度去思考系统的整体安全状况,主动发现攻击对象的漏洞。系统渗透测试的主要形式有^[9-10]:

(1)系统黑盒测试。测试者站在外部观察者的角度去考虑系统的整体安全性,而不关注系统的内部构成;

(2)系统白盒测试。测试者通过了解系统整体安全情况,站在设计者的角度去思考系统整体安全;

(3)系统灰盒子渗透测试。该测试方式介于系统黑盒测试和系统白盒测试之间,对测试者的要求较高,不仅要求测试人员以局外人的角度去思考,同时也要站在设计者的角度去思考。这就要求在两方面达到一种平衡,使测试能够达到全面性、有用性、高效性的要求,所以这要求测试人员具备较高的专业能力。

1.4 系统漏洞发现模型

系统漏洞发现模型^[11-12]的建立有利于漏洞的发现,但是在实际中,没有一种高效的、通用的、抽象的模型可以覆盖绝大多数的具体应用,这也是阻碍系统漏

洞发现的主要原因。目前主要的系统漏洞发现模型都存在时间、环境、独立性的问题。

在云计算的框架下,对云的安全性需要考虑云的内部和外部,但是在一个云中很难区分谁是内,谁是谁外;这就要求把安全问题从独立系统的角度上升到整体的角度去考虑,对云内部的安全分析和对云外部的分析。

2 最优攻击算法

在对网络进行攻击时,需要对网络中的状态进行评估,寻找最佳的攻击对象,然后再对攻击目标发起攻击。最优攻击算法是根据网络中设备的安全等级、设备进出流量、设备漏洞数量进行综合计算,计算出在网络中最容易被攻击的对象,然后发动对该设备的攻击。最优攻击组合由四元组组成 (A, B, C, D) ,该四元组代表某台设备的状况,其中 A 代表设备的入口流量情况, B 代表设备的出口流量情况, C 代表该设备的安全等级, D 代表该设备的漏洞数。

针对设备的网络流量划分入口流量和出口流量,计算设备的平均网络流量。流量的划分通过时间段划分,将一天的网络流量划分为24个时间段,每1小时为一个计算窗口。设备平均流量计算,如公式(1)所示。

$$T_{\text{output}_i} = \frac{\sum_{t=1}^{24} T_{\text{output}_i}}{24}, T_{\text{input}_i} = \frac{\sum_{t=1}^{24} T_{\text{input}_i}}{24}, T_i = \frac{T_{\text{output}_i} + T_{\text{input}_i}}{2} \quad (1)$$

其中, t 表示每天划分的是每小时的流量; T_{input_i} 表示 i 设备的日平均入口流量; T_{output_i} 表示 i 设备的日平均出口流量; T_i 表示 i 设备的日平均流量。

$$\theta_i = \frac{T_i}{n}, D_i = M_i \times \theta_i, BC_i = D_i \times V_i \quad (2)$$

其中, M_i 为人为划分网络中设备的重要程度,取值为1,2,3。3表示重要设备;1表示不重要设备;2表示介于重要与不重要之间的设备。 V_i 表示 i 设备的漏洞数量。最优攻击算法如下所示:

算法:最优攻击算法。

输入:网络设备进口流量、网络设备出口流量、网络设备漏洞数量;

输出:输出最优攻击对象。

开始

(1)根据公式(1)计算 T_i ;

(2)根据公式(2)计算 BC_i ;

(3)对 BC_i 排序,选择最大为攻击对象。

结束

最优攻击算法在攻击对象的考虑中将流量、漏洞、

设备重要程度作为考虑对象,对网络中的设备进行等级划分,有利于选择一个合理的攻击对象,发起相对容易的攻击。

3 私有云间隐私泄漏攻击实例

3.1 私有云间隐私漏泄攻击实例设置

实验环境在 GNS3 网络模拟,由两个边界出口路

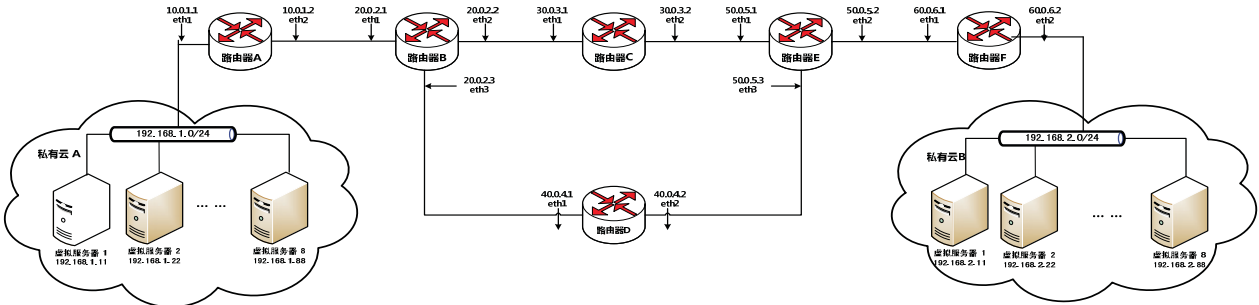


图 1 模拟实验拓扑路由设置信息

表 1 私有云服务器运行配置

私有云 A(B)	运行操 作系统	采用的 虚拟机	虚拟机安装的 操作系统
虚拟服务器 (1~4)	CentOS 6.4 64 位	Xen	2 台 Windows XP3 32 位、 2 台 Fedora 19 64 位
虚拟服务器 (5~8)	Fedora19 64 位	KVM	2 台 Windows XP3 32 位、 2 台 CentOS 6.4 64 位

3.2 私有云间隐私漏泄攻击实例实验场景

实验设置分为三阶段。第一阶段为探测阶段,主要完成对网络环境中流量分布的探测;第二阶段为实施准备阶段,根据第一阶段探测的网络流量分布信息,以及中转路由信息,寻找攻击代价最小的攻击组合,最优攻击组合由三元组组成 (X,Y,Z) 。该三元组代表某设备的状况,其中 X 代表设备的入口流量情况, Y 代表设备的出口流量情况, Z 代表该设备的漏洞数量;最后,在完成第二阶段的攻击后,网络系统以备控制,可以实施对私有云间通讯的监控。

3.2.1 探测阶段

探测阶段主要采用目前主流的网络流量分析系统 NTAS^[13] 和网络漏洞扫描系统 Nessue^[14], NTAS 主要完成对网络全局流量分布态势的分析,实现对全局网络的掌控。Nessue 主要完成对可被攻击对象漏洞扫描,寻找可被攻击对象。根据 NTAS 和 Nessue 搜集的信息,反映出当前网络中的链路状况,计算出最佳攻击路径。

3.2.2 实施准备阶段

该阶段主要完成对选择的合适攻击对象发起攻击,造成被攻击对象网络堵塞,使得私有云选择其他路径通信,同时完成对其他路径的监控,以备第三阶段实施对私有云间通信进行监控。文中选择路由器 D 为

由、两条路由选择路径,所有的路由服务均在 CentOS 上运行。两个私有云,每个私有云有足够的节点,模拟真实网络环境下的情形,私有云配置如表 1 所示。在用例中,使用了两台路由器作为被攻击对象,网络接口采用的是吉比特网络接口。图 1 展示了具体路由配置情况。

实施拥塞的路由,选择路由器 C 为被监控路由。私有云 A 和 B 之间的通信路径由路径一($ABCEF$)和路径二($ABDEF$)组成。

3.3 私有云间隐私漏泄攻击实例的测试

3.3.1 拥塞测试

通过对被攻击对象实施攻击,造成被攻击对象资源消耗枯竭,采用构造虚假连接方式进行。路由器 D 被攻击前后 CPU 使用情况如图 2 所示,内存资源消耗如图 3 所示。

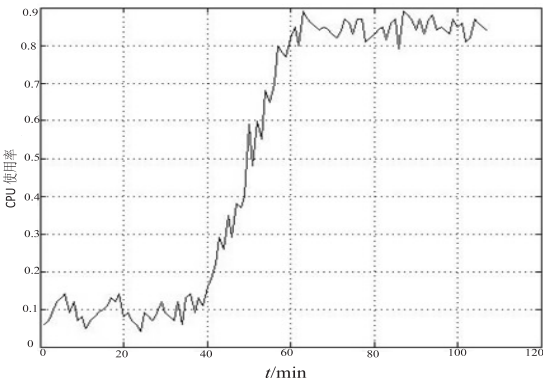


图 2 路由器 D 被攻击前后 CPU 使用率

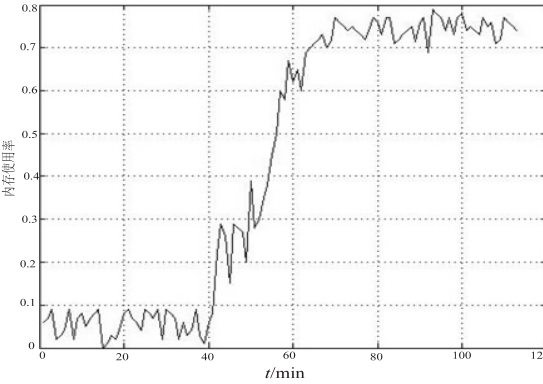


图 3 路由器 D 被攻击前后内存使用率

3.3.2 获取私有云的内部信息

通过在路由器 C 部署监控设备,对经过路径一 (ABCEF) 流量进行分析。文中截取了由私有云 A 中用户使用 telnet 客户端经过路径一访问私有云 telnet

服务器的登录信息,如图 4 所示;私有云 A 中用户使用 MSN 经过路径一与私有云 B 中用户进行通信的信息,如图 5 所示。

Packets1.cap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]						
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help						
Filter: Expression... Clear Apply Save						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.11	192.168.2.11	TCP	78	de-noc > telnet [SYN] Seq=0 win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=1444389 TSecr=0 WS=1
2	0.001690	192.168.1.11	192.168.2.11	TCP	78	telnet > de-noc [SYN, ACK] Seq=0 Ack=1 win=17376 Len=0 MSS=1448 WS=1 TSval=346979 TSecr=1444389
3	0.001741	192.168.2.11	192.168.1.11	TCP	70	de-noc > telnet [ACK] Seq=1 Ack=1 win=32120 Len=0 TSval=1444389 TSecr=346979
4	0.013173	192.168.2.11	192.168.1.11	TELNET	97	Telnet Data ...
5	0.150283	192.168.1.11	192.168.2.11	TELNET	73	Telnet Data ...
6	0.150351	192.168.2.11	192.168.1.11	TCP	70	de-noc > telnet [ACK] Seq=28 Ack=4 win=32120 Len=0 TSval=1444404 TSecr=346980
7	0.150528	192.168.2.11	192.168.1.11	TELNET	73	Telnet Data ...

图 4 私有云 A 与私有云 B 之间 Telnet 服务通信

Packets1.cap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]						
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help						
Filter: Expression... Clear Apply Save						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.11	192.168.2.11	MSNMS	160	MSG 77 U 89
2	5.005034	192.168.1.11	192.168.2.11	MSNMS	160	MSG 78 U 89
3	9.999933	192.168.1.11	192.168.2.11	MSNMS	160	MSG 79 U 89
4	13.143769	192.168.1.11	192.168.2.11	MSNMS	63	PNG
5	13.344744	192.168.2.11	192.168.1.11	MSNMS	66	QNG 45
6	15.003610	192.168.1.11	192.168.2.11	MSNMS	160	MSG 80 U 89
7	20.001423	192.168.1.11	192.168.2.11	MSNMS	160	MSG 81 U 89
8	25.005437	192.168.1.11	192.168.2.11	MSNMS	160	MSG 82 U 89
9	30.004668	192.168.1.11	192.168.2.11	MSNMS	160	MSG 83 U 89
10	35.005905	192.168.1.11	192.168.2.11	MSNMS	160	MSG 84 U 89

图 5 私有云 A 与私有云 B 之间 MSN 服务通信

4 结束语

文中在对私有云间的隐私泄漏的攻击方法研究的基础上,提出了最优攻击选择算法,并对私有云间隐私进行了攻击测试,最终造成私有云间路径拥塞而改变路径,从而达到对私有云间通信的控制,通过对被控制路径的监听完成隐私泄漏。实验结果表明,该方法能够有效地对私有云间的隐私进行窃取。后续的工作是进一步优化算法,以期得到一个对私用云间隐私更有效的攻击方式。

参考文献:

[1] 冯登国,张 敏,张 妍,等. 云计算安全研究[J]. 软件学报,2011,22(1):71–83.

[2] 陈 康,郑纬民. 云计算:系统实例与研究现状[J]. 软件学报,2009,20(5):1337–1348.

[3] 罗军舟,金嘉晖,宋爱波,等. 云计算:体系架构与关键技术[J]. 通信学报,2011,32(7):3–21.

[4] 梁 彬,侯看看,石文昌,等. 一种基于安全状态跟踪检查的漏洞静态检测方法[J]. 计算机学报,2009,32(5):899–909.

[5] Camenisch J. Better privacy for trusted computing platforms

[C]//Proceedings of 9th European symposium on research in computer security. [s.l.]:[s.n.],2004.

[6] Teuton J, Peterson E, Nordwall D, et al. LINEBACKER: bio-inspired data reduction toward real time network traffic analysis[C]//Proc of 6th international symposium on resilient control systems. [s.l.]:IEEE,2013:170–174.

[7] Jack K, Rowell D, Fuguang S H I, et al. Network traffic analysis using a flow table; U. S. ,8432807[P]. 2013–04–30.

[8] 田 伟,许 静,杨巨峰,等. 模型驱动的 Web 应用 SQL 注入渗透测试[J]. 高技术通讯,2012,22(11):1161–1168.

[9] 王晓聪,张 冉,黄赅东. 渗透测试技术浅析[J]. 计算机科学,2012,39(6A):86–88.

[10] 崔 颖,章丽娟,吴 灏. 基于攻击图的渗透测试方案自动生成方法[J]. 计算机应用,2010,30(8):2146–2150.

[11] 陈 恺,冯登国,苏璞睿,等. 一种多周期漏洞发布预测模型[J]. 软件学报,2010,21(9):2367–2375.

[12] 聂楚江,赵险峰,陈 恺,等. 一种微观漏洞数量预测模型[J]. 计算机研究与发展,2011,48(7):1279–1287.

[13] 高彦刚. 实用网络流量分析技术[M]. 北京:电子工业出版社,2009.

[14] 肖 晖,张玉清. Nessus 插件开发及实例[J]. 计算机工程,2007,33(2):241–243.

基于私有云泄漏的攻击方法研究

作者：[张伟](#)，[解争龙](#)，[ZHANG Wei](#)，[XIE Zheng-long](#)
作者单位：[咸阳师范学院 信息工程学院, 陕西 咸阳, 712000](#)
刊名：[计算机技术与发展](#)[ISTIC](#)
英文刊名：[Computer Technology and Development](#)
年，卷(期)：2015 (6)

引用本文格式：[张伟](#).[解争龙](#).[ZHANG Wei](#).[XIE Zheng-long](#) [基于私有云泄漏的攻击方法研究](#)[期刊论文]-[计算机技术与发展](#) 2015 (6)