

通信网恶意代码攻击效果评估研究

戴秋玉,王汝传,李 鹏

(南京邮电大学 计算机学院,江苏 南京 210003)

摘 要:网络攻击效果评估的目的是对网络攻击行为所能达到的攻击效果进行综合评判,从而发现网络中的薄弱点。文中提出了一个网络攻击与效果评估系统:首先恶意代码控制系统框架制定攻击策略对目标系统进行攻击;接着对网络攻击进行破坏能力预估,采用层次分析法定义指标,利用 Delphi 法确定指标权重,最后通过加权法综合效果评估值。三次攻击实验的实测结果表明该系统可以量化实际的网络攻击效果,从而准确评价网络攻击所达到的破坏程度。

关键词:攻击效果评估;破坏能力预估;网络攻击;SIP 协议

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2012)09-0243-03

Malware Attack Effect Evaluation against Communication Networks

DAI Qiu-yu, WANG Ru-chuan, LI Peng

(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: The aim of network attack effect evaluation is to evaluate the attack effect which network attacks achieve. As a result, network weak points can be found. A network attack and effect evaluation system is proposed. Firstly, the system control framework of malicious code works out and implies an attack strategy to the target computer. Secondly, destructive capacity pre-evaluation, indicator selection with analytic hierarchy process, index weight coefficient definition with Delphi method, and integrative evaluation value calculation with weighting method are executed. The results of there experiments indicate that the system can quantify the practical network attack effect. Thereby, the damage that network attacks do could be accurately evaluated.

Key words: attack effect evaluation; destructive capacity pre-evaluation; network attack; SIP protocol

0 引言

随着通信网络技术的飞速发展,网络业务数据化,网络技术 IP 分组化,基于软交换的下一代网络成为通信网演进的主流方向。这一变化给整个社会带来日新月异变化的同时,也带来了新的安全问题。恶意代码对通信网的破坏问题日益突出,恶意代码在通信网中具有快速传播、高度渗透、深入破坏的特点。此外恶意

代码本身也向多途径传播、综合性破坏、高度隐藏等方向发展^[1]。为了检验恶意代码攻击的有效性和网络系统的安全性,需要对网络攻击效果给出定性或定量的评估。由于攻击效果是攻击者作用于被攻击系统所产生的一种效应,因此研究网络攻击效果评估离不开被攻击系统的参与,就不可避免地需要构建相应的网络攻击系统^[2,3]。根据上面的分析,文中提出了一个网络攻击效果评估系统,完成从攻击到效果评估的一系列动作。网络攻击部分设计了一个恶意代码控制系统框架以及两类恶意代码程序。效果评估部分包括两方面:①破坏能力预估^[4];②破坏效果评估。

1 总体设计

1.1 网络攻击效果评估系统结构

本系统结合了恶意代码攻击与效果评估,其系统结构^[5]如图 1 所示。其中,信息搜集模块、攻击预案生成模块、攻击预案执行模块完成网络攻击策略的制定与执行,并将攻击效果日志上传,实现攻击的智能化、自动化与可控化;每个网络攻击预案作用于目标环境的攻击效果是由评估指标体系库中的相应指标来测度

收稿日期:2011-08-18;修回日期:2011-11-21

基金项目:国家自然科学基金(60973139,61170065,61171053,61003039,61003236,61103195);江苏省自然科学基金(BK2011755);江苏省科技支撑计划项目(BE2010197, BE2010198, BE2011844, BE2011189);省属高校自然科学研究重大项目(11KJA520001);江苏省高校自然科学基金基础研究项目(10KJB520013, 11KJB520014, 11KJB520016);高校科研成果产业化推进工程项目(JH2010-14, JHB2011-9);国家博士后基金(20100480048);江苏高校科技创新计划项目(CX10B-196Z, CX10B-200Z, CXZZ11-0405, CXZZ11-0406, CXZZ11-0409);教育部博士点基金(20103223120007, 20113223110002)

作者简介:戴秋玉(1987-),女,江苏无锡人,硕士研究生,研究方向为计算机网络和信息安全;王汝传,教授,博士生导师,研究方向是计算机软件、计算机网络、信息安全、移动代理和虚拟现实技术。

的;由于每个指标对网络攻击效果的贡献程度不同,所以指标权重确定模块根据攻击目的与作用对象来确定所选指标在整个效果评估中的权重;数据采集模块从反馈的攻击日志中分析出攻击前后的指标值;最后攻击效果计算模块对指标值进行归一化,以及计算综合评估结果值,验证攻击所达到的破坏程度。

1.2 恶意代码设计

(1) 恶意代码控制系统框架。

①控制中心部署用于挂载各个独立的恶意代码的 Web 服务器、分级破坏监控程序、存储目标环境信息以及攻击效果日志的 FTP 服务器、僵尸网络控制程序四大功能组件。

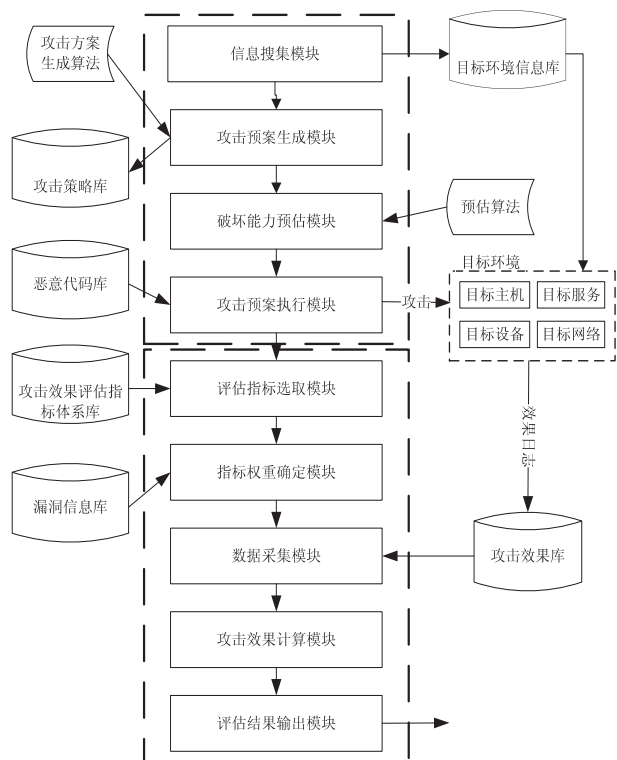


图1 网络攻击与效果评估系统结构

②受害主机植入具有下载功能的蠕虫程序、实施分级破坏的木马程序或僵尸程序,以及其他从控制中心 Web 服务器下载的恶意代码。

控制系统的工作过程:蠕虫传播、主动与控制中心通信、并进行信息搜集,木马下载攻击策略与原子攻击并执行,木马上传攻击日志,蠕虫/木马自删除。

(2) 通信监听攻击。

使用 WinPcap(Windows Packet Capture)编程^[6]来捕获 SIP(Session Initiation Protocol)^[7]应用程序的数据包从中获得 SIP 通信过程中的重要信息,如通信方的用户名、密码等。

(3) 拒绝服务类攻击。

通过攻击 SIP 服务器使其无法正常启动^[8]。具体方法是通过蠕虫控制 SIP 服务器,向植入 SIP 服务器

的木马下达删除 SIP 服务器注册表信息^[9]的攻击命令。

1.3 攻击效果评估

(1) 破坏能力预估。

文中提出的攻击破坏能力预估算法加上破坏能力分级策略主要完成对攻击方案的分析,定性评估攻击方案可以对目标计算机及网络实施的最大综合性破坏能力。

此算法首先设置一个标记变量并设初值为 0,然后遍历某一攻击方案中每一个原子攻击的后果集,并匹配分级策略中的攻击等级,若发现高等级的破坏效果,则修改标记变量为该攻击等级,直至遍历完攻击方案中的所有原子攻击。

(2) 破坏效果评估。

① 评估指标选取模块:根据攻击分类从指标体系库中选取合适的指标。

② 指标权重确定模块:使用 Delphi 法^[10]确定各指标权重,区分其对攻击效果的贡献程度。

③ 数据采集模块:从搜集到的目标信息以及反馈的攻击日志中分析攻击前后的指标值。

④ 攻击效果计算模块:一是将测试指标归一化,二是计算综合评估结果值。

· 指标归一化:消除原始测量数据之间由于评估指标的量纲不同而存在的差异。

对于 CPU 利用率等指标,考虑到其原先性能对攻击效果影响较大,因此指标的归一化值

$$E_i = (A_i - B_i) / (1 - B_i) \quad (1)$$

B_i 为攻击前一刻采集的指标值, A_i 为攻击后指标值, i 为第 i 次的采样值。若进行了 n 次采集,指标均值

$$\bar{E} = \frac{1}{n} \sum_{i=1}^n E_i (i = 1, 2, \dots, n) \quad (2)$$

对于攻击时间这类负向性指标,归一化值

$$E = \max T - \bar{T} / \max T - \min T \quad (3)$$

对于响应延迟这类正向性指标,归一化值

$$E = \bar{T} - \min T / \max T - \min T \quad (4)$$

另外,对某些定性指标值采用预值法对其归一化。

· 网络攻击效果综合:对于简单攻击来说,得到上述指标归一化值后就可以使用公式(5)进行综合,其中 I_i 表示第 i 个评估项的评估结果值(归一化的), ω_i 是其对应的权值。

$$Q = \sum_{i=1}^n \omega_i I_i \text{ 其中, } i = 1, 2, \dots, n; \omega_i \geq 0; \sum_{i=1}^n \omega_i = 1 \quad (5)$$

对于复杂的网络攻击(如组合攻击),一个攻击预案通常是一个原子攻击序列。假设共有 n 个原子攻击,分别记作 $\{A_1, A_2, \dots, A_n\}$, 其权重系数向量 $\omega = \{$

$\omega_1, \omega_2, \dots, \omega_n$ 。原子攻击 A_k 下包含 m_k 个评估指标, 分别记作 $\{C_1^{(k)}, C_2^{(k)}, \dots, C_{m_k}^{(k)}\} (k = 1, 2, \dots, n)$, 其中, $\omega_i^{(k)}$ 表示评估指标 $C_i^{(k)}$ 的权重系数。则每个评估指标相对于攻击目标权重系数

$$W_i^{(k)} = \omega_i^{(k)} * \omega_i (i = 1, 2, \dots, m_k; k = 1, 2, \dots, n)$$

(6)

将公式(6)中得到的 $W_i^{(k)}$ 带入公式(5)的 ω_i 就可以得到组合攻击下的网络攻击效果的综合评估结果^[11]。

2 测试与分析

通信仿真平台。

文中的实验系统是一个基于 SIP 协议的通信平台, SIP 协议凭借其简单、易于扩展、便于实现的特点, 目前在基于软交换的通信网中地位越来越突出, 而且它很大程度上借鉴了其他各中广泛存在的 Internet 协议, 将很好地解决通信网络与互联网的融合, 并且市场上已经有很多支持 SIP 的客户端和服务端软件及软交换设备, 所以文中使用的基于 SIP 的通信网络作为实验平台具有很好的代表性^[12]。通信仿真平台部署如图 2 所示。

首先使用预估算法对制定的攻击策略进行预估, 得出此次攻击效果的定性描述属于攻击级二; 然后对其进行了测试、数据采集与归一化处理得到表 1 的结果。

而三个攻击对总目标的权重如下: $\omega = (0.2, 0.3, 0.5)$ 。

利用公式(1)、(2)得到该网络攻击场景下的攻击效果的综合评估结果为: $Q = 0.5206$ 。

从 Q 值可以直观地评判此次网络攻击对目标环境

的破坏程度, 攻击者可以根据该评估结果决定进一步的动作。

表 1 网络攻击效果评估指标测量数据

攻击类型	评估指标	测量结果	归一化值	权值 $\omega_i^{(k)}$
获取信息 (静态)	获取的信息量 I_{11}	网络环境、驱动、服务、注册表、组策略及补丁、应用程序等	0.8000	0.4
	信息正确率 I_{12}	100%	1.0000	0.3
	攻击时间 I_{14}	20 秒	0.6000	0.3
获取信息 (动态)	获取信息率 I_{21}	92.02%	0.6461	0.2
	信息的有用性 I_{22}	通信方 IP 地址、端口、路由 IP 地址、通信内容、用户名、认证情况	0.7000	0.4
	存储空间占用率 I_{23}	0.05%	0.0005	0.1
	隐蔽性 I_{24}	文件隐藏、进程隐藏、注册表隐藏	0.9000	0.2
	攻击时间 I_{25}	144 秒	0.8000	0.1
拒绝服务	响应延迟 I_{31}	46 秒	0.6667	0.2
	网络带宽占用率 I_{32}	0.3%	0.003	0.2
	CPU 占用率 I_{33}	43.68%	0.4368	0.2
	内存占用率 I_{34}	6.45%	0.0645	0.1
	恢复难度 I_{35}	重新导入注册表项	0.700	0.1
	攻击时间 I_{36}	23 秒	0.5000	0.1
	恢复时间 I_{37}	207 秒	0.5385	0.1

3 结束语

本课题在分析通信网的安全隐患的基础上, 实现了对通信网的恶意代码攻击, 以及对恶意代码攻击进行多方面控制的控制系统框架; 同时通过预估和评估两部分对恶意代码攻击进行定性定量评估。

文中提出的恶意代码攻击效果评估系统可以完成对目标系统的攻击、反馈以及攻击效果的定性定量评估, 但是还有待改善。文中制定的攻击策略比较简单, 攻击类型比较单一, 此外攻击效果评估指标体系还不够完备, 不能完全涵盖所有的网络攻击行为。可以从这几方面展开进一步研究。

参考文献:

[1] Robben S. White Open Problems in Computer Virus Research[C]//Virus Bulletin Conference. [s. l.]:[s. n.], 2001:101-105.

[2] 张义荣, 鲜明, 赵志超, 等. 计算机网络攻击效果评估研究[J]. 国防科技大学学报, 2002, 24(5):24-28.

[3] 张义荣, 鲜明, 王国玉. 一种基于网络熵的计算机网络攻击效果定量评估方法[J]. 通信学报, 2004, 25(11):158-165.

[4] 曹莹莹. 恶意代码的控制技术研究[J]. 计算机技术与发展, 2010, 20(8):128-132.

[5] 汪生, 孙乐昌. 网络攻击效果评估系统的研究与实现-基于指标体系[J]. 计算机工程与应用, 2005(34):149-153.

[6] The WinPcap Team. WinPcap 中文技术文

(下转第 249 页)

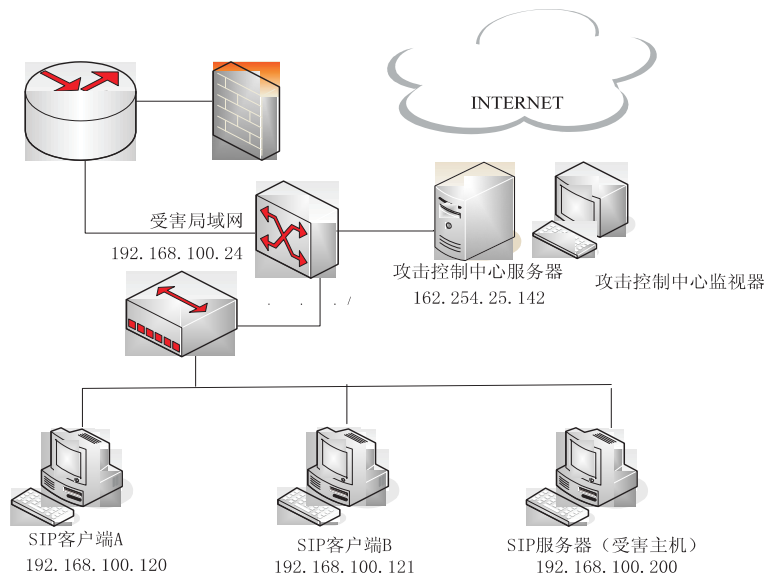


图 2 通信平台实验部署图

而测试后的软件失效为:

$$Risk' = \sum_{i=1}^4 w(S_i) (N \times p_{S_i} + \sum_{j=0}^4 d_{i,j}) \tag{11}$$

经过软件安全性测试,软件安全性改善可用风险降低值来表示,为:

$$\Delta Risk = \sum_{i=1}^4 (w(S_i) \sum_{j=0}^4 d_{i,j}) = \sum_{i=1}^4 \sum_{j=0}^4 w(S_i) d_{i,j} \tag{12}$$

定义带权值的软件缺陷严重度变化矩阵为:

$$DW = \begin{pmatrix} w(S_0) & 0 & 0 & 0 & 0 \\ 0 & w(S_1) & 0 & 0 & 0 \\ 0 & 0 & w(S_2) & 0 & 0 \\ 0 & 0 & 0 & w(S_3) & 0 \\ 0 & 0 & 0 & 0 & w(S_4) \end{pmatrix} \times D = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ -w(S_1)d_{0,1} & w(S_1)d_{1,1} & w(S_1)d_{1,2} & w(S_1)d_{1,3} & w(S_1)d_{1,4} \\ -w(S_2)d_{0,2} & -w(S_2)d_{1,2} & w(S_2)d_{2,2} & w(S_2)d_{2,3} & w(S_2)d_{2,4} \\ -w(S_3)d_{0,3} & -w(S_3)d_{1,3} & -w(S_3)d_{2,3} & w(S_3)d_{3,3} & w(S_3)d_{3,4} \\ -w(S_4)d_{0,4} & -w(S_4)d_{1,4} & -w(S_4)d_{2,4} & -w(S_4)d_{3,4} & w(S_4)d_{4,4} \end{pmatrix}$$

则,软件安全性改善值 $\Delta Risk$ 为矩阵 DW 所有元素和的绝对值。

4 结束语

将 JM 模型用于软件安全性测评,对其作如下改进:注入软件失效严重度参数;测试过程中,增加了对已发现的软件错误(失效)进行严重度降级的处理方式。改进后的 JM 模型更符合软件安全性的定义,并易于工程实践。在改进的 JM 模型基础上所计算的软件安全可靠度,是专门针对软件安全性的一个度量指标,该指标体现了软件安全的可能性。

利用 JM 模型中估算的软件错误总数,及相关测试数据,可以计算软件风险值。软件风险定义不但刻

画了导致事故的危险发生的可能性(概率),还考虑了不同的事故代价(事故后果的严重程度)。这与软件安全性增长测试的目的,减少软件事故风险是相一致的。该项指标更为直观地反映软件的安全性。软件安全性设计和软件安全性测试的最终目标便是减少因为软件因素而导致灾难性事故的风险^[12]。带权值的软件缺陷严重度变化矩阵 DW 直接反映了系统安全性测试的能力,即通过测试软件安全是否得到改善以及改善力度。

参考文献:

[1] NASA-GB-8719. 13B. Software Safety[S]. Washington: NASA,2004.

[2] 樊晓光,褚文奎,张凤鸣. 软件安全性研究综述[J]. 计算机科学,2011(5):14-19.

[3] GJB/Z 102-97. 软件可靠性和安全性设计准则[S]. 北京: 国家技术工业委员会,1997.

[4] 李烈彪,李仙. 计算机系统的可靠性技术[J]. 计算机技术与发展,2007,17(11):148-150.

[5] 胡海宏,沈元隆. 基于用户要求并考虑软件失效的费用模型[J]. 计算机技术与发展,2011,21(7):91-95.

[6] GJB-900-90. 系统安全性通用大纲[S]. 北京:国家技术工业委员会,1991.

[7] Jelinski Z, Moranda P B. Software reliability research[M]// Statistical computer performance evaluation. New York: Academic Press,1972:465-484.

[8] John D M. Software Reliability Engineering[M]. 北京:机械工业出版社,2003.

[9] 楼俊钢,江建慧,帅春燕,等. 软件可靠性模型研究进展[J]. 计算机科学,2010(9):19-25.

[10] 谈维新,沈元隆. 考虑测试效率的软件可靠性模型研究[J]. 计算机技术与发展,2011,21(8):73-76.

[11] 郑垒,沈元隆. 考虑非理想排错过程的软件可靠性模型[J]. 计算机技术与发展,2011,21(8):118-122.

[12] Ericson C A. Hazard analysis technique for system safety[M]. Hoboken(USA):John Wiley & Sons Inc,2005.

(上接第 245 页)

档4.0.1[EB/OL]. [2007-07-23]. [http://www. WinPeap. org. cn/](http://www.WinPeap.org.cn/).

[7] 徐培文. 软交换与 SIP 实用技术[M]. 北京:机械工业出版社,2007.

[8] Sisalem D, Kuthan J, Ehlert S. Denial of service attacks targeting a SIP VOIP infrastructure: attack scenavius and prevention mechanisms[J]. Network IEEE, 2006,20(5):26-31.

[9] 吴坤鸿,乐宏彦. 反 rootkit 的内核完整性检测与恢复技术[J]. 计算机工程,2008(21):129-131.

[10] 胡影,郑康锋,杨义先. 一种基于原子功能的网络攻击效果评估指标体系[J]. 计算机工程与科学,2008,30(10):1-4.

[11] Zhang Lijuan, Cao Yan, Wang Qingxian. Fuzzy-AHP 法在网络攻击效果评估中的应用[J]. 北京邮电大学学报,2006,29(1):124-127.

[12] Choudhary A R. Security-auditing in a Softswitch[C]//Information Assurance Workshop, 2003. [s. l.]: IEEE Systems, Man and Cybernetics Society, 2003:292-293.

通信网恶意代码攻击效果评估研究

作者：[戴秋玉](#)，[王汝传](#)，[李鹏](#)
作者单位：[南京邮电大学 计算机学院, 江苏 南京 210003](#)
刊名：[计算机技术与发展](#)
英文刊名：[Computer Technology and Development](#)
年，卷(期)：2012(9)

本文链接：http://d.g.wanfangdata.com.cn/Periodical_wjfz201209064.aspx