文章编号:1001 - 2486(2002)05 - 0024 - 05

计算机网络攻击效果评估技术研究*

张义荣,鲜 明,赵志超,肖顺平,王国玉
(国防科技大学电子科学与工程学院,湖南 长沙 410073)

摘 要:计算机网络攻击效果评估技术是信息系统安全评估中一个重要而具有挑战性的课题。目前,相关的理论尚不成熟,有关的研究报道较少。简要总结了当前已经存在的主要信息安全的评估方法,在此基础上,从便于实际度量和计算的角度出发,提出了基于网络信息熵的评估技术、基于系统安全层次分析的安全评估框架和基于指标分析的网络攻击效果综合评估技术等三种评估模型,并分析了各自在使用中应注意的问题。

关键词:网络安全;攻击效果评估;网络熵;安全指标;层次分析法(AHP)
中图分类号:TP393 文献标识码:A

A Study on the Evaluation Technology of the Attack Effect of Computer Networks

ZHANG Yi-rong, XIAN Ming, ZHAO Zhi-chao, XIAO Shun-ping, WANG Guo-yu
(College of Electronic Science and Engineering, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: The evaluation technology of the Attack Effect of computer networks is an important and challenging subject of security evaluation in information systems. Nowadays, corresponding theory is not mature and correlative research reports are few. In this paper several currently primary evaluation techniques of information security are concisely analyzed. Then three evaluation models, i.e., the evaluation technique based on network information entropy, the security evaluation framework based on analytical hierarchy and the synthetical evaluation technique based on analytical indexes, are presented in order to conveniently measure and estimate the attack effect. Finally, some problems which must be paid attention to in practice are pointed out.

Key words: network security; attack effect evaluation; network entropy; security index; Analytical Hierarchy Process (AHP)

随着信息技术的广泛应用,对信息技术产品和信息网络系统的依赖性也越来越大,信息安全问题日益突出。如何对计算机网络系统的安全特性进行评估成为一个迫切而具有挑战性的课题。

1 信息系统安全评估技术概述

关于网络信息系统的安全评估,目前还没有形成形式化的评估理论和方法,不过存在着多种多样的安全评估的具体实践方式。现有的安全评估方式可以大致归结为以下四类[1]:安全审计、风险分析[2]、系统安全工程能力成熟度模型(SSE-CMM)[3,4]和安全测评等。以安全审计概念为核心的安全评估思想认为可以通过关于安全的最佳实践(Best Practices)实施与否及其程度来评估 IT 系统的安全性。这一类相关的模型包括美国信息系统审计和控制协会的 COBIT、国际标准化组织(ISO)的 ISO 17799[5]规范等。风险分析模型是从风险控制角度进行的信息安全评估。它通过对要保护的 IT 资产存在的安全威胁、漏洞以及这些安全威胁、漏洞对资产可能造成的损失进行计算,经过数学的概率统计得出网络系统安全性的衡量。现有的大部分通用的信息安全标准,如 ISO 17799、ISO 13335 等,其核心思想都是基于风险的安全理念。系统工程安全能力成熟度模型(SSE-CMM)认为可以通过过程(Process)来保证安

* 收稿日期:2002 - 05 - 27
作者简介:张义荣(1977—),男,博士生。

全。SSE-CMM 的基本思想是:通过对安全工程过程进行管理的途径,将系统安全工程转变为一个定义完好的、成熟的、可测量的过程。它将安全能力划分为五个等级,从低到高,低等级是不成熟的、难以控制的,中等级别是可管理的、可控的,高级别是可量化的、可测量的。SSE-CMM 是一种动态的、螺旋式上升的模型。安全测评则更多地从安全技术、功能和机制角度来进行信息系统的安全评估,这类评估规范有欧洲的 ITSEC、加拿大的 CTCPEC 和 ISO 的信息技术安全评估通用准则[6~8](简称 CC,即 ISO 15408 规范)等。

上述各种安全评估思想都是从信息系统安全的某一个侧面出发,如技术、管理、过程、人员等,着重于评估网络系统安全某一方面的实践规范。在操作上主观随意性较强,其评估过程主要依靠测试者的技术水平和对网络系统的了解程度,缺乏统一的、系统化的安全评估框架,很多评估准则和指标难以量化。因此,本文拟从计算机网络攻击效果评估的角度来对网络的安全特性进行刻画。网络攻击效果评估技术在信息系统的安全评估过程中具有重要意义:一方面,网络构建部门通过对信息网络的模拟攻击和自我评估可以检验系统的安全特性;另一方面,在反击来自敌方的恶意攻击时,网络攻击效果评估技术可以为网络反击样式和反击强度提供合适的应对策略。

由于目前国内外关于网络攻击效果评估技术的研究还不多,已提出的信息系统安全评估的准则和标准在理论上还不成熟。因此,本文着眼于从评估准则和评估指标两个方面提出一些易于度量和计算的评估模型,主要有基于网络信息熵的评估技术、基于系统安全层次分析的安全评估框架和基于指标分析的网络攻击效果综合评估技术等。

2 本文提出的主要网络攻击效果评估技术

2.1 基于网络信息熵的攻击效果评估技术

为了有效评价网络攻击效果,首先要选择恰当的标准对网络的安全性能进行形式化描述。网络安全一般应考虑以下原则:完整性原则、保密性原则、可靠性原则、可用性准则。在评估过程中,可以把被攻击目标的完整性、保密性、可靠性和可用性作为其安全性的一个量度,而攻击前后的安全性差值则可以作为攻击效果的一个评价标准。

如何对网络的上述各项指标进行度量,现在国际上还没有一个通用的标准。利用信息论中的"熵"的概念,现提出评价网络性能的"网络熵"理论。"网络熵"是对网络安全性能的一种描述,网络熵值越小(但不能为负数),表明对该网络系统的了解越少,该网络系统的稳定性越好。对于网络的某一项指标来说,其熵值可以定义为:$H_i = -\log_2 V_i$,V_i 为网络此项指标的归一化的性能参数。显然,网络信息系统受到攻击后,其信息的不确定性增大,系统稳定性变差,熵值应该增加。因此,可采用"熵差"$\Delta H = -\log_2(V_2/V_1)$对攻击效果进行描述。式中,$V_1$ 为网络系统原来的归一化性能参数(可以取为传输速率、保密系数等),V_2 为网络受攻击后的归一化性能参数。经研究发现,对网络安全性能影响较大的主要有以下几项指标:(1)网络数据流量;(2)数据保密性;(3)数据可靠性;(4)数据完整性;(5)延迟时间。现以网络数据流量指标为例,介绍熵差的计算方法。

设测得网络受攻击前的数据流量为 V_1,受攻击后的数据流量为 V_2,把它们进行归一化,得归一化的数据流量分别为:V_1/V_g,V_2/V_g,其中 V_g 为网络的峰值数据流量,可以保证 $0 \leqslant V_2 \leqslant V_1 \leqslant V_g$。则在网络数据流量这项指标上的攻击效果为:

$$\Delta H = -\log_2(V_2/V_g) - (-\log_2(V_1/V_g)) = -\log_2(V_2/V_1)$$

显然,若 $V_2 = V_1$,则 $\Delta H = 0$,表明攻击未取得任何效果;V_2 下降得越厉害,表明攻击的效果越明显,ΔH 也越大,可见 ΔH 确实可以作为攻击效果的一种描述。

网络的整体性能即为以上各项指标的加权和 $H = \sum_{i=1}^{n} \omega_i \times H_i$。相应地,总的攻击效果可表示为 $\Delta H = \sum_{i=1}^{n} \omega_i \times \Delta H_i$。其中 n 为衡量网络性能的指标个数,ω_i 为第 i 项指标的权重。ω_i 依攻击目的和网络环境的不同而定,有以下原则:以窃取敌方信息为目的,则主要考虑对方数据保密性的损失;以篡改敌方信息

为目的,则主要考虑对方数据完整性和可靠性的损失;以破坏扰乱敌军信息系统的正常运行为目的,则主要考虑对方数据可用性的损失。

评估模型建立以后,主要的问题是如何选取各项指标的性能参数 V_i。只有选择恰当的参数,才能对网络攻击的效果做出合理的、客观的评估。对于有些指标(如数据流量等),V_i 的选择较容易,而对于某些指标(如数据的保密性等),则很难找到一个适当的参数进行描述。只有在实践中摸索,通过编制一些必要的工具软件,并经过反复的仿真试验,才可能找到一个有效的评价标准。

2.2 基于系统安全层次分析的评估框架

对计算机网络系统攻击效果的评估,就是对攻击前后计算机网络的安全特征的变化进行评估。安全特征一般可以从完整性、保密性、可靠性、可用性、健壮性等方面来表征。从安全特性的角度出发,可以分析得出如图1所示的安全评估分层框架。最高层是目标层,它是用户关注的主要安全特征;第二层为安全准则层,包括许多安全子准则,它体现安全特性的基本要求;最底层为安全指标层,它是对具体安全属性的测度,通常需要量化。

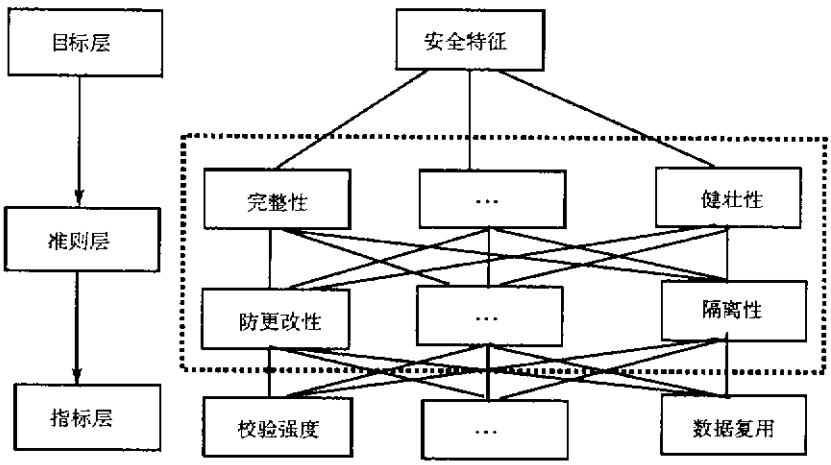

图1 安全评估分层框架

Fig.1 Hierarchy framework of security evaluation

根据对安全机制的深入分析,可逐步确定相应的安全准则。每一安全准则又可进一步细化为许多安全子准则,例如完整性准则可以由防更改性、多样性、隔离性、可审计性等来描述;健壮性准则可以由容错性、模块性、简单性等来描述。同样地,每一安全子准则又可以由许多安全指标来刻画。例如防更改性可以由物理难度、校验强度和自我验证等来描述;隔离性可以由代码隔离、数据隔离、数据复用、环境隔离和可中断性等来描述。其中,指标的选取和量化可以结合 Delphi 法通过建立两两比较判断矩阵加以确定。对单项指标和系统安全能力的综合评估采用层次分析法(Analytical Hierarchy Process)得出。在得出单项指标的得分后,系统安全能力的综合评估可由式子 $S=\sum_{i=1}^{n}\omega_i f(X_i)$ 来计算,式中 ω_i 为第 i 项指标的权重,$f(X_i)$为第 i 项指标的评分。假设第 i 项指标的最低得分为 C_i,则系统安全能力的最低得分为 $S^*=\sum_{i=1}^{n}\omega_i C_i$。于是根据对各单项指标的评价,也可以对系统安全的综合评估划分若干等级。

当计算机网络系统受到攻击时,系统安全能力的综合评估模型 $S=\sum_{i=1}^{n}\omega_i f(X_i)$ 中的某些项指标的得分将降低,从而使得系统安全评估的综合得分值减少,或者说系统安全等级将降低。因此,可以通过网络系统安全综合得分或安全等级的变化来对网络攻击的效果进行定量或定性评价。

2.3 基于指标分析的网络攻击效果综合评估技术

为提高网络攻击的有效性,还应遵循以下原则,并采用相应的数学测度模型予以实施。

·整体性原则:评估攻击对单个网络主机的效能,首先要估计被攻击的整个网络的整体性能在遭受攻击以后的变化情况。

·时效性原则:时效性就是当攻击网络的某个节点时,应是该节点到达数据包或分组最多的时间。这时攻击对该节点性能的降低是最显著的。

·节点和路由优选原则:在确定攻击目标时,应对网络节点和路由段优选。即选择重要性最高的节点和使用概率最高的路由(链路)段。只有这样才能达到对整个信息网络最有效的迟滞和性能降低。

基于整个信息网的攻击效能测度从上述原则出发,应用排队论的基本原理,可考虑采用以下基于整个信息网的攻击效能的评估模型。

a)信息网全网传信总延时

使目标信息子网所传送的各个报文或分组产生最大的延时,是对信息网络攻击的直接战术目的。衡量这个效果可采用'全网传送总延时'这一性能测度模型。设它为 T_d,则其计算公式为:

$$T_d = \sum_{j=1}^{N} \sum_{k=1}^{M(j)} T_{jk}$$

式中 j 为全网的 N 个节点中第 j 个节点;T_{jk} 为第 j 个节点的全部 M 个(M 是 j 的函数)相邻节点至其相邻节点路由段的延迟。

b)重要节点传信延时

重要节点传信延时对网络性能的降低要高于普通节点。设为 T_{hd},其计算公式为

$$T_{hd} = \sum_{j=1}^{N_1} \sum_{k=1}^{M(j)} T_{jk}$$

式中 $j = 1, \cdots, N_1$ 为重要节点序号。

c)网络延迟抖动

网络延迟抖动是指网络平均延迟变化的时间量。网络延迟抖动是衡量多媒体通信网络的重要指标,它关系到网络所提供的服务质量(QoS)。

d)网络和节点吞吐量

网络(节点)吞吐量是指单位时间内(通常为 s)通信网络(节点之间)成功传送的无差错的数据包的数量。当网络发生故障或受到攻击时,网络(或重要节点)的吞吐量必然减少,因此可用作信息网的攻击效能的评估模型。

e)每节点路由表更换的周期

每个路由器节点的路由表,是为保证各节点都是可到达的,且每个路由器都随时掌握其它路由器的状态而设置的。以 TCP/IP 协议为例,它约定每隔一定时间播发一次(与路由协议有关),若超过指定时间某路由器未发出更新的路由表,则表明该路由器不可到达,且很可能是攻击引起后者主要路由中断。

f)系统服务响应时间

系统从接收到请求服务的信号到提供该服务所需的时间。一般说某个网络的服务响应时间都是指其统计平均值。这个值随网络系统的负载变化而变化,负载越大,其值也越大。

g)系统恢复时间

系统从发生故障,到恢复故障前状态,并重新提供服务所需时间。系统恢复时间与系统本身结构组成及操作员的水平都有关。

当然,在建立和分析整个信息网的攻击效能模型时,由于实际评估的网络对象不同,网络承载的业务有所差别,网络提供服务的偏重也有所差异,因此上述评估模型也不应该是一成不变的,而应该根据实际情况有所侧重。比如对于以数据传输业务为主的网络,应主要考虑攻击前后网络(节点)吞吐率、链路利用率和系统服务响应时间等指标的变化。对于以多媒体业务为主的通信网络,应主要从网络(重要节点)传信总延时、链路利用率和网络延迟抖动等指标来对攻击效果建模。

3 结束语

计算机网络攻击效果评估技术是网络安全综合评估技术的重要研究内容。本文提出的几种安全评估模型,包括基于网络信息熵的评估技术、基于系统安全层次分析的安全评估框架和基于指标分析的网络攻击效果综合评估技术,与目前存在的其它安全评估体系相比较,它们的共同特点是评估指标便于度量或计算,可以从定性和定量两个方面对网络攻击效果进行评估,可操作性较强。

当然,从实践角度来看,为了充分利用文中提出的各种评估模型,还有大量复杂的工作要做。比如具体安全指标的选取和测度,安全准则的分析,系统安全等级的划分等,这些都是今后的研究中要着力解决的问题。

参考文献:

[1] 江常青,吴世忠. 一种信息系统安全测度的框架[J]. 信息安全与通信保密,2002,1:26-28.

[2] Canada Communications Security Establishment. Canadian Trusted Computer Product Evaluation Criteria (V3.0e) [S]. 1993.

[3] System Security Engineering Capability Maturity Model (SSE-CMM) [EB]. http://www.se-cat.com/ download/ download.html, 2000-09-06.

[4] SSE-CMM Author Group. SSE-CMM (V2.0b) [M]. 1999.

[5] The International Organization for Standardization. Information Technology-Code of Practice for Information Security Management[S], ISO/IEC 17799:2000(E), 2000.

[6] The International Organization for Standardization. Common Criteria for Information Technology Security Evaluation-Part 1: Introduction and General Model[S], ISO/IEC 15408-1:1999(E), 1999.

[7] The International Organization for Standardization. Common Criteria for Information Technology Security Evaluation-Part 2: Security Function Requirements[S], ISO/IEC 15408-2:1999(E), 1999.

[8] The International Organization for Standardization. Common Criteria for Information Technology Security Evaluation-Part 3: Security Assurance Requirements[S], ISO/IEC 15408-3:1999(E), 1999.