网络系统生存性分析研究

王红艳　刘向东
(中国航天科工集团二院 706 所　　北京　100854)

〔摘要〕 采用随机点过程模拟网络攻击,根据系统对攻击可能导致的状态建立了网络系统状态转换概率矩阵,从而基于系统对攻击的反应建立了网络系统生存性的数学分析方法。
〔关键词〕 网络系统　生存性　转换概率　　〔中图分类号〕 TP309.2　TP393.08
〔文章标识码〕 A　　〔文章编号〕 1000-7857(2005)04-0007-03

A STUDY ON THE SURVIVABILITY OF WEB SYSTEMS

WANG Hong-yan　LIU Xiang-dong
(Institute 706, The Second Academy of China Aerospace Science and Industry Corp, Beijing 100854, China)

Abstract: The Stochastic Point Process was used to simulate attack processes that network systems might suffer from, and the transition probabilities matrix was constructed to simulate the impact of attacks on a certain system. By varying the state of system in the simulation, an analysis method to quantitate survivability of network systems was developed.
Key Words: web system, survivability, transition probability　　**CLC Numbers**: TP309.2　TP393.08
Document Code: A　　**Aticle ID:** 1000-7857(2005)04-0007-03

1 引言

随着信息技术的快速发展，信息网络系统的生存性已逐步成为关注的焦点，因为网络系统之中存在着各种各样需要解决的问题[1]。网络系统生存性是指信息网络系统面对攻击时的反应能力和遭受攻击后的恢复能力。在日益开放的网络环境中,不可能存在绝对完美的网络安全防御机制,我们所要做的是采取尽可能有效的网络安全防御措施在尽可能大的程度上抵制网络安全面临的威胁。工商企业或组织机构只能基于其需求、财力以及实际系统面临的潜在威胁,尽可能使系统生存能力达到一个最理想的期望值。评估一个系统的生存性对系统的安全决策具有重要的指导意义。通过测评分析网络系统当前的设计模式和防御机制对

收稿日期: 2005-03-01
作者简介: 王红艳,女,1977~ ;北京市 142 信箱 406 分箱 4 号中国航天科工集团二院 706 所,工程师, 主要研究方向为网络安全技术;
E-mail:prcwhy@sina.com

(2) EC 为 SYN Flood 类攻击事件。

外部特征需满足:

(1) 时序特征,即 n_2 阶段内事件与 n_1 阶段内的所有事件满足如下时序关系, n_2·succeeds·n_1;

(2) 条件特征,即

n_2.Pre_Info=n_1.Post_Info=GetInfo (Victim(IP,Port)),

n_2.Post_Info=Victim (Port, Active, Non_active)(在已获取端口信息的基础上进行端口攻击)。

同理,可继续归纳 n_3、n_4 阶段的内部和外部特征,以形成特征的规则描述。在检测时,通过分析一定时间段内的网络行为, 当网络事件或攻击事件符合上述阶段的内部特征时,将其加入该阶段。据此形成的各阶段若同时满足阶段的外部特征(时序特征、条件特征)时,即可认为是一次协同攻击。

从上述描述可以看出, 协同攻击是一个有步骤的行为集合,这个集合中的每一步骤之间存在着严格的时序关系。协同攻击检测的关键之处就在于分析协同攻击各阶段的攻击特征和时序关系, 从而形成特征集, 以此作为检测的判据。收集被检测网段在一定时间内的网络行为,先通过阶段特征将网络行为归并为阶段动作集, 然后匹配该阶段的时序关系,从而完成对协同攻击的检测。

4 小结

在协同攻击的检测中, 本文将其划分为功能层次上的检测和时序层次的检测,通过两种检测方式的协作(时序检测需要功能检测的协作)和结果的比对,可以对协同攻击作出有效的判别。

参考文献(References)

[1] 胡昌振. 网络入侵检测的误警问题探讨[J]. 信息安全与通信保密,2003(8):20~22
[2] 经小川,胡昌振,谭惠民. 基于关联序列分析的协同攻击检测技术研究[J]. 武汉理工大学学报,2004,26(6):78~82
[3] John Green. Analysis Techniques for Detecting Coordinated Attacks and Probes[C]. Usenix Networking'99
[4] 胡昌振. 信息安全的概念及方法论探讨 [J]. 科技导报,2004,22(3):18~21
[5] Peng Ning. Abstraction-based Intrusion Detection in Distributed Environments[M]. George Mason University, 2001

(责任编辑　肖庆山)

系统生存性的影响,就可以量体裁衣,制定一个适合实际系统的最佳策略。

鉴于目前仍没有网络系统生存能力的评估标准[1],本文借鉴了 Soumyo[2]等人的观点,采用网络系统生存性的分析方法,作为生存性评估研究的基础。企业管理者可以通过权衡实际系统的配置和系统生存性能之间的关系,制定适合自己需要的较理想的网络系统安全策略。

2 网络系统生存性的分析方法

2.1 分析步骤

整个分析过程分 3 个步骤。如图 1 所示。(1)从遭受攻击的系统或站点出发,首先建立一个攻击过程模型;网络攻击是随机的,因此可以采用随机点过程来模拟攻击过程。(2)其次建立系统的反应模型。系统的生存性反映系统在面临攻击时的反应能力,而系统的反应表现为由一个状态转变为另一个状态,因此系统反应的数学模型可表达为系统以某个可能的状态作为终结的转换概率矩阵;由于所遭受攻击的类型和网络系统的配置等因素直接影响网络系统对遭受攻击的承受能力,因此攻击类型和系统配置是影响概率转换矩阵中概率取值的重要因素。其中系统配置包括系统的设计模式和系统的防御机制。(3)最后进行系统生存性能分析,通过分析遭受攻击后的系统的终结状态,采用数学公式将网络系统生存性能量化。

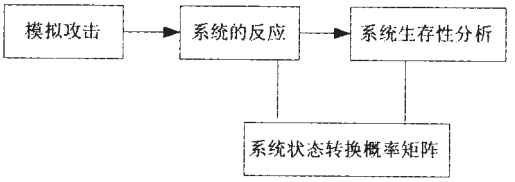


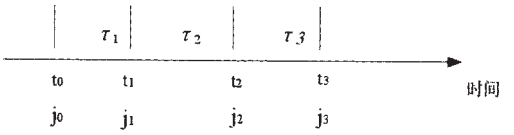
图 1 分析方法示意图

2.2 所用符号的说明

(1) i, j 表示攻击类型,$i, j \in \{J\}$。这里的攻击是指未授权的进攻事件。事件发生顺序按字母顺序排列。(2) $P(j)$ 表示 j 类型攻击发生的概率。(3) $\tau\ (i, j)$=攻击 i 和 j 发生的时间间隔。(4) a 为事件发生速率=$1/\tau$。(5) r, s 表示系统状态,$r, s \in \{S\}$。(6) d 表示系统设计模式,$d \in \{D\}$。(7) m 表示系统的防御机制,$m \in \{M\}$。(8) 系统配置=系统设计模式× 防御机制,即 $\{D\times M\}$。(9) T 为转换概率矩阵,是系统反应的一种表现形式,T 中元素$\{p(r, s)\}$表示系统从 r 状态转变为 s 状态的概率,$\{p(r, s)\}$是关于 i, j, d, m 的函数。(10) n 表示同一攻击对多个站点同时发起的数量。

2.3 攻击过程模拟模型

用随机点过程模型化攻击过程。随机点表示随机发生的攻击事件,每个随机点都有一个标记,表示该随机点所代表的攻击类型。如图 2 所示。第 k 个攻击的发生时间记为 tk,攻击类型表示为 jk,jk 是一个特定区间的值。生存性所考虑的网络环境是无界的,在无界的网络环境中模拟攻击过程,攻击类型的描述应该是多方面的,如攻击的严重程度、单个攻击或多个攻击同时发生的可能性,等等。因此,攻击类型的数学表现形式应是关于攻击严重程度和攻击数量的矢量积,记为$\{J\times N\}$。由于没有攻击数量的统计数据可供参考,本文中对攻击类型只考虑攻击的严重程度,即$\{J\}$。



图中:τ 为攻击时间间隔,t 为攻击发生的时间,j 为攻击类型
图 2 随机点过程(攻击过程模拟模型)

随机点过程可表示为$\{x(t): t \in T\}$,T 是过程的集合,随机变量 t 的取值表示时间,$T\subset R$, 为连续参数。$\{x(t): t \in T\}$是完全联合分布函数:

$$P_{x(t1),x(t2),\cdots,x(tk)}(X1, X2, \cdots, Xk)=Pr(x(t1)\leqslant X1, x(t2)\leqslant X2, \cdots, x(tk)\leqslant Xk)$$

对于有穷集合$(t1, t2, \cdots tk)$,$\{X1, X2, \cdots, Xk\}$,随机变量表示为 $x(t1), x(t2), \cdots, x(tk)$。这里 $t_i \in T$, $Xi \in R$(i=1, 2, $\cdots$, k)。$\{N(t): t \geqslant t_0\}$表示在时间范围$[t_0, t]$发生的攻击事件的数量。独立连续随机变量的特征函数为:

$$\Phi x(iv)=E[\exp\{i\int_{t0}^{T} v'(t)\}], t_0\leqslant T\leqslant 0$$ 是任意矢量函数,表示转换运算,$i=\sqrt{-1}$。关于攻击事件时间间隔的概率密度函数记为 $f(t)$:$f(t)=Pr\{t\leq\tau\leq t+dt\}$。如果这个过程是泊松分布,则密度函数为:$f(t)=a*e^{-at}$;分布函数为:$f(t)=1-e^{-at}$($a$ 表示攻击的速度)。

攻击过程模拟模型中的数据来源应该基于实际的记录和统计,对于模型中还应该涉及哪些参数,参考文献[2]中有其它的观点。

2.4 系统状态转换概率矩阵

如前所述,系统的设计模式和它的防御机制,直接影响系统对攻击的反应能力,系统的反应表现在攻击发生后系统从一个状态到另一状态的转变,研究系统的反应就是研究概率转换矩阵。

设$\{D\}$为系统的设计模式集合,$\{M\}$为防御机制集合。根据前面的符号说明,系统配置为设计和防御机制的组合,表示为$\{D\times M\}$。不同的设计模式和防御机制的组合会导致不同的系统配置。为便于分析,本文假定整个系统的设计模式是固定的,设为 d,设集合 M 有 5 个元素。设攻击类型为 j,系统初始状态为 r,新的状态为 s,s 状态集合$\{S\}$。$\{S\}$集合中的元素可能是正常的状态、遭受攻击过程中的状态、已受损状态、恢复状态或完全失效状态等等。那么系统从状态 r 到状态 s 转化的概率函数为 $P=p(r, s)=p(r, s|j, d, m)$,$P$ 表示设计模式为 d 和防御机制为 m 的系统在发生 j 类型的攻击时,系统从状态 r 到状态 s 转变的概率。这样系统对攻击反应的数学模型可表达为由元素 P 组成的矩阵,设为 T。不失一般性,将系统状态按受损的程度轻重排列,即从 s=1=正常状态 到 s=S 完全的失效状态 进行排序。假设有这样一个攻击,使系统再也不可能到达一个比当前状态“更好”的状态,则矩阵 T 的下三角为 0,如下式所示。

$$\begin{pmatrix} p_{11} & p_{12} & p_{13} & p_{14} & p_{15} \\ 0 & p_{22} & p_{23} & p_{24} & p_{25} \\ 0 & 0 & p_{33} & p_{34} & p_{35} \\ 0 & 0 & 0 & p_{44} & p_{45} \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

T 的元素$\{p(r, s)\}$和 s, j, m 有相关性。(1)$p(r, s)\downarrow s$, $\forall s>r$, j 不变,m 为常量。在攻击类型和防御机制不变的条件下,T 中元素值说明系统从当前状态转化到一个“最差状态”的概率低于到一个“较差状态”的概率。表示系统有良好的抗降级功能,即系统状态恶化的幅度不大。(2)$p(r, s)\uparrow r$, $\forall s>r$, j 不变,m 为常量。在攻击类型和防御机制不变的条件下,系统的脆弱性随着系统状态的恶化而增加。(3)$p(1,1)\uparrow j, m$ 常量。在防御机制不变的条件下,如果所遭受攻击的力度越低,系统保持正常状态的概率就越高。(4)$p(1, s)\downarrow j$, $\forall s>1, m$ 常量。在防御机制不变的条件下,如果攻击的力度越低,则系统保持同一状态而不会降级的概率就越低。(5)$p(r, s)\downarrow m$, $\forall s>r$, j 为常量。在攻击类型不变的条件下,如果防御机制越强,降级概率越低。(6)$p(r, r)\uparrow m, \forall r$, j 为常量。在攻击类型不变的条件下,如果防御机制越强,则系统保持同一状态而不会降级的概率就越高。(7)$p(r, s)\uparrow n$, $\forall s>r$,其它一切都是常量,随着遭受攻击的数量增加,降级概率增大。(8)$\sum p(r, s)=1, \forall r$ 说明系统必须以某一状态结束。

转换概率矩阵的元素计算是很关键的一步,过程复杂,必须判定 $S\times J\times D\times M$ 的可能性。可以通过开发模拟环境产生转换概率矩阵 T 的元素$\{p(r, s)\}$;或者通过分析系统在对攻击的整个反应过程中所经历的状态,根据这些中间状态来计算矩阵元素。如果不能得到所有的相关数据,可以依据实际情况将规则简化运用。如本文就只考虑一种系统设计模式,即 D 的一个元素 d。

可用的数据越多(如不同系统状态之间的转化时间、攻击事件的平均间隔时间、系统完全恢复的时间等等),就能够将攻击类型和系统配置应用到更小的子系统中,这样就越有利于管理员全面地分析和测评其系统的生存性。

2.5 网络系统生存性分析

系统的生存性是衡量一个系统可以承受攻击的能力,即在遭受攻击后系统到达另一状态时,仍然能保证一定级别的功能(或服务)。一般来说新状态 s 是一个已受损的状态,在完全恢复到正常状态之前系统以这个状态作为终结。在电信领域,评价其生存性通常是将受损网络下可负载的流量与网络正常状态下能够负载的流量相比较。采用类似的方法,对信息网络系统的生存性能的数学表达可表示为:

SURV=(系统在新状态 s 的性能) / (正常状态下的性能)

由于系统可能同时具有多种功能或提供多项服务,系统在遭受攻击后到达一个新状态时,分析系统生存性要分别考虑针对不同的功能和服务。例如,系统在遭受攻击后某项功能状态仍然完好无损,则该功能的生存值为 1;如果系统遭受攻击某个功能状态已完全失效,则其生存值为 0;该功能的其它状态的生存值介于(0, 1)区间。

$\varphi(s, k)$ 表示系统功能(或服务)k 在状态 s 的受损的程度,w(k)是该功能(或服务)重要程度的表示。这样信息网络系统的生存性表现为如下形式:

$$\mathrm{SURV}(s)=\sum_k w(k)*\varphi(s, k),\ \text{其中}\ 0\le\varphi(s, k)\le 1, 0\le w(k)\le 1\ \text{且}\ \sum[w(k)]=1$$

假设系统已经定义了一个完整的状态集合$\{S\}$,就可以通过给定的 s 和 k 来计算 $\varphi(s, k)$。要综合看待状态集合$\{S\}$和不同的功能(或服务)集合$\{K\}$。$\{S\}$中的状态元素可能是{正常的状态,攻击过程中的状态,已受损的状态,恢复状态,完全失效状态},或者是 {正常的状态,轻度受损的状态,重度受损的状态,严重受损的状态,完全失效状态}。

SURV(s)的值介于[0,1]之间,0 表示系统完全失效,1 表示系统处在完全正常的状态。

如果在正常状态下系统功能 k 的最佳性能为 $X(k)$;但是在遭遇攻击时却要求系统实际必须达到的性能至少为 $x(k)$,其中 $0\le x(k)\le X(k)$,那么功能 k 在状态 s 所达到的性能表示为 $x'(k, s)$。这样从系统需求的角度出发,系统的生存性可表示为:$\varphi'(k, s)=x'(k, s)/x(k)$。

若 $x'<x$, 即系统没有达到该状态下必需的性能;若 $x'>x$, $\varphi'(k, s)=1$, 表示系统性能超过了该状态下最小要求的性能。

当所有的功能(或服务)都被破坏至最差的状况时,此时系统的生存性表示为:$\mathrm{SURV}(s)=\min_k \varphi(k, s)$。

在很多实际情况中,不可能考虑到系统可能遭受的所有攻击,但是,在攻击(无论是已知或未知)发生的情况下,是能够预见系统由于攻击而导致的各种可能的损坏情况。设功能 (或服务)k 受到 j 类型攻击而损坏至 x 程度的概率为 $p_{k,j}(x)$,就可以模拟出 k 的所有可能的损坏情况,计算系统在每一次攻击后的生存性。如果给定 j 的值,能够接受的破坏期望值为:

$$E[x(k, j)]=\int_0^1 x*P_{k,j}(x)*\mathrm{d}x \quad 0\le x\le 1,$$

则生存性计算为:$\mathrm{SURV}|j=\sum_k w(k)*(1-\mathrm{E}[x(k, j)])$。

如果将系统的功能/服务集合 $\{K\}$ 分为 $\{K0, K1, K2\}$, $K0$ 表示那些相对“不重要”的功能/服务,$K1$ 表示使用频率较高但不是重要的功能/服务,$K2$ 表示重要的功能/服务,那么则有:

$$\mathrm{SURV}(s)=[\prod_{k'}\varphi(s, k')^{w(k')}]*[\sum_k w(k)*\varphi(s, k)];$$

$$\text{或}\ \mathrm{SURV}(s)=1/2*\prod_{k'}\varphi(s, k')^{w(k')}]*[1+\sum_k w(k)*\varphi(s, k)]。$$

其中 $k\in\{K1\}, k'\in\{K2\}$。

此外,可以通过分析比较不同的系统,计算一个系统和其它系统之间“相对的生存能力”,参考文献[3]中的思想对于网络系统生存性能的分析方法有一定的启发意义。

3 结论

本文模拟了网络系统遭受攻击的过程,基于系统的反应,建立了网络系统生存性能分析的基本方法,对将来制定较为理想的网络系统安全策略和网络系统生存性评估方法研究具有一定的借鉴作用。

参考文献(References)

[1] 王红艳,谢小权.网络系统生存性概述[A].见:中国计算机学会计算机安全专业委员会,中国电子学会计算机工程与应用学会计算机安全保密分会.第十八次全国计算机安全学术交流会论文集[C]. 2003. 54~57

[2] Soumyo D. Moitra, Suresh L Konda. A simulation model for managing survivability of networked information systems [R]. CMU/SEI-2000-TR-020

[3] Lilien G L, Kotler P, Moorthy K S. Marketing models[N]. Englewood Cliffs. NJ: Prentice Hall, 1992

(责任编辑 邱夜明)