第 33 卷 第 3 期 计 算 机 工 程 2007 年 2 月
Vol.33 No.3 Computer Engineering February 2007
·安全技术· 文章编号：1000—3428(2007)03—0167—02 文献标识码：A 中图分类号：TP393.08

基于可生存性的系统安全评估方法

杜 君[1]，蒋卫华[2]，李伟华[1]
(1. 西北工业大学计算机学院，西安 710072；2. 第二炮兵工程学院，西安 710025)

摘 要：提出了一种新的计算机系统可生存能力的分析方法，该方法综合考虑系统外部环境和内部组件及其之间的相互关系，描述了系统的可生存能力。阐述了利用该方法对系统进行安全评估的措施及其优势。

关键词：网络安全；可生存性；入侵容忍；安全评估

System Security Evaluation Based on Survivability

DU Jun[1], JIANG Weihua[2], LI Weihua[1]
(1. College of Computer, Northwestern Polytechnical University, Xi'an 710072; 2. Secondary Artillery Engineering College, Xi'an 710025)

【Abstract】 The paper presents a new kind of analysis method for computer system survivability which considers both exterior environment and interior components and their correlations. The method can describe the survivability more precisely and exactly. The priority using this method to security evaluation is also put forward.

【Key words】 Network security; Survivability; Intrusion tolerant; Security evaluation

随着计算机和网络技术的广泛应用，安全问题已经成为信息系统研究的重要领域。一方面，人们越来越依赖于各种计算机系统；另一方面，现有的安全体系仍无法确保系统，尤其是系统所对外提供的一些关键服务的安全。传统的信息安全研究方法完全依赖于独立的安全机制和安全组件对系统进行保护，却忽略了组成系统的各个部件本身及部件之间交互时所应具有的安全特性。

可生存性研究认为系统的任何一个部件(包括安全部件)的安全性都可能受到危害，系统的生存能力体现在整个系统而非单个部件在遭到入侵时仍然能够对外提供有效服务。

可生存能力分析从系统自身的特征和系统整体的结构出发，通过对各方面因素的综合分析得出对系统可靠性和安全性的评价。对系统可生存能力的分析和评估有助于改善系统的安全性能，并确保一些关键服务的可靠性。

1 可生存性概念

1.1 可生存能力的定义

可生存性概念最早由Barnes等人于 1993 年提出[1]。可生存性研究将安全看成一种可伸缩的概念。具有可生存能力的系统，对内，其可生存能力不依赖于任何一个专门的组件；对外，系统可以容忍一定级别的入侵。严格地说，系统可生存性是指系统在网络攻击、系统出错和意外事故出现的情况下仍能及时完成其任务的特性[2]。

传统的网络安全措施将重点放在保持信息的机密性上，而随着各种加密及认证技术的完善，想要破坏系统的机密性已经相当困难，黑客们将目光转向了系统的有效性上。目前常见的多种网络攻击形式都并不对系统产生破坏，只是使之不能对外提供正常的服务，如 DoS 攻击。对于大部分应用程序，特别是大型网络实时应用程序来说，系统的连续有效对外提供服务的特性就显得极为重要。

可生存性研究的目的就是要在网络入侵行为可能或者已经对系统产生威胁和破坏的情况下，保证系统最低限度的有效运行，同时采取必要的措施进行恢复或者重新配置。

1.2 可生存性与传统网络安全性的区别

传统的安全分析方法将系统的安全性看成是一个个单独的个体堆砌或者连接起来，最典型的结论就是“系统的安全性取决于其最薄弱的环节”。这种观点将系统整体的安全性分解为单个组件安全性，认为找到系统最薄弱的环节并加以改善就可以提高整个系统的安全性，减轻了维护和评估系统安全工作量，收到了较好的效果。该方法没有意识到系统组件之间的相互联系对系统整体安全造成的影响，忽视了系统是作为一个整体对外提供服务这一事实。可生存性研究正是抓住了这一问题，它不依赖于任何一个单个的组件保证系统的安全性，而是将系统作为一个整体。系统处在一定的环境之中，由不同的组件构成，系统中任何一个组件都无法左右整个系统整体的安全性。

举个简单的例子，某个操作系统设置的密码很简单，容易破解，那么传统的网络安全评估方法就认为这个系统的安全性很差。但是，系统可生存能力分析并不这么认为：(1)考虑这个系统是做什么的，是数据库，还是 Web Server，还是一台个人电脑；(2)看它所处的环境如何，是否在物理上与非操作人员隔离，是直接暴露在 Internet 上，还是在防火墙后或 DMZ 中，有没有配置病毒防护及入侵检测软件等等；(3)看系统的各项配置，如系统的各种无关服务是否关闭，不必要的网络端口是否禁用等；(4)再看是否配置了一些保证系统生存能力的部件和机制，如备份机制、替换机制、服务退化机制等。在综合考虑了以上因素之后，得出系统整体可生存能力的大小。

基金项目：国家“863”计划基金资助项目“网络协同安全技术研究”(2003AA142060)

作者简介：杜 君(1979－)，男，博士生，主研方向：计算机网络，网络安全；蒋卫华，讲师、博士；李伟华，教授、博导

收稿日期：2006-02-10 **E-mail：**dujun@nwpu.edu.cn

2 可生存能力的描述

2.1 传统信息安全描述

设系统组件集合为 I，所处环境为 E，单个组件的生存能力为 $S_i, i \in I$，整个系统的生存能力为 SS。

传统的“木桶理论”认为系统的安全性取决于其最薄弱的一个环节。

$$SS = Min(S_i), i \in I \quad (1)$$

系统的生存性与构成系统的组件中生存性最薄弱的生存能力相同。黑客在发动网络攻击之前，通常会寻找系统最薄弱的环节作为突破口。要提高系统的可靠性及可生存性，就必须对每个组件的安全特性进行分析考虑，并为比较薄弱的组件配备额外的安全措施，如防火墙、入侵检测系统等。这些额外或者辅助的安全系统很大程度上针对的是系统所可能存在的各种安全漏洞和薄弱环节。

然而，这种思想会导致系统复杂性大大提高，它在保证原有组件安全性的同时，又为系统带来了一系列新的组件和复杂的控制关系。在增加系统开销的同时，很有可能会为系统带来新的漏洞[3]。另外，这种方法将系统的生存能力人为地割裂开来考虑，没有考虑到它们之间的相互关系。

本文认为，系统服务是由多个组件相互配合而形成的。各个组件之间的地位不同，所处的工作环境不同，完成的功能不同。从本质上说，各个组件都不可能具有 100%的可生存能力，但是上面的理论却明显没有考虑到各个组件的地位及其相互关系。

2.2 系统可生存能力描述

整个系统服务的可生存能力的计算方法应当考虑到上述 2 点，即

$$SS = \sigma_s + \sum_{i \in I} S_i + \sum_{i \in I} R_1(E, S_i) + \sum_{i,j \in I} R_2(E, S_i, S_j, K_{ij}) + \ldots \quad (2)$$

其中，σ_s 是系统安全机制参数，代表了系统是否具有备份、替换、服务降级等安全措施；S_i 代表每个组件的生存能力及其地位参数；R_1 是单个组件在系统环境中的关系函数；R_2 是 2 个相互关联的组件及与系统环境之间的关系函数，其中 K_{ij} 为 R_i 与 R_j 之间的相关系数；3 个及 3 个以上组件依此类推。

也就是说，得到系统生存能力大小的问题并不是在构成系统的各个组件中求最大值或者最小值的问题。要充分考虑到系统本身的安全机制，系统组件与环境、两个或者多个组件之间的关系。某个安全性较差的组件可以和其它组件结合起来构成一个更加安全的组件群；单个组件不安全、不可靠，可以使用链状组件群；如果还需要更大的生存能力，可以构建环状或者立体网状组件群。换句话说，如果能够通过各种措施对系统进行安全优化和调整，对上述参数进行最大化，就可以利用并非 100%安全的若干组件，构建接近 100%安全的系统服务。这为我们思考网络系统的安全性提供了一个全新的切入点。

3 系统可生存性分析和评估

利用上述方法，可以对系统的可生存能力大小进行量化的评估。举个例子来说，一个具有简单密码的数据库服务器有可能具有很高的可生存能力，因为它被锁在独立的具有高可靠电源的机房之中，配置了独立的防火墙，仅对外提供数据库查询和修改服务，并定时进行备份操作，而且有专门的操作人员随时进行监控。尽管它的系统密码比较复杂，但是系统没有对外提供任何获取这一密码的途径，而且配置了良好的防护和检测措施。万一出现了故障和意外情况，还可以根据良好的备份数据进行及时恢复。从整体上来说，本系统仍然具备较高的可生存能力。

对系统进行可生存能力大小的评估应当充分考虑系统的内外因素，从整体上对系统的安全性得出定量的分析。可生存性评估包括以下几个主要的步骤：

(1)对系统所处环境以及系统所提供的主要服务进行分析，得到系统环境参数 E；

(2)对系统本身所提供的安全机制进行分析，得到安全机制参数 σ_s；

(3)对相关组件的安全性及地位参数(重要程度)进行分析，得到 S_i；

(4)对组件与环境之间的关系进行分析，得到关系函数 R；多个相关组件之间存在联系的，需要计算相关系数 K_{ij}；

(5)利用式(2)计算系统可生存能力的大小。

需要说明的是，在实际应用中，σ_s、$\sum S$ 以及 $\sum R$ 之间仍然存在地位参数的问题，即它们对系统整体可生存能力大小的影响。地位参数可以根据应用环境的不同采用神经网络的方法训练得到。其它各种参数的取值范围一般设为[0，1]之间的连续值。

为了说明可生存性评估与传统安全评估的区别，对在相同情况下两种方法的评估结果进行简单地比较。为简化计算，把 σ_s、ΣS 以及 ΣR 的地位参数都取为 1，其它各种参数的取值也由[0，1]之间的连续区间简化为{0，1}二值。将评估的结果划分为{优，良，一般，较差，很差} 5 个等级。

从表 1 的分析中可以看出，在相同的条件下，传统网络安全评估和可生存性评估的结果存在明显的不同。可生存性评估将系统作为一个整体，从系统对外提供服务的角度出发，更好地描述了系统的安全性。

表 1 传统安全评估与可生存性评估比较

网络环境	密码	安全组件	服务独立性	响应/替换能力	传统安全评估	可生存性评估
内网中	复杂	有	好，仅作为 DB	有	优	优
内网中	复杂	无	好，仅作为 DB	无	良	一般
DMZ 中	复杂	有	差，同时作为 Web/Ftp/Mail Server	无	一般	较差
Internet 中	简单	有	好，仅作为 DB	有	较差	良
Internet 中	简单	无	差，同时作为 Web/Ftp/Mail Server	无	很差	很差

4 总结

网络安全思想从第 1 代的防御入侵，发展到第 2 代的检测入侵，再到现在的系统可生存性研究，经历了一个不断根据实际情况进行调整的过程。无论如何防御，入侵总会发生，无论如何检测，系统总会遭到不同程度的破坏。在这种情况下系统的安全性在很大程度上应当用系统的生存能力的大小来进行衡量。在考虑复杂系统生存性的时候必须将构成系统的组件及其自身之间以及与环境之间的关系考虑进去。系统的可生存分析性较之传统的网络安全评估，能够更有效地保证系统的安全性。通过在入侵发生前及入侵发生时，对系统进行合理的调整和配置是目前最为实际的系统安全策略。

参考文献

1 Hollway B A, Neumann P G. Survivable Computer-communication Systems: The Problem Working Group Recommendations[R]. Washington: US Army Research Laboratory, 1993.

（下转第 171 页）