文章编号:1000 - 582X(2005)08 - 0056 - 04

生存体系结构模型*

班晓芳,向 宏
(重庆大学 软件学院,重庆 400030)

摘 要:处于 Internet 中的重要信息系统面临的安全问题越来越多,如何增强系统生存能力,使系统在受到破坏后仍能继续提供用户需求的服务已引起人们普遍关注. 笔者介绍了生存性定义,根据生存性具有的抵御、认识、恢复和演化 4 个功能属性设计了信息系统的生存体系结构模型,进而解释了模型中的系统生存需求、生存策略的含义. 并依据生存策略的不同方面给出了为使系统达到生存性的技术措施.

关键词:生存体系结构;生存需求;生存策略;保护;检测和响应;恢复
中图分类号:TP309 **文献标识码**:A

因特网的发展使信息系统的安全问题越来越突出. 目前,越来越多的机构已经将其内部的信息系统接入 Internet,并通过 Internet 向客户及社会提供信息或计算服务. Internet 是典型的无边界、无全局可视域、无全局管控的复杂巨系统. 信息系统一旦进入 Internet,在获益的同时,也将自身置入了充满未知的高风险环境. 影响信息系统安全的因素不仅包括软件故障、硬件故障和人为故障等意外事件,还包括病毒、网络攻击和系统入侵等恶意事件和一些自然灾害事件(如雷电、洪水、地震、战争、停电). 即使是最出色的系统设计者和网络安全管理者也不可能预见所有威胁事件,因此系统将不可避免地受到破坏. 既然系统被攻击乃至被入侵是不可避免的,那么与其站在系统之内,还不如站在系统之上来观察系统安全问题——着眼于系统整体的健壮性和生存能力. 这种能力意味着系统可以被入侵,可以部分组件受损,乃至某些部件并不完全可靠,但只要系统能在结构上合理配置资源,能在攻击下资源重组,具有自优化、自维护、自身调节和功能语义冗余等自我保护能力,就仍可完成关键任务. 具有这种能力的信息系统就是可生存信息系统. 如何使系统在受到攻击后仍能继续提供持续性服务是可生存性研究的内容.

1 研究现状

生存性是目前国际上提出的 Internet 安全的重大课题之一. 早在 1993 年,美国军队研究实验室(ARL) Barnes 等人提出此概念. 1997 年美国成立了信息生存研究学会(Information Survivability Workshop),确立了对生存和生存网络的研究. 这方面的研究已经引起了美国国防高级研究计划局(DARPA)等有关部门的关注. 2001 年我国也开始把这一课题列为"863"攻关项目.

在方法学的研究上,CERT/ CC[1]研究方法有一定特色,可把它总结为 1 个划分、2 个"R",即首先将系统划分成不能攻破的安全核和可恢复部分,然后针对一定的攻击模式,给出相应的抵抗(Resistance)、识别(Recognition)和恢复(Recovery)策略. 基本服务不可攻破,入侵模式是有限集合,并强调系统防护技术的不断进步是生存性方法学研究的前提.

在生存体系结构研究方面,美国福吉利亚大学[2](University of Virginia)和 Portland 大学等单位合作正在开展"关键基础设施保护的信息可生存性"工程研究,包括关键基础设施的可生存性评测、军用和民用基础设施研究及可生存性体系结构工程等.

* 收稿日期:2005 - 04 - 04
基金项目:重庆市科委资助项目(7970)
作者简介:班晓芳(1972 -),女,内蒙古包头人,重庆大学硕士研究生,主要研究方向:信息与网络安全、agent 技术.

由美国国家安全局颁布的信息保障技术框架(Information Assurance Technical Framework ,简称 IATF)提出了"信息保障"的概念,突出纵深防御、主动防御、整体防御和不断进步.把深度防御体系作为安全研究的发展方向.从组织结构、人员培训、制度建设、操作和技术等多个层面考虑信息保障体系.

国内学者提出了用多样化动态漂移的技术途径实现网络生存设计的方法[4]和分布式系统中服务可生存性的定量分析[5].

2 生存性理论

2.1 生存性定义

生存性是指系统在适时模式下,在出现攻击、故障或意外事件的情况下完成基本服务的能力[6].

与传统的安全方法要求中央控制和管理不同,生存性方法是一种在既没有中央控制又没有统一安全策略的情况下,针对高度分布且没有边界的网络环境提出的,它强调系统受到攻击和威胁时依然能够提供基本服务并满足临界条件的业务要求,如安全性、可靠性、正确性、实时响应等,并且在攻击后能在可确定的时间内按照优先级自动恢复所有由于损伤而暂停的服务.其研究范围包括安全性、可靠性、重用性、灾难恢复等,也涉及到系统的动态适应、多样化、信任维护策略等其它方面的内容.可生存性概念的提出并不是计算机应用发展的一个新方向,而是一个综合了其它相关领域的整体安全框架.

2.2 生存性的特征

黑客入侵系统时通常经过以下 3 个阶段:

1) 渗入阶段:入侵者正通过各种方式试图获得系统的控制权,常用的方法是扫描网络中系统漏洞;

2) 探测阶段:入侵者已进入系统并正在探测系统内部的结构和其它信息;

3) 利用阶段:入侵者已部分获得系统的控制权并正在从事各种非授权活动;

针对黑客的入侵步骤,应对措施应集中在以下几点,它也是一个安全的、可生存的信息系统必须具有 4 个关键特征[6]:

1) 抵抗能力(Resistance):系统抵御攻击能力;

2) 识别能力(Recognition):识别攻击和受损范围的能力;

3) 恢复能力(Recovery):在受到攻击时保持关键性服务并在攻击后恢复所有服务的能力;

4) 演化能力(Adaption):改进和发展以减轻未来攻击的影响的能力.

2.3 生存体系结构模型

根据生存系统的 4 个特征,结合系统生存需求和生存策略,建立了一个信息系统的生存体系结构模型.如图 1.

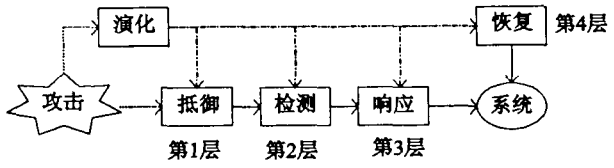

图 1　生存体系结构原理图

该模型提出的保障系统可生存的结构由抵御、认识、适应和恢复 4 部分组成.生存策略的制定是以系统生存需求为基础的.整个系统的运转受系统生存策略的指导和控制.可生存结构模型为系统建立了 4 道防线:第 1 道防线是抵御系统,能够阻止对系统的入侵危害.但是不可能阻止所有的攻击.第 2 道防线是对未能阻止的攻击继续检测,及时发现入侵和破坏.第 3 道防线是实时响应,当攻击发生时维持网络"打不垮",并阻止危害的传播.第 4 道防线是灾难恢复,使网络在遭受攻击后能以最快的速度"起死回生",最大程度上降低安全事件带来的损失.并且系统能重新分配资源,至少能提供降级服务,这层是系统具有生存性的重要体现.生存性演化的作用是根据从入侵中获得的知识改进系统防御、检测和响应、恢复的策略.

该模型认可风险的存在性,认为绝对的安全与可靠性的系统是完全不存在的,只有相对的安全性,其理想效果就是攻击者穿越防御层的机会逐层递减.特别第 4 层的恢复系统,在生存策略指导下,系统被穿透的概率趋于 0,从而达到系统的可生存性.

生存体系结构模型强调了生存策略对整个安全保障体系的支撑作用,这是区别于以往动态网络安全模型的最显著方面.系统生存策略贯穿于模型中的各道防线中,使得系统即使在第 1 ~ 3 道防线被攻击者攻破时,由于系统具有生存恢复策略,系统仍能为用户提供持续性服务.

3 对模型的理解

3.1 系统生存需求

将可生存性作为一个系统功能来研究,在系统设计阶段通过对需求进行可生存性分析,就可以定义该系统的可生存性策略,为从系统结构、编程语言等多个层次进行可生存设计、实施和评估打下基础.生存系统需求定义中应包括的 4 个技术因素:

1) 可接受服务:为了能够应对各种形式的破坏,保证用户的持续性服务需求,系统应提供多种可选服务.如果某种形式的破坏使系统不能提供正常服务,就需要提供另外一种等价的服务形式;

2) 运行环境:包括系统受到的威胁,如软件故障、硬件故障、人为故障、入侵事件和自然灾害事件、政治气候、政策因素等约束系统运行的因素;

3) 服务优先顺序:为了满足用户的服务需求,还要明确哪些系统功能是比较重要的,这些重要功能间的相互依赖关系和哪个功能在什么条件下应优先保证执行;

4) 服务的过渡方式:如果由于某种原因系统不能维持当前服务,则系统将按照可接受服务的定义,通过重新配置,转换到另一种可接受的服务状态;

按照这些定义建立的生存系统,攻击者将很难使系统重要功能失效.在受到攻击的情况下,系统或者可以容忍入侵,或者能够重新配置系统重要功能.

3.2 生存策略

系统生存策略通常从 3 个方面理解:抵御、检测和响应、恢复.这些策略协调配合才能保证系统达到生存性.

3.2.1 抵御策略

可生存系统应能抵御网络攻击、内部故障和外部事件.加密技术、访问控制机制和安全设备都可以用来解决这些问题.保证系统安装了安全补丁,使用了已有的一些产品和服务(如防火墙、认证服务器等),这些均可保护系统不受已发现的攻击类型的攻击.同时,用户对系统操作时也需要进行认证.通过拒绝攻击者对系统配置和属性的探测,防止系统受到精心策划的网络攻击.

3.2.2 检测和响应策略

已知,现有的计算机产品和服务都有不可排除的、未知的脆弱性,因此必须意识到有时保护措施将会失效.例如,不能保证来源于授权地址的程序都不包含恶意代码.而且,也不能保证系统都有正确的配置.因此生存策略的第二步就是检测破坏并给予响应.必须监督系统设施中的每一环节,并且为了对存在威胁的环境有一个较好的认识,检测和响应二者必须紧密结合.可以使用日志分析程序、入侵检测系统和抗病毒程序来检测系统是否受到破坏.当检测到系统已遭受破坏,应有一个及时、正确的响应来保护系统资源,如隔离受攻击的主机和系统中受攻击的部分、把攻击者诱骗到网络陷阱之中,或者向安全管理员发出警告.通过对检测到的破坏行为进行分析,还可以提高系统保护能力.然而实践证明在某些情况下,保护和响应措施对系统持续性运行也不都是很有效.

3.2.3 恢复策略

生存策略的第三方面就是在系统在受到意外破坏并无法提供正常服务时,在最短时间内系统能够恢复某些服务,容忍某些破坏,来支持系统的可生存需求(如保证关键功能持续运行).恢复能力是系统生存能力的重要体现.

当系统中止破坏时,非常有必要评估它对系统的破坏性,并且此时系统应该能够恢复关键服务.为了持续执行任务,或许不需要把所有受到破坏的组件恢复到最初状态,而是以一种降级模式,恢复那些影响系统任务持续执行的服务.因此,必须定义多种用户可以接受的服务(包括降级服务)形式.这些形式是根据约束系统运行的环境而定的.一些破坏或许并不会立即就检测到,而是在系统中扩散一段时间才能检测出来.系统是否能成功恢复依赖于破坏的严重程度(例如多少资源受到影响)、恢复策略以及系统中未受到破坏的资源、系统应提供的服务、全面的破坏评估结果、针对系统不同程度破坏下的恢复策略以及重新配置中的冗余资源,这些信息共同保证系统在受损时能否提供持续性服务.

4 可能采取的生存技术手段

要开发一个生存系统,可以使用多种保证系统生存的技术手段.表 1 为开发生存系统时可能用到的一些技术手段按照生存策略的不同方面进行分类.

表 1 生存技术方法

抵御	检测和响应	恢复
访问控制	日志分析	高级中间件
数据分片并分散存放	病毒验证	动态重配
动态 IP 地址	监控主机	冗余
强制认证	监控应用	降级服务
PKI(公钥基础设施)	移动 Agent	事务恢复
DNSSEC(域名系统安全)	监控网络	捕捉系统信息
IPSec(IP 安全)	计算环境中的状态识别	动态路由
SSL(安全套接层)	SNMPv3(简单网络管理协议)	备份服务器
VPN(虚拟专用网)	IDS(入侵检测系统)	恢复控制器
代理服务	动态路由	移动 Agent
服务注册		
可信操作系统		
认证服务器		
目录服务器		
防火墙		
策略服务器		

5 结束语

随着计算机技术的发展和网络技术的普及,信息系统的安全越来越重要. 可生存网络的研究将成为信息系统安全的重要研究方向之一. 笔者基于国内外学者对可生存的定义和对定义的理解,从重要信息系统的生存需求出发,紧密结合系统达到可生存性需要具有的功能属性,建立了信息系统生存体系结构模型,并总结了可用于建立生存技术现有的技术方法.

网络系统生存性的研究还没有形成一个系统的成熟的、规范的体系,其技术也在不断发展,众多热点和难点问题正在讨论和研究之中,很多新技术有待开发.

参考文献:

[1] LINGER R C, MEAD N R, LIPSON H F. Requirements Definition for Survivable Network Systems [EB/OL]. http://www.cert.org/archive/pdf/icre.pdf, 2004-06-04.

[2] ANOTAI SRIKITJA, DAVID TIPPER, DEEP MEDHI. On Providing Survivable QoS Services in the Next Generation Internet [EB/OL]. http://www.cstp.umkc.edu/public/papers/dmedhi/stm_milcom99.pdf, 2004-06-04.

[3] 黄遵国,卢城,王怀民. 可生存技术及其实现框架研究[J]. 国防科技大学学报,2002,24(5): 29-32.

[4] 郭渊博,马建峰. 分布式系统中服务可生存性的定量分析[J]. 同济大学学报,2002,30(10): 1 190-1 193.

[5] ELLISON R J, FISHER D A, LINGER R C, et al. Survivable Network Systems: An Emerging Discipline [EB/OL]. http://www.sei.cmu.edu/community/easel/pdfs/97tr013.pdf, 2004-06-04.

[6] JOON S P, JUDITH N F. A Strategy for Information Survivability [EB/OL]. http://www.cert.org/research/isw/isw2001/papers/Park-31-08.pdf, 2004-06-04.

Model of Survivable Architecture

BAN Xiao-fang, XIANG Hong

(College of Software Engineering, Chongqing University, Chongqing 400030, China)

Abstract: Critical information system in Internet is in face of increasingly security problems. More attention has been focused on the survivability of information system, which is the capability of system to continue its mission even in the presence of damage to the system. The authors first introduce the definition of survivability. According to four function properties of survivability, which are Resistance, Recognition, Recovery, and Adaption, the authors design a model of survivable system structure and then explain survivability requirement, survivability strategy in this model. Additionally, they provide possible technical solutions for the survivability of systems, categorized by different aspects of our survivability strategy.

Key words: survivable system structure; survivability requirement; survivability strategy; protection; detection and response; recover

(编辑　吕赛英)