文章编号:1001 - 2486(2002)05 - 0029 - 04

可生存技术及其实现框架研究*

黄遵国,卢锡城,王怀民
(国防科技大学计算机学院,湖南 长沙 410073)

摘 要:提出用多样化动态漂移的技术途径实现网络生存设计的方法。分析该技术对网络安全、网络生存的影响,并给出了该技术的体系框架。指出这个研究具有前瞻性、全面性和实际性的特色。

关键词:生存性;网络安全;应急响应;灾难恢复;主动漂移
中图分类号:TP393 文献标识码:B

On Survivabilty Techniques and Its Implementation Skeleton

HUANG Zun-guo, LU Xi-cheng, WANG Huai-min
(College of Computer, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: The method of implementing the network survivability design using the diversity dynamic drifting techniques is proposed here. The influence of this techniques on network security and survivability is analyzed. And an architecture skeleton of this technique is then presented. It is pointed out that the research has the features of prevision, completeness and reality.

Key words: survivability; network security; emergency response; catastrophe recovery; active drifting

信息攻防是此消彼涨的矛盾的统一体,虽然信息攻击技术越来越复杂,但攻击者实施攻击的入行门槛反而越来越低。从 1988 年发生了莫里斯蠕虫第一例网络攻击起,网络攻击花样翻新,防御难度递增。20 世纪 90 年代初网络攻击以社会工程学攻击及会话劫持等为代表,90 年代中期以自动探测与扫描及可执行代码攻击等为代表,现在则以分布式拒绝服务攻击、特洛伊木马等为代表,加上各种黑客联盟的兴起和网上攻击软件的交流,使得在攻击复杂度直线上升的同时,对攻击者的知识要求却在呈指数下降。这个悖论使得攻击者的队伍迅速扩大,网络处于攻击的'汪洋大海'中。

显然,御敌于国门之外的边界防御技术难以从根本上解决信息安全的这个悖论,集成各种防御手段、以实现纵深防御为目的的生存技术成为安全研究的未来发展方向。美国的 911 事件以及事件后世贸中心信息系统的快速恢复的案例说明灾难事件的现实性和纵深防御的必要性。

系统的可生存性是指系统在面临攻击、失效和偶发事件的情况下仍能按要求完成任务的能力。生存性研究强调以任务为本,而不是以系统为本。如果某个系统的构件遭到攻击而瘫痪但仍能保证所执行的任务不受大的影响,则它的安全策略是失败了,生存策略却是成功的。

1 生存性研究现状

生存性研究与关键信息基础设施保护(Critical Infrastructure Protection)紧密相连,其重要性得到广泛的关注。无论是国际还是国内,关注的部门越来越多,投入的资金、研究的队伍越来越大。目前人们正吸收其它学科尤其是可靠性设计的研究成果,开展生存技术的研究。研究重点包括生存性的基本概念、生存性体系结构、生存性系统模型、生存性系统分析与设计、生存性系统工程方法和工具、生存性风险评估、生存性系统评价与测试等。人们在不断寻求开放互联网络环境下的容错、容入侵(Intrusion

* 收稿日期:2002 - 03 - 21
基金项目:国家 863 高技术资助项目(2001AA142090);国家部委资助项目(2001 - 研 2 - A - 014)
作者简介:黄遵国(1958—),男,副研究员。

Tolerance)、容攻击(Attack Tolerance)的硬、软件解决方案。

在方法学的研究上,CERT/CC[1]研究方法有一定特色,可把它总结为一个划分、三个"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,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。

由美国国家安全局颁布的信息保障技术框架[3](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。

国防科技大学计算机学院针对我军纵深防御体系的建设,研究入侵检测与预警、系统隐患分析与修复、应急响应与恢复[4]等关键技术,并取得了进展。

在具体技术研究上,由 DARPA/ITO 资助的"自适应可生存多网络的信息系统生存性"课题,正在开展多个异构网络的关键服务集、受攻击时的 QOS 保障、受损后的网络系统管理策略等相关问题的研究。研究在网络遭到攻击的情况下如何最大限度地减少网络拥塞,以保证关键的网络服务能够优先使用网络资源和尽快地恢复网络的正常交通。

在恢复技术上,马里兰大学对数据库的恢复做了很好的研究。他们以入侵检测为前提,通过评估、隔离、屏蔽等技术实现数据库的损失评估与修复。

虽然关于结点级和部件级应急响应和恢复的研究已相当深入,且取得了可喜的成果,但总体上讲,实现系统级的应急响应与恢复还有许多问题要解决,如:基于结点级的生存策略,被保护的目标仍然处于静止的被动的地位,难以应付众多黑客的持续攻击;镜像备份技术缺乏隐蔽性,且同构系统易出现灾难的骨牌效应;防守反击能力差,恢复的时间不理想等等,为此人们正探索理论上和技术上的新突破。

2 信息系统的应急响应与恢复技术

围绕信息系统的应急响应与恢复技术,我们提出了"多样化动态漂移技术",旨在通过分布式动态备份、多样化主动漂移以及快速恢复等机制,使原来网络中静止的和被动的目标变成运动的主动的目标,通过不断漂移以提高信息系统在信息战环境下的生存能力。探索中注意到:

· 操作系统漏洞的局部性。不同的 OS 有不同的漏洞,如 Unix 的 Buffer 溢出、Windows 的 BO 等,异构操作系统之间的漏洞具有相对的独立性,即使是相同性质的漏洞在不同的 OS 中表现形式也不同。

· 单一环境的脆弱性。单一的物种会产生单一的天敌,单一环境一破皆破。反之多样性可以降低全局损失,只要有一部分存活,就可作为重建的基地。以动态可变来减少被攻击的风险。

· 攻击者的智能性。聪明的攻击者专门寻找系统漏洞实施攻击,由于同构冗余的多个系统的弱点是相同的,系统同时故障的概率虽小,但被攻破可能性却大,因此对于以寻找弱点为特征的信息攻击来说,同构冗余对增强安全保护能力作用不大。异构性和多样化策略可使对手无法了解目标的全部弱点,增强了生存能力。

基于漂移技术的应急响应与恢复系统一般由四部分组成:事前准备的备份系统,灾中响应的漂移系统,灾后的取证反击系统与快速恢复系统。多样化动态漂移通过分布式备份、主动和应急相结合的漂移、结点级的备份及快速恢复机制,构成一个有机的系统框架。

图 1 给出了动态漂移应急响应系统的总体示意图。

其中分布式备份模块完成灾难发生之前的准备,采用一主多备的备份结构,主数据库在运行中定期地向各个备份数据库更新数据,在结点级实现多层次数据的备份。漂移使得主结点和其中一个备份结点换位。灾情评估根据入侵检测报告,调整系统的安全与性能策略,评估发生的灾情,如果现场是可恢复的,则只做系统恢复,否则通过调度控制漂移。漂移后做网络级的恢复或者离线维修。漂移调度系统

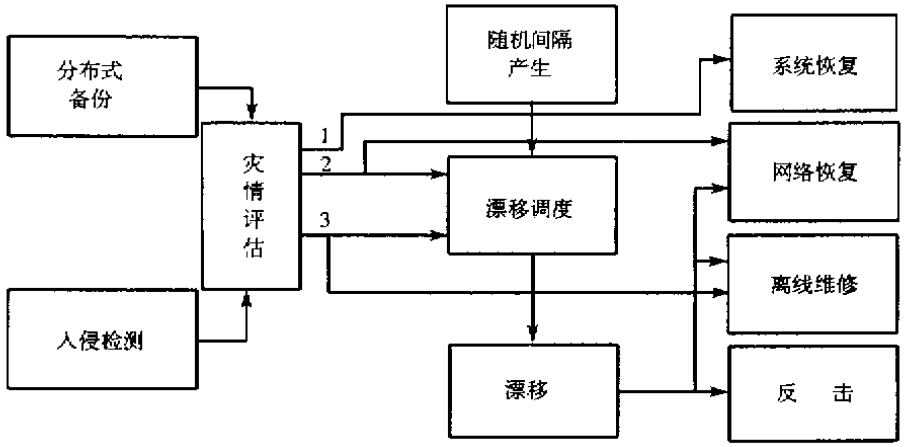

图 1 多样化动态漂移应急响应系统总体框图

Fig.1 Diversity dynamic drifting emergency response system skeleton

完成应用服务的漂移调度,除了根据入侵检测报告进行应急漂移外,还可根据随机间隔产生器产生的随机信号随机地进行主动漂移。两者结合使应用在机动中对外提供服务。整个系统建立在异构的备份服务器池上。主要关键技术如下。

2.1 主动漂移机制

公式 1:$Pt > Dt + Rt$

Pt:在既定的保护方式下,入侵者攻击安全目标所花费的时间;

Dt:从入侵开始到系统能够检测到入侵行为所花费的时间;

Rt:发现入侵行为到系统能够做出足够的响应并将系统调整到正常状态的时间。

那么,针对需要保护的安全目标,上述公式的含义就是在入侵者危害安全目标之前就能够被检测到并及时处理。

公式 2:$Et = Dt + Rt, IF\ Pt = 0$

其中 Et 是系统暴露时间。

公式 2 可以形成两种安全策略,其一就是针对需要保护的安全目标,尽量使 Et 小;其二就是在 Et 时间内尽量使入侵者无所作为。

由前述两个众所周知的公式可以得出如下结论:在加强防护以延长 Pt 的同时,及时地检测和响应恢复以缩短 Dt 和 Rt,是解决安全问题的明确的方向。主动漂移侧重于响应恢复阶段,用快速的灾难漂移来迅速地转移目标以隐藏系统恢复时间,使暴露在外的 Rt 缩短。同时,鉴于灾难的突发性,在灾难尚未到来之前也必须随机地进行目标转移,以达到隐蔽目标,避免灾难的目的,即主动漂移。它基于一种近乎随机的时间调度算法,让应用服务随机地在服务器的备份池间漂移。主动漂移机制涉及随机时间片调度算法;多样化动态漂移算法;跨 WAN 的、无前端调度器、对客户方透明的主动漂移技术等。

2.2 分布式备份及其支撑技术

在分布式网络备份中,结点以组的结构划分,每一组设一个备份服务器,存放组内结点的关键信息的备份,备份服务器之间的关键信息也相互备份。这样,当组内结点被攻破时,可以通过备份服务器恢复该结点的关键信息,而该结点可以借助这些关键信息及时地恢复它的全部功能,并可同时进行针对这一灾难的免疫和自适应处理。

如果该组的备份服务器遭到破坏,则可通过与其异构的相邻的其他组的备份服务器的信息恢复该组的备份服务器的关键信息,然后再以此类推地恢复所有的系统功能。

在每个站点上,本站点的信息构成的数据库为主数据库,它的备份数据库(从数据库)在其它的站点

上,当对主数据库的信息进行修改时,从数据库的数据自动更新。

主结点一旦遭遇事故,数据和应用可以在远程的一个地点很快得到恢复。采用异构异地体系结构,使得入侵者在 Et 时间内无所收获。可选择不同的备份策略、备份周期、备份范围以及网络备份机制等。

2.3 快速恢复机制

快速恢复研究受害结点机修复后的切入如何保证系统不丢失信息,且与系统中的其它有关结点机保持同步通信。其目的是通过系统日志、信息备份以及有效的安全监测来保障资源信息管理系统免受大的安全事故的破坏。

监控程序可以实时发现非法的修改、删除、添加操作,如果是指定的只读文件被删除,可自动在几秒内用备份的正确数据进行恢复,保证系统的正确性。采用隔离、屏蔽、分散、冗余等多种成熟技术可实现应用系统的"保健",防止被污染数据的进一步传播。此外,还可以随时生成恢复列表,列出所有被非法修改的文件,利用紧急备份数据,自动或在用户的干预下进行快速恢复。同时形成相关报告,供事后查询分析。快速恢复技术可在最短的时间内恢复系统,有效地提高系统的生存能力和服务的可用性、正确性。

与此同时,在恢复的过程中应该针对所暴露的漏洞和攻击的类型进行相应的免疫处理,如对漏洞进行修补,增加攻击识别库的内容甚至采用防守反击的方法对攻击事件进行审计和惩罚。

3 结束语

对信息基础设施的要求是平时能保证信息安全,战时遭受打击时能生存并提供正确服务。基于生存性的应急响应和灾难恢复技术,平时可增强目标系统活动的隐蔽性,战时则可以保证在被打击条件下继续完成任务。目前信息基础设施和各类应用系统建设刚刚起步,信息安全和系统生存性方面存在众多隐患,必须引起足够的重视。

参考文献:

[1] Linger R C, et al. Requirements Definition for Survivable Network Systems[R]. http://www.sei.cmu.edu/97icre.pdf, 1999.

[2] Anotai Srikitja, et al. On Providing Survivable QoS Services in the Next Generation Internet[R]. Supported in Part by NSF Grant NCR 9506652 and DARPA under Agreement No. F30602-97-1-0257.

[3] IATF Release 3.0[J]. September 2000 Issued by National Security Agency, Information Assurance Solutions Technical Directors, USA.

[4] Huang Zunguo, Lu Xicheng, Wang Huaimin. A Diversified Dynamic Redundancy Method Exploiting the Intrusion Tolerance[R]. ISW-2000 proceedings, Page 217-221, 2000.10. Boston, USA.