一种应用于安全管理平台的整体安全模型
——态势图模型*)

姚 键[1,2] 陆 荣[2] 孙 虎[3] 茅 兵[1,2] 谢 立[1,2]
(南京大学计算机系软件新技术国家重点实验室 南京 210093)[1]
(南京大学计算机科学与技术系 210093)[2] (盐城市地税局 江苏盐城 224001)[3]

摘 要 安全管理平台强调全局安全目标,整体安全模型是安全管理平台的核心,本文提出了态势图模型,既能反映安全系统的安全能力分布与组织关系,又能描述安全系统的安全状态变迁过程,具有较强的实用性。

关键词 安全管理,安全管理平台,安全模型,态势图

A Global Security Model Applied in Security Management Platform ——Posture-Diagram Model

YAO Jian[1,2] LU Rong[2] SUN Hu MAO Bin[1,2] XIE Li[1,2]
(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)[1]
(Department of Computer Science and Technology, Nanjing University, Nanjing 210093)[2] (Yancheng Local Tax Bureau, Yancheng 224001)[3]

Abstract Global security is emphasized by security management platform. In this paper, a global security model, named POSTURE-DIAGRAM MODEL, is put forward. The model can not only describe distribution of network security mechanism but also describe procedure of network security mechanism changing. The model has more practicality than model given before.

Keywords Security management, Security management platform, Security model, Posture-diagram

1 引言

随着网络中的安全设备种类与数量不断增加,安全管理员已被淹没在成千上万的安全报警信息、审计信息中,急需一种能够自动分析各类安全信息、协同所有安全设备、保障整体安全的全局安全中心。安全管理平台应运而生。安全管理平台是网络安全管理的中枢神经。它从全局视角出发,协同网络系统中的所有安全设备服务于整体安全目标,把一个个原本分离的信息安全孤岛组成一个协同统一的安全体系,实现网络系统安全管理的完备性、目的性、统一性,从而有效提升整体安全水平。笔者认为,安全管理平台要想正确发挥全局领导职能,必须对整个网络中的安全系统正确建模而且该模型应至少满足下面三种要求:

(1)提供全局静态视图。刻画全系统各安全设备(机制)的安全能力、地位和相互关系,指导安全设备补充和部署、安全信息收集、聚类和分析。

(2)提供全局动态视图。对安全系统的安全状态变迁过程抽象,表述安全系统防御、被攻击和恢复的过程。为安全策略的制定、实施和检测提供理论指导和实践依据。

(3)提供定量指标。对安全系统的防御能力,给出一套客观指标体系,并能量化。

当前,安全产品研发已从提供单一安全功能的安全设备,经历两(几)个安全设备联动,发展到安全管理平台的研发阶段,众多安全厂商推出了自己的安全平台产品。例如联想网御安全管理平台[1],IBM Tivoli 安全管理平台[2]。

2 相关研究

安全模型的研究源于 20 世纪 70 年代 Bell&Lapadula[3] 的多级安全模型,该模型主要应用于操作系统的信息保密领域。1988 年,ISO 7498-2 提出 OSI 安全模型,该安全模型定义了 5 类安全服务,8 类安全机制以及相应的安全管理,并对这些服务与相应的机制在 OSI-RM 中的 7 个层次作了分配[4]。该模型具有普遍指导意义。2000 年,IATF 3.0 提出了"深度防御模型(Defense-in-depth)"[5],将整个网络分成若干个区域:(1)基础设施;(2)边界;(3)计算环境;(4)辅助性基础设施。旨在采用多层保护方案,当攻击者成功破坏某层保护机制时,其它保护机制仍能提供附加的保护。相对于静态防御模型,ISS 公司提出了 PPDR 模型[6],侧重动态安全循环,以 policy(策略)为指导,protection(防护)、detection(检测)和 response(响应)组成一个完整的动态循环和逻旋上升过程,强调整体安全目标和连续的管理周期。

以上模型反映了整体安全模型的某些侧面,但是都不能构建一个完整的整体安全模型,也没有细化到具体的网络拓扑中的定量指标,所以都不能用作整体安全模型。本文在分析前人研究的基础上,结合网络实际,提出了一种应用于安全管理平台的整体安全模型—态势图模型。该模型能从空域和时域两方面刻画整体安全形势的变化,并能按不同要求提供多粒度的安全"快照",满足整体安全管理的需要。

3 态势图模型

3.1 安全空间

*)基金项目:国家 863 计划(No. 2001AA142010);江苏省自然科学基金项目(No. BK2002073);国家自然科学基金项目(Noo. 60473091)。姚 键 博士研究生,主要研究领域为安全管理,分布式计算。孙 虎 主要从事领域网络管理。陆 荣 硕士研究生,主要研究领域为安全管理,软件工程。茅 兵 教授,博士生导师,主要研究领域为网络信息安全。谢 立 教授,博士生导师,主要研究领域为分布式计算与先进操作系统等。

首先定义一个一般意义的、适合任何安全系统的安全空间。安全空间由三个维度组成，分别是安全服务能力维(z)、安全深度维(y)和安全层次维(x)。如图1所示。

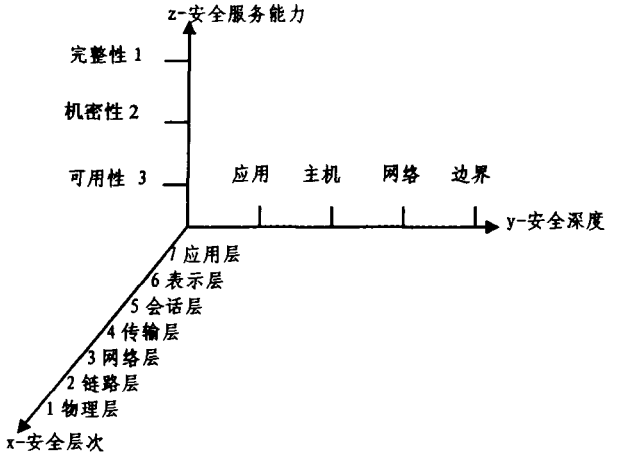


图1 安全空间三维

(1)安全服务能力维—z 安全服务能力维—z表征安全机制提供安全服务的能力。本文假设只有数据完整的前提下，数据的机密性才有意义，也只有数据完整性和机密性得到保证，可用性才有意义，这里的可用性不只是单纯的可访问性。这样建立了完整性，机密性与可用性三者之间的偏序关系，将它们标注在同一轴(z)上。

对z轴第1次细化得到z_1轴，即将三种安全服务能力再分为3个等级[4]，如图2所示。

SML1：基本强度，可以保护低价值数据，抵抗不复杂的威胁。

SML2：中等强度，可以保护中等价值数据，抵抗有组织的攻击的威胁。

SML3：高强度，可以保护高价值数据，抵抗来自国家实验室攻击的威胁。

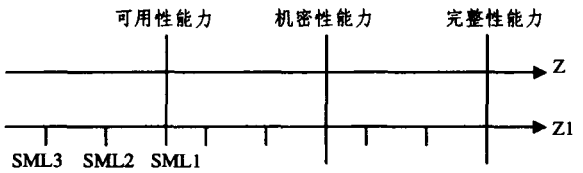


图2 安全服务能力维细化(从Z到Z1)

(2)安全深度维—y 表征安全拓扑，参考"深度防御"的原理在该维度上标注4个刻度从内到外分别为应用、主机、网络、边界。

对y轴第1次细化得到y1轴，y1轴与网络拓扑对应，即由区域细化到IP地址。

(3)安全层次维—x 表征OSI—RM的层次，沿坐标轴方向顺序标注为应用层、表示层、会话层、传输层、网络层、链路层和物理层。

网络安全空间的精度不限于上述的介绍，可以根据实际网络安全系统的表述需要进一步细化和概化。

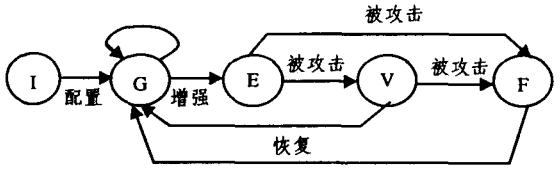
3.2 安全系统的静态表示

在上文安全空间中，任何安全系统表现为若干点的结合。如果一个安全系统中共有100个安全设备，而且每个安全设备仅提供一种安全服务，那么该安全系统在安全空间中就表现为100个点的集合。例如：设备A是某安全系统中的一台部署在边界上的网络加密机：则对应的安全空间的表示为P(3,1,1)——即(网络层、边界、机密服务)，细化一层P(3,192.168.0.1,1.2)——假设该网络加密机的IP为192.168.0.1，加密强度中等SML2。

安全系统在安全空间的表示，可以通过网络拓扑发现结合设备注册自动实现。安全系统在安全空间表示完成后，形成的三维图形称为态势图。通过对态势图分析，安全管理平台能比较直观地发现安全系统中防御部署薄的弱环节，调整安全防御力量的分配。

3.3 安全系统的动态表示

安全系统的运动过程可以抽象成安全状态的变迁[7]，如图3所示。



I-初始态，G-正常态，E-增强态，V-脆弱态，F-受损态

图3 安全状态的变迁图

3.4 态势图的定量表示

安全态势可以用一个二维表表示。二维表是安全系统当前状态在安全空间中的定量表示，表格的横向对应安全空间中的y轴上的数值，表格的横向对应安全空间中的x轴上的数值，表格中的数据对应安全空间中的z轴上的数值，如表1所示。

表1 态势图的二维表表示

	4	3	2	1
7	d_{74}	d_{73}	d_{72}	d_{71}
6	d_{64}	d_{63}	d_{62}	d_{61}
5	d_{54}	d_{53}	d_{52}	d_{51}
4	d_{44}	d_{43}	d_{42}	d_{41}
3	d_{34}	d_{33}	d_{32}	d_{31}
2	d_{24}	d_{23}	d_{22}	d_{21}
1	d_{14}	d_{13}	d_{12}	d_{11}

定义1 安全服务能力 $d_{ij}=\sum_{k=1}^{3} k*\gamma_k$

其中：k定义了偏序关系的安全服务类型，γ_k是安全服务类型权重因子，在上文定义的偏序关系中，可用性安全服务的权重因子>机密性安全服务的权重因子。$k>0$安全机制提供安全保护，$k=0$安全机制的保护能力丧失，$k<0$被保护对象受到攻击，且损失。

定义2 整体防御能力 $D=\sum_{i=1,j=1}^{i=7,j=4}(i*\alpha_i)*(j*\beta_j)*d_{ij}$

其中：i表示OSI-RM中的层次，α_i是层次权重因子。一般层次越高，层次权重因子越大，即$\alpha_7>\alpha_1$。

j表示安全区域的深度，β_j是深度权重因子。一般深度越深(靠近核心)深度权重因子越大，即$\beta_4>\beta_1$。

即整体安全防御能力是各区域、各层安全服务能力的总和。例如：

初始态的整体防御能力 $D_I=0$；

正常态的整体防御能力 $D_G>0$；

增强态的整体防御能力 $D_E>0$ 且 $D_E>D_G$；

脆弱态的整体防御能力 D_V，$0\leqslant D_V<D_G$ 且 $\forall ij$，$d_{ij}\geqslant 0$

受损态的整体防御能力 $D_F<D_G$ 且 $E_{ij}, d_{ij}<0$

定义 3 安全系统脆弱级别 L，最危险级 L_{red}（红色警报）：$D_v=0$。即，安全系统的安全服务能力完全丧失。次危险级 L_{orange}（橙色警报）：$D_v=D_G/2$。即，安全系统的安全服务能力丧失一半。

3.5 态势图模型

表示安全系统安全状态变迁过程的态势图序列称为态势图模型。用该模型表示图 3 的安全系统状态变迁过程如图 4 所示。

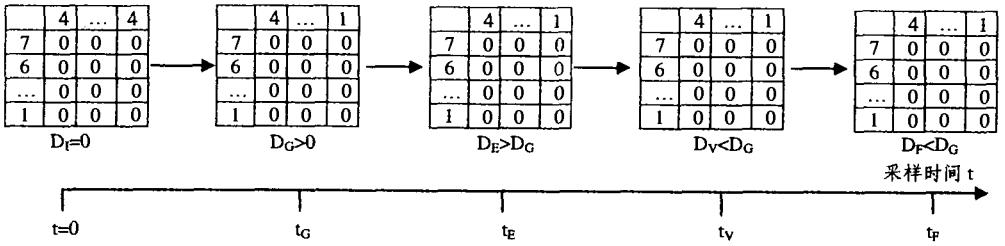


图 4 图 3 对应的态势图模型

态势图模型是一种能根据安全管理需求动态可扩展的模型。其可扩展性表现在两个方面：时间维方面，可以增加或减少采样频率，得到不同帧率的态势图序列；空间维方面可以细化或粗化空间坐标精度，得到不同分辨率的态势图。例如，如果要分析特定时间段攻击者特征，则可用较大采样频率和较高分辨率的态势图模型，精确地显示攻击路径。如果要发布总体安全防御能力，则将空间各维归并成单一标量 D，对于图 4 的归并结果如图 5 所示。

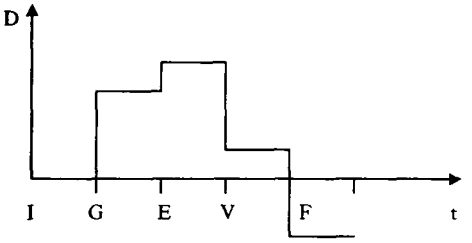


图 5 防御能力变化曲线

小结 本文提出态势图模型，详细阐述了该模型对安全系统的静态、动态表示方法，并定义了安全系统防御能力定量算法。与以往模型相比，该模型较好地满足了安全管理平台的需求，实现协同安全管理的目标。该模型已被应用在南大苏富特安全管理平台中，成为苏富特安全管理平台的中枢。

本文相关的研究工作为国家“八六三”和国家自然科学基金项目奠定了较好的理论基础和相应的系统原型。

致谢 感谢江苏省地税局和盐城市地税局提供为本文提供了网络安全试验环境。

参 考 文 献

1 网御安全管理平台产品白皮书. http://www.infosec365.com.cn/
2 http://www-900.ibm.com/cn/software/tivoli/solution/automation
3 Bell D E, LaPadula L J. Secure Computer Systems: Mathematical Foundations and Model. M74-244, The Mitre Corp., Bedford, Mass. May 1973
4 信息处理系统开放系统互连基本参考模型-第二部分：安全体系结构. GB/T9387.2-1995
5 The Information Assurance Technical Framework (IATF) document. Release 3.1. National Security Agency Information Assurance SolutionsTechnical Directors, 2002
6 信息安全理论与技术. 人民邮电出版社，2003.9
7 Charactering Intrusion Tolerant Systems Using A State Transition Model. http://wwww.anr.mcnc.org/projects/SITAR/papers/darpa00.pdf, 2000

（上接第 34 页）

的一小部分，因而可以通过 Push 与数据分发等技术将这部分信息及时、主动、无拥堵地送给喜爱它的用户，从而构成主动服务网格环境。

参 考 文 献

1 Strogatz S H. Exploring comlex networks, Nature, 2001, 410: 268～276
2 Albert J, Barabási A L. Statistical mechanics of complex networks. Rev. Mod. Phys., 2002(74): 47～97
3 Dorogovtsev S N, Mendes J F F. Evolution of networks, Adv. Phys., 2002, 51: 1079～1187.
4 Adamic L A, Huberman B A. Growth dynamics of the World Wide Web. Nature, 1999, 401: 131
5 Albert R, Jeong H, Barabási A-L. Diameter of the World-Wide Web, Nature 401, Sept. 1999. 130～131
6 Cooper C, Frieze A. A general model of web graph, In ESA, 2001. 500～511
7 Adamic L A, Huberman B A. Power-law distribution of the world wide web, Science, 2000, 287: 2115
8 Albert R, Barbási A-L, Jeong H. Scale-free characteristics of random networks: the topology of the world-wide web. Physica A, 2000, 281: 69～77
9 Barabasi A-L, Bonabeau E. Scale-free Networks. Science American, 2003(5): 50～59
10 Dorogovtsev S N, Mendes J F F, SamukhinA N. Structure of growing networks with preferential linking, Phys. Rev. Lett., 2000, 85: 4633～4636
11 Watts D J, Strogatz S H. Collective dynamics of 'small-world' networks, Nature 393 June 1998. 440～442
12 Barabási A-L, Albert R. Emergence of scaling in random networks, Science, 1999, 286: 509～512
13 Foster I, Kesselman C, Nick J, S Tuecke. The physiology of the grid: An open grid services architecture for distributed systems integration. globus, 2002
14 Foster I, Gannon D, et al. Open Grid Services Architecture Platform (OGSA). 2003. https://forge.gridforum.org/projects/ogsa-wg
15 Web Services Architecture: http://www.w3.org/TR/ws-a rch
16 曾春，邢春晓，周立柱. 基于内容过滤的个性化搜索算法. 软件学报，2004, 14(5): 999～1004