基于数据融合模型的网络安全量化评估系统设计与实现

汪 渊 齐善明 杨 槐
(解放军炮兵学院二系指挥自动化教研室 合肥 230031)

摘 要 当前,对网络安全的整体态势进行定量分析是解决网络安全预警和防范的重要手段。通过对网络安全量化过程进行分析,提出了网络安全量化系统的功能结构,给出了相关量化分析技术,并实现了原型系统。

关键词 网络安全,量化评估,数据融合
中图法分类号 TP393 **文献标识码** A

Construction and Research of Network Security Qualification Evaluation System

WANG Yuan QI Shan-ming YANG Huai
(2th Department of Artillery Academy of PLA, Hefei 230031, China)

Abstract Now making a quantified analysis on the whole situation of the network security is the important means for solving the network security alarm and prevention. Through the analysis on the network security qualification process, this paper proposed the function structure of the network security quantification system, analyzed the related quantification technology, and gave the related function implementation.

Keywords Network security, Quantification evaluation, Data fusion

1 引言

随着网络复杂性的不断增加,如何综合各种确定的与不确定的、完全的和不完全的信息对当前的网络安全态势进行量化分析与智能评估是网络安全领域研究发展需要解决的问题,尤其在网络信息战中,量化评估是指挥者进行各种决策活动的基础。网络安全量化评估指为了获得更精确的安全威胁行为以及得到更全面、及时的网络目前安全状态和威胁估计,涉及检测、关联、相关、估计及数据与信息联合的多级别、多方面的一种处理。本文研究的网络安全量化评估系统是一种协同式主动安全态势评估系统,将多种安全手段(如入侵检测系统、主动式漏洞扫描工具以及相关网络管理工具)融合在一起,使它们实现信息共享,并且利用它们之间信息的互补性,可以进行更大信息范围的关联、整体安全态势的动态推理以及整体的安全威胁分析。目前属于这种类型的系统主要有CCS[1]和DASSA[2]。

2 数据融合模型流程分析

数据融合技术是融合多种信息的一种有效手段[3,4],在网络安全量化评估中,一个完整的信息融合流程主要包括以下功能需求:

(1)特征采集:包括各方面特征信息的采集,即各种入侵检测系统前端针对网络及主机采集的相关信息、网络管理系统采集的网络环境相关信息、漏洞扫描得到的相关信息、人的经验信息、系统的一些相关的历史信息等;

(2) 提取特征及格式化:对各种探测信息进行格式标准化,将数据整合为统一的知识表达形式;

(3)真伪辨别:对于伪信息或无价值的信息应予删除,以消除冗余;

(4)相关处理:判断各信息源的信息是否属于同一入侵,是新入侵行为还是以前发现的入侵行为;

(5)识别:主要是根据各种特征对入侵的类型进行判断;

(6)综合处理:对不同时间和不同地点获得的同一入侵特征信息予以综合;

(7)可信度估计:对入侵特征的真伪程度及其它入侵特征属性的可靠程度做出量化估计;

(8)态势预测:对全部入侵特征联合在一起对网络安全态势及入侵行为和入侵威胁程度进行估计;

(9)价值分析:根据入侵行为的量化指标对入侵行为进行综合价值分析;对各种入侵的威胁程度进行价值分析;

(10)图形显示:把各种数据及相关信息显示成图形或文字,以形成直观网络安全态势分析结果。

量化评估系统中的信息融合层次模型如图1所示。

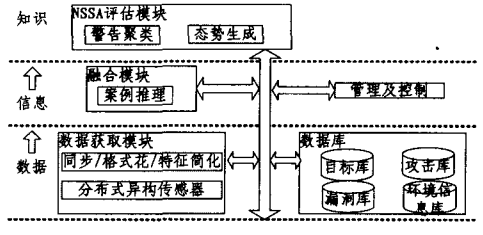

图1 信息融合层次模型

到稿日期:2009-11-06 返修日期:2010-02-07 本文受国防预研基金200109"网络安全量化"项目资助。
汪 渊(1973-),男,讲师,主要研究方向为网络安全及数据集成,E-mail:simplewy@126.com;齐善明(1967-),男,副教授,主要研究方向为指挥自动化和辅助决策;杨 槐(1963-),男,副教授,主要研究方向为数据库系统和辅助决策。

3 原型量化评估系统结构与实现

根据网络安全量化评估的数据融合模型，我们设计了初步的网络安全量化评估系统，其主要包括数据采集模块、关联分析模块、数据库管理模块及态势分析模块，功能性框图如图2所示。

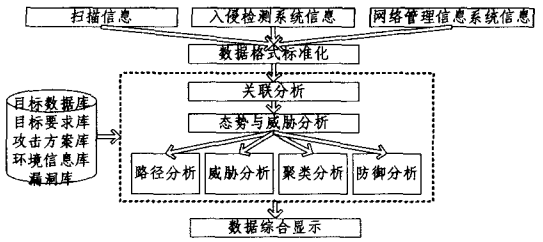

图2 安全量化评估系统功能框图

系统的主要模块说明如下：

1. 数据采集：网络安全整体态势的评估所需的数据源是多方面的，因为每一种安全手段所获取的数据及关注的重点都是片面的。量化系统中考虑的主要数据源如下：(1)入侵检测系统；(2)扫描系统：可以报告主机的或网络的脆弱性，本文中主要采用插件式 Nessus 安全扫描器；(3)网络管理系统：可以报告网络设备的相关信息，其主要功能有：性能监控、故障检测及网络发现；

2. 关联分析：结合各种辅助库，对各种数据源数据进行关联分析，得出攻击的类型，如基于以下因素进行一些合并推理：操作系统类型、软件平台、硬件类型、应用类型等；

3. 态势与威胁分析：对各种攻击行为进行综合显示，并提供基于辅助库的一些攻击企图的推测与分析，如基于拓扑图可以进行攻击发生的可能性分析、代价分析、路线分析；

4. 数据库管理模块：为了实现系统数据融合功能，系统需要建立以下数据库：网络攻击方案库、环境信息库、漏洞库、目标数据库和目标要求库。

4 关键技术分析

4.1 基于案例的安全态势推理

整个网络的多点脆弱性的产生与传播机理用图论来描述较形象且直观，但在软件的具体实现上，用案例推理则较为容易。因为对网络脆弱性的推理分析是基于知识的推理过程，而案例推理对知识的表达比较直观也比较有效，且案例库容易更新，所以在实际问题的解决中应用非常广泛。由于脆弱性的直观表示形式也是由多种属性及相应的后果所组成，其与案例表达方式非常相似，且案例可以表达那些不易分解为单个规则的推理关系，因此用 CBR(case-based reasoning)作为脆弱性分析的推理机制是合适的[5]。案例推理是有效地解决问题的方法，具体推理如图3所示。

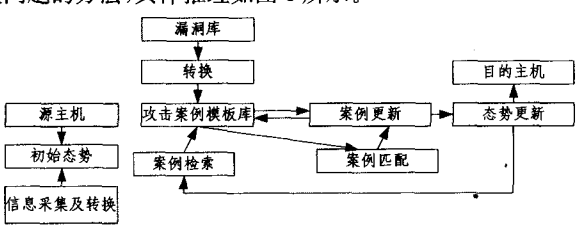

图3 基于案例推理的脆弱性检测

4.2 基于层次分析的漏洞威胁分析

从实际的统计数据显示可以看出，在实际网络环境中许多安全事故的发生都利用了已知的安全脆弱性，同时融合了入侵者的智慧，因此建立完善的已知漏洞信息的威胁程度知识库是网络安全威胁量化分析的一个重要方面。我们通过对网络系统安全机制及安全事故报告的分析，总结出各种安全脆弱性的特点，并运用层次分析法对各种安全脆弱性的威胁进行定量分析[6]。

层次分析法是一种定性与定量相结合的系统评估方法，针对网络安全脆弱性的威胁要素具有一定的层次关系，选择层次分析方法是符合网络安全这个具体问题的，层次分析法的原理及相关概念可以参考文献[4]，它的实施步骤主要有5步：

(1)建立层次结构模型；

(2)构造判断矩阵；

(3)层次单排序及其一致性检验的计算；

(4)层次总排序及其一致性检验的计算；

(5)必要时，对判断矩阵及层次模型作修正与调整。

网络安全漏洞层次分析模型如图4所示，其中各个底层要素的具体含义如下：

(1)条件关联性：指对入侵所需的条件多少及各个条件的确定性进行分析；

(2)入侵可检测性：指对入侵手段的隐蔽性及由此所造成的漏报率进行分析；

(3)入侵可处理性：指对入侵事件的处理所消耗资源多少进行分析；

(4)入侵条件存在的普遍性：指对入侵条件在实际网络环境中存在的可能性进行分析；

(5)入侵条件存在时间：指对入侵所利用的脆弱性已存在的时间进行分析；

(6)入侵可操作性：指对入侵所需的技术要求难度进行分析；

(7)入侵的持续性：指对入侵在达到目的前所需的持续时间进行分析；

(8)入侵后果的影响：指对入侵所能获得的信息重要等级进行分析；

(9)入侵对象的重要性：指对入侵对象角色的重要性进行分析。

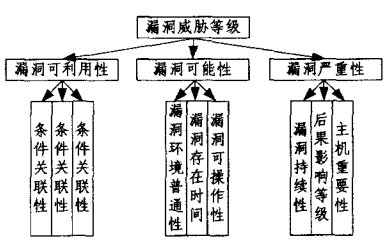

图4 安全漏洞威胁量化的层次分析模型

4.3 基于攻击性质相似度的聚类分析

网络环境中各种安全相关信息量非常大，而且它们有许多是重叠相关的[5]，大量数据的无分类状态隐藏了数据的真实结构，所以对数据进行聚类分析可以揭示大量数据中的真实结构，筛选出有意义的数据特征。

聚类分析主要是确定两个信息源的相似度，相似性计算主要有以下几种类型：

(1)两条信息之间的相似性计算；

(2)两个信息属性之间的相似性计算。

如根据攻击类型的相似性，可以进行聚类分析，分析攻击的企图及不同类型的相似性可以用图 5 的相似矩阵来表示。

	INVALID	PRIVI-LEGE_ VIOLA-TION	USER_ SUBVER-SION	DENIAL OF SERVICE	PROBE	ACCESS_ VIOLA-TION	INTEG-RITY_ VIOLA TION	SYSTEM_ ENV_ CORRUP-TION	USER_ ENV_ CORRUP-TION	ASSET_ DISTRESS	SUSPIC-IOUS_ USAGE	CONNEC-TION_ VIOLATION	BINARY_ SUBVER-SION	ACTION_ LOGGED
INVALID	1	0.3	0.3	0.3	0.3	0.3	0.3	0.3	0.3	0.3	0.3	0.3	0.3	0.6
PRIVILEGE_ VIOLATION	0.3	1	0.6	0.3	0.6	0.6	0.6	0.6	0.4	0.3	0.4	0.1	0.5	0.6
USER_SUBVE RSION	0.3	0.6	1	0.3	0.6	0.5	0.5	0.4	0.6	0.3	0.4	0.1	0.5	0.6
DENIAL OF SERVICE	0.3	0.3	0.3	1	0.6	0.3	0.3	0.4	0.3	0.5	0.4	0.1	0.5	0.6
PROBE	0.3	0.2	0.3	0.3	1	0.7	0.3	0.3	0.3	0.3	0.4	0.8	0.3	0.6
ACCESS_VIO LATION	0.3	0.6	0.2	0.5	0.6	1	0.6	0.6	0.3	0.3	0.4	0.1	0.5	0.6
INTEGRITY VIOLATION	0.3	0.5	0.3	0.5	0.6	0.8	1	0.6	0.5	0.3	0.4	0.1	0.5	0.6
SYSTEM ENV CORRUPTION	0.3	0.5	0.3	0.5	0.6	0.6	0.6	1	0.6	0.3	0.4	0.1	0.5	0.6
USER ENV CORRUPTION	0.3	0.5	0.3	0.3	0.6	0.6	0.6	0.6	1	0.3	0.4	0.1	0.5	0.6
ASSET_DISTR ESS	0.3	0.3	0.5	0.6	0.3	0.3	0.3	0.3	0.3	1	0.4	0.4	0.3	0.6
SUSPICIOUS_ USAGE	0.3	0.3	0.3	0.3	0.5	0.6	0.5	0.6	0.5	0.3	1	0.1	0.3	0.6
CONNECTION _VIOLATION	0.3	0.1	0.1	0.3	0.8	0.3	0.3	0.3	0.3	0.5	0.4	1	0.3	0.6
BINARY_SUB VERSION	0.3	0.3	0.3	0.3	0.3	0.6	0.6	0.6	0.5	0.3	0.4	0.1	1	0.6
ACTION_LOG GED	0.3	0.3	0.3	0.3	0.6	0.5	0.3	0.3	0.3	0.3	0.4	0.3	0.3	1

图 5　攻击类型相似性矩阵

5　系统实现与实验分析

整个网络安全量化评估系统建立在一个实际的网络环境中，系统由客户端和服务器端两部分组成。服务器端提供多种安全检测与防御程序服务，客户端主要是用于操作、配置和显示。在服务端还采用了 plug-in 的体系，允许用户加入执行特定功能的插件，通过插件，可以即时更新和扩展安全量化评估系统功能。系统试验运行环境如图 6 所示。

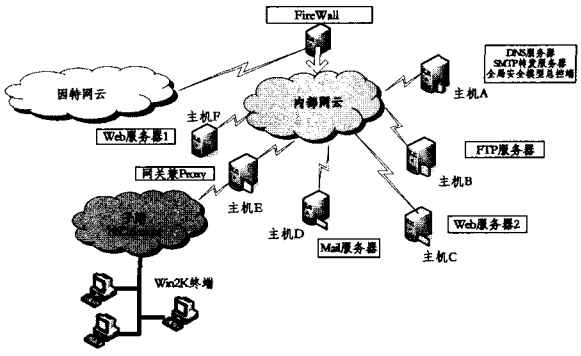

图 6　试验网络配置

配置如表 1 所列。

表 1　目标网络系统配置表

主机名	操作系统类型	是否装有防火墙	是否装有评估系统	运行主要服务	网络带宽
A	Solaris2.7	是	是	DNS,SMTP	1G
B	Redhat7.2	是	是	Wu-FTP6.3, Tlenet	1G
C	Win2KAS(SP1)	是	是	IIS(http,ftp…)	1G
D	Solaris2.7	是	是	Qmail	1G
E	Redhat7.1	是	是	Squid,Nat, telnet	1G
F	Redhat7.1	是	是	Apchace	1G
终端	Win2KP(SP2)	否	否		100M

实验系统中检测的攻击数据如图 7 所示(其中横坐标代表端口号)。

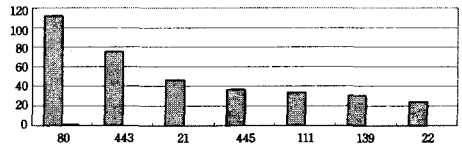

图 7　实验环境下攻击检测数据

在实验中，利用量化评估系统，可以对大量的攻击行为进行深层次的处理，可以针对多步攻击进行推理，对类似攻击进行聚类，并且对攻击可能的渗透路径及威胁提供一定的分析功能，并能提供一定的智能分析功能。

结束语　整个系统主要在 Windows 系列平台上运行，采用的开发工具为 MICROSOFT VC6.0。通过网络安全量化评估系统，可以较好地对大量攻击行为进行分析，增强对网络整体安全态势的理解。整个平台以插件式实现，功能可以根据网络攻防相关技术的发展而扩展，具有可扩展性、低成本性和易用性。同时，网络安全评估量化评估是一个分布式安全信息采集、数据融合和分析的过程，需要涉及到的问题很多，如何对目标网络进行拓扑分析、如何对目标网络进行安全态势估计、如何更好地将人工智能理论融入到具体的软件设计

(下转第 147 页)

(4)报警器时间行为协议(Alert)

(? alert^;! alert#)[1]或者表示为? alert[1]。

前两个构件在{pressure}事件集合上组合后,其时间行为协议为:

```
(τpressure[18]^;τpressure#;
(
! low^[20]▷2(Reset(t);(! alert^;? alert#)[1]);? low[21]#;Idle(18-t)
+! high^[20]▷2(Reset(t);(! alert^;? alert#)[1]);? high[21]#;Idle(18-t)
+Idle(18);
)
)*;
```

4个子构件组合成一个构件(系统/子系统),其时间行为协议为:

```
(τpressure[18]^;τpressure#;
(
τlow^[20]▷2(Reset(t);(τalert^;τalert#)[1]);τlow[21]#;Idle(18-t)
+τhigh^[20]▷2(Reset(t);(τalert^;τalert#)[1]);τhigh[21]#;Idle(18-t)
+Idle(18);
)
)*;
```

该锅炉压力控制系统中存在着时间限制等信息,如果不对行为协议进行实时扩展,则无法对系统行为进行有效的描述。在系统形式化描述的基础上,我们可以方便地根据相容性算法检测系统的各种错误。

结束语 本文针对复杂实时构件系统的快速发展及形式化描述和验证的需求,对主流构件模型及各种实时行为形式化描述方法进行了分析,在对SOFA构件模型采用的行为协议进行实时性扩展的基础上提出了时间行为协议TBP并给出了基于时间行为协议的相容性验证算法。TBP具有良好的形式化基础,语法语义定义完整,对带时间的并发进程表达清晰简洁,可以在构件系统的分析设计中提供构件行为实时属性的形式化描述,减少开发人员对系统行为理解上的歧义。基于TBP模型,可以对构件组合的相容性进行验证,本文为此提供了理论基础。我们将进一步开展构件实时行为建模、验证实用工具的开发实现研究。

参 考 文 献

[1] Szyperski C, Gruntz D, Murer S. Component-Software: Beyond Object-oriented Programming(Second Edition)[M]. New York: ACM Press, Addison-Wesley, 2002: 12-18

[2] Alagar V, Mohammad M. A component model for trustworthy real-time reactive systems development[C]// Formal Aspects of Component Software(FACS'07). Sophia-Antipolis, France: ENTCS, Elsevier, Sep. 2007: 1-15

[3] Moller A, Akerholm M, Fredriksson J, et al. Evaluation of component technologies with respect to industrial requirements[C]// Proceedings of the 30th EUROMICRO Conference(EUROMICRO'04). Los Alamitos, CA, USA: IEEE Computer Society, 2004: 56-63

[4] Xie Fei, Browne J C. Verified systems by composition from verified components[J]. ACM SIGSOFT Software Engineering Notes, 2003, 28(5): 277-286

[5] Jezek P, Kofron J, Plasil F. Model Checking of Component Behavior Specification: A Real Life Experience[J]. Electronic Notes in Theoretical Computer Science, 2006, 160: 197-210

[6] Kofron J. Checking Software Component Behavior Using Behavior Protocols and Spin[C]// Proceedings of the 2007 ACM Ssymposium on Applied Computing. New York: ACM Press, 2007: 1513-1517

[7] Plasil F, Visnovsky S. Behavior Protocols for Software Components[J]. IEEE Transactions on Software Engineering, 2002, 28(11): 1056-1076

[8] Allen R, Garlan D. A Formal Basis for Architectural Connection[J]. ACM Trans. Software Eng. and Methodology, 1997, 6(3): 213-249

[9] 潘颖,赵俊峰,谢冰. 构件库技术的研究与发展[J]. 计算机科学, 2003, 30(5): 90-93

[10] 谢冰,杨芙清. 青鸟工程及其Case工具[J]. 计算机工程, 2000, 26(11): 76-78

[11] Alagar V, Mohammad M. A component model for trustworthy real-time reactive systems development[C]// Formal Aspects of Component Software(FACS'07). Sophia-Antipolis, France: ENTCS, Elsevier, Sept 2007: 1-15

[12] Reed G M, Roscoe A W. A timed model for communicating sequential processes[J]. Theoretical Computer Science, 1988, 58(13): 249-261

[13] Alur A W, Dill D L. A theory of timed automata[J]. Theoretical Computer Science, 1994, 126(2): 183-235

[14] Henzinger T A, Manna Z, Pnueli A. Temporal proof methodologies for timed transition systems[J]. Information and Computation, 1994, 112(2): 273-337

[15] 郭亮,唐稚松. 基于XYZ/E描述和验证容错系统[J]. 软件学报, 2002, 13(5): 913-920

[16] Schneider S A. An operational semantics for timed CSP[J]. Information and Computation, 1995, 116(2): 193-213

[17] Jezek P, Kofron J, Frantisek P. Model Checking of Component Behavior Specification: A Real Life Experience[J]. ENTCS, 2006, 160(6): 197-210

[18] 黄靖,卢炎生,徐丽萍. RTCS:一种具有精确语义的实时构件描述机制[J]. 计算机科学, 2005, 32(8): 205-208

(上接第129页)

中去以及如何更好地协调好人机结合问题等,都需要进行长时间的深入研究。量化涉及到大量专业知识和数学知识,本文对其中的部分问题进行了初步研究,其中的大量细节工作还需进一步研究。

参 考 文 献

[1] D'Ambrosio B, et al. Security Situation Assessment and Response Evaluation(SSARE)[C]// DARPA Info. Survivability Conf. & Expo. 2002

[2] D'Ambrosio B, Takikawa M, Upper D. Representation for Dynamic Situation Modeling IET report[R]

[3] Hall D L. Mathematical Techniques in Multisensor Data Fusion[Z]. Artech House, Inc., 1992

[4] Hall D L, Llinas J. An Introduction to Multisensor Data Fusion[C]// Proceedings of the IEEE. vol 85, January 1997

[5] 汪渊,蒋凡,陈国良. 一种基于安全案例推理的网络安全分析方法[J]. 小型微型计算机系统, 2003, 24(12): 2082-2085

[6] 汪渊,蒋凡,陈国良. 基于图论的网络安全分析方法研究与应用[J]. 小型微型计算机系统, 2003, 24(10): 1865-1869