文章编号:1001 - 2486(2004)01 - 0036 - 05

网络安全脆弱性分析与处置系统的研究与实现*

胡华平,刘 波,钟求喜,庞立会
(国防科技大学计算机学院,湖南 长沙 410073)

摘 要:在分析国内外研究现状的基础上,针对现有的漏洞库系统在漏洞信息的组织、使用等方面存在的不足,采用分布计算技术、数据库技术、Web 技术实现了网络安全脆弱性分析与处置系统。该系统实现了基于 Web 的漏洞库(含补丁库)的访问与维护工具,便于获取相应漏洞的解决方案和下载相应的补丁程序,降低了系统维护的开销,提高了系统的可维护性;补丁推送程序实现了对系统补丁程序的远程推送、漏洞修补和补漏检测,提高了系统的自动化程度,为网络安全脆弱性处置提供了有力工具。

关键词:网络安全脆弱性;漏洞库;中间件技术;Web 技术;补丁程序
中图分类号:TP393.08 文献标识码:A

Study and Implementation of Network Security Vulnerabilities Analysis and Disposition System(NSVADS)

HU Hua-ping,LIU Bo,ZHONG Qiu-xi,PANG Li-hui
(College of Computer,National Univ. of Defense Technology,Changsha 410073,China)

Abstract: After analyzing the research situation and the shortcoming of vulnerabilities database system, the distributed computing technology, database technology and Web technology are used to implement NSVADS. Based on Web, it realizes the access and maintaining tool to vulnerabilities database. The solution to vulnerabilities and patches download can be disposed easily, and the cost of system maintainability can be reduced. Patches pushed modular can realize long-range patches pull, vulnerabilities mend, and vulnerabilities detection. It can improve the system's automatical vulnerabilities mend, and provide helpful tool for disposing the network security vulnerabilities.

Key words: network security vulnerabilities; vulnerabilities database; middle-ware technology; Web technology; patches

随着网络的发展,网络安全问题日益突出,操作系统的安全性已经无法满足对安全高度敏感的部门的需要,黑客入侵事件时有发生。操作系统及在其上运行的应用程序暴露出越来越多的漏洞[1]。目前,分析网络系统的安全隐患一般从分析系统的漏洞或者缺陷开始,如何对这些漏洞进行收集、整理、研究、再现,并提出防范措施,就成了网络信息系统安全的关键环节。

漏洞是指由于系统硬件、软件或者是安全策略上的错误而引起的缺陷,是违背安全策略的软件或硬件特征,是某种形式的脆弱性,从而可以使个别用户能够利用这种脆弱性非法访问系统或者破坏系统的正常使用。无论是硬件平台还是软件平台都存在漏洞[2]。

计算机系统漏洞库主要集中了现有系统中已发现的各种软、硬件漏洞特征和应对措施,它是信息安全基础设施中重要的一环。国外在 1995 年左右便开展了相关的研究工作。目前,国外的许多重要安全组织和厂商都建立了自己的漏洞数据库并开展了相关的研究,一般是从 BUGTRAQ 和 NTBUGTRAQ 等邮件列表中获取漏洞信息,并从 CERT 等安全组织获取修补建议[3~8]。

当前,国外的漏洞数据库主要分为两类,一类是受限分布的私有数据库,它们通常具有重要的商业或军事价值[3,5];另一类是公开可共享的漏洞数据库[7]。由于私有漏洞库具有重要的军事或商业价值,很难获得它的相关资料,因而无法进行相关比较;而后一种漏洞库的利用价值一般都很低,它们主要是

* 收稿日期:2003 - 06 - 02
基金项目:国家 863 高技术资助项目(2001AA142030)
作者简介:胡华平(1967—),男,副研究员,博士后。

为存储信息而不是为实现自动处理设计的,其中部分漏洞库支持简单的查询功能,但是它们通常不支持对所存储信息进行基本的分析工作。国内建有漏洞数据库的组织还很少,而且已经建立的漏洞数据库基本是照搬的描述性安全公告。

上述国内外这些已有的计算机系统漏洞库的共同特点是:建立漏洞库的目的主要是存储与组织漏洞相关的信息,并在此基础上提供这些信息的检索。其中一些组织较好的漏洞库,可以提供良好的检索方式:查找特定版本操作系统的现存漏洞信息,显示特定漏洞的已发布的补丁程序,显示利用有关漏洞的脚本等。但是,这些漏洞库一般不提供应用程序访问接口(API)来支持基于程序的针对系统漏洞(脆弱性)的自动处理,大量的漏洞(脆弱性)数据更多地被用于人工检索,并不能得到及时、高效的利用,造成了一定程度上的资源浪费。例如,系统漏洞(脆弱性)扫描工具用于发现所要检测的信息基础设施的基本安全状态,这些漏洞(脆弱性)扫描工具又几乎完全是以现有的漏洞(脆弱性)特征数据作为依据和基础,而国内外现有的各种漏洞库几乎无法直接、自动地为这些漏洞(脆弱性)扫描程序提供所需要的漏洞特征数据;另一方面,以系统漏洞(脆弱性)扫描的结果为基础而实施的各种应对措施,例如补丁程序的获得和应用,也由于缺乏漏洞库应用程序访问接口而不得不需要大量的人工支持才能得以完成。

因此研制一种集漏洞收集、补丁程序的下载与推送、漏洞修补的验证于一体的网络安全脆弱性分析与处置系统是十分必要的,也是军队、政府机关等与互联网物理隔离的信息系统提升自身网络安全水平所必须的。

1 脆弱性分析与处置系统简介

本文采用分布计算技术、数据库技术、Web 技术实现了脆弱性分析与处置系统。整个系统采用基于 CORBA 技术的三层 Browser/Server 体系结构实现,其逻辑结构见图 1,它建立在 Microsoft Windows NT 4.0/Microsoft Windows 2000 操作系统之上;漏洞库选用关系数据库管理系统 Oracle 8i;对漏洞库中的漏洞相关数据进行发布、更新、查询、删除等的管理信息系统接口模块采用 ASP 技术,以基于 Web 的动态页面方式实现;提供漏洞库应用程序访问接口 API 的漏洞库访问服务基于遵循 CORBA 标准的 StarBus for Java、StarBus for C++ 中间件开发实现;补丁推送程序是驻留在所关心的主机或系统上的代理,它由事件/通告管理服务根据安全策略激活的;系统各部件之间的通信基于 SSL 协议完成。本系统的特点有:

• 高效地规划和组织漏洞存储数据库完成系统漏洞相关数据,包括系统漏洞特征描述、应对措施、补丁程序、系统安全配置策略等的存储;

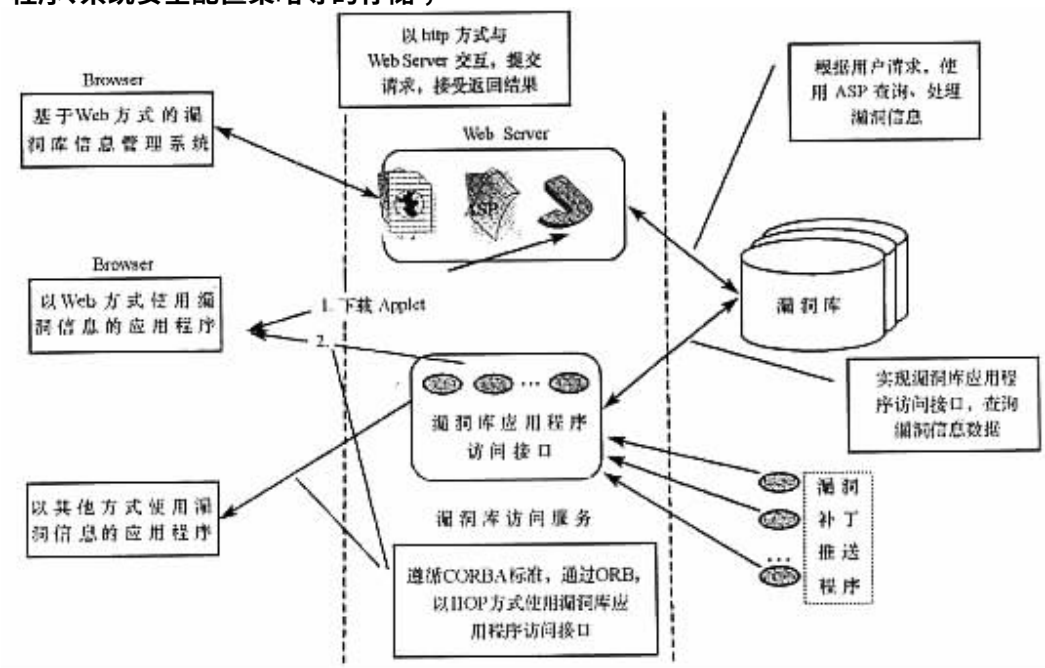

图 1 脆弱性分析与处置系统逻辑结构

Fig.1 The logic structure of NSVADS

• 用户使用 Browser,通过 Web 服务器向后台的漏洞存储数据库提交对漏洞相关数据进行发布、更新、查询、删除、使用等的请求,Web 服务器将处理的结果以动态 Web 页面的方式返回给用户;

• 遵循 CORBA 标准的漏洞库访问服务部署在应用服务层,提供通用的漏洞库应用程序访问接口 API,实现不同应用程序对漏洞库中存储的各类漏洞相关数据的访问和使用;

• 应用程序,例如系统脆弱性扫描工具、系统脆弱性应对程序、攻击程序,根据不同的具体需求,通过遵循 CORBA 标准的对象请求代理 ORB,向漏洞库访问服务提交漏洞相关数据的访问和使用请求,使用漏洞库访问服务封装的漏洞库应用程序访问接口,由漏洞库访问服务从漏洞数据库中获取并返回满足应用程序需求的漏洞相关数据;

• 通过 SSL 协议来实现网络传输的安全性。

2 漏洞库的设计与实现

漏洞库是系统安全隐患分析的核心,集中了常见的各类系统漏洞特征和相应的应对措施、网络系统当前的脆弱性状态,以及和系统漏洞分析与应对措施相关的系统安全配置策略;高效地规划和组织漏洞数据库是使其能够充分发挥作用的关键。漏洞库研究的难点在于:

• 定义通用的漏洞相关数据的描述、使用和交换格式,并且该格式与现有的标准兼容。为了使系统具有较强的开放性,尽可能地为每条漏洞信息提供 CVE (Common Vulnerabilities & Exposures) 编号;

• 设计基于关系数据库管理系统、具备良好扩充性的漏洞数据库,完成系统漏洞相关数据,包括系统漏洞特征描述、应对措施(主要是系统补丁程序)、系统安全配置策略等的存储;

• 设计一个界面友好、使用方便、高效的管理信息系统,以使用户/管理者可以通过良好的人机交互界面,完成存储在漏洞库中的漏洞相关数据的维护,提供对保存的漏洞相关数据的检索和使用。

图2 用户/管理者界面

Fig.2 User/administrator interface

漏洞库的用户/管理者界面如图2所示,它主要由以下模块构成:

(1) 漏洞信息的添加

当用户选择添加功能时,漏洞库系统首先生成一个空漏洞描述页面,等待用户选择该漏洞的种类、输入描述信息以及对应的补丁程序、攻击(测试)程序的名称。在用户提交该页面时,漏洞库系统使用 Request 对象获取用户输入的漏洞信息,并且从序列中获取一个值,结合用户填写的漏洞信息生成该漏洞的惟一标识,然后将该漏洞的信息作为一个记录添加到漏洞库中去。

(2) 漏洞信息的查询

用户可首先选择漏洞的类别,漏洞库系统将用户作出的选择作为查询的条件,在漏洞存储数据库中进行查询操作,得到结果集。调用动态生成页面的程序,生成符合用户查询条件的漏洞的简要信息列表,并且以 Web 页面的形式将这些查询结果返回给用户。

(3) 漏洞信息的更新

漏洞库系统首先在漏洞存储数据库中查询操作系统描述、漏洞类型描述,生成 Web 页面上相应的可选项,然后根据选定的操作系统类型和漏洞类型查询漏洞描述信息中的漏洞标识、漏洞简要描述,生成漏洞描述的简要信息列表;根据用户对该列表的选择,漏洞库系统结合漏洞惟一标识查询漏洞描述信息,生成该漏洞的详细信息描述页面;用户根据该页面,对漏洞存储数据库中的漏洞描述信息进行更新。

(4) 漏洞信息的删除

漏洞库系统首先在漏洞存储数据库中查询操作系统描述、漏洞类型描述,生成 Web 页面上相应的可选项,然后根据选定的操作系统类型和漏洞类型查询漏洞描述信息中的漏洞标识、漏洞简要描述,生成漏洞描述的简要信息列表;根据用户对该列表的选择,漏洞库系统结合漏洞惟一标识查询漏洞描述信

息,生成该漏洞的详细信息描述页面;用户根据该页面,从漏洞存储数据库中删除选定的漏洞描述信息。

漏洞库系统提供相应的上载目录保存补丁程序,然后可以在漏洞信息描述中填写对应所使用的补丁程序名称;在进行漏洞信息查询时,漏洞库系统根据该名称生成相应的超文本链接,提供补丁程序的下载;补丁程序信息的查询、更新、删除与漏洞描述信息的对应操作相类似。对攻击(测试)程序信息的添加、查询、更新、删除与补丁程序的对应操作相类似。

(5) 漏洞信息统计

进入编辑模式后,用户可以点击数据库统计选项,对漏洞存储数据库中的漏洞信息进行统计,获得不同操作系统漏洞的概要统计信息。

3 漏洞库应用程序访问接口

通过定义并且提供漏洞库应用程序访问接口 API,支持以漏洞库中存储的漏洞相关数据为基础的与系统漏洞相关的应用程序的自动处理,结合系统漏洞扫描和系统脆弱性应对,通过预定义的安全策略配置,使系统能够在安全隐患出现和被利用之前有机会将故障自动修复。其难点在于:提供通用的漏洞库应用程序访问接口 API,实现不同应用程序对漏洞库中存储的各类漏洞相关数据的访问和使用。

为了适应整个漏洞库的基于 CORBA 技术的三层 Browser/Server 体系结构,漏洞库应用程序访问接口的设计与漏洞库访问服务的开发按照以下步骤进行:

(1) 使用 IDL 语言来定义和描述漏洞库访问服务的公共接口

IDL 语言描述漏洞库访问服务对外提供、客户方应用程序可以访问的公有操作,即漏洞库应用程序访问接口。

(2) 使用 IDL 编译器生成框架代码

使用 idl 编译器,产生客户方 stub 代码和服务方 skeleton 代码。stub 代码负责将客户应用程序的漏洞库访问请求转换为网络请求。skeleton 代码帮助对象适配器(BOA)将一个具体的漏洞库访问请求传递到漏洞库访问服务对象的具体实现。

(3) 编写客户方主程序代码

客户方主程序主要包括初始化 ORB,获得漏洞库访问服务对象的对象引用,激活漏洞库访问请求三个部分。

(4) 编写漏洞库访问服务程序代码

漏洞库访问服务具体实现通过 IDL 语言定义和声明的漏洞库应用程序访问接口,提供各种应用程序访问和使用漏洞库中数据的支持。

(5) 编译客户和服务器代码

(6) 启动漏洞库访问服务,提供漏洞库应用程序访问接口

4 漏洞补丁推送功能的设计与实现

传统的信息发布技术都是基于请求/应答模式,基于这种模式的技术称为"拉"(pull)技术。在这种模式的系统中,用户请求服务器发回他们感兴趣的信息,信息传输的发起者是用户。采用这种模式的典型应用包括:ftp,gohper,www 等等。在这种系统中,用户必须周期性地检查服务器,才能得到最新的和更新后的信息。而通过采用推送的模式,应用可以将最新的或更新后的信息直接发送给大量的用户,而无须用户自己来取。推送模式吸引人之处在于它允许用户及时得到最新信息。从数据传输的角度来讲,推送是由服务器把信息主动送给客户。和拉相比,虽然数据传输的方向也是由服务器到客户,但是在推送系统中,服务器是主动的,信息传输的发起者是服务器,而不是客户的请求。推送最大的特点是服务器主动而客户是被动的[9]。

目前漏洞库系统所提供的安全服务为被动式服务,即只有用户访问漏洞库系统,查找相关漏洞的补丁程序或运行相关的验证程序,用户所使用系统的安全隐患才被修补,因此,系统的安全隐患的修补更多是靠人的自觉性来完成,缺乏主动性。参照病毒库更新的思路,本文提出漏洞补丁推送的思想,旨在变

被动式服务为主动式服务。其工作原理为：当有新的漏洞补丁程序出现或通过检测发现目标系统存在漏洞时，产生相应的告警事件；事件/通告管理服务以“PUSH”的方式激活驻留在目标系统中的漏洞补丁推送程序；漏洞补丁推送程序根据接收到的告警事件中包含的需要解决的系统漏洞标识，通过漏洞库访问服务，以“PULL”的方式获得对应的漏洞应对措施及相关数据，并最终完成漏洞修补与验证工作。漏洞补丁推送功能示意图如图 3 所示。

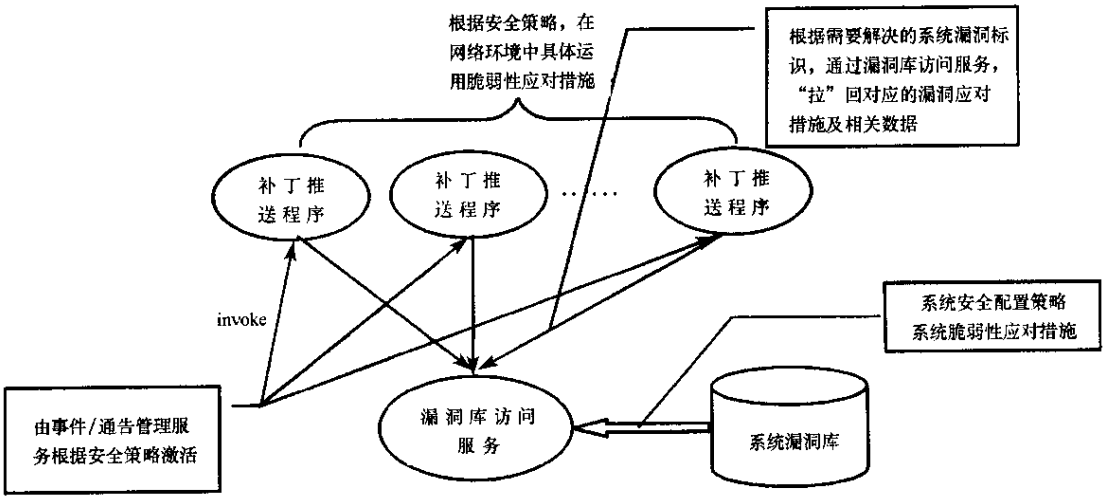

图 3 漏洞补丁推送示意图

Fig.3 The workflow of patches pull

漏洞补丁推送程序主要由初始化 ORB、获得漏洞库访问服务对象的对象引用、激活漏洞库访问请求、应用漏洞补丁等几个部分组成。漏洞补丁推送功能的实现基于 CORBA 分布对象计算标准，采用面向对象的设计方法，使得它具有较好的开放性和分布性，符合当前计算机发展的趋势，可以很好地实现主动服务功能。

5 结束语

网络安全脆弱性分析与处置系统已通过鉴定，该系统整体水平在国内处于领先，其中隐患分析与处置系统体系结构（利用 CORBA 中间件技术建立了数据库、处置业务和用户三层系统体系结构）和补丁程序的自动推送等方面达到了当前国际先进水平，建议该系统尽快推广使用。

虽然建立了脆弱性分析与处置系统，为信息基础设施安全隐患提供有效的解决方案和修补措施，但我们认为至少在系统的全面测试与应用研究、系统漏洞数量的增加、实现网络扫描系统与脆弱性分析与处置系统的联动等方面可以开展进一步的工作。

参考文献：

[1] 刘宝旭，吴海燕，许榕生．网络隐患扫描系统的研究与实现[J]．计算机工程与应用，2002，38(1)：11－13.

[2] 张怡，宣蕾，胡华平．IIS 漏洞原理及防护措施分析[J]．计算机应用，2002，22(4)：31－33.

[3] The CMET database at the Air Force Information Warfare (AFIW) Center (Air Force Information Warfare (AFIW) Center)[R]. http://afiwcweb.lackland.af.mil.

[4] The database at the Computer Emergency Response Team (CERT)[R]. http://www.kb.cert.org/vuls.

[5] The database of the Australian Computer Emergency Response Team (AUSCERT)[R]. http://www.auscert.org.au.

[6] The Coast (Computer Operations, Audit, and Security Technology) Vulnerability Database (CDV)[R]. http://www.cerias.purdue.edu/coast.

[7] The Vulnerability Database at Internet Security Systems (ISS)[R].http://www.iss.net/security_center/.

[8] The Vulnerability Database at INFILSEC (INFILSEC Systems Security)[R].http://www.infilsec.com.

[9] 郭长国．CORBA 事件服务的研究与实现[D]，国防科技大学，1999.