

分布式电信网漏洞管理系统的研究与设计

马子鹏

(西安邮电学院, 陕西 西安 710121)

摘要:漏洞是导致电信网安全隐患的重要原因之一。介绍了电信网漏洞的产生原因及分类方法;结合 CVE 的行业标准,给出了电信网安全漏洞所包含的属性描述;为了实现安全漏洞数据在网络上的传输和不同关系数据库之间的数据共享,采用了基于 XML 的漏洞属性表示模型,用来表示漏洞的属性数据;运用三层 J2EE 设计规范,设计了基于 B/S 模型的分布式电信网漏洞管理系统,以提供对漏洞库中所存储的电信网安全漏洞数据的发布、更新、查询、删除等功能。

关键词:漏洞分类;XML;漏洞表示;分布式

中图分类号:TP302

文献标识码:A

文章编号:1673-629X(2010)07-0145-04

Research and Design of Distributed Telecommunication Network Vulnerability Management System

MA Zi-peng

(Xi'an University of Posts and Telecommunications, Xi'an 710121, China)

Abstract: Vulnerability is an important factor that causes telecommunication network hidden trouble. Introduce the causes of creation and classification methods of vulnerability in telecommunication network. According to CVE, taxonomy and property of telecommunication network vulnerability is reviewed in this paper; In order to share vulnerability data, the presentation of vulnerability data is defined using XML; A distributed telecommunication network vulnerability management system of B/S mode in accord with J2EE component standard is designed to promulgate data, update data, query data, and delete data with the system.

Key words: taxonomy vulnerability; XML; presentation vulnerability; distributed

0 引言

随着现代社会的发展,电信网逐步进入了人们的生活,目前的电信网运行中,存在着诸多不安全的漏洞,由这些漏洞引起的不安全事件,不仅会影响电信网的正常运行,同样会对国家的财产造成严重的损失。

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷,从而可以使攻击者能够在未授权的情况下访问或破坏系统^[1]。电信网漏洞包括一切可导致威胁、损坏电信网安全性(完整性、可用性、保密性、可靠性、可控性)的因素。由于安全漏洞的存在致使非法用户侵入系统或者合法的用户可以进行未经授权的操作,危及了整个电信网的安全。

因此,深入研究电信网安全漏洞并建立可共享的分布式漏洞数据库管理系统对漏洞的进一步研究和对电信网的安全防御都具有重要意义。

1 电信网安全漏洞的产生及分类

产生电信网安全漏洞的主要原因有:一是网络系统以及系统内部本身的设计缺陷包括软件错误和硬件错误,比如出现逻辑错误和算法错误以及在生产产品时导致的产品缺陷。二是漏洞和具体的系统环境密切相关。在不同种类的软、硬设备,同种设备的不同版本之间,由不同设备构成的不同系统之间,以及同种系统在不同的设置条件下,都会存在各自不同的安全漏洞问题。三是漏洞问题与时间紧密相关。随着时间的推移,旧的漏洞会不断得到修补或纠正,新的漏洞会不断出现,因而漏洞问题会长期存在^[2]。

在对漏洞进行研究时,除了需要掌握漏洞本身的特征属性,还要了解与漏洞密切相关的其它对象的特点。漏洞的基本属性有:漏洞类型、造成的后果、严重程度、利用需求、环境特征等^[3]。与漏洞相关的对象包括:存在漏洞的软(硬)件、操作系统、相应的补丁程序和修补漏洞的方法等。

对电信网漏洞进行分类主要根据以下几方面:

(1)根据漏洞被攻击者利用的方式分类。

收稿日期:2009-11-06;修回日期:2010-02-18

基金项目:信息产业部软科学研究资助项目(2005R100)

作者简介:马子鹏(1977-),男,山东冠县人,硕士,助教,研究方向为分布式智能系统和信息安全。

本地攻击:攻击者是系统本地的合法用户或已经通过其它攻击方法获得了本地权限的非法用户。

远程攻击:攻击者是通过网络,对连接在网络上的任意一台机器进行攻击。可分为入侵攻击与破坏攻击两种方式^[4]。

(2)根据漏洞形成的主要原因分类。

同一系统漏洞,对其不同抽象层次研究,可能会归为不同的形成原因。

输入验证错误:未对用户输入数据的合法性进行验证,使攻击者非法进入系统。

缓冲区溢出:向程序的缓冲区中录入的数据超过其规定长度,造成缓冲区溢出,破坏程序正常的堆栈,使程序执行其他命令。

设计错误:程序设计错误而导致的漏洞。其实,大多数的漏洞都属于设计错误。

意外情况处置错误:程序在实现逻辑中没有考虑到一些意外情况,而导致运行出错。

访问验证错误:程序的访问验证部分存在某些逻辑错误,使攻击者可以绕过访问控制进入系统^[5]。

配置错误:系统和应用的配置有误,或配置参数、访问权限、策略安装位置有误。

竞争条件:程序处理文件等实体在时序和同步方面存在问题,存在一个机会窗口使攻击者能够施以外来的影响。

环境错误:一些环境变量的错误或恶意设置造成的漏洞。

(3)根据漏洞对系统安全造成的危害分类。

根据漏洞对系统安全造成的危害可分为有效性、机密性、完整性、安全保护。

(4)根据漏洞对系统安全造成的直接威胁分类。

根据漏洞对系统安全造成的直接威胁可分为:普通用户访问权限提升、本地拒绝服务、远程拒绝服务、服务器信息泄露、远程非授权文件存取、读取受限文件、口令恢复、欺骗等。

2 基于 CVE 的电信网漏洞特征的描述

漏洞上述特点决定了漏洞完整描述的独特性。在对漏洞进行研究时,除了需要掌握漏洞本身的特征属性,还要了解与漏洞密切相关的其它对象的特点。

MITRE 组织的 CVE^[6] (Common Vulnerabilities

& Exposures -- 公共弱点/风险)是一个行业标准,它为公众提供一个所有已知系统弱点和安全漏洞的完整列举及标准化的名字,因为 CVE 是由包括安全软件厂商和学术研究机构在内的 20 多个安全相关组织的代表共同维护的,而且在发布上没有限制,这使得 CVE 列表在信息安全领域里扮演关键的角色。CVE 的标准命名可以使得网络安全领域内系统漏洞数据库和安全工具的数据共享变得更容易。

利用 CVE 这一标准,结合漏洞本身的特征属性与与漏洞密切相关的其它对象的特点,对电信网所存在的安全漏洞用图 1 进行描述。

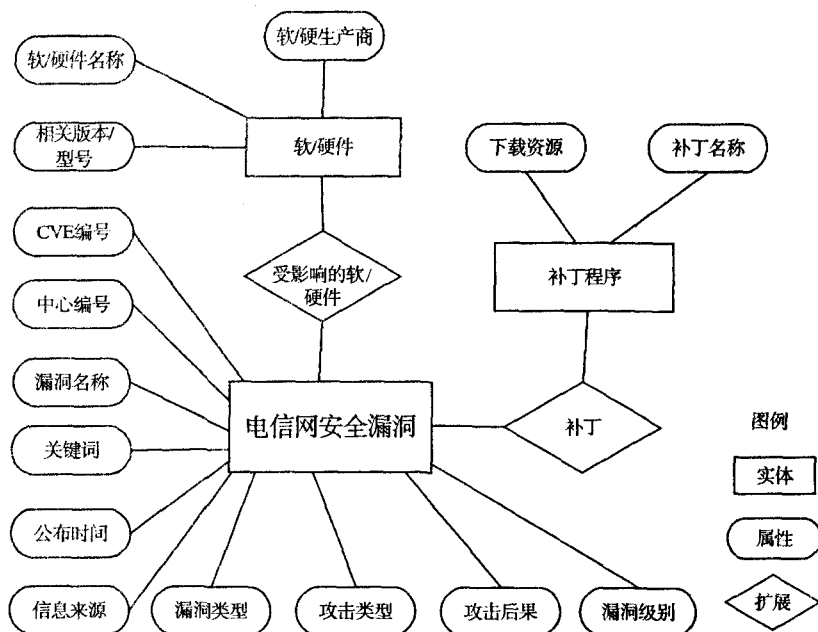


图 1 电信网漏洞的描述

其中电信网安全漏洞以及扩展的受影响的软/硬件和补丁的属性的含义如下:

漏洞名称(vul_name):描述系统安全漏洞的名称。

CVE 编号(vul_cve):给出了一个国际标准的编号。

中心编号(vul_id):描述此漏洞在数据库中的编号,使漏洞在此数据库中有唯一的标识。

关键字(vul_keyword):描述此漏洞最关键的信息。

公布时间(vul_publish_time):描述系统安全漏洞发布的时间。

信息来源(vul_from_position):描述漏洞信息的出处。

漏洞级别(vul_severity):描述系统安全漏洞严重性的级别,用户根据此项知道哪些漏洞对系统造成的危害大,需要立即打补丁。

漏洞类型(vul_type):描述此漏洞根据漏洞成因

的分类信息。

攻击类型 (vul_exploitable): 描述此漏洞根据漏洞被攻击者利用方式的分类信息。

攻击后果 (vul_losstype): 描述此漏洞根据漏洞对系统安全造成危害的分类信息。

软/硬件名称 (vul_affectname): 描述可能会受此漏洞危害的软/硬件的名称。

相关版本/型号 (vul_affectedtion): 描述可能会受此漏洞危害的软/硬件的版本。

软/硬件生产商 (vul_affproductfac): 描述可能会受此漏洞危害的软/硬件的生产商。

补丁名称 (vul_patchname): 描述此漏洞的补丁的名称。

下载资源 (vul_patchsource): 描述此漏洞的补丁的下载网址等资源。

3 基于 XML 的电信网安全漏洞相关数据的表示

XML 是“可扩展标识语言”(eXtensible Markup Language)的缩写,是 W3C 组织于 1998 年 2 月发布的标准,其制定的初衷是定义一种 Internet 上数据表示和数据交换的新标准。XML 是标准通用标记语言 SGML(Standard Generalized Markup Language)的一个子集,也是目前网络上流行的 HTML 语言的延伸。XML 语言实际上是一种定义语言,它能把数据内容与数据表示界面分开,其标记说明了数据的含义,而不是如何显示它,使用者可以自由定义标签,并且能够通过元素之间的嵌套包含来体现层次结构^[7]。这种特性能够让 XML 适合在网络上不同计算环境(无论是不同的操作系统环境,还是不同的设备显示方式)中采用一致的信息表示方式并且现在流行的开发工具(比如 JAVA、Visual C++ 等)都提供了对 XML 格式文件的解析方法。它具有数据格式的标准性、可扩展性、异构集成性、自描述性等优良特性。

为了实现安全漏洞数据在网络上的传输和不同关系数据库(例如 Oracle 和 Microsoft SQL Server)之间的数据共享,结合图 1 对电信网漏洞的描述定义了基于 XML 的电信网安全漏洞数据的交换格式,该格式与现有的 CVE 标准兼容,描述如下:

```
< vulnerability > //系统安全漏洞描述开始
```

```
< vul_name > ... < / vul_name > //描述系统安全漏洞的名称
```

```
< vul_cve > ... < / vul_cve > //给出了一个国际标准的编号
```

```
< vul_id > ... < / vul_id > //描述此漏洞在数
```

据库中的编号,使漏洞在此数据库中有唯一的标识

```
< vul_publishtime > ... < / vul_publishtime > //描述系统安全漏洞发布的时间
```

```
< vul_updatetime > ... < / vul_updatetime > //描述系统安全漏洞被更新、添入数据库中的时间。
```

```
< vul_summary > ... < / vul_summary > //描述与此漏洞相关的详细信息,使用户更进一步地了解此漏洞
```

```
< vul_severity > ... < / vul_severity > //描述系统安全漏洞严重性的级别,用户根据此项知道哪些漏洞对系统造成的危害大,需要立即打补丁
```

```
< vul_type > ... < / vul_type > //描述此漏洞根据漏洞成因的分类信息
```

```
< vul_exploitable > ... < / vul_exploitable > //描述此漏洞根据漏洞被攻击者利用方式的分类信息
```

```
< vul_losstype > ... < / vul_losstype > //描述此漏洞根据漏洞对系统安全造成危害的分类信息
```

```
< vul_affect > ... < / vul_affect > //描述此漏洞可能会对哪些系统造成危害
```

```
< vul_keyword > ... < / vul_keyword > //描述此漏洞最关键的信息
```

```
< vul_patch > ... < / vul_patch > //描述此漏洞的补救方法、补丁的相关信息和补丁下载网址
```

```
< / vulnerability > ///系统安全漏洞描述结束
```

用此方法定义的安全漏洞信息共享十分方便,从漏洞库中导出的信息生成 XML 格式的漏洞信息文件,可以在网络上传输,通过 IE 浏览器查看,也可以把 XML 文件的数据导入不同类型的关系数据库中。

4 电信网安全漏洞特征库管理系统的设计

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应对措施相关的系统安全配置策略。要构建电信网安全漏洞特征库先要设计并建立基于关系数据库管理系统的、易于扩充的漏洞信息存储数据库^[8];实现漏洞库管理信息系统;提供对漏洞库中所存储的漏洞数据的发布、更新、查询、删除、使用等基本交互功能,建立起一个完善的漏洞数据库系统。

整个漏洞库系统建立在 Windows 2000/XP 操作系统平台之上。系统采用三层的 Browser/Server 模式体系结构^[9],应用 J2EE 分布式系统模型进行开发,对漏洞信息存储数据库中的漏洞数据进行发布、更新、查询、删除等的管理信息系统用户图形界面接口模块采用 JSP 技术^[10],以基于 Web 的动态页面方式实现;对

数据库的访问和操作采用 EJB 组件;漏洞信息存储数据库选用关系数据库管理系统(Microsoft SQL Server)。系统的组成与逻辑结构如图 2 所示。

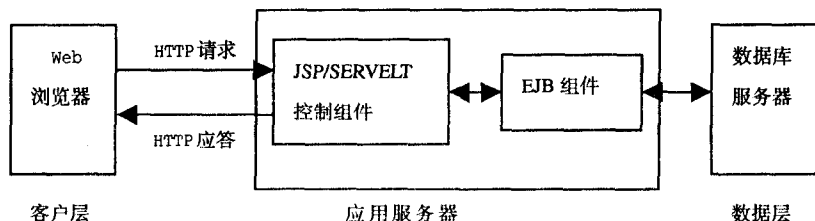


图 2 B/S 模式系统工作原理图

(1)客户层。客户层的浏览器通过 URL 访问应用层的 Web 服务器,由 Web 服务器产生供普通用户使用的服务界面和对漏洞信息存储数据库中的漏洞数据进行发布、更新、查询、删除等管理人员使用的界面,用来输入信息并反馈信息处理结果。

(2)应用服务器层。应用层负责响应浏览器的请求并连接数据库管理系统,在 Web 服务器内配置 JSP 组件以产生动态的页面和调用应用服务器内的 EJB 组件^[11];在应用服务器内配置 EJB 组件以访问数据库并对数据进行必要的处理。该层的功能具有很好的扩充性,根据需要可以方便地添加或删除组件。

(3)数据层。规划数据层,首先要选择数据库管理系统(Microsoft SQL Server);并且根据前面对电信网的安全漏洞数据的描述,高效规划和组织数据信息,设计关系数据库模型,构建数据库。这样就建立起了电信网安全漏洞特征数据库,这一漏洞数据库是在深入分析 CVE 漏洞的特征的基础上建立起来的,能够准确详尽地描述各个漏洞的特征,便于用户根据自己的需要进行检索。同时,由于许多新的漏洞不断出现,加之人们对已有漏洞认识的不断加深,对数据库的及时更新是十分重要的。因此,必须加强对数据库的维护,及时更新数据库数据,查漏补缺,对漏洞数据库不断地进行完善^[12]。

漏洞数据库的主要目的是便于用户查询检索,这样漏洞数据库才有意义。设计提供如下检索:漏洞名称(模糊查询)、CVE 编号(精确查询)、漏洞级别(分类查询)、漏洞类型(分类查询)、攻击效果(分类查询)、攻

击类型(分类查询)、受影响系统(模糊查询)、关键词(模糊查询)。另外,还有供管理员操作的添加、删除、更新等功能。

5 结束语

文中对电信网漏洞分类描述及表示模型进行了较为深入的探讨,并基于 J2EE 设计了一种分布式电信网安全漏洞数据库管理系统,可以利用 Web 浏览器在不同地方存储、查询和

修改各种电信网漏洞的数据,将来也可为电信网安全防御研究人员和普通用户提供数据支持和电信网安全防御方案的支持。

参考文献:

- [1] Bishop M. A Taxonomy of UNIX System and Network Vulnerabilities[R]. Department of Computer Science at the University of California at Davis, 1995: 12-35.
- [2] 单国栋,戴英侠,王航. 计算机漏洞分类研究[J]. 计算机工程, 2002, 28(10): 3-6.
- [3] 那成亮,周廷显,王晓峰. 无线局域网的安全漏洞分析[J]. 遥测遥控, 2003, 24(5): 35-37.
- [4] Common Vulnerabilities & Exposures[EB/OL]. 2004-08-25. <http://www.cve.mitre.org>.
- [5] Krsul I. Software vulnerability analysis[D]. USA: Department of Computer Sciences, Purdue University, 2005.
- [6] 方杰,袁修贵. 基于 J2EE 规范的电信综合网管架构设计[J]. 电脑与信息技术, 2005, 13(5): 35-38.
- [7] 张冰. 电信网络安全漏洞与补丁管理研究[J]. 电信网技术, 2006(7): 14-18.
- [8] 刘波,刘惠,胡华平,等. 计算机漏洞库系统的设计、实现与应用[J]. 计算机工程与科学, 2004, 26(7): 31-33.
- [9] 史斌星,史佳. JAVA 基础编程贯通教程[M]. 北京:清华大学出版社, 2003.
- [10] 乔佩利,王春英,张军. CVE 漏洞库体系的研究与实现[J]. 哈尔滨理工大学学报, 2004, 9(5): 70-72.
- [11] 刘滨,唐朝京,张森强. 基于网络的安全漏洞分类与扫描分析[J]. 信息与电子工程, 2004, 2(4): 318-320.
- [12] 翟钰,张玉清,武维善,等. 系统安全漏洞研究及数据库实现[J]. 计算机工程, 2004, 30(8): 68-70.

(上接第 135 页)

- [9] IEEE Standards Association. Draft IEEE standard for local and metropolitan area networks: media independent handover services[S]. IEEE 802.21. 2008.
- [10] Huang H, Wu J S. A Pre-Binding Update Fast Handover Control Using IEEE 802.21 MIH over 802.16e Networks[C]//2009 WRI International Conference on Communications and Mobile Computing. [s.l.]: [s.n.], 2009: 417-421.

- [11] 雷飞鹏,唐伦,陈前斌. 采用 IEEE802.21 MIH 服务优化 FMIPv6 切换的方案[J]. 通信技术, 2007(9): 52-53.
- [12] An Y Y, Lee K W, Kum D W, et al. Enhanced fast handover mechanism using MIH services in MIPv6[J]. Wired/wireless Internet communication, 2006, 3970: 120-131.
- [13] 唐宏,陈前斌,吴中福,等. 移动 IP 技术中 L2-Trigger 方法研究[J]. 重庆邮电学院学报: 自然科学版, 2003(4): 88-91.