补丁分发与管理系统的设计和实现*

郭海琼[1,2,3]，吴世忠[3]
([1]中国科学院长春光学精密机械与物理研究所，吉林 长春 130033；
[2]中国科学院研究生院，北京 100039；
[3]中国信息安全产品测评认证中心，北京 100089)

【摘 要】近年来不断出现的漏洞导致信息系统经常受到各种攻击和威胁，大部分攻击是因为没有及时安装补丁造成的。文章针对目前补丁管理存在的一些问题，提出了一套补丁分发与管理系统。该系统可控性和可管理性好，提供补丁适用性测试，支持多种组网方案的扩充。实验表明，该系统可以及时跟踪补丁更新，并实施有效部署，确保补丁被及时有效地安装。

【关键词】漏洞；补丁；补丁管理
【中图分类号】TP309 【文献标识码】A 【文章编号】1009-8054(2008) 05-0063-04

Design and Implementation of Patch Distribution and Management System*

GUO Hai-qiong[1,2,3], WU Shi-zhong[3]
([1]Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun Jilin 130033, China; [2]Graduate School of the Chinese Academy of Sciences, Beijing 100039, China;
[3]China Information Technology Security Certification Center, Beijing 100089, China)

【Abstract】Information system is often under various attacks and threats because of its vulnerabilities emerged in recent years and untimely installation of patches. This paper addresses some of the existing problems in patch management and proposes a patch distribution and management system. This system has good controllability, provides applicability test of patches, and supports various network expansions. The experiments indicate that this system can track patch-update timely, implement effective deployments, and ensure patches installed timely and effectively.

【Keywords】vulnerability; patch; patch management

0 引言

近年来，蠕虫、病毒等网络攻击事件频繁爆发，网络安全问题日益突出，大部分的网络攻击都是基于操作系统或应用程序的漏洞进行的。对于每个存在漏洞的系统，及时安装补丁都是非常必要的防范机制，可以有效防止系统被攻击或破坏。

在补丁发布后，由于用户安全意识薄弱和补丁管理的复杂性等原因，往往导致用户不能及时安装补丁，而大部分的网络攻击正是在这段时间内大规模爆发的。这时就要有专门的补丁分发管理工具，用来加强信息系统的安全防护。

文中在分析补丁管理研究现状的基础上，针对存在的问题，提出了一套补丁分发与管理系统。

收稿日期：2007-12-07
作者简介：郭海琼，1982年生，女，硕士研究生，研究方向：信息安全；吴世忠，1962年生，男，研究员，博士生导师，中国信息安全产品测评认证中心主任，研究方向：信息安全。
* 基金项目：通用漏洞评估研究，全国信息安全标准化技术委员会。

1 补丁管理的研究现状

随着黑客技术的不断积累和发展，从一个漏洞被发现到攻击代码实现，再到蠕虫产生，已经从几年前的几个月缩短到现在的几周甚至一天就可以完成，留给管理员进行漏洞修补的时间越来越少。如果补丁管理工作晚于攻击程序，那么信息系统就有可能被攻击，造成机密信息泄漏。表1给出了曾经发生过重要影响的蠕虫、攻击代码和补丁之间的时间关系。

表1 蠕虫、攻击代码和补丁之间的时间关系

蠕虫名称	Nimda	Code Red	SQL Slammer	Blaster	Sasser
补丁发布时间	2000.10.20	2001.06.18	2002.06.24	2003.07.16	2004.04.13
攻击代码发现时间	2000.10.20	2001.06.21	2002.06.26	2003.07.24	2004.04.13
蠕虫出现时间	2001.09.18	2001.07.13	2003.01.25	2003.08.13	2004.05.01
攻击代码与补丁时间差	0 天	3 天	20 天	8 天	0 天
蠕虫与补丁时间差	333 天	25 天	210 天	27 天	20 天

1.1 常见补丁管理产品

目前常见的补丁管理产品主要有以下几个：

(1)SMS

微软服务器管理系统(SMS)是微软提供的面向企业的网络管理软件，它基于Windows 2000动态目录管理，能够协助系统管理员收集企业内部计算机硬件配置和所安装的软件清单，判断哪些机器需要更新，哪些机器可以运行新的软件，并提供了远程故障处理工具。

(2)PatchLink Update

Patchlink公司的PatchLink Update是一种基于代理程序的跨平台补丁解决方案，支持Windows、Unix与Linux。一旦代理程序软件配置在工作站或服务器，它会自动定期检测代理程序，代理程序会针对有问题的计算机提供完整的漏洞分析。基于此分析，管理者可以部署适当的修补程序给一台计算机或其所在群组的每台计算机。

(3) Altiris Patch Management Solution

Altiris公司的Patch Management Solution也是一种基于代理程序的补丁管理工具。它会定期扫描并报告系统中缺少的安全更新，并提供到厂商网站上进行补丁下载的链接，然后按照管理员制定的策略进行补丁分发，最后还会生成关于补丁更新和分发状态的详细报告。

(4)UpdateExpert

St.Bernard公司的UpdateExpert同时支持无代理和使用代理两种方式，提供多平台支持，支持Windows、Linux与Solaris。无代理方式通过一个中央服务器对每个客户端进行扫描并对系统状态进行评估，以决定是否需要应用修补程序。大多数情况下采用使用代理的方式，可以提供更好的带宽控制功能。

1.2 主要问题

(1)可控性差

补丁管理的各个环节都是系统自动完成的，很难实现人工控制。在补丁下载阶段，补丁是直接从厂商网站下载的，管理员不能对补丁下载方式等进行配置，也不能保证补丁下载的可靠性；在补丁分发阶段，只能由管理员对补丁进行统一分发，终端用户不可以主动查看并下载补丁；在补丁安装阶段，补丁是自动进行安装的，用户不能通过控制运行参数来制定补丁安装策略。

(2)可管理性差

补丁是自动下载并安装的，可管理性差。用户不能确定补丁的存放位置，也就不能对补丁进行统一管理，例如不能将补丁导出，进行补丁有效性和安全性测试，以及更深入的研究。

针对上述问题，论文提出了一套补丁分发与管理系统。

2 系统设计和实现

面对数以千计的主机和各种应用，本系统可以及时跟踪补丁更新，并实现有效部署，确保补丁被及时正确地安装。文中从系统设计、系统实现和实验三方面对系统进行介绍。

2.1 系统设计

(1)补丁信息获取

补丁下载服务器与因特网连接，从指定站点获取补丁索引文件，通过对补丁索引文件的解析，按照补丁索引、管理配置要求从补丁厂商站点下载补丁。补丁下载支持各种自定义下载方式(下载线程、下载时间)，在补丁下载时，系统加入MD5校验，确保补丁下载的可靠性。

(2)补丁管理

下载的补丁保存在补丁下载服务器的指定目录下。当补丁下载服务器和补丁分发服务器没有安装在同一台机器上时，通过移动介质将补丁导出，然后通过移动介质将补丁导入到补丁分发服务器。补丁存放目录下的patchindex文件包含所有补丁信息，每次导出补丁都会做本次补丁导出记录，下次导出时以上次导出为基准，将新旧两个patchindex文件进行遍历比对，确定哪些补丁已经存在，哪些补丁不存在，从而保证在上次导出的基础

上实现增量导出，减少工作量。

(3)补丁分发与安装

补丁安装可以采取“推”的方式，由管理员基于IP范围、操作系统种类、补丁检测周期、补丁类别等制定策略，对补丁库中所有补丁制定自动分发策略，自动分发到不同操作系统；也可由管理员选择特定的补丁进行单独分发至全部网络或者某一区域网络。策略发送到客户端后，由客户端注册程序统一执行补丁应用策略。补丁安装也可以采取‘拉’的方式，由用户到指定网站下载并安装补丁。本系统建立测试网络组，在补丁分发前对下载的补丁进行测试，测试完成后将其存入补丁库，以提高补丁的安全性和可靠性。本系统在安装补丁时，通过对运行参数的控制，可以使得补丁更新始终在后台进行，不会影响用户的正常工作。

(4)补丁安装效果评估

当执行预定的补丁策略发生错误时，系统会将错误的相关信息存储到补丁信息库，并通过区域管理器向管理平台发布补丁分发、安装错误通告或警报，还可以通过管理平台查询补丁的分发和安装情况以及漏打补丁。

2.2 系统实现

(1)总体结构

本系统主要由补丁下载服务器、补丁分发服务器和客户端注册程序三大部分组成，其中补丁分发服务器包括环境初始化程序、区域管理器、区域扫描器、winpcap程序以及网页管理平台五个模块，各部分的功能如下：

① 补丁下载服务器

补丁下载服务器安装在与因特网连接的机器上，用于实时下载补丁厂商发布的补丁。补丁下载服务器按照管理配置要求和用户自定义策略下载补丁，并保存到指定目录，用户可以对补丁进行统一管理。

② 补丁分发服务器

——环境初始化程序：SQL Server管理信息库，建立补丁管理系统的初始化数据库。

——区域管理器：系统策略控制及数据接收处理中心，具有控制完成系统相关动作行为的处理功能；同时与本级数据库系统连接，统一接收客户端注册程序提供的用户信息，将用户信息(用户填写的物理信息和系统自动采集的硬件信息)存入数据库。

——区域扫描器：内置于区域管理器中，用于扫描网络中主机状态。扫描器只依据网页管理平台中配置的工作范围进行扫描，扫描器将设备最新状态信息报送至区域管理器，由区域管理器处理后，同数据库中原有信息进行遍历搜索对比，根据管理规则在管理平台上报警。

——winpcap程序：嗅探驱动软件，监听共享网络上传送的数据。可以捕获共享网络上各主机相互之间交换的数据，收集网络通讯过程中的统计信息。

——网页管理平台：本系统的管理配置中心，基于IE浏览器模式提供对系统的控制管理。管理内容包括运行参数设定、信息查询、策略制定、补丁检测等。

③ 客户端注册程序

系统认证和扫描代理，用于接收补丁，收集终端资产的运行状态、相关属性以及补丁安装状态等信息。用户访问指定网站自动获得，用户填写本机信息以及其他必要信息后上报区域管理器。客户端注册程序会自动探测系统硬件信息，连同用户填写的信息一同上报区域管理器。

(2)数据库结构

本系统的数据库包括五个表：客户端补丁下载信息表(Clientpatchdown)、系统信息表(Systeminfo)、补丁分发信息表(Patchdistribute)、系统出错信息表(Errorinfo)、补丁信息表(Patchinfo)，各个表之间的相互关系如图1所示。

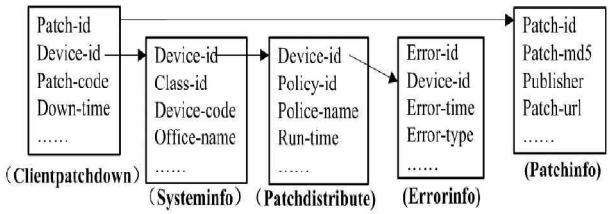

图1 数据库表之间的关联关系

以补丁分发信息表为例，其数据结构如下：

```
typedef struct  issue__info {
short no；// 补丁编号
short user__id；//分发补丁的管理员标识
short policy__id；//补丁的分发策略标识
time__t time ；//分发信息长度
char issue__info[4]；//变长，补丁发布相关信息
} issue__info;
```

(3)系统部署

① 基本架构

对于一般网络(例如1个C类地址或若干个C类地址的局域网)，可使用一套本系统软件。

② 扩展架构

对于大规模的多个局域网或者跨地域广域网(包括基

于国家、省、市、县等多级管理模式的网络结构)，可使用本系统提供的多级级联集中管理功能，即在一个或多个网段各使用一套补丁管理系统，将本级所有安全信息转发至上级管理系统，上一级管理人员对整个网络的安全状况能够完全掌握，上级管理系统可将安全策略分发至下级系统执行。

使用该功能时要求在下级区域管理器的相应选项中填写上级区域管理器的IP地址，便可方便地获得补丁，并实时和上级区域的补丁数量保持一致，只需总部下载补丁，其下级区域无须再额外地下载补丁，其补丁均可从总部的服务器上获得，如图2所示。

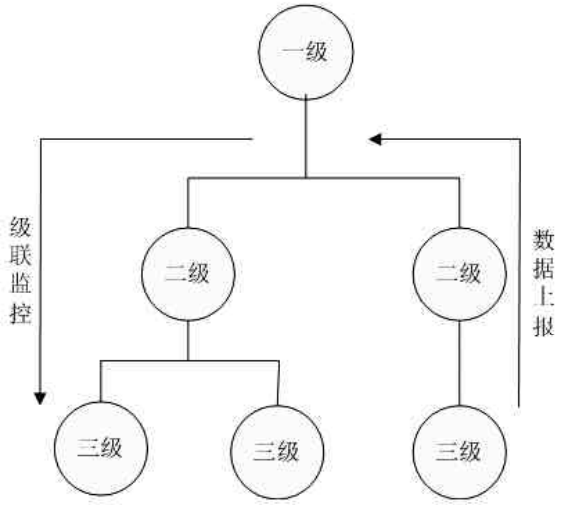

图2 多级级联集中管理构架

3 实验

以下从几个方面将本系统和其他补丁管理产品做了功能对比，结果如表2所示。

(1)补丁适用性测试

在补丁分发前，系统对下载的补丁进行测试，以提高补丁的安全性和可靠性。

(2)补丁导入 /出管理

便于对补丁进行操作和管理。

(3 补丁自动代理转发

提高补丁分发效率，减少网络带宽的占用率，节省网络资源。当网络内有数量较多的计算机下载补丁或者文件时，计算机可以搜索临近IP范围内状态最好的计算机，从这台状态最好的计算机下载相应的补丁或者文件。这样就可以大大减少服务器负载，减少网络带宽的占用率，保证工作的正常进行。

表2 功能对比

产品	SMS	Patchlink	Alitris	UpdateExpert	本系统
补丁分发	√	√	√	√	√
补丁适用性测试				√	√
补丁导入/导出管理					√
补丁自动代理转发					√
补丁分发流量均衡	√	√	√	√	√
终端补丁查询管理	√	√	√	√	√
补丁资源分类管理	√	√	√	√	√
补丁分发策略管理	√	√	√	√	√
提供多平台支持		√	√	√	

4 结语

随着网络的不断发展，软件和系统漏洞越来越多，不断出现的漏洞导致信息系统经常会受到各种各样的攻击，及时安装补丁是预防信息系统遭受安全威胁的有效措施之一。文中提出的这套系统可以对大型网络中补丁的分发、安装等进行有效的管理，保证资产系统中存在的漏洞得到及时、正确的修补，并跟踪资产状态，从而保证整个信息系统的安全。

参考文献

[1] 张翀斌，李守鹏，张晓敏. 专用网络补丁管理技术研究[J]. 信息安全与信息保密，2005(9)：86-88.

[2] 徐鹏，张玉清. 补丁自动管理系统的设计与实现[J]. 计算机工程，2007，33(2)：139-141.

[3] 王林，张小梅. 软件补丁管理在网络信息安全中的作用及趋势[J]. 武汉理工大学学报，2004，27(3)：87-89.

[4] 杨海军，力立. 寻求防患于未然之计-构建补丁管理的框架[J]. 数据通信，2005(2)：35-37.

[5] David Aucsmith.Security：The Changing Threat Environment[DB/OL].2004. http：//www.microsoft.com/whdc/driver/security/defaut.mspx.

[6] Benjurry. 居安思危-论补丁管理[DB/OL]. 2004. http：//xfocus.net/articles/200405/PatchManagement1.pdf.