第 33 卷 第 2 期 计 算 机 工 程 2007 年 1 月
Vol.33 No.2 Computer Engineering January 2007
·安全技术· 文章编号：1000—3428(2007)02—0139—03 文献标识码：A 中图分类号：TP311

# 补丁自动管理系统的设计与实现

徐 鹏，张玉清
(中国科学院研究生院国家计算机网络入侵防范中心，北京 100049)

**摘 要：**随着局域网的规模越来越大，安全现状日益严峻，补丁分发管理等安全防范措施引起了人们的普通关注。该文针对目前补丁管理软件发展现状，进行了补丁自动管理系统的设计开发与实现。该文设计的系统支持中文补丁升级，实现补丁自动下载、检测及安装，支持多种组网方案的扩充，适用于大型网络的补丁分发。

**关键词：**补丁；补丁信息数据库；补丁管理

# Design and Implementation of Patch Auto-management System

XU Peng, ZHANG Yuqing
(National Computer Network Intrusion Protection Center, Graduate School, Chinese Academy of Sciences, Beijing 100049)

**【Abstract】**With the development of the scale of the LAN and the seriously worse situation of the network security, patch auto-management system attracts more and more attention. According to the related works, the paper proposes and realizes a new design of a patch system which can automatically download, detect and install patches and also supports multiple network extension.

**【Key words】**Patch; Patch information database; Patch management

近年来，网络安全问题骤然突出。大范围互联网攻击事件频繁，如 2002 年全球的根域名服务器遭到大规模拒绝服务攻击，2003 年爆发了 SQL Slammer 等蠕虫事件，2004 年爆发了 Blaster 蠕虫事件。另外，随着黑客技术的逐步成熟，各种攻击工具泛滥互联网，使得许多即使没有掌握高深黑客技术的初学者也能发动强力的网络攻击，而且随着网络应用的逐步深入和大范围推广，这些网络攻击事件造成的危害也愈来愈严重，如 SQL Slammer 发作时致使韩国网络基本处于瘫痪状态，我国境内感染主机 22 600 余台，而 2001 年尼姆达蠕虫造成的损失估计大大超过 26 亿美元。

安全漏洞是这些网络安全问题的主要溯源。几乎所有的网络攻击都是基于操作系统或应用程序的漏洞进行的，因此必须要消除漏洞。消除漏洞的根本方法是及时安装相应的漏洞补丁。但是在相应的漏洞补丁发布后，离用户用补丁程序更新系统往往还是有一段时间。一方面是因为有些用户安全意识薄弱，往往要等到大规模的网络攻击开始时，才会想起安装补丁。更重要的原因是，补丁管理工作本身也比较繁琐枯燥，以微软的Windows系统而言，每个星期都有漏洞警报和补丁程序发布，数日一小补，数月一大补，网络管理员不仅要追踪和应用这些最新的升级信息，还要从中鉴别哪些补丁是必须和适用的[1]。

因此补丁自动管理系统的应用不仅能将网络管理人员从日益繁重的手工操作中解脱出来，节约昂贵的人力成本，同时也能针对不同的严重的安全事故，迅速地在大规模网络上部署解决方案，提高网络安全应急响应的速度和效果。

## 1 相关研究现状

在补丁管理领域，国外已经开发出了许多相关软件。如微软公司的免费软件SUS(software update service)和付费软件SMS，它们针对Windows系统的补丁升级，采取C/S模式设计，服务端必须为Windows 2000 sever＋SP2 或Windows 2003 sever版本，其中SMS功能更强，主要为企业提供全面的补丁管理[2]。Yum(Yellow dog update modified)[3]主要向支持RPM方式管理的Linux系统提供升级服务。另外还有Big Fix公司的Patch Manager[4]，它会主动全面地侦测包含各种平台(如Windows或Linux)在网络上的安全脆弱的电脑，并给出恢复措施，是一款综合性的补丁管理软件。

尽管国外的补丁管理软件都已比较成熟，但这些软件一般不支持中文补丁的升级，也没有相应的中文界面，难以满足我国计算机应用的广泛需求；另外，敏感部门在使用上也存在安全隐患。国内在相关领域的研究刚刚起步，目前还没有开发出真正适应于大型网络的补丁管理软件。因此，开发出具有自主知识产权的大规模网络补丁自动管理系统，不仅是国家信息网络安全的需要，也是国内补丁研究发展的需要。

本文结合以上问题，提出一种设计方案，利用微软公司定期更新的Mssecure.xml文档[5]，实现对Windows系列系统的所有中文补丁的自动下载、检测及安装，并支持多种组网方案的扩充，适应大规模网络的补丁分发。

## 2 系统设计

本系统的软件设计思想是采用服务端/客户端(Server/Client)两层结构和模块化的软件开发思路，使系统更加具有可扩展性、可重用性以及方便使用性等。

### 2.1 整体结构设计

通过需求分析，构建如图 1 所示的整体结构设计。

系统由父服务器、子服务器及客户端等组成。

(1)父服务器：它是本系统的核心。其负责从官方网络上自动下载补丁，并将补丁提供给所有的下级子服务器或客户

**基金项目：**国家自然科学基金资助项目(60373040，60573048)；中国科学院研究生院科研启动经费项目

**作者简介：**徐 鹏(1982－)，男，硕士生，主研方向：网络与系统安全；张玉清，副研究员

**收稿日期：**2006-03-31 **E-mail：**xupeng19821116@163.com

端。在整个补丁管理系统中只有父服务器从外网获取补丁，其余组件的补丁均来源于父服务器。因此，父服务器的补丁获取能力决定了整个系统的补丁更新能力。

(2)子服务器：与上级父服务器中的补丁信息保持同步，可以下连客户端或下一级的子服务器。子服务器的设立可以减轻父服务器的补丁分发负担，并方便系统网络结构的任意扩展。

(3)客户端：即具体的用户端，从上级服务器下载所需的补丁及补丁信息，并实现对本地补丁的自动管理。在实际使用中，将客户端连接到通信速率较快的服务端，会提高整个系统的补丁分发效率。

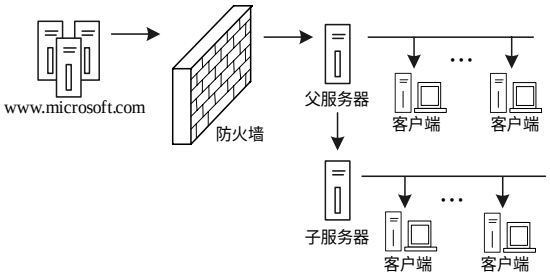


**图 1 补丁自动管理系统整体结构设计**

### 2.2 系统各功能模块设计

根据以上的整体结构设计图，结合对补丁管理系统的分析，采取根据功能来设计软件模块的策略，得到如下的功能模块设计思路。

2.2.1 服务端设计

子服务器和父服务器均视为服务端，主要功能是为客户端提供补丁下载，系统通过如下模块进行相应的功能实现。

(1)获取补丁信息模块：为实现补丁自动管理，必须要满足补丁管理的持续性，即要求系统能够自动跟踪网络上的补丁信息，并始终与官方发布的更新保持一致。该模块可自动从网络上下载最新的补丁信息文档，进行分析，建立相应补丁信息数据库，并将分析得到的信息添加到数据库中。生成的补丁信息数据库可供其它模块调用。

(2)自动下载补丁模块：服务端的主要功能是从网络上获取补丁，父服务器从官方网站上获取，而子服务器从上级父服务器获取。父服务器调用前一模块中生成的补丁信息数据库，获取补丁的下载地址，从而在官方网站上自动下载补丁；子服务器通过指定具体的父服务器地址把父服务器从网络上获取的补丁下载到本地。

(3)通信模块：负责服务端与客户端之间的信息交互，将补丁程序从上级服务器分发到下级客户端或下级子服务器。

2.2.2 客户端设计

(1)更新补丁信息数据库模块：与服务端中的补丁信息数据库相对应，客户端补丁信息数据库记录客户端的补丁信息，如本地补丁部署情况、下载情况等。客户端补丁信息数据库根据其所连接的上级服务端的补丁数据库中的内容生成。该模块自动扫描服务端补丁数据库，如果有新的补丁信息，便将该补丁的基本信息更新到客户端补丁信息数据库。该数据库可供客户端其它模块调用。

(2)补丁检测模块：该模块检测客户端中的补丁下载情况和安装情况，将检测结果写入到客户端补丁信息数据库。根据更新后的客户端补丁信息数据库，可以避免重复下载和安装补丁。

(3)自动下载补丁模块：补丁程序的分发主要通过“拉”的方式实现，即由客户端主动向服务端请求下载。该模块会扫描客户端补丁信息数据库，得到本地未下载补丁列表，并根据列表从指定服务端自动下载补丁。

(4)补丁自动安装模块：补丁自动管理最重要的一步是自动安装。该模块首先扫描补丁信息数据库，得到未安装补丁列表，并根据列表，将已下载的补丁进行自动批量安装，正确更新到客户端中。

### 2.3 软件环境

该补丁自动管理系统主要针对 Windows 系统下的补丁进行管理，因此在 Windows 环境下进行开发。采用 VC6.0 编程开发工具，数据库使用简单方便的 Access，网络编程采用 WinInet。

## 3 系统实现

根据以上的系统设计，考虑到 C/S 结构两层中各自的特点和各功能模块的划分，采取以下的技术路线予以实现。

### 3.1 服务端的实现

服务端主要负责补丁信息的获取，补丁的自动下载及补丁的发布，具体实现步骤如下：

(1)获取中文补丁的补丁信息

补丁信息全部从 Mssecure.xml 文档中获得。Mssecure.xml 文档由微软公司定期发布，它存放了所有补丁的检索信息，其内容包括：所有微软发布过的安全公告 ID，发布时间及漏洞的简单描述；每个安全公告发布的所有补丁的名称，所针对的软件产品及版本；还有补丁安装后的注册键值，补丁在微软官方网站上的下载位置等。

Mssecure.xml 文档保持与微软安全公告同步更新，采用它作为补丁自动管理系统的补丁信息获取源，能保证补丁管理系统中补丁的及时性、可靠性、全面性及持续性。

同种补丁会有许多语言版本，但是目前微软发布的 Mssecure.xml 文档没有针对中文补丁的版本，本系统采用针对英文补丁的版本，文档描述的都是英文补丁的信息，因此必须对补丁信息文档进行相应的转换处理才能获得相应的中文补丁信息。

中文补丁与相应的英文补丁的许多属性信息相同，如注册键值、公告号、所针对的软件产品及版本等，这些信息不用转换。而通过对比发现，将英文补丁名进行部分字符串替换就得到了相应的中文补丁地址。利用这种方法，部分补丁的下载地址也转换得到了。

这样，服务端定时自动从官方发布网址上下载最新的补丁信息文档，并根据以上的转换规则，建立相应的中文补丁信息数据库，就实现了补丁信息的及时更新。

(2)补丁的自动下载

实现补丁自动下载功能的关键在于获得所有补丁的下载地址。Mssecure.xml 文档中含有所有补丁在微软官方网站上的下载地址，但是不能直接利用来下载补丁。因为该系统采用的 Mssecure.xml 文档描述的是英文补丁，从文档中得到的补丁地址都是英文补丁的下载地址；其次，文档中给出的大部分下载地址并不是直接下载地址，只是补丁的下载页面或者搜索页面地址。因此必须作相应的转换处理。

通过对微软官方网站上的补丁下载地址进行分析，有如下研究结果：对于直接下载地址，只用作一些简单的字符替换，便可获得中文补丁的下载地址。如 http://download.microsoft.com/download/win2000platform/patch/q285083/nt5/en-us/q285083_w2k_sp2_x86_en.exe 和 http://download.microsoft.com

/download/win2000platform/patch/q285083/nt5/zh-cn/q285083_w2k_sp2_x86_cn.exe，前者是文档给出的英文补丁下载地址，后面就是替换得到的中文补丁下载地址；对于非直接下载地址，结合补丁公告 ID 和微软赋予每种补丁的唯一标识号 FamilyID，通过读取网页页面源文件代码，也成功得到了相应中文补丁的直接下载地址。

得到所有中文补丁的下载地址后，调用相应的下载函数，便实现了自动下载所有的补丁程序。

(3)通信模块

由于补丁的发布主要通过“拉”的方式完成，即由客户端主动请求从服务端下载，因此服务端只需提供下载服务。本系统建立 IIS 服务器提供 Web 接口。服务端将下载的补丁存放至指定目录，由 IIS 服务器将该目录设为 Web 共享，从而使得客户端能够方便访问并下载补丁。

### 3.2 客户端的实现

客户端的具体实现过程中，着重解决了以下问题。

(1)更新客户端补丁信息数据库

对客户端系统信息进行检测，得出操作系统类型及 Sever Pack 版本号。然后客户端从服务端下载服务端补丁信息数据库。由于补丁信息中包含有补丁所针对的系统类型及 Sever Pack 版本号，利用编程从所有的补丁信息中进行筛选，选择出针对本地客户端应用环境的补丁，这样就得到了客户端补丁信息数据库所需的信息。

(2)补丁检测

每个补丁安装到系统后一般都会在操作系统注册表中建立该补丁的表项，即注册键值。通过查询补丁信息数据库得到补丁注册键值，再利用编程查询操作系统注册表，如果注册表中没有该补丁的注册键值，那么就可判定这个补丁没有安装到本地系统中。判定补丁下载状况只用扫描补丁存放目录下是否含有相应的补丁程序也可以方便实现。

(3)客户端下载补丁

由于服务端提供了 Web 接口供客户端下载，因此只要配置好客户端的服务端 Web 接口地址，就能正常连接到服务端。最后客户端扫描补丁信息数据库得到本地补丁下载情况，同时也得到补丁安装列表，通过调用网络函数，客户端就能直接从服务端下载补丁了。

(4)客户端补丁安装

通过补丁检测后，得到未安装补丁列表。同时根据本地补丁的下载情况，得到待安装补丁列表。

补丁安装后，必须经过重启后才能真正更新到系统中。如果直接批量安装补丁，即安装多个补丁的过程中不重启计算机，就会出现多个补丁安装冲突，导致某些补丁的更新失效。利用批处理文件，通过编程向批处理文件写入多个补丁的安装指令，然后调用并执行批处理文件可以实现批量安装。对于补丁批量安装出现的冲突问题，可以利用微软发布的 Qchain 工具来解决。即在所有补丁安装结束后，调用并运行该工具软件。它会自动对所有补丁更新后的文件版本进行排序，这样便不会出现补丁的更新失效。

### 3.3 系统运行示例

通过系统设计，利用 VC 等编程工具在 Windows 下进行开发，得到一个补丁自动管理系统运行实例，同时搭建补丁系统运行平台，并进行测试。

服务端的运行界面如图 2 所示。图 2 列表框列出了微软发布的所有补丁。显示的补丁详细信息有补丁名和相应的下载地址及下载状态。这样可知，服务端成功地从描述英文补丁信息的文档中获得了中文补丁的信息，并将中文补丁从官方网站上下载到了本地。

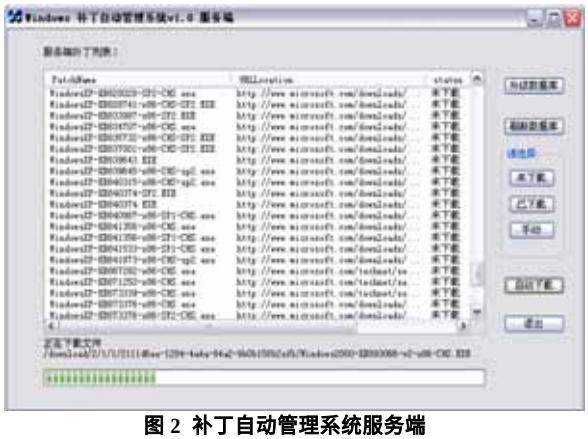

**图 2 补丁自动管理系统服务端**

客户端的运行界面如图 3 所示。客户端检测出的本地机器运行环境是“Microsoft Windows XP Service Pack 2(Build 2600)”。图 3 列表框列出了本地所需的补丁信息，并显示出补丁的下载或安装状态。

**图 3 补丁自动管理系统客户端**

在联机调试的过程中，服务端与客户端的各功能模块均得到相应实现：服务端进行补丁信息获取，补丁库更新及补丁下载；客户端从服务端下载补丁库，对补丁进行检测，并从服务端下载补丁，最后批量安装补丁。整个系统运行稳定，并达到了补丁自动管理的要求。

## 4 系统特点分析

该补丁自动管理系统的特点是利用官方公布的 Mssecure.xml文档[5]，直接通过程序分析XML文档生成补丁信息数据库，免去了人工搜集补丁信息的繁琐。另外补丁信息的升级与官方同步，不需管理员人工维护，保证了补丁管理系统的持续性。补丁自动管理系统自动对补丁信息中的下载字段进行分析，得到补丁的直接下载地址，并且自动批量下载，巧妙地解决了数量庞大的补丁来源问题。通过对同一种补丁的不同语言版本的比较，本文成功地利用描述英文补丁信息的Mssecure.xml文档实现了一套支持中文补丁更新的补丁自动管理系统。

在补丁自动管理系统的开发过程中，要时时考虑到整个软件系统的效率。本系统在补丁自动下载和自动安装时，采用多线程技术保证了高效运行。另外，本系统在安装补丁时，通过对运行参数的控制，使得补丁更新始终在后台运行，不会影响用户的正常使用。 (下转第 147 页)