维普资讯 http://www.cqvip.com

基于日志挖掘的计算机取证系统的分析与设计

国光明[1] 洪晓光[2]

(济南人民警察职业培训学院 济南 250031)[1] (山东大学计算机科学与技术学院 济南 250061)[2]

摘 要 本文主要讨论基于日志的计算机取证分析系统的分析与设计,给出了基于计算机日志的取证分析系统的总体结构和计算机日志分析取证系统日志处理、挖掘与分析子系统结构,并着重讨论了日志数据的预处理、挖掘与分析模块的主要功能与设计思想,并对挖掘模式进行了评估和分析。

关键词 日志,计算机取证,日志挖掘

The Analysis and Design for Computer Forensic System Based on Logs Mining

GUO Guang-Ming[1] HONG Xiao-Guang[2]

(School of Police Occupation Training of Jinan, Jinan 250031)[1]

(School of Computer Science and Technology, Shandong University, Jinan 250061)[2]

Abstract This paper mainly discusses the analysis and design of log-based computer forensics system. The general struc ture of this system is presented and emphasis is laid on a discussion about the main function and design philosophy of modules on log data preprocessing, data mining and analysis.

Keywords Log, Computer forensic, Log mining

1 原型系统的总体结构

本系统采用了数据挖掘技术,对计算机犯罪现场采集的系统日志进行挖掘分析,用以指导计算机犯罪的取证和侦破工作。计算机取证分析系统主要由取证前端(被入侵者攻击的系统,称为目标系统)、后端(取证设备,可以是笔记本电脑或移动 PC)的管理控制台和日志取证数据库以及取证服务器组成。取证前端包括收集目标系统信息、收集日志文件记录和备份、上传日志文件等三个部分。后端的管理控制台主要由日志取证数据库管理、日志取证前端管理、日志记录数据库、日志文件保护与备份、日志挖掘与分析报告等五个部分组成。原型系统总体结构如图 1 所示。

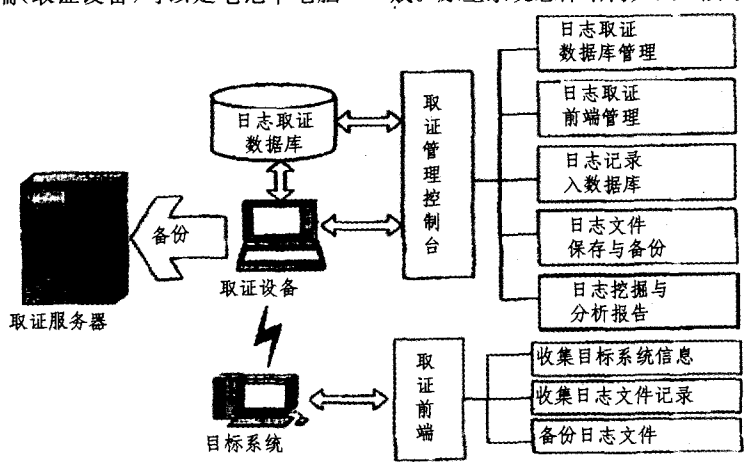

图 1 基于日志的计算机取证系统总体结构图

本文重点讨论的计算机日志分析取证系统日志处理、挖掘与分析子系统结构如图 2 所示。

其中涉及的功能模块包括:

· 日志挖掘分析控制台:一个人机对话的窗口,提供可视化的界面。

· 数据库管理模块:提供数据库的维护功能,可以进行数据表的创建添加、表属性的修改、删除等工作。

· 数据预处理模块:可以根据取证分析的需要,对不同来源的日志记录数据预处理,包括数据的清洗、归约、变换、集成等功能。

· 数据挖掘模块:根据不同的需要,提供各种挖掘算法,对日志数据源进行关联挖掘分析、孤立点检测等,以得到有用的信息。

· 评估分析模块:由于计算机犯罪和计算机取证技术的特殊要求,根据司法人员和专家意见来评估反馈每个步骤可能得到的结果,包括数据预处理过程的完善、挖掘算法实施的

国光明 工程硕士,讲师;洪晓光 教授。

维普资讯 http://www.cqvip.com

改进、提取模式的合理性和可行性分析等。

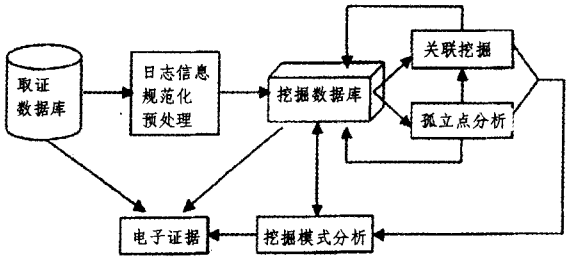

图 2　基于日志的取证系统挖掘分析子系统结构图

本文讨论的重点即在日志的处理、挖掘和分析部分，着重在于探讨如何对日志进行处理、挖掘分析。

2　数据预处理模块的设计

数据源准备部分是整个取证分析的基础，它为后续的分析模块提供真实可靠的、适宜的挖掘数据源。在计算机取证中，因为数据源的准备和预处理过程需要涉及对数据的转换和选择步骤，所以这一部分的准备工作需要在法律法规许可的范围内进行，并且每一步骤，必须要由可靠的书面记录来说明。

2.1　数据预处理方法

数据挖掘中的预处理阶段主要是接收并理解用户的知识发现需求，确定发现任务，抽取并处理与任务有关的数据源，根据背景知识中的约束性规则对数据进行合法性检查，通过清洗、归约、集成等操作，生成供数据挖掘核心算法使用的目标数据，即知识基。知识基是原始数据库经数据汇集处理后得到的二维表，纵向为属性，横向为记录。它汇集了原始数据库中与发现任务相关的所有数据的总体特征，是知识发现状态空间的基底，也可以认为是最初是的知识模板。

一般系统的审计日志信息的量非常庞大，并且存在杂乱性、重复性和不完整性的问题。由于取证收集的原始数据来源不一，有网络连接日志、系统审计日志、应用系统日志、防火墙日志、数据库日志等等，这些应用的审计机制的配置并不完全相同，所产生的审计日志信息存在一定的差异，因此有些数据显得杂乱无章，这是日志杂乱性问题所在。重复性是指对于同一个客观事物在系统中存在其两个或两个以上完全相同的物理描述。在 Unix 操作系统中的审计日志信息存在许多重复和冗余现象，例如在 Unix 系统中，记录用户登录的日志有 Lastlog，UTMP，WTMP 等，这三个日志记录的内容虽然有所区别，Lastlog 记录每个用户最近一次登录时间和每个用户的最初目的地，UTMP 记录以前登录到系统的所有用户，而 WTMP 文件记录了用户登录和退出事件，但是我们还是可以看出，这三个日志文件中存在很多相同的项目，这样就带来了数据的重复和冗余问题。不完整性是由于实际系统存在的缺陷以及一些人为因素造成的数据记录的缺失，或者数据记录中出现数据属性值的丢失或不确定的情况。在黑客入侵或者计算机犯罪行为人完成操作后，为了隐藏其入侵的痕迹，他经常会对一些审计日志文件进行修改、删除操作，这样就会造成必要数据的丢失或者数据库的某个数据的丢失。

为此，我们需要对这些原始的数据源进行数据预处理，通过数据清理、数据归约、数据变换、数据集成等方法，对系统的审计日志信息进行预处理，产生可供挖掘和进一步处理的数据源。

• 数据清理的任务是要去除源数据即审计日志信息数据中的噪声数据和无关数据，处理遗漏数据和清洗脏数据，去除空白数据和在知识背景上的白噪声，考虑审计日志信息的时间变化和它们的数据变化，主要是对重复数据和缺值数据进行处理，去除重复数据记录，填补缺省数据。

• 系统审计日志中有些数据属性对提取安全规则没有影响，这些属性的加入会大大影响数据挖掘效率，甚至可能导致数据挖掘结果的偏差，产生误导作用，因此，有效地对数据进行简化是很有必要的。数据归约简化是在对发现任务和数据本身内容理解的前提下，最大限度地精简数据集。这个步骤主要通过两种途径：属性的选择和数据的抽样，分别对系统审计日志信息中的属性和记录进行简化。属性选择包括根据需要提取的安全主题对数据的属性进行剪枝、并值等相关操作。剪枝就是去除对提取安全规则没有贡献，或者贡献率很低的属性值。并值就是把相近的属性进行综合归并处理。

• 在审计日志信息中，有些属性域需要做一定的变换处理，使得挖掘的结果能够合乎我们的习惯逻辑和表达，如在审计日志记录中，时间维的属性值总是以当时的系统时间为准，但是在某些情况下，我们不需要知道准确的时间关系，而只需要知道大致的时间范围段，比如上午、下午、晚上这样的时间段划分，所以我们要根据需求，做一定的数据变换工作。数据变换也属于概念分层的范围，即通过收集并用较高层的概念替换较低层的概念来定义数值属性的一个离散化。概念分层可以用来归约数据，通过这种概化，尽管细节丢失了，但概化后的数据更有意义，更容易理解，并且所需的空间比原数据少。

• 数据集成主要是将多个文件中的异构数据源进行合并处理，解决语义的模糊性。该部分主要涉及数据的选择，数据的冲突性以及数据的不一致性问题处理。在计算机取证分析中，审计日志的来源不同，因此这些审计信息的数据存在许多不一致的地方，如结构、单位、值域、含义等。另外，同一个系统的不同应用部分，它们对某一个安全主题相关的内容可能在几个审计日志中都包含了，而这些审计日志数据的结构往往不一致。当我们要提取与某一个安全主题相关的信息时，就需要把这些不同结构的数据进行集成，从而达到数据的统一化和规范化。

在实际的数据挖掘应用中，数据清理、数据集成和数据归约不一定都用到，我们需要根据实际情况和需求，在知识背景下合理地对源数据进行预处理。

2.2　日志记录的预处理和特征提取

在系统的主机日志和网络日志中，每一条记录都包含一些主要的属性信息和一些次要的信息，如来自 Microsoft IIs 日志的一条记录可能包含：用户 IP、用户名、日期、时间、服务类型、计算机名、服务器 IP、连接时间、接收字节数、发送字节数、服务状态、win32 状态、请求类型、操作目标等信息。但是在取证分析中，有些信息不是非常重要的，比如发送字节数和接收字节数等；有些信息则可以通过预处理中的概化方法，比如对时间信息，我们可以进行概化处理，方便挖掘；而用户 IP、服务器 IP、连接时间等则是一些关键信息，必须保留原始样式。同时对于不同的日志来源，这些格式并不固定，所以需要进行日志记录的规范化预处理(如图 3 所示)。

规范化格式处理的目的是为了达到以下几个目标：完整性、可扩展性、简单性。完整性要求规范化处理后的日志包含

维普资讯 http://www.cqvip.com

所有的需要信息，否则这个日志在计算机取证分析中就不可用。可扩展性是要求这种方法必须能容纳不同的系统日志和应用日志使日志在类型上不受限制。简单性是要求规范化格式处理后的日志，要容易被后面的挖掘算法处理分析，同时也方便日志数据库的设计实现。

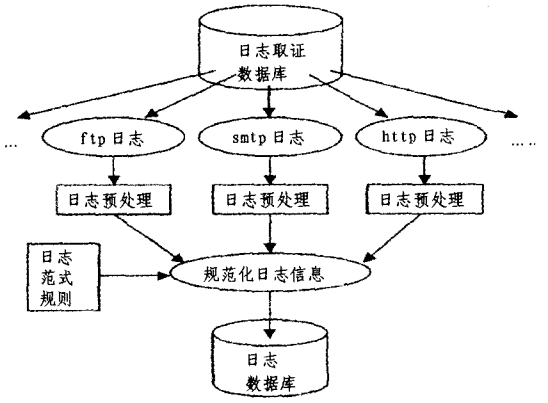

图 3　日志规范化处理流程模块图

利用数据挖掘技术的另一个关键问题是进行属性特征的选择，通过上述步骤对数据进行规范化格式预处理后，还需要对数据进行进一步的特征属性选取。

主要选取的关键特征包含以下几个方面：

· 连接特征：如一个用户连接的建立时间、连接持续的时间、通讯双方的主机 IP 和端口号、结束状态等。

· 内容特征：登录次数、登录成功次数、登录失败次数、对重要文件的访问状态、匿名登录的次数等。

· 统计特征：某一时间段内，对某个资源访问的次数和状态等。

网络事件通常在时间上具有很强的相关性，因此考虑在检测数据的处理中加入基于时间的统计特性，相当于在更抽象的层次上观察数据。我们采用时间窗的概念，针对每一条日志连接记录，统计出在指定时间窗口内与当前连接记录在属性上存在某种联系的连接记录，包括以下两种统计方式：

· 检查在一个时间窗口以内目标地址是某台主机的记录；

· 检查在一个时间窗口以内目标端口是某服务端口的记录。

这样，这里就有一个时间窗口大小的选择，文[55]的大小设置为 2 秒，这可以作为计算机取证分析系统的参考参数来实现时间窗口大小的设置。在具体系统实现时，我们可以作为用户自定义在对原始日志进行规范化格式处理的同时，系统设置和提取这些关键特征属我们可以利用数据挖掘算法进行分析取证，得到所需的信息。

2.3　数据库的设计

通过对各类系统的日志文件格式和日志在系统中的存放位置以及名称等形式化分析，对各类日志进行统一的描述和规范化格式处理，我们可以建立一个日志文件的信息库。同类系统的日志文件在格式上有相同的地方，如 windows 系统的三个系统日志文件、IIS 日志的几种日志类型、类 Unix/Linux 的 Apache 日志，甚至防火墙系统日志、IDS 系统日志等，他们的格式虽有一定的差别，但记录的内容基本上一样。

因此，在设计日志取证数据库时，可以对同类系统的日志进行扩展，设计出同类日志的扩展日志格式，使其可以容纳同类系统的日志信息，便于日志挖掘过程的进行。下面是日志取证数据库的关键数据表的结构定义：

表 1　日志信息 logInfo

标识符	意义	类型	值域
LogInfoID	日志信息编号	Int	长度≤4
LogCataLogID	日志分类编号	Int	长度≤4
SystemID	系统编号	Int	长度≤4
LogFileName	日志文件名	Varchar(50)	长度≤50
DefaultPath	日志文件缺省存储路径	Varchar(200)	长度≤200
LogFormat	日志文件格式	Varchar(200)	长度≤200
LogFormatFile	日志文件格式配置文件	Varchar(100)	长度≤100
LogHeadRowNum	日志文件头的行数	Int	长度≤4
ListSepartor	日志文件字段分割符	char(10)	长度≤10
LogRemark	日志描述	text	

表 2　目标系统日志 TargetSysLo

标识符	意义	类型	值域
TargetSysLogID	目标系统日志编号	Int	长度≤4
TargetSysInfoID	目标系统信息编号	Int	长度≤4
LogInfoID	日志信息编号	Int	长度≤4
LogFileSize	日志文件大小	Char(10)	长度≤10
LogFileCreateTime	日志文件创建时间	Datetime(8)	长度≤8
LogFileModifyTime	日志文件修改	Datetime(8)	长度≤8
LogFileLastAccess Time	日志文件最后访问时间	Datetime(8)	长度≤8
LogFileStorePath	日志文件存放路径	Char(100)	长度≤100
MD5Value	日志文件 MD5 值	char(32)	长度=32

表 3　原始日志数据 OriginalityLogDat

标识符	意义	类型	值域
OriginalityLogDataID	原始日志数据编号	Int	长度≤4
LogInfoID	日志信息编号	Int	长度≤4
TargetSysLogID	目标系统日志编号	Int	长度≤4
OriginalityLogData	原始日志数据	text	

表 4　目标系统信息 TargetSyslnf

标识符	意义	类型	值域
TargetSysLogID	目标系统信息编号	Int	长度≤4
SystemID	系统编号	Int	长度≤4
IP	目标系统 IP 地址	Char(32)	长度≤32
MAC	目标系统 MAC 地址	Char(50)	长度≤50
HostName	目标系统主机名	Vchar(50)	长度≤50

表 5　扩展日志文件 ExtendedLogFil

标识符	意义	类型	值域
ExtendedLogfileID	扩展日志文件编号	Int	长度≤4
ExtendedLogfileName	扩展日志文件名	Char(20)	长度≤20
LogCataLogID	日志分类编号	Int	长度≤4

扩展日志文件是对同类日志文件格式进行统一的扩展，主要有 Windows 系统日志 WinSysLog，类 Unix/Linux 系统日志 UnixLinuxSystemLog，类 Unix/Linux 的 syslog 日志 UnixLinuxSyslog，IIS 日志 IISLog，Appache 服务日志 ApacheLog，数据库日志 SQLLog，防火墙日志 FirewallLog，入侵检测系统日志 IDSLog，反病毒软件查杀记录 AntiVirusLog，DNS 服务日志 DNSLog，代理服务日志 ProxyLog，ICQ/OICQ 聊天记录 ICQLog 和路由器 RouteLog 等。根据扩展日志文

维普资讯 http://www.cqvip.com

件表的每一项扩展日志文件名，可以设计一个以扩展日志文件名为表名的数据表。

3 挖掘与分析平台的设计

完成数据源的准备工作后，我们采用关联分析方法从这些数据中找出各个数据项之间的关联规则，从而经过分析得出关联入侵模式；然后采用异常点分析算法对所有数据或局部数据中的异常部分进行分析，进一步挖掘数据之间存在的某种事实。但是应用于计算机取证分析的数据挖掘方法并不局限于这几种，其他如分类、聚类方法等挖掘算法，也将随着计算机取证分析研究的深入和挖掘算法的进一步完善，会得到更好的应用，数据挖掘方法将为计算机取证分析工作提供强有力的支撑。

因此我们在设计挖掘与分析模块的时候，充分考虑到将来的发展趋势，着眼于系统的伸缩性和可扩展性，采用分层结构的框架来设计挖掘和分析平台，将挖掘分析应用部分分为四个层次：数据层、挖掘算法层、挖掘任务层、模式表示层。框架结构如图 4 所示。

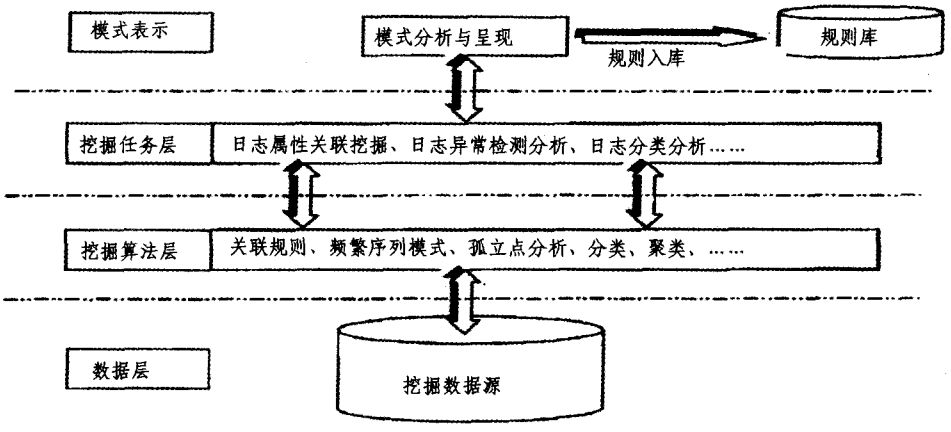

图 4 挖掘层次分析结构框架图

• 数据层：经过规范化预处理的日志及其他审计数据，为挖掘数据源部分。

• 挖掘算法层：提供关联规则、频繁序列模式分析、孤立点分析、分类算法、聚类算法等挖掘算法的具体实现，以接口的形式提供给挖掘目标层的任务挖掘。

• 挖掘任务层：根据具体的挖掘任务，利用挖掘算法层提供的算法，对挖掘数据源进行日志属性的内部关联挖掘、时间序列挖掘、异常检测、日志分类或聚类分析等.

• 模式表示层：把挖掘得到的结果以易于用户理解的直观方式呈现给用户，便于用户对模式进行评估和分析，并将有用的信息和规则加入规则库。

以分层结构来设计挖掘分析平台，结合了计算机取证分析工作的特点和数据挖掘技术快速发展的现况，既满足了现阶段数据挖掘在计算机取证领域的应用，也增加了整个系统方案的灵活性和可扩展性。

4 挖掘模式的评估与分析

因为计算机取证分析的特殊要求，所获得的结论必须具备严谨性、可靠性，必须符合法律程序。要符合这些要求，一方面需要侦察人员和专家的法律意识，保证所做的每一个步骤都符合法律上对取证的要求，另一方面我们对所取得挖掘模式结果必须进行评估和分析，在专家知识的支持下，也通过在原始证物中寻找计算机入侵和犯罪的事实痕迹，来支持挖掘结果的，证明结果的可靠性和可行性，而且呈现在法庭上的证据，必须是有原始证物中的依据。同时在这个过程中，也不断修改挖掘参数和指标、侦察的思路和突破口，以求从电子证据中找出尽可能多的反映犯罪事实的根据来。

挖掘模式评估与分析的结构如图 5 所示。

为了使数据挖掘的结果可以用以支持打击计算机犯罪活动，为电子证据的法庭出示提供指导和帮助，我们必须对数据挖掘的结果模式进行评估和分析，因此这里提供两个评估分析接口：挖掘模式评估接口和原始日志分析接口。

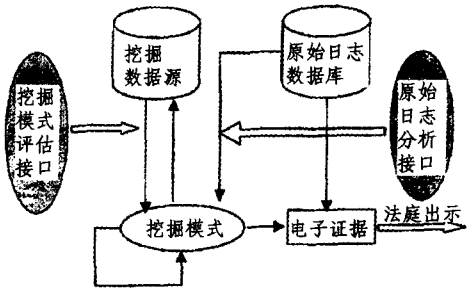

图 5 挖掘评估与分析模块结构图

• 挖掘模式评估接口提供对数据挖掘结果的评估与反馈。因为在对计算机取证收集的电子证据进行数据挖掘时，因为挖掘任务的需要，存在参数的设置和属性的选取与设置问题，另外为了保证挖掘结果的完备性，还需要从不同的地方着手，因此一个反馈与评估的过程是必需的。所以在取证分析系统中，我们提供挖掘模式评估接口，以确保数据挖掘方法的应用能够合法与合理，能尽可能多地从原始日志中得到一些隐藏的、不易发现的信息，供侦察人员的指导和参考。

• 原始日志分析接口提供原始日志数据库的分析比较。在数据挖掘获得的模式中，如果发现一些与计算机犯罪有关的可疑迹象或者异常情况，则可以以此为突破口，通过原始日志分析接口，在原始日志数据库中查找相应的原始材料进行进一步的分析勘察，找出事实证据来。

小结 本文以计算机取证分析的实际功能需求，讨论了基于日志的计算机取证分析原型系统设计中应该考虑和需要解决的几个问题，以数据挖掘的技术要点和过程为出发，从数据源的准备和数据预处理、数据挖掘分析方法的实现、挖掘模式的评估分析这三部分来分析和设计关于计算机取证分析的

维普资讯 http://www.cqvip.com

原型系统，着重讨论了各个部分功能模块的设计思想和主要目的。

参 考 文 献

1 林晓东，刘心松. 文件系统中日志技术的研究. 计算机应用，1998，118(1)

2 徐著. 基于数据挖掘技术的入侵监测模型：[博士学位论文]. 中科院高能物理研究所，2001

3 赵小敏. 基于日志的计算机取证技术的研究及系统设计与实现[D]：[硕士学位论文]. 浙江工业大学，2002

4 Han Jiawei，Kamber M. 数据挖掘—概念与技术. 范明，孟小峰译. 北京：机械工业出版社，2001

5 屈定春，林原. 一种新型的数据库应用— 数据采掘. 计算机应用研究，1996(6)

（上接第 295 页）

资料表明：1)从收入构成上看，2005 年中国软件产业的总收入达到了 3900 亿元(其中国内市场贡献率为 90%)，比上一年增长将近 40%(其中软件出口为 5%，软件外包为 2%)；未来中国，整个软件业收入将以 20%增长。2)从行业结构上看，2005 年中国软件产业整体收入中，53%来自软件产品、34%来自系统集成、13%来自软件服务(在国外正好倒过来)，中国软件产品增长率是 35%、软件服务增长率是 66%；未来中国，服务的比例会越来越高，最终会跟国际产业结构接轨。这说明“中国软件市场潜力巨大，敏捷软件开发需求迫切”，因为中国现行软件开发模式仍较偏重于传统软件开发模式(例如瀑布模型、结构化方法、原型法、面向对象方法等)，不能适应潜力巨大的软件市场需要，从而亟需全国性倡导软件开发模式的创新，大力倡用包括敏捷方法在内的新型软件开发方法。

瓶颈 2——软件交付速度的观念陈旧。有数据表明，从交付的功能和时间来看，中国前两年实施 ERP 的平均上线速度约为国外 6 倍。这首先要归因于国内企业利用自己后发优势(例如汲取了国外同行经验教训而少走弯路，可通过改变自身业务流程去适应所购打包软件来缩短定制化过程，很多行业用户无计算机系统的历史遗留大包袱等)；其次也不排除其它非正常因素影响，例如行政干预、业务部门片面要求上线速度(比如硬性规定什么时候上线)等。但软件开发三要素——速度、成本和质量，相互影响、彼此制约、密不可分。这种片面追求速度，必然使开发成本增加，而软件系统的高效性、灵活性、扩展性、鲁棒性等下降。因此，应改变传统软件交付速度老观念，应在项目范围、进度上有适度弹性，要倡用敏捷软件开发方法，以兼顾速度、成本和质量。

瓶颈 3——软件价值实现的理念落后。迄今为止，仍有不少人认为：1)软件的功能就等于价值；软件功能越多、系统越复杂、解决问题越多，价值就越大；但绝非功能越多越好，因为用户根本不会去用那些多余功能，而多余功能却会使维护成本激增、可扩展性降低。2)软件一旦上线，就实现了全部价值。但软件上线仅意味着当前生命周期的结束，也预示着下一生命周期的开始。一个优秀软件的总体价值，寓于它的多个生命周期中。据统计，国内企业 IT 投资，其 80%用于新产品的开发，20%用在现有系统的扩展(在国外恰好相反)。因此，需转变传统软件价值实现的落后理念，要提倡软件价值的长效实现观，应倡用敏捷软件开发方法。

瓶颈 4——现行从业人员素质培养的机制落后。软件产业是日新月异、蒸蒸日上的知识经济型高新技术行业。它的软件从业人员(例如在职程序员等)素质必须实行终生培养制，只有这样才能适应和满足软件产业生存和发展的需要，因为舍此将无以应对软件需求的高品质、软件技术的高难度、软件开发的高质量、软件发展的高速度。但中国现行软件从业人员素质的传统培养机制，往往落后于软件产业发展的客观要求，使软件从业人员素质不能更好地满足软件开发、更新、维护的新需要。因此，中国需对现行从业人员素质培养机制的创新，通过各种手段与方式，积极建立现行从业人员素质培养的新式长效机制，以确保软件从业人员素质和软件科学技术进步能彼此适应、与时俱进。

瓶颈 5——后备从业人员素质培养的模式脱节。高等院校、中专学校相关专业的学生们，是软件产业的从业人员后备大军。目前国内外对 IT 人才培养均较为重视，但从目前国内相关专业的软件专业技能教学的教学内容、教学方法、教学模式等来看，由于计算机教育学研究长期不足，致使大部分高等院校、中专学校相关专业现行教学，都处于“先从面向过程入门，再转向学习面向对象”的滞后脱节状态，未能推行和实现“使面向过程与面向对象实现协调与统一”的科学教学思想，更未能提倡和实现与软件开发技术进步保持同步并与之配套的教材体系和教学思想等。因此，应加强计算机教育学研究，促使国内外高等院校、中专学校相关专业加大教育改革和创新力度，争取更及时、更平稳、更有效地适应软件界的变化与发展。

瓶颈 6——支持敏捷软件方法的开发工具、集成环境之匮乏。与支持传统软件方法的开发工具、集成环境相比，人们(包括软件产业的现行从业人员、后备从业人员)深感支持敏捷软件方法的开发工具、集成环境之严重匮乏。众所周知，缺乏开发工具和集成环境支持的软件开发方法，其应用往往困难，其推广常常不易。敏捷软件开发方法的应用与推广，离不开支持它的开发工具和集成环境，需要研究和推出更成熟、便捷、人性化、可视化的开发工具、集成环境，以及在此类开发工具、集成环境支持下进行敏捷软件开发的成功典型案例库。为此，教育界和产业界应紧密结合，实时互动地提供敏捷开发典型案例库，进而推广到更宽广领域，供人们认知和实践敏捷思想参考，促进教育界和产业界的高素质人才的供需平衡。

结论 敏捷软件开发是优势突出、大有可作为的软件开发新方法。但是还应主动消除人们暂时对敏捷开发的若干认识偏误，并及时采取对症下药、切实可行的有效措施，疏通各个推广瓶颈，中国的敏捷软件开发一定会迎来蓬勃发展的春天！

参 考 文 献

1 Beck K. 解析极限编程——拥抱变化. 唐东铭译[M]. 北京：人民邮电出版社，2002

2 Succi G，Marchesi M. 极限编程研究. 张辉译[M]. 北京：人民邮电出版社，2002

3 Newkirk J，Martin R C，王钧译. 极限编程实践. [M]. 北京：人民邮电出版社，2002

4 王晓毅. TDD：金字塔上神像的光芒. [J]. 程序员，2006(09)