应用层异常检测方法研究

谢柏林 余顺争 王 宇
(中山大学电子与通信工程系 广州 510275)

摘 要 目前绝大部分异常检测方法只利用数据包的头部信息来检测网络攻击,即仅仅从网络层、传输层来分析网络的异常情况。而研究表明现在的网络攻击主要发生在应用层,因此从应用层来分析网络异常的研究就显得十分重要。首先介绍了入侵检测和异常检测的研究现状,突出强调了应用层异常检测的重要性,接着详细介绍了目前几种主要的应用层异常检测方法,最后讨论了应用层异常检测所面临的挑战。

关键词 应用层,异常检测,网络安全
中图法分类号 TP393 **文献标识码** A

Research on Application Level Anomaly Detection

XIE Bai-lin YU Shun-zheng WANG Yu
(Department of Electronics and Communication Engineering, Sun Yat-Sen University, Guangzhou 510275, China)

Abstract Most of the network anomaly detection approaches are based on packet header fields, while the payload is usually discarded, namely they detect network attacks only from network layer and transport layer. Unfortunately, most of today's attacks happen on the application level, so the research of the application level anomaly detection is very important. We first introduced the current status of intrusion detection and network anomaly detection, and emphasized the importance of the application level anomaly detection. Then we introduced the main approaches of the application level anomaly detection in detail. Finally we discussed the challenges of the application level anomaly detection.

Keywords Application level, Anomaly detection, Network security

1 引言

随着网络技术的发展,互联网已渗透到人们生活的方方面面,人们的生活越来越离不开网络。2008年中国互联网络信息中心(CNNIC)发布的中国互联网发展状况统计报告显示国内网民总人数已达2.1亿,普及率达16%[1]。然而随着网络的延伸,网络安全问题受到人们越来越多的关注。网络所面临的安全问题也是层出不穷,例如:蠕虫病毒、垃圾邮件、僵尸网络(Botnet)、零日攻击(zero-day attack)等。曾经作为最主要安全防范手段的防火墙,显然不能满足当今网络的安全需要。作为对防火墙有益的补充,入侵检测系统(Intrusion Detection System, IDS)显得越来越重要。入侵检测系统通过收集和分析网络数据流、系统审计记录等,来发现和识别网络中的入侵行为和入侵企图,从而提供对网络内部攻击、外部攻击和误操作的实时检测。

根据信息来源的不同,入侵检测可分为:基于主机的入侵检测和基于网络的入侵检测(本文所提到的入侵检测除特别说明外都是指基于网络的入侵检测)。根据分析方法的不同,入侵检测可分为:误用检测(Misuse Detection)和异常检测(Anomaly Detection)。由于误用检测准确度高、技术相对成熟,因此大部分入侵检测系统都采用误用检测技术。然而误用检测最大的缺陷是不能识别出未知攻击和新出现的攻击,因此面对零日攻击、多形态蠕虫病毒(Polymorphic Worm)时,误用检测就显得无能为力。零日攻击通常基于未知的安全漏洞或还没有被厂商修复的安全漏洞,这类攻击可以轻易地绕过误用检测系统。零日攻击极具杀伤力,因为任何人都很难对未知的情况做出正确的反应,此种攻击成功率高、隐蔽性强。Levy Elias在文献[2]中对零日攻击做了较为详细的介绍。另外误用检测也不能有效识别僵尸网络,因为研究者很难准确获得僵尸网络的特征信息,因而部分学者开始利用异常检测技术来检测僵尸网络,例如在文献[3,4]中,学者们都开始尝试利用异常检测的方法来发现僵尸网络。理论上讲,异常检测能识别任何攻击,包括上面所提到的零日攻击、多形态蠕虫病毒、僵尸网络,因而异常检测比误用检测更有前途。

异常检测是通过建立网络的正常行为模型,来发现网络的异常情况,从而达到识别攻击的目的。异常检测有效的前提条件是:网络的攻击行为总是与网络的正常行为不同。在异常检测的研究过程中,研究者们提出了各种各样的异常检测方法,这些检测方法基本上可分为3大类,即:基于统计的

到稿日期:2008-05-13 本文由国家高技术研究发展计划("863"计划)(2007AA01Z449),国家自然科学基金-广东联合基金重点项目(U0735002)资助。

谢柏林(1982-),男,博士研究生,主要研究方向为网络应用层异常检测、应用过程跟踪,E-mail:xiebailin96@126.com;余顺争(1958-),男,教授,博导,主要研究方向为网络异常检测、网络主动防护;王 宇(1983-),男,博士研究生,主要研究方向为网络流量异常检测。

方法、基于机器学习的方法、基于数据挖掘的方法[5]。这些检测方法中的绝大部分只分析数据包的头部信息，例如 IP 地址、端口号、TCP 标志位 SYN，ACK 等，而忽略了应用层负载信息。也就是说绝大部分异常检测方法只从网络层和传输层来分析网络的异常，而没有考虑网络应用层的情况。然而研究表明大部分攻击发生在应用层[6]，而这些攻击流在网络层和传输层的表现和正常数据流没有明显区别，因而那些只分析数据包头部信息的检测方法很难识别出这些攻击。文献[7,8]表明：目前绝大部分异常检测系统能准确、快速地检测出网络层和传输层的攻击，例如 ARP 中毒、SYN 泛洪攻击、Teardrop 攻击等，而面对发生在应用层的攻击时就显得力不从心。例如文献[7]对几种基于机器学习的异常检测系统所做的测试表明：绝大部分异常检测系统在检测 U2R(User to Root)，R2L(Remote to Local)等应用层攻击时，检测率都达不到 50%，甚至有些异常检测系统一种应用层攻击也不能识别出来。因此，应用层异常检测的研究就显得十分有必要。

2 应用层异常检测方法

目前国内外有不少学者正在研究如何从应用层来检测网络攻击，他们提出了一些有效的异常检测方法，这些方法都是从应用层的角度来识别网络攻击。这些方法中的绝大多数只针对某种具体应用的异常检测，而不能检测应用层的其它攻击。例如，文献[9]中提出了一种用于检测应用层泛洪攻击的方法，该方法主要针对 HTTP 请求发动的洪泛攻击。国外 Santa Barbara 大学的学者们在文献[10-12]中提出了一种用于检测 Web 攻击(web-based attack)的方法。目前能识别出应用层多种攻击的方法大体可分为两大类，即：基于负载字符统计分布的方法[13]、基于负载关键词(Keywords)的方法[14,15]。本文将在接下来的章节中详细介绍目前几种典型的应用层异常检测方法。

2.1 基于负载字符统计分布的方法

2.1.1 PAYL 方法

PAYL 方法是由哥伦比亚大学学者 Ke Wang 等人在 2004 年提出的[13]。从应用层来看，网络数据可以理解为字符流或者字节流，PAYL 方法是通过分析数据包负载的字符统计分布，来检测应用层攻击。该方法的理论依据是：一般而言，标准的网络服务都有预先分配的固定端口号。比如 20 端口用于 FTP 的数据传送，21 端口用来传送 FTP 命令，22 端口用于 SSH，80 端口则用于 Web 服务。而且每种应用都有它自己特定的协议，即使是同一应用，不同网络环境下数据包负载的字符统计分布也不一样。以端口 22 来说，由于使用该端口的数据被加密，因此使用该端口的数据包负载的字符分布应该是比较均匀的。而使用端口 21 的数据包负载包含的应该主要是由用户通过键盘输入的字符。简而言之，该方法的理论依据是：不同端口代表不同的应用，不同应用的数据包负载的字符统计分布不同；即使是相同的应用，在不同网络环境下数据包负载的字符统计分布也不一样。

该方法在计算数据包负载的字符统计分布时采用了 n-gram 分析法，n-gram 分析法已经被广泛应用到很多领域中。作者 M. Damashek 在文献[16]中第一次对 n-gram 分析法做了全面、详细的介绍。在 PAYL 方法中，一个 n-gram 指的是数据包负载中连续 n 个相邻的字符集。也可以理解为：用一个宽度为 n 的滑动窗口依次滑过整个负载，一次滑过一个字节，每向前滑动一次，滑动窗口所覆盖的 n 个相邻的字符集就是一个 n-gram，图 1 所示的是 5-gram 的情况。

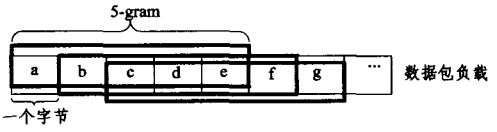

图 1 5-gram

在 PAYL 方法中，对于一个数据包负载来说，它的特征向量就是每一个 n-gram 出现的相对频率。用每一个 n-gram 在该数据包负载中出现的次数除以该数据包负载中所有 n-gram 出现的次数，得到的值就是每个 n-gram 相对出现的频率。最简单的情况就是 1-gram，它的特征向量的值就是计算 256 个字符集中每一个相对出现的频率。

该方法具体流程如下：(假设采用该方法来检测流入某个校园网的数据的异常情况)

(1) 模型训练阶段：首先采集尽量多的流入该网络的正常数据包，然后把端口号(80，21，22，23 等)和数据包负载长度都一样的数据包归为同一个类。在每个类中，采用 n-gram 分析法计算出每个数据包负载中每个 n-gram 出现的相对频率，然后计算出这个类中每个 n-gram 相对频率的平均值和方差，用这个平均值和方差来构建这个类的模型。为了减少模型的数量，在模型训练阶段，如果两个相邻模型的差异比较小，我们就合并这两个模型。

(2) 异常检测阶段：对于新进来的数据包，首先计算出该数据包负载中每个 n-gram 出现的相对频率，即 n-gram 的统计分布。根据端口号和数据包负载长度来确定该数据包所对应的模型，然后把该数据包负载的 n-gram 统计分布与它相对应的模型进行比较，在比较过程中采用马氏距离(Mahalanobis Distance)来计算它们之间的差距。如果它们之间的差距超过某个阈值，就认为这个数据包是异常的。反之，则认为该数据包是正常的。

哥伦比亚大学的学者们在文献[17-19]中证实该方法能有效识别蠕虫病毒、零日攻击、模拟攻击(Mimicry Attack)。该方法的优点是：计算简单，训练过程可以无监督进行，而且训练过程对噪声不太敏感。该方法主要缺陷是目前很多 P2P 应用为了躲避封杀，开始使用 IANA 分配给其它应用的标准端口，例如目前有一些 P2P 应用也使用 80 端口。在这种情况下，不同应用都使用相同的端口，这与 PAYL 方法的前提条件不相符，因此在这种情况下该方法就显得不太适用。

2.2 基于负载关键词(Keywords)的方法

2.2.1 ALAD 方法

学者 Matthew V. Mahoney 和 Philip K. Chan 在文献[14]中提出了一种应用层异常检测的方法，简称为 ALAD(Application Level Anomaly Detection)方法。在该方法中，作者第一次尝试利用应用层负载的关键词来检测应用层攻击。在 ALAD 方法中，对于每个数据包它的关键词就是该数据包负载的每一行的第一个词。在该方法中数据包负载的行就是以换行符“\n”为标志的，如果一个数据包的负载中没有换行符“\n”，就把这个数据包的所有负载数据看成是一行，而数据包负载的词是以空格符为标志的。因此，一个数据包可能有多

个关键词，即包含多个换行符。ALAD 方法是通过构造联合属性对(关键词|目的端口)，来检测网络应用层攻击，并且该方法只分析数据包负载的前 1000 个字节。该方法的流程大体如下：

(1) 模型训练阶段：首先采集尽量多的正常数据包，然后提取出这些数据包中联合属性对(关键词|目的端口)的取值，把这些取值保存起来作为这些数据集训练出的模型。

(2) 异常检测阶段：首先对新进来的数据包进行预处理，提取出它的关键词和目的端口，然后构造联合属性对(关键词|目的端口)。最后与模型进行比较，如果在模型中能找到该属性对的取值，就认为该数据包是正常的。反之，则认为该数据包是异常的。

该方法的优点是：能识别出部分应用层攻击。该方法主要缺陷是过于简单，因而很多应用层攻击都不能识别。例如在检测 Web 攻击(Web-based attacks)时就显得无能为力，因为 Web 攻击流也采用 80 端口，并且攻击数据包的关键词和正常 Web 数据包的关键词都是一样的(即 GET，POST，ACCEPT 等)。

2.2.2 Like Zhang 等人提出的方法

2007 年，学者 Like Zhang 和 Gregory B. White 在 ALAD 方法的基础上提出了一种新的基于负载关键词的应用层异常检测方法[15]。在该方法中，对于每个数据包来说，它的关键词就是该数据包负载的第一行的第一词。在该方法中，数据包负载的行和词的定义跟 ALAD 方法相同。因此，在该方法中一个数据包只有一个关键词，另外该方法也利用了数据包的一些头部信息。该方法具体流程如下：

(1) 模型训练阶段：首先采集尽量多的正常数据包，然后提取出每个数据包的关键词和该关键词的值。在该方法中，关键词的值是指：在数据包负载的第一行中除了关键词外，剩下的所有可打印的 ASCII 字符集。例如：如果一个数据包负载的第一行字符集是："GET /download. html HTTP/1. 1\r\n"，那么它的关键词是 GET，关键词的值为："/download. html HTTP/1. 1"。另外还要提取出数据包的一些头部信息，如：源地址、目的地址、源端口号、目的端口号。在该方法中，作者共提取出九个属性，即：IP 头部长度、IP 版本号、数据包长度、源地址、目的地址、源端口号、目的端口号、负载长度、负载关键词。然后利用主成分分析法(PCA)找出变化范围最大的属性，即这些属性最能反映网络异常情况。在该方法中，作者最后选取的属性是：源端口号、目的端口号、负载长度、关键词。最后构造出几个联合属性对，如：源端口|关键词、关键词|关键词的取值、关键词|负载长度。在模型训练阶段，收集所有数据包中这几个联合属性对的取值，然后把这些值保存在一张哈希表中，作为这些数据集训练出的模型。表 1 为模型训练时所用的一些联合属性对，图 2 为该方法在模型训练阶段的流程图。

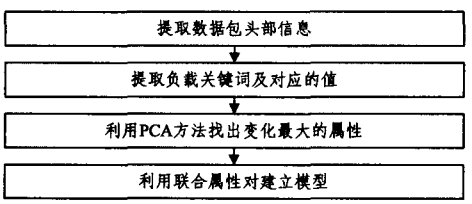

图 2 模型训练阶段流程图

表 1 模型训练时所用的一些属性对

属性对	取值
目的端口|关键词	80|GET，80|POST，25|RCPT，…
关键词|关键词的取值	GET|/download. html HTTP/1. 1，…
关键词|负载长度	GET|1020，HEAD|980，…

(2) 异常检测阶段：首先对新进入的数据包进行预处理，提取出所需联合属性对的取值。然后跟模型进行比较，即：检查该数据包中联合属性对的取值是否在哈希表里。如果取值在哈希表中，就认为该数据包是正常的。反之，则认为该数据包是异常的。

该方法的优点是：性能比 ALAD 方法要好，能识别出更多的应用层攻击。该方法主要缺陷是：对存储空间需求比较大、检测速度比较慢。表 2 为这三种应用层异常检测方法的一个比较。

表 2 应用层异常检测方法比较

应用层异常检测方法	检测原理	主要优点	主要缺点
PAYL	利用负载字符统计分布来检测应用层攻击	计算简单，训练过程全自动、无监督	不太适用于当今网络环境
ALAD	利用负载关键词及目的端口号来检测应用层攻击	能识别出部分应用层攻击	过于简单，很多应用层攻击都不能识别
Like Zhang 等人提出的方法	利用负载关键词及数据包一些头部信息来检测应用层攻击	性能比 ALAD 方法要好	对存储空间需求比较大，检测速度比较慢

3 应用层异常检测面临的挑战

目前应用层异常检测的研究正处于起步阶段，虽然应用层异常检测有很大的发展潜力，但它面临着许多挑战，这些挑战可以归纳为以下 6 个方面：

(1) 所有的异常检测方法都可以分为两个阶段，即：模型训练阶段和异常检测阶段。在模型训练阶段，由于用于模型训练的数据很难达到理想状态，这些数据往往包含一些攻击流，因此由这种数据训练出的模型不能准确反映网络的正常行为，而用该模型进行异常检测时，会降低异常检测方法的检测率。另外当今网络流量十分庞大，包含各种各样的应用数据流，这些因素使得很难在模型训练阶段建立起一个能准确反映正常数据流的模型。因此和其它异常检测方法一样，应用层异常检测也面临着的一个挑战是在模型训练阶段，如何降低噪声对模型的影响。

(2) 跟其它异常检测方法一样，应用层异常检测也存在虚警(False Positive)过高的问题。这是异常检测存在的最大缺陷，也是异常检测方法广泛应用所面临的最大障碍。Axelsson 在文献[20]中指出：为了使异常检测能应用到实际网络环境中，异常检测的误报率应该低于 1/100，000。因此，应用层异常检测面临的最大挑战是：如何设计出有效的策略来降低误报率。

(3) 目前公开的能用于异常检测研究的数据集中，绝大部分数据只包含数据包的头部信息，而没有应用层负载数据。例如 CAIDA 网站[21]上面提供很多可用于异常检测研究的数据，这些数据只包含数据包头部信息，而没有应用层负载数据。目前公开的包含数据包负载的数据只有 MIT 林肯实验室在 1998 年和 1999 年公布的 DARPA IDS 数据集。该数据

集是通过模拟产生的，文献[22]指出：产生这些数据的方法和数据本身都存在很多问题，并且这些数据不能很好地模拟出实际的网络环境。而评估应用层异常检测方法所需的数据必须包含应用层负载，所以应用层异常检测面临的一个问题是：缺少公开的可用于研究和评估应用层异常检测方法的数据集。

(4) 应用层异常检测面临的另一个挑战是：如何应对模拟攻击(Mimicry Attack)。模拟攻击的概念在文献[23]中首次被提出，模拟攻击是假设攻击者在完全清楚异常检测模型的方法、参数设置的情况下，通过构造检测系统认为是正常的数据来隐藏攻击过程，从而绕过入侵检测系统。模拟攻击通常使用“字节替换”(byte substitution)和“数据填充”(padding)的方式来使攻击流服从异常检测系统所定义的“正常数据流”的特点[24]。

(5) 数据包负载包含的信息比数据包头部包含的信息多很多，并且数据包负载信息更能反映出应用层的异常情况，怎样才能更有效地利用负载信息还有待进一步的研究。另外应用层数据一般会涉及到个人隐私，因此应用层异常检测面临的一个挑战是怎样才能既保护用户的隐私权又能实现应用层的异常检测。一般而言，如果检测过程是全自动、无监督的，那么就不会侵犯用户的隐私权。

(6) 目前有些应用数据采用加密技术，对于这种情况，像ALAD这种利用负载关键词的方法就显得不太适用。因为在这种情况下，数据包负载的关键词不能准确反映出应用层异常的情况，所以应用层异常检测面临的一个挑战是如何应对数据加密的情况。

结束语 目前网络攻击主要发生在应用层，而传统的异常检测方法不能有效识别出这些攻击，因此应用层异常检测的研究就显得十分有意义。应用层异常检测是异常检测的一个新方向，目前应用层异常检测的研究正处于起步阶段。虽然应用层异常检测面临着一些挑战，但它的前景是光明的，应用层异常检测也为异常检测的研究指明了一条新的出路。

参 考 文 献

[1] CNNIC. 第21次中国互联网络发展状况统计报告[R]. http://www.cnnic.net.cn/uploadfiles/pdf/2008/1/17/104156.pdf, 2008

[2] Levy E. Approaching Zero[J]. IEEE Security & Privacy Magazine, 2004, 2(4): 65-66

[3] Binkley J R, Singh S. An Algorithm for Anomaly-based Botnet Detection[C]// SRUTI'06: 2nd Workshop on Steps to Reducing Unwanted Traffic on the Internet. San Jose, USA: 2006: 43-48

[4] Villamarin-salomon R, Brustoloni J C. Identifying Botnets Using Anomaly Detection Techniques Applied to DNS Traffic[C]// Fifth IEEE Consumer Communications & Networking Conference. Las Vegas, Nevada, USA, 2008: 476-481

[5] Patcha A, Park J M. An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends[J]. Computer Networks: The International Journal of Computer and Telecommunications Networking, 2007, 51(12): 3448-3470

[6] Wang H J, Guo C, Simon D R, et al. Shield: Vulnerability-Driven Network Filters for Preventing Known Vulnerability Exploits [J]. ACM SIGCOMM Computer Communication Review, 2004, 34(4): 193-204

[7] Lazarevic A, Ertoz L, Kumar V, et al. A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection[C]// SIAM International Conference on Data Mining. Cathedral Hill Hotel, San Francisco, USA, 2003: 25-36

[8] Lippmann R, Haines J W, Fried D J, et al. The 1999 DARPA Off-line Intrusion Detection Evaluation [J]. Computer Networks, 2000, 34(4): 579-595

[9] 谢逸，余顺争. 应用层洪泛攻击的异常检测[J]. 计算机科学，2007, 34(8): 109-111

[10] Kr C, Toth T, Kirda E. Service Specific Anomaly Detection for Network Intrusion Detection [C]// Proceedings of the 2002 ACM symposium on Applied Computing. Madrid, Spain, 2002: 201-208

[11] Kruegel C, Vigna G. Anomaly Detection of Web-based Attacks [C]// Proceedings of the 10th ACM Conference on Computer and Communication Security. Washington, DC, USA, 2003: 251-261

[12] Kruegel C, Vigna G, Robertson W. A Multi-model Approach to the Detection of Web-based Attacks[J]. Computer Networks, 2005, 48(5): 717-738

[13] Wang K, Stolfo S J. Anomalous Payload-Based Network Intrusion Detection[C]// Seventh International Symposium on Recent Advances in Intrusion Detection, RAID 2004. Sophia Antipolis, France, 2004: 203-222

[14] Mahoney M V, Chan P K. Learning Nonstationary Models of Normal Network Traffic for Detecting Novel Attacks [C]// Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. Edmonton, Alberta, Canada, 2002: 376-385

[15] Like Z, White G B. Anomaly Detection for Application Level Network Attacks Using Payload Keywords[C]// Proceedings of the 2007 IEEE Symposium on Computational Intelligence in Security and Defense Applications. Honolulu, Hawaii, USA, 2007: 178-185

[16] Damashek M. Gauging Similarity with n-Grams: Language-Independent Categorization of Text[J]. Science, 1995, 267: 843-848

[17] Wang K, Cretu G, Stolfo S J. Anomalous Payload-Based Worm Detection and Signature Generation[C]// Eighth International Symposium on Recent Advances in Intrusion Detection, RAID 2005. Seattle, Washington, USA, 2005: 227-246

[18] Parekh J J, Wang K, Stolfo S J. Privacy - preserving Payload - based Correlation for Accurate Malicious Traffic Detection[C]// Proceedings of the 2006 SIGCOMM Workshop on Large-scale Attack Defense. Pisa, Italy, 2006: 99-106

[19] Wang K, Stolfo J J. Anagram: A Content Anomaly Detector Resistant to Mimicry Attack[C]// Ninth International Symposium on Recent Advances in Intrusion Detection, RAID 2006. Hamburg, Germany, 2006: 226-248

[20] Axelsson S. The Base-Rate Fallacy and the Difficulty of Intrusion Detection[J]. ACM Transactions on Information and System Security, 2000, 3(3): 186-205

[21] CAIDA 网站网址：http://www.caida.org/

[22] Mchugh J. Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory[J]. ACM Transactions on Information and System Security (TISSEC), 2000, 3(4): 262-294

(下转第52页)

6. 计算学科中的系统科学方法
主要内容：系统科学的基本思想；软件开发中为什么要引入系统科学方法；结构化方法；面向对象方法。

7. 社会和职业的问题
主要内容：计算的社会背景；道德分析的方法；职业和道德责任；基于计算机系统的风险和责任；团队工作；知识产权；隐私和公民自由；计算机犯罪。

8. 探讨与展望
主要内容：包括计算本质的认识历史、第三次数学危机与希尔伯特纲领、图灵对计算本质的揭示等问题的探讨，以及从"计算机导论"课程的构建、教程的继续完善、《计算机专业规范》的实施等问题入手，对计算教育的发展所作的简单展望。

4 两类"计算机导论"课程的比较

综上所述，尽管两类"计算机导论"课程的侧重点不同，但本质上是一致的，都是关于学科本质特征的基础概念或思想与方法的讲授。

为便于理解，我们用"思想与方法"替代计算思维定义中的"基础概念"。于是计算思维又可定义为：是运用计算机科学的思想与方法进行问题求解、系统设计以及人类行为理解的涵盖了计算机科学之广度的一系列思维活动。

两类课程都严格的将"计算机操作"的内容置于课程之外。周教授认为，在"计算机导论"课程的教学中，最悲哀莫过于不经过"脑子"而是以"计算机操作"来理解计算学科的概念；笔者则认为，"计算机导论"课程与那些以"计算机操作"为内容进行设置的所谓"计算机导论"根本就是两码事，并以电子学科作类比，认为即使某人已相当熟练地操作电子产品（如家用电器），也不能说明他已相当了解电子学科一样来阐述这个道理。

以计算思维为基础的"计算机导论"强调的是抽象与自动化，而以学科思想与方法为基础的"计算机导论"强调的是抽象、理论和设计，它们都反映了计算的本质：什么能有效地自动进行？相对而言，后者更易于学科各分支领域概念的划分，也更易于教学。另外，作为第一类课程主要内容的"学科深层次问题"，显然已包含在第二类课程关于学科的基本问题之中。

课程最大的不同在于，以计算思维为基础的"计算机导论"大篇幅的介绍了计算思维对其他学科的影响，以及作者所在学校的特色。而以学科思想与方法为基础的"计算机导论"在强调学科抽象、理论和设计 3 个最基本的概念以及学科的基本问题后，大篇幅的介绍了学科的核心概念、学科采用的数学方法和系统科学方法、社会与职业问题、学科中有争议的问题以及未来的计算教育等。

显然，两类"计算机导论"课程各有所长，可以相互吸收和借鉴。这种相互的吸收和借鉴，有助于以"计算思维能力"培养为核心的"计算机导论"课程的教学改革，也有助于计算学科其他课程的教学改革。

结束语 本文所讨论的两类"计算机导论"课程都涉及到面向学科思维能力的培养，这种思维能力的强大被周以真教授清晰而又系统地描述了出来，并得到学术界的广泛关注和支持。

周教授描述的计算思维其实一直隐藏在我们的教学之中，可以说，计算学科的教学其实也就是关于计算思维的教学，只不过以往的教学没有将这种思维的特征明显地表示出来。这样，就引出了下面两个富有挑战性的问题：

1. 什么样的教学更有助于计算思维能力的培养？

2. 什么样的策略适用于计算思维能力培养的评估？

本文所讨论的两类"计算机导论"课程都引起了计算机界广泛关注，相对而言，以学科思想与方法为基础的"计算机导论"被更多的高校采用；而以计算思维为基础的"计算机导论"讲授的对象是大学所有学科一年级的新生，更需注意的是，这种以"计算思维"为核心的内容，相继被美国和欧洲列为保持国家科技与教育世界领先地位的关键之所在[9-10]，并得到大量经费的资助，如 2008 年启动的总经费为 75000 万美元的美国国家科学基金会（NSF）重大基金资助计划 CDI（Cyber-Enabled Discovery and Innovation，Cyber 能够实现的科学发现与技术创新）的支持[9]。

相对于英美等西方发达国家，目前，我国大学的计算机基础教学理念的侧重点有所不同，前者强调的是学科思维能力的培养，后者强调的是应用能力的培养。希望国内的计算机教育工作者暂时放下手上的工作，静下心来认真地思考一下这种不同。

参 考 文 献

[1] Denning P J, et al. Computing as a discipline. Communications of the ACM, 1989, 32(1)

[2] ACM/IEEE-Curriculum 2001 Task Force. Computing Curricula 2001, Computer Science. IEEE Computer Society Press and ACM Press, 2001

[3] The Joint Task Force for Computing Curricula 2005. The Overview Report. A cooperative project of ACM, AIS, and IEEE-CS. Sept 2005

[4] CS2001InterimReview(draft). 2008. http://wiki.acm.org/cs2001/index.php? title=Main_Page

[5] Wing J M. Computational Thinking. Communications of the ACM, 2006, 49(3)

[6] Wing J M. Computational Thinking and Thinking about Computing[EB/OL]. 2008. http://www.cs.cmu.edu/~wing/publications/Wing08a.pdf

[7] 董荣胜，古天龙. 计算机科学与技术方法论[M]. 北京：人民邮电出版社，2002

[8] 董荣胜. 计算机科学导论——思想与方法[M]. 北京：高等教育出版社，2007

[9] http://www.nsf.gov/crssprgm/cdi/

[10] BCS. The science of thinking: Europe's next policy challenge [EB/OL]. 2008. http://www.sciencebusiness.net/documents/thinking.pdf

（上接第 24 页）

[23] Wagner D, Soto P. Mimicry Attacks on Host-based Intrusion Detection Systems[C]// Proceedings of the 9th ACM Conference on Computer and Communications Security. Washington, DC, USA, 2002: 255-264

[24] Fogla P, Lee W. Evading Network Anomaly Detection Systems: Formal Reasoning and Practical Techniques[C]// Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria, Virginia, USA, 2006: 59-68