信息来源：<http://blog.eviloctal.com/evilhsu/>  
  
入侵检测技术综述  
1.什么是入侵检测，为什么需要入侵检测？  
1.1 为什么需要入侵检测  
1.1. 1黑客攻击日益猖獗，防范问题日趋严峻  
随着计算机技术的发展，在计算机上处理业务已由基于单机的数学运算、文件处理，基于简单连结的内部网络的内部业务处理、办公自动化等发展到基于企业复杂的内部网、企业外部网、全球互联网的企业级计算机处理系统和世界范围内的信息共享和业务处理。在信息处理能力提高的同时，系统的连结能力也在不断的提高。但在连结信息能力、流通能力提高的同时，基于网络连接的安全问题也日益突出：  
● 具Warroon Research的调查，1997年世界排名前一千的公司几乎都曾被黑客闯入。  
● 据美国FBI统计，美国每年因网络安全造成的损失高达75亿美元。  
● Ernst和Young报告，由于信息安全被窃或滥用，几乎80%的大型企业遭受损失  
● 在最近一次黑客大规模的攻击行动中，雅虎网站的网络停止运行3小时，这令它损失了几百万美金的交易。而据统计在这整个行动中美国经济共损失了十多亿美金。由于业界人心惶惶，亚马逊(Amazon.com)、AOL、雅虎(Yahoo!)、eBay的股价均告下挫，以科技股为主的那斯达克指数(Nasdaq)打破过去连续三天创下新高的升势，下挫了六十三点，杜琼斯工业平均指数周三收市时也跌了二百五十八点。遇袭的网站包括雅虎、亚马逊和Buy.com、MSN.com、网上拍卖行eBay以及新闻网站CNN.com，估计这些袭击把Internet交通拖慢了百分二十。"  
看到这些令人震惊的事件，不禁让人们发出疑问："网络还安全吗？"  
  
  
目前，我国网站所受到黑客的攻击，还不能与美国的情况相提并论，因为我们在用户数、用户规模上还都处在很初级的阶段，但以下事实也不能不让我们深思：  
1993年底，中科院高能所就发现有"黑客"侵入现象，某用户的权限被升级为超级权限。当系统管理员跟踪时，被其报复。

1994年，美国一位14岁的小孩通过互联网闯入中科院网络中心和清华的主机，并向我方系统管理员提出警告。  
1996年，高能所再次遭到"黑客"入侵，私自在高能所主机上建立了几十个帐户，经追踪发现是国内某拨号上网的用户。  
同期，国内某ISP发现"黑客"侵入其主服务器并删改其帐号管理文件，造成数百人无法正常使用。  
1997年，中科院网络中心的主页面被"黑客"用魔鬼图替换。  
进入1998年，黑客入侵活动日益猖獗，国内各大网络几乎都不同程度地遭到黑客的攻击：  
　　　　　　　　2月，广州视聆通被黑客多次入侵，造成4小时的系统失控；  
　　　　　　　　4月，贵州信息港被黑客入侵，主页被一幅淫秽图片替换；  
　　　　　　　　5月，大连ChinaNET节点被入侵，用户口令被盗；  
　　　　　　　　6月，上海热线被侵入，多台服务器的管理员口令被盗，数百个用户和工作人员的账号和密码被窃取；  
　　　　　　　　7月，江西169网被黑客攻击，造成该网3天内中断网络运行2次达30个小时，工程验收推迟20天；  
同期，上海某证券系统被黑客入侵；  
　　　　　　　　8月，印尼事件激起中国黑客集体入侵印尼网点，造成印尼多个网站瘫痪，但与此同时，中国的部分站点遭到印尼黑客的报复；  
同期，西安某银行系统被黑客入侵后，提走80.6万元现金。  
　　　　　　　　9月，扬州某银行被黑客攻击，利用虚存帐号提走26万元现金。  
　　　　　　　　10月，福建省图书馆主页被黑客替换。  
1.1.2 传统的安全产品足够吗？  
Internet的开放性以及其他方面因素导致了网络环境下的计算机系统存在很多安全问题。为了解决这些安全问题，各种安全机制、策略和工具被研究和应用。然而，即使在使用了现有的安全工具和机制的情况下，网络的安全仍然存在很大隐患，这些安全隐患主要可以归结为以下几点:  
　　(1) 每一种安全机制都有一定的应用范围和应用环境。防火墙是一种有效的安全工具，它可以隐蔽内部网络结构，限制外部网络到内部网络的访问。但是对于内部网络之间的访问，防火墙往往是无能为力的。因此，**对于内部网络到内部网络之间的入侵行为和内外勾结的入侵行为，防火墙是很难发觉和防范的。**　　(2) 安全工具的使用受到人为因素的影响。一个安全工具能不能实现期望的效果，在很大程度上取决于使用者，包括系统管理者和普通用户，不正当的设置就会产生不安全因素。例如，NT在进行合理的设置后可以达到C2级的安全性，但很少有人能够对NT本身的安全策略进行合理的设置。虽然在这方面，可以通过静态扫描工具来检测系统是否进行了合理的设置，但是这些扫描工具基本上也只是基于一种缺省的系统安全策略进行比较，针对具体的应用环境和专门的应用需求就很难判断设置的正确性。  
　　(3) 系统的后门是传统安全工具难于考虑到的地方。防火墙很难考虑到这类安全问题，多数情况下，这类入侵行为可以堂而皇之经过防火墙而很难被察觉；比如说，众所周知的ASP源码问题，这个问题在IIS服务器4.0以前一直存在，它是IIS服务的设计者留下的一个后门，任何人都可以使用浏览器从网络上方便地调出ASP程序的源码，从而可以收集系统信息，进而对系统进行攻击。对于这类入侵行为，防火墙是无法发觉的，因为对于防火墙来说，该入侵行为的访问过程和正常的WEB访问是相似的，唯一区别是入侵访问在请求链接中多加了一个后缀。  
　　(4) 只要有程序，就可能存在BUG。甚至连安全工具本身也可能存在安全的漏洞。几乎每天都有新的BUG被发现和公布出来，程序设计者在修改已知的BUG的同时又可能使它产生了新的BUG。系统的BUG经常被黑客利用，而且这种攻击通常不会产生日志，几乎无据可查。比如说现在很多程序都存在内存溢出的BUG，现有的安全工具对于利用这些BUG的攻击几乎无法防范。  
　　(5) 黑客的攻击手段在不断地更新，几乎每天都有不同系统安全问题出现。然而安全工具的更新速度太慢，绝大多数情况需要人为的参与才能发现以前未知的安全问题，这就使得它们对新出现的安全问题总是反应太慢。当安全工具刚发现并努力更正某方面的安全问题时，其他的安全问题又出现了。因此，黑客总是可以使用先进的、安全工具不知道的手段进行攻击。  
对于以上提到的问题，很多组织正在致力于提出更多的更强大的主动策略和方案来增强网络的安全性，然而另一个更为有效的解决途径就是入侵检测。在入侵检测之前，大量的安全机制都是根据从主观的角度设计的,他们没有根据网络攻击的具体行为来决定安全对策，因此，它们对入侵行为的反应非常迟钝，很难发现未知的攻击行为，不能根据网络行为的变化来及时地调整系统的安全策略。而入侵检测正是根据网络攻击行为而进行设计的，它不仅能够发现已知入侵行为，而且有能力发现未知的入侵行为，并可以通过学习和分析入侵手段，及时地调整系统策略以加强系统的安全性。  
1.2什么是入侵检测  
　　入侵检测是对传统安全产品的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息，并分析这些信息，看看网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。这些都通过它执行以下任务来实现：  
　　　◆ 监视、分析用户及系统活动；  
　　　◆ 系统构造和弱点的审计；  
　　　◆ 识别反映已知进攻的活动模式并向相关人士报警；  
　　　◆ 异常行为模式的统计分析；  
　　　◆ 评估重要系统和数据文件的完整性；  
　　　◆ 操作系统的审计跟踪管理，并识别用户违反安全策略的行为。  
　　对一个成功的入侵检测系统来讲，它不但可使系统管理员时刻了解网络系统（包括程序、文件和硬件设备等）的任何变更，还能给网络安全策略的制订提供指南。更为重要的一点是，它应该管理、配置简单，从而使非专业人员非常容易地获得网络安全。而且，入侵检测的规模还应根据网络威胁、系统构造和安全需求的改变而改变。入侵检测系统在发现入侵后，会及时作出响应，包括切断网络连接、记录事件和报警等。  
2.入侵检测技术简介  
2.1入侵检测系统功能构成　　  
一个入侵检测系统的功能结构如图一所示，它至少包含事件提取、入侵分析、入侵响应和远程管理四部分功能。  
  
事件提取功能负责提取与被保护系统相关的运行数据或记录，并负责对数据进行简单的过滤。  
入侵分析的任务就是在提取到的运行数据中找出入侵的痕迹，将授权的正常访问行为和非授权的不正常访问行为区分开，分析出入侵行为并对入侵者进行定位。  
入侵响应功能在分析出入侵行为后被触发，根据入侵行为产生响应。  
由于单个入侵检测系统的检测能力和检测范围的限制，入侵检测系统一般采用分布监视集中管理的结构，多个检测单元运行于网络中的各个网段或系统上，通过远程管理功能在一台管理站点上实现统一的管理和监控。  
  
2.2入侵检测系统分类  
　　入侵检测系统根据其检测数据来源分为两类[7]：基于主机的入侵检测系统和基于网络的入侵检测系统。基于主机的入侵检测系统从单个主机上提取数据（如审计记录等）作为入侵分析的数据源，而基于网络的入侵检测系统从网络上提取数据（如网络链路层的数据帧）作为入侵分析的数据源。通常来说基于主机的入侵检测系统只能检测单个主机系统，而基于网络的入侵检测系统可以对本网段的多个主机系统进行检测，多个分布于不同网段上的基于网络的入侵检测系统可以协同工作以提供更强的入侵检测能力。  
2.2.1基于主机的入侵检测系统  
　　基于主机的入侵检测系统将检测模块驻留在被保护系统上，通过提取被保护系统的运行数据并进行入侵分析来实现入侵检测的功能。  
　　基于主机的入侵检测系统可以有若干种实现方法：  
　　检测系统设置以发现不正当的系统设置和系统设置的不正当更改。例如COPS（Computer Oracle and Password System）系统。  
　　对系统安全状态进行定期检查以发现不正常的安全状态，例如Tripwire系统。  
　　通过替换服务器程序，在服务器程序与远程用户之间增加一个中间层，在该中间层中实现跟踪和记录远程用户的请求和操作。例如TCPwrapper。  
　　基于主机日志的安全审计，通过分析主机日志来发现入侵行为。  
基于主机的入侵检测系统具有检测效率高，分析代价小，分析速度快的特点，能够迅速并准确地定位入侵者，并可以结合操作系统和应用程序的行为特征对入侵进行进一步分析。目前很多是基于主机日志分析的入侵检测系统。基于主机的入侵检测系统存在的问题是: 首先它在一定程度上依赖于系统的可靠性，它要求系统本身应该具备基本的安全功能并具有合理的设置，然后才能提取入侵信息；即使进行了正确的设置，对操作系统熟悉的攻击者仍然有可能在入侵行为完成后及时地将系统日志抹去，从而不被发觉；并且主机的日志能够提供的信息有限，**有的入侵手段和途径不会在日志中有所反映，日志系统对有的入侵行为不能作出正确的响应，例如利用网络协议栈的漏洞进行的攻击，通过ping命令发送大数据包，造成系统协议栈溢出而死机，或是利用ARP欺骗来伪装成其他主机进行通信，这些手段都不会被高层的日志记录下来。**在数据提取的实时性、充分性、可靠性方面基于主机日志的入侵检测系统不如基于网络的入侵检测系统。  
2.2.2基于网络的入侵检测系统  
　　基于网络的入侵检测系统通过网络监视来实现数据提取。在Internet中，局域网普遍采用IEEE 802.3协议。该协议定义主机进行数据传输时采用子网广播的方式，任何一台主机发送的数据包，都会在所经过的子网中进行广播，也就是说，任何一台主机接收和发送的数据都可以被同一子网内的其他主机接收。在正常设置下，主机的网卡对每一个到达的数据包进行过滤，只将目的地址是本机的或广播地址的数据包放入接收缓冲区，而将其他数据包丢弃，因此，正常情况下网络上的主机表现为只关心与本机有关的数据包，但是将网卡的接收模式进行适当的设置后就可以改变网卡的过滤策略，使网卡能够接收经过本网段的所有数据包，无论这些数据包的目的地是否是该主机。网卡的这种接收模式被称为混杂模式，目前绝大部分网卡都提供这种设置，因此，在需要的时候，对网卡进行合理的设置就能获得经过本网段的所有通信信息，从而实现网络监视的功能。在其他网络环境下，虽然可能不采用广播的方式传送报文，但目前很多路由设备或交换机都提供数据报文监视功能。  
　　网络监视具有良好的特性：理论上，网络监视可以获得所有的网络信息数据，只要时间允许，可以在庞大的数据堆中提取和分析需要的数据；可以对一个子网进行检测，一个监视模块可以监视同一网段的多台主机的网络行为；不改变系统和网络的工作模式，也不影响主机性能和网络性能；处于被动接收方式，很难被入侵者发现；可以从低层开始分析，对基于协议攻击的入侵手段有较强的分析能力。网络监视的主要问题是监视数据量过于庞大并且它不能结合操作系统特征来对网络行为进行准确的判断。  
　　由于基于网络的入侵检测方式具有较强的数据提取能力，因此目前很多入侵检测系统倾向于采用基于网络的检测手段来实现。  
2.3入侵检测分析技术  
　　入侵分析的任务就是在提取到的庞大的数据中找到入侵的痕迹。入侵分析过程需要将提取到的事件与入侵检测规则进行比较，从而发现入侵行为。一方面入侵检测系统需要尽可能多地提取数据以获得足够的入侵证据，而另一方面由于入侵行为的千变万化而导致判定入侵的规则越来越复杂，为了保证入侵检测的效率和满足实时性的要求，入侵分析必须在系统的性能和检测能力之间进行权衡，合理地设计分析策略，并且可能要牺牲一部分检测能力来保证系统可靠、稳定地运行并具有较快的响应速度。  
　　分析策略是入侵分析的核心，系统检测能力很大程度上取决于分析策略。在实现上，分析策略通常定义为一些完全独立的检测规则。基于网络的入侵检测系统通常使用报文的模式匹配或模式匹配序列来定义规则，检测时将监听到的报文与模式匹配序列进行比较，根据比较的结果来判断是否有非正常的网络行为。这样以来，一个入侵行为能不能被检测出来主要就看该入侵行为的过程或其关键特征能不能映射到基于网络报文的匹配模式序列上去。有的入侵行为很容易映射，如ARP欺骗，但有的入侵行为是很难映射的，如从网络上下载病毒。对于有的入侵行为，即使理论上可以进行映射，但是在实现上是不可行的，比如说有的网络行为需要经过非常复杂的步骤或较长的过程才能表现其入侵特性，这样的行为由于具有非常庞大的模式匹配序列，需要综合大量的数据报文来进行匹配，因而在实际上是不可行的。而有的入侵行为由于需要进行多层协议分析或有较强的上下文关系，需要消耗大量的处理能力来进行检测，因而在实现上也有很大的难度。  
　　入侵分析按照其检测规则可以分为两类[2]：  
　　基于特征的检测规则。这种分析规则认为入侵行为是可以用特征代码来标识的。比如说，对于尝试帐号的入侵，虽然合法用户登录和入侵者尝试的操作过程是一样的，但返回结果是不同的，入侵者返回的是尝试失败的报文，因此，只要提取尝试失败的报文中的关键字段或位组作为特征代码，将它定义为检测规则，就可以用来检测该类入侵行为。这样，分析策略就由若干条检测规则构成，每条检测规则就是一个特征代码，通过将数据与特征代码比较的方式来发现入侵。  
　　基于统计的检测规则。这种分析规则认为入侵行为应该符合统计规律。例如，系统可以认为一次密码尝试失败并不算是入侵行为，因为的确可能是合法用户输入失误，但是如果在一分钟内有8次以上同样的操作就不可能完全是输入失误了，而可以认定是入侵行为。因此，组成分析策略的检测规则就是表示行为频度的阀值，通过检测出行　　为并统计其数量和频度就可以发现入侵。  
　　这两种检测规则各有其适用范围，不同的入侵行为可能适应于不同的规则，但就系统实现而言，由于基于统计检测规则的入侵分析需要保存更多的检测状态和上下关系而需要消耗更多的系统处理能力和资源，实现难度相对较大。  
　　近几年，为了改进入侵检测的分析技术，许多研究人员从各个方向入手，发展了一些新的分析方法，对于提高入侵检测系统的正确性、可适应性等起到了一定的推动作用。下面是几个不同的方向。  
2.3.1统计学方法  
　　统计模型常用于对异常行为的检测,在统计模型中常用的测量参数包括审计事件的数量、间隔时间、资源消耗情况等。目前提出了可用于入侵检测的5种统计模型包括：  
　　(1) 操作模型:该模型假设异常可通过测量结果与一些固定指标相比较得到,固定指标可以根据经验值或一段时间内的统计平均得到,举例来说,在短时间内的多次失败的登录很可能是口令尝试攻击。  
　　(2) 方差:计算参数的方差,设定其置信区间,当测量值超过置信区间的范围时表明有可能是异常。  
　　(3) 多元模型:操作模型的扩展,通过同时分析多个参数实现检测。  
　　(4) 马尔柯夫过程模型:将每种类型的事件定义为系统状态,用状态转移矩阵来表示状态的变化,若对应于发生事件的状态矩阵中转移概率较小,则该事件可能是异常事件。  
　　(5) 时间序列分析:将事件计数与资源耗用根据时间排成序列,如果一个新事件在该时间发生的概率较低,则该　　事件可能是入侵。  
　　入侵检测的统计分析首先计算用户会话过程的统计参数,再进行与阈值比较处理与加权处理,最终通过计算其"可疑"概率分析其为入侵事件的可能性。统计方法的最大优点是它可以"学习"用户的使用习惯,从而具有较高检出率与可用性。但是它的"学习"能力也给入侵者以机会通过逐步"训练"使入侵事件符合正常操作的统计规律,从而透过入侵检测系统。  
2.3.2入侵检测的软计算方法  
　　入侵检测的方法可有多种,针对异常入侵行为检测的策略与方法往往也不是固定的,智能计算技术在入侵检测中的应用将大大提高检测的效率与准确性。所谓软计算的方法包含了神经网络、遗传算法与模糊技术。  
2.3.3基于专家系统的入侵检测方法  
　　基于专家系统的入侵检测方法与运用统计方法与神经网络对入侵进行检测的方法不同,用专家系统对入侵进行检测,经常是针对有特征的入侵行为。  
　　所谓的规则,即是知识。不同的系统与设置具有不同的规则,且规则之间往往无通用性。专家系统的建立依赖于知识库的完备性,知识库的完备性又取决于审计记录的完备性与实时性。特征入侵的特征抽取与表达,是入侵检测专家系统的关键。将有关入侵的知识转化为if-then结构(也可以是复合结构),if部分为入侵特征,then部分是系统防范措施。  
　　运用专家系统防范有特征入侵行为的有效性完全取决于专家系统知识库的完备性,建立一个完备的知识库对于一个大型网络系统往往是不可能的,且如何根据审计记录中的事件,提取状态行为与语言环境也是较困难的。例如,ISS公司为了建立比较完备的专家系统,一方面与地下组织建立良好关系,并成立由许多工作人员与专家组成的X-Force组织来进行这一工作。  
　　由于专家系统的不可移植性与规则的不完备性。现已不宜单独用于入侵检测,或单独形成商品软件。较适用的方法是将专家系统与采用软计算方法技术的入侵检测系统结合在一起,构成一个以已知的入侵规则为基础,可扩展的动态入侵事件检测系统,自适应地进行特征与异常检测,实现高效的入侵检测及其防御。  
3.内外产品及研究现状  
　　入侵检测是网络安全领域中一个较新的课题。以往，网络安全工作者以主动的安全机制作为研究的重点。虽然每一种安全机制或安全策略的应用都可以使系统在某方面的安全性有较大的改善，但是网络体系结构的开放性特征和计算机软件本身固有的特性使得网络入侵仍然非常普遍，并且在目前的条件下入侵问题很难通过提出新的安全策略来彻底解决，因此，检测网络入侵行为就变得非常重要和有意义了。从90年代开始有了一些针对具体入侵行为或具体的入侵过程进行的入侵检测的研究和系统，94年以后逐渐出现一些入侵检测的产品，其中比较有代表性 的产品有ISS（Internet Security System）公司的RealSecure，NAI(Network Associates,Inc)公司的Cybercop和Cisco公司的NetRanger。现在入侵检测系统已经成为网络安全中一个重要的研究方向而越来越受到重视。  
　　目前的入侵检测系统大部分是基于各自的需求和设计独立开发的，不同系统之间缺乏互操作性和互用性，这对入侵检测系统的发展造成了障碍，因此DARPA（the Defense Advanced Research Projects Agency,美国国防部高级研究计划局）在1997年3月开始着手CIDF(Common Intrusion Detection Framework，公共入侵检测框架)标准的制定。现在加州大学Davis 分校的安全实验室已经完成CIDF标准[9]，IETF（Internet Engineering Task Force, Internet工程任务组）成立了IDWG(Intrusion Detection Working Group，入侵检测工作组)负责建立IDEF[10]（Intrusion Detection Exchange Format，入侵检测数据交换格式）标准，并提供支持该标准的工具，以更高效率地开发IDS系统（Intrusion Detection System,入侵检测系统）。  
　　国内在这方面的研究刚开始起步，目前也已经开始着手入侵检测标准IDF（Intrusion Detection Framework，入侵检测框架）的研究与制定。  
4.入侵检测技术的发展方向  
　　可以看到,在入侵检测技术发展的同时,入侵技术也在更新,一些地下组织已经将如何绕过IDS或攻击IDS系统作为研究重点。高速网络,尤其是交换技术的发展以及通过加密信道的数据通信,使得通过共享网段侦听的网络数据采集方法显得不足,而大量的通信量对数据分析也提出了新的要求。随着信息系统对一个国家的社会生产与国民经济的影响越来越重要,信息战已逐步被各个国家重视,信息战中的主要攻击"武器"之一就是网络的入侵技术,信息战的防御主要包括"保护"、"检测"与"响应",入侵检测则是其中"检测"与"响应"环节不可缺少的部分。  
近年对入侵检测技术有几个主要发展方向:  
(1) 分布式入侵检测与通用入侵检测架构  
　　传统的IDS一般局限于单一的主机或网络架构,对异构系统及大规模的网络的监测明显不足。同时不同的IDS系统之间不能协同工作能力,为解决这一问题,需要分布式入侵检测技术与通用入侵检测架构。CIDF以构建通用的IDS体系结构与通信系统为目标,GrIDS跟踪与分析分布系统入侵,EMER-ALD实现在大规模的网络与复杂环境中的入侵检测。  
(2) 应用层入侵检测  
　　许多入侵的语义只有在应用层才能理解,而目前的IDS仅能检测如WEB之类的通用协议,而不能处理如LotusNotes、数据库系统等其他的应用系统。许多基于客户、服务器结构与中间件技术及对象技术的大型应用,需要应用层的入侵检测保护。Stillerman等人已经开始对CORBA的IDS研究。  
(3) 智能的入侵检测  
　　入侵方法越来越多样化与综合化,尽管已经有智能体、神经网络与遗传算法在入侵检测领域应用研究,但是这只是一些尝试性的研究工作,需要对智能化的IDS加以进一步的研究以解决其自学习与自适应能力。  
(4) 入侵检测的评测方法  
　　用户需对众多的IDS系统进行评价,评价指标包括IDS检测范围、系统资源占用、IDS系统自身的可靠性与鲁棒性。从而设计通用的入侵检测测试与评估方法与平台,实现对多种IDS系统的检测已成为当前IDS的另一重要研究与发展领域。  
(5) 网络安全技术相结合  
　　结合防火墙、PKIX、安全电子交易SET等新的网络安全与电子商务技术,提供完整的网络安全保障。  
总结  
　　入侵检测作为一种积极主动地安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。从网络安全立体纵深、多层次防御的角度出发，入侵检测理应受到人们的高度重视，这从国外入侵检测产品市场的蓬勃发展就可以看出。在国内，随着上网的关键部门、关键业务越来越多，迫切需要具有自主版权的入侵检测产品。但现状是入侵检测仅仅停留在研究和实验样品（缺乏升级和服务）阶段，或者是防火墙中集成较为初级的入侵检测模块。可见，入侵检测产品仍具有较大的发展空间，从技术途径来讲，我们认为，除了完善常规的、传统的技术（模式识别和完整性检测）外，应重点加强统计分析的相关技术研究。