绿盟+ SECURITY

2008/08 总第002

技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

本期看点 HEADLINES

主办：绿盟科技
策划：绿盟内刊编委会
地址：北京市海淀区北洼路4号益泰大厦三层
邮编：100089
电话：(010)6843 8880-8661
传真：(010)6872 8708
网址：www.nsfocus.com

Nsmagazine@nsfocus.com

2008/08 总第 002

绿盟+
NSFOCUS

目录 CONTENTS

NSFOCUS 2008 年 07 月之十大安全漏洞

声明：本十大安全漏洞由NSFOCUS**（绿盟科技）安全小组 <**security@nsfocus.com**>根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出，仅供参考。**

1．多家厂商 DNS 实现缓存中毒漏洞

NSFOCUS ID: 12124

http://www.nsfocus.net/vulndb/12124

综述：

DNS协议是TCP/IP协议组的一部分，允许 DNS 客户端查询 DNS 数据库将主机名解析为 IP 地址。

DNS 协议实现规范中包括一个 16 位的事件ID。由于协议实现中的弱点，用于验证 DNS 响应事件的 ID 和源端口号随机性不够强，可以轻易的预测，这就允许攻击者创建匹配期望值的 DNS 请求伪造响应，而 DNS 服务器会认为该响应有效，因此简化了缓存中毒攻击。

危害：

远程攻击者可能利用该漏洞对DNS服务器的用户进行欺骗，进而进行拒绝服务攻击、网络钓鱼和金融欺骗。

2．7 月紧急补丁更新修复多个漏洞

NSFOCUS ID: 12137

http://www.nsfocus.net/vulndb/12137

综述：

Oracle Database 是一款商业性质大型数据库系统。

Oracle发布了2008年7月的紧急补丁更新公告，修复了多个Oracle产品中的多个漏洞。这些漏洞影响Oracle产品的所有安全属性，可导致本地和远程的威胁。包括：

1.WWV_RENDER_REPORT软件包存在PLSQL 注入漏洞。

2.Linux和Linux平台的一个set-uid程序中存在安全漏洞。

3.Internet Directory 服务进程在处理畸形的LDAP 请求时的空指针引用。

4.DBMS_AQELM软件包的缓冲区溢出漏洞。

危害：

远程攻击者可能利用这些漏洞进行拒绝服务，获取敏感信息甚至完全控制服务器。

3. 新浪 DLoader Class ActiveX 控件 DonwloadAndInstall 方式任意文件下载漏洞

NSFOCUS ID: 12147

http://www.nsfocus.net/vulndb/12147

综述：

新浪UC是融合了P2P思想的开放式即时通讯和娱乐平台。

新浪UC客户端所安装的DLoader Class ActiveX 控件没有正确地验证对 Donw-

loadAndInstall方式的输入，如果用户受骗访问了恶意网页并向该方式传送了畸形参数，就会导致向用户系统的任意位置下载文件。目前已有蜜罐网络检测到该漏洞正在被积极的利用。

危害：

远程攻击者可能利用该漏洞以浏览者身份执行任意指令。

4. Microsoft SQL Server 信息泄露及缓冲区溢出漏洞（MS08-040）

NSFOCUS ID: 12128

http://www.nsfocus.net/vulndb/12128

综述：

Microsoft SQL Server 是一款流行的SQL 数据库系统。

SQL Server管理内存页面重用的方式存在漏洞，重新分配内存时，未能初始化内存页面。具有数据库操作员权限并成功利用此漏洞的攻击者可以访问客户数据。

SQL Server中的转换功能没有充分地检查输入字符串，在处理 INSERT 语句前没有执行充分的检查。通过认证的攻击者可以利用这些漏洞触发缓冲区溢出，从而执行任意指令。

危害：

远程攻击者可能利用该漏洞获取敏感信息甚至执行任意指令。

5．Sun Java JDK/JRE 多个远程安全漏洞

NSFOCUS ID: 12135

http://www.nsfocus.net/vulndb/12135

综述：

Solaris 系统的 Java 运行时环境（JRE）为JAVA 应用程序提供可靠的运行环境。

Sun Java 在处理 applet、JMX 客户端、JWS、XML 时存在多个安全漏洞，可能允许恶意用户绕过某些安全限制、泄露系统信息、导致拒绝服务或完全入侵有漏洞的系统。

危害：

远程攻击者可能利用这些漏洞以浏览者身份执行任意指令。

6．Windows 资源管理器保存搜索文件远程代码执行漏洞（MS08-038）

NSFOCUS ID: 12118

http://www.nsfocus.net/vulndb/12118

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。

Windows资源管理器没有正确地解析保存搜索（.search-ms）文件。如果用户受骗打开并保存了特制的.search-ms 文件的话，Windows资源管理器就会退出并以可利用的方式重新启动，导致在用户系统上执行任意指令。

危害：

远程攻击者可能利用该漏洞以浏览者身份执行任意指令。

7. Microsoft Access 快照查看器 ActiveX 控件任意文件下载漏洞

NSFOCUS ID: 12108

http://www.nsfocus.net/vulndb/12108

综述：

Microsoft Access 是微软 Office 套件中的关系数据库管理系统。

Microsoft Access 中捆绑了快照查看器 ActiveX 控件用于方便的查看Access报表快照，该控件没有正确的验证某些输入参数。如果用户受骗访问了恶意站点的话，就可能导致将站点上的文件下载到用户机器的任意位置。目前这个漏洞正在被积极的利用。

危害：

远程攻击者可能利用该漏洞以浏览者身份执行任意指令。

8. Firefox CSSValue 数组数据结构远程代码执行漏洞

NSFOCUS ID: 12146

http://www.nsfocus.net/vulndb/12146

综述：

Firefox 是一款流行的开源WEB 浏览器。

Mozilla的内部CSSValue数组数据结构对 CSS 对象的引用计数器使用了过小的变量，如果攻击者对常见的CSS对象创建了大量引用，当浏览器试图释放仍在使用的CSS对象时计数器会被溢出，导致拒绝服务或在用户机器上执行任意指令。

危害：

远程攻击者可能利用该漏洞以浏览者身份执行任意指令。

9. Mozilla Firefox URI 拆分绕过安全限制漏洞

NSFOCUS ID: 12140

http://www.nsfocus.net/vulndb/12140

综述：

Firefox 是流行的开源 WEB 浏览器。

Firefox可以处理来自用户或程序可访问的命令行接口的URI，如果使用管道符号通过命令行接口向Firefox传送了多个URI，就会在启动Firefox 时在标签页中打开了URI。攻击者可以利用这个漏洞向Firefox传送应由其他应用所处理的URI。由于Firefox 可能认为发送的URI 来自于本地内容来源，因此远程内容可以绕过基于来源的安全限制。

危害：

远程攻击者可能利用该漏洞绕过某些安全限制。

10. Linux Kernel sys32_ptrace() 函数多个释放后使用漏洞

NSFOCUS ID: 12129

http://www.nsfocus.net/vulndb/12129

综述：

Linux Kernel 是开放源码操作系统 Linux 所使用的内核。

Linux Kernel 的 arch/x86/kernel/ptrace.c 文件中的 sys32_ptrace()函数可能会溢出 task_struct结构的refcount字段，本地攻击者可以在x86-64 平台上利用这个漏洞触发释放后使用，导致系统崩溃。

危害：

本地攻击者可能利用该漏洞进行拒绝服务攻击。

绿盟科技紧急通告(Alert2008-04)

新型自动化 SQL 注入攻击引发大规模网页挂马

发布日期:2008-06-04

综述:

2008年5月14日，绿盟科技客户服务中心400热线接到某网站客户的紧急求助电话，网站页面遭到破坏，请求绿盟安全工程师现场应急。该网站遭遇网页篡改，正常网页内容被替换为大量的</i-]或</title¡-]，且持续发生“网页被篡改－手工恢复－再次被篡改－再次恢复…”的现象。经过现场工程师分析，这次攻击同绿盟近期处理的多起应急响应事件基本一致，均是由于网站遭受自动化SQL注入攻击的破坏而导致。

紧接着，来自网络世界（Network World）的报道，进入5月后，中国大陆、香港及台湾地区有数千个网站遭遇新一轮SQL注入攻击，引发大规模网站挂马等安全事件。在过去的4个月中，之前已有3次大规模攻击，受害者包括某知名防病毒软件厂商网站、欧洲某政府网站和某国际机构网站在内的多家网站。据Microsoft估算，感染页面数最多超过10，000页面/天。

分析:

经过绿盟科技NSFocus安全小组分析，该轮攻击使用Google搜索引擎定位网页中包含的动态ASP脚本，测试脚本是否存在SQL注入漏洞并确定注入点，最终试图遍历目标网站后台SQL Server数据库的所有文本字段，插入指向恶意内容的链接。攻击的整个过程完全自动化，一旦攻击得逞，这些自动插入的数据将严重破坏后台数据库所存储的数据，动态脚本在处理数据库中的数据时可能出错，各级页面不再具有正常的观感。被攻击站点也可能成为恶意软件的分发点，访问这些网站的网民可能遭受恶意代码的侵袭，用户的系统被植入木马程序从而完全为攻击者控制。

攻击对象主要为运行IIS Web Server的ASP站点，其后台数据库使用微软SQL Server。由于配置错误，网站底层SQL Server使能了最为危险的存储过程之一“xp_cmdshell”，使得攻击者可以在Web服务器端执行操作系统命令。

详尽分析及解决方法，请参看绿盟网站
http://www.nsfocus.net/index.php?act=alert

绿盟科技紧急通告(Alert2008-04)

微软发布6月份安全公告　修复多个严重安全漏洞

发布日期:2008-06-11

综述:

微软发布了6月份的7篇安全公告，这些公告描述并修复了10个安全漏洞，其中4个漏洞属于“紧急”风险级别。攻击者利用这些漏洞可能远程入侵并完全控制客户端系统。

我们强烈建议使用Windows操作系统的用户立刻检查一下您的系统是否受此漏洞影响，并按照我们提供的解决方法予以解决。

分析:

微软发布了6月份的7篇最新的安全公告:MS08-030到MS08-036。这些安全公告分别描述了10个安全问题，分别是有关Windows操作系统、IE浏览器和DirectX中的漏洞。

1. MS08-030—**蓝牙栈中的漏洞可能允许远程执行代码(**951376**)**

2. MS08-031—Internet Explorer **累积安全更新(**950759**)**

3. MS08-032—ActiveX Kill Bit **累积安全更新(**950760**)**

4. MS08-033—DirectX **中的漏洞可能允许远程执行代码(**951698**)**

5. MS08-034—WINS **中的漏洞可能允许权限提升(**948745**)**

6. MS08-035—**活动目录中的漏洞可能导致拒绝服务(**953235**)**

7. MS08-036—**实际通用多播(**PGM**)中的漏洞可能导致拒绝服务(**950762**)**

详尽分析及解决方法,请参看绿盟网站
http://www.nsfocus.net/index.php?act=alert

证券期货业维稳工作反思

文/徐一丁　行业技术部

维稳工作提上日程

由于业内的几起安全事件，证券期货业从今年4月底开始了对网站及相关系统的安全检查，后来扩大到了对信息系统的全面安全检查，持续进行了2个月左右。

4月29日，证监会举行了全国安全工作视频会议，传达了加强“当前形势下的维稳和信息系统安全工作”的精神。强调了“维稳工作在当前具有特殊的重要意义。发展是第一要务，维稳是第一责任”，同时指出了当前证券期货业内存在的主要安全问题，提出了“长效机制”和对近期要完成加强信息安全方面的任务部署。

5月下旬，证监会又发布了《关于开展全行业信息系统安全检查的通知》，即58号文。督促全行业各单位认真贯彻落实对行业信息安全保障工作进行的重点部署，查找突出的技术隐患并加以整改；同时要求对全行业的信息系统安全状况进行一次全面的调查和摸底，为下一步工作提供科学、准确的决策依据。

发现的问题及解决办法

绿盟科技长期为证券期货业提供专业的安全服务与产品，针对此次的维稳工作，绿盟科技在全国各地为20余家业内公司提供了渗透测试、风险评估、安全加固和相关咨询等服务。下面将工作中发现的主要问题进行简要地总结说明：

名称	说明	影响目标	危害
XSS跨站	利用网站程序对语句缺乏过滤与转换，达到脚本注入的目的	二者经常被结合在一起利用，针对Web网站、数据库系统	被非法控制 屏蔽（伪造）页面信息 执行攻击命令 拒绝服务攻击 重要信息泄露
SQL注入	对恶意代码缺乏过滤与屏蔽，形成注入点		
口令管理不当	口令强度不足 口令结构简单 口令保存方法不当 口令保质期过长	服务器 数据库 网络设备	攻击者获得各类权限
系统漏洞多补丁打不全	漏洞非常多，很多都是高危知道有漏洞，但不好修补	操作系统 应用系统 数据库 网络设备	被远程控制 病毒蠕虫传播 拒绝服务 重要信息泄露
业务网与办公网直连	办公网与业务网都连笔记本，U盘控制不严	业务系统	严重的安全隐患 办公网安全事件直接威胁业务网

如上表所示，证券公司信息系统内的主要问题，确实集中在4.29会议中提到的几个方面上，都有可能导致严重的后果。下面介绍一下相关问题的解决方法，以供大家参考

XSS及SQL注入漏洞

在编程中应注意过滤各类恶意的代码输入，在客户端输入程序与服务器端接受的程序编码时都应注意过滤；还应限制Web用户和数据库用户的访问权限。

由于网站程序代码并不容易很快更改，也可以采用临时的解决措施，利用Web应用防护设备，对上述的恶意请求进行过滤，达到从网络上防止这类攻击的目的。

口令管理不当

采用合格的系统口令，并定期更改，这里不再赘述。或者借助第三方的强认证系统，如双因素身份认证令牌或证书系统。

系统漏洞较多，补丁不全

因为证券公司网站与交易系统等直接与生产相关，因此打补丁时需要尤其注意，不可影响正常的业务。打补丁前应在相同的试验系统上事先测试，准备好备用机和备用系统，在闭市期间打补丁。注意打补丁之后马上验证，确保补丁生效，而且没有影响业务的正常运行。

在有些服务器不适合打补丁的时候，可以采取一些辅助安全手段，如网络访问控制、主机访问控制、安全配置加强和入侵检测系统等。

办公网与业务网直连

根本的解决办法肯定是将办公终端与业务终端分开，即办公终端只能访问办公网段及Internet，业务终端只能访问业务网。不过这种改进设想时简单，而马上实行起来比较困难，因为将会涉及到很多员工，会对业务运行产生较大影响。而且员工需要配置两台计算机，一台上业务网，一台上办公网，添置设备本身就是不小的投入。这方面要结合公司实际，制订改进计划。

对问题根源的反思

其实上述这些问题从技术上说都不难解决，而且证券期货业应该是最重视信息安全的行业之一，为什么安全工作做了这么多年，这些问题还是普遍存在呢？笔者认为有以下几个主要原因：

信息系统只重视业务实现，而不重视安全

这是证监会4.29会议中重点谈到的一个问题，也是当前很多问题的根源。“重视业务实现，不重安全”的情况决定了后面的很多事情，其实不被重视的不仅仅是安全，而是业务系统建设的总体均衡。

很多证券公司在上业务系统的时候，尤其在近两年行情好的情况下，往往为了赶行市而大干快上。假如新业务延迟一个月推出，则可能少赚千万计的钱款。这导致IT人员的计划往往不能在充足的日期段里执行，安排得非常紧。

系统开发商、集成商是下一层级的压力承受者，他们需要在最后期限之前拿出一个“能用”的系统。形同“用鞭子抽着赶着”，所以做出来的系统很容易存在着各方面的漏洞，很多还是严重的漏洞。在检查中，我们发现多个网站系统存在XSS、SQL注入等漏洞，与开发时间紧、难以保证质量的情况密切相关。

系统一旦上线，每天都必须实时处理大量查询、交易的操作，即使有闭市期间的缓冲，能进行的调整也非常受限制。因为不能影响业务，影响业务就是影响赚钱。证券公司在不断地上新业务，老的问题还没有解决，新的问题又已经出现。在业务系统必须持续运转的情况下，“积重难返”，随着系统规模越来越庞大，问题也越积越多，导致风险同样也越来越高。这是个比较根源的问题，它的影响深远，也进一步导致了后面的几个问题。

技术人员缺乏所需的知识、技能、习惯

这里不单指安全方面的知识、技能和习惯，也包括系统维护、网络维护等方面。如系统漏洞多的问题，有时候技术人员已经知道有漏洞存在，但明知有漏洞却不敢去打补丁，因为打了补丁不知道业务系统是否会受到影响，甚至对服务器是否还能正常重启都没有把握。主要原因在于他们还不完全了解自己管理的系统，没有做到了如指掌，加上责任重大，所以不是迫不得已的情况下都不会去冒险。其实不只是证券期货业，在整个金融行业，这种现象都普遍存在着。

另一方面，“技术不完全合格”也不单是指证券公司的人员，同样包括一些开发商和集成商的人员。如果编程技术合格，那么XSS、SQL注入的漏洞在很大程度上是可以消除的。又如：办公网与业务网直连这种情况，在系统集成时的架构设计上也可以避免。

从这个角度说，证券公司需要合格的技术人员，也需要技术过硬的合作伙伴来协助建立并维护系统。相关技术人员都应有丰富的经验，以满足证券公司复杂环境的需要和高标准要求。

日常安全意识不足

与知识技能相关的是意识，安全意识是保证知识技能可以发挥作用的关键。什么才是安全的口令，应当如何进行口令管理，在今天基本已经被所有的技术人员所了解，而我们在本次检查中仍然发现了很多用户名、口令过于简单，容易猜测的情况，还有很多过期账户和长期不使用的账户没有被禁止或删除。具备了必要的安全知识，还要在日常工作中切实地做出来，才能真正达到效果。

同样，安全意识并不只是信息技术人员才应具备的素质，证券公司全体人员都应意识到自己在信息系统安全中的角色和位置、自己应该如何去与公司的安全体系结合。这一点做到了，Internet上即使攻击横行、病毒泛滥，也不至于对办公网产生大的影响，更不会进一步威胁到业务网。

意识靠教育来培养，靠制度来固化。证券公司全体人员的整体动员和参与，同样是信息系统建设的长期任务之一。

证券公司业务特点限制

从客观情况看，一些问题无法有效纠正也与行业特点有很大关系，并不都是证券公司的主观问题。

信息安全的基础目标是“完整性、可用性、保密性”，在各个行业都有不同的侧重。如政府、涉密、制造等行业特别重视保密性；电信运营商最重视可用性。金融行业信息系统的安全直接关系到钱财，在这方面要求最高，要求每一个目标都要不折不扣地做到。

证券公司是金融行业里对信息系统依赖和要求最高的。投资者的心情随着近两年行情几起几落，证券公司信息系统的安全稳定运行直接关系到国家和社会稳定的大局。简言之：“信息系统绝不能再出事了”。事件使证券公司从高层领导到基层技术人员都承担了很大的压力，因此在处理安全问题时采取保守求稳的策略也是可以理解的。

行业的特点无法改变，证券公司应当在这种特定条件下找出适合自己的安全管理办法，满足不断变化的信息系统安全保障需要。

建立信息系统安全长效机制

上图是根据证监会4.29精神，绿盟科技在5月初为证券公司客户设计的工作步骤。目前第一阶段已经进行完毕，证券公司需要在已经全面加强系统的基础上，制订维护保障规范和应急预案，做好奥运保障工作。

紧张的奥运保障之后，信息系统建设会有一段相对平缓的时间，证券公司可以抓住这个时机进行规划设计，然后在后面几年内逐步推行，以达到建立适合自己的信息安全长效机制。但需要注意的是，IT建设与安全规划并不是一件简单易行的事情，即使是经验丰富的专家也不可能通过一次交流和会谈就能为证券公司设计出合理的规划，这需要对证券公司的多次研讨、调研，最好是做一次全面的安全现状评估。接下来，在今后几年的执行过程中要注意不断地检查，去修正可能存在的偏差，同时适应信息系统的变化。这样建立的信息系统，才可以确保安全和稳定地运行，真正成为证券公司长远发展的基础。

探寻下一代安全网关

文/崔云鹏　产品市场部

安全网关正面临日益严重的挑战

对于从事网络安全建设的人来说，安全网关几乎是我们第一个需要接触的安全产品，它可以说是网络防护的第一道防线。经过多年的发展，安全网关更已经是技术成熟、功能稳定的代名词，大量应用于各种网络环境中。但是，安全问题无止境，我们先看一看下面的数据：

1.国家工业和信息化部公布，截至2008年2月，我国网民数达2.21亿人，超过美国居全球首位；

2.CNCERT CC抽样计算，2007年我国大陆地区被植入木马的主机IP数995154，是2006年的22倍；

3.2007年全世界感染僵尸程序的主机数达623万个，其中我国大陆有362万个，占据了一半以上；

4.2007年中国大陆被篡改网站的数量达到61228个，比2006年增长1.5倍；

5.当前攻击统计中，90%以上利用了WEB、电子邮件、P2P和IM协议进行传播和泄密。

网络用户的安全防护不到位，恶意攻击者数量在增加，攻击手段呈现多样化，使得安全网关正面对日益严峻的挑战。很多攻击利用了网络应用做掩护，例如隐藏在HTTP 80端口，甚至隐藏在无固定端口号的P2P协议中，这使得传统安全网关对此根本无能为力。

安全网关发展的历史

什么是安全网关，它是指设置在不同网络或网络安全域之间的一系列部件的组合的统称。它可通过监测、限制、更改跨越安全网关的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，并通过检测阻断威胁，以及采取网络数据加密等手段来实现网络和信息的安全。

安全网关按照功能和用途划分，可以分为防火墙、VPN网关、UTM、IPS、防病毒网关、防垃圾邮件网关、抗DDoS网关等各种类型。其中最早出现，也是最主要的安全网关类型就是防火墙。

追溯安全网关的早期历史，其实就是防火墙的历史，最早的防火墙安全网关出现在20世纪80年代初，当时的采用简单包过滤技术（Packet filter）的路由器，由于具有了简单的安全功能，成为了世界上最早的防火墙，也是现在安全网关的雏形。

但是在防火墙出现之后的十几年里，由于网络以及网络安全对于大众来说还略显遥远，尽管在实验室或者军事上，网络防火墙有了一些技术进展，但相对于高速发展的IT行业来说，网络防火墙的发展缓慢了很多。伴随互联网的普及，在中国20世纪90年代中后期以来，网络越来越成为人们生活的一部分，随之而来，网络的安全性成为越来越重要的问题，网络防火墙开始普遍地走进中国IT人的视野里，防火墙也进入了发展的黄金时期。

这个时期的防火墙，其实更像一个内置了安全功能的多网卡服务器，硬件一般是采用x86 CPU做核心处理器；软件功能则在包过滤技术和应用代理技术的基础上，采用了状态检测技术。防火墙一个里程碑式的技术就是在防火墙内，对通过的TCP/IP协议的连接状态进行记录监控，在不同安全区域之间的访问，根据防火墙安全策略进行阻断或者放行，从而实现一种高效转发、应用无关的安

全防护，这对防火墙的普及化起到了很大的作用。

随着防火墙技术的日益成熟和更多的安全威胁出现，安全网关从单一的防火墙开始分化成各种各样的形态，以单一功能为主的如WEB防护防火墙、抗DDoS安全网关、VPN网关，以功能综合为代表的则是UTM（UnifiedThreatManagement）统一威胁管理系统。

安全网关发展趋势和存在的问题

近年来，伴随着网络及时、快速的发展，安全网关市场竞争明显加剧，安全厂商也开始做不同的尝试。目标是试图突破安全网关的技术瓶颈，主要集中在两个焦点上：硬件构架之争、安全网关胖瘦之分。

硬件构架之争，其本质是安全网关核心处理芯片的选择。现在主要有三类处理芯片：X86 CPU、ASIC、NP。传统安全网关大多采用X86 CPU作为安全网关功能的处理芯片，CPU完成了数据转发、状态检测、应用深度分析一系列工作；ASIC则是专用处理芯片，在硬件芯片中，利用逻辑实现网络数据的快速处理；NP网络处理器，则是专用的网络处理器，一般内部有多个网络引擎，指令上经过专门优化，从而实现对网络数据的快速转发。

但是三种硬件构架的芯片都面临着自己的难题，X86计算能力较强，可以做任何安全网关的功能，但是其网络转发算法没有任何特殊优化，而且设计上经常受PCI总线带宽的限制，很容易在高端网络遇到性能瓶颈；NP和ASIC安全网关类似，都是为解决安全网关性能瓶颈所出现的，但是无论是ASIC的硬件逻辑，还是NP的微码引擎，都是专注于网络IP层的数据转发，受制于计算能力，在对应用协议处理、报文深度分析上，则显出不足。

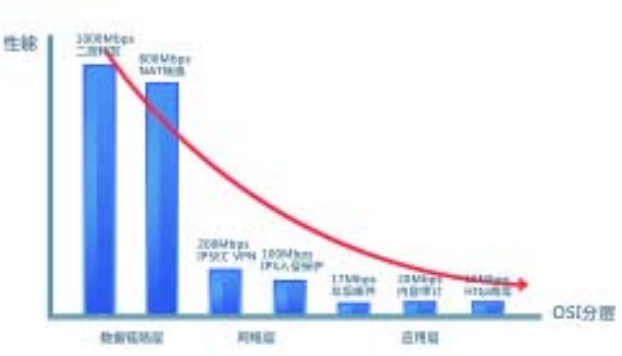


图1 ASIC/NP安全网关应用防护性能下降

安全网关胖瘦之分，则来自于UTM（Unified Threat Management）统一威胁管理概念提出，在UTM安全网关里面，除了传统防火墙的状态检测、访问控制、VPN等功能，还将防病毒、防垃圾邮件、IPS、网页过滤等众多的安全功能集中于此，这就是胖安全网关，它很好的解决了网络安全威胁多样性的问题，在一个网关处，统一解决各种安全攻击，从而使用户节省投资并且可以实现多种安全策略的统一协调。

另一类观点则支持瘦安全网关，即在安全网关上，不应有过多功能。因为多而不精，对于一些小型安全厂商来说，其技术实力无法面

面俱到，将各个功能都充分做好，这使得很多技术实力不足小厂商的UTM产品都会有功能短板；其二是性能问题，UTM使用时在应用级防护—如防病毒、IPS出现巨大的性能下降，使得UTM打上了性能不足的标签。

什么是下一代安全网关

毫无疑问，近些年来这些安全网关的技术变化，虽然有其不足之处，但还是对现在安全问题的定向反映，有其合理之处。对于未来安全网关的发展方向，可以从未来需求趋势做一下探讨。笔者认为未来网络将会从以“路由器为核心”的转发型网络，向以“服务和数据为核心”的应用网络转变，因此未来网络攻击会有一些明显的需求特征：

1.传统4层防火墙的普遍应用，使得攻击技术会转而面向传统安全网关的盲区—应用安全，针对某些应用的专项攻击、或者利用某些应用作为攻击通道将会成为主流；

2.视频、语音等大数据业务会决定网络带宽继续扩大，对安全网关转发性能的需求是持续的；

3.电子商务、网上银行、投资理财、虚拟交易等应用会使网络攻击更加具有吸引力，攻击频率会加大，攻击方式也会多样化；

4.传统局域网内网的扩大和复杂，使得网络内部受到攻击和泄密更加的严重。

因此，下一代安全网关NGSG（Next Generation Security Gateway），应该面向这些网络威胁新趋势，专注于应用层防护的高性能安全网关，它具有一系列特点，以适应未来3～5年的网络威胁防护发展趋势。

NGSG应该专注应用安全

应用安全防护是未来NGSG的重中之重，对应用安全的防护好坏决定了NGSG能否真正解决安全实际问题。针对WEB服务、电子邮件、数据服务器、电子商务、VoIP和视频会议的抗DDoS攻击、P2P的监控、IM的监控，内容审计都会是未来应用安全防护的重点。相对于TCP/IP协议的整齐划一，应用协议最大特点是应用协议多样性、多变性，例如Smart Tunnel技术，使得很多P2P软件具有变端口能力，一般安全网关的协议端口判断根本无法检测到这类P2P软件。

图2 NGSG智能协议识别

当然，新一代专注应用安全网关不会是传统的应用代理防火墙，应用代理技术有着无法解决的性能问题和应用协议过于单一的问题。

NGSG的应用防护技术的基础应该是高准确率的应用协议识别技术—例如智能协议识别技术，不依赖于端口或者某些协议特征，而且具备更强的行为关联分析能力，从而可以对应用级安全威胁做到准确灵活的判断，并为应用级防护阻断做好准备。

NGSG应该是多核构架为主的高性能网关

硬件构架是为功能服务的，NGSG选择了多核，其根本原因还是因为NGSG要承担应用级防护重任。高性能处理芯片ASIC和NP受制于应用协议计算能力不足，很多ASIC和NP构架的安全网关通常还会内置一颗X86 CPU做辅助，对于防病毒、IPS等应用协议防护的计算还是需要X86完成，这大大降低了ASIC或者NP作为未来主流安全网关芯片的可能性。

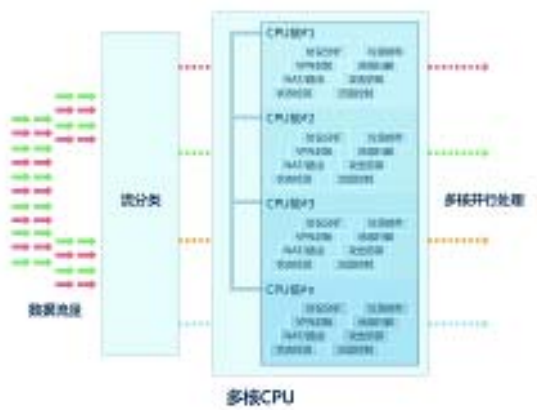


图3 多核CPU并行处理技术

CPU的多核技术是X86 CPU的一次重大变化，它使得在CPU频率无法继续大幅提升的情况下，利用并行计算，使性能再次有了提高。从原理上看，多核CPU很像NP处理器，一颗CPU上集成了多个处理核心，很多多核CPU通常还会对在网络转发的指令或者机制做专门优化，但是同NP不同的是，多核CPU的计算能力依旧保持了传统X86 CPU的优势，采用并行计算处理应用级防护，并可能最终解决早期UTM的性能问题。

NGSG应该是动静防御的完美结合

在网络攻击日益复杂的今天，攻击者不断尝试着各种新型攻击手段，零日攻击普遍出现，最终用户经常没有机会为主机打补丁，或者无法经常变更防护策略。而传统安全网关防护通常是静态防护，设定固定的安全区域，对固定协议端口号进行判断，设置固定的防护规则，调整困难使得静态防御机制很难独立应对未来高速多变的网络攻防的需要。

动态防御的机制则是指NGSG应该具有可升级的防护规则，可以检测攻击动态特征，甚至发现部分未知攻击，并能主动消除防护隐患。NGSG应该同时拥有动静两种机制，既可以对一般安全问题进行静态统一防护，也可以对随时变化甚至尚未出现的威胁做出反应。

NGSG应该是网络统一防护系统的一个有机组成部分

在一个典型的局域网中，通常会有一系列安全相关的产品：安全网关、主机防病毒软件、内网主机安全软件、路由器、交换机、

IDS……。安全网关在网络防护中会占据最重要的地位，但不可能是全部。如果网络中众多安全组件只是独立的执行各自的安全任务，组件之间没有协调，无法统一防护，其实是在浪费各自的资源，而且降低安全防护的效果。

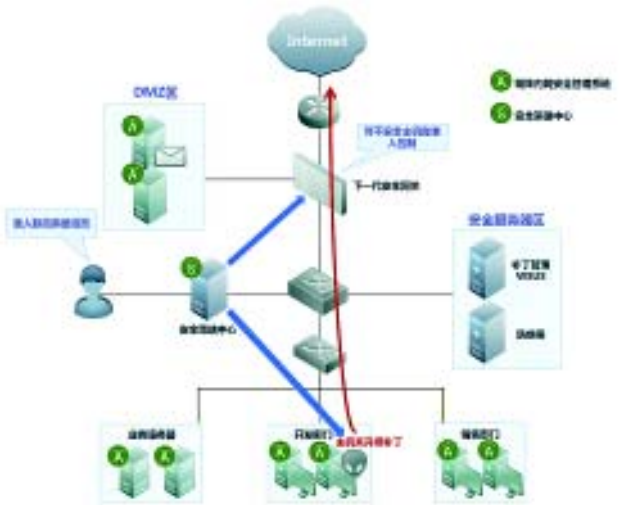


图4 多安全系统统一协作

如何同其他产品实现协同一致，实现防护策略的统一下发，多系统联动防御威胁，是在NGSG需要实现的基本功能。这可以采用统一安全管理中心，将安全策略自动分解为不同产品的设置，并且能实现多个安全产品之间的信息通信，在威胁来临的时候，对攻击做到全网联防联治。

总结

随着网络威胁的变化，很多技术领先型的安全网关厂商在NGSG下一代安全网关领域中已经有了实质性的进展。例如：很多NP、ASIC安全网关厂商开始发布基于多核处理器的高性能安全网关，WEB应用防火墙、P2P监控设备等应用安全级别的安全网关开始出现，IPS/IDS的协议识别技术的发展更是为NGSG解决了重要的安全防护技术壁垒。

可以相信，在不久的将来，一个基于多核、性能超过10G甚至数十G，并将WEB/MAIL/P2P等威胁减小到最小的NGSG将会逐渐走上安全产业大舞台的中央。

信息安全等级保护的今天和明天

文/程文静 孙铁 服务产品部

1 概述

自1994年国务院颁布的《中华人民共和国计算机信息系统安全保护条例》规定我国“计算机信息系统实行安全等级保护”以来，经过了十几年的发展，目前等级保护的组织架构、标准体系、技术体系建设已日趋成熟，随着2007年43号文的实施、等级保护大会的召开以及2008年《公安机关信息安全等级保护监督检查工作规范（试行）》的发布，标志着信息安全等级保护工作即将进入到一个新的发展阶段。

本文从等级保护政策标准现状、等级保护发展状况、等级保护发展趋势等内容简单介绍等级保护的今天和明天，为各行业信息系统主管单位和负责人增进对等级保护了解、指导等级保护建设提供借鉴。

2 等级保护政策标准现状

对信息系统实行等级保护是国家法定制度和基本国策，是国家意志在信息安全中的体现。因此这项工作的发展是以各个时期国家发布的政策标准作为标志的。

2.1 政策现状

目前在等级保护方面国家发布的主要政策有：

1994年2月	《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）
2003年7月	《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号文件）
2004年9月	发布《关于信息安全等级保护工作的实施意见》（公通字［2004］66号）
2007年6月	公安部、保密局、国密局、国信办联合印发《信息安全等级保护管理办法》（公通字［2007］43号）
2007年7月	《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861号）
2008年	《公安机关信息安全等级保护检查工作规范（试行）》

147号令中规定，“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。第一次提出信息系统要实行等级保护，并确定了等级保护的职责单位。

2003年《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）的出台明确提出了 “要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。

此后，2004年9月公安部、国家保密局、国家密码管理局、国务院信息办联合印发了《关于信息安全等级保护工作的实施意见》（公通字[2004]66号），指出 “信息安全等级保护是保障和促进信息化建设健康发展的一项基本制度”；2007年6月四部委联合出台了《信息安全等级保护管理办法》（公通字[2007]43号），明确了信息安全等级保护制度的基本内容、流程及工作要求，明确了信息系统运营使用单位和主管部门、监管部门在信息安全等级保护工作中的职责、任务；2007年7月，四部委又联合下发了《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861号），就定级范围、定级工作主要内容、定级工作要求等事项进行了通知。

43号文与861号文的出台，标志着信息安全等级保护工作在全国范围内进入到开展与实施阶段。

2008年公安部又颁布了《公安机关信息安全等级保护检查工作规范(试行)》，规范了公安机关对等级保护工作的检查。

2.2 标准现状

为保障全面实施信息安全等级保护制度，经公安部会同有关部门组织专家制定了包括《计算机信息系统安全保护等级划分准则》(GB17859-1999)、《信息系统安全等级保护定级指南》、《信息系统安全等级保护基本要求》、《信息系统安全等级保护实施指南》、《信息系统安全等级保护测评要求》等国家标准和技术指导文件，初步形成了信息安全等级保护标准体系，基本能够满足国家信息安全等级保护制度全面实施的需求。

3 等级保护发展状况

目前等级保护工作发展状况主要集中在以下几个方面：

3.1 定级工作完成

2007年7月20日“全国重要信息系统安全等级保护定级工作电视电话会议”召开之后，电信、广电、民航、铁路、税务、海关、银行、电力、证券、保险等国家重要信息系统的运营使用单位及其主管部门认真组织积极落实等级保护工作，目前基本完成了全国重要信息系统的定级工作任务。

重要信息系统定级工作的顺利完成，使国家对重要信息系统的分布有了比较明确的认识，有利于在等级保护建设和管理中提供系统性、针对性、可行性的指导和服务，有利于在信息化建设过程中同步建设信息安全设施，保障信息安全与信息化建设相协调。

3.2 行业等级保护

随着等级保护工作的不断深入和开展，围绕着国家颁布的文件和标准，各重点行业也加强了对等级保护工作的研究力度，颁布了一些行业文件和标准。

比较典型的有，原信息产业部2008年1月29日，下发了《电信网和互联网安全防护管理指南》等32项通信行业标准，其中等级保护作为其中重要一部分内容。整个体系分为三层，第一层为整个安全防护体系的总体指导性规范，明确了对电信网和互联网安全防护的定义、目标、原则，并说明了安全防护体系中的角色划分以及体系组成。第二层从宏观的角度明确了如何进行安全防护工作，规范了安全防护体系中安全等级保护、安全风险评估、灾难备份及恢复等三部分工作的原则、流程、方法、步骤等。第三层对电信网和互联网安全防护范畴中的固定通信网、移动通信网、互联网和增值业务网安全防护工作的实施进行了具体规范，其中增值业务网包括消息网、智能网等业务平台以及业务管理平台。

在电力行业，为贯彻落实国家关于开展信息系统安全保护等级定级工作的要求，国家电网公司发布部门文件“关于印发《国家电网公司信息系统安全保护等级定级指南（试行）》等的通知(信息技术〔2007〕60号)”、国家电力监管委员会发布“关于印发《电力行业信息系统等级保护定级工作指导意见》的通知(电监信息[2007]44号)”，用于指导电力行业定级工作的开展。

3.2 行业等级保护

在等级保护服务实施中测评机构的测评报告和测评结果对等级保护实施结果具有极大影响。对于三级以上的重要信息系统来说，按照43号文要求，测评和检查每年都将进行，因此如果等级保护在全国开展起来，等级保护以及相关的测评和检查将是每年安全服务

的一个重要主题，而且测评和检查结果将是判定围绕等级保护所实施的安全建设是否合规的一个重要依据。

3.3 测评机构建立

如果等级保护建设工作在全国范围内开展起来的话，现有的测评机构数量是难以满足等级保护测评要求的。因此目前各地也在积极进行测评机构的建设工作，以满足本地区等级保护的测评需求。

3.4 后续工作开展

在定级备案工作完成后，各单位将开展后续的系统安全建设、等级测评、监督检查。

目前，各个行业完成定级工作后，正在积极准备进行安全建设和整改，也就是按照相关的管理规范和技术标准，以自身安全需求为出发点，进行等级保护的规划和设计，使用符合国家有关规定、满足信息系统安全保护等级需求的信息技术产品，进行信息系统安全建设或者改建工作，完成等级保护工作的基线安全建设。

定级后的建设整改可以有两个流程：一个是定级后进行等级建设，然后引入第三方测评，根据整改建议进行整改；另一个流程是定级完成后直接引入第三方测评，再进行等级整改。

4 等级保护未来发展趋势

根据等级保护工作开展情况来看，等级保护发展将有如下的趋势：

4.1 等级保护行业化

由于每个行业在国家政治、经济、军事、外交等活动中的职能不同，所以信息系统在行业内所发挥的作用对行业职能影响不同，信息和信息系统被破坏后对等级保护客体的影响也有所不同。对本行业职能的认识，行业主管部门一般比信息系统的运营、使用单位具有更高的站位、更宏观的视野，从而可以保证做出更准确的判断。

因此为了使等级保护工作更能体现行业安全特点，更有针对性和实效性，同时为了在纵向上实现对等级保护的控制，一些重点行业主管部门可能在今后会在国家文件政策指导下进行符合本行业安全需求的等级保护行业标准、行业等级保护实施方法等文件的制定，用以指导本行业的等级保护工作。

所以，等级保护的检查也将会以联合工作组的方式进行。

4.2 与传统安全服务的结合

4.2.1、等级保护与风险评估

等级保护与风险评估之间互为依托、互为补充，存在着紧密的联系。等级保护是国家一项信息安全政策，而风险评估则是贯彻这项制度的方法和手段。

等级保护确定了信息系统安全保护的等级，要求风险评估过程应充分考虑安全等级保护的要求，风险评估的结果可作为等级保护安全建设的参考。

风险评估为等级保护工作的开展提供基础数据，是等级保护定级、建设的实际出发点。通过安全风险评估，可以发现信息系统可能存在的安全风险，判断信息系统的安全状况与安全等级保护要求之间的差距，从而不断完善等级保护措施。

另外，等级保护中、高级别的信息系统不一定就有高级别的安全风险。

4.2.2、等级保护与系统安全建设

当引入等级保护的概念后，系统安全防护设计思路会有所不同：

4.2.2.1由于确定了单位内部代表不同业务类型的若干个信息系统的安全保护等级，在设计思路上应突出对等级较高的信息系统的重点保护。

4.2.2.2安全设计应体现并保证不同保护等级的信息系统满足相应等级的保护要求。满足等级保护要求不意味着各信息系统独立实施保护，而应本着优化资源配置的原则，合理布局，构建纵深防御体系。

4.2.2.3划分了不同等级的系统，就存在如何解决等级系统之间的互连问题，因此必须在总体安全设计中规定相应的安全策略。

4.2.2.4不同等级的系统需要满足不同的安全管理要求，但所有的信息系统又都可能在同一个组织机构的管理控制下，如何实现等级保护的管理体系也需要在总体安全设计中给予规定。

4.3 等级保护的长期性

无论是采用那种等级保护建设流程，都应该认识到等级保护工作的长期性。等级保护的建设和整改应伴随着系统生命周期的一个不断循序渐进的过程。希望通过一期两期的安全活动或安全项目达到等级保护目标的想法是不可能的，也是不现实的。

应该说在等级保护整个过程中，定级阶段是相对简单的，难点是定级后如何进行建设和整改。这也是等级保护工作能够真正落在实处的关键阶段。也是目前各种矛盾相对集中的一个阶段。因此等级保护是一个长期的过程，必然会经历从摸索到成熟、从被动到主动的阶段的逐步演进。

技术评估的现状和发展

文/梁伟　服务产品部

信息安全的关键要素

随着各种信息化建设的不断发展，暴露出来的各种安全问题也越来越引起业界的重视，信息安全建设也就成了信息化建设过程中一个不可或缺的重要环节。

谈到信息安全，“风险”一词是不得不提的。信息安全的核心概念是安全风险，安全风险即：由于系统存在的脆弱性、人为或自然的威胁导致安全事件发生的可能性及其造成的影响。既然安全风险所关注的是安全事件的可能性及影响，那么，引起安全事件的各类威胁和脆弱性也就成为了“风险”这一关键要素值的基础来源。具体各要素可参考下图。

对于一个信息系统，威胁和资产相对于脆弱性来说更具有客观性，而脆弱性是可以被主动发现且修补的。从上图中我们可以看出，脆弱性相对于威胁和资产也起到了更为关键性的作用。

技术评估的方式和方法

脆弱性既然是安全风险中一个基础的关键要素，那么，发现脆弱性就是信息安全工作中的关键前提。脆弱性一般分为管理脆弱性和技术脆弱性，这里我们着重讨论发现技术脆弱性的一些传统方式，即：技术评估的传统手段，以及这些方法中存在的问题和可改进的地方。

在传统的技术评估过程中，技术脆弱性的检测通常分为两种基础手段：远程安全扫描和本地手工安全检查。

远程安全扫描就是使用扫描设备通过网络探测的方式，将探测结果结合设备内置的漏洞库进行分析，从而获取远程被评估系统中可能存在的脆弱性。这种方式的最大优点就是速度快，大部分工作自动完成，无需人工较多的介入。而其缺点也是显而易见的，就是探测过程中未得到系统授权，因此由于权限问题可能无法获取足够支撑后期分析的信息源，而且，被评估系统的一些防护措施（例如防火墙）也可能导致扫描过程中获取的信息不完整。

为了远程扫描上信息的不完整这一缺陷，作为扫描信息的补充方式，手工安全检查也是技术评估过程中不可缺少的一种方式。手工安全检查的过程在被评估系统上进行，通过手工检查，获取足够的信息来弥补远程扫描信息的不足。两种方式一个从外、一个从内，从两个不同的方向上发现系统中的缺陷。

从整体工作上来看，以上两种方式似乎已经足以发现所有的技术脆弱性，但结合实际情况来看，仍存在着一些问题：

分析人员技能决定脆弱性的发掘

在传统评估过程中，尤其是手工安全检查，获取的数据一般均为“中间结果”，即系统当前设置与快照，而对于当前设置是否能达到必

要的安全要求，需要取决于对该“中间结果”分析人员的技能。不同技能的人员，可能从中发现的安全问题也不同。显然，对于技能不高的分析人员，也就可能无法发现全部的安全隐患。

缺少对“个性化”应用程序的关注

所谓“个性化”应用程序主要是指一些第三方应用程序，这里所说的第三方应用程序并不只是Web Server、数据库这样的应用，还应包括一些常见的日常应用程序，如：Adobe Acrobat Reader。这些常用软件都有可能存在着不同程度的安全隐患。

Web脚本安全

Web安全问题已经是现今最大的安全问题之一，而Web安全又主要集中在Web脚本中，如：SQL Injection（SQL注入），XSS（Cross Site Script跨站脚本），RFI（Remote File Inclusion远程文件包含）。Web应用往往会因为几行脚本的问题而使整个系统陷入严重的安全威胁之中。

技术评估的改进和发展

近些年来，由于安全事件的频发，入侵者对安全技术关注点也较以前发生了一些转移，所以信息安全的关注点也发生了相应的变化。技术评估作为信息安全建设的一项基础工作也迫切需要改进，以便能适应新时代的信息安全问题。

结合上面所提出的各种问题，技术评估的一些改进可参考下图。

图中描述了针对一个典型的系统所展开的技术评估工作中需要进行的工作。

基线扫描

基线扫描不同于远程扫描，它在扫描过程中会要求用户输入被扫描系统的用户名和口令，即在获得授权的情况下对系统进行检测，加之内置了符合不同法规的安全标准值与检测到的结果进行对比。这样，就避免了分析人员因技能不足而无法发现全部脆弱性的问题。

手工检查

由于基线扫描设备已经解决了权限与授权的问题，因此手工检查将作为辅助手段，主要用于检查第三方应用安装情况，并结合已有漏洞库来判断第三方应用安全性。

配置分析

加强对应用的关注，通过对应用程序的配置检查，从配置上发现配置上的安全问题。

渗透测试

渗透测试属于高端技术类服务，通过专业测试人员模拟入侵者的常用入侵手法，对被评估系统进行一系列的安全检测，从而发现问题。渗透测试的好处在于，相比于代码审计工作周期要短，且不存在用户源程序泄露的隐患，而测试人员都具有较高技术能力，能够精准的控制测试结果和深度从而避免对系统造成致命的伤害。

结束语

目前，为适应信息化发展，各类应用软件更新换代频繁，而在这些频繁的动作下，隐藏的却是更多的安全问题。纵观我们日常频繁使用的软件，Adobe Acrobat Reader、Microsoft Word、Outlook等等，都曾经被挖掘出危害程度不同的漏洞，但是这也就意味着技术评估需要更细粒度的工作来识别更多的安全隐患，才有可能制定更加有效的安全防御方案。技术评估从系统层向应用层的转变，也必将是其发展方向，尤其是随着信息系统等级保护的推进步伐逐渐加快，技术评估已经到了转变思考方式的时候了。

P2P：让人欢喜让人忧

文/陶智　产品市场部

随着互联网的普及和网络应用的蓬勃发展，互联网正逐步改变着人类的生活和工作方式。而P2P的出现则更让我们体会到了在网络上自由互联、传送数据的乐趣。然而，P2P技术为我们的工作和生活提供便利的同时，也带来了更多的安全隐患。

说到P2P，很多人经常听到，也有些人略知一二，可它究竟是什么东西，它是如何带给我们全新的互联网体验，又带给我们什么安全风险呢？

认识P2P

P2P，全称叫做“Peer-to-peer”对等互联网络技术（点对点网络技术），它通过系统间的直接交换达成计算机资源与信息的共享。P2P技术是当前国际计算机网络技术领域研究的一个热点，被《财富》杂志誉为将改变互联网未来的四大新技术之一，目前微软、Sun、IBM等很多著名的企业和公司都投入到对P2P技术的研究之中。

P2P最根本的思想，在于它打破了传统的Client/Server模式，在对等网络中，每个节点的地位都是相同的，具备客户端和服务器双重特性，可以同时作为服务使用者和服务提供者。

因此P2P技术为文件共享、即时通讯、深度搜索、分布计算、协同工作等提供了更灵活高效的模式，但也为信息安全带来了新挑战。

P2P应用广泛

P2P技术自诞生以来，从最初的文件共享、软件下载、即时通讯，到目前方兴未艾的网络视频、网络电话，特别是网络视频为P2P近年来应用的热点和重点，可以说P2P已成为改变互联网的重要技术之一，走进越来越多的家庭、企业。

P2P之文件共享

我们经常能听到“BT下载”。所谓BT，即BitTorrent，是一种新颖的下载方式，从本质上说属于P2P软件的文件共享类别。

通常情况下，文件下载的工作原理是把文件由服务器端传送到客户端，例如FTP，HTTP等等。这样就产生了一个问题，随着用户的增多，对带宽的要求也随之增多，还会导致服务器崩溃，所以很多下载服务器都有用户数量和最高下载速度的限制，这样就给用户造成了诸多不便。

正因如此，P2P下载方式出现之后，很快就成为了下载迷们的最爱，许多用户利用P2P软件来交流最新的电影大片或软件。P2P下载软件可在下载的同时，也为其他用户提供上传，所以不会随着用户数的增加而降低下载速度，使用非常方便。其特点简单的说就是：下载的人越多，速度越快。

目前主流的P2P文件共享软件BitTorrent、BitComet、迅雷、POCO、电驴eMule、百宝、PP点点通、酷狗kugoo、VaGaa哇嘎、比特精灵、天网Maze、百度下吧等，成为用户下载电影、电视剧、软件、资料等首选工具，用户群非常庞大。

P2P 之即时通讯

即时通讯（Instant Messenger，简称IM）软件可以说是目前上网用户使用率最高的软件，无论是老牌的ICQ，还是国内用户量第一的腾讯QQ，以及微软的MSN Messenger都是大众关注的焦点，它们能让你迅速地在网上找到你的朋友或工作伙伴，可以实时交谈和互传信息。而且，现在不少IM软件还集成了数据交换、语音聊天、网络会议、电子邮件等功能。IM即时通讯软件基于P2P技术，因此它的覆盖范围广，信息传播速度快。

目前主流的即时通讯软件有国际的ICQ、MSN Messenger、Yahoo Messenger、Skype和国内的QQ、新浪UC等。QQ成为一般用户特别是年轻人日常联系的工具，MSN成为上班一族的首选，在全球，每天有数以千万计的用户登录微软、雅虎以及腾讯的即时通讯服务网络，处理工作中的问题，或者从事个人的社会交往。

P2P 之网络视频

所谓网络视频是指用户通过网络或者特定数字信道边下载边播放多媒体数据的一种工作方式。网络视频应用的一个最大的好处是用户不需要花费很长时间将多媒体数据全部下载到本地后才能播放，而仅需将起始几秒的数据先下载到本地的缓冲区中就可以开始播放，后面收到的数据会源源不断输入到该缓冲区，从而维持播放的连续性。目前市面上主要的网络视频系统有微软公司的Windows Media、Real公司的Real System等。但是随着网络技术的发展，基于P2P的网络视频技术已经开始出现，对网络状况和音视频质量带来很大改进。采用基于P2P的网络视频技术，用户可以根据他们的网络状态和设备能力与一个或几个用户建立连接来分享数据，这种连接能减少服务器的负担和提高每个用户的视频质量。P2P技术在网络视频应用中特别适用于一些热门事件，即使是大量的用户同时访问网络视频服务器，也不会造成服务器因负载过重而瘫痪。目前主流的P2P网络视频软件有PPLive、PPStream、UUSee、QQLive和Joost等软件。用户可以利用软件享受到体育比赛和重大活动直播、影视节目轮播、点播、聊天室广播、网络电台等业务。

2006年春节联欢晚会期间，中央电视台使用P2P和内容分发网络（CDN）技术向全球进行同步视频直播；晚会当晚央视网站页面点击量达到2.96亿次，页访问次数达4792万次，收看春节晚会视频直播的人次为410万，其中89万来自海外。

据iResearch统计，2006年中国网民中日均使用用户数量有1000万人，占P2P网络视频用户的25%，预计到2010年日均使用用户数量有6300万人，占P2P网络视频用户的40%。网络视频将成为日常生活的必需品。

P2P 之网络电话

VoIP又称IP电话，是Voice over IP的缩写，这种技术通过对语音信号进行编码数字化、压缩处理成压缩帧，然后转换为IP数据包在IP网络上进行传输，从而达到了在IP网络上进行语音通信的目的。VoIP的实现优势在于获得更低成本的传统语音与传真服务，同时用户还将受益于基于VoIP的具有突破性的新型服务，如呼叫中心、统一消息处理等。目前，越来越多的企业开始采纳VoIP技术，并从中获益。

Google、AOL、Yahoo、MSN、Skype等厂商的即时通讯软件也都具备VoIP功能，已成为广受网络使用者欢迎、用以取代市话的通讯软件。以最知名的Skype为例，全球已有1.5亿名注册用户。

Skype是由KaZaA的开发者开发的一款P2P软件，它提供“计算机-计算机”间的免费呼叫服务、语音邮件、即时消息、快速呼叫、电话会议等功能，同时它还提供了一个称为Skype-out的付费呼叫服务，这种服务是通过Skype软件连接到传统固定电话或移动电话进行通话的。

最引人注意的是Skype采用“端对端”加密，极具保密性。其加密算法与美国政府用来保护机密数据安全的算法相同，保证了Skype在信息（语音、即时消息、文件）发送之前进行加密，在接收到的时候进行解密，不会在中途被窃听。

P2P喜忧参半

P2P技术在下载、流媒体、VoIP等领域得到飞速发展，体现了互联网最根本的内涵自由和免费，它的主要优点如下：

- 对等性高：非中心化，互联网回归本色—联系和传输；
- 扩展性强：用户扩展与资源、服务、系统同步扩展；
- 健壮性高：服务分散和自适应，耐攻击、高容错性；
- 性价比高：P2P成本低、存储和计算能力强；
- 负载均衡：分布存储和计算，整个网络负载得以均衡。

P2P的应用种类众多，得到了用户的广泛使用和认可，然而在火热的应用背后也潜伏着不少危机，具体来说有如下几个方面：

1、严重占用带宽

如果多个用户同时使用P2P软件进行下载，或者使用P2P流媒体软件观看在线视频，会占用大量网络带宽，严重影响其他用户的正常工作。这不仅给企业、政府、学校等带来困扰，还给电信运营商带来极大的影响。

据统计数据显示，随着P2P的大量应用，P2P流量成为运营商城域网的主要流量，占到40-60%，晚上甚至有90%，下载型和视频类业务占P2P流量的大部分，而流到城域网外的P2P流量占全网流量的60%以上；当前大多数P2P工具为了保证传输质量，往往创建大量的连接，而这些连接并未传输数据，白白地消耗网络资源。

2、网络病毒传播

在P2P环境下，方便的共享和快速的选路机制，为网络病毒提供了更好的入侵机会。共享电影中带恶意链接，下载软件中带木马病毒，已成为普遍现象。由于某些P2P应用如Skype采用加密传输技术，使传统的安全技术无法检测Skype数据通讯，也给了其传输的恶意程序逃过监控的可能，甚至Skype的用户计算机可能被植入恶意代码而变成僵尸网络（botnet）大军中的一员，目前已发现通过Skype文字聊天传播的蠕虫病毒，因此通过P2P传播的病毒，波及范围大，覆盖面广，造成的损失很大。而继电子邮件之后，即时通讯软件已经成为病毒入侵的新“通道”。

3、影响工作效率

企业员工沉迷于上网聊天、下载电影、看网络视频不能自拔，从而影响了正常的工作。

4、企业机密泄露

在企业办公电脑上，内部员工能够毫不困难地利用即时通讯软件向外界传输企业机密文件，从而令企业蒙受重大损失，而加密的数据传输让管理员无能为力。

5、知识产权保护

P2P共享网络提供了一个大范围文件共享的平台，用户通过它可以与其它网友交换共享出来的音乐、视频、图书、图片、软件、游戏等，普遍存在着版权问题。P2P下载及网络视频的繁荣加速了盗版媒体的分发，提高了知识产权保护的难点。

6、QoS无法保证

目前的P2P应用基于互联网，且对不同节点缺乏了解和控制，应用的**QoS**无法保证。如BT下载经常出现文件下载到快结束时，种子消失，所有的努力都白费了。P2P流媒体业务用户热门的节目看起来还不错，但是一些比较冷门的节目，虽然从菜单上能看到，但是往往不能真正的使用，体验比较差。

如何解决这些问题呢？我们首先需要了解P2P技术，只有知道P2P技术实现、应用特点、发展趋势，我们才能针对性提出解决方案。

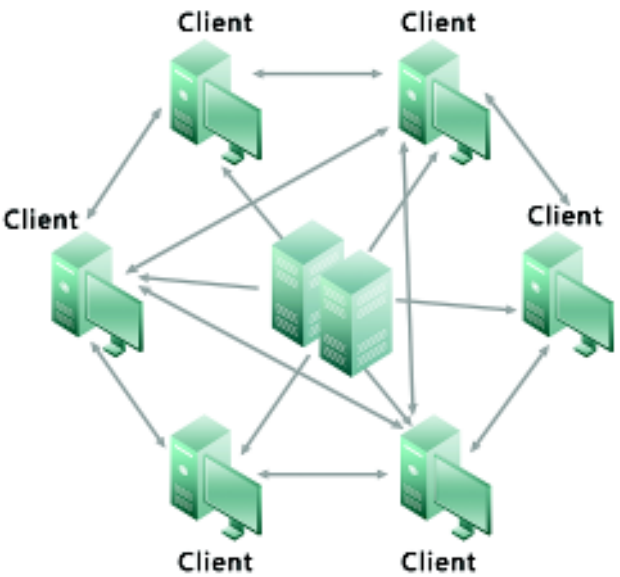
P2P 技术趋势

随着P2P技术的发展，P2P网络架构出现Tracker网络、DHT网络两类不同实现方式。

1、什么是Tracker网络?

Tracker是指运行于服务器上的一个服务程序，也称Tracker服务器。这个程序能够追踪到底有多少人同时在下载或上传同一个文件。客户端连上Tracker服务器，就会获得一个正在下载和上传的用户的信息列表，根据这些信息，P2P下载客户端会自动连上别的用户进行下载和上传。

一般来说，客户端首先连接Tracker服务器获取用户信息，根据所获得的正在进行下载和上传的用户列表，与其他客户端进行文件交换，这是传统实现方式。如下图所示：

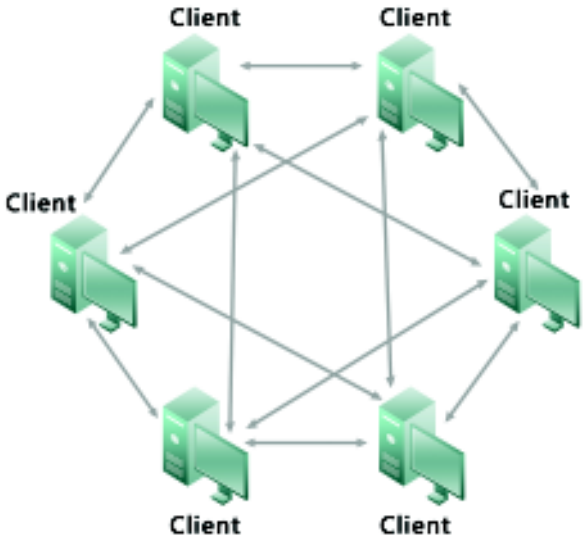


Tracker 网络

2、何为 DHT 网络?

DHT 的全称是Distributed Hash Table（分布式哈希表技术），采用DHT的网络不需要中心节点服务器，而是每个客户端负责一个小范围的路由。我们可以把整个DHT网络想象成一个大城市，那么每个客户端就好比城市里各个角落的地图，上面绘制了附近区域的地形情况，把这些地图一汇总，城市的全貌就出来了。

一般来说，任何一个运行P2P客户端的用户都可以作为DHT网络中的节点 ，用户信息分散在DHT网络各节点中，这是新的实现方式，提高下载稳定性，但更难控制。如下图所示：



DHT 网络

可以说，DHT 网络的出现是提高 P2P 通讯质量，也为了躲避网络监管，逃避限制浏览 P2P 资源网站、禁止访问 Tracker 服务器、封闭 P2P 通讯端口等传统限制措施。

随着 P2P 技术的不断应用，其技术越来越完善。我们从 P2P 的文件共享、软件下载、即时通讯、网络视频、网络电话等各类应用技术研究中可以看到P2P技术的发展趋势主要体现在两个方面：

1、P2P 应用协议加密

BitComet 是最具代表性的BT 下载客户端之一，从其V0.63 版本开始，BitTorrent 协议去除旧版协议头加密，采用全新的传输协议加密机制，该传输加密协议提供完全随机的报头，主要目的是为了避免被协议识别；如果使用更强的RC4加密模式，兼容Azureus和uTorrent的协议加密算法，则该传输加密协议可以对内容进行封装、避免被监听，这样使得检测和识别BT流量更加困难。由于无法识别加密的P2P流量，从而对 P2P 流量的限制和封堵无从下手。而 Skype、Vonage 及其它 VoIP 软件使用专属通讯协议，采用了“端对端”高强度加密技术，以确保通讯内容隐密。

为了加强通讯机密性，规避网络监管，应用协议加密越来越多的受到P2P软件厂商的青睐，已成为P2P应用软件未来发展趋势之一。

2、混合多协议通讯

迅雷是目前国内应用较为广泛的一种P2P下载软件，它使用的多资源超线程技术快速传递网络上的计算机资源，下载速度快，带宽利用率高，还提供数据校验，保证下载数据的准确性。讯雷采用的技术具有一些特点：

迅雷采用跨协议通讯，同时支持 Http、Ftp、BT、Emule 和迅雷

P2P协议，多协议之间相互切换，不仅规避可能的网络监管，而且还能够与BT、Emule等其他客户端通讯，建立更广泛的通讯网络。

迅雷采用P2SP技术，它除了包含P2P以外，更多了个S（P2SP的“S”是指服务器）。P2SP有效地通过多媒体检索数据库这个桥梁，把原本孤立的服务器和其镜像资源以及P2P资源整合到了一起。也就是说，在下载的稳定性和下载的速度上，都比传统的P2P或P2S有了较大的提高。

为了扩大应用规模，提高P2P通讯效率，规避网络监管，越来越多的P2P软件厂商采用混合多协议通讯，已成为P2P应用软件的未来发展趋势。

因此P2P技术在不断应用过程中，越来越向强通讯加密、多协议混合方向发展，也给P2P的监管提出很大的难题。

P2P应对之策

对于风起云涌的P2P技术，可以说让人欢喜让人忧。但针对不同的组织及企业，我们往往需要考虑不同的应对策略。一种是限制策略，严格控制P2P，保证企业利益，而另外一种是疏导策略，利用P2P技术，发展增值运营，提高网络效率。

限制策略

作为企业CIO/网络管理员，考虑的是如何保证企业网络可用、可控。因此采用限制策略，严格控制P2P，保证P2P流量控制在不影响业务应用的前提下，保证各种P2P网络应用可监测、可控制，满足企业对员工上网行为的合规要求。

要对P2P进行管理，首先要能够对P2P应用进行识别，这是P2P管理的核心技术，一般P2P管理技术分为P2P检测技术和P2P控制技术两类。

P2P检测技术

常用的P2P检测技术包括传统的端口检测技术、最新的协议识别技术。

1、端口检测技术

作为传统检测技术的代表，端口检测根据TCP/UDP的端口来识别应用，检测效率高。例如早期Edonkey使用端口为4661–4662，BT使用端口为6881-6890。

随着IP网络技术的发展，端口检测技术适用的范围越来越小。事实上，协议与端口是完全无关的两个概念，标准协议可以运行在任意端口，我们经常看到运行在8080端口的Http流量、通过80往往采用动态端口技术，因此要检测这些P2P应用，无法单纯依赖端口检测，而必须识别P2P应用协议。

2、协议识别技术

在高速网络飞速普及的今天，P2P下载、网络视频、VoIP、即时通讯、网络游戏等迅速普及，这些崭新的网络应用大部分使用了一种被称为Smart Tunnel（智能隧道）的技术，该技术正是为了避开类似协议端口映射表技术的产品而诞生的。其特点是：服务端（或接收端）没有绑定任何固定的端口，客户端(或发起端)可以自行使用任意随机端口连接服务器。

作为新一代检测技术，协议识别技术通过动态分析网络报文中包含的协议特征，发现其所在协议，然后递交给相应的协议分析引擎进行处理。具备了协议识别技术的产品，能够在完全不需要管理员参与的情况下，高速智能准确地检测出运行在任意端口的应用层协议，对于运用了Smart Tunnel技术的P2P软件也能准确地捕获分析。深入而细致

的协议识别技术能够极大地提高检测的准确性，降低误报率。

协议识别技术是多种技术的综合应用，包括基于RFC标准的协议分析技术、基于逆向工程的协议分析技术、基于模式匹配的特征检测技术、基于关联分析的统计检测技术，相互配合才能达到更好的效果。

■ 基于RFC标准的协议分析技术

目前有很多已知的、通用协议，例如HTTP、FTP、DNS、SMTP等，都有协议的RFC文档，规定了协议特有的消息和命令字以及状态迁移机制，通过分析数据包里的这些专有字段和状态，就可以精确可靠地识别这些公开、标准的P2P协议。

■ 基于逆向工程的协议分析技术

一些未公开协议，例如当前多数的P2P协议，厂家出于多方面的考虑，并不公开其协议细节，这时一般需要通过逆向工程识别协议机制，这类方法工作量大，而且协议的变化快，要保持各种协议变化的及时跟踪，必须有大量的人力投入和不断的技术跟踪才能保证检测的高效性，因此要有较强大的研发队伍作后盾。

■ 基于模式匹配的特征检测技术

模式匹配是将协议解码后的域值与事先精心提取的特征（规则）进行匹配，从中发现P2P应用行为。这种基于特征（规则）的检测是一项传统而成熟的检测技术，提供了很高的准确性与广泛性。通过不断升级的特征库，可以在第一时间检测到各种已知的P2P应用。

■ 基于关联分析的统计检测技术

端口检测可以逐包进行，模式匹配可以逐流进行，而基于关联分析的统计检测是更为复杂的技术。一般来说，对单个会话的特征检测就能够识别一些传统的P2P应用协议，但越来越多的P2P应用采取协议加密、协议模糊等规避监管的技术，简单的数据分析已无法准确识别新型P2P应用，需要在IP碎片重组、TCP会话跟踪、TCP流汇聚的基础上，通过单包模式匹配、单会话多包关联分析、多会话关联分析等综合手段来精确识别P2P应用特征，通过统计分析各种P2P应用的连接数、单IP的连接模式、上下行流量比例关系、数据包发送频率等行为特征来对P2P应用类型进行区分，以提高协议识别能力。

P2P控制技术

在对P2P应用进行有效检测之后，管理员即可对P2P应用进行控制。常用的P2P控制技术包括P2P流量控制技术和P2P内容控制技术。

1、P2P流量控制技术

P2P流量控制技术表现为基于对象的多因素限制，可以基于协议/端口、基于源/目的IP地址或网段、基于时间（上下班时间、工作/非工作时间）、基于流量（最大限制带宽/最小保证带宽/最大会话数）、基于优先级别等多种因素，通过灵活多样的控制手段达到限制P2P流量的目的。

企业根据不同对象灵活制定适合的控制策略，从而保证企业重要业务服务的正常运行。比如，对那些长时间、大量占用网络带宽的P2P用户可以实施控制，限制其带宽使用情况。针对作息规律、只在某一时间段内流量比较大的P2P用户，可以设定分时策略，只在网络高峰期控制其流量。

举些例子如下：

允许公司所有员工上网，但总带宽最大10Mbps；允许公司员工BT下载，但BT总带

宽最大5Mbps；

行政部BT下载带宽最大 300Kbps，其中每IP最多30Kbps；开发部BT下载带宽最大200Kbps，其中每IP最多50Kbps；

上班时间，分配给邮件最小保证带宽5Mbps，BT下载最大限制带宽2Mbps，邮件流量的优先级别最高；下班时间，BT下载最大限制带宽5Mbps，HTTP流量的优先级别最高。

2、P2P内容控制技术

P2P内容控制技术表现为对P2P应用行为和P2P应用传输内容两方面的限制，其中行为限制的结果表现为允许或禁止用户的P2P应用行为，如允许使用MSN聊天，禁止BT下载，而内容限制的结果则表现为禁止P2P应用的敏感内容传输，如MSN聊天时禁止包含公司机密信息的内容。两者都能达到限制P2P达到合规要求的目的。

以MSN Messenger的控制为例，P2P内容控制技术不仅可以控制MSN的以下行为：用户登录、用户下线、用户接收信息、用户发送消息、用户传送文件、用户状态改变为离开、用户音频聊天、用户视频聊天等。还可以控制MSN的以下内容：用户登录账户、聊天内容关键字、传送的文件大小、传送的文件名等。

举一些形象的例子：

允许某些人MSN登录，但不允许其发送消息；

允许某些人MSN聊天，但不允许其发送文件；

不允许在聊天中涉及企业机密关键字的内容；

允许上班禁止使用MSN，而下班允许使用MSN；

只允许某些人员使用MSN等等。

疏导策略

当然，作为运营商，网络资源是其生财之道，因此，如何有效的发挥手中网络资源的价值是运营商当前非常关心的事情，而一种叫做P2P cache的技术为运营商提供了新的思路。

P2P cache（P2P缓存代理）技术的核心思想为“大禹治水，重在疏导”。在运营商网络内部部署P2P cache系统，通过缓存外网的P2P内容向内网用户提供服务，同时主动引导本地内网P2P用户优先相互交换内容。这样既可以为内网用户提供可管理控制的P2P服务，保证（或者控制）用户的P2P应用体验；又可以缓解P2P应用对网络出口的压力，减少P2P流量对网络品质和网络服务的影响。

此外，还可以通过P2P CDN（内容分发网络）技术，可以在P2P cache系统基础上建设基于P2P的网络视频服务平台，提供直播、点播、下载、个人视频发布和共享等服务，同时可以充分利用P2P cache中已经缓存的健康内容，迅速向网内用户提供服务，将P2P的管理转化成一种增值服务。

结论

经过多年的技术发展和演进，P2P技术已经得到大量的应用，正吸引越来越多的企业投入到这方面的开发及应用。如何解决P2P发展面临的安全、管理、标准及版权等问题，是摆在政府、企事业单位以及运营商面前的难题。单纯封堵P2P并不能完全解决问题，而引导P2P业务的合理应用也不失为一种新的思路。

SQL 注入何去何从

文 / 赵旭　产品市场部

本文首先简单介绍Web应用的发展历程，然后针对Web应用重要安全威胁之一——SQL注入攻击进行重点介绍。分析了SQL注入的成因和危害，并回顾了其发展历史和趋势，最后介绍攻击防护思路。

WEB 应用的发展

WWW最初源自一种创造性的思想：新的网络层协议、新的服务软件实现网络连接并处理客户各种各样的需求，新的客户软件可以远程浏览服务器、并搜索整个服务器获取所需信息。在因特网早期，WWW仅意味着提供静态网页内容的Web站点，而Web浏览器只是被发明用于获取及显示这些静态网页内容。

到了今天，Web领域发展了很多崭新的应用，人们可以通过Web平台在线享受到丰富的服务。近年来比较著名的Web应用包括：

- 网上购物（Amazon、淘宝）
- 社交网络（MySpace）
- 网上银行（各大银行）
- Web 搜索（Google、百度）
- 电子拍卖（eBay、淘宝）
- 博客（Blogger）
- Web 邮件（Hotmail）
- 信息交互（Wikipedia）

除了用于公众互联网，Web应用也被广泛用于企业内部，发挥关键的商业职能，如访问人力资源业务、管理公司资源。一些传统采用C/S（需要安装客户端软件）架构的商业应用服务，如ERP、Email等都可以基于Web，也就是说，我们可以通过浏览器来访问这些资源，而无需额外安装客户端软件。这种趋势甚至影响到传统的桌面办公软件，如文字处理软件、电子制表软件等也正逐渐向Web化迁移。对此，Google提供了Google Apps，而微软提供了Office Live。[1]

伴随新兴Web应用产生的是新兴安全威胁。Web服务器以其强大的计算能力、处理性能及所蕴含的高昂价值，成为被攻击的主要目标。攻击者可以利用Web应用程序的漏洞进行渗透，从而偷取私人信息、进行金融欺诈，甚至是针对其他用户实施恶意行为（如网页挂马）。来自著名安全公司Symantec的2007年威胁报告表明，Web应用漏洞比例占所有漏洞的66%。来自世界知名信息技术研究咨询公司Gartner的数据也表明，当前针对企业网站或系统层。

SQL 注入介绍

传统上，远程溢出是渗透测试里最有效的办法，但经过一些利用远程溢出漏洞蠕虫的肆虐，现在很多网络管理员的安全意识增强了，一般都能及时安装系统补丁，而且软硬件厂商针对溢出问题提供了很多解决方案。可以说以后溢出在渗透测试中的路越来越窄。这时候对Web应用程序（CGI程序）的渗透是一个非常好的途径，因为CGI程序开发要求的技术含量相对较小，攻击需要付出的代价也相对较小。如果CGI程序员没有很好的安全意识（通常Web应用的开发周期很短，也就意味着相应的检查、测试、质量保证等环节所用的时间很少），那么这些CGI程序就有可能成为突破点。[6]

下面将介绍CGI攻击的一大分支—SQL注入攻击。

SQL注入是目前因特网上最为滥用的攻击方式，通过Google或百度进行搜索，我们可以找到大量的文章和信息。这类攻击的泛滥，一方面由于Web应用的多元化及经济价值所在，当前攻击者的驱动力从单纯的爱好转为经济利益；另一方面，攻击软件的泛滥降低了技术门槛。如SQL注入自动化攻击引擎实现了“目标锁定、发现注点及注入攻击”全过程自动化，尤其是自动完成“发现注点”这一关键步骤，极大便利攻击者为其提升攻击成功率。

1、成因与危害

很多Web应用程序都使用数据库来存储信息。SQL即结构查询语言（Structured Query Language），美国国家标准学会（ANSI）定义的一种标准语言，用于访问、查询关系数据库系统。SQL指令作为前端Web和后端数据库之间的接口，很多Web站点都会利用用户输入的参数动态地生成SQL查询请求。攻击者通过在URL、表格域，或者其他的输入域中输入自己的SQL指令，以此改变查询属性，骗过应用程序，从而可以对数据进行不受限的访问。

SQL注入漏洞成因在于Web应用程序对用户提交CGI参数数据未做充分检查过滤。用户提交的数据可能会被用来构造访问后台数据库的SQL指令，如果这些数据过滤不严格就有可能被插入恶意的SQL代码，从而非授权操作后台的数据库，导致敏感信息泄露、破坏数据库内容和结构、甚至利用数据库本身的扩展功能控制服务器操作系统。利用SQL注入漏洞可以构成对Web服务器的直接攻击，还可能利用服务器攻击第三方的浏览网站的其他用户。

2、历史

下面我们简单回顾一下SQL注入的相关历史[2]。

■ 1998年12月，Rain Forest Puppy（RFP）在著名安全杂志《Phrack》第54期上发表文章《NT Web技术漏洞》，首次提到应用SQL注入的攻击技术，需要注意的是，当时RFP在文中没有使用“SQL注入”这一术语；

■ 1999年2月，Allaire发出安全通告《动态查询中的多SQL指令》，讨论SQL注入攻击这类安全威胁；

■ 1999年5月，RFP与Matthew Astley发出安全通告《NT ODBC远程危害》，介绍如何将VBA代码注入到Access SQL查询中；

■ 2000年2月，RFP发表文章《我是如何渗透Packetstrom网站的—SQL注入渗透wwwthreads应用程序一瞥》，披露如何利用wwwthreads应用程序的漏洞进行SQL注入，从而获取对数据库服务器的控制；

■ 2000年9月，David Litchfield在Blackhat欧洲会议上发表主题演讲《评估IIS上的应用》，介绍如何使用“SQL插入”（SQL insertion）技术通过ASP应用程序攻击数据库服务器；

■ 2000年10月，Chip Andrews在SQL-Security.com上发表《SQL注入FAQ》，首次公开使用“SQL注入”这个术语；

■ 2001年4月，David Litchfield在Blackhat会议上发表主题演讲《通过ODBC错误信息远程分解Web应用程序》，介绍了一种新型SQL注入攻击技术，采用该种技术可准确获

取到数据库架构；

■ 2002年1月，Chris Anley发表论文《针对SQL Server的高级SQL注入》，首次对SQL注入攻击进行深度探讨；

■ 2002年6月，Chris Anley发表论文《更为先进的SQL》，补充其同年1月发表的论文；

■ 2004年Blackhat会议上，0x90.org发布了SQL注入工具SQeaL (Absinthe的前身)。

3、新型SQL注入攻击

SQL注入攻击技术出现已有10年历史，期间该种攻击技术被广为利用，并持续发展。2007年底出现了新型的攻击方式。过去SQL注入攻击针对特定的Web应用程序，攻击者事先已经了解到了底层数据库的架构以及应用程序注入点。而现在的新型攻击与以往有很大不同。它将可能攻击任何存在SQL注入漏洞的动态ASP页面。

来自网络世界（Network World）的报导，2008年5月13日，在中国大陆、香港及台湾地区有数万个网站遭遇新一轮SQL注入攻击，并引发大规模挂马。来自微软今年5月的报导，在过去的4个月中，之前已有3次大规模攻击，受害者包括某知名防病毒软件厂商网站、欧洲某政府网站和某国际机构网站在内的多家互联网网站，感染页面数最多超过10，000页面/天。[4][5]

具体攻击原理，如下图所示。黑客首先使用Google搜索引擎定位网页中包含的动态ASP脚本，测试脚本是否存在SQL注入漏洞并确定注入点，最终试图遍历目标网站后台SQL Server数据库的所有文本字段，插入指向恶意内容（即黑客控制的服务器）的链接。攻击的整个过程完全自动化，一旦攻击得逞，这些自动插入的数据将严重破坏后台数据库所存储的数据，动态脚本在处理数据库中的数据时可能出错，各级页面不再具有正常的观感。被攻击站点也可能成为恶意软件的分发点，访问这些网站的网民可能遭受恶意代码的侵袭，用户的系统被植入木马程序从而完全为攻击者控制。

微软研究表明，采用该种攻击方式的趋势将急速增长。主要有两方面原因：第一是由于恶意自动化攻击工具泛滥，该种工具使用搜索引擎发现存在SQL注入漏洞的站点。其次，僵尸网络正在进行SQL注入攻击，以更大范围地扩大僵尸网络。[5]

防护技术

尽管由于攻击的泛滥，人们防护SQL注入的安全意识已大为提升，但仍然有众多的人缺乏系统的防护概念。下面将简要介绍如何从全面、系统的角度来正确防护SQL注入（如下图所示[3]），在此希望能抛砖引玉。

1、开发阶段

在Web应用编码阶段需要对输入进行细致的验证，使用静态查询（如使用参数化查询）。且遵循“最小权限准则”，即只赋予应用程序完成其功能的最基本权限。以下是关于最小权限的一些建议：

- 不要使用root权限访问数据库
- 为数据表设定限制的可读/可写权限
- 慎用数据库存储过程

2、测试阶段

在测试阶段采用以下两种方式，确保Web应用程序代码的安全性：采用源代码审核方式，从编程者角度审视代码是否存在漏洞；执行渗透测试，从攻击者角度检查代码的安全性。需要注意的是，尽管完成以上两步，仍不能确保100%的安全，但这两种方法对于确保应用程序质量是必须的。

3、产品化阶段

在产品化阶段，Web应用已经正常上线、对外提供服务。此时，可能会发现Web应用存在一定安全隐患，但对各类组织来说，在该阶段进行代码整改很不现实，因为这意味着组织需要付出较大代价。因此，推荐使用专用的Web应用网关。这种设备工作在应用层，因此对Web应用防护具有先天的技术优势。基于对Web应用业务和逻辑的深刻理解，Web应用网关对来自Web应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站站点进行有效防护。当然，对于SQL注入的防护，存在策略配置精准性的问题，否则会引起相应的误报或漏报。

综上所述，对于SQL注入防护，理想的解决思路是在Web应用生命周期的各个阶段做出相应的努力。

总结

SQL注入攻击作为当前Web应用安全热点之一，从1998年第一次出现至今，已有10年发展历史，被广为利用并持续发展。

伴随新兴Web应用产生的是新兴安全威胁。Web服务器因为其强大的计算能力、处理性能及所蕴含的高昂价值，成为当前最为主要的攻击目标。

从2007年底开始，互联网上出现了新型的自动化攻击方式，并在2008年引发了大规模的网页挂马。如何有效防护SQL注入攻击，需要采用综合、系统的方法来解决问题，即在Web应用生命周期的各个阶段做相应的努力。

参考资料

[1] The Web Application Hacker's Handbook, Dafydd Stuttard & Marcus Pinto, 2008

[2] Data-mining with SQL Injection and Inference, David Litchfield, 2005

[3] Advanced Topics on SQL Injection Protection, Sam NG, SQLBlock.com, 2006[4] Mass SQL injection attack targets Chinese Web sites

http://www.networkworld.com/news/2008/051908-mass-sql-injection-attack-targets.html

[5] SQL Injection Attack

http://blogs.technet.com/swi/archive/2008/05/29/sql-injection-attack.aspx

[6]《网络渗透技术》，XFocus Team，许治坤、王伟、郭添森、杨冀龙，2005

揭秘数据库的访问审计

文/蒲新宇　产品市场部

已成燃眉之急

随着信息系统业务不断发展，数据库系统应用范围越来越广。企业的财务数据、贸易记录、工程数据等均需要利用大量的数据库资源。

同时，由于数据库的作用和影响越来越大，企业数据库信息安全面临严峻挑战日渐明显。近年来不断发生的重要敏感数据的被窃取、篡改问题，被引起的高度重视，成为迫切需要解决的问题。

威胁与风险并存

由于企业数据库系统用户众多，涉及数据库管理员、内部员工及合作方人员等，网络管理更加复杂，企业数据库面临的主要安全威胁与风险如下：

数据库账户和权限的滥用

表现一：缺少针对数据库管理员监控机制

数据库管理员拥有数据库系统管理、账号管理、权限分配等系统最高权限。如果数据库管理员利用工作之便，窃取敏感信息、篡改毁坏重要业务数据，对企业数据库安全的打击将是致命的。

表现二：合法用户权限滥用

数据库系统的操作管理采用分权管理形式，包括多个账号，如普通账号、用于数据库日常维护的临时账号；如果上述账号权限被内部人员或合作方人员用来窃取、恶意损毁数据库的重要业务数据，在短时间内管理者极难察觉发现数据被篡改或删除，事后也难以追查取证，造成难以弥补的损失，甚至带来灾难性的后果！

数据库自身日志审计的缺陷

表现一：难以实时监测发现问题

数据库系统自身的日志审计功能可以记录各种数据库系统修改、权限使用等日志信息，并不能帮助管理者及时发现定位问题；同时由于不能实时监测报警，因此在数据库异常安全事件发生时，无法第一时间报告给管理者，导致管理者不能及时采取有效措施。

表现二：影响数据库服务器运行与性能

数据库自身日志审计也会占用大量的硬盘空间，降低数据库服务的性能，甚至可能影响正常应用的顺利进行，同时面对成千上万条日志记录，如何筛选出有用信息也是客观存在的问题。

安全需求紧迫

根据对企业数据库系统的威胁与风险分析，企业的数据库安全需求主要集中在以下方面：

一是，全面监测数据库超级账户、临时账户等重要账户的数据库操作。

二是，实时监测数据库操作行为，发现非法违规操作能及时告警响应。

三是，详细记录数据库操作信息，并提供丰富的审计信息查询方式和报表，方便安全事件定位分析，事后追查取证。

因此通过在企业网络中部署安全审计系统，可有效监控数据库访问行为，准确掌握数据库系统的安全状态，及时发现违反数据库安全策略的事件并实时告警、记录，同时进行

安全事件定位分析，事后追查取证，保障企业数据库安全。

基本标准评价

是否能够很好地帮助管理者完成对数据库访问行为的监测是数据库安全审计系统的基本标准。一个完善的安全审计系统应该从几个方面评价：

一是，具有全面丰富的数据库审计类型。

二是，具有细粒度的数据库操作内容审计。

三是，能准确及时的违规操作告警响应。

四是，可以全面详细的审计信息，丰富可定制的报表分析系统。

五是，自身的安全性高，不易遭受攻击。

由此可见，能通过网络数据的采集、分析、识别，实时监控网络中数据库的所有访问操作，同时支持自定义内容关键字库，实现数据库操作的内容监测识别，发现各种违规数据库操作行为，并及时报警响应、全过程操作还原，从而实现安全事件的准确全程跟踪定位和全面保障数据库系统安全的数据库安全审计系统，才是一款合适的产品。

特性分析

全面的审计类型

系统应覆盖ORALCE、SQL SERVER、MY SQL、DB2、Sybase、Infomix等主流数据库系统。

灵活的审计策略

系统应支持基于内容关键字、IP地址、用户/用户组、时间、数据库类型、数据库操作类型、数据库表名、字段名等多种组合数据库审计策略，从而全面监测发现各种非法操作及合法用户的违规操作。

数据库操作信息还原

系统应实时审计用户对数据库系统所有操作（如：插入、删除、更新、用户自定义操作等），并完全还原SQL操作命令包括源IP地址、目的IP地址、访问时间、用户名、数据库操作类型、数据库表和字段名等，实现安全事件准确全程跟踪定位，为事后追查取证提供有力支持。

多种业务运维操作审计

系统需要支持对TELNET、FTP等操作的命令级审计和全过程记录。

审计信息管理

系统需支持数据库审计事件信息的备份、恢复、清除、归并等功能；日志信息应能保存到SQL Server，Oracle等大型数据库中。

系统需提供详细的综合分析报表、自定义等多种类型报表模板，支持生成：日、周、月、季度、年度综合报表。报表应支持MS Word、Html、JPG等格式导出。

丰富的管理能力

为不影响数据库系统自身运行与性能，系统需采用旁路监听部署模式。

系统需支持多种响应方式，包括发送邮件、安全中心显示、日志数据库记录、打印机输出、运行用户自定义命令、TCPKiller等方式及时报警响应。

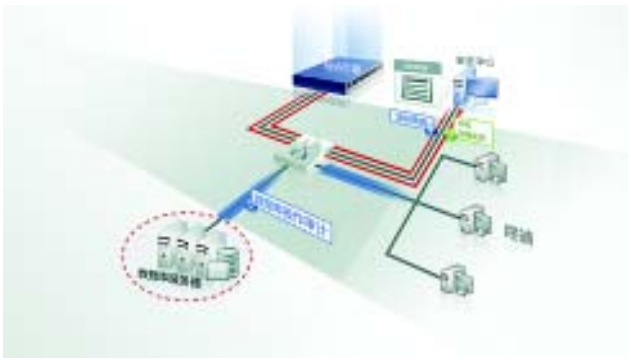
高可靠的自身安全性

系统需具有安全、可靠、高效的硬件运行平台；采用强加密的SSL加密传输告警日

志与控制命令，避免可能存在的嗅探行为，保证数据传输的安全。

典型部署及效果

典型的数据库安全审计部署拓扑图如下：



通过在企业内网核心交换机上旁路部署安全审计系统网络引擎，实时审计所有用户对数据库服务器的操作。在企业的网络管理区部署1台服务器作为安全审计系统的安全中心，管理安全审计系统网络引擎，并具有系统监控和审计日志管理功能。

通过部署安全审计系统将帮助企业实现：

实时监控数据库各种账户（如超级管理员、临时账户等）的数据库操作行为，准确发现各种非法、违规操作，并及时告警响应处理，降低数据库安全风险，保护企业数据库资产安全。

全面记录还原数据库操作信息，提供丰富的审计信息查询方式和报表，方便安全事件定位分析，事后追查取证。

由此可见，数据库安全审计系统的方案部署同样也需要讲究科学和方法，这样才会收到事半功倍的效果。

企业安全战略浅谈

文/王红阳　服务产品部

随着业务的不断增长，企业、组织IT的依赖性更大，IT比以往更复杂。在业务的核心竞争力方面，企业、组织已经投入了很大的精力。但安全威胁永无止境、安全漏洞不断披露、新兴攻击手段变幻莫测，这一切已足以使得企业、组织在安全保护方面疲惫不堪。

当今的监管环境日益严格，在财务、IT方面的任何一个疏忽都有可能造成非常严重的灾难，它可能使得一个企业、组织名誉扫地，也可能使得相关负责人引咎辞职。

安全战略是企业、组织保证业务/IT相一致并顺畅运行的灵魂，领导层应对安全战略负责。制定企业安全解决方案的长远发展路线，必须从安全战略的角度出发。

在安全战略方面，应当做好如下的工作：

对信息安全的态度

领导层对信息安全的积极肯定、重视坚持的态度会给企业、组织的信息安全工作带来很大的好处，也可以在一定程度上提升全员的信息安全意识水平。在很多安全体系框架的关键成功因素部分，“领导层批准”放在了第一位，由此可见其影响力及重要性。

信心

越清楚的了解、越清晰的知道，就越能增强信息安全的信心。如果领导层自身在信息安全方面就缺乏信心，有可能会失去自己的判断力，不能从本质上看问题，片面听取部分厂商的建议，结果只能是逐渐的从安全项目中吸取教训。长此以往，信心会越来越少。

安全认知

外部威胁与内部威胁不断发生变化，新的合规要求也不断出现，做好安全工作，抵抗内外部威胁、保持合规是一项全员的工作，需要做好安全认知。从“听说”到“见到”，再到“体验”，这需要很长的过程，所以安全认知要提早做、不断做、生动化。

风险评估与合规

随着企业、组织对安全的理解越来越深入，很多独立的风险评估部门、合规监管部门、内部审计部门相继成立，这在一定程度上也反映了企业、组织的信心和态度。

ISO 27001 接受度

在信息安全领域中，ISO 27001提供了一个非常好的规范。通过ISO 27001认证是企业、组织安全工作做好的认可，依照ISO 27001建立信息安全管理体系是企业、组织安全成熟度不断提高的表现。

安全技能与专家

解决安全问题仅仅有态度还不够，还需要对应的技能，这包含团队技能、个人技能、专家技能。领导层应重视安全技能的培养，也要维持专业的专家顾问团队，为企业、组织的信息安全工作出谋划策。

安全投资

相比前几年，安全投资已经在加大。如果领导层仍保持“安全投入产出比是多少”的过时观点，将对企业、组织的信息安全工作极为不利。因为安全不同于IT的其他方面，出了问题往往都是致命的，对公司的品牌、领导层的口碑、客户关系都会造成深远的影响。所以在新的时代应树立新的安全观点，由“安全投入产出比是多少”转为“投入多少钱最为合理”，这才是正确的做法。

安全支出

毫无疑问，购买好的安全产品、使用好

的安全服务、培养好的安全人员都需要很大的安全支出，将钱花在最关键的地方来解决关键的问题，这也是领导层所要考虑的。

外包与协作

不同企业、组织由于安全要求和文化风格的不同，信息安全工作会采取独立完成、与合作厂商协作、部分外包、完全外包等多种方式。领导层应在企业、组织文化的基础上，综合考虑这几种方式的利与弊，选择最可靠的、最实用的、最放心的方式。

安全体系为安全战略服务。安全体系一般包含安全组织体系、安全管理体系、安全技术体系。

■ 安全组织体系中，要建立组织、明确职责、提高人员安全技能、重视雇用期间的安全、要与绩效结合。常见的组织架构分为三层：领导层、管理层、执行层，由上至下和同一层的协调关系、职责授权需要确定。

■ 在安全管理体系中，以安全策略为主线，落实安全制度和流程，对记录存档。绿盟科技从最佳安全实践出发，将安全管理体系中的过程动态化、持续化，包含风险评估程序、企业安全计划、安全项目管理、运行维护监控、安全审计程序、持续改进计划等，真正与企业的安全建设和安全保障过程结合起来。

■ 在安全技术体系中，将多种安全技术相结合，包含准备、预防、检测、保护、响应、监控、评价等。面对不断出现的新兴威胁，需要多种安全技术的协调与融合。

安全体系像是企业、组织的免疫系统，体系的不断完善、组织/人员的尽职尽责、全员的风险预警意识，才能真正做到主动管理风险。

在制定和实施企业安全战略时，应当遵循以下原则：

■ **安全战略必须满足业务需求**。企业处于一个不断变化的业务环境之中，因此企业 IT 解决方案应当能够满足不断变化的企业业务需求，企业安全战略应该能够随着企业对 IT整体解决方案的变化而变化，确保企业业务顺畅的运行。

■ **安全战略必须适应企业文化**。安全战略的实施很大程度上依赖于人的行为习惯，能否与企业文化相适应是新的安全战略顺利实施的非技术性关键因素。

■ **安全战略必须全体动员参与**。在制定与实施安全战略时，必须使整个企业都参与进来，而不仅仅限于管理层，还要确切的了解安全战略从哪个层面得到多大的支持。

■ **安全战略具有长期性**，也面临很多的不确定性，因此企业在制定和实施IT安全战略的时候，除考虑满足功能性需求以外，还应该最大程度规范化整个实施流程，确保实施的可延续性。

电信IP骨干网络异常流量及其检测

文/王卫东　产品市场部

随着电信IP网络带宽的不断扩大，网络上的流量也在成倍的增长，流量的成分也越来越复杂。经济利益的驱动和网络攻击技术门槛的降低使得异常流量也呈爆炸式的增长趋势。电信IP网络异常流量分析也成为一个重要课题。

1 异常流量的分类

异常流量的分类有很多方法，但是最切合实际的方法是从网络运维人员的视角进行分类。从运维人员的角度来看，具有以下三个特征之一的流量都属于异常流量：

(1)对网络的正常运行不利，影响网络的正常服务。

(2)损害组织机构自身经济利益。

(3)违反现行法律法规的流量。

注意，这里运维人员对异常流量的判断是主观的，并不仅仅局限于蠕虫传播和DDoS攻击等这些具有普遍危害性的流量。例如对于某些网站，会非常反感竞争对手的恶意下载以及搜索引擎爬虫的频繁访问。从第三方来看，这样的访问是一种正常网络访问，而这些访问会造成网站服务器性能下降，甚至无法为真正的用户提供服务。运维人员自然会将其视为异常流量。按照这样的分类，异常流量包括：

- 网络层DDoS攻击：SYN Flooding、ACK Flooding、ICMP Flooding、UDP Flooding等。
- 应用层DDoS：CC攻击、传奇攻击、SIP攻击、DNS攻击等。
- 蠕虫传播。
- 二层攻击：ARP Flooding、ARP欺骗等。
- P2P下载流量。
- 控制层攻击：针对路由协议的攻击，如BGP攻击。
- 用户自定义访问行为：如竞争对手或搜索引擎爬虫的频繁访问、非法VoIP、宽带私接用户、垃圾邮件等。

2 异常流量检测技术

异常流量的检测分为两个过程：流量数据的采集，流量数据的分析。数据采集的方法大体上分为两类：流量镜像(SPAN)和流级数据(Netflow或sFlow)采集。(注：有文章把SNMP也当作一种流量采集的方法。由于该方法采集的数据粒度太粗，可供分析的信息也很少，因此实际上很少有人把它作为主要的分析手段，仅仅作为一种辅助的方法，采集到的数据只作为参考。)数据的分析方法上也可以分为两类：基于数据包信息的特征检测和行为分析)和基于包头信息(或聚合后的包头信息)的统计分析。由于流级数据本质上是一种聚合后的包头信息，不包含应用层及数据净荷（Payload）信息，所以对于流级数据，无法使用第一种检测方法。

下面用两个表格对两种采集方式以及检测方法做一个简单比较。

	镜像数据采集	流级数据采集(Netflow, sFlow)
设备支持能力	部分设备支持流量镜像	Cisco, Juniper, Huawei, Foundry等主流厂商的设备支持
数据时间特性	时间粒度可以很细，实时性较好	时间粒度中等，有延迟
数据采样支持	不支持采样， 采集设备可以自行采用	支持采样
信息丰富度	包含7层协议信息，但缺少路由相关的信息，如AS, Next hop	sFlow包含部分7层协议信息，Netflow和sFlow均包含路由信息
对网络的影响	对设备性能有一定影响，采集设备嵌入式部署时影响网络的运行，部署完毕后影响消除，但存在单点故障隐患	在采样输出情况下，对设备性能影响很小，无须嵌入式部署，无须改变网络拓扑
部署的灵活性	缺乏灵活性和可扩展性	可扩展性好，对部署位置限制无严格限制，只需IP可达
部署的成本	往往需要在多个位置部署，因此成本较高	一台设备可以采集多个设备上的流量，因此成本较低
适合部署位置	接入层或汇聚层	通常是在核心层
适用环境	链路带宽在千兆以下，流量较小的网络环境	适用与各种带宽的网络环境中

	基于数据包全部信息的检测	基于统计分析的检测
适用数据源	镜像数据	镜像数据，流级数据
基本原理	深度包检测， 特征匹配， 会话重组	按照不同的统计规则对包数和字节数以及流数进行统计，对比相应的基线数据
检测效率	较低	较高
准确性	准确	统计意义上的准确，即在大流量环境下
适用环境	流量较小的网络环境	流量较大的网络环境

3 基于统计分析的异常流量检测

从上述比较可以很容易看出，基于统计分析的异常流量检测方法更适用于运营商骨干网络。因此本文着重介绍这种检测方法的原理以及一些检测指标。所谓的检测指标，就是一个统计规则。例如，SYN Flooding 指标，就是把所有TCP-flag 为SYN 的流量统计出来。

3.1 异常流量的检测原理

一言以蔽之，异常流量检测的原理就是比较检测指标实际测量值和基线值的大小，前者大于后者则产生告警。由此可见检测指标的选取及计算以及基线的生成是异常流量检测最关键的两个过程。为了使这两个过程更加科学，首先要对检测指标和基线做一下分类比较。

检测指标	定义	适用基线的指标		
		固定基线	周期性基线	非周期性基线
流量相关型	只有检测指标测量值达到相当大的时候才会触发告警，若指标值相对较小，则不告警。	无	总流量，Web应用流量	各种泛洪攻击
流量不相关型	即使检测指标测量值没有达到很大流量，但是已经累积了一定次数，仍然要告警。	ICMP请求/应答比	无	蠕虫传播，端口扫描，P2P通讯

3.2 基线算法

3.2.1 固定基线

固定基线是一条水平直线，并无算法可言，通常是根据经验或是实验测量的结果得来。例如ICMP 请求响应比（ICMP Req/Rsp）在正常情况下大约为10:1。有ICMP 攻击的时候会远远高于这个值。

3.2.2 动态周期性基线

周期性基线通常是根据历史数据计算得到的，通常是一个单周期数据轮廓线。这条曲线由若干数据轮廓点组成。每个轮廓点代表一个采样时点。例如，假设基线周期为24小时，采样时点间隔为5分钟，则轮廓线由288个轮廓点组成。第N个轮廓点的值都是由一组同为第

N个采样时点的实际测量值（历史数据）计算得来的。一个新的实际测量值如果没有超过基线范围，则取代那组历史数据中最陈旧的一个，用来计算新的轮廓值。如果一个新的测量值超过基线范围，则被丢弃，不参与新轮廓值的计算。如此循环往复，基线则始终保持在动态的变化。

计算轮廓点的具体方法有很多，最常用的有三种：算术平均、加权平均、置信区间。为了增加基线的准确性，还可以多采用一些历史数据，并采用混合算法。也就是在历史数据学习期的前段采用算术平均，生成初步的基线。然后继续积累历史数据，对所有这些更多的历史数据采用加权平均和置信区间算法。这样既满足了实际应用系统对缩短学习期的要求，又兼顾了基线计算准确性的要求。

时间	[illegible]	[illegible]	[illegible]	[illegible]	……	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
星期一	4.3	3.5	5.6	6.1	4.2	2.9	3.2	4.5	5.1	6.7
星期二	2.5	2.8	5.3	5.6	6.2	2.8	2.9	3.1	6.8	7.3
星期三	4.9	3.8	6.6	7.3	5.6	2.9	5.3	3.6	5.9	5.3
星期四	4.5	4.9	5.6	2.9	5.6	2.9	6.1	4.2	2.9	2.5
星期五	3.1	4.7	2.8	5.3	5.6	6.2	3.6	5.9	5.3	2.9
星期六	2.8	5.3	3.4	2.5	2.8	5.3	5.6	5.6	2.9	5.3
星期日	5.3	3.8	4.1	5.6	5.6	2.9	3.5	5.6	6.1	2.9
基线值	5.5	5.8	7.2	7.8	6.7	6.7	6.5	6.5	7.3	7.8

表 3.1 周期性基线历史数据的选取

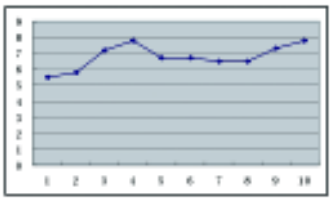


图 3.1 周期性基线示意图

3.2.3 动态非周期性基线

动态非周期性基线与周期性基线相比，最大的区别是历史数据的选取方法。非周期基线的历史数据是当前时间向前推移若干个采样时点的实际测量值。向前推移的时间范围称为时间窗口，因此这种基线也称为移动窗口基线。计算轮廓点的方法同样有前述的三种（即算术平均、加权平均、置信区间）。以表3.2所示为例，每一个格子表示一个时间片，从当前时间片向前推移5个时间片，选取5个数据，计算当前时间片的基线。这5个时间片构成了一个不断移动的时间窗口。

																			当前时间片
…	4.3	3.5	5.6	6.1	4.2	2.9	3.2	4.5	5.1	6.7	2.9	5.6	2.9	6.1	4.2	2.9	2.9	3.5	…
…	…	…	…	…	…														
	4.3	3.5	5.6	6.1	4.2														
		3.5	5.6	6.1	4.2	2.9													
			5.6	6.1	4.2	2.9	3.2												
				6.1	4.2	2.9	3.2	4.5											
					4.2	2.9	3.2	4.5	5.1										
						2.9	3.2	4.5	5.1	6.7									
							…	…	…	…	…								
													2.9	6.1	4.2	2.9	2.9		
														6.1	4.2	2.9	2.9	3.5	

表 3.2 移动窗口基线历史数据的选取

3.2.4 两种动态基线的比较

	周期性基线	非周期性基线
历史数据选取	多个不同的基线周期内相同的采样时点的一组数据，可以概括为“垂直选取”	以当前时间为向前推移若干个采样时点，可以概况为“水平选取”
计算方法	如果数据样本较少，建议采用算术平均法。如果样本较多，可以采用加权平均、置信区间或混合算法。	建议采用置信区间或混合算法。

3.3 异常流量检测指标

异常流量检测的另一个关键过程就是检测指标的选取和计算。下面按照异常流量的类型，分别介绍各种检测指标。

3.3.1 网络层 DDoS 的检测指标

异常种类	检测指标（统计方法）
SYN Flood	TCP-Flag=SYN，包个数=1
ICMP Flood	协议号=0，目的端口=0，流量占比
	ICMP 请求响应比
UDP Flood	协议号=6，流量占比
	协议号=6，进入流总流量比
Stream Flood	TCP-Flag=ACK, ToS=0x08, 协议号=17，总流量
TCP-flag Null	TCP-Flag=0，总流量
PSH&ACK 攻击	TCP-Flag=PSH&ACK
IGMP Flood	协议号=2，目的端口=0
Reset Flood	TCP-Flag=RST，包个数=1
Connection Flood	单位时间内TCP 连接数目的变化
其它TCP-Flag异常	有些文献上提出有9种左右的TCP-Flag异常
空链接攻击	源地址=目的地址，TCP-Flag=SYN
伪造源地址或端口扫描	源地址的随机度（分散度）突然增加，IP地址的个数突然增多

3.3.2 应用层 DDoS 的检测指标

异常种类	检测指标（统计方法）
DNS Query Flood	协议号=6或17 端口号=53
HTTP Get Flood	目的端口号=80,8000,8080,449,平均每个流所含包数

3.3.3蠕虫传播及某些行为异常的检测指标

异常名称	异常名称检测方法
Code Red Worm	目的端口=80,协议类型=TCP,包数=3,字节数=144,总字节和总包数
硬盘杀手	目的端口=137,协议类型=UDP,字节数=78,总字节和总包数
2003蠕虫王	目的端口=1434,协议类型=UDP,字节数=404,总字节和总包数
冲击波	目的端口=135,协议类型=TCP,字节数=48,总字节和总包数
冲击波杀手	目的端口=2048,协议类型=ICMP,字节数=92,总字节和总包数
振荡波	目的端口=445,协议类型=TCP,字节数=48,总字节和总包数
蠕虫传播	外网地址频繁访问内网地址的NetBIOS端口（TCP和UDP port 137,138,139,445）
	目的IP和目的端口突然增加,且包数和字节数分别相同
异常行为	telnet/ssh/rlogin 的源，目的地址相隔很远
异常数据包	目的端口=23、53,包大小>1000Byte
伪造源地址	源地址∈黑IP地址空间

3.3.4 P2P 流量的检测指标

P2P 流量有如下 5 个特点：

1)大流量的主机分布相对有限：通常10%的IP地址的流量占到总流量的 90%。这样可以找到 P2P 通讯的主机范围

2)并发连接数高且有突然增大的情况：进行P2P 下载的主机，一定会有很高并发连接数

3)端口变化率：由于多数P2P下载软件使用了“端口跳跃”技术，因此在 P2P 下载过程中，主机端口会不断变化

4)基于拓扑分析的特征：由于P2P下载的端点都会用一些缺省的端口与其它端点通讯，通过分析流记录可以找到这些端点间的拓扑关系以及用来确认该主机是否为P2P端点的特异值，当特异值达到一定水平，即可确认该主机为 P2P 端点

5)大量空闲连接：P2P 端点通常都会有很多空闲连接，在流记录上就表现为很多流量很少的记录。

根据上述5个特点，我们可以重点检测流量排名前10% 的IP 地址的并发连接数以及IP端口变化率，并把是否有P2P客户端默认端口通讯以及是否有大量的流量很小的连接作为附加判断条件。

3.1 异常流量检测实例

在电信运营商的实际网络中，利用上述这些检测算法，能够有效的检测到异常流量。在图3.2 中，我们可以看到，有三个正在持续的告警事件，被攻击IP是同一个目的地址。实际上这是同一告警行为同时被三个不同的检测算法检测到了。这三个告警不仅从不同的角度全面展示出攻击的行为特征，也互相印证了各自对攻击检测的准确性。

图 3.2 异常流量告警图示

图 3.3 P2P 流量告警

值得特别指出的是，P2P流量虽然是一种正常的网络业务，但由于这种业务对带宽资源的严重占用，在很多场合，都被当作一种异常流量来看待。因此对P2P流量的检测是很多网络维护人员非常关心的问题。上述P2P检测算法的准确性，在运营商实际网络中可以准确地检测到多种P2P流量。在图3.3中，可以看到，实际网络中有大量的P2P流量存在。

4、总结

本文从异常流量分类入手，给出常见的异常流量检测技术对比分析，最后详细介绍了基于流技术的采集与统计分析的异常流量检测原理和检测方法。

数据库安全初探

文 / 孙平　服务产品部

数据库安全模型和等级

数据库系统安全模型是对数据库系统的安全需求和安全策略的抽象，当前主要的模型是访问控制策略模型，用于描述系统中数据的保密性和完整性，常用的数据库安全模型如下：

自主访问控制策略模型（DAC）

MS SQLServer、Oracle、DB2、Informix 支持 DAC 模型。

具有一定的保护能力，采用的措施是自主访问控制和审计跟踪。

用户对不同的数据对象有不同的存取权限，而且还可以将其拥有的存取权限转授给其他用户。

强制访问控制策略模型（MAC）

Trusted Oracle 7、Oracle8i/9i/10g/11g、DB2 9、Informix Dynamic Server 11 都支持 MAC 模型。

在强制访问控制系统中，客体（各种逻辑数据对象）被赋予不同的安全标记属性，或称为“密级”（security level）；主体（用户或用户进程）根据访问权限也被分配以不同的许可级（security level）。主体根据一定的安全规则访问客体，以保证系统的安全性和完整性。

在 MAC 机制中，存取权限不可以转授，所有用户必须遵守由数据库管理员建立的安全规则，其中最基本的规则为“向下读取，向上写入”。即只有当主体的密级不小于客体的密级并且主体的范围包含客体的范围时，主体才能读取客体中的数据；只有当主体的密级不大于客体的密级，并且主体的范围包括客体的范围时，主体才能向客体中写数据。有利于保证数据库的高度安全性，使得数据库中的信息流单向不可逆，保证了信息流总是低安全级别的实体流向高安全级别的实体，因此避免了在自主访问控制中的敏感信息泄漏的情况。

数据库系统的多级安全模型是以多级关系数据模型为基础，在数据库中的所有主体（用户、进程）和客体（文件、数据）都被分配了安全标签（Label Security），安全标签标识一个安全等级。访问控制执行时对主体和客体的安全级别进行比较，例如数据库 PL/SQL 程序包以“秘密”的安全级别运行，假如程序包在运行时被攻击，攻击者在目标数据库中只能以程序包的“秘密”安全级别进行操作，它将不能访问数据库中安全标签为“机密”以及“绝密”的数据。

Oracle Label Security 最早在 Oracle8i 中引入，并在 Oracle 10g 中得到了极大加强。Oracle Label Security 是内置于 Oracle 数据库引擎中的过程与约束条件集，该数据引擎实施对在单个表或整个模式上的“行”级访问控制，其对查询的修改是透明的，当 Oracle9i 数据库在解析各个 SQL 语句时，它也检测各个表是否受到某个安全策略的保护，根据该用户的访问权限，Oracle9i 数据库向该语句的 WHERE 子句中添加安全性谓词。因为这些都发生在数据库引擎的内部，所以不管该 SQL 语句的来源如何，用户都不可能绕过该安全性机制，读取该用户没有访问权限的数据或程序包。

基于角色的访问控制策略模型（RBAC）

Oracle8i/9i/10g/11g、DB2 9、Informix

Dynamic Server 11、MS SQLServer 支持RBAC 模型。

RBAC 核心模型包含了 5 个基本的静态集合，即用户集(users)、角色集(roles)、特权集（perms)（包括对象集(objects)和操作集(operators)，以及一个运行过程中动态维护的集合，即会话集(sessions)。

国内流行的 MS SQLServer 、Oracle、DB2、Informix 数据库都达到了C2级安全标准，其中Oracle、Informix–Online Secure数据库还正式通过了 NCSC B1 级安全标准的测试，这是目前国内商用数据库的最高安全级别，随着企业对安全需求的提高，支持多级安全的B级数据库正在成为新的安全热点。

数据库安全等级可以参照在可信计算机系统评测标准(TCSEC)橙皮书定义的安全等级：

1)无保护级（D级）

2)自主保护级(C级)

自主安全保护级(C1级)：要求用户在使用前必须登录，但不能控制进入系统的用户的访问级别等。

控制访问保护级(C2)：以用户权限为基础，进一步限制用户执行某些系统指令。C2级系统还采用了系统审计。

3)强制保护级(B级)

标记安全保护级(B1级)：它是支持多级安全(比如秘密级和绝密级)的第一个级别，提供安全策略模型的非形式化描述、数据标记以及命名主体和客体的强制访问控制，并消除测试中发现的所有缺陷。

结构化保护级(B2级)：要求计算机系统中所有对象加安全标签，而且给设备(如工作站、终端和磁盘驱动器)分配安全级别，例如用户可以访问一台工作站，但可能不允许访问装有人员工资资料的磁盘子系统。

安全区域保护级(B3级)：要求用户工作站或终端通过可信任途径连接网络系统，这一级必须采用硬件来保护安全系统的存储区。

4)验证保护级(A级)

这是橙皮书中的最高安全级别，这一级有时也称为验证设计(verified design)。A级附加一个安全系统受监视的设计要求，合格的安全个体必须分析并通过这一设计。另外，必须采用严格的形式化方法来证明该系统的安全性。而且在A级，所有构成系统的部件的来源必须安全保证，这些安全措施还必须担保在销售过程中这些部件不受损害。例如，在A级设置中，一个磁带驱动器从生产厂房直至计算机房都被严密跟踪。

在上述安全等级中，B1和B2的级差最大，因为只有B2、B3和A级系统才是真正的安全等级，才经得起程度很高的严格测试和攻击。

数据库安全机制

数据库安全机制包括身份验证(authentication)、授权(authorization)、访问控制（Access Control)、数据库加密(DB Encrypt)、推理控制(Inference Control)、隐私保护(Privacy Protection)、数据库监控(DB Monitor)等，由于篇幅所限，下面简要介绍一下大家较为陌生的数据库推理通道和推理控制。

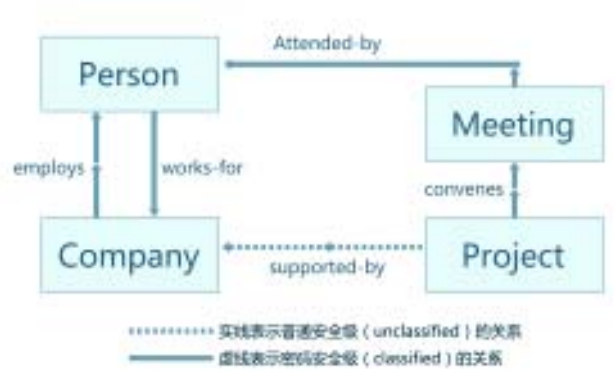
推理通道和推理控制

数据库推理通道(Inference Channel)指用户通过合谋、拼凑等方式从合法获得的低安全分类级别数据，绕过强制访问控制机制，

推导出高安全分类级别的数据，造成未经授权的信息泄露。常见的推理通道有以下4种：

1．执行多次查询，利用查询结果之间的逻辑联系进行推理。用户一般先向数据库发出多个查询请求，这些查询大多包含一些聚集类型的函数（如合计和平均值等）。然后利用返回的查询结果，在综合分析的基础上推断出高级数据信息。

2．利用不同级别数据之间的函数依赖进行推理分析。数据表的属性之间常见的一种关系是“函数依赖”和“多值依赖”。这些依赖关系有可能产生推理通道，如下图所示：



3．利用数据完整性约束进行推理。例如关系数据库的实体完整性要求每一个元组必须有一个唯一的键。当一个低安全级的用户想在一个关系中插入一个元组，并且这个关系中已经存在一个具有相同键值的高安全级元组，那么为了维护实体的完整性，DBMS会采取相应的限制措施。低级用户由此可以推出高级数据的存在，这就产生了一条推理通道。

4．利用分级约束进行推理。一条分级约束是一条规则，它描述了对数据进行分级的标准。如果这些分级标准被用户获知的话，用户有可能从这些约束自身推导出敏感数据。

目前常用的推理控制方法可以分为两类：

在数据库设计时找出推理通道：主要包括利用语义数据模型的方法和形式化的方法。这类方法都是分析数据库的模式，然后修改数据库设计或者提高一些敏感数据的安全级别来消除推理通道。

在数据库查询期间消除推理通道：包括多实例方法以及在检测到潜在的推理通道时就拒绝或修改查询的方法。

数据库安全原则

数据库及其承载的应用系统需要遵守一些基本的安全原则：

隔离原则（Compartmentalize）

隔离原则的目标是分解并减少攻击面，例如采用防火墙、最小特权帐户、最小特权代码等。采用隔离原则需要考虑如何取舍系统内容，预测攻击时可以访问的资源，以提供限制潜在损害的措施。

最小特权原则（User Least Privilege）

最小特权的实质是任何实体（用户、管理员、进程、应用和系统等）仅拥有该主体完成规定任务所必须的权限，此外没有更多的权限。

最小特权原则可以尽量避免将系统资源暴露在攻击之下，减少因遭受攻击而受到的损失。

纵深防御原则（Defense in Depth）

纵深防御原则不仅依靠安全机制和安全服务的组合，而且通过建立协议层次、信息流向等纵向结构层次，构筑多种有效防御措施阻止攻击并发出警报。

用户输入不信任原则（Do Not Trust User Input）

用户输入不信任原则的依据是用户输入是对目标系统进行攻击的主要武器，因此，需要对输入保持高度警惕，直到确认没有恶意。

关卡检查原则（Check at the Gate）

关卡检查原则强调尽早实施认证和授权，将攻击阻止在第一道门槛之外。

失效保护原则（Fail Securely）

失效保护原则意味着在系统失效时，不能让敏感数据失去保护被任意访问，失效时的返回信息应当友好且不泄露系统内部详细信息。

最弱连接安全化原则（Secure the Weakest Link）

最弱连接安全化原则要求强化系统最薄弱环节的安全监测和缓解措施，安全人员应意识到系统弱点，以免危急整个系统的安全。

建立默认安全原则（Create Secure Defaults）

需要为系统的安全措施建立默认的安全配置基线，包括默认账号、默认权限、默认策略等，这也是保持系统简单化的重要方法。

减少攻击面原则（Reduce Your Attack Surface）

减少攻击面的具体措施是去除或禁止一切不必要的模块、协议和服务，其目的是减少攻击可以利用的漏洞，如删除不必要的数据库组件、例子数据库、数据库账号等。

技术动态

绿盟科技在国家信息中心“网络安全技术培训会”上发表主题演讲

4月14日至16日，由国家信息中心网络安全部举办的国家经济信息系统“网络安全技术培训会”在扬州举行。国家信息中心系统领导，全国30多个省、市信息中心工程师参加了技术培训大会。培训会旨在进一步提高国家经济信息系统各单位的网络安全技术水平，更好地承担重要信息系统的信息安全保障任务。

绿盟科技作为业界最早开展安全服务的专业企业，应邀参加了此次培训。培训会上，绿盟科技服务产品部高级安全顾问孙铁向与会的代表做了主题为“信息安全等级保护”的演讲，演讲从安全服务角度、等级保护设计实施要点、等级保护目标等几个方面，阐述了绿盟科技在信息安全等级保护方面的“方法论”，博得与会代表的一致好评。

“专攻术业，成就所托”。绿盟科技一直以“巨人背后的专家”为己任，致力于网络安全事业，并在国内率先开展专业安全服务业务，建立了完善的专业安全服务体系(NSP-S)，而且具备国内最高级安全服务资质，连续多年被评为“值得信赖的安全服务品牌”。

信息安全等级保护自2007年6月正式全面启动以来，已经把信息安全等级保护制度落实到信息安全规划、建设、评估、运行维护等多个环节，以促使信息安全保障状况得到根本改善。凭借在信息安全界多年专业服务的经验积累，绿盟科技将积极推动我国信息安全等级保护体制的完善和应用实践，并为持续推进我国信息安全产业的快速发展，发挥模范带头作用。

绿盟科技成为国家级火炬计划项目承担单位

绿盟科技最近获得了科技部火炬高技术产业开发中心颁发的“国家火炬计划项目证书”，正式成为国家级火炬计划项目承担单位。绿盟科技拳头产品“冰之眼网络入侵保护系统”被列入国家火炬计划项目序列。

火炬计划是一项发展中国高新技术产业的指导性计划，于1988年8月经国家批准，由科学技术部(原国家科委)组织实施。火炬计划的宗旨是实施科教兴国战略，贯彻执行改革开放的总方针，发挥我国科技力量的优势和潜力，以市场为导向，促进高新技术成果商品化、高新技术商品产业化和高新技术产业国际化。其要求被列入火炬计划的项目，必须具有我国自主知识产权，技术水平在国内同行业中居领先地位，项目市场前景好，产业规模大，有较强的市场竞争能力和较大的市场覆盖面，在同行业中起到示范带动作用。

绿盟科技成为国家级火炬计划项目承担

单位，一方面证明了绿盟科技在安全产品与技术研究方面已经处于国内领先地位，同时

也标志着国家对于绿盟科技研发、创新实力的认可和支持。绿盟科技将继续坚持创新和专业的精神，并以“巨人背后的专家”为己任，致力于信息安全建设和安全产业发展，力争做出更大的贡献。

绿盟科技应邀对利比亚国家电信公司进行培训

4月中旬，绿盟科技应大阿拉伯利比亚人民社会主义民众国（The Great Socialist People's Libyan Arab Jamahiriya）国家电信企业和国内通信设备制造商的特别邀请，本着对外合作交流和技术支持的目的，对利比亚的电信项目进行了为期10天的网络安全技术培训。

培训课上，绿盟科技安全顾问分别针对网络安全、信息安全、安全协议、安全架构、安全事件分析、日常安全习惯、网络安全设备等信息安全科普知识与攻防技术进行了系统地讲解和认真的培训辅导。课间通过讲师“授业、解惑”，学员积极提问、细致笔记、亲自操作以及互动交流，使得培训收到了很好的效果。由于时间缘故，一些课程做了精简，学员们迫切希望进一步来中国接受更加系统的安全培训。

进入2008年以来，绿盟科技极光远程安全评估系统先是获得了国际权威的西海岸认证，证明绿盟科技产品已达到国际水平；接着是参加美国旧金山RSA大会，亮相国际舞台；本次受邀为利比亚电信企业做培训，再一次证实了绿盟科技专业培训服务在国际市场的品牌影响力。而这些举动，均标志着绿盟科技已经迈出了进军国际市场的坚实步伐。

绿盟科技参加中国网通“IDC 增值产品与网络信息安全产品交流会”

6月3日上午，绿盟科技应邀出席了由中国网通在京举办的“IDC 增值产品与网络信息安全产品培训及交流会”，公司行业技术部高级安全顾问刘炅代表公司发表了题为《运营商宽带互联网安全增值》的主题演讲。演讲从运营商宽带互联网安全增值业务设计、DDoS 流量清洗安全增值、安全增值合作经验三个方面阐述了绿盟科技在IDC增值与网络安全方面的经验积累和方案部署。

绿盟科技在运营商IDC产品和解决方案部署方面积累了丰富的经验。在增值产品方面，尤其对资源预留、安全基线评估制定 、

流量监控 、安全事件通知 、流量分析报告、流量清洗、攻击防护报告尤其有深入的研究和实战部署经验。宽带互联网安全增值，赢在“差异化”，绿盟科技秉承专业和创新的精神，

在去年已经在业界率先推出了DDoS流量清洗安全增值的“安全岛”防护方案，而随着绿盟科技产品和解决方案的进一步研究开发，将会更加科学、先进、广泛地应用在运营商宽带互联网安全增值的实践中。

我们相信，随着运营商安全增值方案的逐步推广及众多方案模块的陆续推出，绿盟科技不但将为运营商打造绿色、安全的业务网络环境，还将携手运营商一同将这些专业的解决方案与服务带给更广泛的用户群体，为运营商的业务转型贡献一份力量。

产品动态

绿盟科技两款“黑洞”高端流量分析新品成功上市

经过近一年的紧张研发和测试，2月份绿盟科技成功地推出两款高端流量分析产品—“黑洞”流量分析系统 NTA SP2000 和 NTA SE2000。

作为绿盟科技“黑洞”品牌下的一个重要产品线，“黑洞”流量分析系统是一款基于流技术（如Netflow、sFlow等）的骨干网流量分析产品。主要功能包括异常流量检测和流量的统计分析。它既可以作为流量分析产品单独部署，也可以作为异常流量检测产品与黑洞的 Defender 产品一起构成流量清洗与净化的解决方案进行部署。

与业界同类产品相比，“黑洞”流量分析系统具有四大特点：算法先进、结构灵活、性能强大、即插即用。算法先进性体现在基线的全自动生成和可检测异常流量种类丰富两个方面，异常检测算法的种类超过50种，覆盖几乎全部攻击型的异常流量。而其系统的软件架构采用结构化设计，可以动态加载检测算法，具有很强的灵活性。黑洞流量分析系统的数据处理能力也非常强大，每秒钟可以处理超过8万条记录。而系统上线也只需要非常简单地配置操作，即插即用。

SP2000 主要适用于运营商环境，包括路由分析功能以及与路由和自治域相关的流量分析；SE2000主要适用于企业办公网和校园网环境中，主要功能与 SP2000 相同。二

者在流量数据处理性能、动态流量建模、异常检测精度、检测算法动态加载技术、攻击监控和分析报告、可靠性等方面均做了很多优化，功能特性指标显著。

绿盟科技“黑洞”流量分析系统具有业内非常多的成功应用案例，而高端新品的成功上市，将进一步提升用户对骨干网络流量的监控能力，也使“黑洞”流量清洗解决方案更加完善。

绿盟科技冰之眼入侵检测、防护系统再获荣誉

绿盟科技冰之眼入侵检测、防护系统近日再次获得《网管员世界》杂志社2007年度编辑选择奖。编辑选择奖是《网管员世界》杂志社针对业内主流产品，针对产品技术领先性、用户使用情况、厂商售后服务、市场综合表现等方面，通过行业用户调查以及专家组评审后选出的，代表了《网管员世界》对国内安全产品的肯定与推荐。

随着网络安全形势的迅速变化，绿盟科技依靠独立自主的研发力量，在吸取国外先进安全产品经验的基础上，发挥熟悉国内市场的优势，不断推出、改进自己的安全产品，并在产品推广的同时，努力做好扎实的售后服务工作，从而在广大国内用户群中建起了良好的用户口碑，并一步步赢得了用户们的信任。绿盟科技的冰之眼网络入侵检测/保护系统在数年间依靠良好的特性为广大用户服务，受到广大用户的肯定，连续多年在国内权威机构的评测中独占鳌头，成为国内安全产品的著名品牌。

绿盟科技极光远程安全评估系统“漏洞管理系列”正式上市

6月6日，绿盟科技远程安全评估系统新品—极光“漏洞管理系列”正式上市。

极光“漏洞管理系列”产品可以对网络风险进行全方位管理和分析，网管员通过此模块可以对所有信息资产设备进行资产风险管理。对于大规模网络用户，由于网络资产繁多、IP地址记忆非常繁琐，则通过资产管理与用户组织结构或网络拓扑结构的紧密结合，以规范的命名方式统一对网络资产进行管理。

目前政府、事业单位、金融企业、能源企业和通信运营商等用户都已经逐步重视漏洞的检查工作，通过定期的网络扫描将风险定位。但是由于网络环境的复杂性，以及大量的主机数量，导致漏洞修补给网管员带来巨大的工作量，可是没有漏洞修补的漏洞检查对解决整体资产安全没有根本的意义。

绿盟科技将先进的“漏洞管理”理念贯穿于整个产品实现过程之中，在国内首创了开放的工作流程平台，真正与资产相结合，完成发现资产漏洞、预警并解决漏洞的整套自动化过程。绿盟科技“漏洞管理系列”产品用户界面设计区别于原有的安全评估系统，从资产的角度出发，以新的工作流程对产品进行使用与操作，更加符合企业客户的漏洞管理需求。

市场动态

绿盟科技应邀出席中国政府CIO大会

3月13日，由中国信息协会信息主管（CIO）分会主办的“中国政府CIO大会”在中科院国家科技图书馆报告厅召开，旨在盘点2007年电子政务重要成果、展望2008年电子政务发展趋势、探索以CIO体制为核心的电子政务管理体制。绿盟科技作为拥有自主知识产权并一直追求创新和专业服务的企业级网络安全解决方案供应商，应邀出席了大会。

应主办方特别邀请，绿盟科技政府行业资深安全顾问代表公司发表了题为《等级保护建设面面观》的主题演讲。演讲从等级保护知识要点、建设方案的设计、建设实例、等级保护评测四个方面展开系统论述，精彩的演讲博得与会CIO专家一致好评。

政府信息化建设作为中国信息化市场中最大的市场和“一把手”工程，为政府信息化的推动起到了“破冰”作用。自2003年以来，我国电子政务发展一直保持着较高的增长势头，政府CIO概念也已经越来越得到业界的广泛认可和关注。鉴于绿盟科技在国内率先开展专业安全服务业务，建立了完善的专业安全服务体系(NSPS)，具备国内最高级别的安全服务资质，且连续多年被评为“值得信

赖的安全服务品牌”，会上荣膺为中国信息协会信息主管（CIO）分会理事单位。

绿盟科技出席全国电力信息化大会并获“电力行业信息安全优秀解决方案奖”

3月27日，由中国电力企业联合会主办的“2008年全国电力企业信息化大会”在昆明隆重召开。大会旨在推进电力信息化技术进步，配合电网企业、发电企业信息化规划的实施。

绿盟科技作为企业级网络安全解决方案提供商，应邀出席了该届电力信息化盛会。会上，行业技术高级安全顾问徐一丁代表公司做了题为《安全技术在电力行业等级保护中的应用》的精彩演讲。

本届大会是为推进电力行业信息化建设召开的阶段性工作年会。各发电集团公司、各电网公司、火力发电厂、水电厂和供电局的信息化主管领导、信息中心主任、相关生产部门负责人共计300多人参加了大会。许多参会代表对绿盟科技的演讲产生了极大的兴趣，会后主动找到绿盟科技与会代表进行了更加系统、深入的交流。

会上，绿盟科技凭借在国内电力行业的多年服务经历，对电力行业信息安全建设的深入理解，以及包括专业服务、客服支持、产品及解决方案部署等多方面的安全实施能力，荣膺“电力行业信息安全优秀解决方案奖”。

绿盟科技再获“最值得信赖的安全服务品牌”奖牌

4月22日，主题为“可信安全－生态融合”的第九届中国信息安全大会在京隆重召开。本次大会聚焦网络社会可信环境与秩序、企业业务与安全管理融合问题。作为特邀嘉宾，绿盟科技应邀出席了这次业界的盛会。

会上，绿盟科技服务产品部高级安全顾问孙铁代表公司在“安全融合–产品创新”主题分论坛发表了题为《信息安全等级保护》的专题演讲。演讲从等级保护概述、实施办法、目标以及绿盟科技在等级保护中所起到的积极作用等方面做了精彩论述，并得到与会代表的一致好评。

作为业界值得信赖的、领先的、专业的

安全解决方案提供商，绿盟科技以专业的安全服务协助用户设计、维护、改进安全战略，保持长期的竞争优势。历经8年专业服务实践，绿盟科技目前已形成了业界最完善的专业安全服务体系和独到的专业安全服务方法。

鉴于绿盟科技在中国率先开展专业安全服务业务，建立了完善的专业安全服务体系（NSPS），并具备国内最高级安全服务资质，绿盟科技再次荣获大会组委会颁发的“中国信息安全值得信赖的安全服务品牌”奖牌。这是绿盟科技第五次荣获该奖项。

绿盟科技喜获“移动运营商最佳安全服务奖”奖杯

2008年4月20日正值中国移动通信集团公司（简称“中国移动通信”）成立八周年之际，绿盟科技凭借长期以来参与移动运营商网络与信息安全体系建设的实践成果，以及专业的安全服务和有效的解决方案，喜获《通信产业报》和“通信产业网”联合颁发的“移动运营商最佳安全服务”奖杯。

中国移动成立八年来，每年都取得极大的发展，业务定位从移动通信专家，到移动信息专家的确立，都诠释着中国移动的蜕变。现在的中国移动不论是在话音业务收入，还是新业务推出、移动互联网的发展等方面都走在了行业前列。与此同时，中国移动的网络与信息安全建设也在不断的前行，从基于组织、管理、技术体系的安全建设规划，到各种安全试点的展开，再到各项安全建设内容的落地

等都为中国移动的业务发展提供了有力的保障。

2000年，在中国移动独立建司的时候，绿盟科技也于这一年正式成立。成立之初，绿盟科技完全以安全服务起步，通过自身的安全技术提供客户所不擅长的安全内容，逐渐形成了完整的安全服务体系。近年来，绿盟科技不仅为各级移动提供了安全预警、SOX缺陷修补、安全评估、安全加固等专业安全服务，而且还为北京、广东、新疆、湖北等多个省/市移动提供了安全策略设计、安全体系建设，安全域划分等安全咨询服务，并通过及时的应急响应服务来降低安全事件对业务运行所造成的影响。同时，绿盟科技凭借着长期的安全研究积累、对行业的深刻理解，受邀并协助中国移动进行了相关的安全规范编写，为中国移动的安全规划演进出谋划策。

现在，八岁的绿盟科技正积极投身于中国移动的各项安全建设中，为中国移动的业务网络安全事业贡献力量，矢志成为中国移动背后的安全专家。

绿盟科技参加日本国际网络通信展

6月9日至13日，一年一度的2008国际网络通信展览会（Interop Tokyo）在日本东京国际展览中心隆重开幕。Interop大会是展示网络通信领域最新技术和方案的盛会，也是国际前沿网络技术和产品的集中亮相舞台，云集了世界范围内的网络及电信方面的专业人士，堪称是该领域世界最大展会之一。出席本次展会的主要公司有Juniper、 Avaya 、Nokia、Cisco 、华为等大型跨国企业，以及NTT、NEC、Panasonic、Fujitsu等日本本土强势企业。

作为面向国际市场的企业级网络安全解决方案供应商和本届展会新锐参展厂商，绿盟科技携带业界领先的入侵检测/防护系统、远程安全评估系统、抗拒绝服务系统、内容安全管理系统、安全审计系统、内网安全管理系统等安全产品与解决方案应邀参加了此次盛会，并成为包括华为在内的仅有两家中国内地参会企业之一。

作为一个具有全球视野的中国公司，绿盟科技建立并维护的全球最大的中文漏洞库，已经成为业界广泛参考的标准；公司“极光”远程安全评估系统已经率先在亚洲获得英国西海岸实验室（West Coast Labs）的权威认证，成为获得此认证的全球第六款漏洞管理类产品。通过八年来不懈的努力，绿盟科技凭借专业精神、专业技能、专业流程和专业品质，向客户提供了高质量的产品与解决方案和专业服务。同时，在坚持一边自主创新，一边加强与国际交流的基础上，技术和产品已经达到国际领先水平，向国际市场迈出了坚实的步伐。

在参加Interop展会之前，绿盟科技已经在今年4月7日参加了在美国旧金山举办的全球顶尖的信息安全盛会— RSA Conference大会，向全球的合作伙伴展示了国际领先的网络安全技术、产品与解决方案。我们相信，随着绿盟科技国际化进程的步伐加快，必将让国际市场更加了解中国信息安全企业的雄厚实力。

NSFOCUS

THE EXPERT BEHIND GIANTS 巨人背后的专家

绿盟+ 技术版
与安全人士分享技术心得
Share technique experience with security professionals

Nsmagazine@nsfocus.com