



Campus-network Operation and Security Technologies

教育网络技术论坛

# 教育网络技术论坛（COST）月报

第 1 期

2009 年 1 月

教育网络技术论坛 秘书处

本期责任编辑：段海新

版权声明：欢迎转载，但请注明出处

## 目 录

开篇寄语 / 段海新 .....	1
“教育网络技术论坛”工作委员会和顾问委员会成立 .....	2
技术沙龙第 8 期: 多出口校园网的路由和域名问题 / 傅宇凡整理 ..	4
专题讲座第 3 期: 反病毒技术必由之路—主动防御 / 东方微点公司 ..	7
2008 年 12 月份漏洞信息点评 / 郑先伟 .....	8
近期关注的热点问题总结 / 姚星昆整理 .....	13
中山大学第四届信息化工作年会论坛 / 傅宇凡整理 .....	16
从黑屏事件谈校园软件正版化问题 / 段海新 .....	20

## 开篇寄语

清华大学信息网络工程研究中心 段海新

2009, 新的一年开始了, 我们的论坛 1 岁了。希望我们的论坛能够发挥校园网运行和安全技术交流的桥梁作用, 同时也加深我们之间的了解和友谊。

在成立以来一年多的时间里, 有了论坛里各位老师的热心参与和支持, 我们的论坛发展的还算顺利。目前在我们论坛上实名注册的老师有七百多位, 一年来组织了各项活动十二次, 发布各种文档一百多份。我们建立起了网站、邮件列表、视频会议系统、讨论区、博客等交流的平台, 尽管还存在着诸多问题需要改进, 但毕竟我们走出了第一步。

近期我们论坛成立了工作委员会和顾问委员会, 主要来自于校园网运行管理第一线、并有多年经验的老师和技术人员, 他们的工作完全是义务性的。我希望我们的工作委员会是开放性的, 欢迎更多有经验的老师加入我们; 我个人很高兴能有机会和工作委员会里的老师一起, 为校园网运行管理技术交流和信息共享作一点力所能及的工作。

从 2009 年起, 我和论坛工作委员会的老师开始整理编写《教育网络技术论坛 (COST) 月报》, 计划每月一期, 总结近期论坛的活动, 让没有时间关注论坛的老师也能了解论坛的动态。我自任第一期的责任编辑, 与论坛里的姜开达老师等老师一起讨论过, 目前计划开设以下栏目:

- 近期论坛活动回顾, 回顾近期组织的技术沙龙、讲座等活动;
- 近期安全风险点评: 针对最新的漏洞、攻击方法作一些分析;
- 论坛关注热点话题: 整理 QQ 群、邮件列表、讨论区、博客等系统中大家关注的热点话题;
- 校园网和信息化通报: 收集各高校校园网或信息化建设中相关的动态信息, 希望对其他学校有所借鉴;
- 业界动态事件分析: 针对业界相关动态所作的一些分析;
- 相关项目动态: 主要介绍论坛和各高校开发的一些运行管理系统的建设和应用情况。
- 相关软件和工具介绍: 介绍网络和系统管理中的常用软件和工具。

欢迎各位老师对月报的形式和内容提出宝贵的意见和建议, 同时也欢迎各位老师向月报投稿, 请发送到我的邮箱: [duanhx\[AT\]tsinghua.edu.cn](mailto:duanhx@tsinghua.edu.cn)。

## “教育网络技术论坛”工作委员会和顾问委员会成立

为了促进高校校园网运行和安全管理经验和技术的交流,成立“教育网络技术论坛”工作委员会(以下简称委员会)。委员会由网络运行管理的教师或技术人员自愿组成,主要职责包括发现校园网运行管理的常见问题,组织技术专家研讨相关的解决方案,并组织本地区校园网管理和技术交流活动。

委员会在 CERNET 专家委员会指导之下开展工作,设顾问委员,由 CERNET 专家委员会成员担任。委员会设常务工作委员 5-7 人(其中主席、副主席各一人),主持论坛的日常活动;委员会设秘书处,负责论坛平台的建设、活动的组织联络、文档收集发布等工作。

第一届工作委员会成员、常务工作委员及主席、顾问委员会成员,由自愿或推举产生,任期一年,秘书处设在清华大学网络中心;以后的组成成员及其产生办法另行商定。

第一届顾问委员和工作委员会成员名单如下(排名不分顺序):

### 一、顾问委员

- 李星教授(清华大学)
- 龚俭教授(东南大学)
- 李之棠教授(华中科技大学)
- 马严教授(北京邮电大学)
- 汪为农教授(上海交通大学)
- 张蓓教授(北京大学)
- 李卫教授(西安交通大学)

### 二、工作委员会成员(32人):

- |               |               |
|---------------|---------------|
| ● 李斌奇(集美大学)   | ● 张焕杰(中国科技大学) |
| ● 谢锐(上海交大)    | ● 于广辉(大连理工)   |
| ● 姜开达(上海交大)   | ● 黄鹂声(电子科大)   |
| ● 常潘(华东师范大学)  | ● 陈文波(兰州大学)   |
| ● 陈晓筹(厦门大学)   | ● 邹仁明(中国农业大学) |
| ● 李肖坚(广西师范大学) | ● 温占考(东北大学)   |
| ● 刘家宁(海南师范大学) | ● 王振华(北京邮电大学) |
| ● 陈军(山东大学)    | ● 尚群(北京大学)    |

- 郭 焯 (浙江大学)
- 杨 望 (东南大学)
- 王 宇 (东北大学)
- 段海新 (清华大学)
- 商尔从 (中山大学)
- 闫 华 (复旦大学)
- 云 霞 (浙江大学)
- 王竹威 (北京大学)
- 李云春 (北京航空航天大学)
- 石 岗 (武汉大学)
- 涂 浩 (华中科技大学)
- 何海涛 (中山大学)
- 高 岭 (西北大学)
- 李信满 (CERNET 网络中心)
- 苏 和 (大连理工大学)
- 向 望 (复旦大学)

### 三、常务工作委员

- 段海新 (清华大学), 工作委员会主席
- 姜开达 (上海交大), 工作委员会副主席
- 张焕杰 (中国科技大学)
- 于广辉 (大连理工大学)
- 李信满 (CERNET 网络中心), 工作委员会副主席
- 商尔从 (中山大学)

### 四、秘书处联络人:

1. 傅宇凡 (《中国教育网络》), 论坛活动组织与联络

Email: fuyf@cernet.com

电 话: 010-62603857, 传 真: 010-62790637

地 址: 北京清华大学东门信息科学技术大楼 4-206

邮 编: 100084

2. 郑先伟 (清华大学/CCERT), 论坛技术平台建设与维护

Email: zxw@tsinghua.edu.cn

电 话: 010-62784301

地 址: 北京清华大学东门信息科学技术大楼 1-213

邮 编: 100084

## 技术沙龙第 8 期：多出口校园网的路由和域名问题

《中国教育网络》 傅宇凡 整理

2008 年 11 月 26 日下午，“校园网管理与安全论坛”在上海交通大学组织了“多出口校园网的域名和路由问题”的技术研讨会。会议由上海交通大学谢锐老师主持，CERNET 专家委员会委员汪为农教授致辞，中国科技大学张焕杰、厦门大学陈晓筹、浙江大学邹池佳以及赛尔网络李信满技术报告。由于很多老师对研讨会主题比较关注，气氛比较热烈。研讨会现场 30 多人，网上视频会议参与 133 人，对这一话题的讨论一直延续到论坛及 QQ 群里，目前还有不少的讨论。

### 1、会议讨论的内容

#### (1) 汪为农教授（上海交通大学网络中心）致开幕辞

校园网与公众网之间的性能问题曾经给不少学校带来过不少麻烦。部分原因在于，国内多个运营商并存，各大运营商之间由于商业的竞争；国内网际互通游戏规则缺失，以大欺小的现象一直存在。选择多出口解决这一问题，是解决公网访问问题不得已的措施。目前，百分之七十到的高校都是多出口的，上海交大于 2007 年松口多出口。但是目前问题仍然普遍存在，既要解决从校内访问校外的速度问题，还需要解决从校外的公网访问校内资源的速度问题，让 CERNET 的服务质量提升。

#### (2) 陈晓筹：多出口校园网的路由策略应用

厦门大学网络中心的陈晓筹老师报告的主要内容包括：1) 首先把访问的地址空间划分成若干个集合，以便制定各种访问政策；2) 然后介绍了不同地址空间相互访问时的控制政策，包括地址转换 (NAT)、策略路由(Policy Routing)和访问控制列表 (ACL) 以及路由映射 (Routing Map)。3) NAT 和 PBR 不同设备时，如何进行路由策略；NAT 和 PBR 同一设备时，如何进行路由策略。厦门大学校园网出口用一台独立的 NAT 设备解决复杂的地址转换问题。陈晓筹老师以厦门大学校园网为例，介绍了在厦门城域网、教育网、中国电信多个出口环境下的一些技术措施和解决方案。陈晓筹老师的技术报告提纲参见[1]。

#### (3) 张焕杰：基于 Linux 的校园网多出口策略路由和域名实现

来自中国科技大学网络中心的张焕杰老师介绍了基于 Linux 系统的解决方案。张老师首先分析了多出口校园网路由问题的原因，然后介绍了基于源地址的策略路由实现原理。张老师凭借多年 Linux 系统开发和校园网运行的工作经验，

详细阐述了 Linux 下基于连接跟踪信息的策略路由和基于 Linux 的校园网多出口策略路由实现。为解决服务器的外网访问问题, 张老师还介绍了几个开源的软件, 比如 Nginx 反向代理等, 为解决域名解析的问题, 张老师介绍了 DNS 系统 BIND 视图 (view) 的配置。最后介绍了科大校园网如何利用多个出口为用户提供服务的政策和系统的界面。陈晓筹老师的技术报告提纲参见[2]。

#### (4) 邹池佳: 浙江大学校园网多出口部署经验介绍

浙江大学网络中心的邹池佳老师介绍了浙江大学校园网多出口部署的经验。邹老师首先介绍了校园网多出口的需求和由此带来的好处, 然后分析了多出口环境下的问题。邹老师介绍了浙江大学校园网出口的路由政策和解决方案, 然后重点介绍了服务器部署时路由和域名的配置。最后介绍了浙江大学下一步的工作, 特别是如何解决多链路的负载均衡问题。陈晓筹老师的技术报告提纲参见[3]。

#### (5) 李信满: CERNET 网络资源介绍

赛尔网络公司网络服务技术总监李信满介绍了 CERNET 现有的一些网络资源, 包括各大知名的门户网站、商业网站、专业论坛等等。目前很多 CERNET 的用户不知道这些资源的现状, 部分学校更新免费地址不及时, 导致 CERNET 引进资源的利用率低, 这也影响 ICP 的积极性。另外, 由于部分学校的 DNS、路由的配置存在一些问题, 导致访问这些资源的性能不高。李信满博士重点推荐和介绍 CERNET 上的直联资源, 还表示以后会更多地关注终端用户的感受与体验, 解决学校访问外部网站慢的问题。李信满博士的报告提纲参见[4]。

#### (6) 自由讨论的情况

现场提问热烈, 网上视频的提问达到 75 个问题。主要分为两类:

第一类: 策略路由的性能问题。

策略路由对于设备性能影响怎样? 与学校规模关系如何? 国外对于校内服务器的访问? 系统维护的问题? 许多老师还关注到负载均衡交换机的问题。

关于邮件服务器的访问有三到四家学校都同时关注并提问, 涉及邮件服务的各个方面。

第二类: 设备及计费策略问题。

多出口的计费策略是什么样的? 设备的价格及面对的规模是什么样的? 是否有开源的系统? 尤其关注科大的系统产品化问题。

总的来说: 目前多出口的路由策略和解决方案是比较复杂。由于各个学校各有特色, 每个学校的方案都不相同, 有些东西还是相通的。比如 DNS 解析、逆

向代理、反向代理等。

## 2、会议小范围内的调查情况

**复旦大学：**校园网有 6 个接口，分别接入教育网 x 2、电信 x 2、网通、上海科技网；主要路由器是 cisco、H3C；主要交换机是 cisco、H3C；校园网主干带宽是万兆，百兆到桌面

**上海立信会计学院：**校园网有 3 个接口，分别接入教育网、电信、有线通；主要路由器是 H3C、6608；主要交换机是 H3C、9500；校园网主干带宽是千兆，百兆到桌面

**同济大学：**校园网有 2 个接口，分别接入电信、教科网；主要路由器是 cisco6509；主要交换机是 Huawei、3026；校园网主干带宽是 1G，百兆到桌面

**华东理工大学：**校园网有 4 个接口，分别接入 cernet、电信、网通、铁通；主要路由器是 cisco、华为；主要交换机是神码、锐捷、华三、cisco；校园网主干带宽是千兆/万兆，100M 到桌面

**上海中医药大学：**校园网有 3 个接口，分别接入教科、科技、铁通；主要路由器是 Extreme 6808；校园网主干带宽是 1000M，百兆到桌面

**上海大学：**校园网有 4 个接口，分别接入教育网、电信、移动、上海科技网；主要路由器是华为；主要交换机是阿尔卡特 9000；校园网主干带宽是万兆，100M 到桌面

**上海交大医学院：**校园网有 3 个接口，分别接入 cernet、上海科技网、中国科技网；主要路由器是华为 N\_80、8016；主要交换机是锐捷；校园网主干带宽是 2.5G，100M 到桌面

## 3、参考链接：

- [1] 陈晓筹，多出口校园网的路由策略应用，  
[http://forum.ccert.edu.cn/upload/files/yaoxingkun\\_2008\\_1127\\_945.pdf](http://forum.ccert.edu.cn/upload/files/yaoxingkun_2008_1127_945.pdf)
- [2] 张焕杰，基于 Linux 的校园网多出口策略路由和域名实现，  
[http://forum.ccert.edu.cn/upload/files/yaoxingkun\\_2008\\_1127\\_946.pdf](http://forum.ccert.edu.cn/upload/files/yaoxingkun_2008_1127_946.pdf)
- [3] 邹池佳，浙江大学校园网多出口部署经验介绍，  
[http://forum.ccert.edu.cn/upload/files/yaoxingkun\\_2008\\_1127\\_948.pdf](http://forum.ccert.edu.cn/upload/files/yaoxingkun_2008_1127_948.pdf)
- [4] 李信满：CERNET 网络资源介绍，  
[http://forum.ccert.edu.cn/upload/files/yaoxingkun\\_2008\\_1127\\_950.pdf](http://forum.ccert.edu.cn/upload/files/yaoxingkun_2008_1127_950.pdf)

## 专题讲座第 3 期:反病毒技术必由之路—主动防御

北京东方微点信息技术公司 刘旭 周福军 (段海新 整理)

2008 年 12 月 18 日, CCERT 邀请北京东方微点信息技术公司总裁刘旭、经理周福军先生为教育网络技术论坛作了一次题为“反病毒技术发展必由之路——主动防御”的专题技术报告。清华大学网络中心的部分教师和研究生在清华参与了现场的技术交流,论坛中来自全国各高校的六十多名教师和技术人员通过视频会议参加了这次讨论。

报告的主要内容包括以下几个方面:

- 趋利性病毒攻击已成网络最大危害
- 杀毒软件的脆弱性与全球病毒新特点
- 反病毒发展必由之路—主动防御
- 微点主动防御软件介绍

东方微点的技术人员在现场结合具体的案例(比如熊猫烧香病毒)介绍了微点主动防御产品的技术特点,并与现场和网络上的老师和同学进行了交流和讨论。

这次的专题报告“反病毒技术发展必由之路——主动防御”讲稿可以从下面的地址下载: <http://forum.ccert.edu.cn/document/>

在主题报告之后,截至 2009 年 1 月 10, 50 多所高校的老师开始试用微点公司的主动防御产品,具体信息参见: <http://bbs.media.edu.cn/thread-1843-1-1.html>

## 2008 年 12 月份漏洞信息点评

郑先伟 清华大学信息网络工程研究中心

12 月份暴露的漏洞数量较多，我们需要特别关注的漏洞有如下几个。

### 1、IE 浏览器对象处理内存破坏漏洞 (MS08-078)

(1) 该漏洞对应 CVE 编号: CVE-2008-4844

(2) 影响系统:

- Microsoft Internet Explorer 5.01
- Microsoft Internet Explorer 6
- Microsoft Internet Explorer 7

(3) 漏洞信息:

IE 浏览器的数据绑定功能中存在一个远程执行代码漏洞(作为有效的指针引用)。当数据绑定处于启用状态(系统默认状态是启用的)时,某些情况下系统会发布对象而不更新数组长度,这就使得程序有机会访问已删除对象的内存空间。这可能导致 Internet Explorer 处于可利用状态并意外退出。攻击者可以通过构建特制的网页来利用该漏洞。当用户查看网页时,该漏洞可能允许远程执行代码。成功利用此漏洞的攻击者可以获得与登录用户相同的用户权限。

(4) 漏洞风险分析:

目前利用该漏洞的网页木马程序正在网络上大面积的泛滥。当用户使用了未修补漏洞的 IE 浏览器访问包含有此类攻击代码的网页时漏洞就会被利用,这可能导致 IE 浏览器自动下载大量的其他木马程序在系统上运行。虽然几乎所有版本的 IE 浏览器都存在这个漏洞,但是目前网络利用最多的还是针对 IE7.0 版本的攻击程序。另外一个值得注意的地方是这些包含攻击程序的网页并不一定需要用户点击相关的链接才能被利用。它还可以通过其他一些手段来激发漏洞,如通过向 Word 文档中植入 ActiveX 控件,而控件中附带着链接木马网页的命令,一旦用户打开这种特制的 word 文档浏览器就会自动链接到木马网站。

(5) 解决办法:

厂商已经针对该漏洞发布了相应的安全公告和补丁程序,建议用户尽快安装相应的补丁程序,您可以通过 windows 的自动 update 功能或者是 WSUS 服务自动更新补丁程序,也可以手动下载补丁程序安装,补丁下载地址:

<http://www.microsoft.com/china/technet/security/bulletin/ms08-078.msp>

## 2、SQL Server 中的漏洞可能允许远程执行代码(961040)

(1) CVE 编号: CVE-2008-5416

(2) 影响系统:

- Microsoft SQL Server 2000 Service Pack 4
- Microsoft SQL Server 2000 Itanium-based Edition Service Pack 4
- Microsoft SQL Server 2005 Service Pack 2
- Microsoft SQL Server 2005 x64 Edition Service Pack 2
- Microsoft SQL Server 2005 with SP2 (用于基于 Itanium 的系统)
- Microsoft SQL Server 2005 Express Edition Service Pack 2
- 带 Advanced Services Service Pack 2 的 Microsoft SQL Server 2005 Express Edition
- Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) Service Pack 4
- Microsoft SQL Server 2000 Desktop Engine (WMSDE)
- Windows Internal Database (WYukon) Service Pack 2

(3) 漏洞信息:

SQL Server 的 `sp_replwritetovarbin` 扩展存储过程中存在堆溢出漏洞。如果远程攻击者在参数中提供了未初始化变量的话, 就可以触发这个溢出, 向可控的位置写入内存数据, 导致以有漏洞 SQL Server 进程的权限执行任意代码。

在默认的配置中, 任何用户都可以访问 `sp_replwritetovarbin` 过程。通过认证的用户可以通过直接的数据库连接来利用这个漏洞。另外这个漏洞可以通过 SQL 注入攻击直接利用。

(4) 漏洞风险分析:

漏洞的攻击代码已经在网络上被公布, 这个漏洞对那些使用 SQL Server 服务器的网站影响较大, 虽然漏洞信息显示需要有一个有效的用户连接才能利用该漏洞。但是针对那些有 SQL 注入漏洞的网站来说, 攻击者可以通过网页 SQL 注入攻击来利用该漏洞, 攻击成功后可以以网页数据库用户的权限在系统上执行任意操作。

(5) 解决办法:

目前厂商还没有提供相应的补丁程序, 建议用户随时关注厂商的更新信息。在没有补丁前您可以使用一些临时的设置来缓解该漏洞的风险, 临时解决办法请参见: <http://www.microsoft.com/china/technet/security/advisory/961040.msp>

### 3、微软写字板文件转换器远程代码执行漏洞

(1) CVE 编号: CVE-2008-4841

(2) 影响系统:

- Microsoft Windows XP SP3
- Microsoft Windows XP SP2
- Microsoft Windows Server 2003 SP2
- Microsoft Windows Server 2003 SP1
- Microsoft Windows 2000SP4

(3) 漏洞信息:

写字板是 Windows 操作系统中附件所提供的简单文本编辑工具。

对于没有安装 Word 的用户, 可以使用写字板的文本转换器来打开.doc 格式文档。写字板程序中存在一个漏洞, 如果用户使用转换器打开了特制的.doc、.wri 或.rtf 格式文档的话, 就可能触发内存破坏, 导致执行任意代码。目前该漏洞已经开始在网络上被利用。

(4) 漏洞风险分析:

漏洞的攻击程序已经在网络上发布了。这个漏洞对那些没有安装 office 软件的系统(这些系统往往是一些有专用功能的服务器, 如 web 服务器)影响较大。因此用户应该尽量避免在服务器上做一些无关的操作。

(5) 解决办法:

厂商目前还没有提供该漏洞的相关信息和补丁程序, 我们建议用户随时关注厂商的更新。在没有补丁的情况下, 建议用户对一些来历不明的文档持谨慎态度。

### 4、Mozilla Firefox 最新版本修复多个安全漏洞

(1) 这多个安全漏洞的 CVE 编号包括: CVE-2008-5500、CVE-2008-5501、CVE-2008-5503 、 CVE-2008-5504 、 CVE-2008-5505 、 CVE-2008-5506 、 CVE-2008-5507 、 CVE-2008-5508 、 CVE-2008-5510 、 CVE-2008-5511 、 CVE-2008-5512、CVE-2008-5513

(2) 影响版本:

- Mozilla Firefox < 3.0.5
- Mozilla Firefox < 2.0.0.19
- Mozilla Thunderbird < 3.0.5
- Mozilla SeaMonkey < 1.1.14

### (3) 漏洞信息:

Mozilla Firefox 发布了最新版本的 Firefox 浏览器来修复之前版本中存在的多个漏洞, 这些漏洞可能导致执行任意代码、泄露敏感信息、本地越权越权执行脚本、执行跨站脚本攻击和网络欺诈。

### (4) 漏洞风险分析:

目前 firefox 在市场占有率接近 30%, 由于其多数为用户自己安装, 因此很难包含到整体的安全策略当中 (无法使用 windows 的自动升级), 用户不一定会及时升级, 有可能会成为一些单位整个安全策略中的盲点。

### (5) 解决办法:

建议用户及时下在最新版本的 Firefox 安装。下载地址:  
<http://www.mozilla.org/>

## 5、Cisco 6509 的 IPV6 MLD 功能的 BUG (CSCsj16969)

### (1) CVE 编号: 暂无

### (2) 影响版本:

- CISCO IOS < 12.2(18)SXF10

### (3) 漏洞信息:

根据中国科技大学张焕杰老师提供的消息, 并参考网络上的信息证实 CISCO 6500 系列路由器的 IPV6 MLD 功能实现上存在一个错误, 当接收到特定的 MLD 报文时可能导致路由器重起。

### (4) 漏洞风险分析:

IPv6 网络正在各个高校加速部署, 错误的 MLD 报文可能并不一定来源于恶意的攻击。根据张焕杰老师那边反馈的信息该 BUG 可能导致 6509 路由器自动重起, 即便是双引擎的机器, 也会一起重起甚至直接停在 bootrom 状态从而需要手工断电后重起才能恢复。

### (5) 解决办法:

升级 IOS 到最新的版本(12.2 (18) SXF10)。

临时解决办法: 在全局范围内关闭 IPv6 MLD 监听功能, 命令为

```
no ipv6 mld snooping
```

（6）参考连接：

[http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/hybrid/release/notes/ol\\_4563.html](http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/hybrid/release/notes/ol_4563.html)

<http://blog.ccert.edu.cn/blog.php?do=showone&type=blog&itemid=88>

## 近期关注的热点问题总结

清华大学信息网络工程研究中心 姚星昆整理

### 1、校园网多出口调查情况一览

在技术沙龙第八期:多出口校园网的域名和路由问题(上海) 活动之后,论坛发起了关于校园网出口类型和带宽的调查。共收到 36 所学校的问卷。

详细参见: <http://bbs.media.edu.cn/redirect.php?tid=1943&goto=lastpost#lastpost>。

### 2、校园网多出口条件下 QQ 登录问题

民航飞行学院在 12 月初,校内部分用户不能正常登陆 QQ,有的用户在同一台机器上同时登录两个 QQ 号,只有一个能登录成功。民航飞行学院的校园网出口由电信,网通,教育网三部分组成。他们经过调试,如果将网通和电信两条路由断掉一条时,大家登录都没问题。

咨询过北大,上海商学院,河南科技大学等高校后,大家一致认为:把 QQ 登录服务器的地址汇总,默认走一个出口。同时也咨询了腾讯,得到的回复和我们得出的结论也是一样的。

最终,民航飞行学院采用了走单一出口,顺利解决了这个问题。不过这个情况在很多高校依旧存在。

### 3、反病毒新技术——主动防御产品申请试用

2008 年 12 月 18 日,CCERT 邀请北京东方微点信息技术公司总裁刘旭、经理周福军先生为教育网络技术论坛作了一次题为“反病毒技术发展必由之路——主动防御”的专题技术报告。报告之后众多高校的老师要求试用微点的产品。

目前已有 59 所学校申请并拿到试用的产品,详细名单参见:  
<http://bbs.media.edu.cn/viewthread.php?tid=1898&extra=page%3D1>。

### 4、IE 0DAY 攻击漏洞 (MS08-078)

MS08-078 漏洞出现之后,论坛及时转发了微软的相应公告,在 QQ 群中广泛宣传,并将内容下发到校内的用户,使学校用户的损失最小化。

详细信息参见:2008 年 12 月份漏洞信息点评。

## 5、WSUS 和 360 做升级服务的优缺点

微软的黑屏事件后，360 的补丁升级功能再次得到广大用户的认可。在校园网内也有不少拥护者。微软的 WSUS 和 360 究竟哪个更胜一筹呢？

先说说 WSUS，WSUS 是微软的 Update 服务器，全面支持微软的各种系统，更权威、更安全，同时学校的 WSUS 服务器管理员也可以对其补丁筛选，进行优化配置。采用 WSUS 升级，速度快，占用出口和国际带宽小。但是，需要在客户端进行设置，由于校园网内的用户水平差异较大，用户配置起来困难，使得很多用户不太愿意使用。

对于 360，除了系统补丁更新之外，还能对其他的软件进行更新。对用户的要求低，只要按照提示进行操作即可，无需用户在进行其他的操作。

对于使用 WSUS 升级还是使用 360 升级，主要还是取决于用户的使用习惯。我们的经验和建议仅供用户参考。

## 6、DNS 解析——多出口惹的祸？

近期，在 DNS 解析方面又出现了不少的事故，尤其以武汉音乐学院和山东鲁东大学比较突出。

武汉音乐学院：

除电信外的其它线路都可以正常解析该校的主页 [www.whcm.com.cn](http://www.whcm.com.cn) 以及学校的二级网站。检查 DNS 的配置后，没有任何异常。后与电信联系，电信答复需要交费才可以给解析。万般无奈下，武汉音乐学校把这一情况上报教育网的省节点。节点的工作人员答复需要 7 个工作日左右可以正常解析。一周后电信的用户能顺利访问学校的主页和二级站点。至今也不清楚节点是如何操作。

山东鲁东大学：

在一个周末网通无意中将鲁东大学断网 5 个小时之后，再恢复就出现了很多怪问题，鲁东大学网络中心至今也不能解释原因，同时 ne40 的很多配置不能生效。在重新调整 ne40 后，突然发现邮件不能收取从电信来的邮件，电信的 dns 也解析不了，再深入测试，发现路由不固定，中间出现了很多不该出现的地址，无法解释。结论：PBR，NAT，链路负载（智能 dns）之间相互影响，关联的因素太复杂。

DNS 无法正确解析，DNS 服务器的配置问题是占很小的一部分，而大部分的问题还是路由和其他原因造成的。

## 7、干掉迅雷的 IP

在 P2P 的工具中, 迅雷是目前应用最为广泛, 同时也是消耗带宽最多的软件。对于日益紧张的带宽, 我们应该如何合理管理 P2P?

复旦大学向望老师, 使用封掉迅雷的资源服务器 IP 的方法, 成功抑制迅雷下载, 并收到了显著的效果。在封掉 IP 后使用迅雷只能连接到一个资源, 这种方法就是需要有人维护一份实时的迅雷资源服务器 IP 列表, 比较有难度。

向望老师给出了一份迅雷的资源服务器 IP 地址列表:  
<http://bbs.media.edu.cn/viewthread.php?tid=1944&extra=>, 希望大家可以共同维护这个 IP 列表。

## 中山大学第四届信息化工作年会论坛

傅宇凡 整理

2008 年 12 月 23 日, 校园网管理与安全论坛本年度最后一次技术沙龙广州中山大学举行。这也是论坛第一次与具体学校的信息化工作结合, 倡导关注高校校园网信息素养的培养。中山大学副校长许家瑞说: 这是一次与自己的用户“拉家常”的机会。对其他学校来说, 这是一次值得推广的交流。

此次技术交流共有三个分论坛, 分别是信息安全论坛《信息安全大家谈》、校园网治理论坛《校园网的“稳”与“快”》、多媒体教学论坛《PPT 与教学》。本文选摘其主要观点与大家共享。

### (1) 信息安全论坛《信息安全大家谈》

主持人: 中山大学信息中心副主任 蓝国秋

参与辩论嘉宾:

- 周春山教授, 教师代表, 中山大学地理科学与规划学院副院长, 中山大学城市与区域研究中心主任, 博士生导师。
- 孙全民老师, 院系网管员代表, 中山大学政务学院。
- 学生代表
- 段海新博士, CCERT 专家代表, 国际信息系统安全认证专家(CISSP), 现任清华大学信息网络工程研究中心网络与信息安全研究室主任
- 吴汝明副主任, 中山大学信息网络中心专家

### 观点摘录:

#### CCERT 段海新:

我个人感觉, 计算机病毒木马仍然是我们个人用户还有校园网的运行管理人员所面临最头疼的问题。病毒不再是以破坏计算机系统功能为目标, 它有可能窃取真正有效的数据, 越来越多商业的应用转移到互联网上, 比如网络游戏, 网络购物, 网上银行, 以盈利为目的的病毒, 或者是木马则越来越多。

道高一尺, 魔高一丈, 究竟是道高一尺, 魔高一丈, 还是魔高一尺, 道高一丈呢? 个人感觉可能黑客的攻击技术总是领先一点点, 防病毒软件的人通常是在新的攻击出来以后, 才会琢磨对应的措施, 如果是防病毒软件的人总琢磨新的

攻击方法的话，他本身就是一个黑客，而不再是防病毒人员。

因此，防病毒软件总是属于被动的防止。正是因为这一点，我们的同学不能完全依赖于防病毒软件，你必须得有一些防范措施，在防病毒软件没有查出这个病毒之前，你应该有一些良好的习惯，把它杜绝掉。

#### **中大信息与网络中心吴汝明：**

构建信息安全体系，最起码要从以下的四个方面入手。第一，规划先行，第二，政策到位，第三方法创新，第四，服务要提升。

人往往是最薄弱的环节，我们要更新曾经的安全观念和认知文化，这个是非常重要的。很多国家，特别是欧盟国家，他们是非常重视安全意识。我们网络中心也做了很多尝试，近一两年，我们通过帮助台，通过发海报，或者是剪报，或者是小册子，或者是书签的形式给大家提供联系的方式等等，我们在希望提高安全意识方面，多给大家一些途径，更多一些认识。

人是一个因素，加上有效的安全措施，这个才是构建我们防范信息网络安全的第一道防线。第一道防线是要有预防意识。第二要有措施，信息网络安全是需要所有的用户共同参与的，并且我们的用户也要承担起来我们应该承担的责任。

#### **中大地理科学与规划学院周春山：**

再好的政策体系法规，也还需要个人的防范意识，从我的角度来看，我经常听到我的学生，对其他的老师讲我的计算机瘫痪了，格式化了，重新装。如果是我的学生这样提出来我会批评他。需要安装正版的软件，不浏览非正规的东西，这是我的基本要求。对数据是备份的，我用不同的硬盘备份，一个放在办公室，一个放在家里。城市规划的产品全部是电子产品，这些决定我的数据安全是首要的。对我来讲意识是非常重要的。

#### **上海交通大学网络中心姜开达：**

所有的用户都提高安全意识，会让 ARP 欺骗病毒没有藏身之地，但是有个别用户有问题，就会影响校园网正常运行。现在在上海有一些高校的老师，有意向改变传统的校园网结构，采用流量控制的设备将不同的用户直接进行隔离，有一些优点，也有一些缺点，主要是改变传播的管理模式，也可以解决 ARP 欺骗病毒。但治根的办法还是，所有的用户都提高安全意识，ARP 欺骗病毒才没有藏身之地。

#### **北京大学信息网络中心江岳：**

从技术角度上来说，出现问题不一定是网络的问题，但是对于用户来说他不

管那么多,只要他不能用,他不管是谁的问题,反应都会很激烈。如果已经中了病毒的这些,大体上来说没有什么太好的解决办法,最好的问题是把这个病毒在落地前就把它防住。防病毒软件不是一个灵丹妙药,它只是起到一定的作用,用户的使用习惯才是最重要的问题。

## (2) 校园网治理论坛 《校园网的“稳”与“快”》

**主持: 中山大学信息网络中心网络管理部主任 何海涛**

随着校园网规模的扩大,上网的稳定性和访问外网的速度已成为用户关注的焦点,这也是当前校园网治理的主要内容。本次论坛邀请了教师嘉宾、学生嘉宾、运营商嘉宾和网络中心的专家,就大家所关心的这两个问题展开讨论、各抒己见,增进了双方的理解,明确校园网的治理将是一个“持续性改进、阶梯性进步”的过程。

何海涛:我们目前校园网的稳定性,应该说是我们目前校园网治理最为重要的问题,我们在这块主要是采用了四个方面的举措。

第一,我们优化了网络架构。第二,做了设备的升级。第三,升级了我们认证的系统。第四,我们主动对病毒进行防御。

速度是每个人在上网时最关注的焦点问题。我们建议,校园网的策略优先保证教学科研,学习为主的,而对于生活的,目前的资源无法得到保证,当然在带宽充裕的时候,我们也会适当考虑,但是这绝对不是目前的一个重点,需要蛙跳式的前进。

在网络稳定性方面,要提高我们的服务水平,第一,从服务体系方面我们参照一些国际 IT 服务管理的规范,以及中国电信的金牌的服务策略,来构建整个中大的服务体系。第二,从服务内容,我们目前已经提供了 24 小时服务的途径,进行主动的服务。从渠道上,我们大概有三个,电话,邮件和网站。我们从三个层次不断提升我们服务的水平。从 ITTLE 平台上,可以了解到目前网络运行的信息、统计的数据,各个校区的基本情况等等。

## (3) 多媒体教学论坛 《PPT 与教学》

**主持人: 中山大学信息与网络中心网络教育技术部王竹立博士**

电子讲稿,又叫幻灯片,俗称 PPT,目前已成为绝大多数教师上课的主要辅助工具。但我们真的会用 PPT 吗? PPT 到底给教学带来哪些好处? 什么样的 PPT 是好的 PPT? 中山大学教师应用 PPT 进行教学的水平如何? 学生对教师的 PPT 有什么看法? PPT 用于教学有没有局限性? 用 PPT 教学应该注意哪些问题? 让我

们一起分享大家的共同经验。

详情请参见：录制回放

[http://video.ccert.edu.cn/main/frame.asp?language=Chinese&site\\_id=MjA4&service\\_type=MA](http://video.ccert.edu.cn/main/frame.asp?language=Chinese&site_id=MjA4&service_type=MA)==

## 从黑屏事件谈校园软件正版化问题

清华大学信息网络工程研究中心 段海新

摘要：本文从微软黑屏事件谈到校园软件正版化问题，只反映作者本人的观点，欢迎讨论。作者反对把对微软的声讨变成为盗版软件正名，主张遵守法律、尊重知识产权，并呼吁高等学校培养学生使用正版软件的意识，为技术创新、为国产软件的发展提供一个法制环境。

### 1. 引言

关于微软“黑屏事件”，我曾经参加过青年科学家论坛（YOCSEF）和清华团委组织的两次论坛，听过几个专家、名人的报告，他们旗帜鲜明地声讨微软的行为，他们大多数打着反对霸权主义、维护国家安全、支持民族产业等等旗号，甚至主张微软“黑屏有罪”、中国用户“盗版有理”；这样的观点是被主流所支持的，据网上的统计说，80%以上的用户持类似的观点。根据我对周围学生和同事的观察，上面的数据是合理的。

我觉得这一现象反映出，我国当前对知识产权保护方面的“主流民意”是非常畸形的，这反映出大多数民众缺乏法治观念，缺乏对知识产权应用的尊重。宣传这种观点不利于培养保护环境，不利于我国信息产业的发展。

在组织校园网管理与安全论坛的过程中，我也接触过不少主管校园信息化建设和运行的老师，知道不少学校正在推行软件的正版化。我觉得这是一件好事，不仅有利于校园网的管理和安全，而且能够培养学生使用正版软件的习惯，更深的意义上，可以培养学生尊重知识产权、遵守法律的意识，这对培养公民意识、建设一个法治社会，应该是一件好事。

以下我从这两个方面谈一谈我个人的看法，纯粹是个人的观点，欢迎批评指正。

### 2、黑屏有罪吗？

我不是法律专业人士，我看到不少名人主张微软的“黑屏”是一种黑客行为，“操控了用户的电脑”，甚至侵害了“国家的信息安全”。我更相信一些安全专业人员（如郭振忠律师）的分析，微软的行为不构成犯罪，甚至违法也算不上。

我要补充的是，现代法律精神讲“无罪推定”、“谁主张谁举证”，微软真的操控用户的电脑了吗？如果微软利用补丁更新植入了后门操控用户的电脑、或者收集了用户的隐私信息，甚至危害到“国家的信息安全”，那么，完全可以利

用现有的技术手段找出证据。虽然拿不到微软操作系统和补丁的全部源代码，现有对二进制程序的“逆向工程”技术也可以找到足够的证据。现在有些技术人员甚至可以根据微软发布的补丁，找到操作系统中的漏洞从而入侵系统。既然危害到了“国家信息安全”，那么，集国家之力找到些证据应该不是什么难事儿；难道因为微软有条件这么做，就给它安一个“莫须有”的罪名？

操作系统、防病毒软件、以及许多软件都需要在线更新，需要远程下载一些程序或者数据，这些操作很多是用户可以配置的，甚至可以说是用户授权的。微软是否给用户提供了足够明确的可选项我不知道，但是法律上没有定义这种更新是一种违法行为。

### 3、盗版有理？

主张“盗版有理”的用户可能不再少数，而且振振有词，比如网络名人方兴东博士就为盗版找出了很多理由：

- (1) 微软黑屏是为了促进 Vista 升级，赚取更多利润；
- (2) 盗版问题不是因为中国人的道德问题，美国人也盗版；
- (3) 微软全球统一价格对中国用户来说太高了；
- (4) 用户是上帝，微软应该善待消费者！

由于篇幅所限，我不想展开论述我的观点。针对上述反问几个问题：

(1) 微软利用合法的手段为企业赚取更多利润，有什么不正当的吗？微软声称过自己要“为人民服务”或者“无私奉献”吗？

(2) 美国人也盗版，中国人跟着盗版难道就没有道德问题了吗？美国年轻人还吸毒呢？我了解到美国对盗版行为打击力度很大，第一个传播 P2P 软件的网络——Napster 因此垮掉了；

(3) 因为定价太高，我们盗版就有理了？如果这个理由站得住脚，我们完全有理由到商店里去偷、去抢！何况，如果微软以低于全球其他地方的价格卖给中国，但是有倾销的嫌疑了！

(4) 盗版的用户也是微软的上帝吗？没有购买的契约关系，就凭偷了别人的东西就成了别人的上帝，天理何在？

### 4、中国盗版最大的受害者是谁？

中国盗版最大的受害者是微软公司吗？很多人并不这样认为，比如方兴东博士就认为微软靠盗版成就了他的垄断地位，是受益者。失去了中国市场，那些国

际上的大型软件厂商只是损失了部分利益。这些厂商早在进入中国之前就已经赚了足够的钱，足以支撑他们暂时在中国赔本赚吆喝，培育市场。

中国用户盗版最大的受害者是中国自己的软件产业。对国内的软件企业来讲，如果失去了中国市场或者不能从中受益的话，他们也就失去了全部市场，将永无出头之日，更别说走出国门了。

中国国内不乏优秀的软件厂商、优秀的软件技术人员，但是因为盗版的原因，几乎无法生存。特别是在中文处理相关的软件方面，国内的企业和技术人员有很大优势。也许很多用户像我一样最早使用的文字处理软件是 WPS，而不是微软的 Word。金山词霸也是很多机器装机必备的软件，然而，金山公司却无法靠这个软件来生存，只好跟 google 公司合作。

现在微软操作系统内置的“微软拼音输入法”，是以很低的价格从哈工大王小龙教授那里买来的。在 90 年代初，王小龙教授所开发的拼音输入法已经很好用了，与当时的全拼、联想等输入法相比可以说一支独秀。据王教授身边的一个同学介绍，王教授很大一部分精力放在为防范反跟踪而设置一些陷阱上，但是仍然无法防范盗版。虽然我觉得转让给微软有些不公平，但是不这样又会怎样呢？如果有一个尊重知识产权的环境，又会怎么样呢？

## 5、校园软件正版化问题

校园里使用盗版软件的可以说比比皆是。我遇到过不少学生，他们觉得盗版软件用起来也没有什么问题，使用正版软件也没有什么优势。对于这一点，我无言以对。如果我们纯粹从对自己的利害为判断准则，使用盗版软件有时的确是没有坏处的。

也许大多数人只是软件的使用者而不是开发者，也许 80% 的声讨微软的用户中绝大多数不会自己开发软件。然而，如果你有机会编写软件并以此为生，甚至创办自己的软件公司，你希望自己的劳动成果不被尊重、永远无利可图吗？没有了法治的途径，“让一部分人先富起来”，只能是让一部分有特权的人富起来，也许我们多数平头百姓都没有这样的机会。如果因为自己现在是一个穷人就主张杀富济贫，那么在你有幸成为富人的时候，也就成了自己主张的牺牲品。

在大学校园中，大部分用户只是软件的使用者，但是也有一小部分将来会成为软件的创作者。然而，即便这一小部分用户，又没有考虑到将来，希望别人尊重自己的辛勤劳动、尊重自己的聪明才智？

对于负责校园网运行管理的老师来说，微软的黑屏事件给我们一个推行正版软件的机会，借机宣传使用盗版软件的坏处、推行软件的正版化。至少存在以下

几点好处:

(1) 减少潜在的安全问题, 比如类似微软操作系统安全漏洞的补丁更新, 有些盗版用户无法更新。

(2) 购买正版软件, 同时购买的是售后的服务;

(3) 最为重要的是, 不去违反法律;

(4) 给学生、教师一个普法的教育、尊重知识产权;

对我们从事计算机相关研究与开发的技术人员来说, 保护知识产权, 其实也就是保护我们自己。宣传正版意识, 加强知识产权保护相关的立法和执法, 为软件企业和人才创造一个公平、自由的竞争环境, 保护他们的合法权益, 也许是我们今天应该做的。

## 6、总结

在当前的条件下, 我无意声讨盗版用户和企业的法律或道德责任, 只是不希望看到借声讨微软黑屏的名义为盗版行为正名。很希望我们的校园网运行管理人员, 能够借此机会宣传正版, 尊重知识产权, 为国内、国外的软件厂商创造一个良好的、公平的法治环境。

我一直相信, 真正平等、自由、民主的社会, 一定是个法治社会。法律面前人人平等, 在遵守法律的前提下, 也就是公平的规则面前, 每个人、企业能够公平地、自由地竞争, 充分展示自己的才华和创新能力。社会为每个人和企业提供公平竞争、自由发展的机会, 并不能保证竞争结果的平等; 但是我们不能用暴民思想杀富济贫, 剥夺了企业的合法权益 (更多的是国产软件企业), 使这些企业或技术人员无法利用自己的劳动、创新和技术赚取利润, 其实也就扼杀了平等和自由发展的基础。