China SoftCon 2010

中国软件 自主创新 十年一剑

web安全体系&网银安全策略

一、遵循的安全原则

1、物理数据使用全盘加密软件

2、开放端口最小化，开放80或443端口

3、权限最小化，框架只读化

最简单实现方法：使用有写保护的U盘

4、动态脚本提交数据严格过滤

一、遵循的安全原则

5、数据库传输要过滤，尽量不用access

必须使用的时候，使用odbc方式指到web的外部空间

6、传输管理只使用VPN，不能为了方便自己开后门

7、内网不是篱笆墙，一视同仁保障安全

8、尽量不使用开源的网站代码

如果使用要修改验证部分和session的构造方法

一、遵循的安全原则

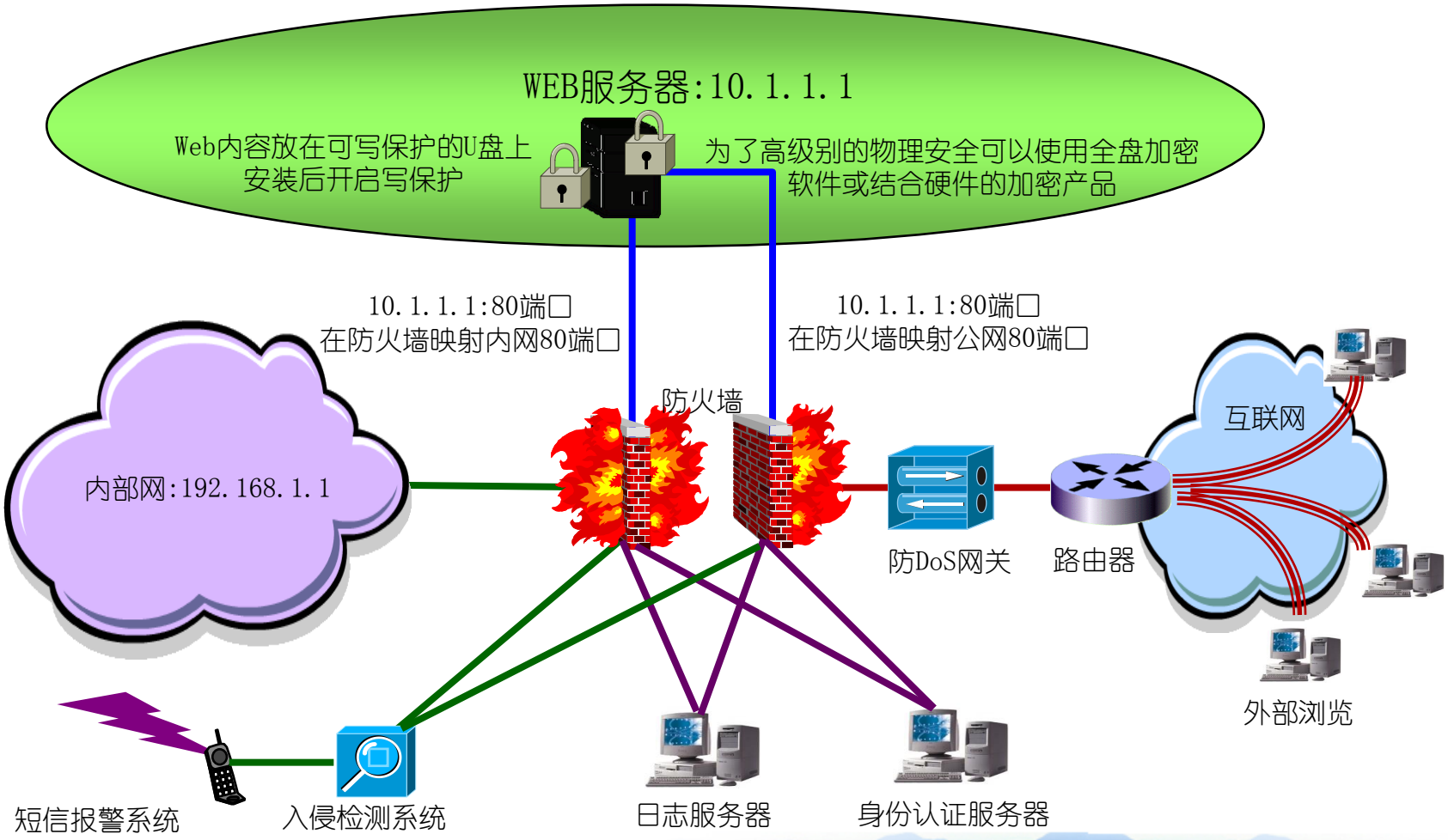
9、高级别的安全需要使用身份验证网关

10、及时跟踪弥补web服务组件的安全漏洞

11、建立内部或外包的安全团队

12、结合实际情况建立完善的管理制度最终上升为完整的web安全体系

二、依据安全原则建立web模型



三、现有的攻击模式对这个模型的影响

（一）模拟物理攻击

直接在机房读改物理硬盘

物理数据使用全盘加密软件或使用身份验证的硬件和磁盘加密联动进行防护。这样可以防御物理拿到硬盘进行读取、分析、篡改数据。

三、现有的攻击模式对这个模型的影响

（二）模拟网络攻击

1、动态cgi、asp、php、jsp、aspx动态web文件的权限控制和代码比对检测不合理造成入侵隐患，如：注入、上传网马、暴库、泄露服务器关键信息等

三、现有的攻击模式对这个模型的影响

（二）模拟网络攻击

物理上只读确保不被篡改无法上传木马，提交脚本的过滤可以防止注入，单一的web网站服务防止旁注。暴库、泄露服务器关键信息对于这个模型无效。找到了也无法连上或得到文件。跨站只要session的构造方法绑定ip，cookie算法自建基本上就没问题了。

三、现有的攻击模式对这个模型的影响

（二）模拟网络攻击

2、数据库与web在同一个主机，数据库开放对外的连接造成主机漏洞，通过数据库打开其它服务或建立账号导致web服务器不安全。

例如mysql、sqlserver等等

本模型对外只有一个端口这些大量的漏洞安全都可以忽略。

三、现有的攻击模式对这个模型的影响

（三）模拟对系统和其他应用进行攻击

操作系统和系统开启的其他服务出现漏洞对其进行攻击。

本模型对外只有一个端口这些大量的漏洞安全都可以忽略。

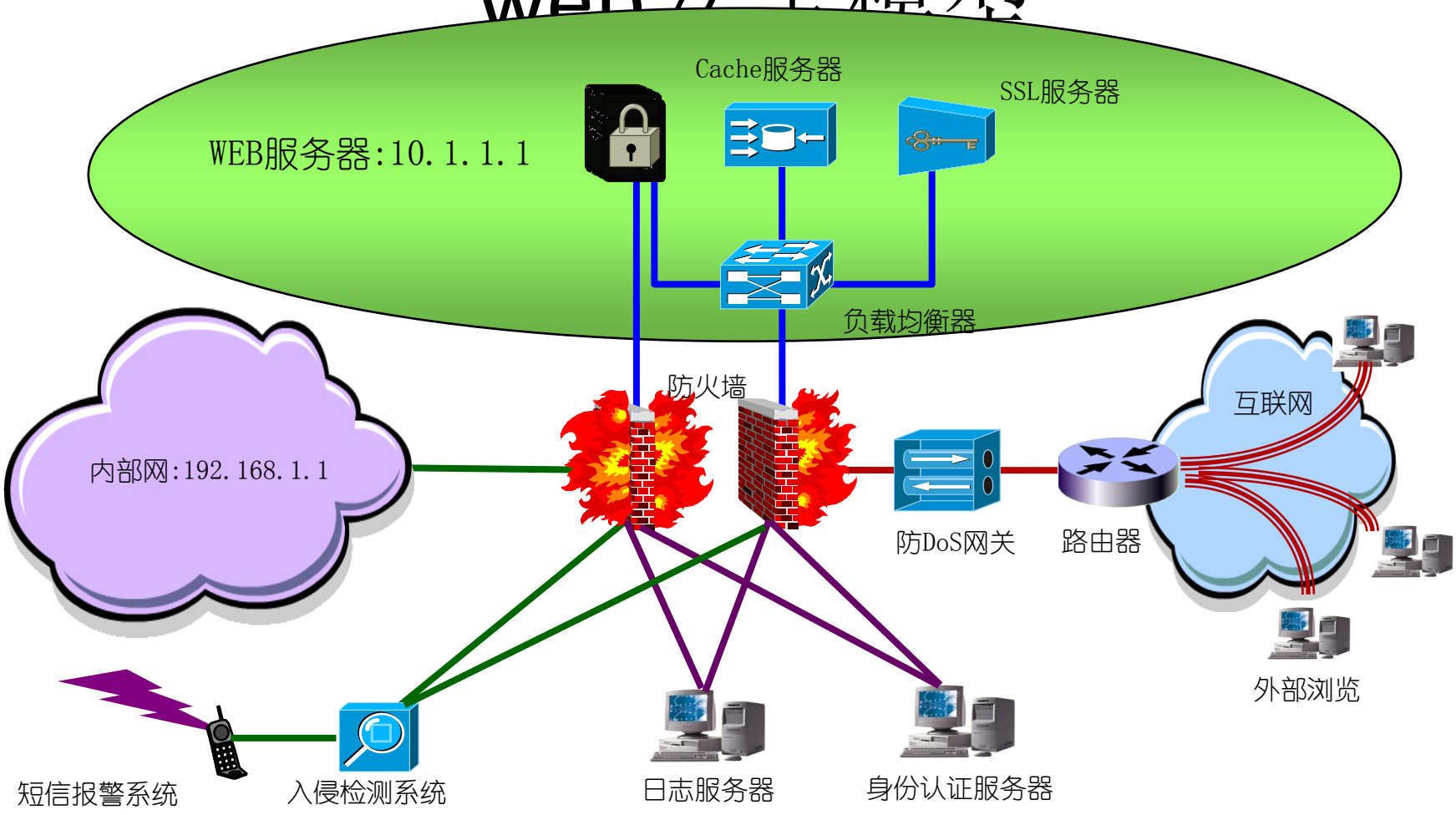
三、现有的攻击模式对这个模型的影响

（四）模拟对web应用服务漏洞进行攻击

web应用服务出现漏洞对其进行攻击。

web服务程序只要找相应的安全团队及时跟踪就可以确保安全，而且大部分的漏洞也不能危害这个模型的安全。

四、依据安全原则建立高投入web安全模型



五、如何结合技术制定管理办法

（一）安全管理原则

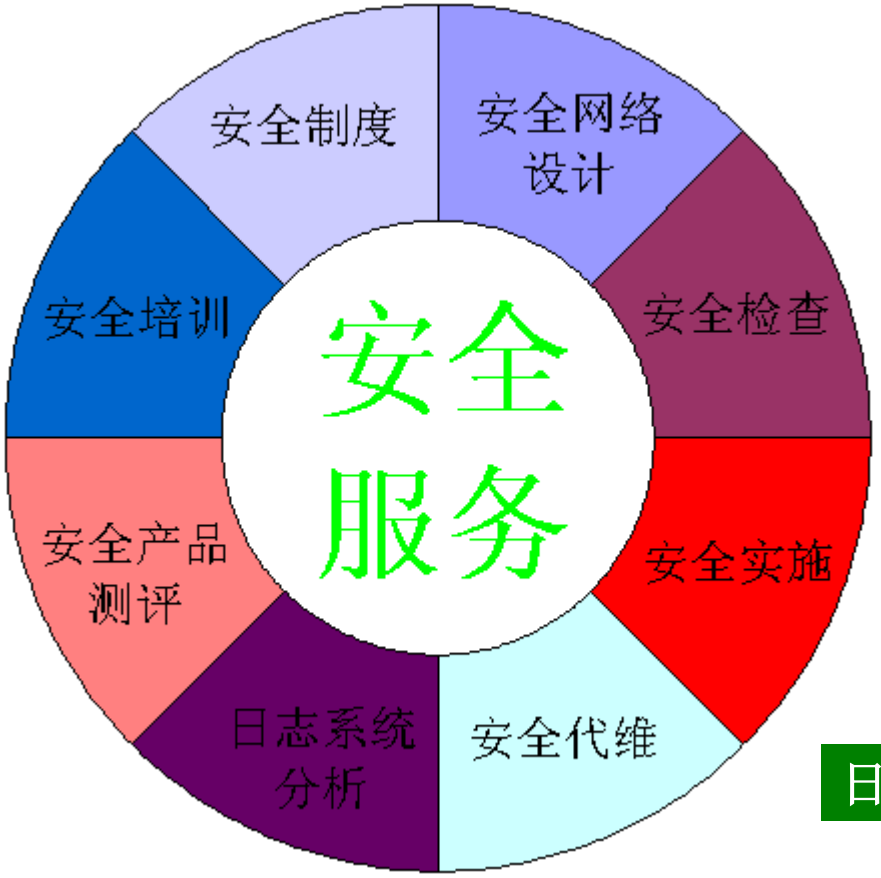
偏重技术结合管理 –可以使用技术的情况下尽量使用技术来进行安全控制。因为人是最不好限制的，即使技术上限制还有人想办法突破限制。不能把技术上能解决的问题放到管理上，既增加企业的管理成本，也带来了安全隐患。

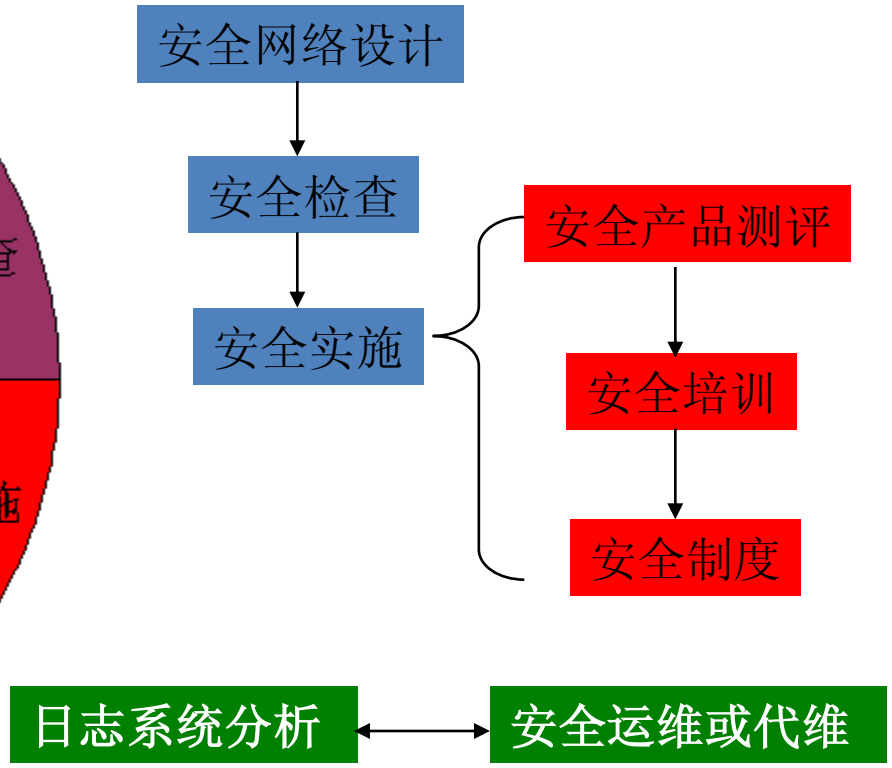
五、如何结合技术制定管理办法

（二）安全管理规范

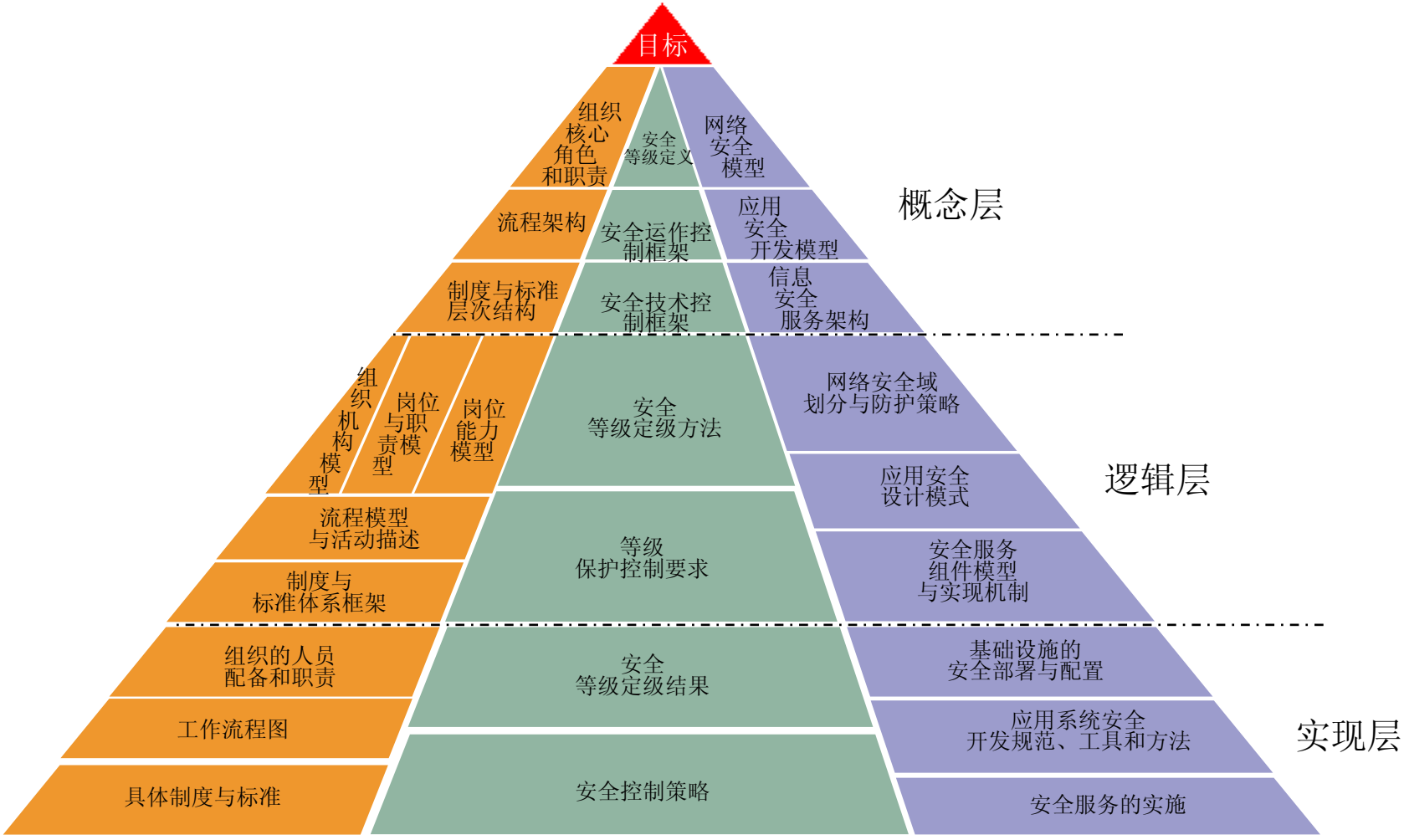
按照模型-〉合适的安全服务团队-〉完善的风险管理流程-〉健全的信息安全制度和标准-〉不断提升基础设施的安全性-〉最后要有定期的审计流程

六、安全服务建设技术流程





七、安全体系的建立



一、网上银行的现状

1、网上业务爆炸式增长

2、安全隐患是发展的主要障碍

3、网银安全设计流程存在误区

4、地下黑产对网银的威胁

二、现有的解决方案

1、使用密码验证

2、使用证书加密码验证（U盾）

3、使用手机短信密码验证

4、使用动态密码验证

三、网银的攻击手段

1、拦截帐号、密码和证书发送给黑客

2、使用远程控制操作网银

3、粘虫技术突破U盾

4、篡改交易封包内容或内存内容

四、网上银行安全解决方案

五、手机银行安全解决构想

1、遵循双平台认证原则

2、使用语音技术

3、附加证书签名