大企业安全测试技术及全新的信息安全边界

关键字：安全测试　端到端防护体系

安全测试审计　　安全边界

www.huawei.com

HUAWEI

袁明坤

认证资质

CISP、信息安全情报分析师、CIW安全讲师、PMP、ISO27001 LA、OSCP进攻性安全专家、华为兼职讲师

OWASP核心成员

华为技术：

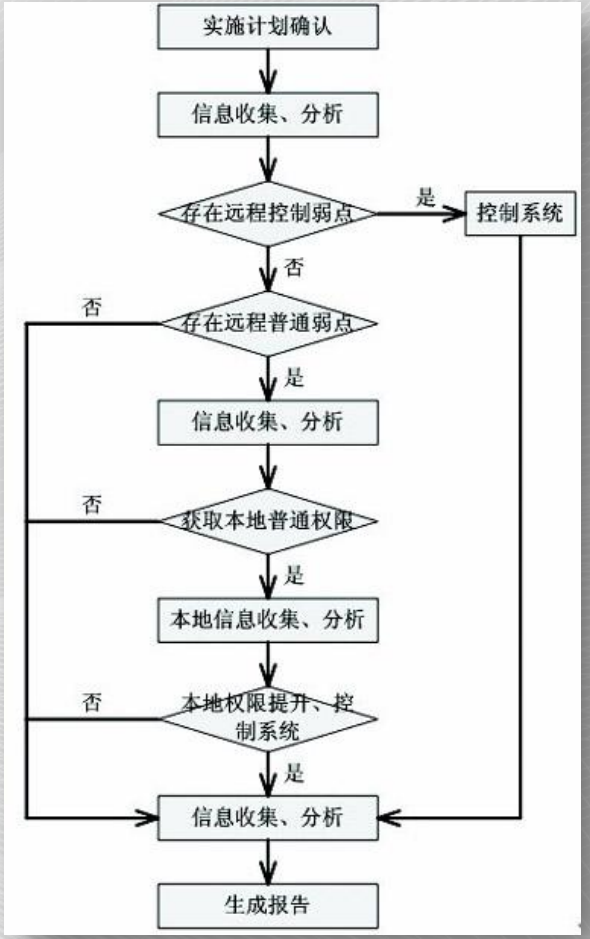
内部产品安全测试

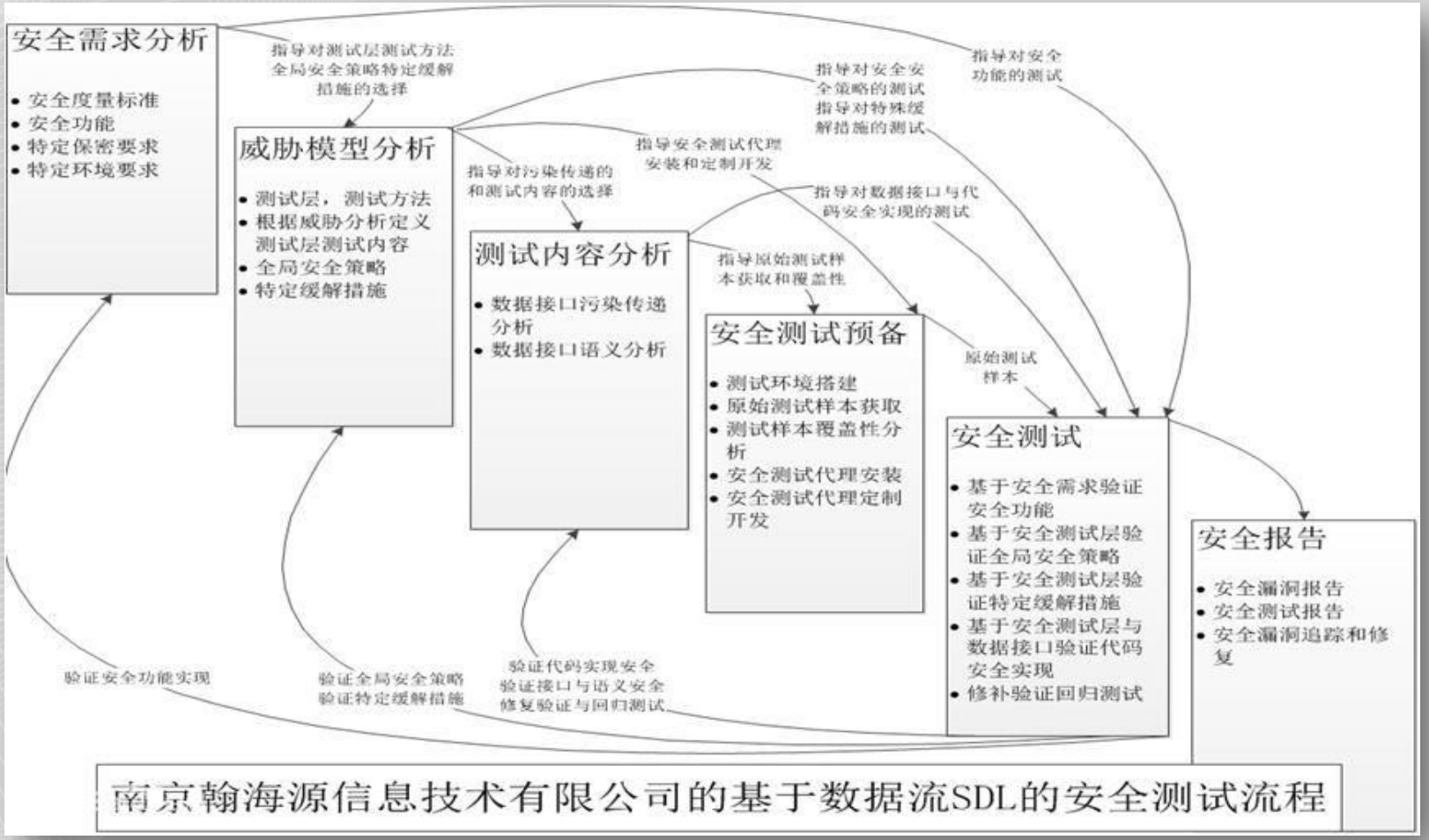
外部安全服务解决方案

议程

- 华为安全测试技术框架
- 华为安全测试技术流程
- 端到端的安全体系
- 新的安全边界

渗透测试&安全测试


实施计划确认
信息收集、分析
存在远程控制弱点
是
控制系统
否
存在远程普通弱点
否
是
信息收集、分析
获取本地普通权限
否
是
本地信息收集、分析
本地权限提升、控制系统
否
是
信息收集、分析
生成报告


安全需求分析
• 安全度量标准
• 安全功能
• 特定保密要求
• 特定环境要求
指导对测试层测试方法全局安全策略特定缓解措施的选择
威胁模型分析
• 测试层，测试方法
• 根据威胁分析定义测试层测试内容
• 全局安全策略
• 特定缓解措施
指导对污染传递的和测试内容的选择
测试内容分析
• 数据接口污染传递分析
• 数据接口语义分析
指导安全测试代理安装和定制开发
指导对安全安全策略的测试指导对特殊缓解措施的测试
指导对安全功能的测试
指导对数据接口与代码安全实现的测试
指导原始测试样本获取和覆盖性
安全测试预备
• 测试环境搭建
• 原始测试样本获取
• 测试样本覆盖性分析
• 安全测试代理安装
• 安全测试代理定制开发
原始测试样本
安全测试
• 基于安全需求验证安全功能
• 基于安全测试层验证全局安全策略
• 基于安全测试层验证特定缓解措施
• 基于安全测试层与数据接口验证代码安全实现
• 修补验证回归测试
安全报告
• 安全漏洞报告
• 安全测试报告
• 安全漏洞追踪和修复
验证安全功能实现
验证全局安全策略
验证特定缓解措施
验证代码实现安全
验证接口与语义安全
修复验证与回归测试
南京翰海源信息技术有限公司的基于数据流SDL的安全测试流程

测试技术驱动力

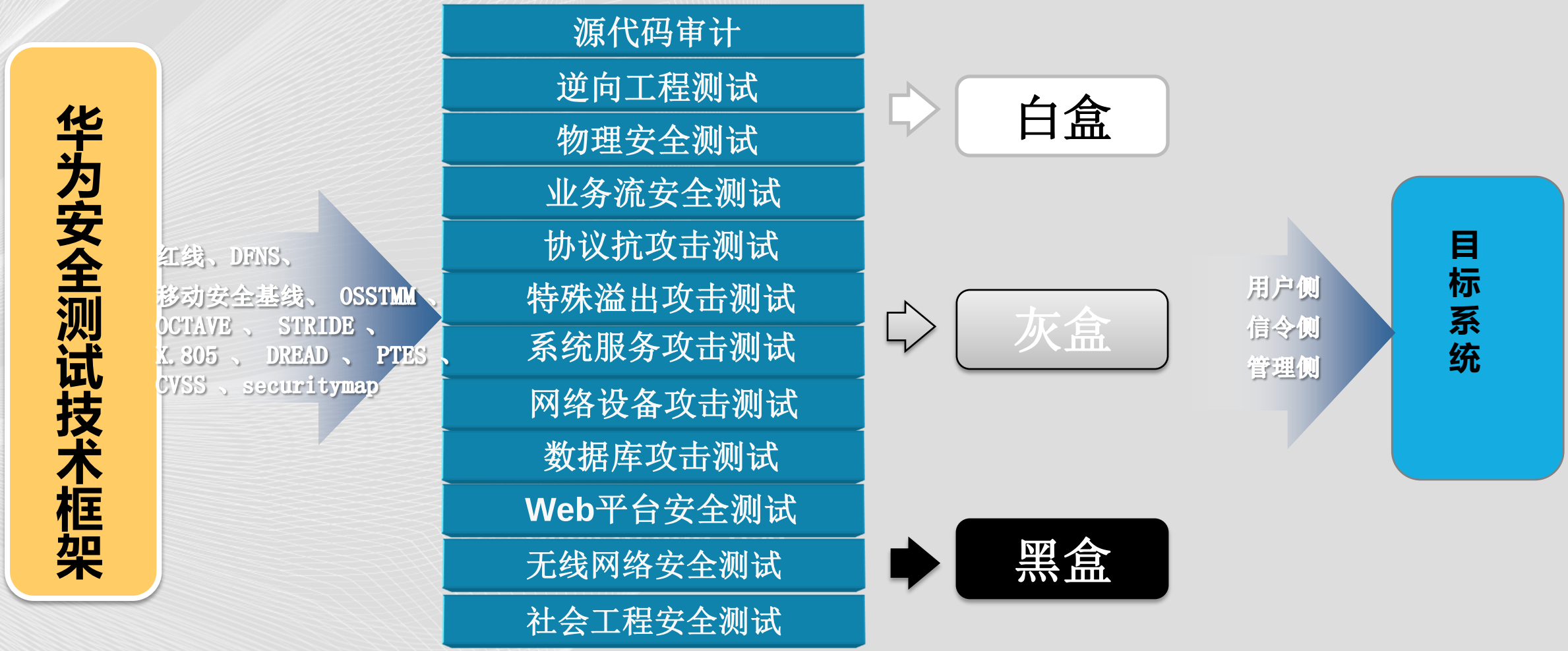
需求驱动

BT 21 cn、NIST、x805 、各运营商特殊安全要求

安全红线、安全能力建设,深度安全测试全面推广

服务创新

Huawei Security Testing Methodology Framework

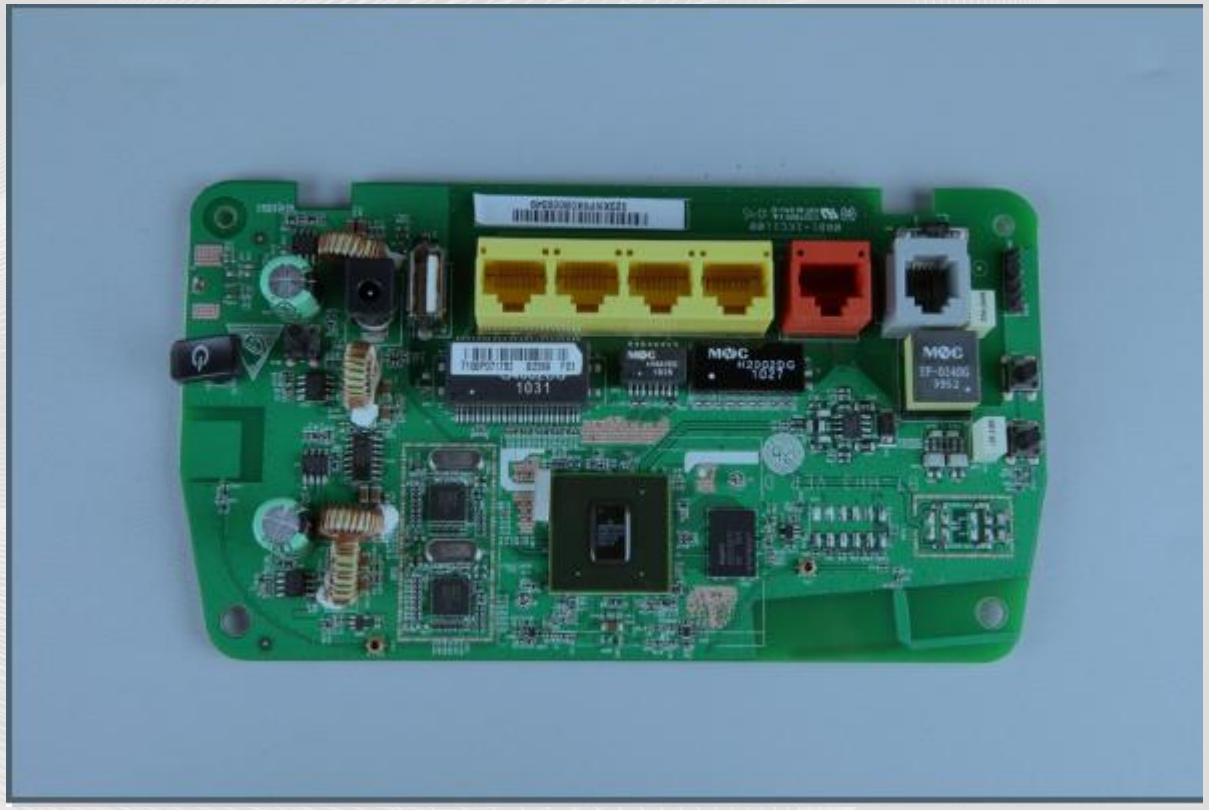


安全评估测试框架（依照项目要求进行裁切设计）

III 渗透测试-数据库系统类

测试名称	测试内容	使用工具	分析要点	更新人员	风险计数器（高危 红色 中：黄色，低绿色）	说明文档
oracle （1512）	Oracle 信息收集	Oracle TNSLSNR或者OTNSCmd	执行测试以下命令：[ping] [version] [status]	袁明坤		■ perl tnscmd.pl -h ip_address
	口令破解	checkpwd.exe或者OAK	弱口令字典猜+F54解，说明字典范围	袁明坤		1. 用法：checkpwd.exe SCOTT:F894844C34402B67
	Oracle缺省帐号密码猜解	手工+DBVisualizer	检查以下缺省用户的密码与用户名是否相同：	傅奎		
	hash分析	orabf	需要取到hash文件才能进行猜解	袁明坤		orabf [hash]:[username] [options]
	Oracle Sid 破解	guesssid	暂无	王申楠		用法：sidguess.exe host=ip地址 port=端口 sidfile=字典文件 地址：http://www.red-database-security.com/
	oracle TNS安全检测	lsnrcheck.exe	暂无	王申楠		地址：http://www.integrigy.com/downloads/lsnrcheck.exe
	Oracle配置文件审计	手工	查看关键的配置信息	袁明坤		
	检查是否启用数据库审计	手工	Oracle审计日志可以通过自身开关启动。部分企业为避免审计带来系统负担，采用旁路审计方式进行审计，此时需检查审计设备是否工作正常。	傅奎		sysdba帐号登录系统，执行：show parameter audit。若审计选项为DB或OS，则表示已开启，否则未开启
	数据库备份及日志文件分析	手工	查看记录中是否包含password等敏感信息	袁明坤		

物理&固件安全

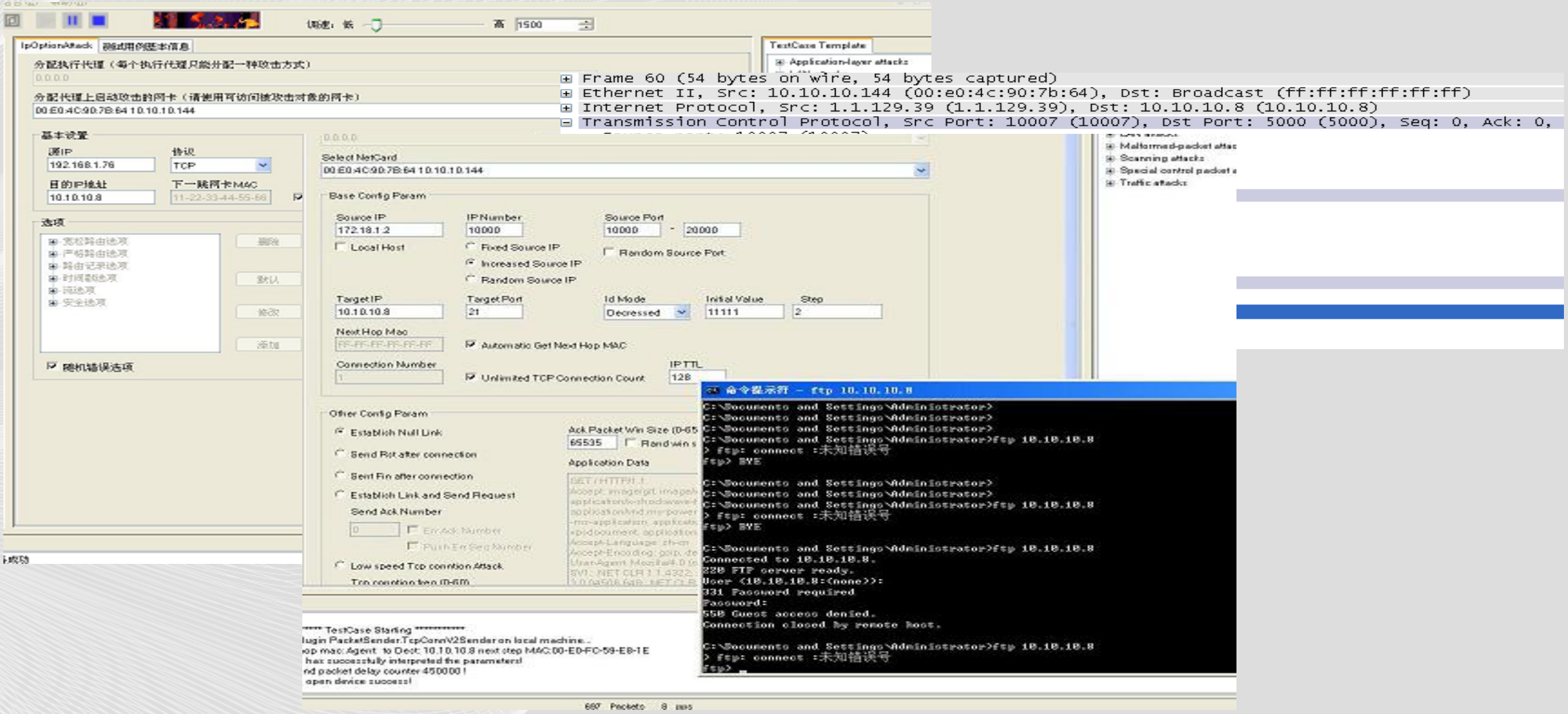


Port Label	Port type
ADSL	RJ11
BT Infinity	RJ45
Ethernet 1-4	4x RJ45
USB	USB
Power	Power jack

IDA View-A | Hex View-A | Structures | Enums | Imports | Exports

```
LOAD:00018C78 aSdcard          DCB "sdcard",0
LOAD:00018C7F aFileupload      DCB "fileupload",0
LOAD:00018C8A aSdfile          DCB "sdfile",0
LOAD:00018C91 aNvramul_cgi     DCB "nvramul.cgi",0
LOAD:00018C9D aCss             DCB "/css/",0
LOAD:00018CA3 aEtagSS          DCB "ETag: %s",0xD,0xA
LOAD:00018CA3                  DCB "%s",0
```

协议抗攻击测试


Frame 60 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: 10.10.10.144 (00:e0:4c:90:7b:64), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 1.1.129.39 (1.1.129.39), Dst: 10.10.10.8 (10.10.10.8)
Transmission Control Protocol, Src Port: 10007 (10007), Dst Port: 5000 (5000), Seq: 0, Ack: 0,
IpOptionAttack
TestCase Template
Base Config Param
Other Config Param
Source IP
IP Number
Source Port
Target IP
Target Port
Id Mode
Initial Value
Step
Next Hop Mac
Connection Number
IP TTL
Establish Null Link
Send Rst after connection
Sent Fin after connection
Establish Link and Send Request
Low speed Tcp conntion Attack
Application Data
命令提示符 - ftp 10.10.10.8
Connected to 10.10.10.8.
220 FTP server ready.
User (10.10.10.8:(none)):
331 Password required
Password:
550 Guest access denied.
Connection closed by remote host.

安全基线设计（实例）

业务系统网元	风险级别	风险名称	风险影响	基线解决方法
APM	高	任意文件下载漏洞	攻击者可获取服务器任意文件及用户敏感信息如FTP帐号口令，数据库连接口令，并可通过此控制AAA服务器。	方法一、 HS_DFNS_WEB_CODE_TRANS_01： 必须在服务器端采用白名单对上传或下载的文件类型、大小进行严格的限制 HS_DFNS_WEB_CODE_TRANS_02： 禁止以用户提交的数据作为读/写/上传/下载文件的路径或文件名，以防止目录跨越攻击； 建议对写/上传文件的路径或文件名采用随机方式生成，或将写/上传文件放置在有适当访问许可的专门目录。对读/下载文件采用映射表（例如，用户提交的读文件参数为1，则读取file1，参数为2，则读取file2）。防止恶意用户构造路径和文件名，实施目录跨越攻击。 对URL中文件参数和程序中文件名变量进行安全检查，禁止跨目录访问系统敏感文件和目录，如访问/etc/passwd，/etc/shadow,/etc/xinetd.d/vsftpd等

安全测试矩阵

安全测试矩阵		
安全测试模块	测试领域说明	是否测试
威胁分析	评估威胁来源层面	Yes
	评估威胁来源可能性	Yes
	评估威胁存在的潜在环境	No
硬件检查	设计文档安全视检	No
	安全架构检查	Yes
	组件识别	No
	危险组件安全评估	No
	硬件主体安全视检	Yes
代码审计	源代码审计	No
	硬件代码审计	No
	本地源代码开发过程文档审计	No
	代码认证信息审计	No
	固件更新来源检查	Yes
	固件反编译功能检查	Yes
界面测试	以太网接口	Yes
	WIFI接口	No
	USB接口	Yes
	ADSL	No
	3G&4G	No
协议压力测试	端口压力测试	No
	DoS	No
	IP 协议测试(tcp,udp)	No
业务安全测试	业务接口安全性分析	Yes
	业务逻辑安全性分析	Yes
	业务相关协议测试	Yes
渗透测试	社会工程测试	No
	脆弱性扫描测试	Yes
	开放服务测试	Yes
	web测试	No
	数据库测试	Yes
	os安全测试	Yes
	认证方式测试	Yes
	fuzz测试	Yes

生成当前业务系统安全测试矩阵

识别测试覆盖范围

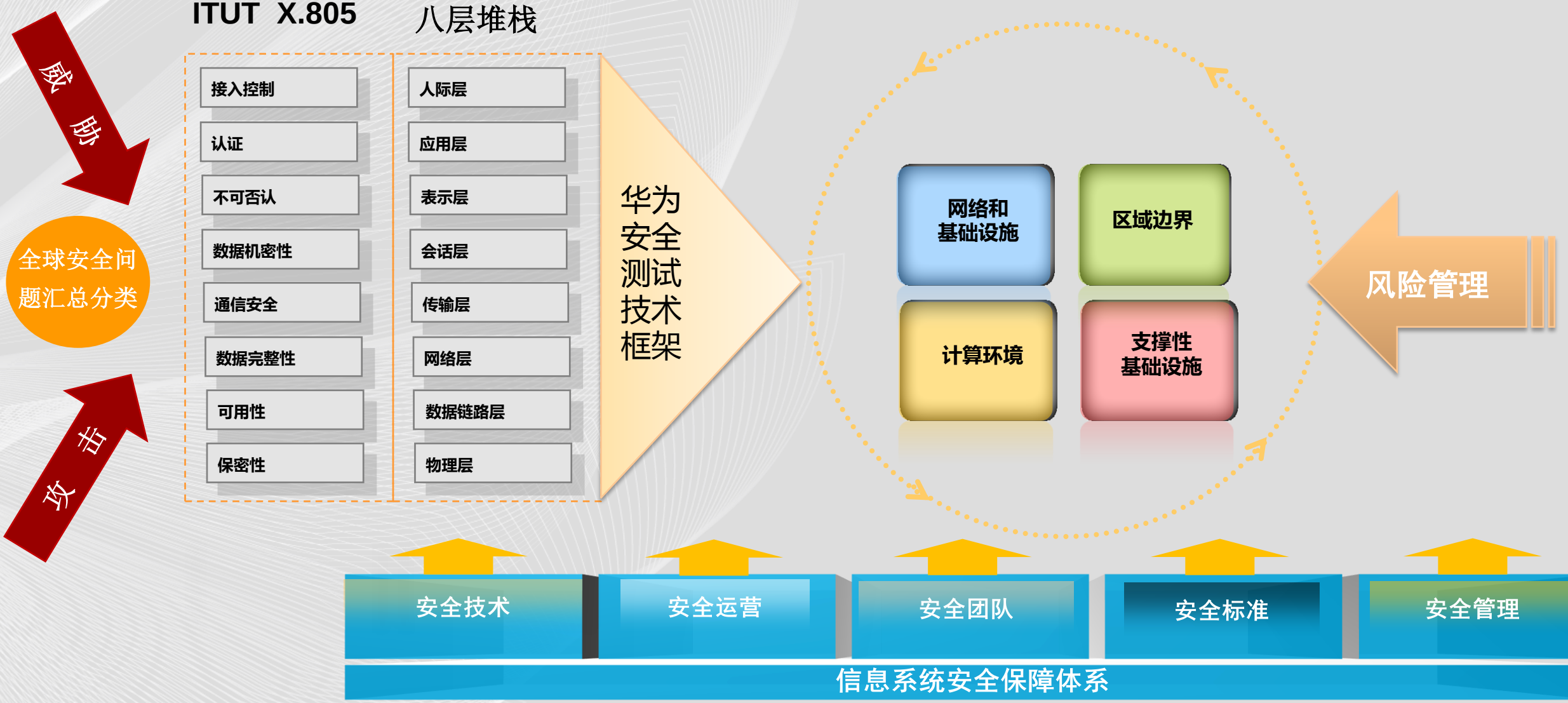
定制化的安全测试框架

固定标准来框架测试内容及范围，使专业人员和非专业人员可以针对安全测试的过程和结果达成共识,也可以使甲乙双方达成商务上的认可.

议程

- 华为安全测试技术框架
- 华为安全测试技术流程
- 端到端的安全体系
- 新的安全边界

整体安全保障方案


威胁
全球安全问题汇总分类
攻击
ITUT X.805
八层堆栈
接入控制
认证
不可否认
数据机密性
通信安全
数据完整性
可用性
保密性
人际层
应用层
表示层
会话层
传输层
网络层
数据链路层
物理层
华为安全测试技术框架
网络和基础设施
区域边界
计算环境
支撑性基础设施
风险管理
安全技术
安全运营
安全团队
安全标准
安全管理
信息系统安全保障体系

威胁识别

TRVA 威胁分析表

X.805安全纬度	含义	可能面临威胁
鉴权与身份（Authenti		1、 识别可能遭受攻击的组件 2、 已知漏洞攻击绕过鉴权与身份认证 3、 web及telnet 管理面攻击 4、 TR069协议绕过
权限控制（Access control）	此纬度主要防止对网络资源的未授权使用， 包括网元、存储的信息、信息流、业务与服务以及应用程序等。	1、 vpn ，IPsec 保护功能被绕过 2、 防火墙类访问控制措施缺陷 3、 USB 接口攻击
日志与审计（Non-repudiation）	此纬度主要防止个人或实体对已经执行过的操作进行抵赖。	1、 审计系统日志是否全面（是否涉及隐私泄露） 2、哪些攻击有日志。
机密性（Data confidentiality）	此纬度主要对数据提供保护使之不被非授权地泄露。	1、 固件被反编译 2. 硬件中敏感数据文件被非法获取 （ssl key类机密信息）
通信安全（Communication security dimension）	如：采用IPSec ESP保护终端的媒体流在接入XXX时（无论是移动或固定方式），即使被窃听也不会造成通信信息的非授权地泄露。	1、 访问通话信息：攻击者捕获报文，获得敏感信息 2、 IP/TCP/UDP/ICMP 协议Fuzz攻击 3、 802.1x ，UPnP ，IGMP 协议攻击
完整性（Date integrity ）	此纬度主要确保数据的准确性，对非授权地删除、修改能够提供指示 如：XXX网络在计费信息中采取的数据完整性保护的安全机制，防止计费信息被非法的篡改。	1、 固件更新来源被篡改
可用性（Availability）	此纬度主要确保授权的访问不被拒绝（包括容灾）。如：XXX网络边沿采用了防DOS攻击的安全机制，保证合法用户可以正常访问XXX网络，而不受到DOS攻击的影响。	1、IP DoS攻击攻击：单用户发起IP层Dos攻击。导致系统过载而无法处理正常业务。
隐私保护（Privacy）	此纬度主要针对个人的信息提供保护，例如个人访问过的WEB站点、个人的位置数据、以及个人的通信内容包括语音、短信等。	1、 用户账号密码泄露 2、 网络信息泄露

stride 说明

威胁	定义	对应的安全属性
Spoofing（伪装）	冒充他人身份	认证
Tampering（篡改）	修改数据或代码	完整性
Repudiation（抵赖）	否认做个的事情	不可抵赖性
InformationDisclosure（信息泄露）	机密信息泄露	机密性
Denial of Service （拒绝服务）	拒绝服务	可用性
Elevation of Privilege （提升权限）	未经授权获得许可	授权

风险定量

DREAD 说明			
等级 / 说明	高3	中2	低1
Damage Potential 影响等级	获取完全验证权限；执行管理员操作；非法上传文件	泄露敏感歇息	泄露其他信息
Reproducibility 重复性	攻击者可以随意再次攻击	攻击者可以重复攻击，但是有限制	攻击者很难重复攻击
Exploitability 易用性	初学者可以短期内掌握攻击方法	熟练的攻击者才能完成这次攻击	漏洞利用条件非常苛刻
Affected users 受影响用户	所有用户，默认配置，关键用户	部分用户，默认配置	极少数用户，匿名用户
Discoverability 利用难度	漏洞很明显，攻击条件很容易获得	在私有区域，部分人能看到，需要深入挖掘漏洞	发现该漏洞及其困难

DREAD 风险分析矩阵						
说明 / 风险	Damage Potential 影响等级	Reproducibility 重复性	Exploitability 易用性	Affected users 受影响用户	Discoverability 利用难度	总计
	3	3	1	2	3	12
	3	3	1	2	3	12
	1	3	3	1		8
	3	2	3	2	2	12
	2	3	3	1	1	10
	2	2	3	1	1	9
	3	2	2	2	2	11
	2	2	2	2	2	10
	3	3	2	2	3	13

风险分析

威胁及风险控制策略总结				
分类	说明	免费短信威胁分析结论	暴力破解威胁分析	
威胁	威胁编号			
	威胁描述			
攻击场景分析（需绘制模型图）	攻击条件			
	攻击技术			
	攻击步骤			
现有安全机制评估	现有安全机制			
	威胁指数			
	威胁检测维护机制			
	差距分析			
	改进建议			

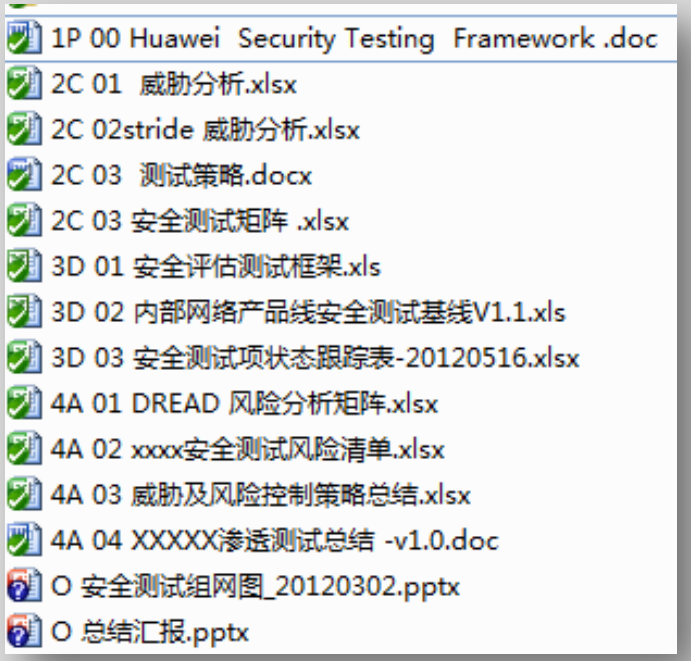
风险闭环

xxxx安全测试/新增风险问题清单

编号	类别	名称	风险值	风险级别	是否确认	处理意见	责任人
NV-01	信息泄漏	xxx日志路径设置不当导致敏感信息泄漏	10	中			工程
NV-02		xxxx配置文件路径不当导致服务器敏感泄露	11	中			工程
NV-03		xxxxx页面PMS系统绝对路径泄露	7	低			QS
NV-04		xxxxxxp配置文件路径不当导致服务器敏感泄露	10	中			QS
NV-05		xxxxx帮助文档包含员工工号信息	7	低			
NV-06		代码注释中存在员工姓名	7	低			工程
NV-07	密码安全	配置文件明文存储数据库账号密码（Database..cfg）	10	中			
NV-08		配置文件明文存储密码(loginInfo.xml)	10	中			
NV-09	编码安全	不安全的Cookie存储方式(HTTP Only)	11	中			QS
NV-10		xxxx模板导入功能可导入非法文件	14	高			QS
NV-11		xxxxxxTask页面可执行系统风险命令	13	高			QS
NV-12		xxxxx Task功能可打包操作系统所有文件	13	高			QS
NV-13	跨站攻击	xxxxx Task描述信息输入框存在跨站脚本攻击漏洞	12	高			QS
NV-14		xxxxx模板文件导入未作合法性检查存在XSS漏洞	12	高			QS
NV-15		xxxxx计划任务描述输入框存在跨站脚本攻击漏洞	12	高			QS
NV-16		XXXX页面存在跨站脚本攻击漏洞	7	低			工程
NV-17	权限控制	XXXXt未对DumpPath输入框做权限控制	6	低			传送
NV-18		HA配置管理界面未做访问鉴权	6	低			QS
NV-19		XXXX Maintenance Suite备份软件未限定备份目录	6	低			工程
NV-20		xxxx后台未授权用户任意访问	15	高			QS
NV-21	配置缺陷	Web服务器启用了代理功能（8080）	11	中			

项目技能传承

- 00 安全评估测试框架
- 01 威胁分析模型
- 02 安全测试策略
- 03 安全测试矩阵
- 04 网络安全红线建议说明
- 05 DREAD 风险分析矩阵
- 06 威胁及风险控制策略总结 或 安全测试风险清单
- 07 安全测试报告
- 08 人员培养计划



人员提升计划--大纲

安全测试技术

- 通用攻防技能|高级扫描技术
- Web 安全|windows主机攻防| Linux/Unix攻防|数据库攻防 |网络层攻防技术|社会工程技术 |恶意代码分析技能 |终端安全技术 |安全评估技术框架实战
- 代码安全分析与审计| 逆向工程 | 硬件安全 | 高级无线攻防(3g 手机)

威胁识别

- 全网安全综述|云安全|无线安全(初级)
- IPV6安全技术|物联网安全| 安全评估技术框架 | 威胁建模
- 8纬度安全防护技术

风险控制技术

- 风险评估技术 | 业务安全评估技术
- 应急响应及取证技术

安全管理

- 网络安全体系概述|网络安全体系设计
- ISO27001|信息安全等级化保护体系| COBIT控制框架| SOX萨班斯法案
- 典型企业安全框架|信息安全体系规划与治理模拟
- 企业安全团队架构

讲师技巧

- 内训课程分析介绍|职业理念训练| 专业技巧及教法训练
- 教学互动能力训练|课程设计能力训练|

议程

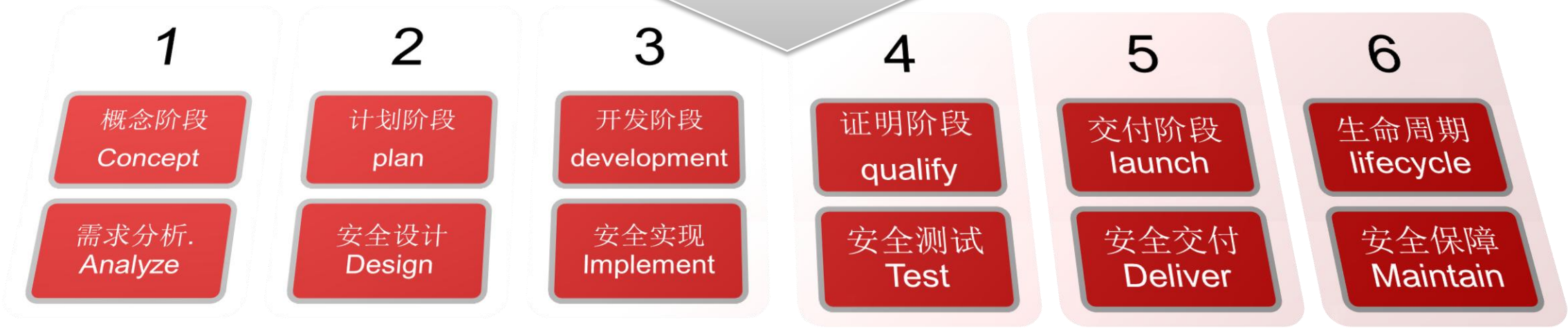
- 华为安全测试技术框架
- 华为安全测试技术流程
- 端到端的安全体系
- 新的安全边界

vulnerability database

threat&attack database

security design pattern database

华为端到端基准线
安全性体系结构



增强型端到端的安全性保障服务

---看得到的安全 ,全生命周期的安全保障

解决方案层层检测	交付过程安全保障	安全运维持续改进
输出	输出	输出
• 产品安全白皮书 • 产品安全评估报告 • 产品安全测试矩阵	• 系统上线前安全评估报告 • 系统环境威胁分析报告	• 业务系统安全优化咨询报告 • 安全测试审计报告 • 安全人员培训课程（可选）

Security Test Audit Report 安全测试审计报告

Security Verification Certification

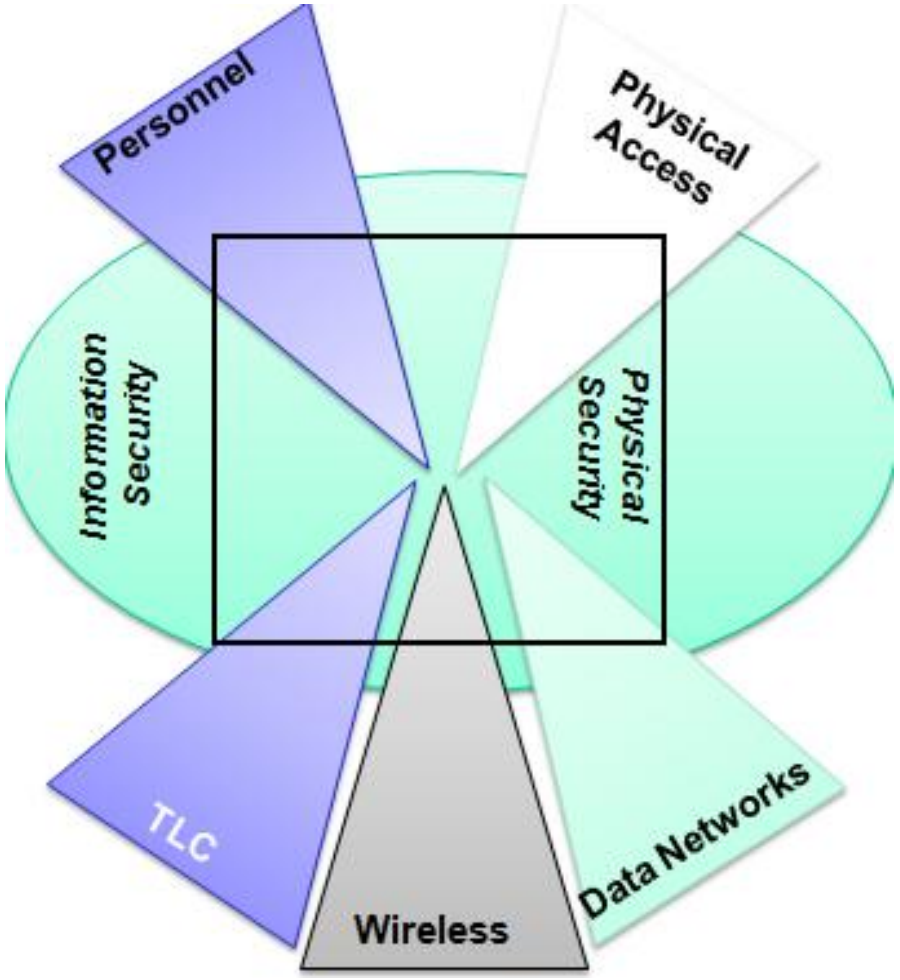
Phase阶段	TASK 工作内容	Description目标	COMMENTS 注释
A. Induction Phase 汇总阶段 （了解的审核要求，范围，和此范围内的测试约束条件。通常情况下，测试类型最好是确定此阶段之后。）	**a.1. POSTURE REVIEW 态势评估**	确定被评估企业的经营目标和市场范围，确定业务需要遵循的法规政策，行业标准及企业文化和规范特性，确定评估过程中	所有已知的环节都要测试覆盖到，C阶段可以用来补充保障测试完整性
	1.1 Identified business objectives and markets. 确定企业目标战略和市场		
	1.2 Identified legislation and regulations applicable to the targets in the scope. 确定目标企业适用的，需要遵守的法律法规及其他行业规章条例		
	1.3 Identified business policies. 确定企业方针政策		
	1.4 Identified business and industry ethics policies. 确定企业和业界的伦理道德规则（潜规则）		
	1.5 Identified operation cultures and norms. 确定运营文化和规范要求		
	1.6 Identified operation times and flows applicable to the targets in the scope. 确定操作的时间和流程适用的范围内的目标		
	1.7 Identified all necessary Channels for this scope. 确定关键路径和所有通道路径		
	1.8 Identified all Vectors for this scope. 确定范围内所有主体		
	a.2. LOGISTICS 安全测试背景调查	确定测试范围，明确任务完成标准，确定测试风险，确定可接受风险，明确何种情况下需要停止测试	了解审计本身的风险，这将最大限度地减少错误和提高工作效率
	2.1 Applied testing safety measures. 实用测试安全保障措施及规程		
	2.2 Determined and accounted for test instabilities. 明确描述测试风险		
	2.3 Determined and accounted for downtime in scope. 明确描述测试可能引起的中断时间及范围		
	2.4 Determined and accounted for test pace according to the test environment and the security presence.明确描述测试环境和安全现状		
	a.3. ACTIVE DETECTION VERIFICATION 主动探测验证	明确接口，端口信息，确定误报信息，明确测试约束条件，确定防护规则有效性	通过主动探测了解现状，为B，D阶段提供必要保障

RAVs | Sheet1 | Check List

议程

- 华为安全测试技术框架
- 华为安全测试技术流程
- 端到端的安全体系
- 新的安全边界

攻击路径



OSSTMM

在2.0基础上改进和提升的OSSTMM3.0版本将测试内容分为3层：

- **PHRSEC**
- **SPECSEC**
- **COMSEC**

Thank you

www.huawei.com

Wall of Sheep

OWASP 杭州区沙龙

用户名	密码	IP	协议类型
		74.125.140.108	IMAP
		:110	POP
		210.2.*.*:21	FTP
		211.167.*.*:993	IMAP