

# TAF WG4 信息安全工作组汇报

**杨正军**  
2017年8月



中国信息通信研究院  
<http://www.caict.ac.cn>

「我们·在路上」

### 工作内容



- WG4组通过工作组会议、技术交流会等形式展开工作；
- 以技术文件、协会标准、研究报告等方式输出工作内容。

- 发布了7项协会标准
- 在研2项标准
- 发布3份研究报告

### 专注安全



- 北京握奇数据系统有限公司
- 北京豆荚科技有限公司
- 北京奇虎科技有限公司
- 江苏通付盾信息科技有限公司
- .....

自2014年以来，WG4组迅速成长为终端信息安全领域的聚合型平台，并吸纳多家专注安全领域的公司加入TAF。

## TAF | WG4

### 成果输出

- 基于标准开展检测认证

### 国际合作

TAF与Global Platform、FIDO  
国际标准组织开展合作

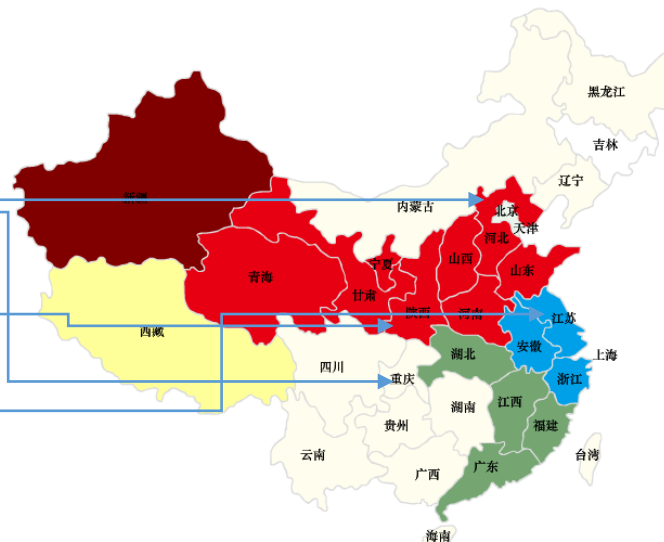
2017年TAF 信息安全工作组 (WG4) 共拟召开**3**次技术交流会、**4**次小组会

2017/03/22/北京

2017/6/12/武汉

2017/9/7/西安

2017/12/南京



时间	演讲主题	演讲人
9:00~9:30	移动未知威胁感知与防御	傅建明(武汉大学)
9:30~10:00	Android security in O	李东方(谷歌)
10:00~10:20	茶 歇	
10:20~11:00	“永恒之蓝”引发的移动安全思考	倪昶溪(中国信通院)
11:00~11:30	iOS 漏洞检测与安全防护技术	陈美坤(通付盾)
11:30~12:00	移动漏洞的防护闭环	陈霖林(安天)
12:00~14:00	午 餐	
14:00~14:30	从 Wanacrypte 看移动端勒索软件的现状与趋势	张源(复旦大学)
14:30~15:00	我国移动智能终端预置应用软件安全发展报告	董斐(中国信通院)
15:00~15:40	蝴蝶效应与程序错误-Chrome 漏洞分析	龚广(奇虎360)
15:40~16:00	茶 歇	
16:00~16:30	路由器和 Android 的双生蠕虫	李伟(猎豹移动)
16:30~17:00	浅谈安卓恶意程序的鉴定和溯源	钱林松(科锐逆向)

时间	演讲主题	演讲人
9:00~9:30	TEE 安全评估总结(软件)	焦四攀(中国信通院)
9:30~10:00	TEE 安全评估总结(硬件)	魏凡星(中国信通院)
10:00~10:20	茶 歇	
10:20~11:00	媒体融合与 ChinaDRM	王磊(ChinaDRM)
11:00~11:30	TEE/SE 在第三方支付的应用	孙元博(蚂蚁)
11:30~12:00	为连接设备设计安全与信任	王俊超(ARM)
12:00~14:00	午 餐	
14:00~14:40	TEE 的机遇与挑战	夏虞斌(上海交大)
14:40~15:10	华为终端在 TEE 应用领域的创新和探索	李雨航(华为)
15:10~15:40	TEE Sim 在物联网模组中的应用	吴俊(上海果通)
15:40~16:00	茶 歇	
16:00~16:30	总结和讨论	全体

2017年6月12日，TAF WG4 举办2017年“移动漏洞威胁防护及应对”技术交流会。来自谷歌、武汉大学、复旦大学、安天、猎豹移动等单位的专家学者出席了本次大会并发表演讲，60余家企业的150余人参加了本次会议。本次会议对移动漏洞的成因、现状、危害进行了深入分析，并对漏洞的防护和应对提出切实可行的参考方案，是移动漏洞技术领域的一次盛会。

2017年9月7日，TAF WG4拟在西安召开“2017年TEE技术与行业发展交流会”

## 推进《移动智能终端应用软件预置与分发管理暂行规定》落地

### 标准规范

- 《移动智能终端应用软件分类与可卸载实施指南》，CCSA行业标准、TAF协会标准
- 《移动智能终端预置软件信息公开指南》，TAF协会标准

### 政策出台

- 前期调研：拟定了重点针对移动智能终端生产企业和互联网信息服务提供者的应用软件预置和分发行为，加强行业管理、保障消费者合法权益的工作思路；
- 起草规定：广泛听取移动智能终端生产企业、互联网企业、基础电信运营商、地方通信管理局等的意见，拟定了《规定》（征求意见稿）；
- 征求意见：我部根据公开征求意见期间收到的反馈意见，对《规定》做了进一步的修改和完善。此外，我部还按照国际惯例，将《规定》向WTO/TBT进行通报；
- 规定发布：在上述工作基础上，我部按照规定流程于2016年12月正式发布《移动智能终端应用软件预置和分发管理暂行规定》。

### 摸底测试

- 2017年5月1日起，检测机构对2016年销量TOP15的手机生产企业参照《暂行规定》相关要求进行摸底抽检，督促企业进行补充、修改。

### 正式实施

- 宣贯：在北京、深圳、上海、西安多次召开宣贯会议，向厂家宣贯并解读可卸载、明示等相关要求。

序号	应用名称	功能描述	类别	注意事项
1	桌面	提供系统桌面功能，若卸载系统界面无法显示	基本功能类-操作系统基本组件	至多有一个可设置为不可卸载
2	主题	提供系统主题	基本功能类-操作系统基本组件	至多有一个可设置为不可卸载
3	计算器	数学计算	扩展功能类	应支持卸载
4	邮件	提供电子邮件收发、展示功能	扩展功能类	应支持卸载
5	壁纸	提供桌面壁纸	基本功能类-操作系统基本组件	最多保留一个不可卸载
6	游戏中心	提供多种游戏下载分发，与应用商店等同处理，仅保留一个	基本功能类-操作系统基本组件	最多保留一个不可卸载
7	天气	获取世界上一个或多个城市当前气温和未来十天的天气预报	扩展功能类-终端厂商扩展应用	应支持卸载
8	黑洞、雷光、泡泡等	Android原生壁纸	基本功能类-操作系统基本组件	最多保留一个不可卸载
9	地图	检测地址信息，并与其它应用交互	扩展功能类-终端厂商扩展应用	应支持可卸载

## 漏洞安全检测

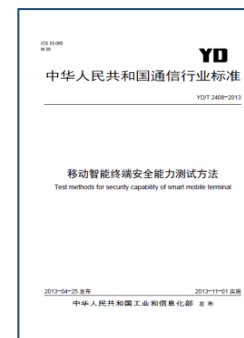


配合YD/T《移动智能终端安全能力技术要求》新标准实施，正式开展漏洞5级检测。提供线下线上检测业务及培训服务。

# 5级

**操作系统漏洞要求  
应用软件漏洞要求**

移动智能终端应保证不含有CNVD与CNNVD6个月前公布的高危漏洞。



## 漏洞安全标准\权威发布

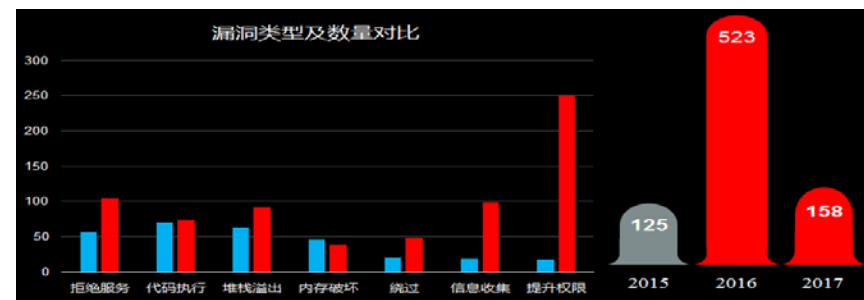


《移动智能终端漏洞威胁评价方法》标准讨论

## 漏洞安全研究



移动智能终端漏洞危害评价方法  
移动智能终端安全能力技术要求  
移动智能终端安全能力测试方法  
漏洞安全检测报告



## 落实网络安全法

- 第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

## 推进信息安全检测认证



根据行业所需制定协会标准

智能终端安全评测

应用软件安全评估

TEE一致性评估



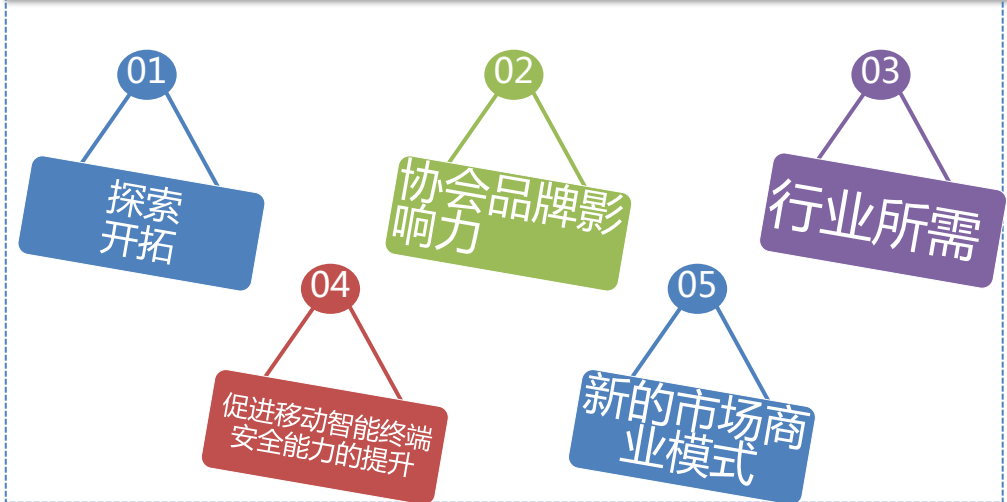
利用第三方实验室进行测试



	<b>ZTE S2010</b> 厂家：中兴 完成时间：2015-06-02 操作系统：Android 5.1		<b>SM-P355C</b> 厂家：三星 完成时间：2015-04-02 操作系统：Android 5.0.2 等级：1-5
--	--	--	---

TAF平台对检测结果进行公示

在TAF平台开展检测认证工作，一方面满足行业所需，促进移动智能终端安全能力的提升，另一方面对协会在整个行业所起作用进行探索和开拓，进一步扩大协会的品牌和影响力，让TAF协会会员受益。



谢谢聆听，  
敬请批评指正！