智能手机安全漏洞研究

国家计算机网络入侵防范中心

张玉清

zhangyq@nipc.org.cn

2012，11，29

Xdef会议，武汉

内容提要

- 一 引言
- 二 手机漏洞研究发展现状
- 三 手机安全方向论文发表现状
- 四 未来趋势展望

内容提要

- ✓ 一 引言
- ◆ 二 手机安全漏洞现状
- ◆ 三 安全国际顶级会议手机论文情况
- ◆ 四 未来趋势展望

一 引言

手机安全已成为必须解决的重要社会问题

2011年02月22日 发布

FT中文网 商业/传媒与文化

首页 中国 全球 经济 金融市场

2011年02月22日 06:48 AM

Android在中国深陷吸费沼泽

中国红麦软件总裁 刘兴亮 为英国《金融时报》中文网撰写

蹊跷的是，盛世往往就会伴随着危机。刚刚步入2011年，Android在中国就遭遇了“吸费”之痛，一如谷歌在华高速发展之际，在2010年却遭遇了“退出”之痛。

手机僵尸病毒

手机间谍软件

运营商面临“三座大山”

1. 移动客户：**用户投诉频发**；
2. 媒体和社会：手机安全被**频繁曝光**；
3. 工信部：安全问题，**谁接入谁负责**

一 引言

- 手机已成为现代社会中不可或缺的通信工具
  - 截至**2011**年**2**月底，国内移动通信用户总数突破**10**亿
  - 早在**2007**年，手机在国内城市的普及率已达**93%**



一 引言

- 智能手机开始逐步普及
- 什么是智能手机？
  - 目前尚不存在严格的定义
  - 一般认为应符合以下特征
    - 搭载统一且开放的操作系统平台
    - 具备强大的处理能力和存储能力
    - 提供多样化的通信方式

一 引言

□ 智能手机的安全问题开始浮现

- ✓ 案例：手机僵尸病毒
  - ■ **2010年11月7日，央视《每周质量报告》首度报道**
    - □ 被感染手机自动向其他手机用户发送带毒短信
    - □ 用户一旦阅读短信并访问恶意链接，就会感染成为新的“僵尸手机”
  - ■ **9月第一周：100万部手机感染，每天消耗用户话费约200万元**
  - ■ **截至2011年10月，变种已达10种以上，累积感染用户数量突破150万**

内容提要

- 一 引言
- ✓ 二 手机安全漏洞现状
- 三 安全国际顶级会议手机论文情况
- 四 未来趋势展望

二 手机安全漏洞现状

- 智能手机漏洞简介
- 形成原因
- 发展历史及研究现状
- 挖掘与利用技术

二 手机安全漏洞现状

- ✓ 智能手机漏洞简介
- □ 形成原因
- □ 发展历史及研究现状
- □ 挖掘与利用技术

2.1 智能手机漏洞简介

- 手机病毒传播方式多种多样
  - 短信/彩信中的带毒链接
  - 手机软件捆绑安装
  - 手机漏洞（手机安全漏洞）
- 漏洞
  - 又称“脆弱性”（接下来将不加区分地使用这两个术语）
  - 是信息系统在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷和不足
  - 攻击者可以利用漏洞，在未授权的情况下访问或破坏系统
- 智能手机是一个复杂的软硬件系统，同PC一样存在漏洞的威胁

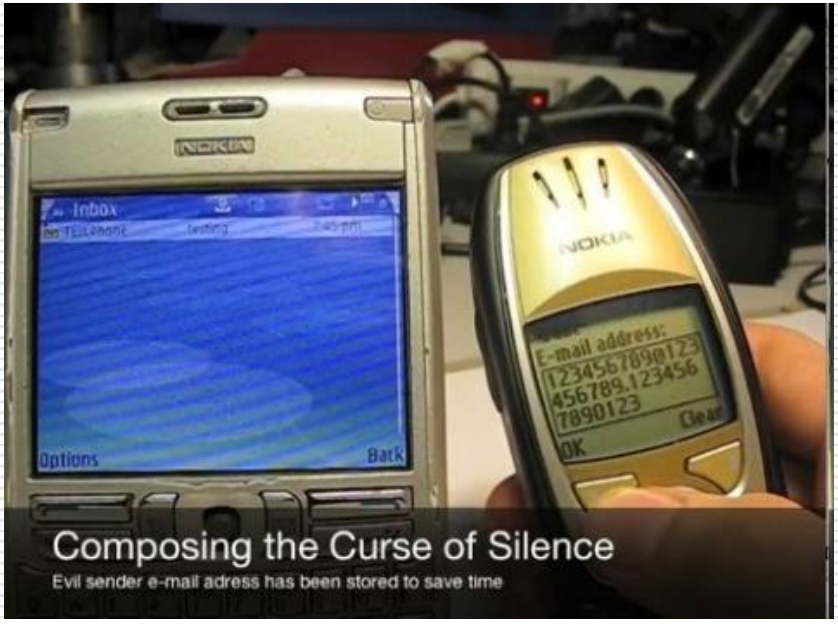
安全漏洞的威胁

- 漏洞导致安全威胁
  - 近年来，计算机病毒、木马、蠕虫和黑客攻击等日益流行，对国家政治、经济和社会造成危害，并对Internet及国家关键信息系统构成严重威胁。绝大多数的安全威胁是利用系统或软件中存在的安全漏洞来达到破坏系统、窃取机密信息等目的，由此引发的安全事件也层出不穷。
- 案例
  - **2010**年微软极光漏洞导致**Google**被攻击事件
  - **2011**年远程命令执行漏洞导致**360**和**QQ**大战事件
  - **2012-11-24**，**Android**短信欺诈漏洞已遭大规模利用，超**120**万部手机中招　　中国新闻网

2.1 智能手机漏洞简介

- 案例1：诺基亚智能手机“沉默的诅咒”（2009）

  - ✓ 使用短信向诺基亚S60系统的智能手机发送一条长度超过32字符且以空格结尾的email地址
  - ✓ 将导致对方手机在不知不觉中失去接收短信和彩信的功能
  - ✓ 必须重新对手机进行格式化才能恢复正常



2.1 智能手机漏洞简介

- 案例2：花旗银行iPhone应用程序漏洞 (2010)

  - ✓ 花旗银行iPhone手机银行的应用程序中存在敏感信息泄漏漏洞
  - ✓ 在保存信息时，会意外的泄露客户iPhone中的隐藏文件
  - ✓ 这些资料也可能会在用户和PC用iTunes进行同步的时候通过iPhone保存到PC中，造成敏感信息进一步的扩散

2.1 智能手机漏洞简介

- 案例3：**HTC Android**系统权限绕过漏洞 **(2011)**

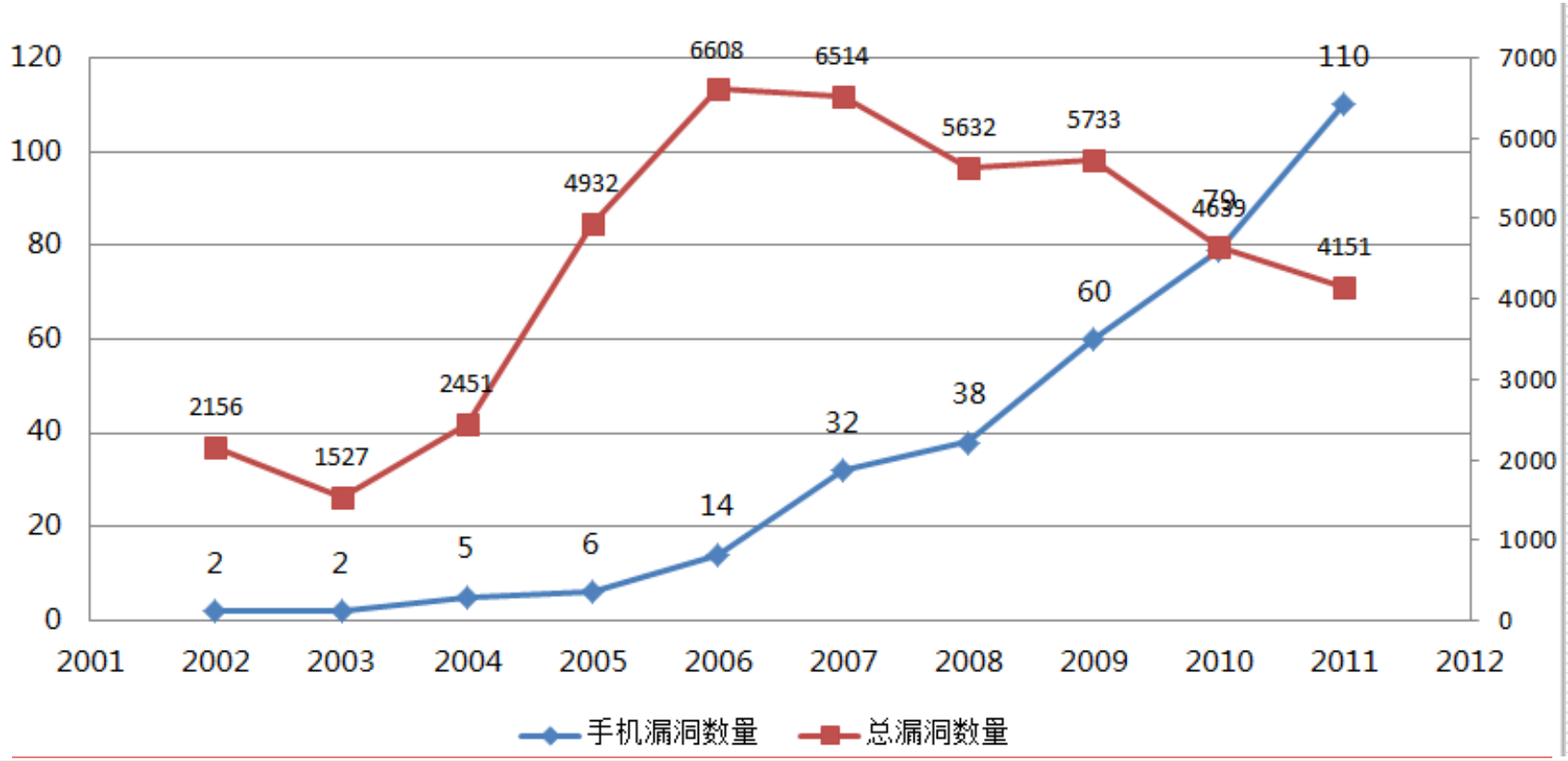
  - ✓ 使用**HTC Sense**界面的手机存在权限绕过漏洞
  - ✓ 应用程序只要拥有**Internet**访问权限就可以通过这个漏洞将用户的私人信息发送到指定的设备当中
  - ✓ 通过该漏洞甚至可以通过安装相关的应用程序来实现整部手机的控制。

2.1 智能手机漏洞简介

- 上述三个案例仅仅是手机漏洞可能造成危害的冰川一角
- 利用各类手机漏洞，攻击者可以：
  - 令手机失去通信功能，造成拒绝服务（案例1）
  - 窃取存储在手机上的敏感信息（案例2）
  - 监听用户的通话、短信和彩信
  - 令手机发送垃圾信息，制造恶意扣费并使手机网络拥塞
  - ……
- 危害严重，有必要展开深入研究

2.1 智能手机漏洞简介

- 手机漏洞数量的年度走势



（数据来源：NVD）

2.1 智能手机漏洞简介

- 国际上，手机安全漏洞方面的研究在近两年已经成为了热门领域
  - 在著名的**Blackhat**黑客会议上，每年都有研究者对手机上的安全漏洞挖掘展开讨论
- 国内在手机漏洞方面的研究仍刚刚起步，已经不能适应社会经济发展的需求
- 我们课题组在国内最早展开手机安全漏洞研究

二 手机漏洞研究发展现状

- 智能手机漏洞简介
- ✓ 形成原因
- 发展历史及研究现状
- 挖掘与利用技术

2.2 形成原因

- 智能手机的软硬件结构与PC平台并无根本区别
  - 硬件方面
    - 基于处理器和存储器两大核心部件
    - 根据存储程序工作原理设计
  - 软件方面
    - 基于分页的内存管理、多任务/多线程
    - 部分手机操作系统直接由PC操作系统衍生而来
- 因此，手机漏洞的形成原因与PC平台具有一定的相似性
- 但由于手机这个移动通信平台的特点，手机漏洞的表现方式具有自身的独特之处

2.2 形成原因之一：设计错误

- 设计错误
  - 系统在设计时考虑不周全，往往引入安全漏洞
  - 具有一定规模的系统都不可避免存在设计错误
- 手机系统中的设计错误往往存在于两个方面
  - 用户界面
    - 设计不合理的用户界面允许攻击者扰乱正常的界面交互，阻止用户使用手机的功能，或者泄漏手机中的敏感信息
  - 通信协议设计上的错误
    - 例如通信协议的身份认证部分存在问题，攻击者能够借此绕过安全机制，获取未授权访问

2.2 形成原因之一：设计错误

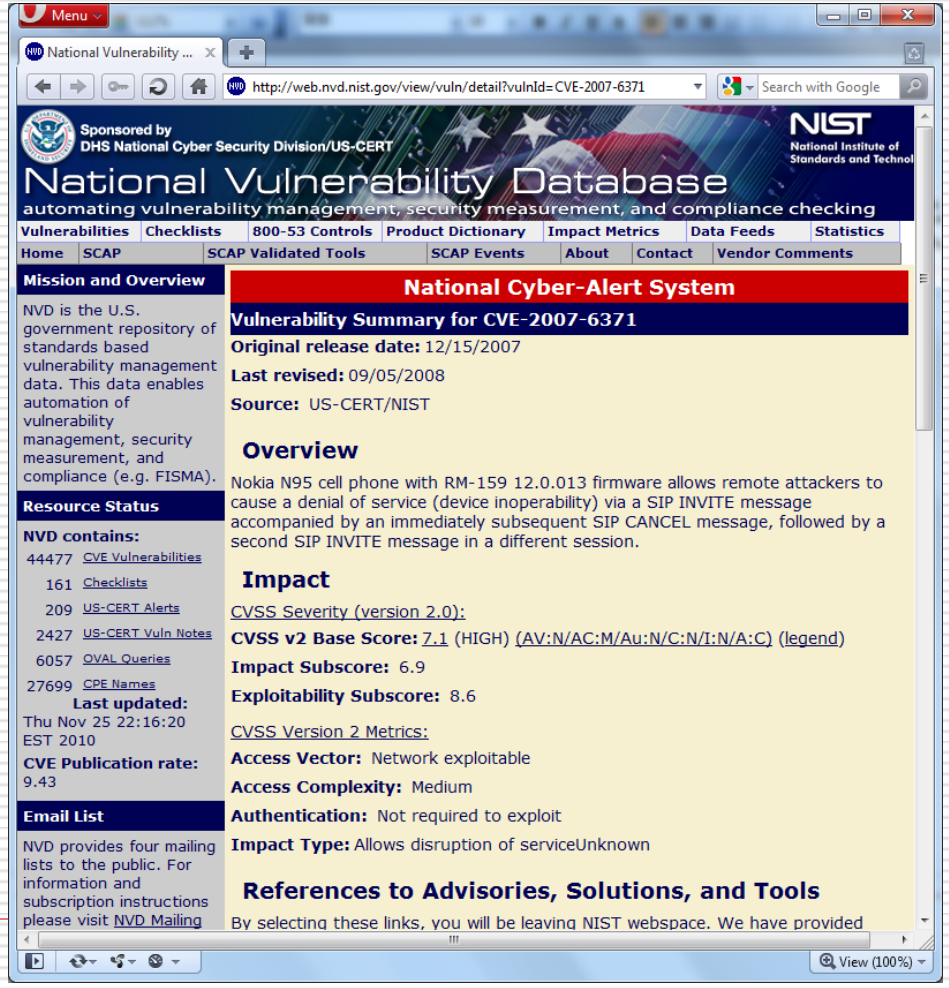
- 案例：iPhone屏幕锁绕过漏洞
  - 通过紧急呼叫轻松绕过锁屏限制
  - 可以查看：
    - 最近通话记录
    - 本机联系人列表
    - 语音邮件

2.2 形成原因之二：异常条件处理失败

- 异常条件处理失败
  - 手机平台硬件资源受限，要求程序有很强的健壮性
  - 如果程序对异常条件处理不当，有可能导致整个操作系统崩溃或无响应
  - 对用户来说，表现为手机无法响应用户的按键操作，造成拒绝服务

2.2 形成原因之二：异常条件处理失败

- 案例：诺基亚**N95 SIP**消息拒绝服务漏洞
  - 向手机发送一条**SIP INVITE**消息后紧接着发送一条**SIP CANCEL**消息
  - 导致手机出现拒绝服务（不响应用户操作）

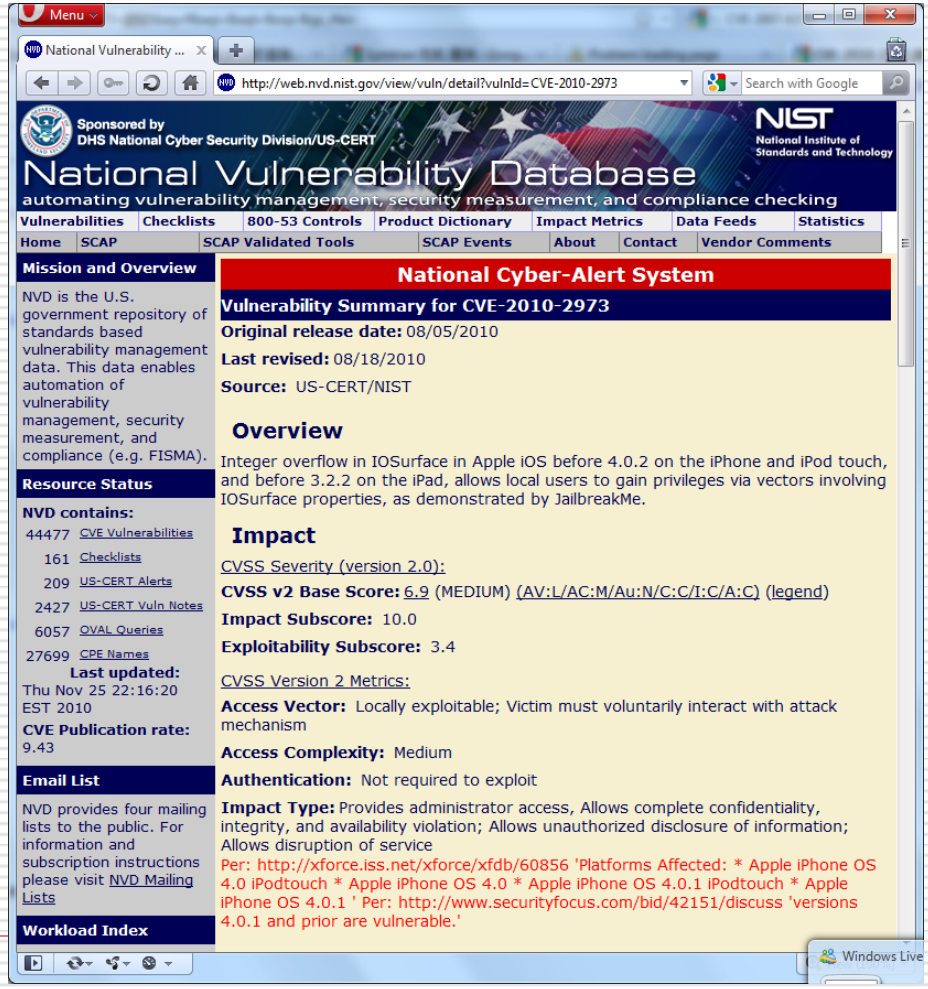


2.2 形成原因之三：边界条件错误

- 边界条件错误
  - 设计程序时需要对缓冲区等进行边界检查
  - 错误或不完整的边界检查会在处理非正常输入时造成程序执行错误
  - 此类漏洞中最常见的为缓冲区溢出类漏洞
    - 往往导致任意代码执行
    - 允许攻击者向手机中植入恶意软件，危害严重

2.2 形成原因之三：边界条件错误

- 案例：**iPhone**整数溢出漏洞
  - 存在于**iPhone**操作系统**iOS**的**IOSurface**组件中
  - 本地用户可以利用该漏洞提升权限
  - 将该漏洞与另外一个漏洞结合可实现**iPhone**的越狱



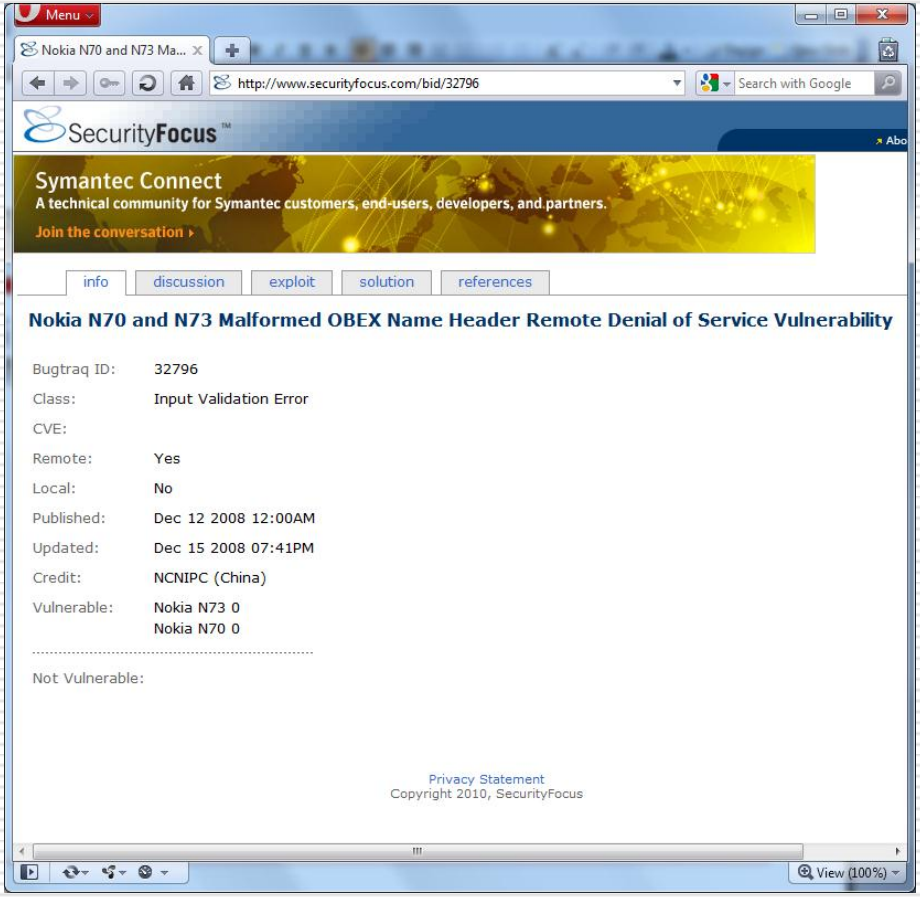
2.2 形成原因之四：输入验证错误

- 输入验证错误
  - 在处理输入信息时，对输入信息中的特殊字符串或者格式验证不完全
  - 可能导致拒绝服务，或者泄漏敏感信息，甚至会导致执行任意代码或权限提升

2.2 形成原因之四：输入验证错误

- 案例：诺基亚**N70/N73**蓝牙**OBEX**协议拒绝服务漏洞

- ✓ 若**OBEX**协议的**Name**字段包含如下特殊字符，将导致对方手机死机：
  - **Tab (0x09)**
  - **Line feed (0x0a)**
  - **Vertical tab (0x0b)**
  - **Form feed (0x0c)**
  - **Carriage return (0x0d)**
  - **‘:’ (0x3a)**
  - **‘\’ (0x5c)**



二 手机安全漏洞现状

- 智能手机漏洞简介
- 形成原因
- ✓ 发展历史及研究现状
- 挖掘与利用技术

2.3 发展历史

- 同步于智能手机本身的发展历史
- 可以划分为三个阶段
  - 固化程序型漏洞阶段
  - 系统接口型漏洞阶段
  - 手机应用型漏洞阶段

2.3 发展历史 – 固化程序型漏洞阶段

- 固化程序型漏洞阶段
  - 时间：**2002**年至**2004**年
  - 手机系统特点
    - 处于功能手机（**Feature Phone**）到智能手机（**Smart Phone**）的过渡阶段
    - 多数手机都不具备通用操作系统平台
    - 大量应用软件固化于手机内部芯片中，系统可扩展性较弱
  - 漏洞只存在于手机内固化的程序中
    - 一般不具备普遍性，仅在特定的手机机型中存在

2.3 发展历史 - 固化程序型漏洞阶段

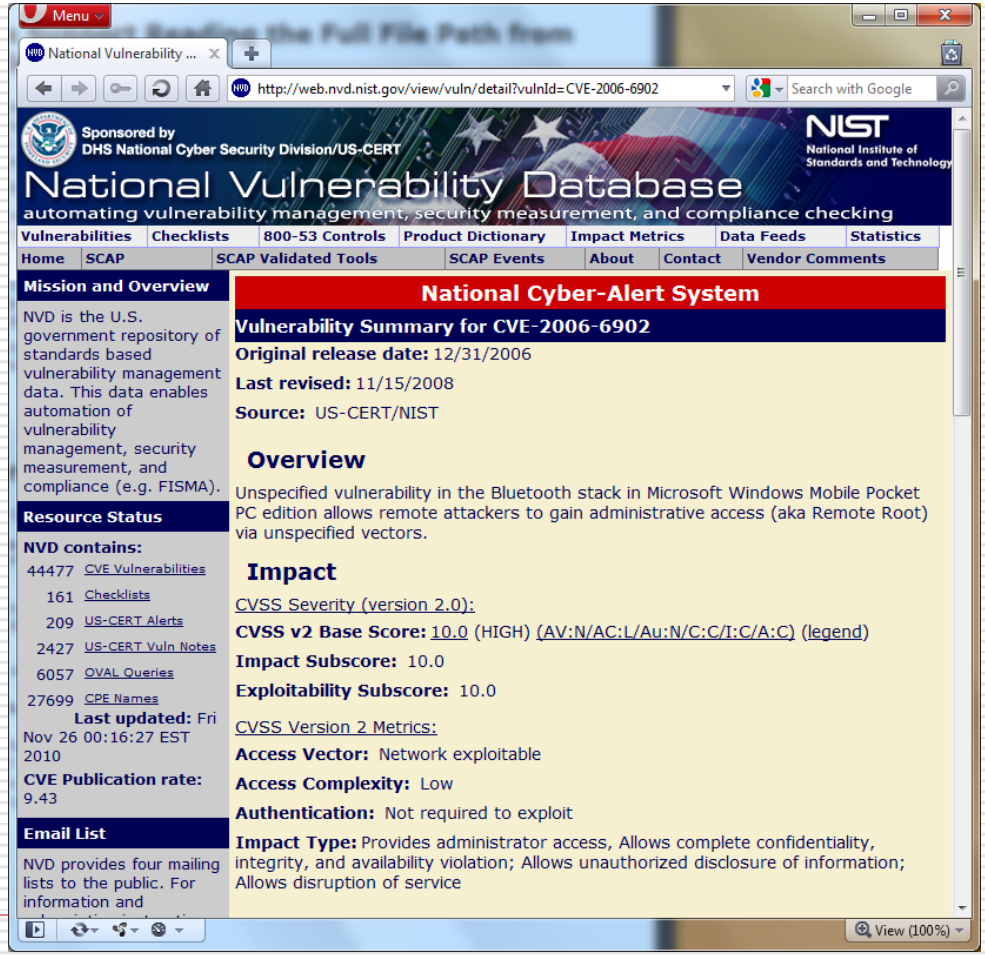
- 案例：西门子**3568i**手机短信拒绝服务漏洞
  - 手机在接收到含有特定字符的短信时系统崩溃
  - 仅影响**3568i**这一款特定的机型

2.3 发展历史 - 系统接口型漏洞阶段

- 系统接口型漏洞阶段
  - 时间：**2004**年至**2008**年
  - 手机系统特点
    - 智能手机日趋成熟，开始在中高端市场普及
    - 用户刚开始接受向手机中安装应用的概念
    - 手机应用以多媒体播放和游戏为主，网络应用较少
  - 该阶段的研究主要集中于系统接口和协议栈上

2.3 发展历史 - 系统接口型漏洞阶段

- 案例：**Windows Mobile**蓝牙协议远程管理员权限访问漏洞
  - 存在于**Windows Mobile**这一通用的智能手机操作系统平台
  - 受影响的系统组件为蓝牙协议栈

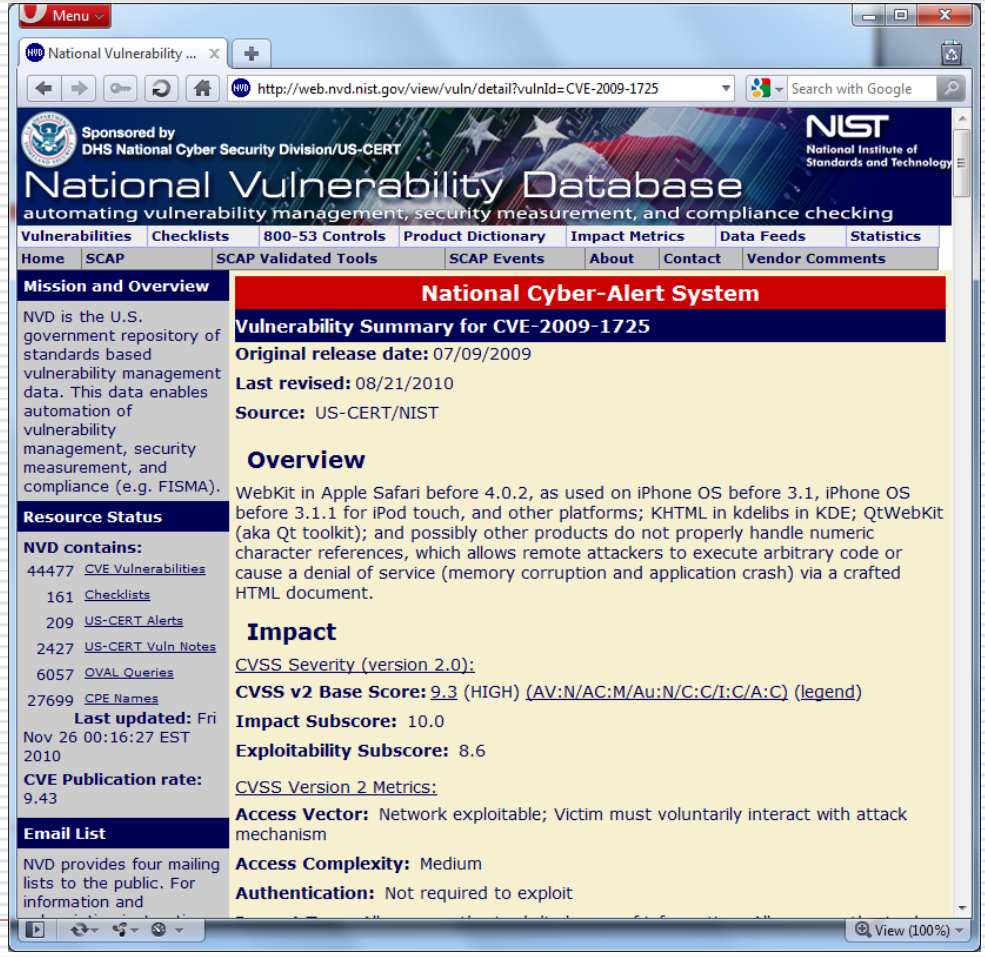


2.3 发展历史 – 手机应用型漏洞阶段

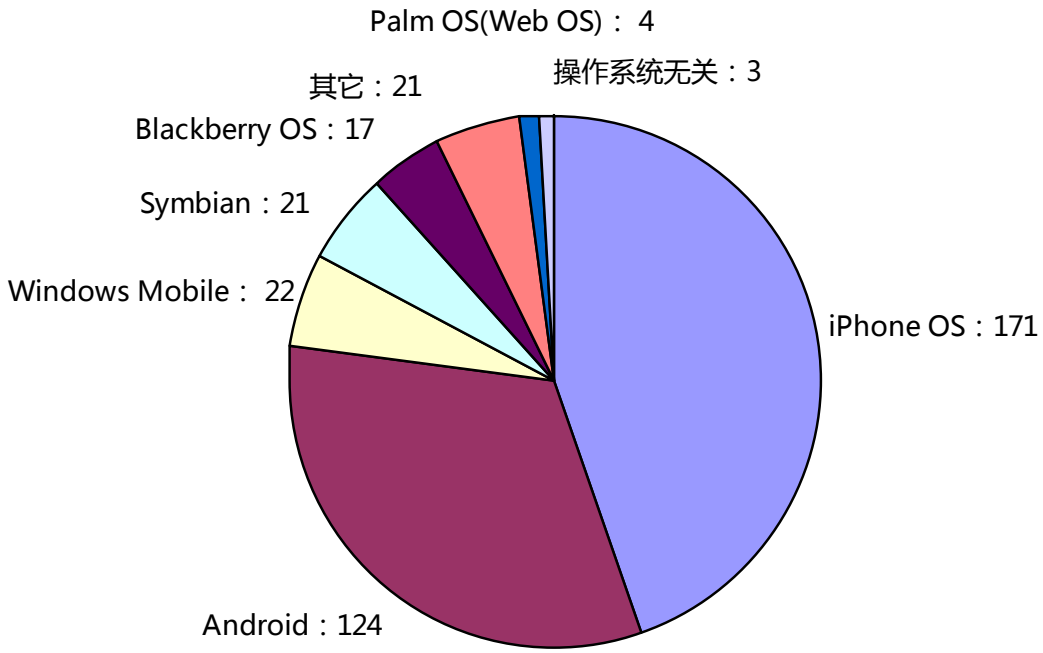
- 手机应用型漏洞阶段
  - 时间：**2008**年至今
  - 手机系统特点
    - 创新的手机操作系统带动智能手机市场进一步扩大
    - **3G**普及，带宽大大提高，无线数据业务普及
    - 手机中引入**NFC**、手机支付等新技术
    - 用户形成安装手机应用的习惯，其中大部分均为无线互联网应用
  - 手机漏洞的研究热点转向大量引入的新技术，以及第三方应用，特别是互联网应用

2.3 发展历史 - 手机应用型漏洞阶段

- 案例：**Mobile Safari** 畸形字符引用内存污染漏洞
  - 存在于**iPhone**浏览器**Mobile Safari**的内核中
  - 由于**PC**平台和手机平台共享代码，此漏洞同时也影响**Safari**的桌面版本



2.3 研究现状 – 手机操作系统角度

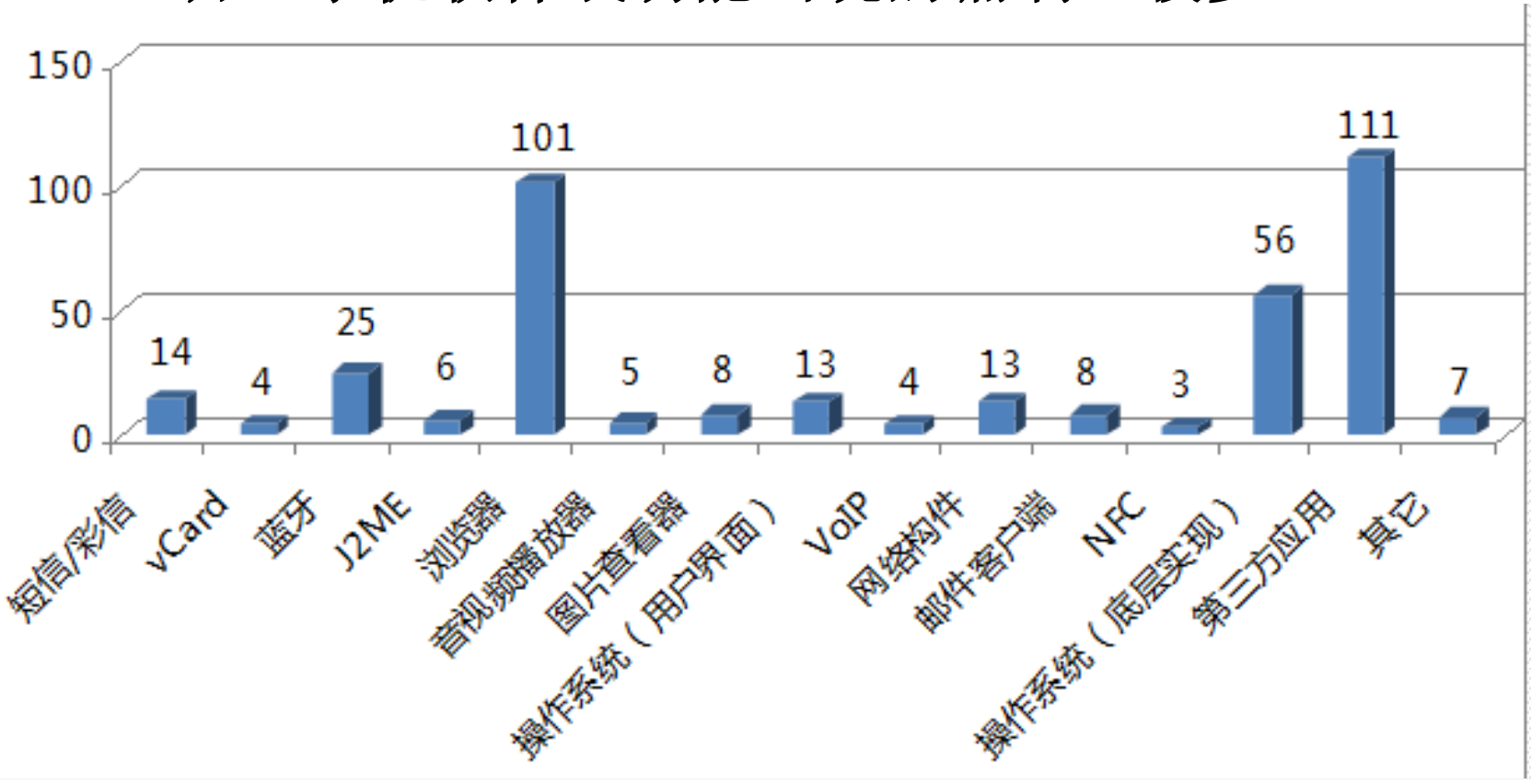


2.3 研究现状 – 手机操作系统角度

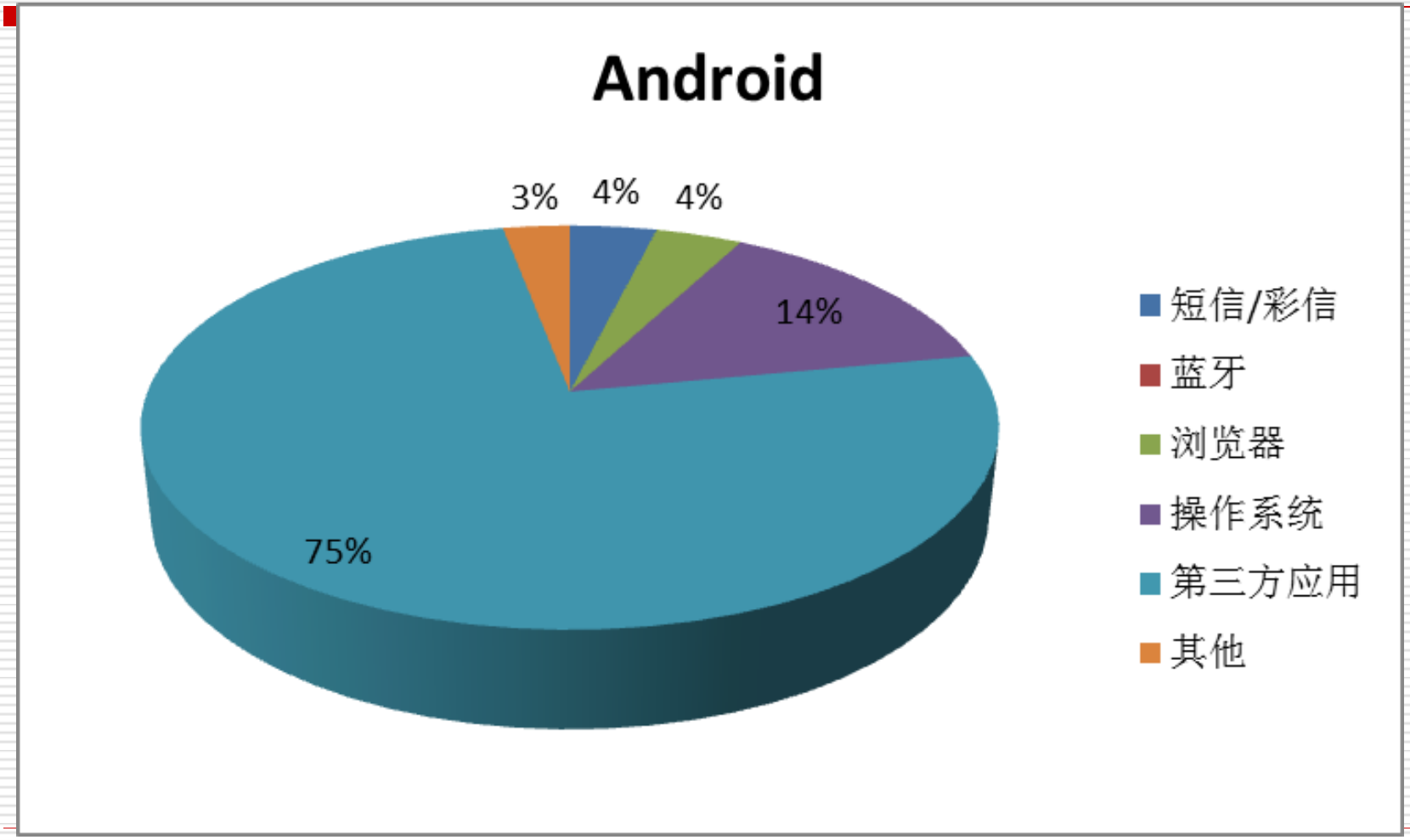
- 从手机操作系统的角度来看
  - 最突出的手机操作系统为**APPLE iOS(iPhone OS)**，以**171**个漏洞、**46%**的比率位居第一
  - **Android**系统是近年来的安全热点，共发现**124**个漏洞，占总数的**32%**，排名第二
  - **Windows**和**Symbian** 分占总数的**6%**和**5%**，排名**3**、**4**

2.3 研究现状 – 手机功能角度

- 从漏洞所影响的手机功能角度来看
  - 哪些手机软件或功能出现的漏洞比较多？



Android——漏洞类型



2.3 研究现状 – 手机功能角度

- 手机浏览器有关的漏洞
  - 处理畸形输入的漏洞，包括生成畸形数据的 **JavaScript** 和畸形的页面文件
  - 对输入缺乏有效验证，导致跨站脚本攻击和敏感信息泄漏
  - 设计错误，用户无法根据屏幕显示做出合理的判断，攻击者可以借此实施欺骗攻击

2.3 研究现状 – 手机功能角度

- 第三方应用有关的漏洞
  - 对隐私数据缺乏保护，攻击者可以借此绕过权限机制窃取隐私数据
  - 内嵌的**webkit**组件对网页型输入缺乏有效验证，导致跨站脚本攻击和敏感信息泄漏
  - 设计错误，对安全协议的实现存在漏洞，导致攻击者可以通过中间人攻击等方式窃取数据或经济利益

2.3 研究现状 – 手机功能角度

- 蓝牙协议栈有关的漏洞
  - 主要集中于**OBEX**（对象交换）协议中，如
    - 用户界面设计错误
      - 在接到大量**PUSH** 请求时持续显示模态对话框，使用户无法操作手机
    - 对协议字段中的畸形输入处理不当，引发系统崩溃
      - 如特殊字符、超长字符串或无效的长度值等
    - 处理**OBEX FTP**操作时出现规范化错误，导致目录遍历

Bluetooth®

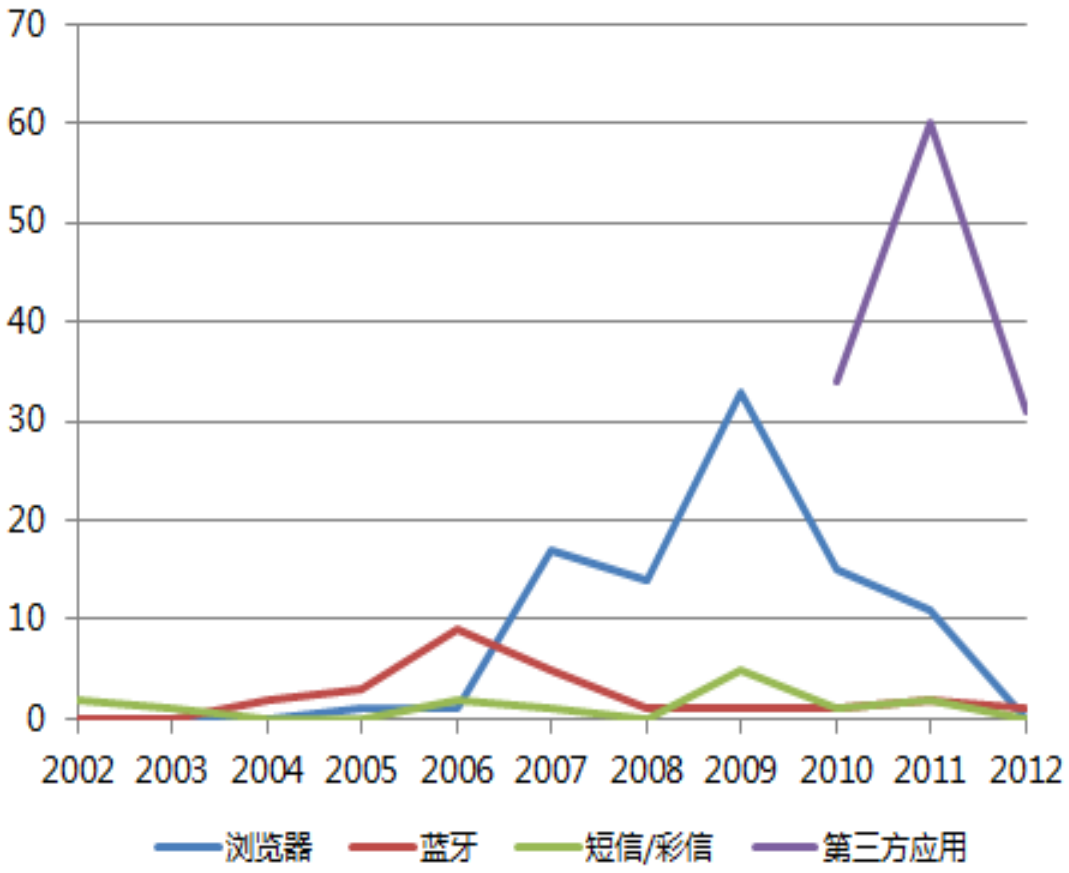
2.3研究现状 - 手机功能角度

- 短信和彩信有关的漏洞
  - 绝大多数都与无法正确处理畸形消息有关
    - 特殊字符
    - 超长字符串
  - 另外一部分属设计错误
    - 攻击者可以利用这些漏洞隐藏自己作为发送者的身份，或掩盖其恶意企图

2.3 研究现状 – 手机功能角度

- 系统用户界面有关的漏洞
  - 源于不合理的用户界面逻辑
  - 往往存在于如下界面元素中
    - 查找
    - 自动补全
    - 口令锁定
  - 攻击者可对这些功能进行正常的操作，绕过系统的访问控制，获取手机用户的敏感信息

2.3研究现状 - 手机功能角度



- 最近几年传统浏览器、蓝牙、短信有关的漏洞数量持续减少
- 大量第三方应用的漏洞频频出现
- 特别是，单单2010年便有2个银行提供的智能手机应用存在严重的用户名和密钥管理漏洞，极易导致用户的经济财产遭到直接的损害。

二 手机安全漏洞现状

- 智能手机漏洞简介
- 形成原因
- 发展历史及研究现状
- ✓ 挖掘与利用技术

2.4 手机漏洞挖掘 – 相似性

- 智能手机的漏洞挖掘与PC平台有相通之处
  - 智能手机软硬件工作机制与PC并无根本区别
  - 某些手机操作系统直接由PC 操作系统衍生而来，共用一部分代码
  - 智能手机上漏洞的产生机理和利用方式都与PC平台类似
- 手机漏洞的挖掘技术可以借鉴PC平台上成熟的方法和理论

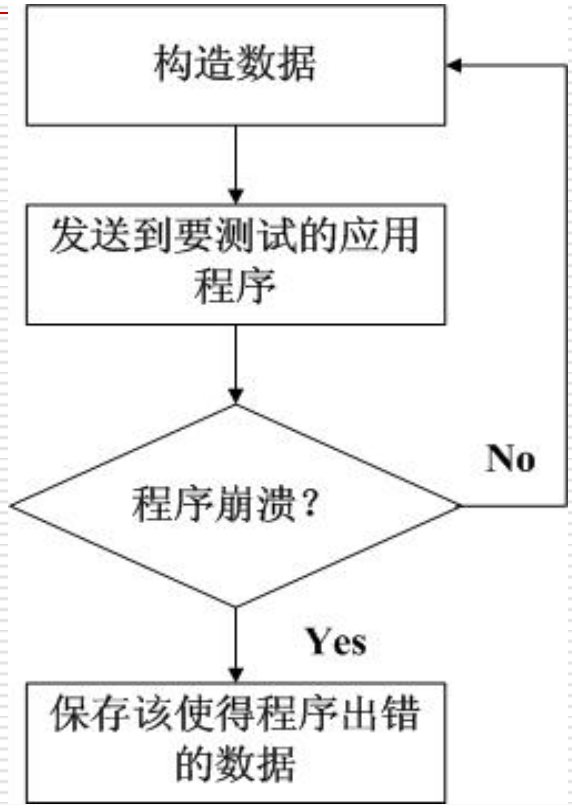
2.4 手机漏洞挖掘 – 独特性

- 但智能手机也有其独特性
  - 硬件处理能力远不及**PC**
  - 操作系统和开发工具开放度不够
  - 通信网络为封闭的专有网络
- 应根据手机平台的具体特点，对已有的漏洞挖掘技术进行修改和扩充

2.4 手机漏洞挖掘 – 关键技术

关键技术：Fuzzing

- ✓ Fuzzing技术：使用大量半有效（semi-valid）的数据作为应用程序的输入来进行漏洞挖掘的方法
- ✓ 优点：高度自动化，效率比较高，能够快速的找到缓冲区溢出、格式化字符串和规范化错误等漏洞，没有误报率
- ✓ 缺点：对不同挖掘对象需要进行定制，通用性较差；比较依赖于研究者的给出的Fuzz策略
- ✓ 目前国内外多数安全工作者使用Fuzzing技术来进行漏洞挖掘

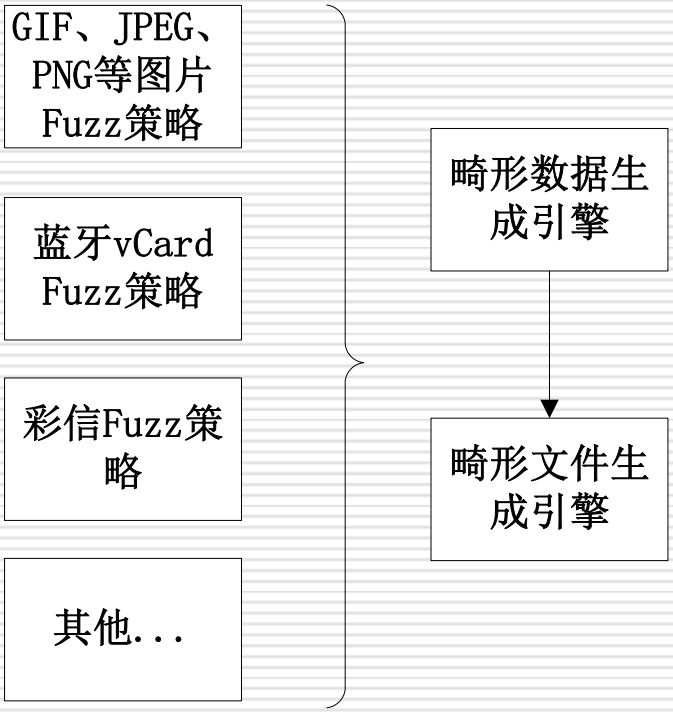


【“小心的静态分析不是万能的，一定要结合Fuzzing技术” -- 微软安全响应中心 】

2.4 手机漏洞挖掘 – 关键技术

关键技术：畸形数据生成

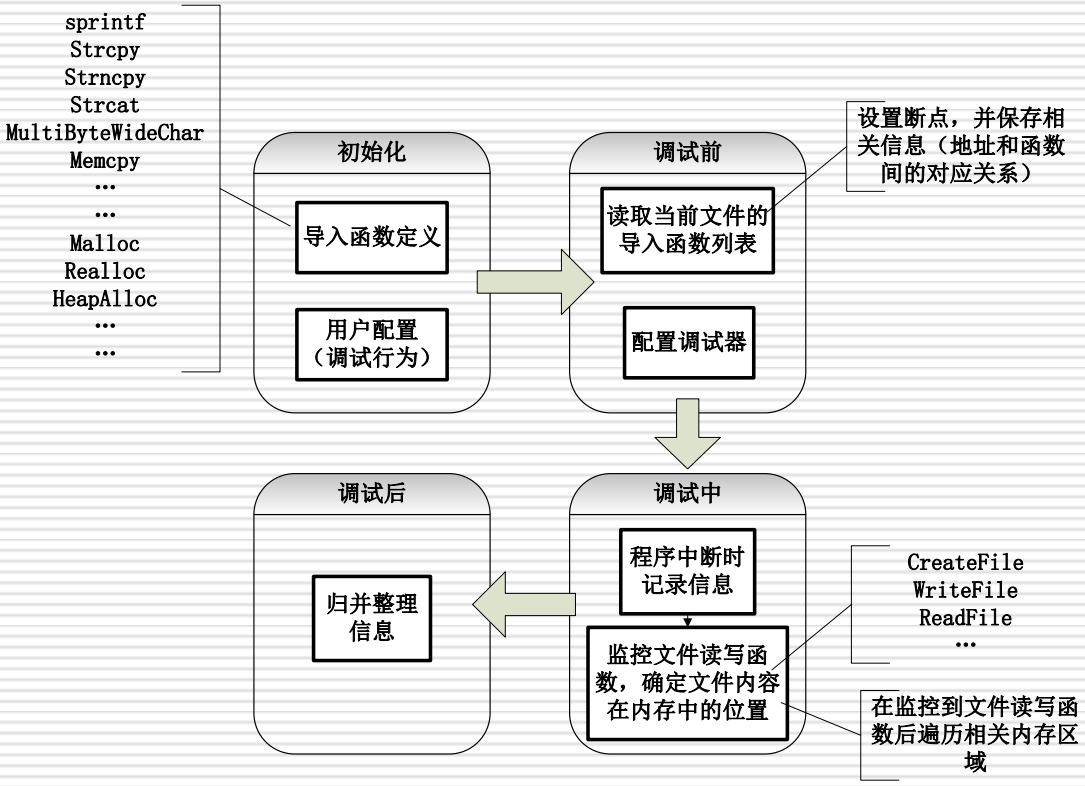
- ✓ 通过对各种挖掘对象进行分析，提出挖掘（**Fuzz**）策略
- ✓ 由于软硬件的限制手机平台上测试往往耗时较长，所以需要精简畸形数据的生成数量
- ✓ 相对而言，某些畸形数据在手机上不会触发漏洞，可以抛弃；例如，在特定条件下，过长的畸形字符串会使得操作系统直接报错退出



2.4 手机漏洞挖掘 – 关键技术

关键技术：程序行为跟踪

- ✓ 记录程序在处理不同输入时的运行轨迹
- ✓ 畸形数据一般需要通过特定的函数调用才能触发漏洞；如果畸形数据不会被特定函数调用，那么就不可能触发相应漏洞，也就没有必要进行测试
- ✓ 输出结果可以用于优化**Fuzz**畸形数据的生成



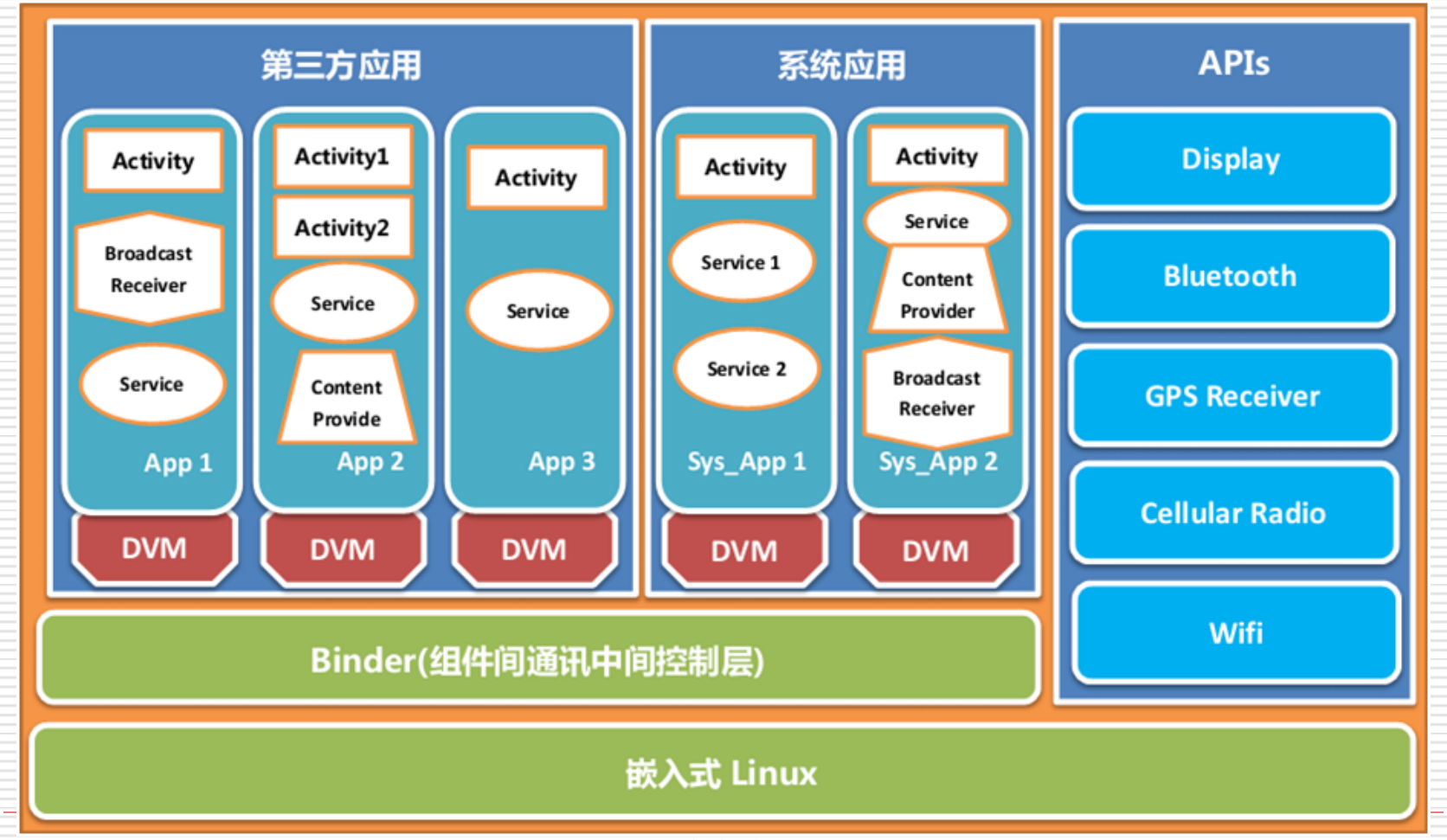
案例：Android平台Intent漏洞挖掘

- Android应用按照组件类型的不同分为Activity、Service、Broadcast Receiver和Content Provider四种类型。

- 组件间通讯的传递媒介——Intent:

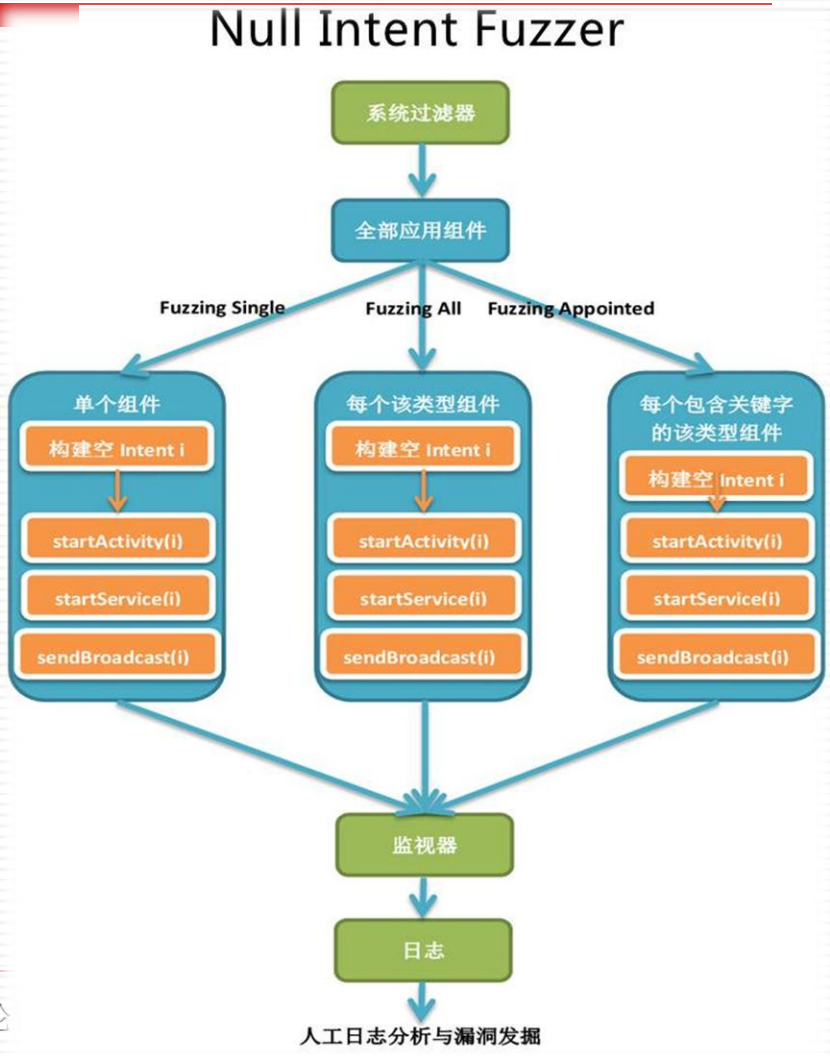
在同一应用或不同应用之间的通信过程中，Intent起着一个媒体中介的作用，专门提供组件互相调用的相关信息，并可实现调用者与被调用者之间的解耦。

Android应用架构



Intent Fuzzer

- 对暴露在外面的其他程序的组件名称进行了统计分类，并实现了通过列表的形式供用户选择。然后构造测试数据的Intent对目标组件进行测试。



Intent Fuzzer程序界面

Service崩溃统计

类型	进程	应用
原生应用	android.proces	
原生应用	com.android.bl	
原生应用	com.android.m	
原生应用	com.cooliris.me	
第三方应用	com.sina.weibo	
厂商自主应用	com.huawei.and	
厂商自主应用	com.huawei.gp	

com.tencent.mm

!!!Process Name

Details: java.lan

!!!Process Name

Details: java.lan

com.huawei.mm

java.lang.NullPo

崩溃的组件

Android原生

厂商自主应

第三方应

Broadcast Receiver崩溃统计

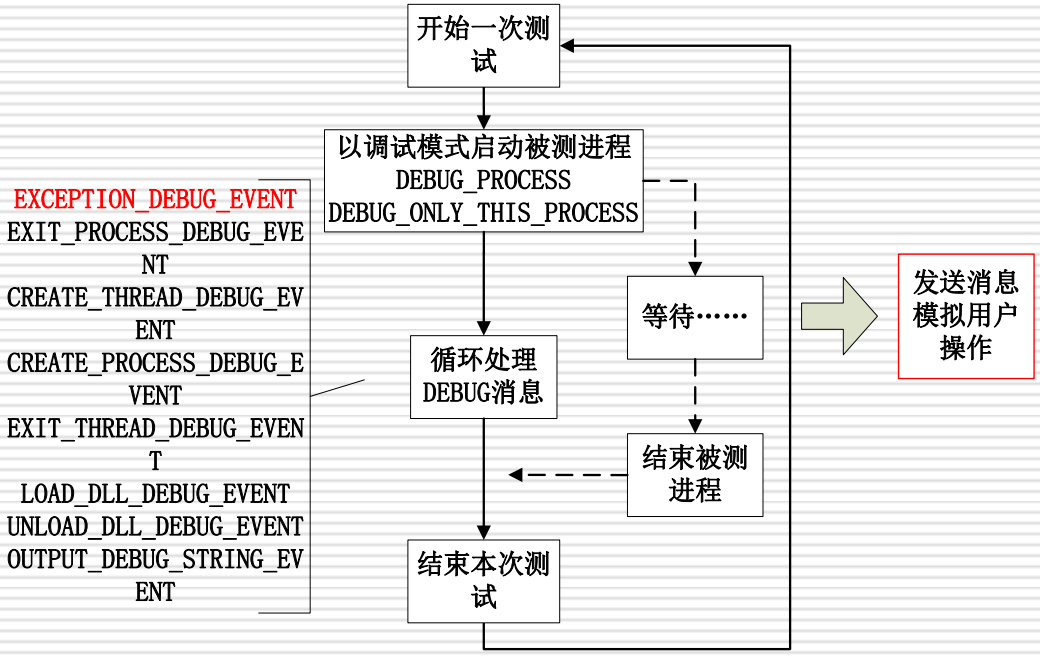
类型	进程	应用
原生应用	android.process.acore	通讯录
原生应用	com.android.providers.calendar	日历
原生应用	com.cooliris.media	图库
原生应用	com.android.browser	浏览器
原生应用	com.android.phone	电话
原生应用	com.android.mms	短信
原生应用	android.process.media	多媒体
原生应用	com.android.calendar	日历
原生应用	com.android.deskclock	桌面时钟
第三方应用	com.tencent.mm	微信
第三方应用	com.dianping.v1	大众点评
第三方应用	com.tencent.mobileqq	qq
第三方应用	com.keramidas.TitaniumBackup	钛备份
第三方应用	com.moji.mjweather	墨迹天气
第三方应用	com.sina.weibo	新浪微博
第三方应用	com.noshufou.android.su	授权管理
第三方应用	vStudio.Android.GPhotoPaid	Camera360
第三方应用	com.sds.android.process.ttpod	千千静听
第三方应用	com.uc.browser	UC浏览器
厂商自主应用	com.huawei.mmitest2	华为自带测试程序
厂商自主应用	com.huawei.updata	华为升级程序

Intent Fuzzer漏洞分析

2.4 手机漏洞挖掘 – 防范中心成果展示

文件格式漏洞Fuzz测试平台

- 针对手机环境，自主开发专用文件格式Fuzz测试平台
- 通过对被测进程进行监控，自动化的完成Fuzz测试流程
- 在已发布的Fuzz平台中，是目前唯一能够在手机上工作的测试平台。（参考 www.fuzzing.org）



2.4 手机漏洞挖掘 – 防范中心成果展示

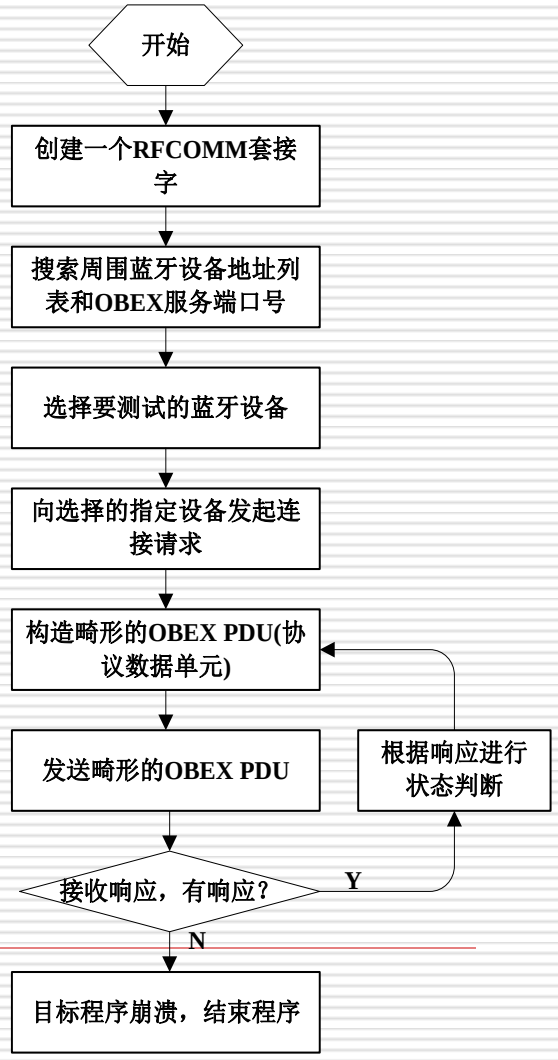
蓝牙协议Fuzz测试平台

- ✓ 用于挖掘蓝牙设备漏洞的Fuzz工具
- ✓ 能够对包括智能手机在内的各种蓝牙设备进行测试

82 00 A3 C3 00 00 00 8F 01 00 09 00 2E 00 2E 00 2F
49 00 92 42 45 47 49 4E 3A 56 43 41 52 44 53 49 4F
4E 0D 0A 56 45 52 3A 32 2E 31 0D 0A 4E 3A 48 6F
75 66 75 3B 43 68 65 6E 67 0D 0A 46 4E 3A 48 6F
75 66 75 20 43 68 65 6E 67 0D 0A 4F 52 47 3A 4E 49
50 43 0D 0A 54 45 4C 3B 43 45 4C 4C 3A 31 33 35
30 31 32 39 38 34 30 36 0D 0A 54 45 4C 3A 30 31 30
36 38 38 33 36 32 36 30 0D 0A 45 4D 41 49 4C 3A
63 68 65 6E 67 68 6F 75 66 75 40 31 32 36 2E 63 6F
6D 0D 0A 45 4E 44 3A 56 43 41 52 44 0D 0A

引发漏洞的关键数据

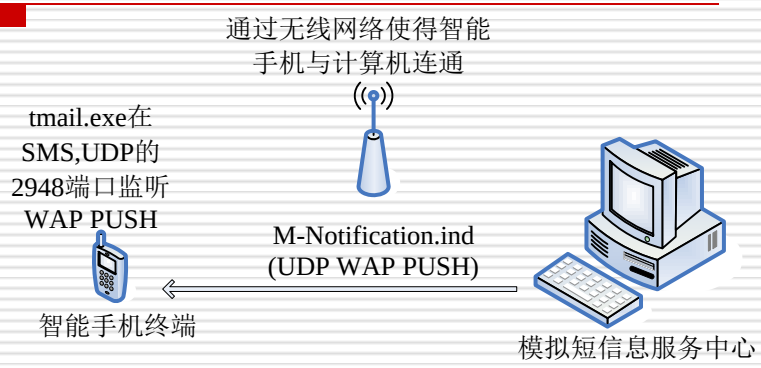
能够引发蓝牙漏洞（未公开）的数据包截图

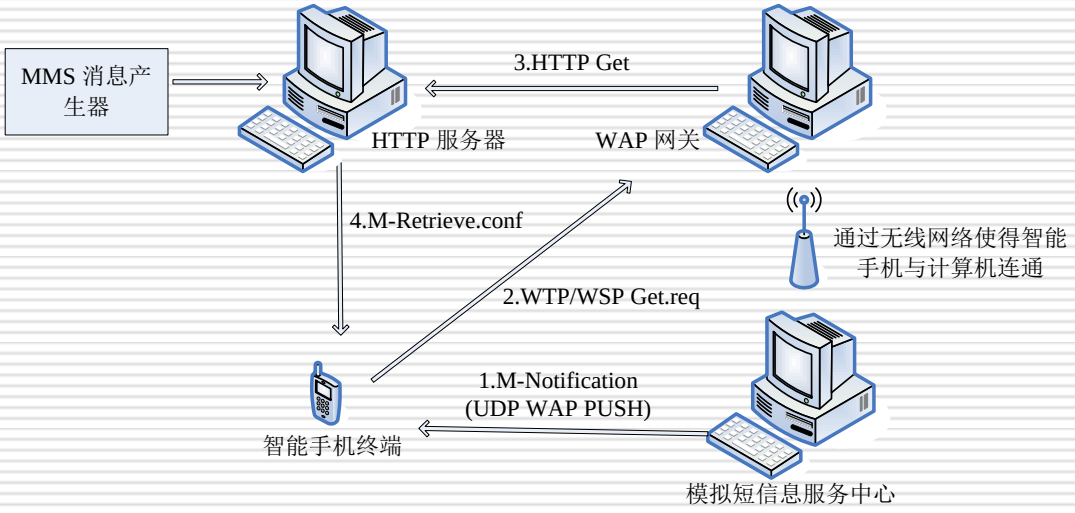


2.4 手机漏洞挖掘 – 防范中心成果展示

彩信协议Fuzz测试平台

- ✓ 用于彩信漏洞挖掘的工具和环境
- ✓ 通过模拟环境测试彩信，极大的降低了挖掘成本

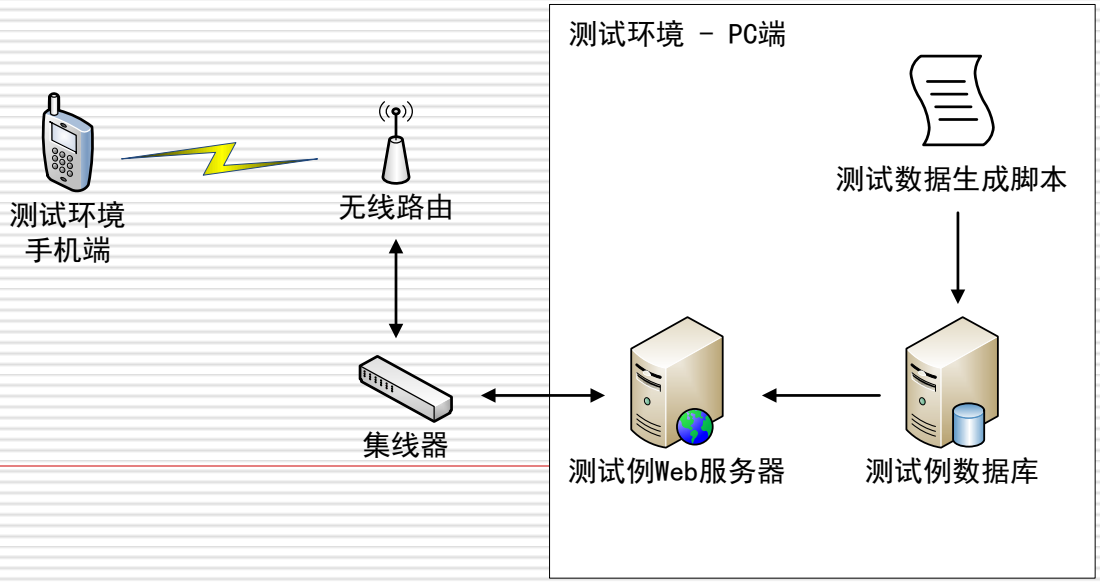




2.4 手机漏洞挖掘 – 防范中心成果展示

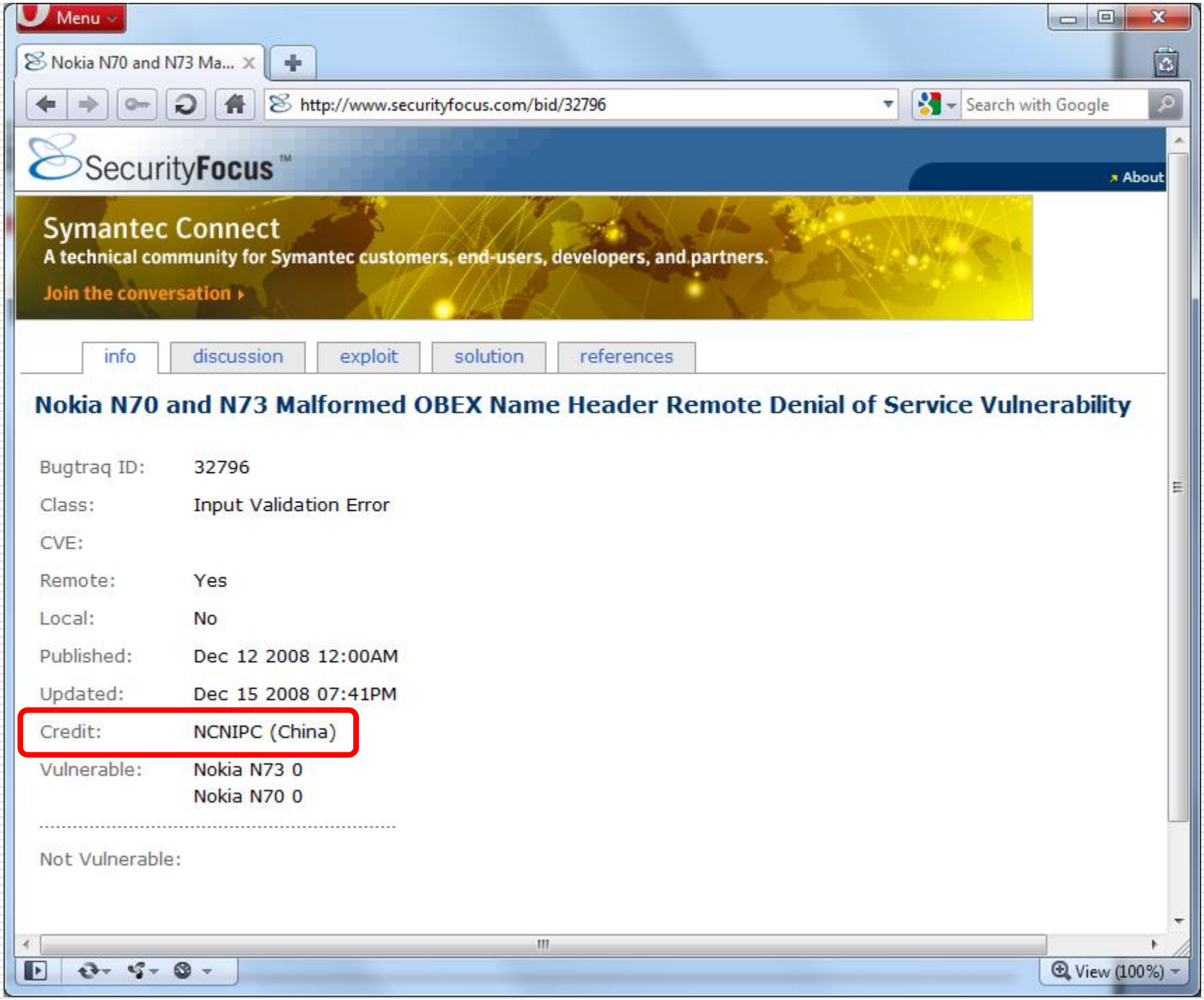
浏览器Fuzz测试平台

- ✓ 用于测试手机浏览器在处理畸形图象文件时可能出现的漏洞
- ✓ 充分利用PC机强大的计算和存储能力，将测试例的生成和存储交由PC端完成，手机浏览器运行脚本访问PC端存储的大量测试例，提高了测试效率



2.4 手机漏洞挖掘 – 成果展示

- 挖掘出的漏洞包括：
  - **Nokia N70 OBEX**拒绝服务漏洞（高危漏洞，http://www.securityfocus.com/bid/32796）
  - **Lyrics Magic For Smartphone**畸形**M3U**文件缓冲区溢出漏洞（高危漏洞）
  - **Pocket Music Player ASX**文件拒绝服务漏洞
  - **UMD**阅读器文件拒绝服务漏洞
  - **Mobile Safari**内存污染（**double-free**）漏洞（**CVE-2010-4494**）


Menu
Nokia N70 and N73 Ma...
http://www.securityfocus.com/bid/32796
Search with Google
SecurityFocus
About
Symantec Connect
A technical community for Symantec customers, end-users, developers, and partners.
Join the conversation
info
discussion
exploit
solution
references
Nokia N70 and N73 Malformed OBEX Name Header Remote Denial of Service Vulnerability
Bugtraq ID: 32796
Class: Input Validation Error
CVE:
Remote: Yes
Local: No
Published: Dec 12 2008 12:00AM
Updated: Dec 15 2008 07:41PM
Credit: NCNIPC (China)
Vulnerable: Nokia N73 0
Nokia N70 0
Not Vulnerable:
View (100%)

About the security content of iOS 4.3

- **libxml**

Available for: iOS 3.0 through 4.2.1 for iPhone 3GS and later, iOS 3.1 through 4.2.1 for iPod touch (3rd generation) and later, iOS 3.2 through 4.2.1 for iPad

Impact: Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution

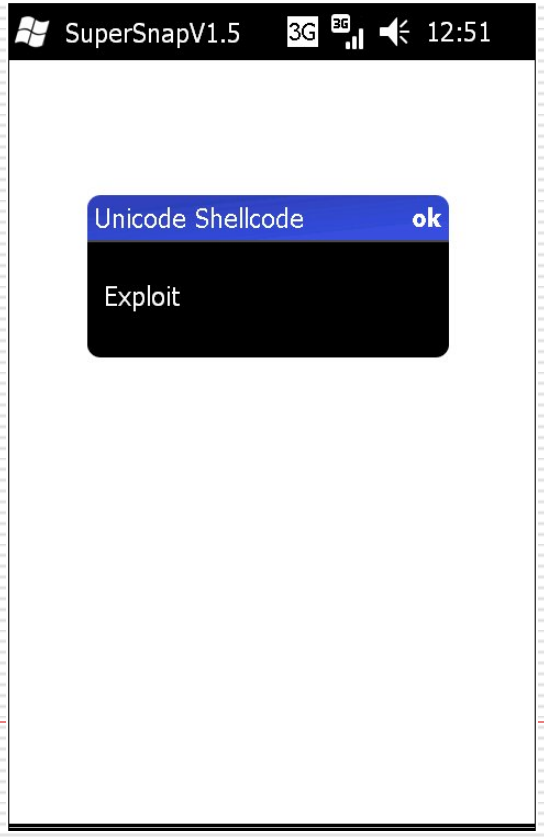
Description: A double free issue existed in libxml's handling of XPath expressions. Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution.

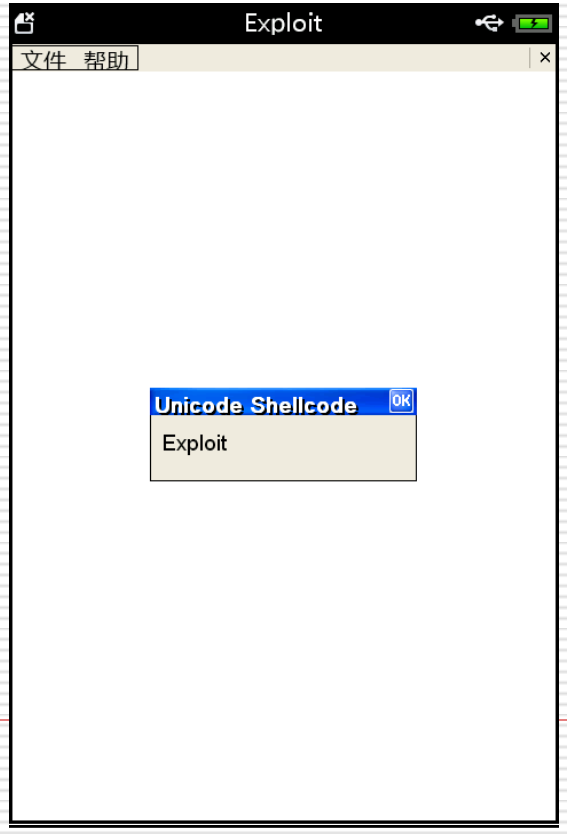
CVE-ID

CVE-2010-4494 : Yang Dingning of NCNIPC, Graduate University of Chinese Academy of Sciences

2.4 手机漏洞利用 – 防范中心成果展示

- 对Lyrics Magic漏洞进行利用





内容提要

- 一 引言
- 二 手机安全漏洞现状
- ✓ 三 手机安全方向论文发表现状
- 四 未来趋势展望

三 手机安全方向论文发表现状

- 近几年来，各大会议关于手机安全的文章不断涌现，统计**2006-2012年3月**安全国际顶级会议中有关手机安全的论文**51篇**，可得知现阶段手机安全的总体研究现状。

- **S&P(Oakland)**，**IEEE Symposium on Security and Privacy**
- **CCS**，**ACM Conference on Computer and Communications Security**
- **Usenix**，**Security Usenix Security Symposium**
- **NDSS**，**ISOC Network and Distributed System Security Symposium**
- **ESORICS**，**European Symposium on Research in Computer Security**
- **RAID**，**International Symposium on Recent Advances in Intrusion Detection**
- **ACSAC**，**Annual Computer Security Applications Conference**
- **DSN**，**The International Conference on Dependable Systems and Networks**
- **IMC**，**Internet Measurement Conference**

usenix

20th USENIX Security Symposium

AUGUST 8–12, 2011 • SAN FRANCISCO, CA

MAY 22-25, 2011 AT THE CLAREMONT RESORT, OAKLAND, CALIFORNIA, USA

IEEE Symposium on Security and Privacy

Sponsored by the IEEE Computer Society Technical Committee on Security and Privacy in cooperation with the International Association for Cryptologic Research (IACR)

NDSS Symposium 2012

Hilton San Diego Resort & Spa
San Diego, California
5-8 February 2012

19th Annual Network & Distributed System Security Symposium

N D S S

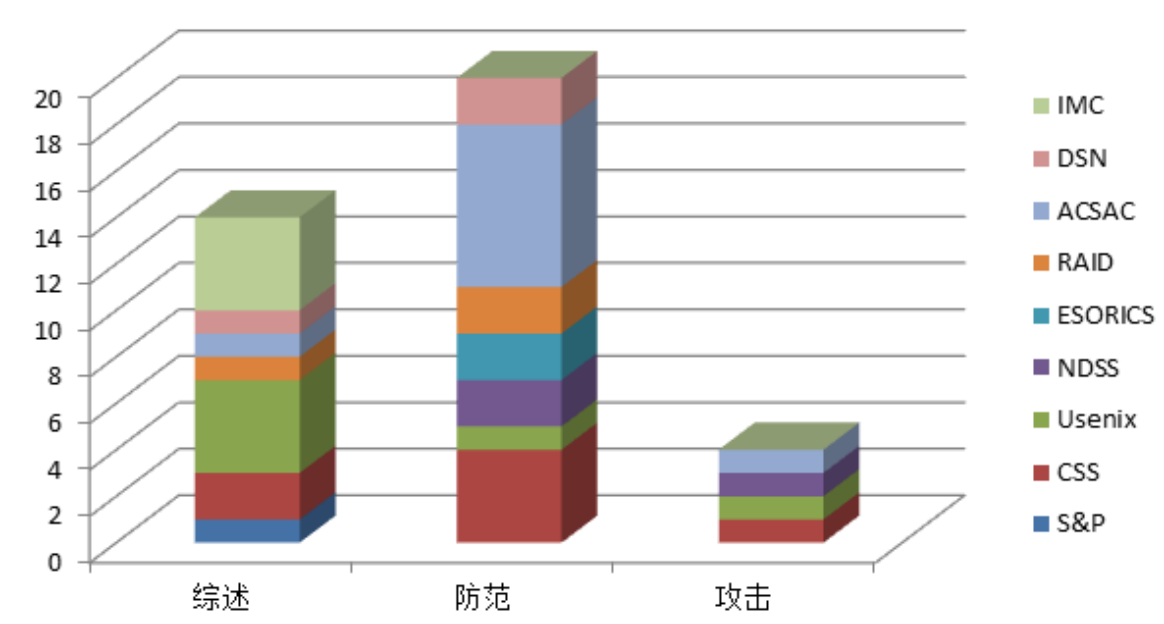
S Y M P O S I U M

CCS 2011

18th ACM Conference on Computer and Communications Security

OCT 17-21 2011. SWISSÔTEL Chicago, Chicago, IL, USA

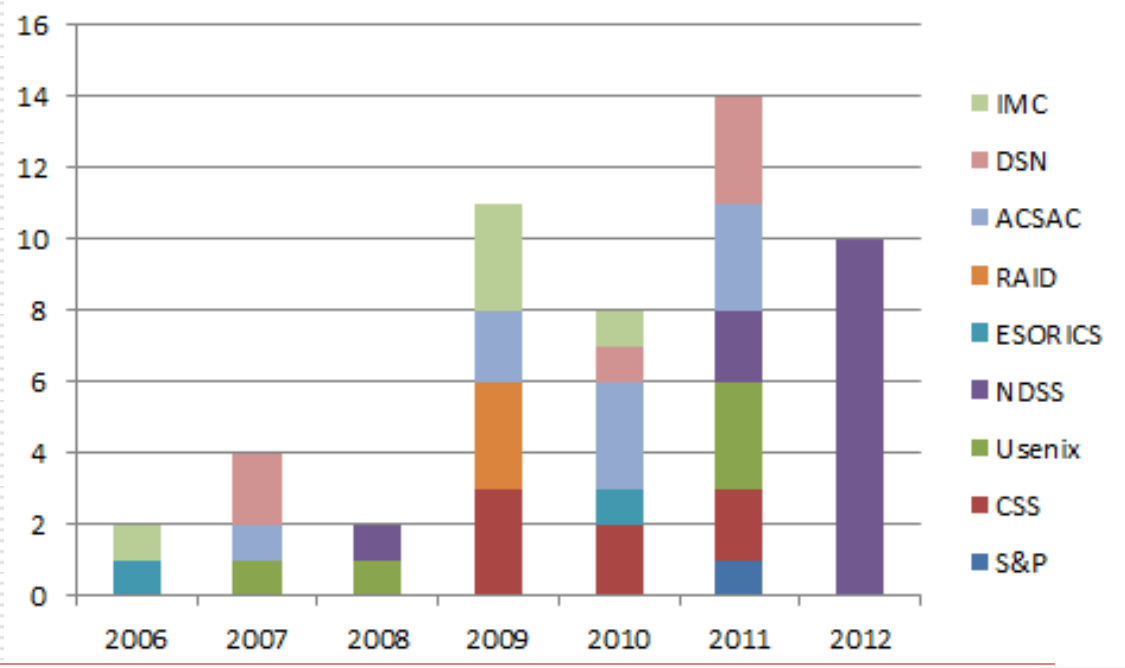
各个会议文章类型统计



- 基本上将论文的类型分为综述、防范和攻击三类
- 各大会议上手机相关论文的类型多为综述或防范型文章
- 多数是针对现有手机系统安全问题进行分析，提出改进意见或开发相关应用。

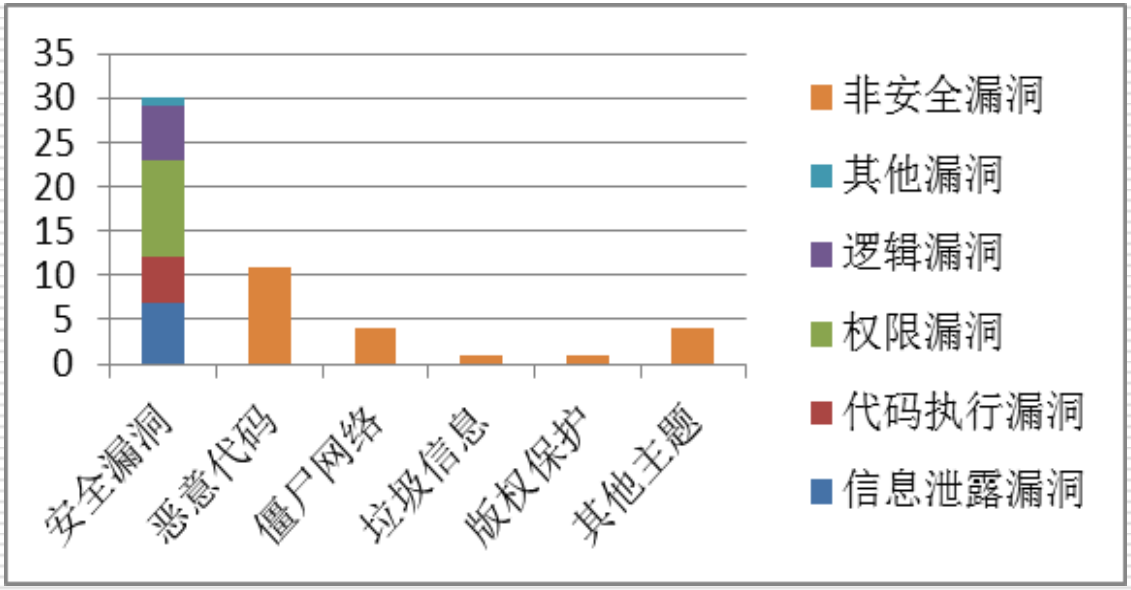
各会议历年手机方面论文数量统计

- **2011**年开始，论文的发表呈现井喷趋势。
- 在刚刚召开的**NDSS 2012**会议上，手机安全相关的论文有多达**10**篇，超过了**2010**年全年各顶级安全会议智能手机安全论文数总和（**8**篇）
- 尤其是开源的、应用市场管理相对宽松的**Android**系统，其安全问题更是成为了研究的焦点。



论文方向统计

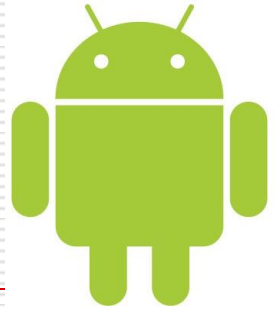
- 在智能手机安全这些论文中，安全漏洞占据着核心地位，所占比例达到了**57%**。
- 其中，权限漏洞、信息泄露漏洞、代码执行漏洞和逻辑漏洞占据了漏洞研究的主要方面



内容提要

- 一 引言
- 二 手机安全漏洞现状
- 三 安全国际顶级会议手机论文情况
- ✓ 四 未来展望

四 未来趋势展望 – 手机安全



- 手机安全与计算机系统安全许多地方类似，但又有其特殊性
- 手机安全漏洞逐年加速增长，正在引起人们的重视
- 安全国际顶级会议中手机安全论文成热点，但关注点在于第三方应用和新型技术的安全问题
- 有效的、震惊世人的大规模手机攻击尚未问世
- 历史将重现，手机安全问题：手机病毒--》漏洞利用与攻击
- 大规模手机攻击指日可待
- 随着智能手机功能和性能的增强，日常生活中的普及，在可见的未来，手机信息隐私和安全将成为最重要的信息安全研究领域。

谢谢！

张玉清

zhangyq@nipc.org.cn

发改委信息安全专项

- 1 移动智能终端信息安全风险评估指南
- 2 移动智能终端恶意代码处理指南
- 3 移动智能终端安全应用配置要求
- 4 移动智能终端漏洞验证方法
- 5 移动智能终端漏洞修复指南
- 6 移动智能终端漏洞标识格式要求
- 7 移动智能终端接口安全技术要求第1部分：无线接口
- 8 移动智能终端接口安全测试方法第1部分：无线接口
- 9 移动智能终端接口安全技术要求第2部分：卡接口
- 10 移动智能终端接口安全测试方法第2部分：卡接口

- 蓝牙安全指南