Android安全－伪命题？

周亚金

http://yajin.org

Android安全和你我息息相关

- 设备安全
  - Android系统漏洞：MasterKey[1]，addJavascriptInterface [2], FakeID[3], Webview XSS[4] …
  - 厂商定制漏洞
    - 手机厂商[5][6]：三星,LG,HTC,SONY,Google,中华酷联 …
    - 芯片厂商：联发科，高通 … : 提权
  - Linux 漏洞[7] – 通杀所有机型
  - Android碎片化[5]导致问题变得更加严重
- 数据安全
  - 恶意App[9][10]：获取用户隐私数据
  - 有漏洞App[11]：被动泄漏用户隐私数据
  - 设备丢失：内存数据安全 - 银行和支付类App
  - 开发者云端口令泄漏：用户数据自动同步到云端，开发者口令泄漏导致用户隐私数据泄漏

Android安全和你我息息相关

- 通信安全
  - 中间人攻击：Android会自动连接存储的无线热点，没有机制去验证热点的身份。对于在人群拥挤的场合进行中间人攻击的可行度非常高(CMCC)
  - HTTP：App采用HTTP传输敏感数据：登录token
  - HTTPS：SSL 不正确使用[8]，不采用certificate pining[12]
- 其他（硬件相关）
  - GSM嗅探：OsmocomBB，成本非常低[13]
  - NFC
  - …

我们该怎么办

- 设备：我们有选择吗？
- 第三方ROM：该用哪一个？
- App：很无奈，装还是不装？

引用

[1] https://bluebox.com/technical/commentary-on-the-android-master-key-vulnerability-family/
[2] https://labs.mwrinfosecurity.com/blog/2013/09/24/webview-addjavascriptinterface-remote-code-execution/
[3] https://bluebox.com/technical/android-fake-id-vulnerability/
[4] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6041
[5] Lei Wu, Michael Grace, Yajin Zhou, Chiachih Wu, Xuxian Jiang,
"The Impact of Vendor Customizations on Android Security," CCS 2013
[6] http://share.csdn.net/slides/1034
[7] CVE-2013-2094
[8] Sascha Fahl, Marian Harbach, Thomas Muders and Matthew Smith
“Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security”, CCS 2012
[9] Yajin Zhou, Zhi Wang, Wu Zhou, Xuxian Jiang
"Hey, You, Get off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets”, NDSS 2012
[10] Yajin Zhou, Xuxian Jiang, "Dissecting Android Malware: Characterization and Evolution“, Oakland 2012
[11] Yajin Zhou, Xuxian Jiang, "Detecting Passive Content Leaks and Pollution in Android Applications,“ NDSS 2013
[12] https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning
[13] http://radiowar.org/hardware/gsm-hack-for-osmocombb.html

Thanks

http://yajin.org