捍 卫 信 任 2 0 1 9 京 麒 国 际 安 全 峰 会

移动生态安全探索与实践

——主讲人 韩紫东

腾讯安全移动安全实验室

韩紫东 高级安全研究员

研究移动安全与IoT安全领域，专注安全生态相关研究

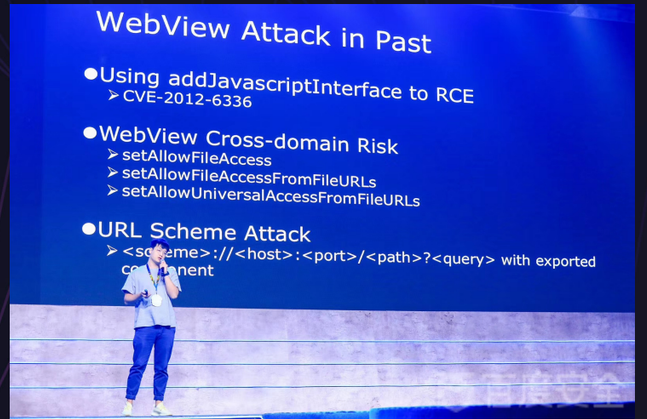
GeekPwn2018黑客屋挑战赛/GeekPwn 2019 手机破解挑战赛

Defcon China 2019 《Bridge Attack》相关议题分享

HITB 2018 CommSec 《 Who Hijacked My Smart Home: One URL to Hack ALL IoT Devices 》安全议题分享

针对移动应用和物联网生态安全的攻击 Bridge Attack

针对应用抽象Bridge的攻击手法，目标移动应用和IoT生态
漏洞利用成本低，远程攻击效果大，危害广



Defcon China2019 Bridge Attack 分享

厂商的开发生态化与安全壁垒
静默安装应用漏洞

多款智能手机存在远程任意静默安装APP的高危漏洞

厂商生态化的安全壁垒：后门与漏洞模糊的界限

GeekPwn2019 破解智能手机

物联网安全生态问题
” 黑客屋 “攻击场景

IoT生态场景多样，窃取用户隐私危害性高

对生态安全破坏的持久性更大

GeekPwn 2018 ” 黑客屋 “攻击场景模拟

移动开发与安全新趋势

移动应用生态安全

物联网与移动安全

移动生态安全总结与展望

移动开发与安全新趋势

京麒

2019移动应用开发发展趋势

厂商生态化尝试与实践 – 快应用联盟

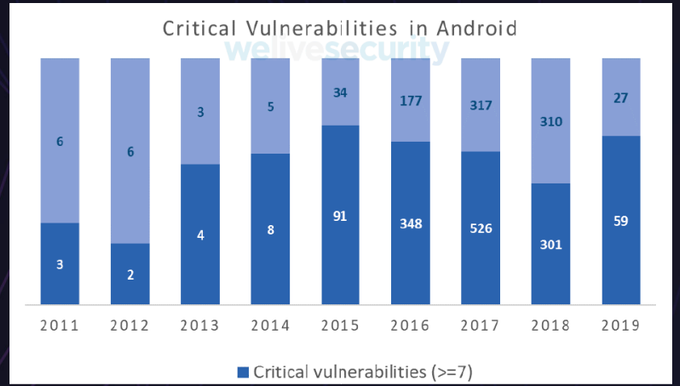
- 连接厂商硬件能力，布局场景化分发
- 响应Android原生Instant App/PWA概念以及微信/支付宝小程序

厂商生态化尝试与实践 -- 快传联盟

- 打破厂商跨品牌传输壁垒
- 响应Android原生Fast Share概念，本土生态化尝试

2019Android系统严重漏洞情况

- 2019年相比2018年漏洞数量急剧下降
- 2019年严重漏洞的占比升高，其中29%允许执行恶意代码
- 90%的android设备使用android pie之前的版本，而74%的android甚至不运行oreo



移动生态安全风险 -- 冰山一角

- 生态安全问题逐步浮出，与隐私安全数据安全等息息相关
- 更多的生态安全需要引起厂商的关注和重视

2019MOSEC：腾讯安全披露“文件分享”中的安全危险

来源：东方资讯 2019-05-31 14:44

拥有上亿用户的高频安卓应用——文件分享类应用被爆存有安全隐患。腾讯安全玄武实验室在5月30-31日于上海召开的第五届MOSEC移动安全技术峰会上，一次性披露了文件分享类应用的多个漏洞。这些漏洞一旦被非法攻击者掌握，将对数亿用户的传输文件和隐私数据安全造成极大威胁。目前，腾讯安全已在第一时间将发现的所有漏洞传递给了相关手机厂商，并协助其修复了大部分安全漏洞。

Develop Fast Without Risk?

移动开发与安全新趋势

移动开发

- 轻应用/快应用/Hybrid
- 组件化，生态化
- 万物互联之物联网

移动安全

- 生态安全Bridge Attack
- 账户体系安全风险
- 隐私泄漏与移动肉鸡威胁

移动应用生态安全

传统移动应用安全问题

远程安全风险

- Webview 安全问题
- Intent Scheme 攻击
- SSL证书错误忽略
- Janus漏洞风险
- ZippDown漏洞风险
- 应用克隆风险

...

本地安全风险

- 本地组件安全
- 本地拒绝服务漏洞
- 文件全局读写
- 本地开放端口
- 隐式Intent信息泄露

...

移动生态安全趋势

厂商对生态化的管理

-应用市场，账户体系，快应用/轻应用等

-收敛权限，增强用户体验，利于管理

生态化的安全风险

-复杂的应用场景，漏洞攻击面增加

- 生态化体系化，漏洞危害性更广泛

厂商生态化尝试与实践

生态场景：业务赋能 + 智慧场景

云-端：账户/支付/应用体系 + 开放平台服务

技术栈：前端与Native深层次，多元化融合

系统层：Custom Os + 硬件支持 == 得心应手的生态化

快应用/轻应用/Hybrid开发下的应用安全问题（以Hybrid模式为例）

-轻量跨平台，移植性高

-效率介于Native App、Web App之间

-原理：通过JSBridge让Native与Js通信，配合WebView显示

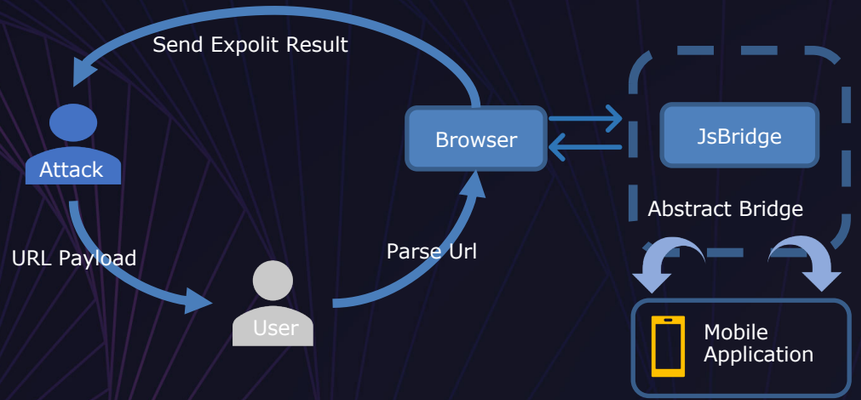
HyBrid App开发下的生态安全：Bridge Attack

Bridge Attack

利用HyBrid App中的核心:JsBridge

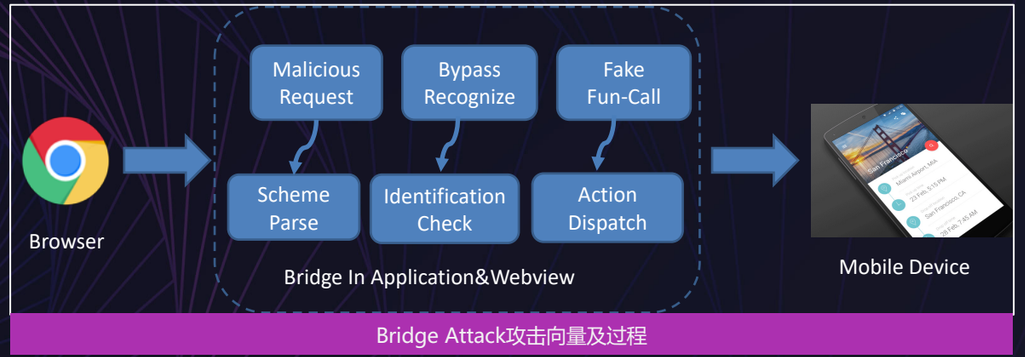
远程威胁：借助Intent Url Scheme

攻击效果：与JsApi能力成正比



*“UnOffical ” definition of **Bridge Attack***

Bridge Attack中的核心问题：信任域的处理



风险危害与JsApi能力成正比

- 轻易的跨域风险，造成隐私敏感数据泄漏（直接携带cookie/token）
- 甚至提供远程执行部分代码的能力，一旦被利用，风险极大

```
@JavascriptInterface
public void sendClientRequest(@NotNull String str) {
    Observable<Response<ResponseBody>> deleteCall;
    AjaxEntity ajaxEntity = (AjaxEntity) BridgeUtils.a(str, AjaxEntity.class);
    if (ajaxEntity != null && ajaxEntity.getData() != null) {
        AjaxInfo ajaxInfo = (AjaxInfo) ajaxEntity.getData();
        final String callback = ajaxEntity.getCallback();
        if (ajaxInfo.getType() != null) {
            Map<String, Object> a2 = BridgeUtils.a(ajaxInfo.getData());
            HashMap hashMap = new HashMap();
            if (a2 != null) {
                for (Map.Entry next : a2.entrySet()) {
                    hashMap.put(next.getKey(), next.getValue().toString());
                }
            }
            HttpUrl.Builder a3 = BridgeModel.a(ajaxInfo.getUrl());
            String type = ajaxInfo.getType();
            char c2 = 65535;
            switch (type.hashCode()) {
                case 70454:
                    if (type.equals("GET")) {
                        c2 = 0;
                        break;
                    }
                    break;
                case 79599:
                    if (type.equals("PUT")) {
                        c2 = 2;
                        break;
```

权限不当的Jsapi接口能力滥用

Web安全问题在新场景中的角色

XSS攻击

新场景：高权限域执行能力暴露，完全形态JSBridge Attack
传统攻击：获取Cookie/Token

开放重定向漏洞

新场景：绕过不当校验时机，执行JSBridge Attack
传统攻击：钓鱼网站/SSRF

域名校验方法不当

新场景：不当域名校验方法，绕过校验逻辑，执行攻击
传统攻击：业务域名安全校验

移动生态安全风险

- 智慧赋能，智慧连接的设计打破了既定的生态安全壁垒
- 账户/支付/应用服务体系增强了攻击的可能性与破坏性

移动应用生态安全 -- 越界的组件设计

本意：

- 轻应用/快应用/Hybrid化核心功能点
- 厂商生态化开发关键环节，App组件化关联与管理

越界：

- 生态化的同时收敛了安全边界，耦合性增强
- JsBridge 引入了Web特性，却对Web安全问题的处理不够（系统和开发者）
- 账户体系安全风险随之递增，复杂的组合场景未必能应对的面面俱到

移动应用生态安全

JSBridge Attack 攻击能力与厂商生态化开发中对App的设计及功能复杂度相关

传统Web 安全在移动应用新生态安全场景中扮演着更重要的攻击面

厂商的生态化管理与开发更需要注重安全问题

物联网与移动安全

隐私数据争夺新战场

物联网与隐私保护

万物互联，隐私数据安全更重要

IoT设备更有生态效应（智能家居，工控设备等）

物联网设备与隐私息息相关

隐私数据争夺新战场

物联网与隐私保护

设备种类繁多，与生态场景更贴近

普通数据，敏感数据甚至与人身安全有关联

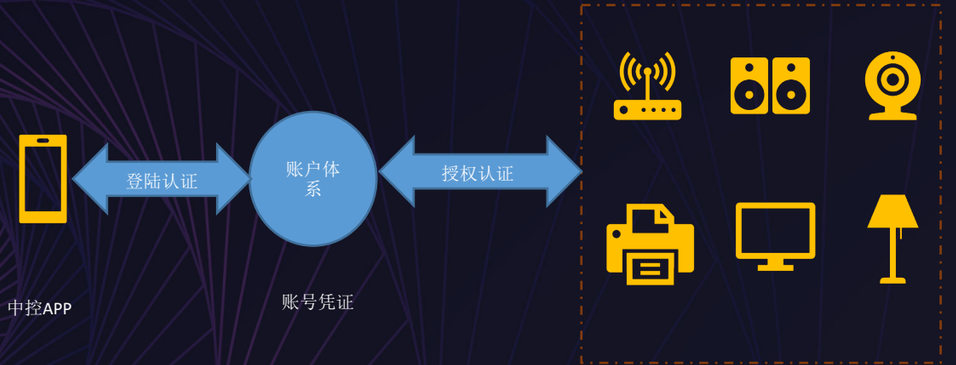
设备类型	设备名称	CWE	安全影响
	Gator 2 smartwatch	CWE-359：泄露隐私信息（侵犯隐私）	攻击者可以访问包含软件版本、IMEI、时间、定位方法（GPS与Wi-Fi）、位置坐标、电池电量等信息。
	路由器D-Link DIR-600和DIR-300	CWE-200：信息泄露	攻击者可以读取设备的敏感信息，或使其成为僵尸网络的一部分。
	三星智能电视	CWE-200：信息泄露	攻击者可以找到用于录音的二进制文件。
	家庭安全摄像头	CWE-359：泄露隐私信息（侵犯隐私）	用户的私人照片可能被攻击者盗取并公布到互联网上。
	智能成人玩具We-Vibe	CWE-359：泄露隐私信息（侵犯隐私）	攻击者可以获取设备温度和振动强度等信息。
	iBaby M6婴儿监视器	CWE-359：泄露隐私信息（侵犯隐私）	攻击者可以查看用户的信息，包括视频录像等。

设备认证，账户体系的隐患

- Token泄漏导致账户体系风险暴露

设备认证，账户体系的隐患

- 一号通用成了黑客的通行证

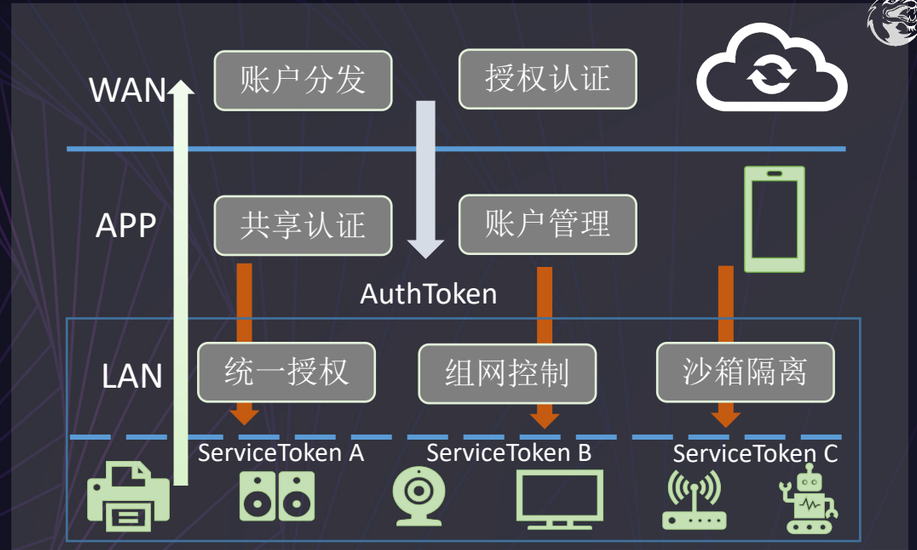


平行权限带来的隐患

- 系统APP与开放三方APP之前的平行权限
- 私网IoT设备沙箱体系下的平行权限

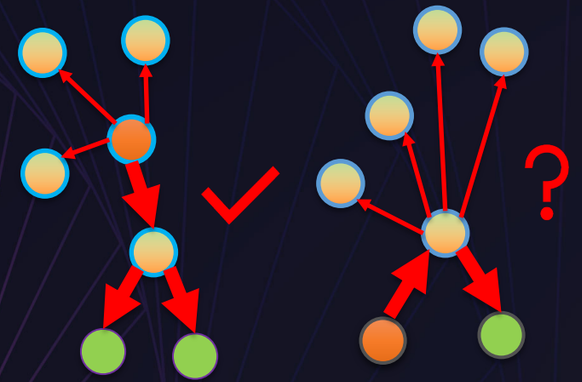
Token泄露导致生态体系崩溃

- 复杂应用场景下的认证体系设计
- 生态化场景放大了认证能力的边界



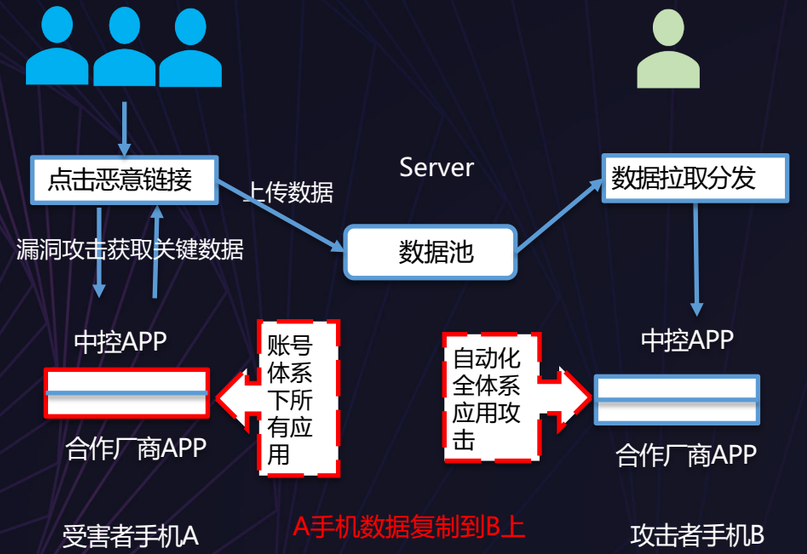
攻击模型（水滴攻击模型）

- 1）应用生态体系下APP—扩散+跳板式攻击
- 2）IoT生态安全场景：逆流+跳板式攻击



攻击效果：“另类”应用克隆

- 1）水滴攻击：单点打穿账户生态安全体系
- 2）隐私泄露：生态化场景下信息链泄露



开发者对物联网安全隐患认知不足

物联网与移动安全

- 物联网安全逐步形成生态安全，移动安全也是其中重要的一个环节
- 重视移动安全，相对忽视物联网安全

物联网生态安全影响

- 更接近用户隐私数据与生态场景
- 攻击后驻留效果更明显，隐蔽性及持久性更强

物联网与移动安全

物联网安全是生态安全的新趋势，移动安全又是其中重要核心

打造生态应用场景的同时，不可忽视便捷带来的隐患（如账户/认证风险）

重视物联网安全，保护隐私数据及正视安全问题

移动生态安全总结与展望

生态化是移动安全发展的重要趋势

生态化安全中厂商对安全与用户体验的衡量把控，权限收敛的同时重视安全边界

开发者对JSBridge Attack与Web问题新应用场景的理解

重视物联网生态场景中的安全问题与隐私数据保护意识

移动安全发展趋势于生态安全的理解和新生技术掌握

指纹/人脸识别等AI技术的涌入，黑科技背后带来不成熟的风险，如何权衡发展利弊
大数据与万物互联，隐私保护成为移动安全发展的新战场，如何守护

如何应对生态安全风险

规范开发，重视移动安全生态安全问题

审核扫描，系统化的同时与安全团队形成生态闭环

保护隐私，隐私数据是生态链条重要一环

合作共赢，积极应对安全风险，开放的态度合作沟通，共赢互助

THANKS