



正面向你繁花似锦，
背面连接暗无天日。



赵云翔

目录

CONTENTS

one

为什么

我们会遇到安全问题？

TWO

不法分子通过什么方式对我们的设备进行攻击？

Three

病毒

通过什么方式进入我们的设备

The End

面对这些，我们应该怎么做？



one

为什么

我们会遇到安全问题？

WHY?

利益

Interest

利益的驱使

1

移动支付
迅速发展，

2

网络账户
共联共享。

3

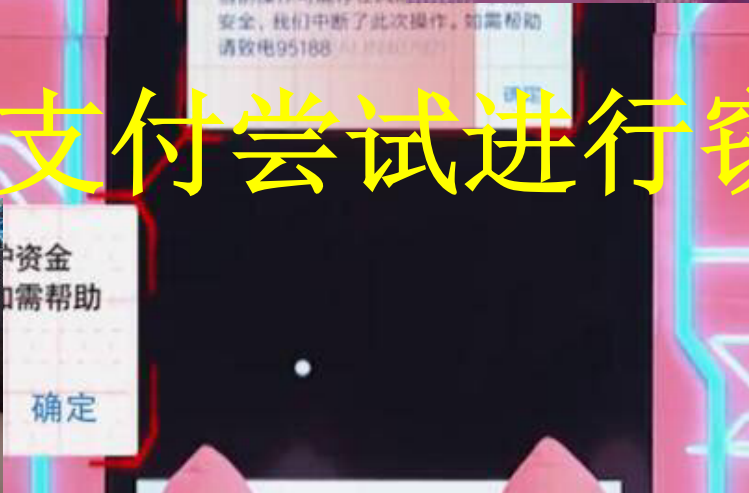
物联网的
普及壮大。

4

信息交互
通讯工具。




某节目中对移动支付尝试进行窃取






众多网络社交账号中保存了大量个人信息安全，各种盗号等威胁不断存在。

For 45 Minutes



物联网，智能家居的迅速普及带来的不只有便利



手机号中绑定了许多的个人账户，一旦被窃取，损失惨重
5G信息时代的到来，对我们数据安全考验更加巨大。

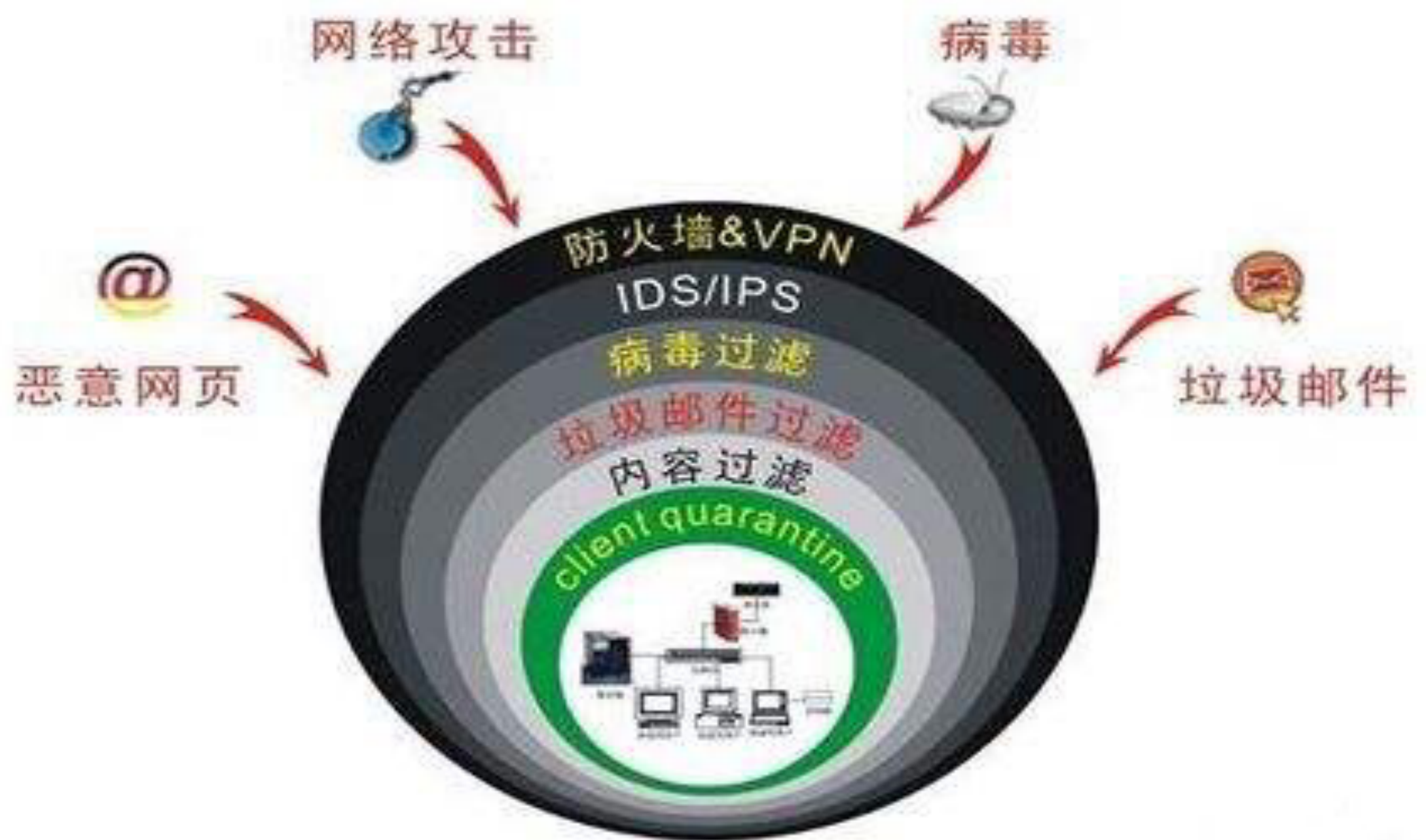
TWO

不法分子通过什么方
式对我们的设备进行
攻击？



攻击方式类型展示图







病毒

病毒

权限获取

远程操控

Three
病毒
通过什么方式
进入我们的设备



移动设备

无线连接

有线连接

被动下载

主动下载

无线连接入侵方式

1. 设备连接未知的无线局域网络
2. 运营网络中基站攻击方式
3. 通过短信彩信等方式发送未知连接诱导打开

有线连接方式

设备通过数据线等有线连接方式对设备进行病毒植入



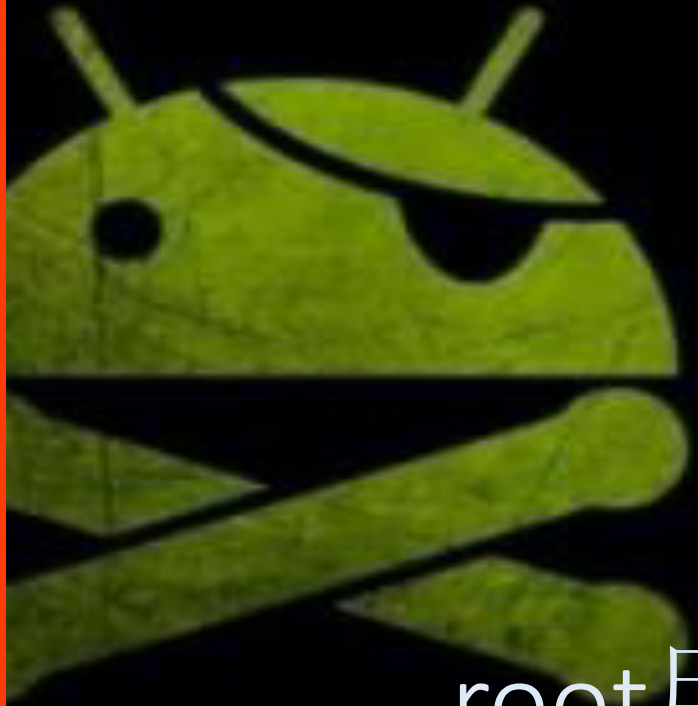
20 嘶吼白帽子
19 技术沙龙

回到
设备本身

Back to the device itself

安卓系统Root ios系统越狱

手机最高权限的获取真的有必要吗？



#ROOT

root用户是系统中唯一的超级管理员，它具有等同于操作系统的权限。

我们真的可以完全信任与手机自带的安全系统吗？

国内外诸多手机厂商在近几年的发展中越来越看重安全，形成了各家自己的安全系统，那么他们真的可以信任吗？

The End

面对这些，我们应该怎么做？

What on earth should we do?



作为用户

As user

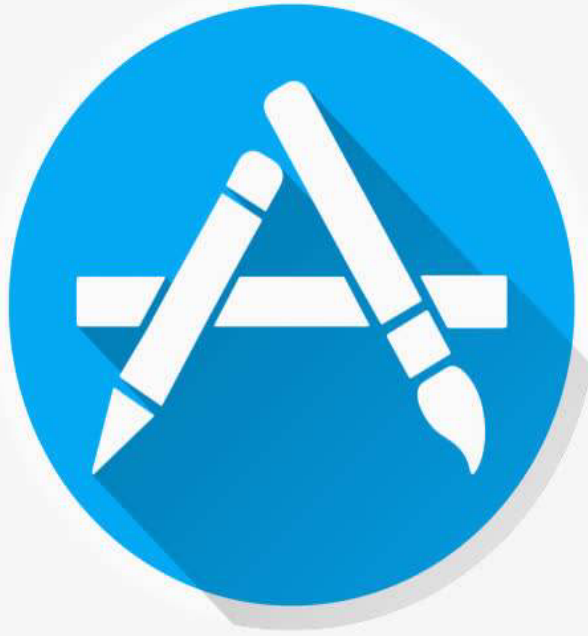
手机越狱和root要慎重

安卓root和苹果越狱会带来便利,可以安装更多软件,实现更多高级功能。但如果安装到恶意APP,可以读写删除手机文件、监听截取手机短信等。

建议:非专业人员切勿越狱或Root,要在官方市场下载应用

智能家居存在威胁不容忽视

现象;技术人员研究发现,现在可以通过之前编写好的破解程序,利用用户注册门锁的手机号码进行破解。建议;最好使用不太常用的手机号码注册,不要把撷手机号轻易交给不熟的人



使用手机APP要谨慎

现象现在恶意AP程序越来越多,各类非官方下载渠道常被恶意应用。

建议:·手机用户不使用来历不明的AP,使用正规渠道下载

·安装时要注意“应用权限”与产品功能是否直接相关

使用防病毒软件,为手机安全加上防护网

摄像头攻击多留心

现象:家庭摄像头已成黑客攻击对象,很可能导致个人隐私泄露

等。

建议:·不要使用预设密码,重置密码越复杂好,需要定期更换

·摄像头不要对较私密空间,浴室、床等位置要尽量躲开

·在家时可以关闭摄像头电源或用遮挡物挡住

陌生人发微信红包勿乱点

现象:不法分子将手机病毒伪装成微信红包诱导消费者领取,遇到陌生人发送“红包”不要乱点,很可能带有病毒。

建议:如果点开红包需要填写个人信息等,肯定是骗局,要第

一时间关闭手机网络,修改网银、支付宝等密码,然后通过正规途径删除病毒。

免费打印片有危险

现象:照片打印成为部分商家吸粉利器,且很容易泄露用户信息,比如,扫描二维码可能会让手机感染病毒。



人脸识别也危险

观象在之前央视315晚会上,人脸识别
技术曾被曝出安全隐患,

仅凭两部手机、一张随机正面照和一
个换脸APP,就

能通过3D脸模骗过人脸识别系统。

建议;在这术还没有成熟 之前,
慎重使用!

虚假二维码泄漏信息

现象:不法分子通过虚假伪装一个网站生成二维码,在受害者扫描二维码时,通过云端软件获取当事人账号、密码等

建议见码检查,千万不要见码就扫

作为开发者

As a developer

20 嘶吼白帽子
19 技术沙龙

只能用自己最大的努力
为用户创造更安全的环境！

加油，中国开发者

邪不压正

Good prevails over evil

回归最本质的信息安全

THANKS!

