

移动互联时代的隐私保护

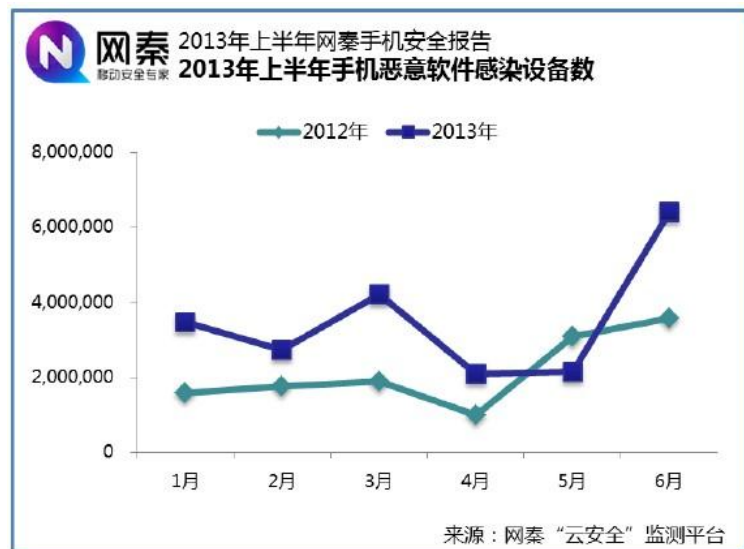
网秦 严挺

智能手机成为首要攻击目标

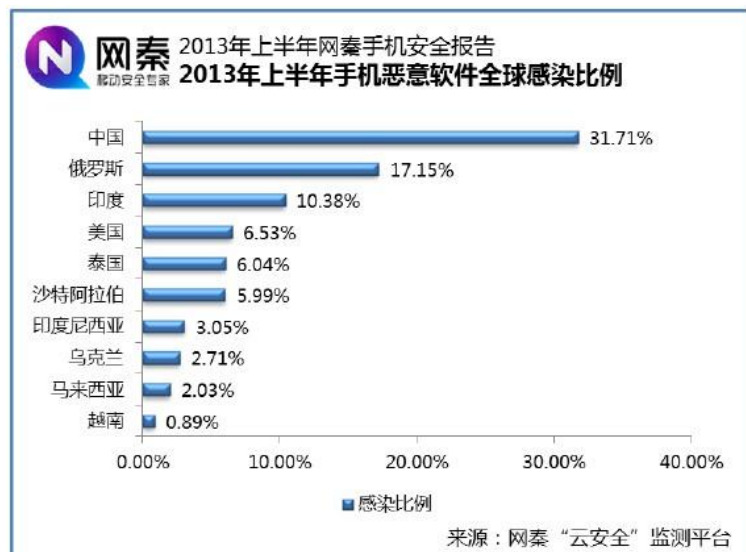
终端型号多样化：不同厂商、不同平台、不同版本，缺乏统一有效的安全机制；

海量应用软件：应用软件开发上线门槛低，大多存在编码漏洞；

BYOD深入应用：政府、企业移动信息化的兴起，内部数据成为黑客关注重点。



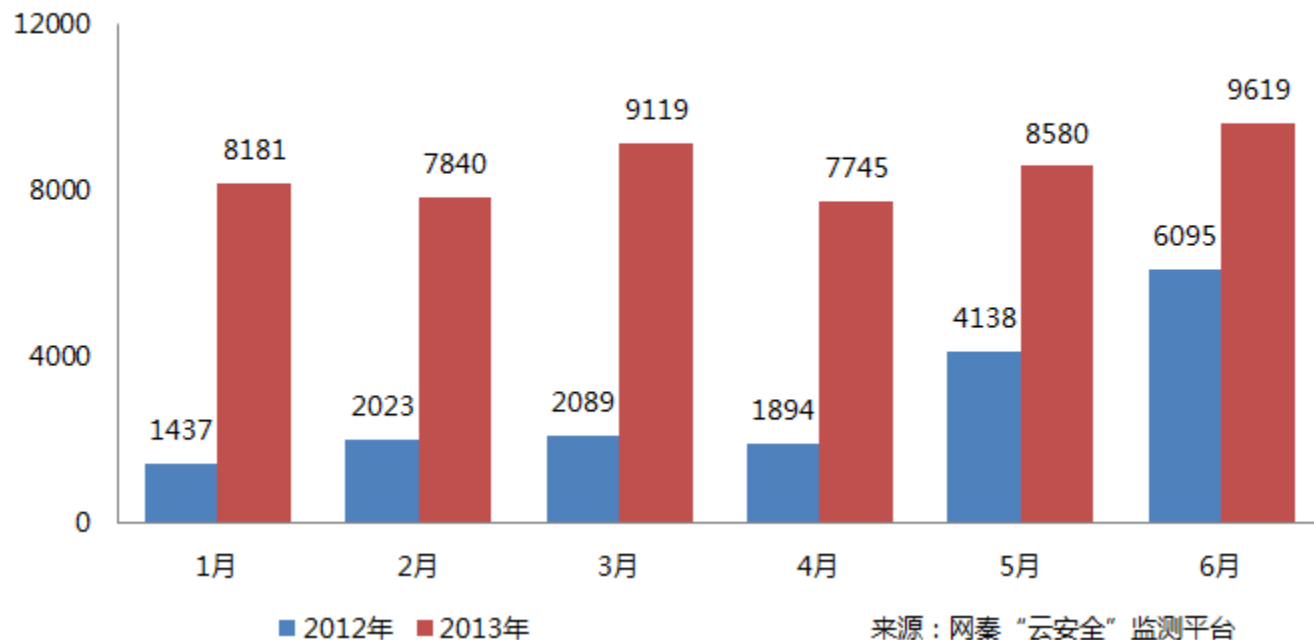
2013年上半年全球感染手机**2102万部**，同比2012年上半年增长**63.8%**。



中国大陆地区以**31.71%**的感染比例位居首位，俄罗斯（17.15%）、印度（10.38%）、美国（6.53%）位居其后

恶意软件迅猛增长

2013年上半年手机恶意软件增长情况



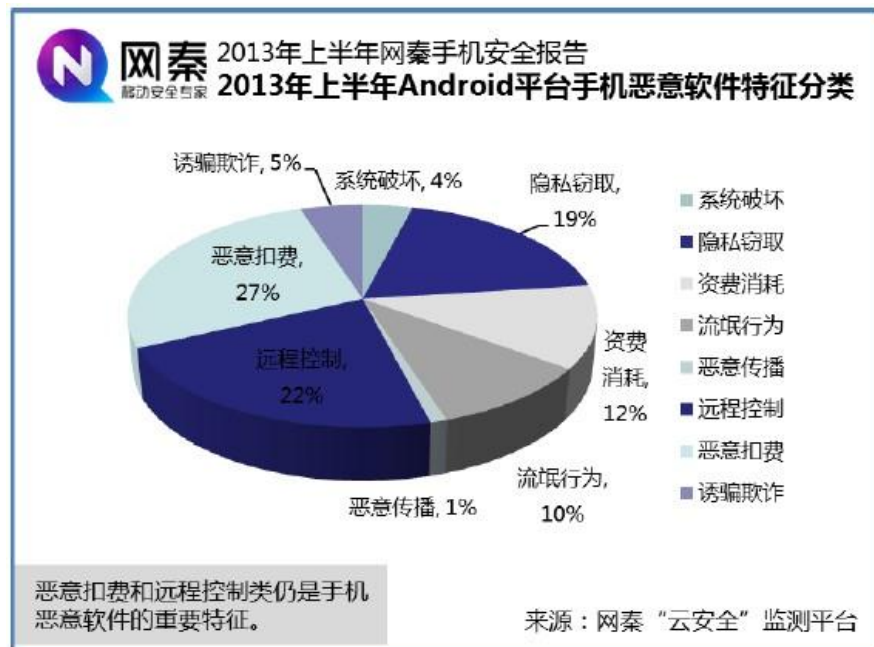
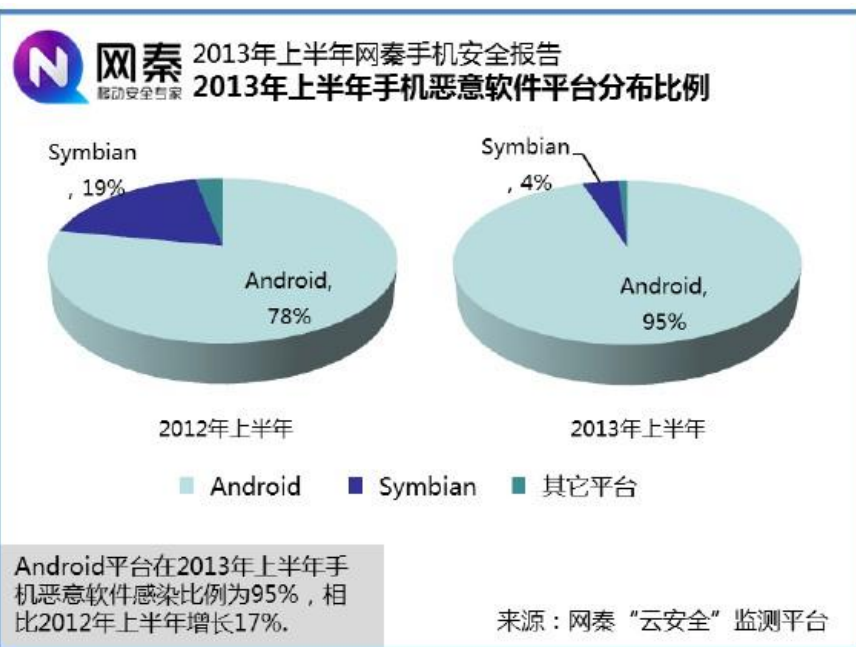
2013年上半年3月份和6月份数据增长较快，6月份查杀9619款恶意软件，居上半年首位。

2013年上半年单月相对于2012年同期有较大增长，尤其以第一季度前3个月的恶意软件数据增长幅度最为明显。例如3月份查杀9119款，同比2012年3月份增长336.5%。

Android平台成为攻击重灾区

开源操作系统：Android是基于Linux的开放源代码系统，可利用漏洞较多；

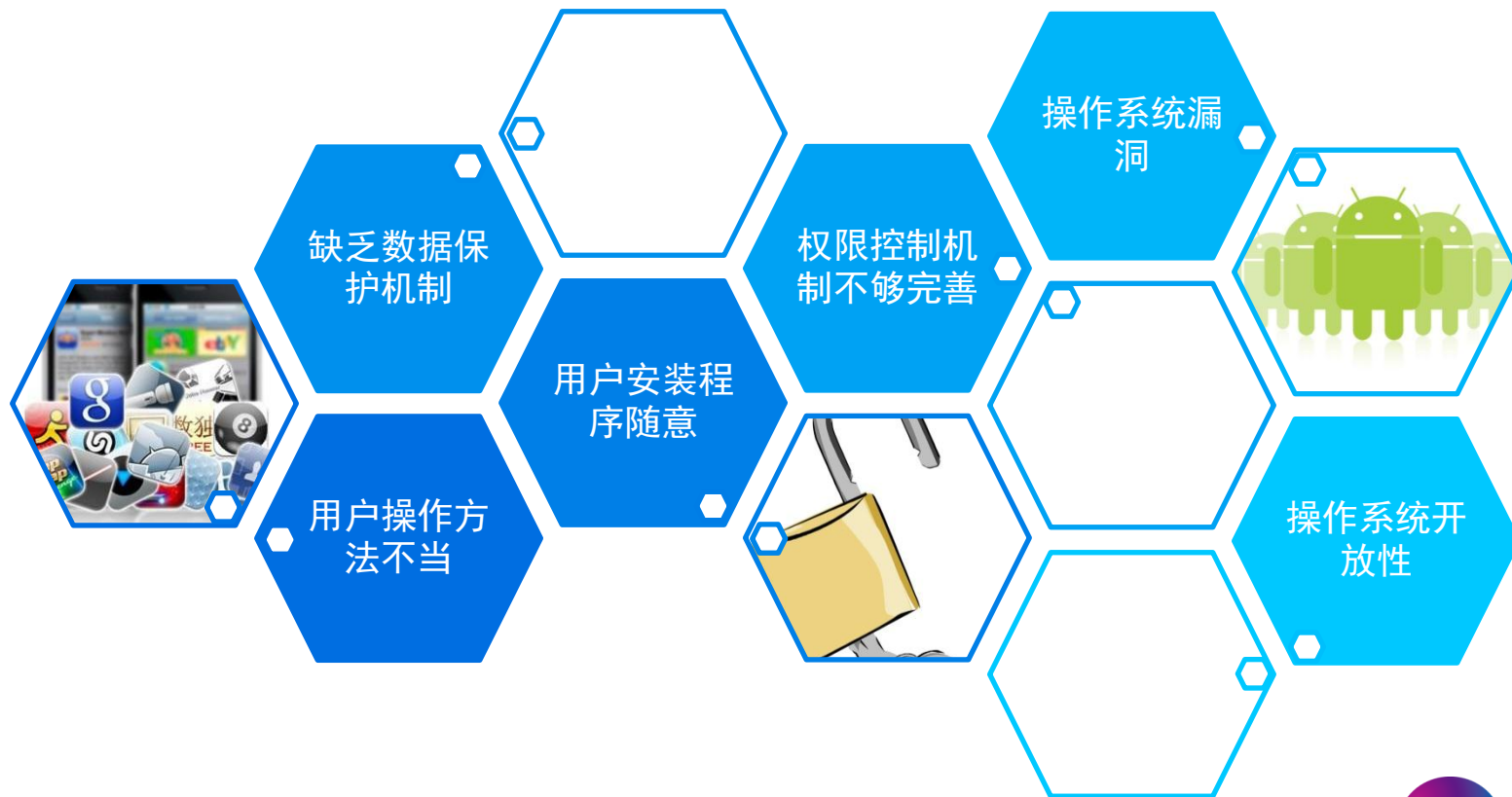
应用传播渠道开放：应用商店、下载站监管机制弱，应用程序质量难以保证。



用户隐私泄露途径多样



智能手机根源问题不容忽视



几款典型隐私窃取案例



a.privacy.JPush.GEN 伪装为瑞士军刀工具箱

病毒安装后，不但后台会上传联系人，通话记录，浏览器书签信息，还会插入短信，彩信，获取并上传用户及用户好友的QQ号码，用户使用QQ音乐听过的音乐名称。个人猜测，获取音乐名称，可以获取用户平时喜好；获取QQ号码，可用来通过邮件方式配合用户喜好发送广告推广类型的垃圾邮件。



a.payment.CalDX.b 伪装为手电筒应用

该病毒会监听手机启动广播和短信广播，CalDX 开启后会发送短信，短信号码为"15981905078"，短信内容为"register2"，泄露用户手机号码，当病毒作者向安装此软件的用户发送短信内容以"*S#"开头且以"*E#"结尾的远程控制指令短信时，会解析短信内容，更新发送的号码，内容和发送时间，并且屏蔽远程控制指令。



影响较大的隐私窃取事件

CSDN拖库事件

ORACLE3800W

某某酒店2000W

QQ群关系7000W

...

CNET科技资讯网 2月27日 国际报道：据路透社报道，网络安全公司Hold Security周三发布的一份调查报告称，该公司仅利用三周时间，在网络黑市上发现了3.6亿不同的个人账户信息被黑客兜售。这些个人账户信息包括常常被用作用户名的电子邮件地址和文本中的大多数未加密口令。



技术发展总体趋势

典型产品技术

- 开源软件产品
(TaintDroid)
- 商用软件产品
(TrustLook)
- 商用硬件产品
(Samsung)

典型安全技术

- 软硬结合保证
(KNOX)
- 基础技术平台
(Dionaea)
- 硬件安全增强
(TrustZone)
- 软件检测提升
(aDFAer)
- 综合安全检测
(iTestin)

典型融合技术

- 传统移动结合
(PCI DSS)
- 加固和虚拟化
(Wrapper/Container)
- 传统安全技术 (安全合规)

典型安全技术

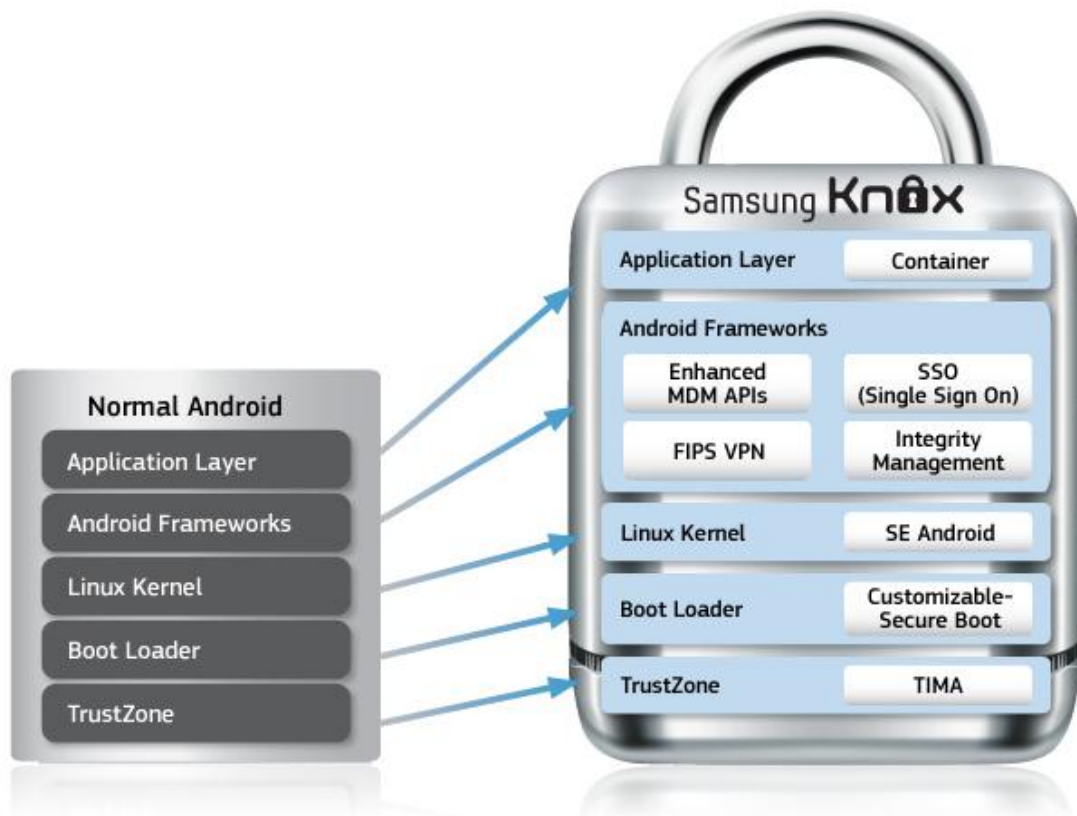


典型产品技术



典型安全技术：Samsung Knox

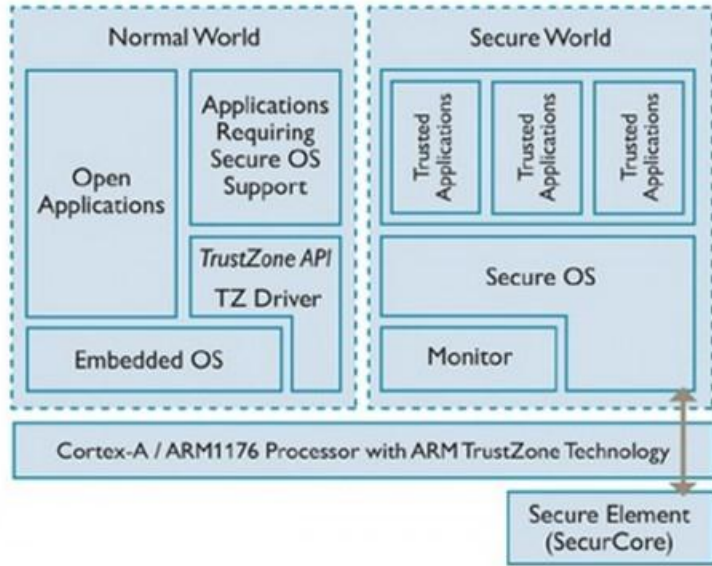
Android企业级安全解决方案：（ 硬件 + Framework + APP ）



典型安全技术：TrustZone

TrustZone技术

在同一个系统中为安全数据打上标签然后进行划分，并且在硬件上对安全信息和非安全信息进行清晰的区分。这一区分使得安全的代码和数据不需要再被编译就可以在操作系统中进行执行，同时不容易受到攻击。



Software Architecture of TrustZone

典型融合技术

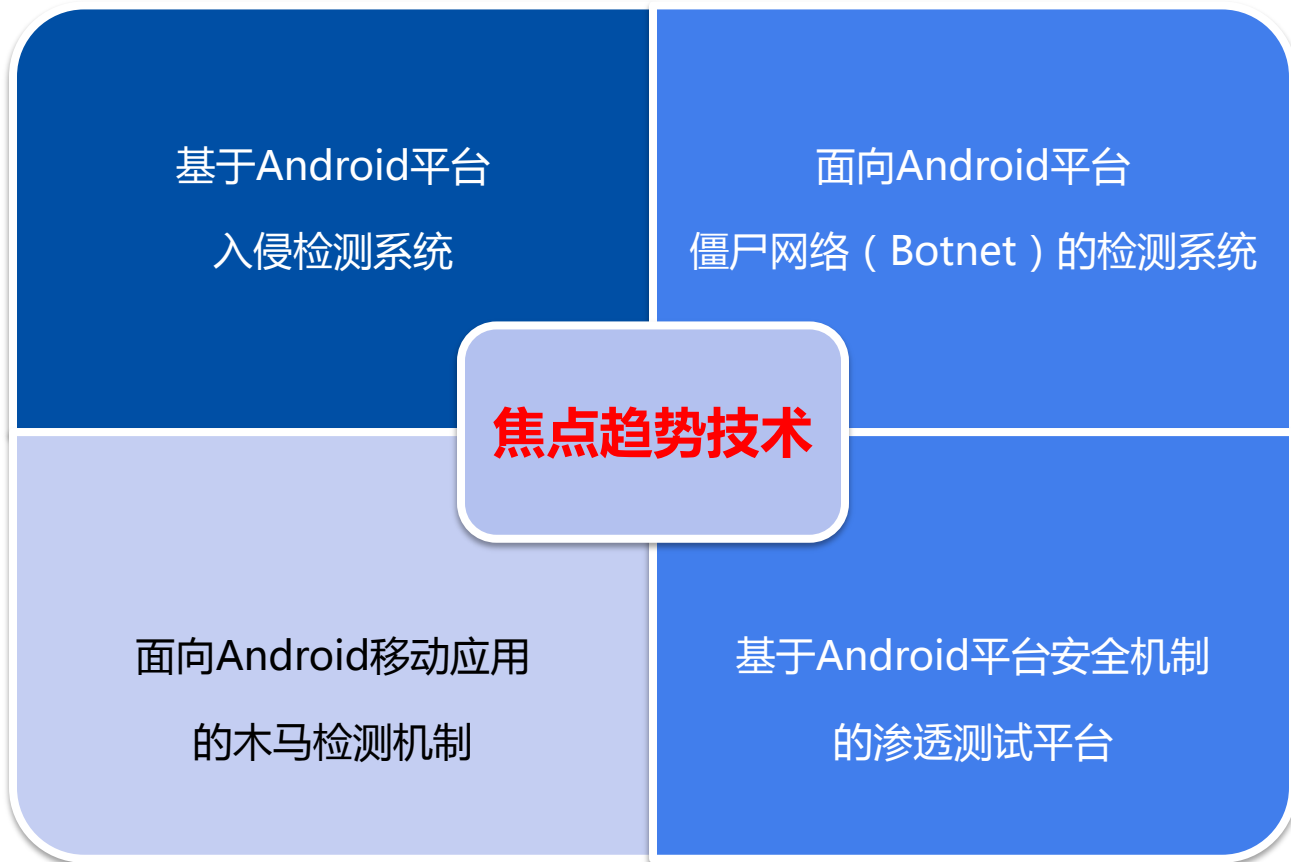
- 面向移动领域的安全合规
- 提供军用加固移动设备系统
- 制定针对移动设备和BYOD的政策与标准
- 规定应用程序和数据与私人数据隔离

- 应用安全加固，代表厂商 Mocana
- 系统漏洞发掘，代表厂商 Bluebox
- 移动安全策略，代表厂商 Sophos
- APT攻击数据分析，代表厂商 CrowdStrike

- 移动安全的持卡人数据安全要求
- 移动支付要求P2P数据的安全保证
- 未授权信息访问和机密信息加密规定

将传统安全技术融合到移动安全领域

焦点趋势技术



机遇

1. 行业期待更完备的更富创新意识的移动设备隐私保护解决方案！
2. 建设信息安全强国成为国家战略！



谢谢

网秦移动集团 (NYSE : NQ) 2014