FREEBUF | 企业安全 俱乐部

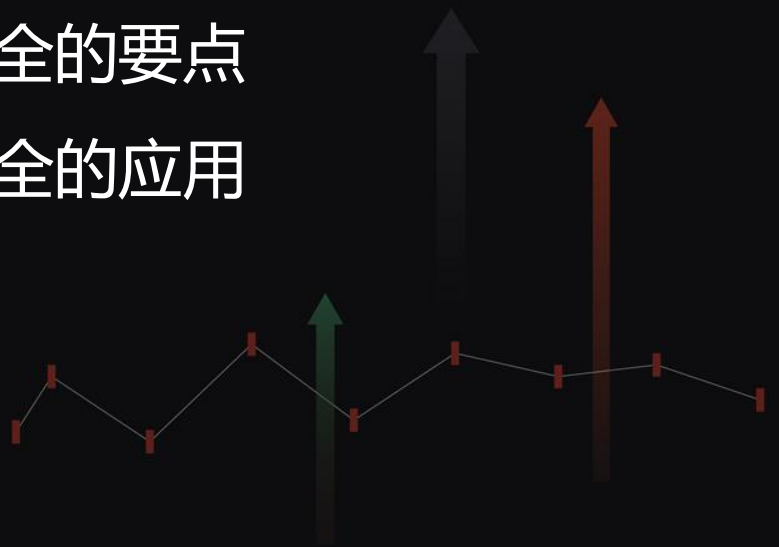
网络安全等级保护在移动安全中的应用

韩云　爱加密安全服务总监

2019企业安全俱乐部　等保专场

目录

- ✓ 移动应用程序面临的安全风险
- ■ 网络安全等级保护的移动互联扩展要求解读
- ■ 网络安全等级保护移动安全的要点
- ■ 网络安全等级保护移动安全的应用
- ■ 爱加密公司



移动应用程序面临的安全风险

据统计，每年至少新增150万种移动恶意软件，至少造成超过1600万件的移动恶意软件攻击事件。爱加密持续关注我国移动应用安全问题，专注于构建移动应用安全生态圈。通过移动应用大数据平台，为政府和企业客户提供移动安全报告的数据支撑，协助其对移动应用安全事件进行监测并协调处置。

爱加密全国移动APP安全性研究报告，旨在让移动手机用户了解APP风险隐患对个人隐私信息及资金安全等方面所造成的威胁，提高其安全防范意识。通过对App违法违规收集使用个人信息行为的通报，协同有关主管部门、APP供应商、APP提供商等，共同营造安全的移动应用环境，促进网络安全的规范化、安全化、健康化发展。

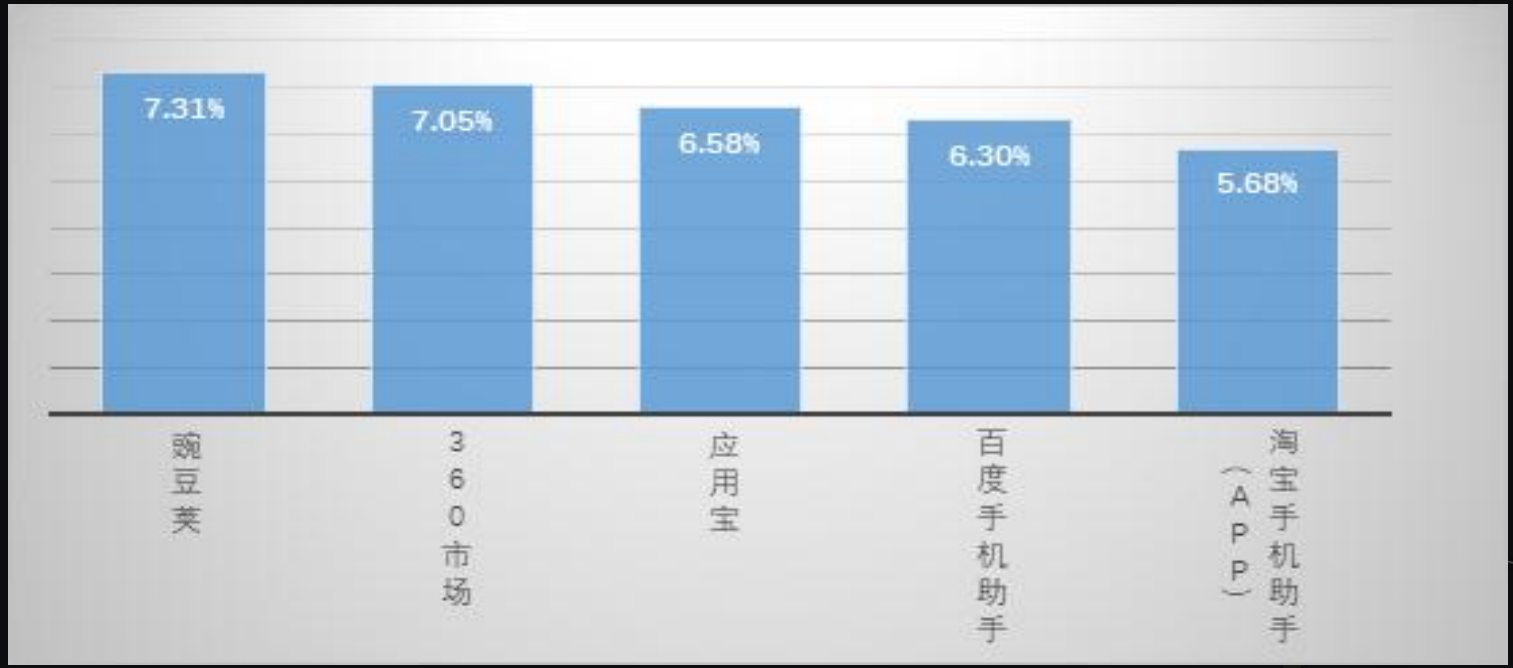
移动应用程序面临的安全风险

根据爱加密大数据中心提供的数据，截止3月底大数据中心已收录Android app应用270多万个，IOS应用190多万个，其中50%以上的APP都存在漏洞威胁，5.24%的APP存在病毒，30%以上的APP存在不同程度的越权、超范围收集等违规行为。

游戏娱乐类APP 53万，约占总量的20%，存在高风险漏洞最多，在所有app中相对最不安全。金融理财类APP位居第二，有26万，约占总量的10%。教育培训类APP排名第三，有13万，约占总量的5%。

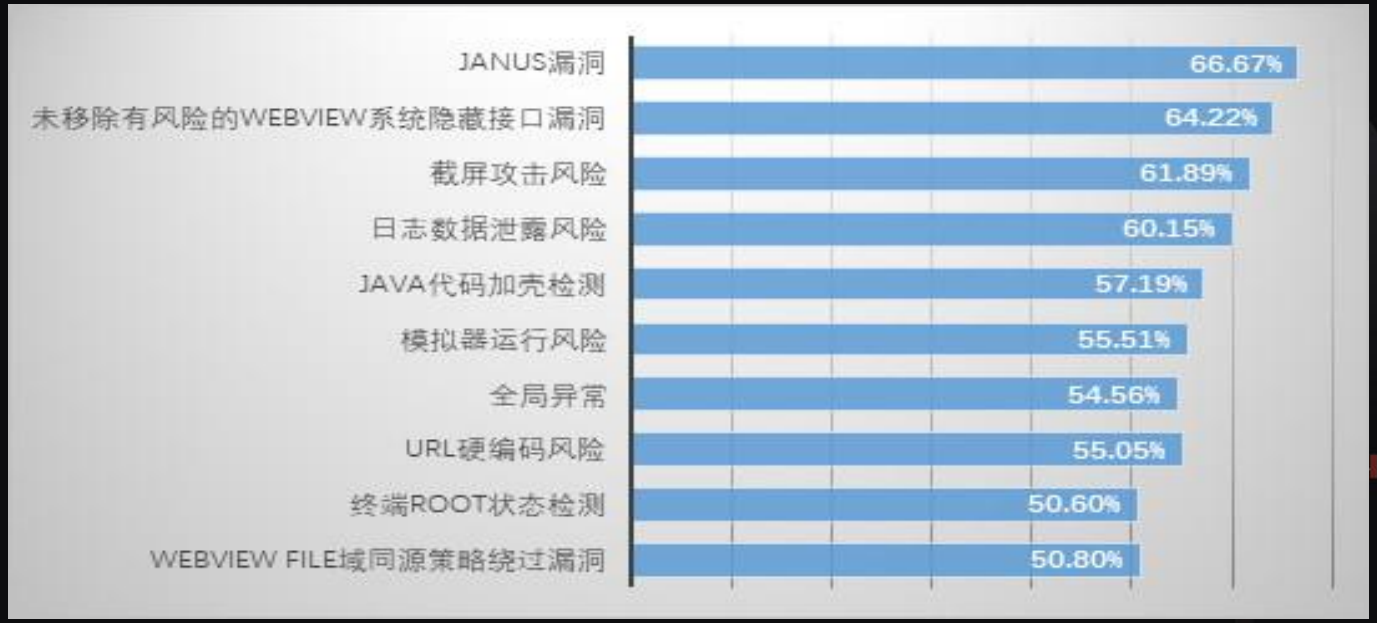
移动应用程序面临的安全风险

从应用市场拥有APP数量来看，目前上线的APP市场有500+，其中豌豆荚、360市场、应用宝占据应用市场排名前三甲。



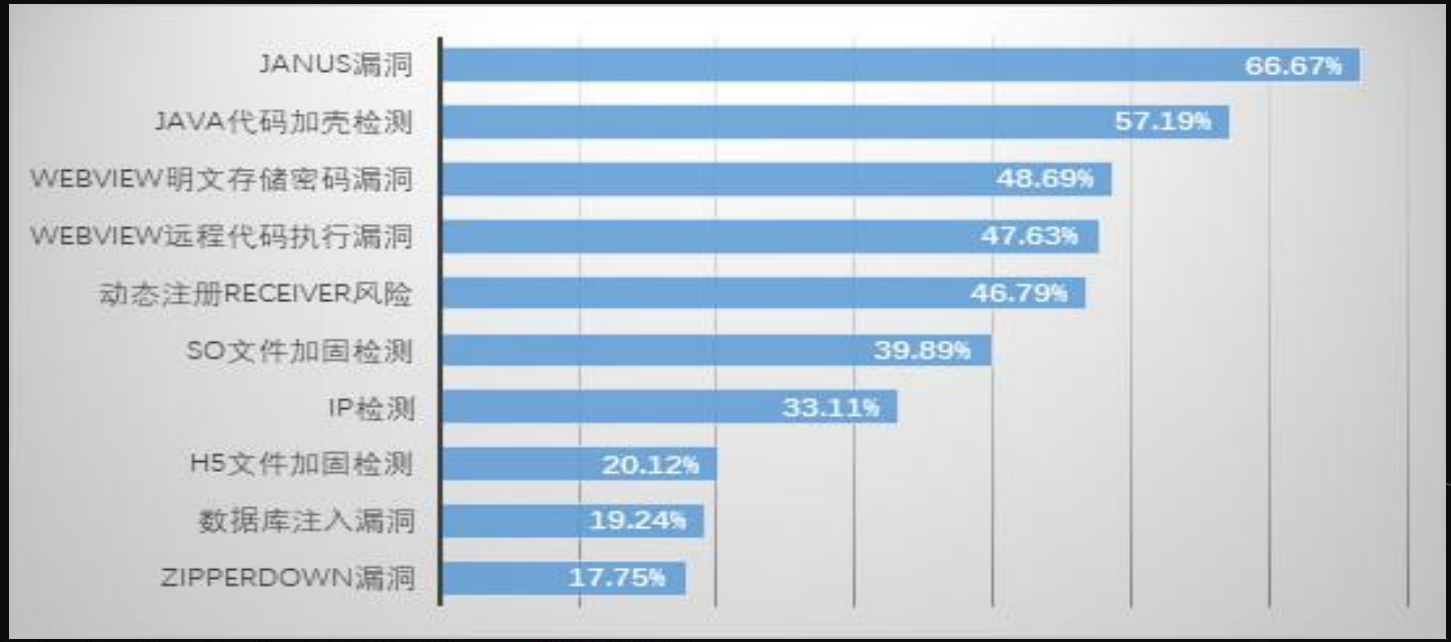
移动应用程序面临的安全风险

爱加密移动应用安全平台扫描了270多万个APP，其中，有漏洞的APP约183万个，占监测总数的67.77%。排名前三的漏洞分别是：Janus漏洞、未移除风险的WebView系统隐藏接口漏洞、截屏攻击风险漏洞。



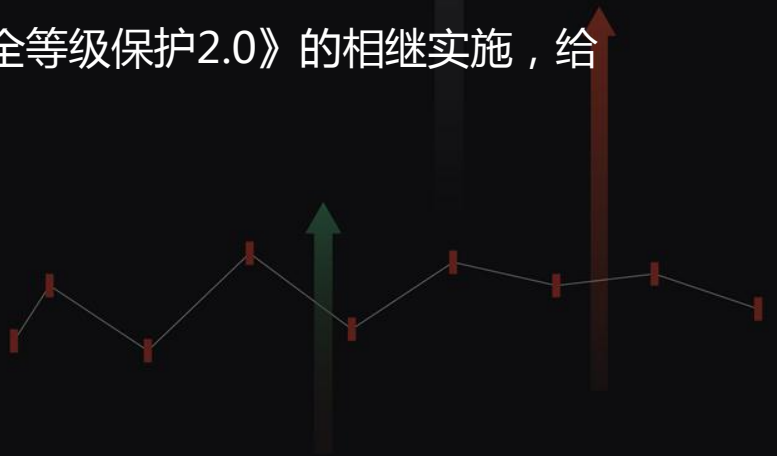
移动应用程序面临的安全风险

从APP漏洞种类来看，存在Janus高危漏洞的APP数量最多，占监测总数的66.67%；其次是Java代码未加壳漏洞，占监测总数的57.19%；排在第三位的是WebView明文存储密码漏洞，占监测总数的48.69%。



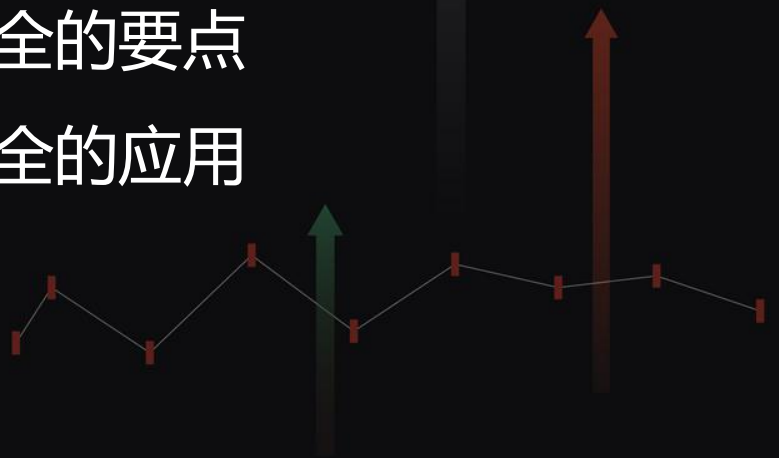
移动应用程序面临的安全风险

在移动安全发展迅速的今天，不法分子的攻击手法层出不穷，并快速更新迭代，移动应用攻击场景也随之日趋复杂。除此之外，随着云计算和大数据技术的成熟与普及，越来越多的企业和机构聚焦于移动应用中个人信息的价值，但国家为了营造更安全健康的网络环境，对相关行为的约束却已上升至法律法规层面，执法力度也在逐渐加强。《网络安全法》、《个人信息安全规范》《网络安全等级保护2.0》的相继实施，给我们移动安全提供了相关标准和依据。



目录

- 移动应用程序面临的安全风险
- ✓ 网络安全等级保护的移动互联扩展要求解读
- 网络安全等级保护移动安全的要点
- 网络安全等级保护移动安全的应用
- 爱加密公司



网络安全等级保护的移动互联扩展要求（三级）

- ◆ 安全物理环境
  - ➢ 无线接入点的物理位置

应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

解读：应为无线接入设备的安装选择合理的位置，避免过度覆盖和电磁干扰；检查物理位置与无线信号覆盖的合理性；测试电磁干扰的情况；

- ◆ 安全区域边界
  - ➢ 边界防护

应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

解读：检查并测试有限网络和无线网络之间是否部署无线接入网关设备，网关设备（无线准入设备、无线防火墙等）

网络安全等级保护的移动互联扩展要求（三级）

- 访问控制

无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。

解读：检查无线接入设备的认证开启情况，是否采用认证服务器或者国家密码管理机构批准的密码模块进行认证；

- 入侵防范

本项要求包括：

a)应能够检测、记录非授权无线接入设备；

解读：检查和查看是否能够检测和验证非法授权的无线接入设备和移动终端的接入行为；

网络安全等级保护的移动互联扩展要求（三级）

b)应具备对针对无线接入设备的网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录；

解读：告知我们应该具备网络扫描、DDOS攻击、密钥破解、中间人攻击和欺骗攻击等设备并检测；

c)应能够检测到无线接入设备的SSID广播、WPS等高风险功能的开启状态；

解读：如果有无线接入设备的SSID广播、WPS等高风险功能应开启状态，并能出具报告；

d）应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID广播、WEP认证等；

解读：应关闭SSID广播、WEP认证等存在风险的功能；

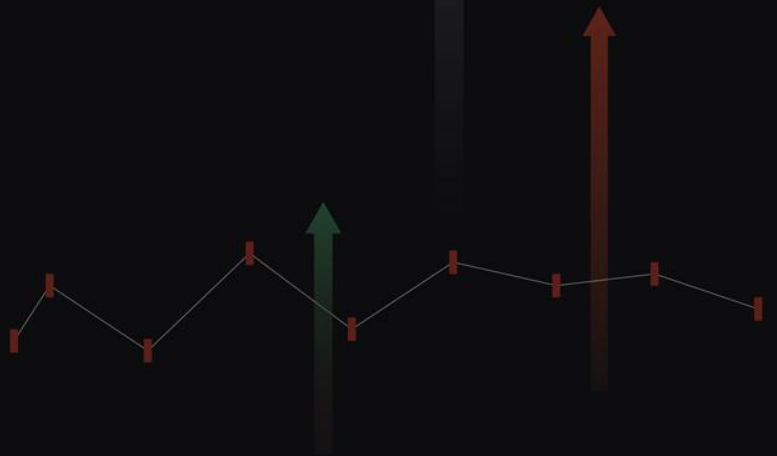
网络安全等级保护的移动互联要求

e)应禁止多个AP使用同一个认证密钥。

解读：这一项告诉我们，是否设置认证秘钥，如果设置了多个AP，是否使用了不同的秘钥。

f）应能够阻断非授权无线接入设备或非授权移动终端；

解读：告诉我们，要具备阻断阻断和验证非授权无线接入设备或非授权移动终端；



网络安全等级保护的移动互联要求

- ◆ 安全计算环境
- ➢ 移动终端管控

本项要求包括：

a)应保证移动终端安装、注册并运行终端管理客户端软件；

解读：告诉我们移动终端是否安装、注册并运行终端管理客户端软件；

b)移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等。

解读：告诉我们移动终端管理系统是否设置了对移动终端进行远程控制及设备生命周期管理等安全策略；

网络安全等级保护的移动互联扩展要求（三级）

- 移动应用管控

a）应具有选择应用软件安装、运行的功能；

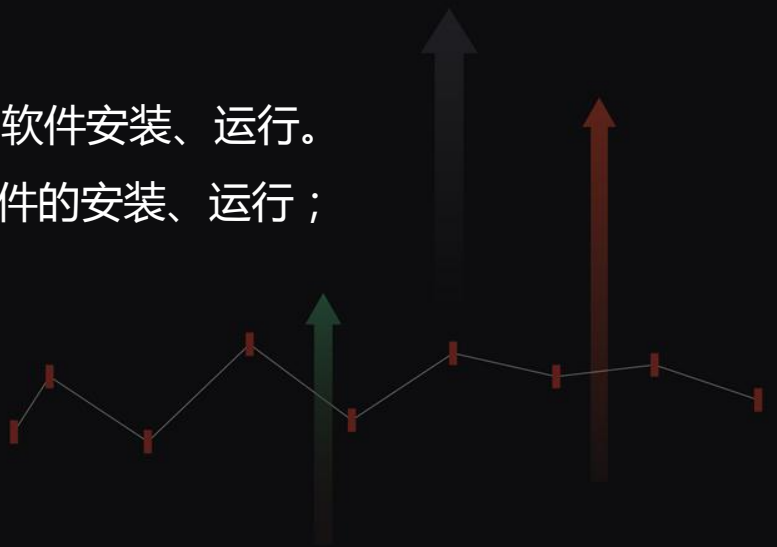
解读：查看是否具有选择应用软件安装、运行的功能；

b) 应只允许指定证书签名的应用软件安装和运行；

解读：查看全部移动应用是否由制定证书签名；

c) 应具有软件白名单功能，应能根据白名单控制应用软件安装、运行。

解读：查看是否具有白名单功能并验证是否能控制软件的安装、运行；



网络安全等级保护的移动互联扩展要求（三级）

- ◆ 安全建设管理
- ➢ 移动应用软件采购

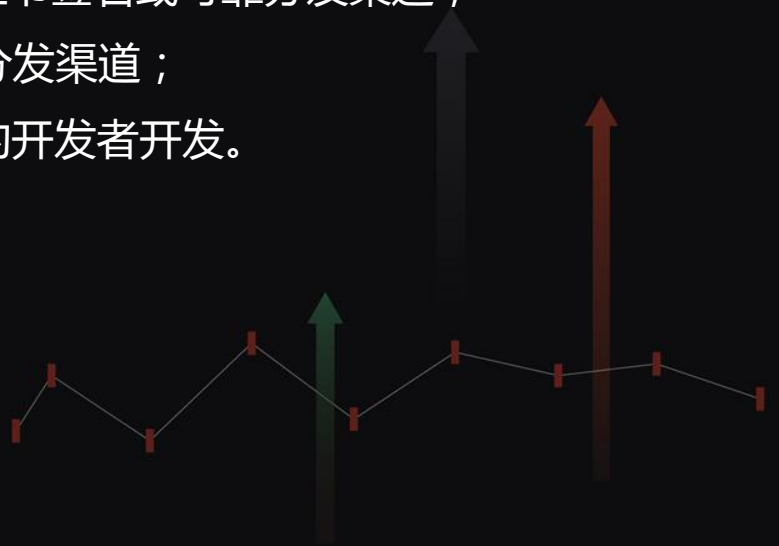
本项要求包括：

a)应保证移动终端安装、运行的应用软件来自可靠证书签名或可靠分发渠道；

解读：移动应用软件是否来自可靠证书签名或可靠分发渠道；

b)应保证移动终端安装、运行的应用软件经由指定的开发者开发。

解读：检查移动应用软件是否由制定的开发者开发；



网络安全等级保护的移动互联扩展要求（三级）

- 移动应用软件开发

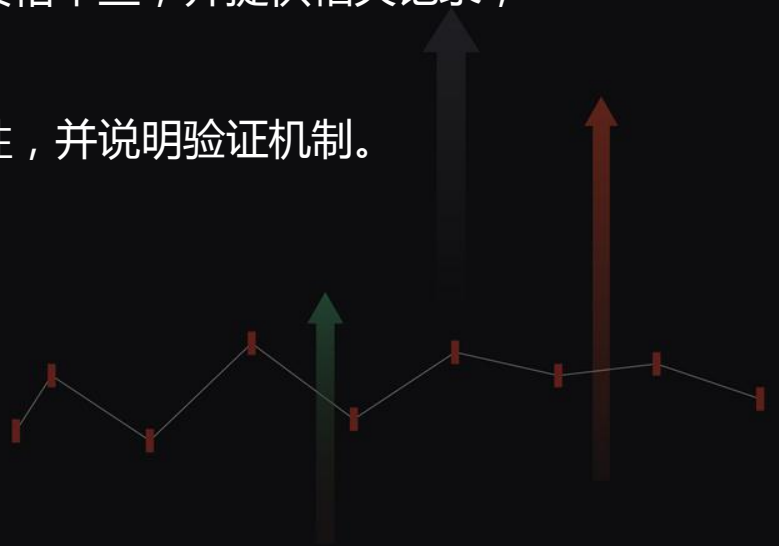
本项要求包括：

a)应对移动业务应用软件开发者进行资格审查；

解读：主要检查移动业务应用软件开发者是否进行资格审查，并提供相关记录；

b)应保证开发移动业务应用软件的签名证书合法性。

解读：查看开发移动业务应用软件的签名证书合法性，并说明验证机制。

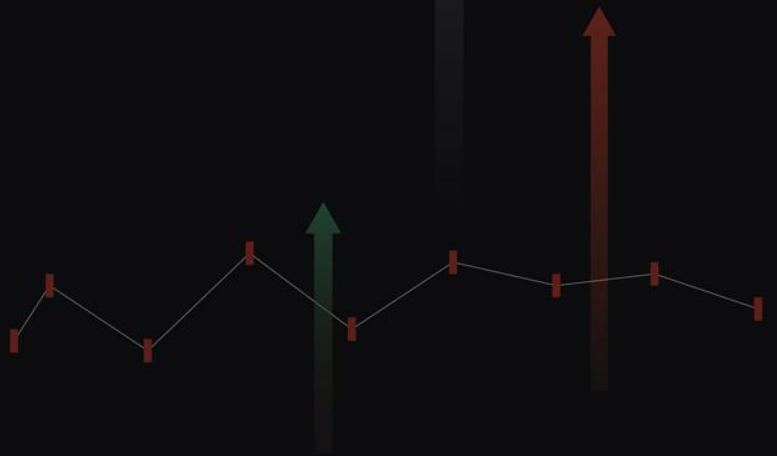


网络安全等级保护的移动互联扩展要求（三级）

- ◆ 安全运维管理
- ➢ 配置管理

应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。

解读：查看是否建立合法无线接入设备和合法移动终端配置库，并通过配置库识别非法设备。



网络安全等级保护的移动互联扩展要求（总结）

网络安全等级保护是在原来等级保护1.0的基础上的升级，扩大了保护的范围，使等级保护保护的更加精准；《网络安全法》明确规定了“国家实行网络安全等级保护制度”，确定了等级保护制度的法律地位。网络安全等级保护的新标准涵盖了个人信息的重要性，把个人信息列入等级保护是对个人信息的重要程度的体现，也是保护个人信息的重大举措。

网络安全等级保护它是中国网络安全的重大成就、是中国网络安全保障的重大创举、是中国网络安全界广大人民智慧的结晶、是中国网络安全的基石、是维护国家安全、社会秩序、公共利益的根本保障，是中国网络安全历史发展的趋势。

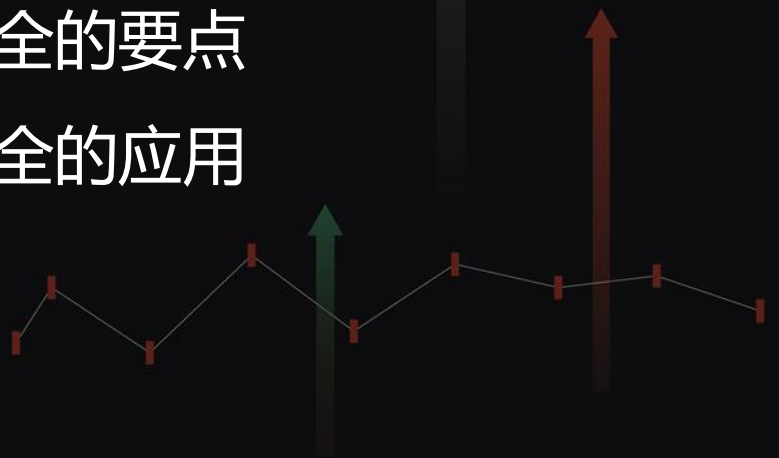
网络安全等级保护的移动互联扩展要求（总结）

等级保护2.0的关键信息是在原来1.0的基础上增加的部分，例如云计算安全、移动互联安全、物联网安全工业控制系统安全及应用场景；从这一点来看，等级保护2.0和我们透露的网络安全等级保护的标准不再是单一的，网络安全需要全面的、多方位的、多角度的共同发展，是全网络、全产业、全社会的责任和义务，需要维护和支持；

爱加密作为移动安全服务商之一，我们公司很看重国家安全，一直以来都很关注国家相关政策，积极响应国家号召，等级保护2.0专门提出了移动互联安全扩展要求对我们公司是一种鼓励和支持，为以后在移动安全方面开展工作提供了依据和保障。

目录

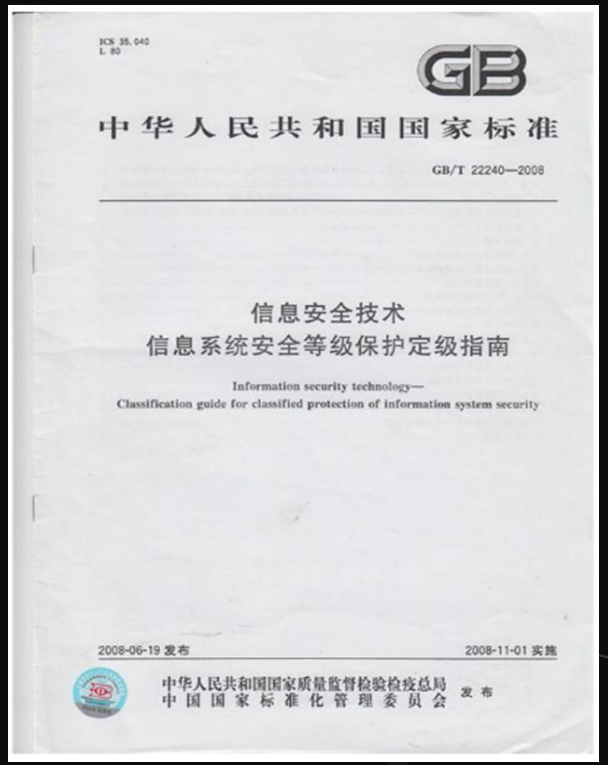
- 移动应用程序面临的安全风险
- 网络安全等级保护的移动互联扩展要求解读
- ✓ 网络安全等级保护移动安全的要点
- 网络安全等级保护移动安全的应用
- 爱加密公司



网络安全等级保护移动安全的要点

- 移动互联技术的等级保护对象进行定级

采用移动互联技术的等级保护对象应作为一个整体对象定级，移动终端、移动应用和无线网络等要素不单独定级，与采用移动互联技术等级保护对象的应用环境和应用对象一起定级，符合等级保护总体思想，就是将保护对象作为一个整体考虑其安全防护要点。


ICS 35.040
L 80

GB

中华人民共和国国家标准

GB/T 22240—2008

信息安全技术
信息系统安全等级保护定级指南

Information security technology—
Classification guide for classified protection of information system security

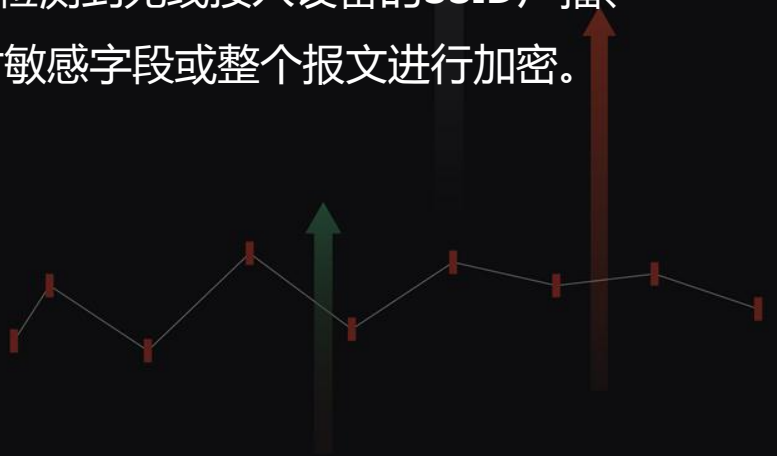
2008-06-19 发布　　2008-11-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

网络安全等级保护移动安全的要点

- 无线安全接入安全

无线网络安全防护方面部分要求针对无线网络安全接入与安全传输的问题，在标准中提出了对无线网络设备安全接入、入侵防范、通信传输等方面的安全要求。例如：应能够检测、记录、定位非授权无线接入设备；应能够检测到无线接入设备的SSID广播、WPS等高风险功能的开启状态；在无线通信传输中对敏感字段或整个报文进行加密。



网络安全等级保护移动安全的要点

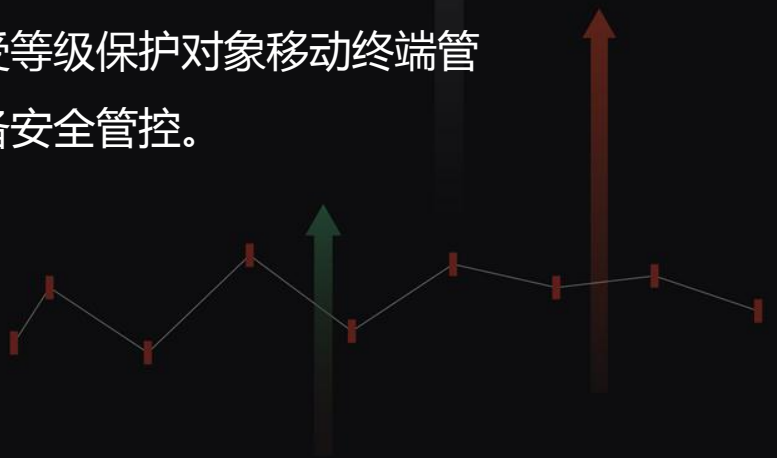
- 移动APP安全防护

移动应用安全防护方面部分要求针对移动应用app存在的被篡改、被假冒的问题，标准要求采用校验技术保证代码的完整性同时，应保证等级保护对象业务移动应用软件开发后、上线前经专业测评机构安全检测等。针对移动应用app发布的问题，在移动应用app发布渠道与管理中要求应保证移动终端安装、运行的应用软件来自可靠证书签名或可靠分发渠道。

网络安全等级保护移动安全的要点

- 移动终端安全防护

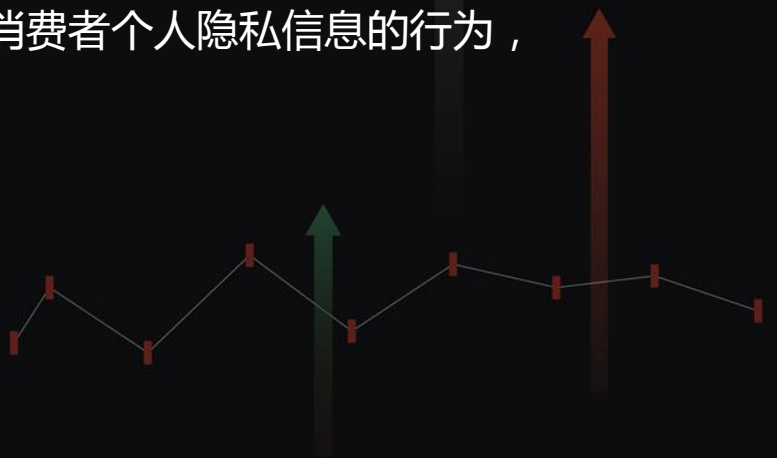
移动终端安全防护方面部分要求针对移动终端的安全，标准主要对移动终端的安全环境、应用安装管控、终端自身安全进行了要求，例如：应将移动终端处理访问不同等级保护对象的进行应用级隔离；应具有软件白名单功能，应能根据白名单控制应用软件安装、运行；移动终端应接受等级保护对象移动终端管理服务端的设备生命周期管理、设备远程控制、设备安全管控。



网络安全等级保护移动安全的要点

- 移动APP个人信息安全保护

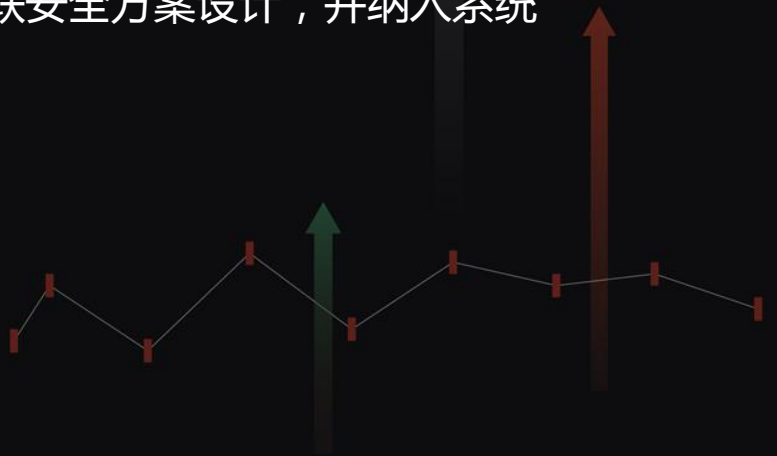
各行业主管部门依托第三方检测机构开展本行业内的移动App个人信息安全检查，对各行业移动App个人信息保护水平进行摸底，建立个人信息安全检查长效机制，定期对本行业内移动App进行抽查；严厉惩处中各类违法违规行为，公安部门开展打击个人信息贩卖的黑色产业链行动，对于侵犯消费者个人隐私信息的行为，形成常态化监管机制。



网络安全等级保护移动安全的要点

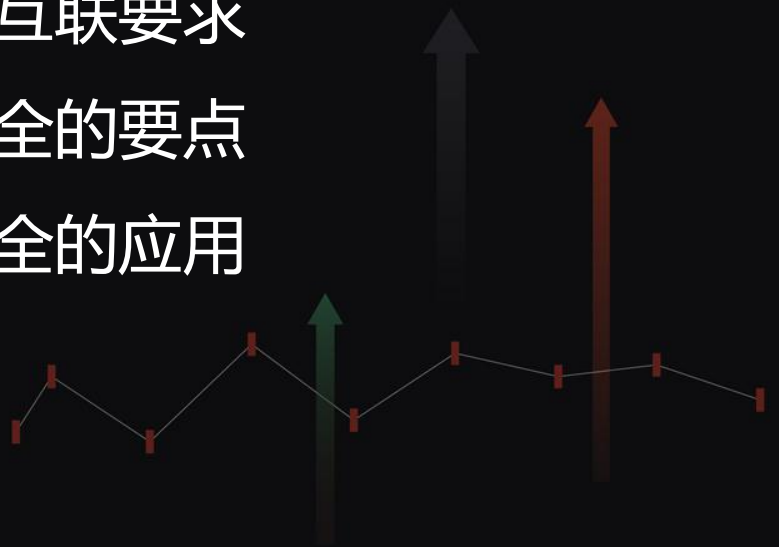
- 移动互联安全管理要求

移动互联安全管理方面部分要求在安全管理方面，标准要求建立移动互联安全管理制度，对移动终端实施安全控制和管理。设置移动互联安全管理员，明确管理职责。加强终端设备管理，在移动终端设备丢失后进行远程数据擦除。在系统建设前要求根据信息系统的安全保护等级进行移动互联安全方案设计，并纳入系统总体方案设计。



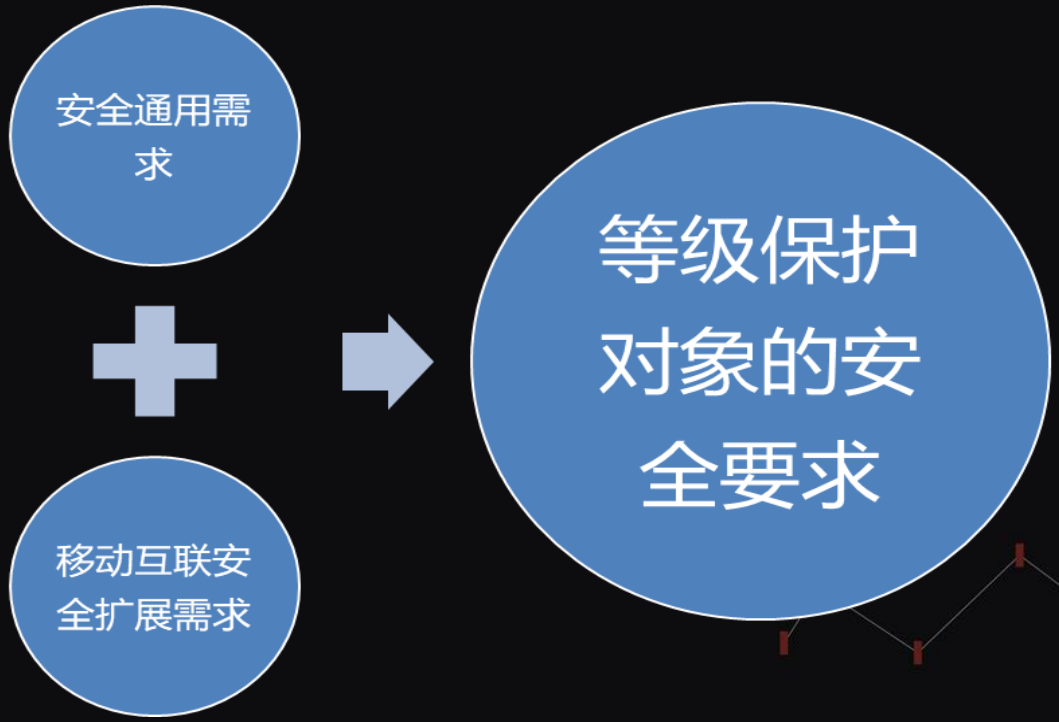
目录

- 移动应用程序面临的安全风险
- 网络安全等级保护的移动互联要求
- 网络安全等级保护移动安全的要点
- ✓ 网络安全等级保护移动安全的应用
- 爱加密公司



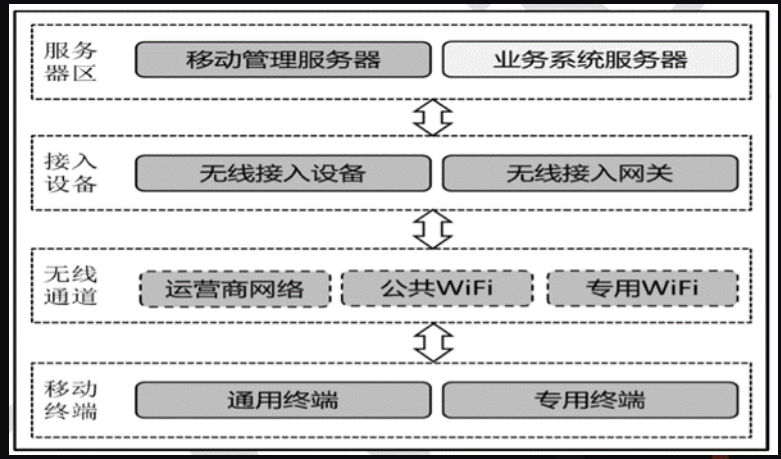
网络安全等级保护移动安全的应用

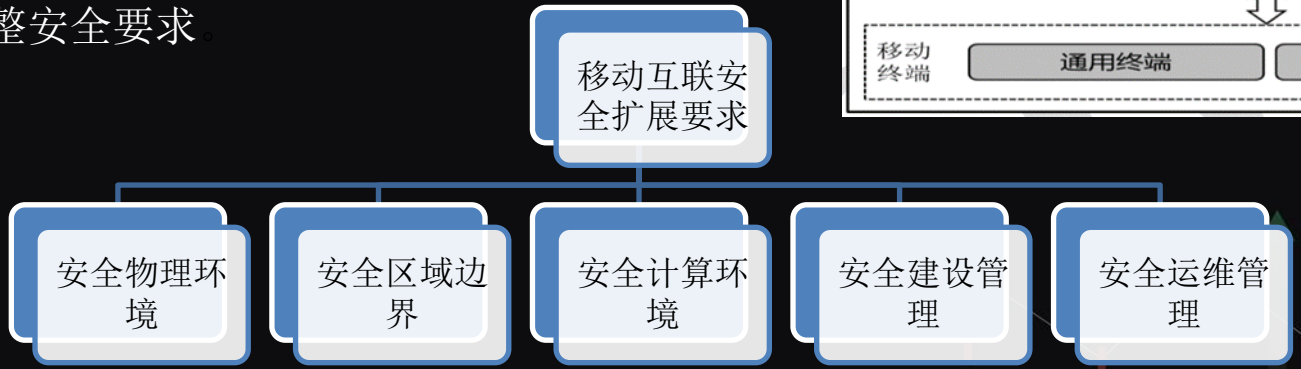
- 安全要求组成



网络安全等级保护移动安全的应用（三级）

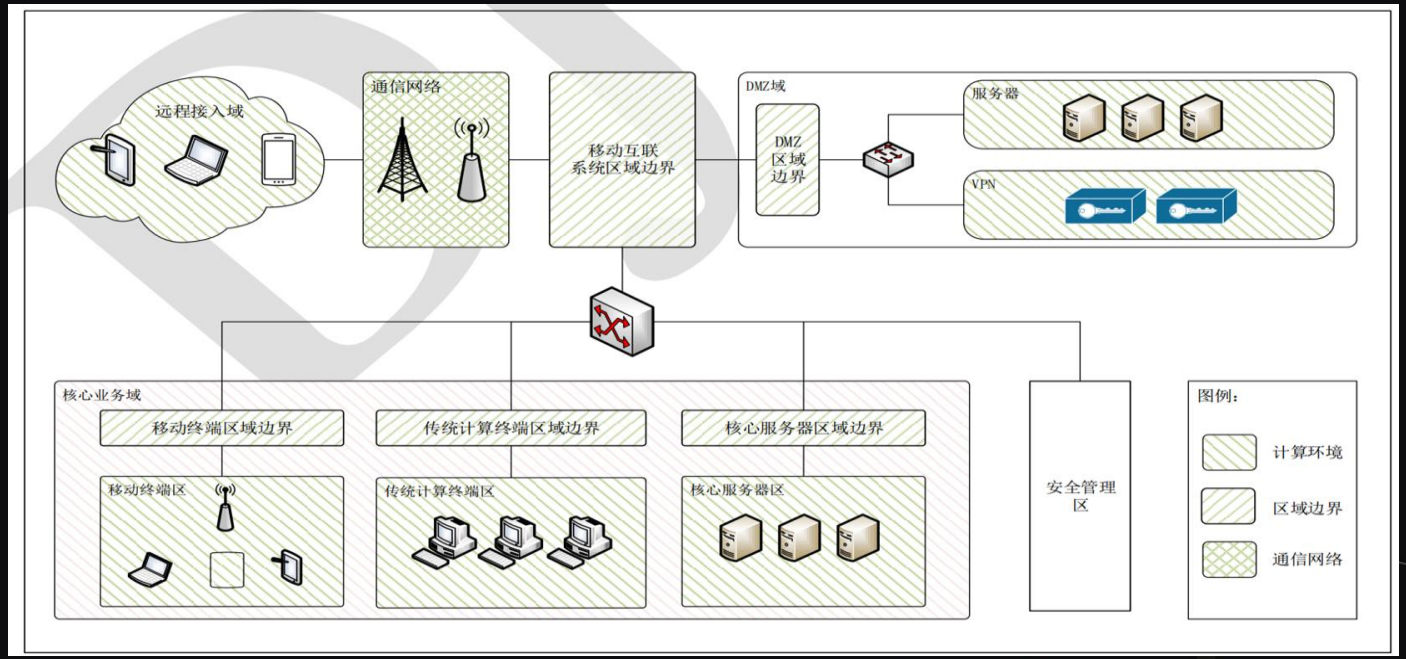
本标准的移动互联安全扩展要求主要针对移动终端、移动应用和无线网络部分提出特殊安全要求，与安全通用要求一起构成对采用移动互联技术的等级保护对象的完整安全要求。





网络安全等级保护移动安全的应用

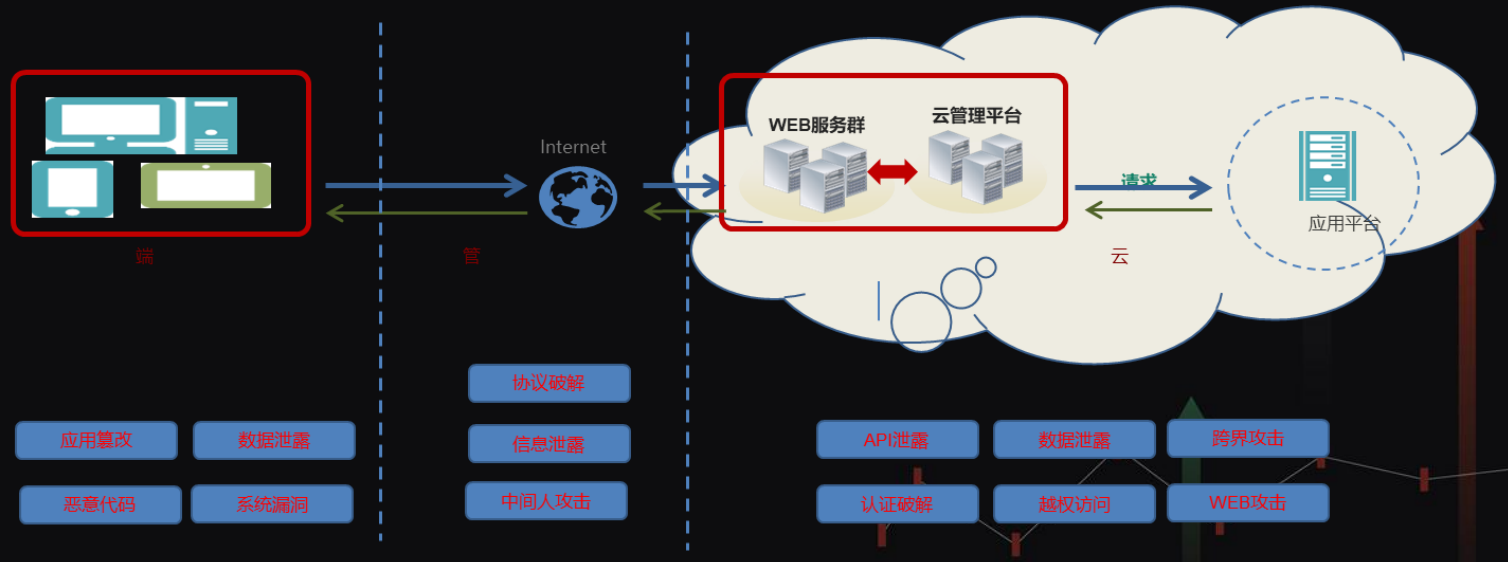
- 移动应用安全框架



网络安全等级保护移动安全的应用

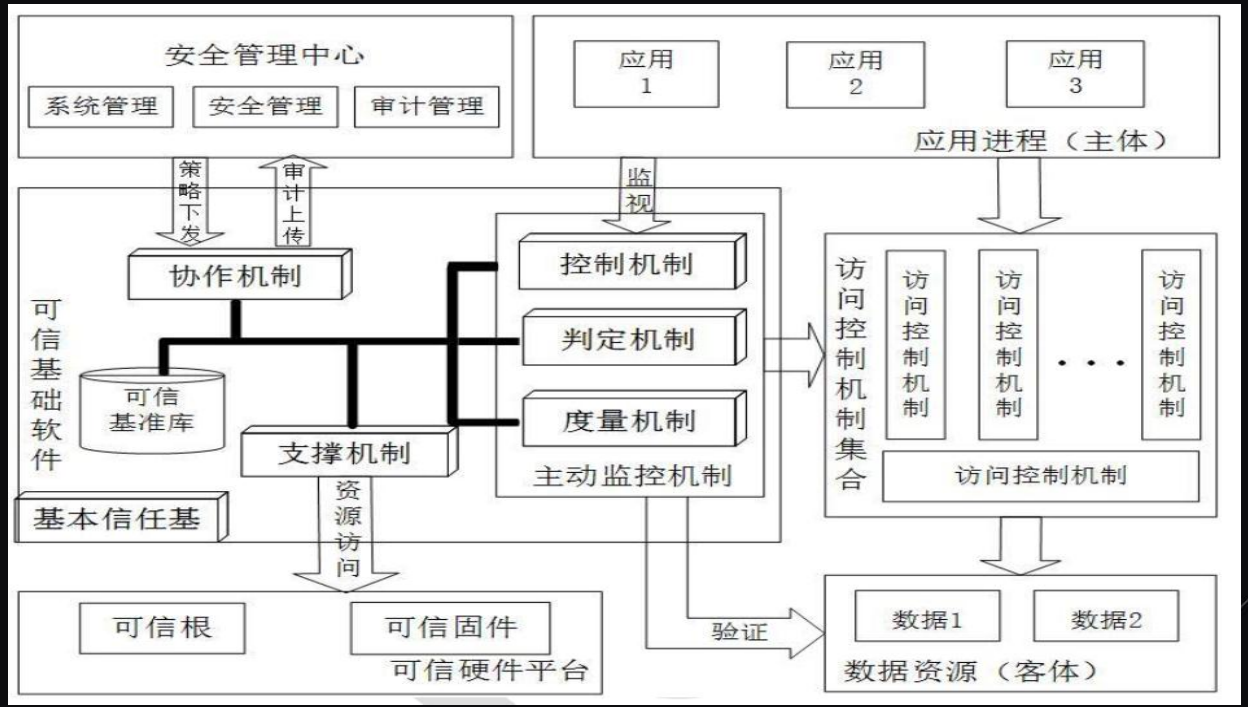
- 基于“云”、“管”、“端”架构，移动互联网核心保护对象及安全威胁。

基于“云”、“管”、“端”架构，移动互联网核心保护对象及安全威胁。



网络安全等级保护移动安全的应用

- 移动安全可信计算的应用



- 统一工具配置
- 统一时间管理
- 统一应用监视
- 统一信任管理

网络安全等级保护移动安全的应用

- 移动安全完整性与加密需求设计

应用防逆向

数据防篡改

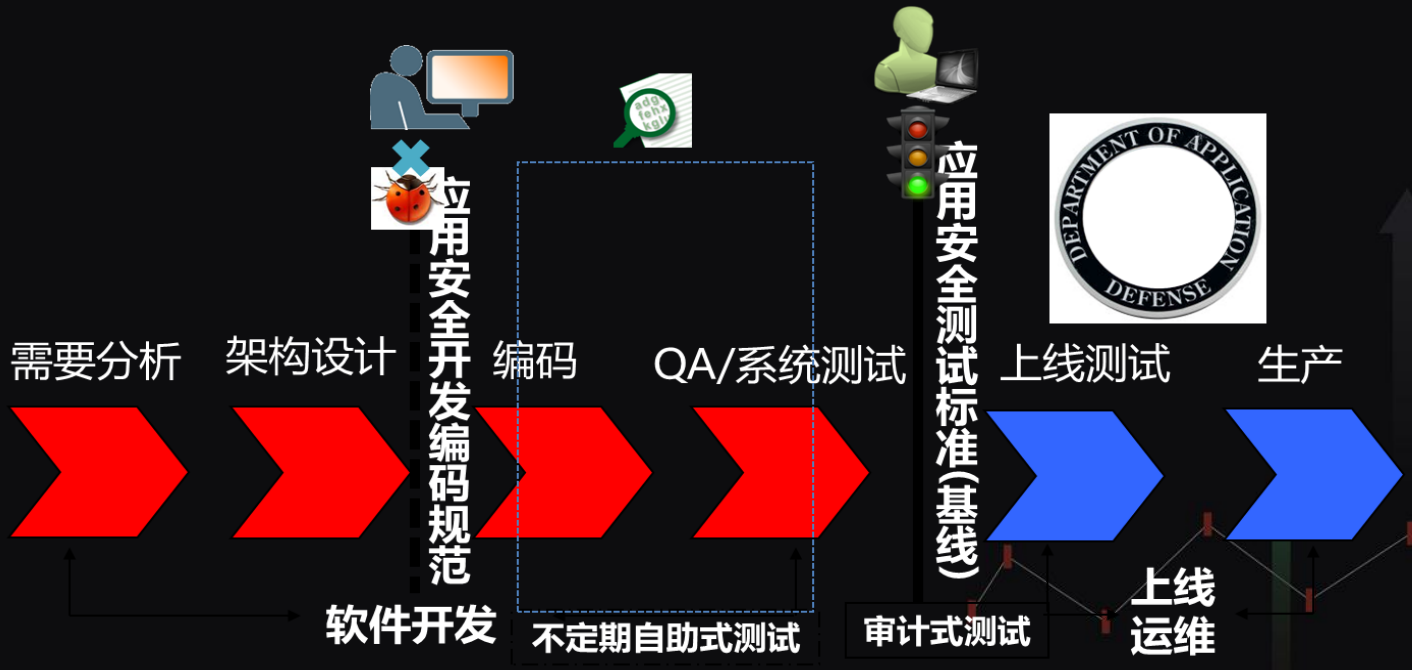
运行防调试

数据防泄漏

页面防劫持

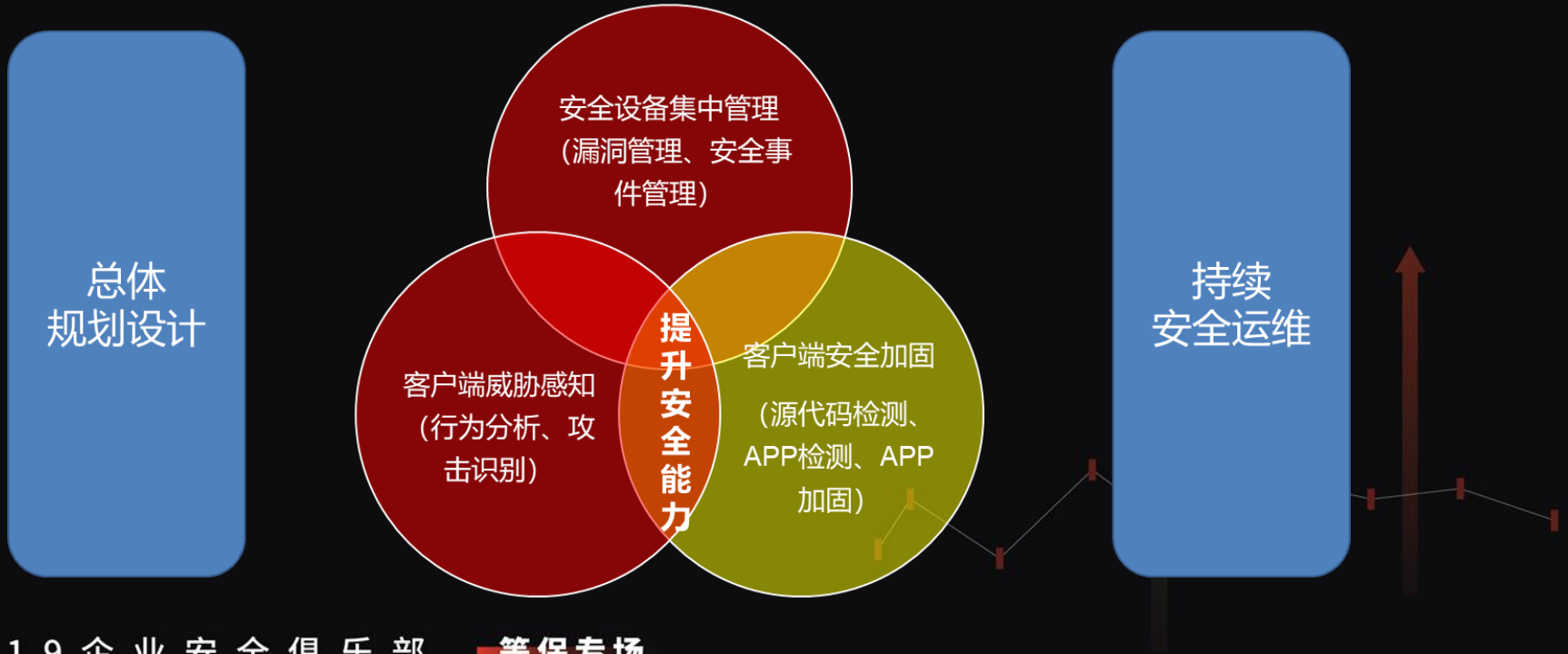
网络安全等级保护移动安全的应用

- 移动安全软件开发安全需求设计



网络安全等级保护移动安全的应用

- 移动安全总体设计

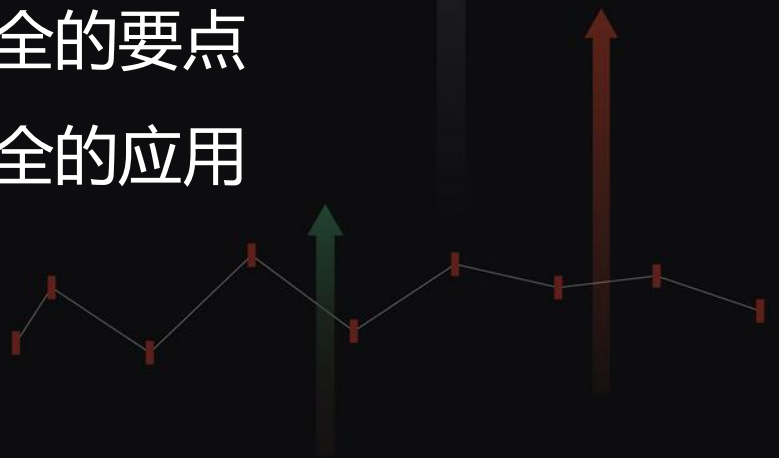


网络安全等级保护移动安全的应用

➢ 移动安全阶段规划

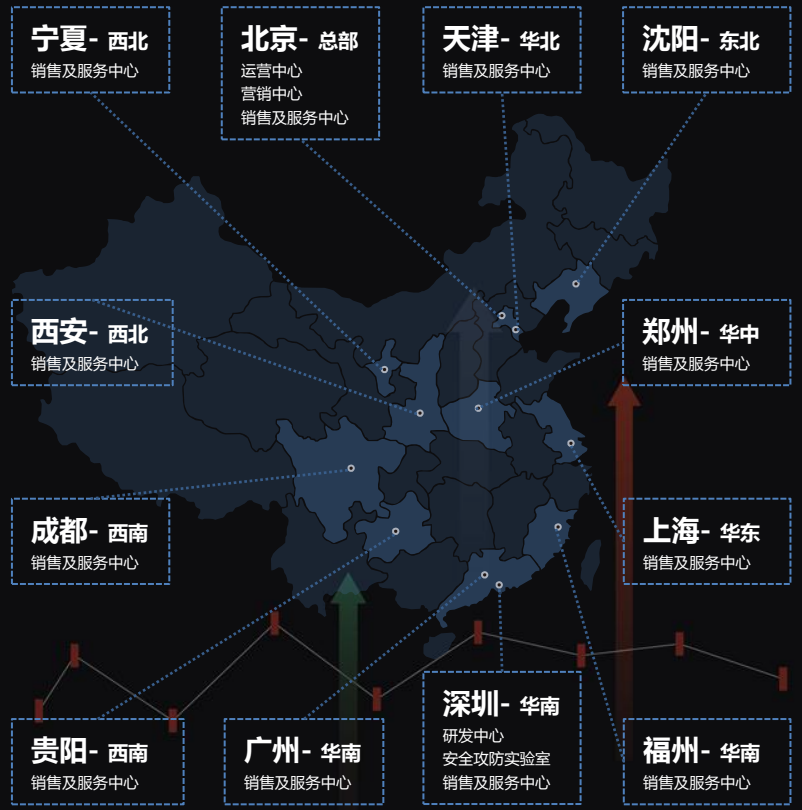
目录

- 移动应用程序面临的安全风险
- 网络安全等级保护的移动互联扩展要求解读
- 网络安全等级保护移动安全的要点
- 网络安全等级保护移动安全的应用
- ✓ 爱加密公司



关于爱加密 www.ijiami.cn

爱加密是国内知名的移动信息安全综合服务提供商，拥有安全检测、安全加固、安全感知与安全运营四大产品体系，是为移动应用提供全生命周期安全服务的移动信息安全品牌。爱加密至今共服务移动应用100万+，监控互联网应用1500万+，服务行业客户覆盖政府、运营商、金融、游戏、教育等多个行业。



行业用户服务 2000+

市场保护APP 100万+

网络监控APP 1500万+

智能终端设备 10亿+

2019企业安全俱乐部 等保专场

智能安全加固的提出者和定义者——首创“自加固”技术，业内定义了智能加固的概念

07 第七代智能自加固

06 第六代双重VMP

05 第五代Dex VMP

04 第四代混合加密

03 第三代Dex源码分离

02 第二代Dex加壳

01 第一代源码混淆

- iOS全量测试服务（100+）
- Android全量测试服务（200+）
- web应用全量测试服务（100+）
- 微信公众号全量测试服务（50+）
- SDK合规测评服务（50+）
- 国家、行业合规测评服务（182+）

企业荣誉--行业权威

- 网络信息安全漏洞库（CNNVD）优秀技术支撑单位
- 全国信息安全标准化技术委员会会员
- SHCERT网络安全应急服务支撑单位
- 上海市公共互联网网络安全工作先进集体
- 绿色安卓联盟“最佳贡献企业”
- 胡润百富中国最具投资价值新星百强榜北京50强
- “物联之星”最具影响力物联网安全企业奖
- 中国网络安全企业50强
- 金融科技优秀解决方案创新奖——移动威胁态势感知平台
- 中国通信标准化协会全权会员单位
- 中国移动应用安全领域自主创新品牌10强
- 移动应用安全联盟成员单位
- 互联网金融支付安全联盟成员单位
- 中国反网络病毒联盟（ANVA）成员单位

2019企业安全俱乐部 —等保专场

企业资质

www.ijiami.cn

- CESSCN通信网络安全服务风险评估1级（行业独有）
- 中国信息安全测评中心EAL3级别认证（行业独有）
- 通过公安一所研究所信息安全等级保护评测
- CCRC一级风险评估资质
- CMMI 三级认证软件开发企业
- “双软”认证（软件产品、软件企业）
- 通过中国软件评测中心的软件产品功能测试
- 中国反网络病毒联盟（ANVA）成员单位
- OWASP《移动应用安全检测基准》发起单位
- 通过ISO9001质量管理体系认证
- 通过ISO20000信息技术服务管理体系认证
- 通过ISO27001信息安全管理体系认证
- 通过AAA级企业信用等级证书
- 北京高新技术企业
- 软件著作权（51个）
- 应用安全联盟成员单位
- 互联网金融支付安全联盟成员单位
- 中关村网络安全与信息化产业联盟成员
- 2014中国信息安全最具影响力企业
- 2014年度中国移动应用安全领域领军企业奖
- 中国移动应用安全领域自主创新品牌10强
- 中国人保承保（产品责任险、职业责任险）

2019企业安全俱乐部 等保专场

政府支撑单位

www.ijiami.cn

中共中央网络安全和信息化委员会办公室
Office of the Central Cyberspace Affairs Commission

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

CNCERT/CC
国家互联网应急中心

CAICT
中国信息通信研究院
China Academy of Information and Communications Technology

中华人民共和国公安部
The Ministry of Public Security of the People's Republic of China

参与制定了网信办、工信部、公安部等监管单位的移动应用、移动支付安全规范并与国家互联网应急中心、中国信息安全测评中心等多个行业监管单位深度合作与服务支撑

序号	支撑单位	服务内容
1	中国信息安全测评中心	安卓漏洞挖掘
2	国家病毒中心	移动端安卓病毒情况/app的VPN情况
3	国家互联网应急中心	移动Android APP原创漏洞
4	国家互联网反病毒联盟	移动端安卓病毒情况
5	深圳网监	每周提供一定数量的APP的高危漏洞信息
6	株洲市网络与信息安全通报中心	APP恶意行为分析

序号	支撑单位	标准名称
1	工信部国家应急响应中心	移动互联网应用程序安全加固能力评估要求与测试方法
2	中国信息通信研究院标准所	移动信息化可信选型认证评估
3	公安部第三研究所	移动安全保护产品检测条件
4	公安部第三研究所	移动应用安全检测产品安全技术要求
5	广东省地方标准委员会	移动互联网应用服务安全检测要求
6	公安部第三研究所	信息安全技术SDK安全技术要求
7	广东省网络空间安全协会	物联网安全技术要求
8	电信一所	新型城域物联专网建设标准
9	浙江电检所	移动应用安全标准
10	中国通信标准化协会	移动互联网应用程序安全加固系统评估标准
11	中国通信标准化协会	移动互联网应用程序安全加固能力评估要求与测试方法
12	长城网互联网中心	移动应用安全检测标准与检测方法

爱加密公司

公司优势

- 垂直领域的技术与市场领先者
- 全面的权威资质认证
- 遍布全国的分公司与办事处
- 所有产品均为自主研发，拥有核心代码及知识产权
- 与网信办、工信部、公安、CnCert、计算机病毒防治中心等深入合作

技术优势

- 领先的双重VMP加固核心技术
- 创新的iOS加固技术
- 纯净防护，不侵入源代码
- 全面的Android、iOS、H5和物联网嵌入式系统覆盖
- 高性能、不影响兼容性
- 众多核心技术及软著、专利

人员优势

- 70%的专业技术人员
- 风险评估相关技术人员超过40人
- 众多CISSP/CISA/CISP/PMP/CISAW等专业安全资质认证

方案优势

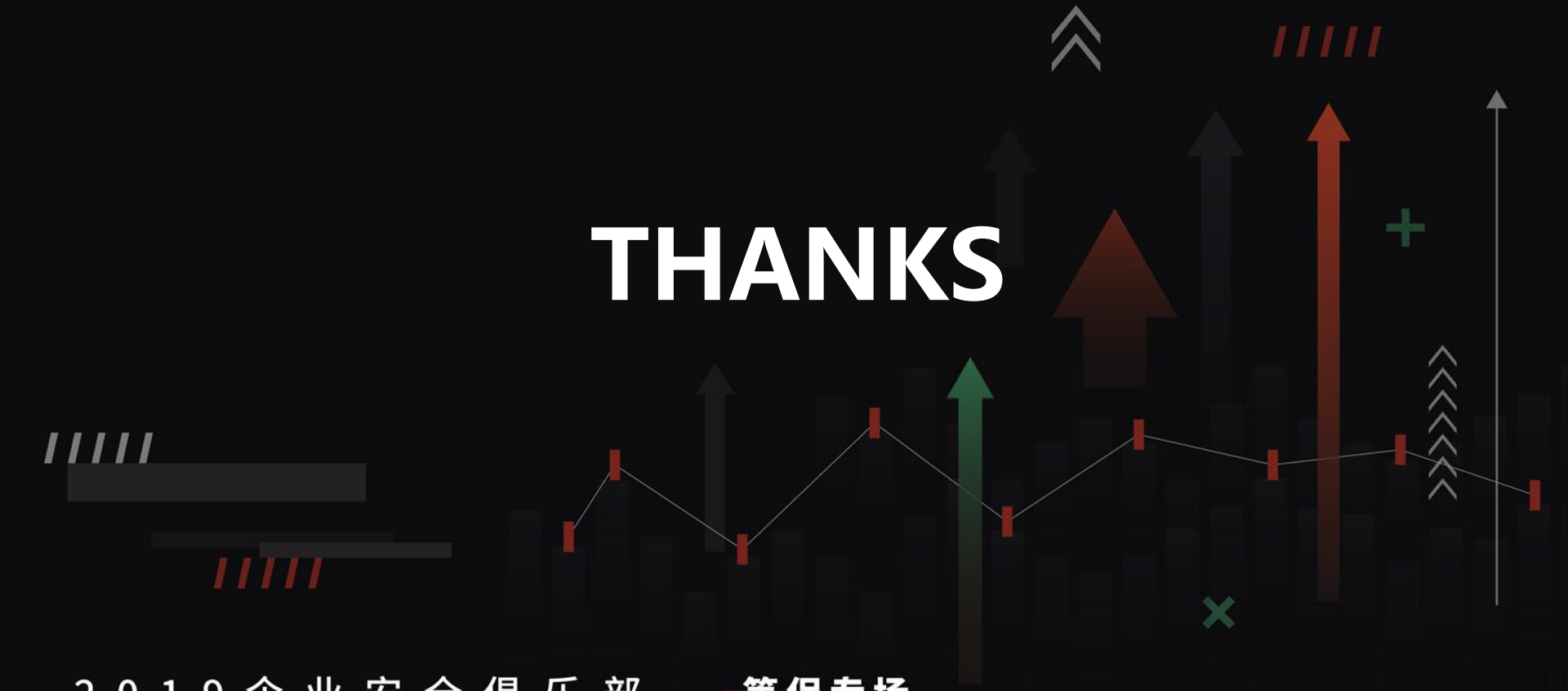
- 移动安全全生命周期解决方案
- 物联网解决方案
- 安全态势感知解决方案
- 安全大数据解决方案
- 业务风险治理解决方案
- 围绕国家网络安全法和等保2.0的方案设计思想

经验优势

- 超过2000+的行业标杆客户
- 专业的服务和响应团队
- 专业的评估服务流程


各类银行
交通银行 BANK OF COMMUNICATIONS
中国银行 BANK OF CHINA
恒丰银行 EVERGROWING BANK
浦发银行 SPD BANK
兴业银行 INDUSTRIAL BANK CO.,LTD.
广发银行 CGB
平安银行 PING AN BANK
中国民生银行 CHINA MINSHENG BANK
中国邮政储蓄银行 POSTAL SAVINGS BANK OF CHINA
农信银资金清算中心 RURAL CREDIT BANKS FUNDS CLEARING CENTER
河北银行 BANK OF HEBEI
乌鲁木齐银行 BANK OF URUMQI
bsb 包商银行
华潤銀行
浙商银行 CHINA ZHESHANG BANK
证券保险等
交银施罗德 BOCOM Schroders
华泰证券 HUATAI SECURITIES
平安证券 PING AN SECURITIES
光大证券 EVERBRIGHT SECURITIES
华创证券 HuaChuang Securities
爱建证券
光大保德信基金管理有限公司 Everbright Pramerica
西部证券
汇付天下 金融支付专家
中国银联 China UnionPay
国金基金 GFUND
富国基金 Fullgoal Fund
泰康人寿 TAIKANGLIFE
翼支付
互联网金融
宜人贷
立业贷 www.liyedai.cn
搜易贷 搜狐集团旗下公司
LU.com 陆金所
前海航交所
理财咖 www.lcaika.com
金条子
天虹
在线贷 www.zxd.com
UA融易贷
地标金融 DIB FINANCE
闲钱宝 51XQB.COM
微财富
大麦理财 damailicai.com
财富中国 FINANCE OF CHINA
龙贷
大型政企
掌上电力
国家电网公司 STATE GRID
中国移动 China Mobile
和
电宝
中国体彩网 www.lottery.gov.cn
EXPRESS 顺丰速运
厦门航空
CNPC 中国石油
HUAWEI
美的 Midea

FREEBUF | 企业安全 俱乐部



2019企业安全俱乐部 等保专场