2017年度移动APP安全漏洞与数据泄露现状报告



出品方:FreeBuf研究院

关于FreeBuf研究院

FreeBuf.COM是斗象科技旗下、国内领先的互联网安全新媒体，每日发布最专业的安全资讯、技术剖析，分享国内外最新安全资源，是最受安全从业者与爱好者关注的网络安全网站与社区。FreeBuf研究院则集结了行业内经验丰富的安全专家和分析师，常年对信息安全技术、行业动态保持追踪，呈现最专业的安全行业现状和趋势分析。

关于启明星辰

启明星辰信息技术有限公司成立于1996年，由留美博士严望佳女士创建，是一家拥有自主知识产权的网络安全高科技企业。作为与国际接轨、勇于创新的先行者，启明星辰公司致力于提供具有国际竞争力的自主创新的安全产品和最佳实践服务，帮助客户全面提升其IT基础设施的安全性和生产效能。

指导单位

中国泰尔实验室

数据及内容支持

漏洞盒子

启明星辰

中国泰尔实验室

中国信息通信研究院安全研究所

目录

第一章 概述 1

1.1 背景 1

1.2 Key Findings 2

第二章 移动App信息泄露与安全漏洞现状 3

2.1 移动App高速发展现状 3

2.2 用户眼中的移动App安全现状 4

2.3 移动App安全漏洞与信息泄露的现状与危害 6

第三章 导致移动App数据泄露的形式与成因追溯 12

3.1 移动App信息泄露的形式 12

3.2 案例列举 14

3.3 移动端内存敏感数据泄露 18

3.4 移动App安全漏洞及信息泄露成因 20

第四章 解决方法与安全建议 25

4.1 移动App开发安全建议 25

4.2 合规本身是一种投资 27

附录 28

第一部分 概述

1.1 背景

近10年来，移动设备在消费领域乃至此后企业领域的扩展，从速度和数量来看都是相当惊人的。早在2014年，ANDREESSEN HOROWITZ分析师Benedict Evans就说：“移动正在啃噬这个世界（Mobile is Eating the World）。”[1]这从来就不是夸张，全球范围内移动设备的数量早就在多年前超越了世界人口总和。从2007年苹果推出初代iPhone革新智能手机至今短短10年，移动行业的市场规模都在急速增长。

Statista的数据显示，2016年全球范围内智能手机的出货量约在15亿台左右，预计到2020年这个数字会增加到17.1亿；到2018年，全球手机用户总数将达到25.3亿人次——其中1/4都来自中国。仅2016年中国智能手机市场规模都已经超过1336亿美元。[2]

我们在《2017金融行业应用安全态势报告》中提到，无论是移动设备数量的爆发式增长、移动市场规模的扩大，还是移动技术的发展令互联网流量激增，都急剧增大了信息安全的攻击面——攻击者有了更多的突破口针对个人和企业组织实施入侵。[3]

与许多技术由上至下，从企业到消费市场的发展方式不同，移动技术始于消费用户领域。这就一定程度意味着移动设备和软件前期对于安全的不重视，安全在移动领域的起步相较桌面和其他传统领域也明显更晚。仅从操作系统层面来看，去年CVE Details报告显示，Android系统全年记录在册的漏洞数量达到523个，成为CVE排行榜上名副其实的漏洞之王[4]。而移动安全又是个不仅相关于系统和漏洞，多方面、多层级的问题，就应用层即面临配置、网络传输、第三方App等安全问题。

FreeBuf研究院在中国泰尔实验室的指导下，辅以漏洞盒子、启明星辰和中国信息通信研究院安全研究所的数据与内容支持，从第三方移动App安全及信息泄露的角度共同撰写了这份报告。在数据研究和分析过程中，我们选择了金融、购物、医疗、社交、游戏、娱乐、交通与出行、生活服务等八个分类的892款Android平台的流行App作为样本，借由启明星辰的应用自动化安全测试平台，来发现移动App存在安全风险与漏洞。与此同时，我们以企业组织的移动App开发者、项目管理人员和安全专家为对象，下发近200份问卷，尝试解读造成移动App安全漏洞和问题的根源；企业对象涵盖大中小不同规模；另外也针对移动App普通用户下发近300份问卷，了解应用安全在普通用户中的需求和位置。

这份报告旨在从移动App安全漏洞和数据泄露的角度来窥见移动App的安全现状，以及移动领域的开发者和安全专家在App安全开发方面的不足，并期望以此帮助开发者和安全专家，以及项目管理人员在进行相关App安全决策时给出参考和指引。

值得一提的是，虽然这份报告并不专注于企业级App的安全问题可能对企业安全造成的危害，而更多将注意力集中在消费类移动App的漏洞、数据泄露、仿冒等安全风险的层面，但BYOD工作方式也能够让这类移动App对企业安全造成影响；且报告对于企业级App开发亦有一定的参考价值。

在《中华人民共和国网络安全法》于6月1日起开始施行的当下，相关移动App开发与安全的企业组织有义务“防止网络数据泄露或被窃取、篡改”。解决报告即将阐述的App漏洞和安全问题已经不只是企业组织和开发者应该做的，而是必须做到的。

因此无论从安全问题造成的用户和企业直接损失，挽救企业信誉的角度，还是按照相应规范进行App开发、遵守《网络安全法》的角度来看，移动App漏洞、数据泄露和其他安全问题都应该成为企业组织、开发者和安全专家重视的问题。

1.2 Key Findings

- 过往10年移动App在数量和规模上的爆发，为攻防双方开辟了新战场；
- 移动App更出色的安全性可以成为吸引和留住用户的差异化竞争要素；
- 用户对于移动App安全普遍更为乐观，而开发者则恰好相反；
- 65%接受测试的移动App至少存在1个高危漏洞，平均每个App就有7.32个漏洞；
- 娱乐类移动App成安全漏洞重灾区，每10个娱乐类移动App就有9个至少包含一个高危漏洞；
- 社交类App被仿冒的几率相较其它类别平均高出10倍以上，仅社交类App被仿冒占比达到测试中所有仿冒移动App的近六成；
- 多达88%的金融类App都存在内存敏感数据泄露问题；
- 移动App安全问题的主要原因在于开发和安全的分化：69%的开发者认为安全是其他人的工作；
- 在开发者看来，强制合规仍是移动App安全的最大驱动力，这或为造成当前移动App安全问题的一大原因。

第二部分 移动App信息泄露与安全漏洞现状

2.1 移动App高速发展现状

如背景部分所述，移动技术的发展主要是由消费市场反哺企业市场，并在企业组织间发展铺陈的。消费用户对于安全级别的要求更低，决定了移动技术在大规模应用于企业市场前期是存在大量风险的。如果不谈消费用户可能遭遇的信息泄露与各种损失，从受访者反馈的数据来看，即便是从事App开发的这些企业组织，89%都允许员工将个人移动设备带到企业中，即时下流行的BYOD办公方式（Bring Your Own Device），以期提升办公效率和生产力。

企业组织在这种场景下很难限制员工个人移动设备及移动App的使用。这些App可能来自不受信任的源，而员工个人移动设备又需要连接和处理敏感数据。

另外，如果企业期望随时能够联系客户，并增加业务机会，移动技术的应用也就成为了必要选择。这些是移动技术和App带来的更多可能性，但也正因如此，企业组织需要为此承担更多的责任。然而企业级App本身的安全性也并不比普通App更好[5]，所以移动App的安全问题现如今早已不仅是普通消费用户需要担心的问题，更是企业应该重视的问题。

> “过去10年移动App的爆发，为攻防双方开辟了新战场。”

我们在对待移动平台及App的安全威胁时，又无法照搬传统桌面平台的经验，一方面在于移动设备感染恶意程序的几率在其遭遇攻击威胁中的占比近些年虽然在逐步增多，但相较其它安全威胁类型占比并不大，这原本是桌面平台面临的主要威胁；而根源在于移动设备暴露于更广范围的风险之下——因为移动设备的本质是“移动”，它需要穿梭于各种网络环境，遭遇攻击的可能相当多样。

另一方面就在于海量的移动App：越来越多的应用发布到应用商店中，越来越多的应用被用户下载。

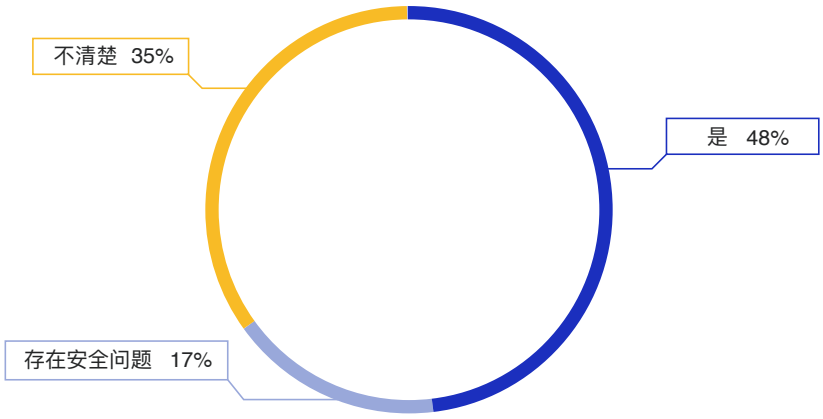
Statista最新数据显示，Google Play应用商店1月份的应用数量达到了280万款，苹果App Store应用商店应用数量则为220万——9年前这个数字是800款；苹果预计到去年9月，App Store中App下载累计次数达到1400亿次。而移动用户平常87%的时间都是花在移动App之上。[6]

这份数据从移动安全的角度来说，表征的是移动平台的攻击面变得越来越大，风险也越来越大。过去10年移动App的爆发，甚至可以说为攻防双方开辟了一个全新的战场。这场战争的最重要参与者，即开发者，在安全问题上又是严重滞后的。这也是这份报告专注于移动App安全漏洞及数据泄露的原因。

2.2 用户眼中的移动App安全现状

在“新战场”为攻防双方开辟如此之久的当下，普通消费用户与企业用户眼中的移动App安全现状似乎仍旧相当“乐观”。这是FreeBuf研究院针对移动App发放近300份问卷后获得的统计结果。

在用户看来，自己所用的移动App是安全的吗?



近一半（48%）的受访用户认为自己所用的移动App是安全的——在我们的随机采访中，不少受访者表示自己只从Android和iOS官方应用市场下载移动App，所以手机中的App是安全的；仅有17%的受访者认为自己使用的移动App存在安全漏洞；其余用户则表示不清楚移动App安全情况如何。

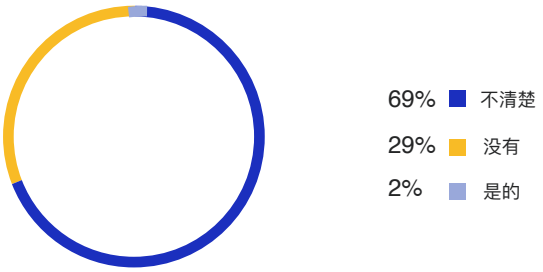
用户对安全问题普遍较乐观

在本次针对移动App用户的调查中，我们还发现一个有趣的问题。企业App用户相比普通App用户，对App安全的担忧明显更甚，尤其是从事App开发的开发者和项目管理人员。这群人对于移动App安全也普遍更没有信心，这个问题并不是没来由的。有关这一点，我们还将在3.2章节中进行更为详细的阐述。

实际上从后续章节针对App安全漏洞的追踪也不难发现，用户对于移动App的安全问题的确过于乐观，或者他们并不清楚移动App到底存在怎样的安全隐患；且这份报告测试的所有移动App都来自官方应用商店或手机制造商出厂搭载的应用商店，却依旧充斥着各种安全漏洞。但有趣的是，安全在普通用户眼中也的确成为使用一款移动App的考虑因素，即便可能并非首要因素。

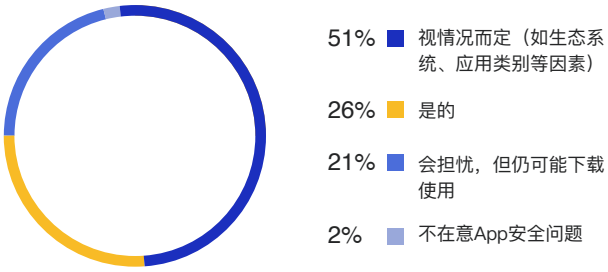
移动App用户依旧在意安全问题

你是否经历过因移动App安全漏洞而导致的个人信息泄露或其他安全威胁



虽然绝大部分用户（29%）都没有经历过，或者并不清楚（69%）自己是否因移动App安全漏洞而导致个人信息泄露，但后面这七成用户在信息泄露的问题上是存在担忧的。而且这些受访者中，明确表示在下载使用一款移动App之前，不在意安全问题的比率仅有不到2%；26%的用户则认为，在明确或怀疑一款App存在安全隐患的情况下，就会放弃下载使用；超5成受访者（51%）表示需要视情况而定，但金融类、医疗健康这些数据十分敏感的应用必须要首先考虑安全问题；其余21%的用户虽然对安全问题有担忧，但仍然倾向于下载使用所需的应用。

若明确或怀疑一款App存在安全问题，你是否考虑弃用该App?



这对移动App开发者而言显然是需要明确的问题：即用户的确在意移动App安全性。不止于此，Arxan去年《第5次应用安全年度现状安全报告》的统计结果显示，82%的用户表示若已知正在使用的App存在安全缺陷，且有更为安全的App可替代，他们会改投其他App门下[7]。从FreeBuf研究院的调研结果来看，国内的情况或更为复杂，26%的受访者表示如果的确知道使用的App存在高危安全风险，则会更换其他同类应用；仅有2%的受访者表示不在意App安全问题，但更多的人（51%）认为需要看情况，尤其是如果对某些App存在重度依赖，或对其生态系统存在依赖，则很难更换。

> 移动App更为出色的安全性可以成为吸引和留住用户的差异化竞争因素

不过这也提醒了移动App开发者和企业组织，移动App更为出色的安全性可以成为吸引和留住用户的差异化竞争要素。我们认为，随着当代攻击方的越来越强悍，这种竞争优势未来可能会表现地愈加突出，直到所有的开发者都明确了解到安全为其业务带来的好处。这种趋势意味着，安全融入到开发和业务环节中或许也只是时间问题。

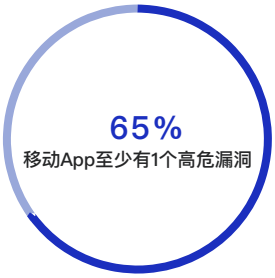
2.3 移动App安全漏洞与信息泄露的现状与危害

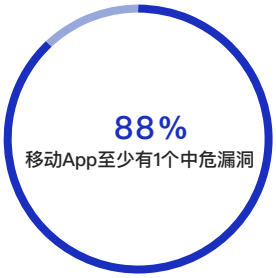
移动App用户对于安全有如此乐观的态度，而从我们的移动App测试来看，现实就比较骨感了。这份报告以金融、购物、社交、游戏、娱乐、医疗健康、生活服务、交通与出行几大分类的892款流行Android移动App为样本，借由启明星辰的移动应用自动化安全检测平台进行扫描检测。

启明星辰移动应用自动化安全检测平台通过对892个样本App进行逆向分析静态检测，以及动态检测，做到移动App更为全面、深度的安全扫描。整个过程还将模拟交互检测，自动化渗透检测，服务器指纹探测等多种检测方式相结合，以期发现移动App存在的各类潜在安全漏洞与风险。

一般来说，静态检测是通过代码反编译的方法还原App源代码，然后采用源码审计的方法对其进行检测。但在实际检测中，由于静态检测的环境限制，这种检测方式并不能覆盖漏洞验证。且静态检测发现的大多数漏洞，其利用条件较为苛刻，漏洞影响也不尽相同——这也是常见的移动App安全检测平台所用静态检测引擎的通用缺陷。因此本次测试还配合了动态检测：将移动App安装到定制化的虚拟运行环境中，从而模拟真实环境，对移动应用常见的脆弱点进行检测。我们期望通过这样的测试方法，尽可能做到报告呈现数据的针对性更强、测试参考价值更大。

> 用户很乐观，现实很骨感。从统计结果来看，65%的移动App至少存在1个高危漏洞；平均每1个App就有7.32个漏洞。







从针对Android平台移动App测试结果来看，65%的移动App至少有1个高危漏洞，88%至少有1个中危漏洞，96%至少有1个低危漏洞。如果不看漏洞严重程度与漏洞类型，则平均每1个App就有7.32个漏洞。且本次测试的漏洞仅涉及到移动App客户端本身，并不涉及服务器端（如认证/授权等）以及通讯与网络相关漏洞。

这些漏洞包含：

本地拒绝服务、应用反编译、外部存储设备信息泄露、硬编码敏感信息泄露、运行其它可执行程序、剪贴板信息泄露、Java层SSL中间人攻击、Android系统Sqlite数据库注入、动态加载DEX文件、PendingIntent包含隐式Intent信息泄露、WebView组件忽略SSL证书验证错误、WebView组件远程代码执行、WebView明文密码保存、Android APP allowBackup、Broadcast Receiver组件任意调用、Service组件任意调用、Activity公开组件、Content Provider组件任意调用、ZIP文件解压目录遍历、弱加密算法等漏洞。

在这些漏洞类型中，排名前10（测试App出现最多的漏洞）的分别是

1. Activity公开组件暴露
2. Broadcast Receiver组件调用漏洞
3. Service组件任意调用漏洞
4. 运行其它可执行程序漏洞
5. 应用反编译
6. 硬编码敏感信息泄露漏洞
7. 本地拒绝服务漏洞
8. 外部存储设备信息泄露漏洞
9. PendingIntent包含隐式Intent信息泄露漏洞
10. Android App allowBackup安全漏洞

值得一提的是，本次测试并没有针对iOS移动平台的移动App作测试。或许许多用户对于iOS都有其安全性明显优于Android的迷思，实际上如果仅从移动App生态来看，国外统计与评测机构的大量数据都表明，iOS平台移动App的安全性甚至还略差于Android平台。Arxan在《第5次应用安全年度现状安全报告》中明确提及：“虽然iOS操作系统通常被认为相比Android更安全，但在研究中，iOS App却比Android平台有着更多漏洞。[7]”我们的这份报告不再对此作更多说明。

2.3.1 移动App漏洞严重性评级

漏洞标准是关于漏洞命名、评级、检测、管理的一系列规则和规范，为信息安全测评和风险评估提供了基础。启明星辰在本次移动App安全测试中采用了CVE作为标识漏洞的统一标准。CVE是美国的MITRE公司开发的一个为公开的信息安全漏洞或者暴露进行命名的国际标准。在漏洞严重程度分级方面，报告也参考了OWASP相关内容标准。

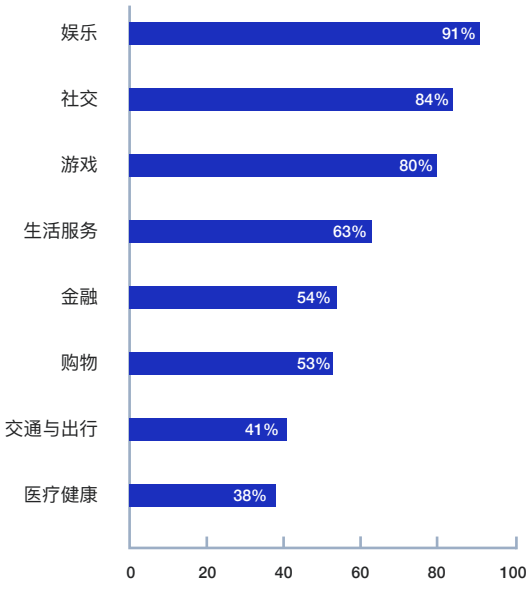
高危：此类安全漏洞存在较大安全风险，可被直接利用，能够直接或潜在造成系统破坏，或对数据完整性、机密性和/或可用性造成潜在威胁；考虑其利用的逻辑、复杂性，攻击发生可能性较大或一般。

中危：此类安全漏洞可对应用产生一定程度的影响和/或破坏，或无法被直接利用，但能够协助攻击者发动更多的攻击。

低危：并不构成直接的威胁，本身造成破坏性的概率较小，在与其它安全漏洞配合的情况下可发动更多的攻击。

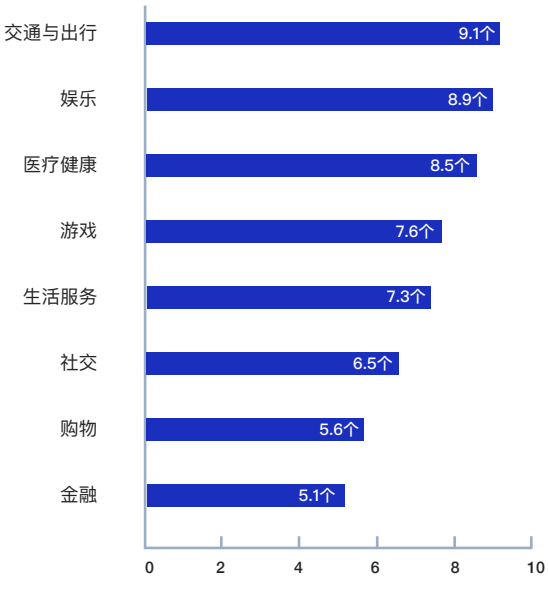
2.3.2 从App类别看安全漏洞危害

至少有1个高危漏洞的占比



本次测试选择了8个类别的应用，这8个类别分别是金融、购物、社交、游戏、娱乐、医疗健康、生活服务、交通与出行，是Android用户使用最为频繁或装机量最大的类别，也是日常接触最多以及安全漏洞可能波及范围最广的类别。从启明星辰的测试结果来看，社交、游戏和娱乐类移动App的安全漏洞数量最多，且高危漏洞占比最大，可能对用户造成的危害最严重。

平均一个App包含的漏洞数量



其中娱乐类移动App的近期版本中，至少有1个高危漏洞的App占比达到91%——也就是说每10个娱乐类App就有9个是含有至少1个高危漏洞的，相较本次测试App总量均值，高出了近三成的比例。我们统计的的娱乐类移动App包括音乐流媒体、视频流媒体、在线直播、VR类、搞笑类（如糗事百科）等类别。

高危漏洞举例如应用反编译缺陷，也就是指移动App的APK包容易被反编译为可读文件，稍加修改后就能打包成新的APK；破坏性还包括容易造成软件破解、内购破解、软件逻辑修改、插入恶意代码、替换广告商ID等。也就是说娱乐类移动App超过九成的比例都存在应用极易被反编译的高危安全风险。下面将提到的其它类别也如是。

再比如中危级别的安全漏洞中，几乎所有娱乐类App都包含硬编码敏感信息泄露漏洞，这类漏洞是指用户名、密码、密钥等敏感信息硬编码在程序中，逆向分析App可获取敏感信息。

> 每10个娱乐类移动APP就有9个至少包含一个高危漏洞

除了娱乐类App之外，游戏与社交类移动App也属于安全漏洞的重灾区。测试样本中，约84%的社交类移动App存在至少1个高危漏洞，80%的游戏App存在至少1个高危漏洞；这两个数据相比所有测试App均值也高出了近两成的比例。尤其在游戏类App中，敏感数据泄露的比例相较一般应用多出近3倍；社交类数据泄露比例相比均值多出超过4倍，用户名、密码和用户邮箱都是社交类App泄露的主要个人数据。

在数据泄露问题中，值得一提的是移动端内存攻击成为攻击者获取用户敏感数据的重要方式。所谓的内存敏感数据泄露，是指攻击者直接通过获取内存空间数据的方式，窃取、篡改、劫持程序的核心交互数据。这个问题在移动App数据泄露安全风险方面表现得尤为突出，针对该问题，后续还会有章节作详细解读。

从总的安全漏洞占比情况来看，金融和购物类移动App的表现最佳。就启明星辰测试的所有漏洞类别来看，部分App没有检测到漏洞，或者不存在高危漏洞以及中低危漏洞数量较少，这在其它类别中已经比较难得。这两个类别的安全性做得相对更好并不让人感觉意外，因为当涉及到金钱交易时，开发者总是需要更专注其安全性。

这里的金融类App包含银行、保险、证券、信贷、理财、支付等子分类，其中一部分的确都涉及到真金白银，以及用户隐私数据的交互。但即便如此，依旧有过半（54%）的金融类App存在至少1个高危漏洞，即便或许并不直接导致信息泄露，应用反编译这类问题依旧可以产生被社工的后果；购物类App的这一数值为53%，中低危漏洞占比相对更低——购物类App不仅包含O2O式综合线上购物平台，也包括某些厂商（如服饰、超市、数码、二手类买卖平台等）所推的官方App。这两个类别平均每个App的漏洞数量约为5–6个。

如果要单就高危漏洞占比情况来看，医疗健康类和交通出行类App中包含高危漏洞的比例是最低的：测试中，约38%的医疗健康类App，与41%的交通与出行类App包含至少1个高危漏洞。不过这两个类别的移动App单就敏感数据泄露方面的成绩并不出色，且中低危漏洞数量也不少。医疗健康类别中，平均一个移动App有8.5个漏洞；而交通与出行类App中，平均一个移动App就有9.1个漏洞。

比如某医疗健康类应用包含中危级别的剪贴板敏感信息泄露漏洞：对于非高权限的App而言，就可以通过剪贴板功能来获取密码管理器中的账户密码信息——Android剪贴板的内容是向任何权限的App开放的，很容易被嗅探泄密；该应用还存在动态加载DEX文件漏洞：App外部加载的DEX文件未作完整性校验，加载的DEX易被恶意应用劫持或进行代码注入，攻击者进而可执行恶意代码，进一步实施欺诈、获取帐号密码等恶意行为。

最后生活服务类App取样涵盖了快递、饮食、天气、招聘、租房、通信等领域，这个类别的移动App基本处于所有测试App安全漏洞数量及占比的平均水平，63%的生活服务类App至少包含一个高危漏洞。总的来说，无论是哪个类别的移动App，安全性表现都算不上出色，即便个别App的漏洞数量较少也无法表明整个大类的安全措施是到位的。

2.3.3 移动App仿冒之殇

本次测试的移动App高危漏洞中，有一项应用易遭遇反编译的问题：如果某个App存在该问题，则意味着移动App的APK包容易被反编译为可读文件，稍加修改后就能打包成新的APK；破坏性还包括容易造成软件破解、内购破解、软件逻辑修改、插入恶意代码、替换广告商ID等。

这个问题导致了大量仿冒应用的出现，这些仿冒应用可能对开发者造成恶劣的影响，如大量游戏App被某些不法渠道替换广告商ID后重新封装；更糟糕的是，如果攻击者对应用反编译，插入恶意代码后对用户可能造成更大范围的影响，包括用户个人信息泄露，还可能导致直接或间接的经济损失。

> 仿冒移动App出现的诸多渠道都极为主流，不少是OEM制造商所推机型出厂时预置的官方应用商店

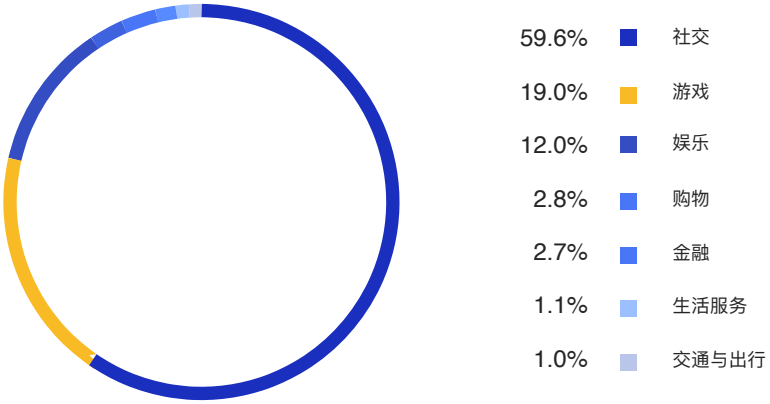
《2017金融行业应用安全态势报告》中呈现的数据表明移动App遭遇的仿冒攻击日益增加，金融类移动App的仿冒情况去年已经呈现逐月递增的趋势，每月增加的金融类仿冒移动App平均超过100款[3]。在本次报告中，启明星辰于今年4月份总共30天时间，监控397个不同渠道，针对多个不同类别的892款移动App做了全面追踪，以期了解移动App的仿冒情况。这些移动App依旧覆盖金融、购物、社交、游戏、娱乐、医疗健康、生活服务、交通与出行几个领域。这些移动App在不同渠道过去30天的下载量至少也有数十万次，多的可达数千万次。

其中有些有趣的数据呈现，追踪每个类别的样本都能发现相应的仿冒App：如出行类的28个样本出现仿冒移动App，16个渠道中存在相应的仿冒App；再如购物类22个样本出现仿冒移动App，17个渠道存在相应仿冒App——而且这些渠道都相当主流，不少是国内手机厂商所推机型出厂时预置的官方应用商店。

> 社交类App被仿冒并产生影响的几率相较其它类别应用平均高出10倍以上。仅社交类App被仿冒的占比，达到本次测试中所有仿冒移动App的近六成。

另一方面，与我们所想的有所不同：从我们测试每个应用平均数百万次的下载总量来看，网页端的下载总量超过移动客户端的下载量，且超出约31%。可见许多Android用户还是有从web端下载移动App的习惯，这也从侧面表明，在我们监控的诸多渠道之外，还有大量Android用户会从不受信任的第三方源下载移动App，这也加大了移动App可能对用户产生的危害，不管是从安全漏洞方面，还是从仿冒App、恶意App方面。

仿冒移动App感染情况占比（依据下载量）



从启明星辰的测试结果来看，社交类移动App被仿冒的情况明显高于其它类别。在397个渠道中，依据不同渠道出现仿冒App的次数及其下载量来统计（而非被仿冒App的个数），社交类App被仿冒并对用户产生影响的几率相较其它类别应用平均高出10倍以上。仅社交类App被仿冒的占比，达到本次测试中所有仿冒移动App的近六成。

举例某款明星粉丝社区交流App，275个渠道出现该App的仿冒版本，下载量最大的渠道（应用商店）中其仿冒版移动App的下载量在一个月的时间内就达到了20万次。虽然我们并没有追踪该仿冒App的具体仿冒行为，但不难想见，此类仿冒能够对普通用户造成多大程度的个人数据泄露损失，甚至经济损失。

仿冒App出现的根源或许并不能单纯归结至原App开发者，但这些App易遭遇反编译的安全风险却是不可忽视的。

2.3.4 有关敏感信息泄露

这份报告在行文中多次提到敏感信息泄露或数据泄露——我们之所以将侧重点瞄准移动App漏洞可能导致的信息泄露，原因是多方面的，不仅是报告第一章提到在《中华人民共和国网络安全法》自6月1日起开始施行对企业组织和开发者提出更多安全的强制合规需求，还在于全球范围内大量开发者参照的安全实践OWASP Top 10风险中，敏感数据曝光（Sensitive Date Exposure）一直都是其中的重要组成部分；而且实际上，其它类别的风险威胁，如各种注入式攻击、安全错误设置、未受保护的API（OWASP Top 10 2017新入榜）、弱加密算法等都有可能导致敏感信息泄露。

另外，诸如移动端内存敏感数据泄露的问题在移动App中也非常普遍。报告参考的移动App自动化安全测试提到的绝大部分漏洞也都能够潜在造成数据泄露的结果。即便是最直接的个人/敏感信息泄露问题，也足够占到所有漏洞总数的五成以上。而移动App的仿冒，更是用户个人信息泄露的大敌。因此我们认为有必要将敏感数据泄露问题单独成章，在接下来的章节中进行更为细致的探讨。

任何移动App的个人及敏感数据泄露，都应当受到用户和开发者的重视，即便或许许多普通用户会认为部分数据的泄露是微不足道的。这些数据对于攻击者而言存在极大价值，大量移动App的个人数据泄露，即使不能用于直接经济或情报利益的攫取，却完全能够用于社工；且这些信息环环相扣，如攻击者在获取用户的用户名和地理位置信息后，就能进一步解锁该用户的其它敏感信息，并作更具针对性的社工攻击。

通常移动App端的敏感数据泄露包括：Email、用户名、密码、IMEI（International Mobile Station Equipment Identity，是移动网络用于标识设备有效性的）、用户姓名、地理位置、设备Mac地址，及更多移动App在本地存储的信息等。

3.1 移动APP信息泄露的形式

如报告第二章相关移动App安全漏洞现状呈现部分提到的，漏洞以及其它安全问题导致的移动App信息泄露是移动技术面临的一大安全风险——某些安全漏洞即便并不直接与信息泄露挂钩，却也存在信息泄露的潜在风险；而移动App的仿冒很多情况下也造成了用户敏感数据泄露；此外，如不安全第三方SDK/代码、不安全的数据存储等问题也都能导致敏感数据泄露：像是移动端内存中的敏感数据大多以明文形式存储也构成信息泄露甚至其它恶意行为的基础。

但移动App信息泄露并不只是安全漏洞、不安全数据存储等导致的，其泄露途径是多种多样的，总体来看可以分为主动泄露和被动泄露两种形式，此章节将对一些主流的泄露形式进行总结。所谓主动泄露是指在App使用者可以控制信息，并在知情的状态下，主动将信息泄露出去；所谓被动泄露是指App使用者在未知情况下的信息泄露。通常主动泄露多因为隐私保护意识不强造成的；而被动泄露多由于产品本身技术能力不足造成。

3.1.1 主动泄露

主动泄露大多是由于信息拥有者自我安全保护意识不强，导致信息主动暴露在互联网上，通常会有以下泄露形式：

社交媒体

网上购物、博客、论坛、即时通信工具已经成为时下互联网用户的一大沟通方式，其留言评论功能是社交网络的重要组成部分。信息拥有者会无意间通过移动App主动在互联网上发布敏感信息，例如在购物软件中透露个人身高体重，甚至联系方式、住址等信息；博客留言板泄露个人敏感数据；朋友圈的信息分享等。

调查问卷

在日常生活中可能经常会碰到各种形式的“调查问卷”、“购物抽奖活动”，免费资源申请、会员卡申请等活动，这些活动通常会出现在某个移动App中，如微信公众号等。

信息收集发起者会有意或者无意地收集被调查方的敏感信息（如个人详细联系方式、家庭住址等个人信息），而信息拥有者也会因为自己主观安全意识的薄弱会导致个人信息的泄露。

3.1.2 被动泄露

被动泄露大多是在信息拥有者无意识状态下，由于技术漏洞、被动采集等形式而导致的信息泄露，通常会有以下泄露形式：

常规漏洞

应用本身的安全问题是攻击者常用的窃取信息的方式之一，常见漏洞如代码注入、API越权、XSS、暴力破解等。移动App的常规安全漏洞，以及包括不安全第三方SDK或代码、不安全数据存储在内的移动App安全问题也是这份报告的关注重点，第二章已经就这些漏洞的现状与危害作了相应的数据呈现。

客户端的木马/病毒/恶意软件

由于使用者不良的操作习惯可能导致终端设备中毒/下载木马/下载到恶意软件。这种行为会导致数据的严重泄露。

不安全的通信协议

文本传输、电子邮件、即时通信...不同规范、协议帮助互联网的世界有序运行。而许多协议的利用如HTTP、FTP等在设计之初并没有考虑过安全因素，却出于某些原因（如使用方便性、开发者习惯、某些历史版本继承原因等），应用使用着不安全的协议。通常这些协议会存在明文传输数据、缺少访问控制等缺陷，也会直接导致数据泄露的问题。

不安全的第三方SDK或代码

第三方SDK或代码在应用开发中经常被用到，然而使用者却无法追溯第三方SDK及代码的可靠性与安全性。开发者由于个人的工作习惯往往会导致使用不安全的第三方SDK及代码。这将会带来许多未知的安全风险，常见的恶意行为有：收集用于定位和追踪用户的信息，如设备的ID和未知信息；收集用户的邮箱地址以及安装在用户设备的应用程序列表；读取短信、邮件、电话通讯记

录和联系人列表等，在没有任何访问控制措施的情况下通过Web服务公开共享这些数据；数据的明文传输等。

不安全的数据存储

为了应用更快捷有效地运行，开发者需要将应用数据存储在本地，这些数据中就有涉及使用者的敏感信息，如：应用软件的登录账户信息；购物软件的个人信息（身份证、家庭住址、交易密码等）。因此，应用中需要可靠的加密措施对这些敏感数据进行保护。然而，基于开发商及开发者对安全认知不足，多数应用采用弱加密或不加密的方式，这种行为会大大降低攻击者破解的难度，导致信息泄露。而移动端的内存敏感数据泄露问题也可以归结到此类别中。

不安全的数据使用

弱口令已经成为整个安全界为之头疼的话题，这个完全没有技术难度的话题上却时刻挑战着用户的数据安全。无论是企业的运维人员抑或普通的大众用户，依旧存在使用弱口令的习惯，而这一安全陋习也会导致了其数据泄露。

网络钓鱼

有时，我们通过某些渠道收到一些奇怪的网站链接：通知你领奖；通知你更改密码信息；通知你即时兑换积分、里程；通知你登录认证信息过期，重新登录等等。这类网站信息就是恶意攻击者经常使用的网络钓鱼手段，其目的最重要的就是为了搜集信息。

应用程序访问

在安装许多移动App时，用户经常会看到弹出对话框，申请“向您发送通知”或“使用您的位置”等权限。如果用户点“允许”，这些应用便可扫描并把手机信息上传到网际网路云端服务器，这样手机使用者的位置、通话记录、甚至家庭住址等都很容易被人窃取。

Log文件

Log文件在开发过程中有着重要作用，它能有效帮助开发者定位bug信息，解决实际问题。同时，它还有效地起着追溯审计的作用。然而日志中也会存在敏感信息如用户名/密码，传输数据等。

不安全的配置文件

全局可读文件，应用内存在其它任何应用都可以读取的私有文件，可能造成信息泄漏；App调试风险，允许程序被调试；私有文件存在敏感文件泄露风险；App备份风险，允许程序备份，可能导致用户信息泄露。

企业的不合规的数据搜集

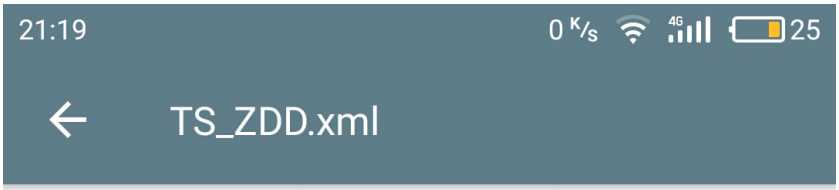
出于某种目的，企业会在应用中植入某些数据采集功能，实现数据搜集目的。主要形式有通过WebService远程数据传送；通过业务进行用户行为采集等。

3.2 案例列举

3.2.1 不安全的数据存储/传输/log输出

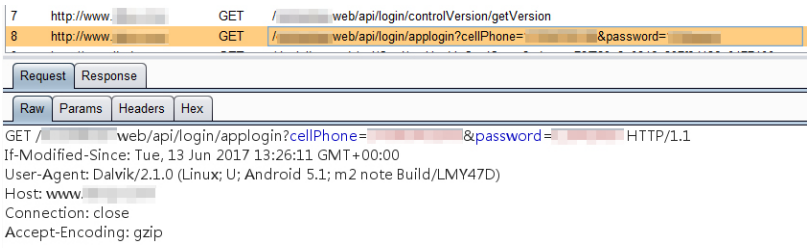
针对上述移动App安全漏洞及可能导致的信息泄露等安全问题，在本章节中进行具体的案例列举。如开发者对安全认知不足，多数应用已然采用弱加密或不加密的方式，这种行为会大大降低攻击者破解的难度，导致信息泄露，这类App案例相对普遍。

如本地明文存储账号密码：



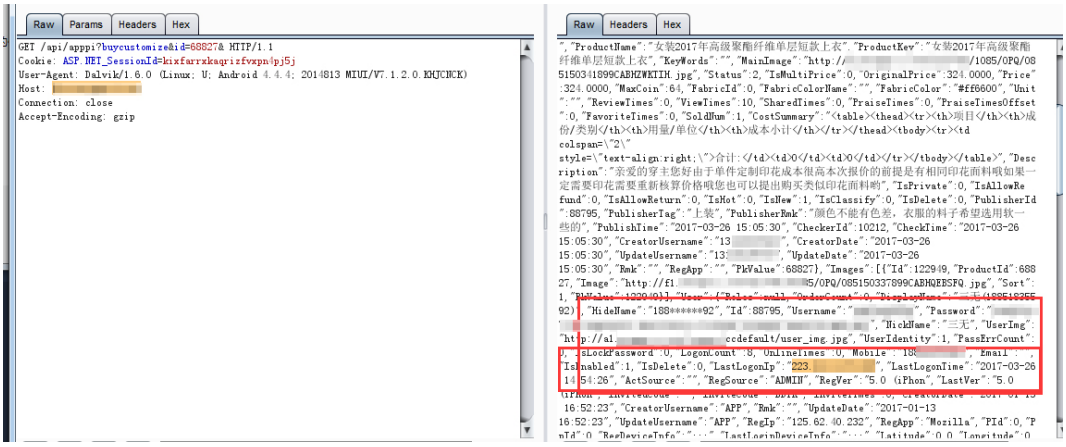

```
<?xml version='1.0' encoding='utf-8'
standalone='yes' ?>
<map>
    <string name="username">[redacted]</string>
    <string name="password">[redacted]</string>
    <boolean name="isSave" value="true" />
    <boolean name="isNewVersion" value="false" />
</map>
```

使用http传输明文密码:

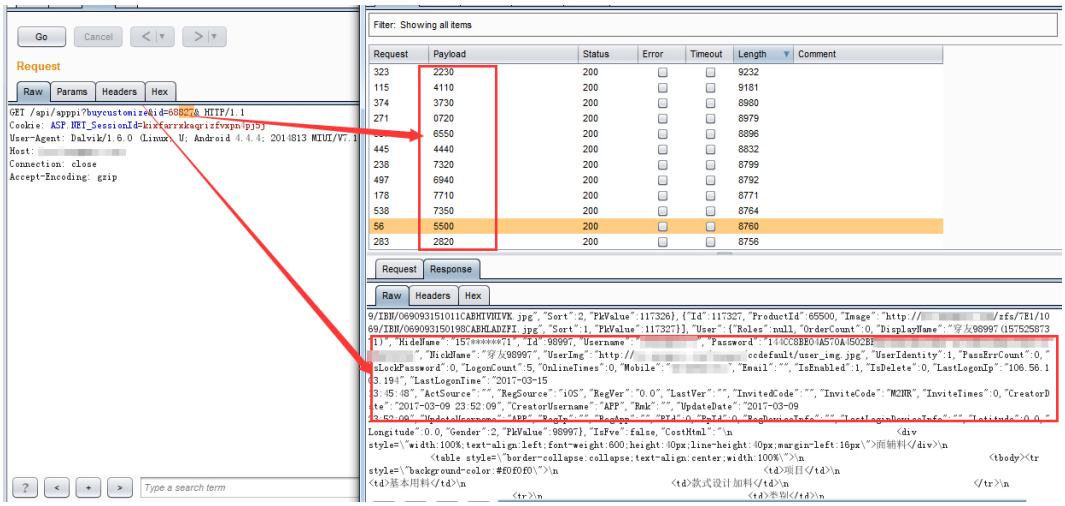


3.2.2 API接口越权导致的信息泄露

在某购物类App中，用户在点击购买商品时，App后台会调用API接口查询对应用户的个人信息。这部分信息，不会显示在App界面，但通过工具抓包可以看到返回的信息中包含未经打码的个人敏感信息，包括姓名，手机，登陆IP，甚至数据库中Hash密码也返回给前端。



更为严重信息泄露问题，App缺乏权限控制，遍历请求中的用户ID，攻击者可轻易获得全站的用户用户名，密码，手机等敏感信息。



在某物流公司的移动端应用中，我们也可以看到App API相类似的信息泄露问题，甚至都不需要身份验证，外部均可任意调用App接口查询寄送物流信息，造成上千万物流订单敏感信息泄露。

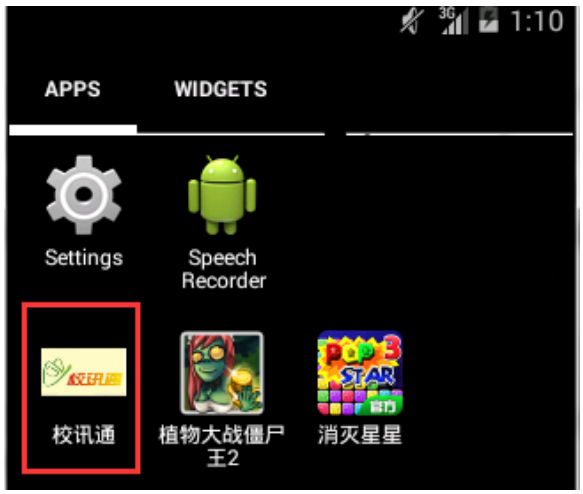



```
{
  - list: [
      - {
            cargoName: "货物",
            orderNo: "NO10[redacted]",
            transNo: null,
            userId: "353[redacted]",
            shipperMobile: "181[redacted]",
            consigneeName: "陈[redacted]",
            orderStatus: "WOID",
            evaluate: null,
            senddate: 1491[redacted],
            shipperName: "陈[redacted]",
            shipperProvince: "江苏省",
            shipperCity: "南京市",
            shipperArea: null,
            shipperAddress: "麒麟[redacted]",
            consigneeMobile: "183[redacted]",
            consigneeProvince: "江苏省",
            consigneeCity: "盐城市",
            consigneeArea: null,
            consigneeAddress: "富[redacted]",
            cargoVolume: 1,
            cargoWeight: 1,
            cargoPiece: 0,
            remarks: null,
            productTypeName: "定日达",
            orderId: null,
            orderOrigin: null,
            shipDept: null,
            einoEscoSecondCode: null,
            einoEscoSecondName: null,
            errcode: null,
            errmsg: null
        },
```


3.2.3 客户端的木马/病毒/恶意软件

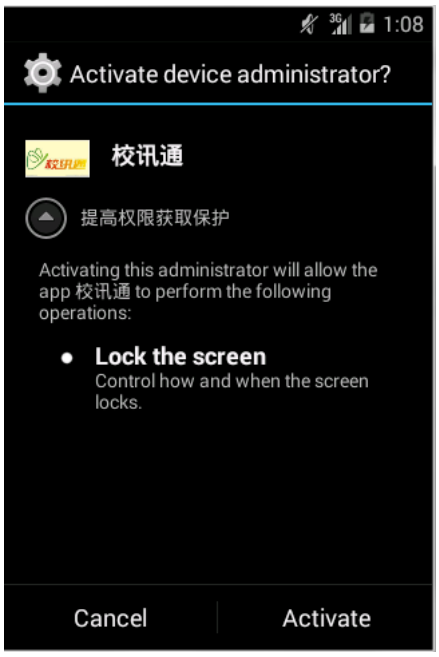
漏洞盒子平台监控到近期手机木马App，利用某银行在线支付业务特点，盗刷用户银行卡。

第一步：诱导用户安装木马App，并隐藏图标



不法分子通过地下黑产拿到身份证、银行卡号、电话号码，定向给用户发送诱骗信息，如“您好，这是你孩子近期成绩情况，请重视，[校讯通/成绩单]xxxxx.cn/pmg”,不少家长用户误以为真，点击了链接导致手机并静默安装了木马APP软件。

点击“校讯通”APP图标，弹出如下界面，询问是否激活并获取相关权限，一般用户由于缺少信息安全防卫疑似会轻易点击“Activate”。之后提示用户“应用卸载成功”，实际是隐藏了图标。





第二步：利用某银行在线支付业务特点，拦截用户短信，盗刷用户银行卡

经过对App行为分析发现，木马通过拦截用户短信，利用某银行在线支付业务，购买虚拟产品盗刷银行卡。而某银行在线支付，输入用户手机，短信验证码，卡后六位即可支付成功。



即使用户未开通在线支付业务，不法分子在知道用户手机号码、卡号、验证码情况下，也可代替被害者完成在线支付注册（实际不需要到柜台通过u盾介质开通）。由于客户端已经中招，木马App可以将银行的支付验证码拦截并删除，整个过程用户都毫不知情。



上图：监控不法分子邮箱发现的部分受害者被盗刷信息

3.3 移动端内存敏感数据泄露

由于移动端内存敏感数据泄露，在所有数据泄露问题中显得相对突出和重要，所以这里将移动端内存敏感数据泄露问题单独为一个章节进行探讨；中国泰尔实验室为这部分内容提供了数据和内容支持。2017年年初至今，中国泰尔实验室研究人员单独对上述892个移动App的敏感信息保护进行检测，发现其中96.2%的移动App存在内存敏感数据泄露风险。

移动App在运行过程中会在本地保存缓存文件、配置文件、数据库文件等数据，同时在内存中会保留程序常驻内存数据、网络传输数据明文阶段数据、本地存储数据明文阶段数据等敏感数据。移动端内存敏感数据泄露，即是指攻击者可以通过直接获取内存空间数据的方式，窃取、篡改、劫持程序的核心交互数据。

> 多达88%的金融类APP都存在内存敏感数据泄露问题

3.3.1 内存敏感数据为何需要保护?

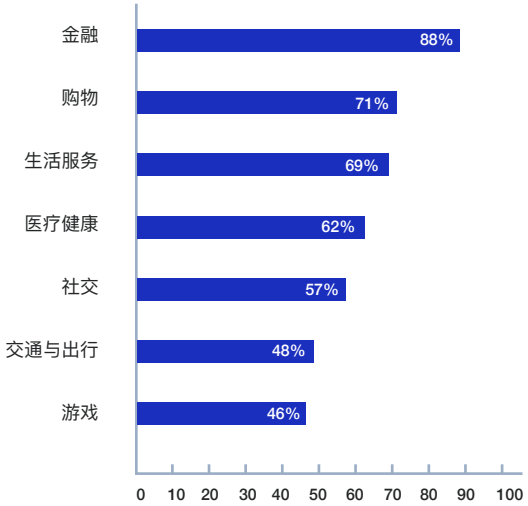
中国泰尔实验室研究人员通过对移动应用信息泄露的检测分析发现，按照移动应用使用场景可将敏感数据泄漏情况分为三类：

第一是用户信息泄漏，指移动应用在主动或被动的情况下，泄漏用户个人敏感数据，如用户姓名、身份证号、联系方式、地址等；第二是登录信息泄露，指移动应用在登录过程中，泄漏本应用的用户登录相关信息，如登录账号、登录密码、短信验证码等；第三是交易信息泄露，指的是涉及业务交易的过程中，泄漏用户交易相关信息，如交易账户、交易金额、开户行名称、开户行地址等。

这些数据在移动终端内存处理过程中，大多是以明文的形式进行的，容易受到攻击。一方面手机银行等移动APP在运行过程中，用户在进行转账汇款等交易时输入的账号、开户行等敏感数据信息在写入移动终端内存时，可被黑客利用相关技术手段进行篡改，使得原本要转给亲友或企业的资金被转入黑客指定的账户。同时，黑客也可以通过获取移动终端内存相关数据，劫持手机银行等移动APP运行时关键Activity组件，对登录或支付界面进行劫持替换，窃取用户登录或交易的敏感数据。

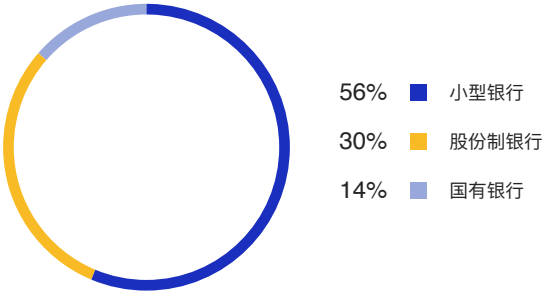
3.3.2 内存敏感数据泄露现状

不同类型移动应用内存敏感数据泄漏情况

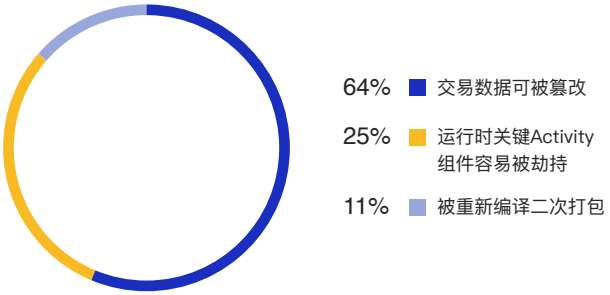


虽然从总的移动App安全漏洞数据来看，金融类App在安全性方面相较其它类别表现尚可，但中国泰尔实验室研究人员通过对892个移动App的内存敏感信息泄露进行检测分析发现，仅内存敏感信息泄露问题，移动金融类App位居榜首，存在内存敏感数据泄漏风险的金融类App占比高达88%，其次为购物类和生活服务类移动App。

存在内存敏感信息泄漏风险银行类型分布情况



手机银行APP存在部分风险问题



实验室研究人员检测分析结果显示，金融类App中存在内存敏感数据泄露高危风险的手机银行App涉及国内多家大型商业银行，中小银行的内存敏感数据泄露风险更高。被检测的手机银行App存在自身防御手段较弱、易被破解等安全风险，导致用户在使用手机银行App进行转账、支付等操作时，容易被黑客通过相应的技术手段劫持用户的转账交易信息，致使用户的转账交易资金被非法窃取。

《2017金融行业应用安全态势报告》提到，金融服务行业已经成为攻击者的主要攻击目标——且互联网与移动金融近两年发展迅速，而金融类App的内存敏感数据泄露问题的确给用户的隐私和财产安全带来了严重威胁[3]。

中国泰尔实验室建议企业应当利用独立SDK检测工具来提高移动应用的安全等级，针对风险点进行安全防护，增加移动应用在运行过程中敏感数据的保密性，达到防查看、防盗用、防篡改的目标；同时对移动应用中的数据进行加密处理，并在运行时动态解密。

此外应在安全组件设计过程中加入内存敏感数据防御功能来解决此类问题：如在App开发阶段，对程序核心数据进行代码阶段的迁移保护；在App编译阶段，对程序核心数据进行格式变换的保护及解析，确保程序核心数据及敏感数据在整个Android生命周期中都处于安全状态。而安全与设计的融合也是下文的研究分析中将要从更大范围强调和展开的内容。

3.4 移动App安全漏洞及信息泄露成因

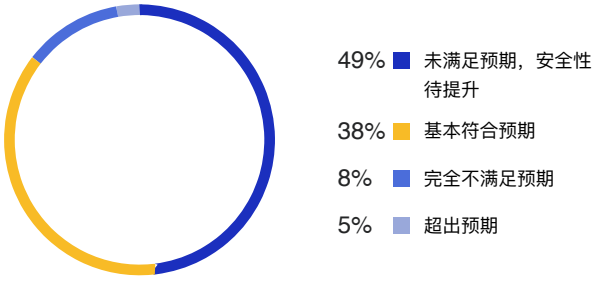
为了追踪和深入了解移动App安全漏洞及信息泄露问题，我们针对移动App开发者、项目管理人员下发了近200份问卷，期望从根源上窥探当前移动App安全现状的成因，并尝试就问题本身提出有价值的建议。Arxan在《第5次应用安全年度现状安全报告》中激进地提到，其受访50%的企业组织对移动应用安全几乎是0预算状态[7]。从我们的统计结果来看，超过七成的受访者（72%）均表示其App开发有安全方面的专门开支，但也很少有开发者或项目管理人员知道这笔开支在整个项目，或者企业级App安全在企业IT预算中的占比情况。

不过我们依旧发现，即便再怎么呼吁将安全融入到开发和运营流程中，就现如今国内移动App的现状来看，安全似乎仍然是明确脱离于开发之外的话题。这一点从开发者的反馈就能表现出来，也表明移动App的安全问题依旧任重道远。

开发者对于App安全性普遍更悲观

在2.2章节中，报告提到一般用户对于移动App安全性是相当乐观的，而在那份针对消费用户的问卷中，部分参与开发过程的受访者已经表现出对于移动App安全的消极态度。在这份主要针对开发人员和项目管理人员（及部分安全专家）的问卷中，从开发的角度来说，受访者明显认为移动App安全性做得不够到位。

在开发者看来，移动App的安全性是否到位?



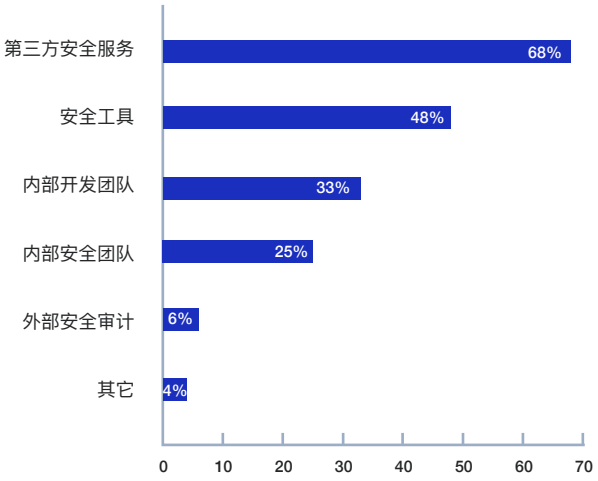
近一半受访者（49%）认为，自家App安全性未满足预期，需要提升；8%受访者则表示开发的App在安全性上完全不满足预期，理应推倒重来；38%的开发者与安全专家认为其App安全性基本符合预期，仅5%认为安全性超出预期。这和前文提到48%普通消费用户认为使用的App是安全的这一结论恰好相反，足见消费用户对于App安全的自信绝大部分是盲目的。更何况在很多情况下，普通用户还会从未受信任的源下载App，其盲目性会显得更加突出。

且即便是开发者，对于移动App安全性的认识也可能是不到位的。比如在某些App曝出安全漏洞或用户数据因此泄露的事件之后，其他同类业务的开发者和安全专家会庆幸，幸好不是自家App，或因此认定自家App安全性做得是到位的。实际情况可能和App的市场影响力，以及攻击者的目标都有关，而并非是安全性足够到位。

开发与安全的分化是根本原因

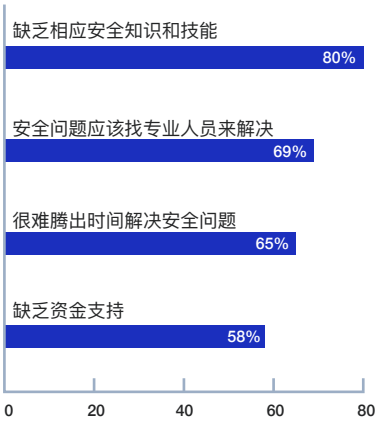
SANS Institute近几次的《应用安全现状：拉近距离》报告都反复提到了Builder和Defender之间的分化和距离[8]。这里的Builder就是指App开发者（架构、开发、设计）与App开发决策人员，而Defender除了运营之外，则是泛指负责App安全的研究人员，可以是企业内部的专门安全人士，也可以是外部安全服务团队。SANS的这份报告重在从企业内部App及其安全的角度来阐述移动App的安全问题。其中提到一个有趣的现象，即超过25%的Defender并不知道企业中使用和管理多少应用，而这原本是Builder可以很容易为Defender提供的信息，足见开发和安全是何等分裂。从我们的统计来看，面向普通消费用户的移动App，在国内的情况也大同小异。

应用安全主要依靠



从FreeBuf研究院的统计结果来看，绝大部分开发团队的移动App安全会依赖第三方安全服务提供商（68%）和安全工具（48%），较少企业组织或开发团队拥有独立安全人员，或者说安全问题可由自己解决。这个问题是由来已久的，且早前被开发者认为是理所应当的，即我负责开发，不负责安全。而且即便是内部有专门安全人员的开发团队，开发和安全依旧存在分化的问题。

内部开发团队解决安全问题的难处在于



69%的开发者认为，“安全问题就应该找安全专业人员解决”，言下之意即安全是其他人的工作，这个比例在2017年看来显得有些令人惊讶。认为“很难腾出时间解决安全问题”和“团队缺乏资金支持”的占比达到了65%和58%，但最多比例的开发者（80%）认为难点在于自己“缺乏相应的安全技能和知识”。可见开发者和安全专家之间的确存在较大鸿沟，或者也可以认为安全培训在App开发中是极为缺失的。

> “69%的开发者认为，安全是其他人的工作”

> 开发者与安全专家工作的优先级存在差异，开发者更专注于移动App的功能特性及更新，还需要及时交付App。

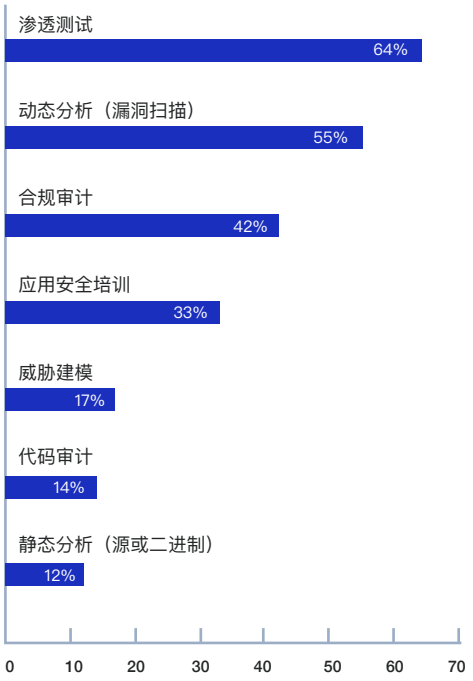
从“很难腾出时间解决安全问题”这一选项可表征的是，开发者所专注的主要是移动App的功能特性及其更新，开发团队需要按照要求及时将App交付到市场上。这可能也正是开发人员默认“我负责开发，不负责安全”的根源所在，因为毕竟安全专家没有这方面的压力。另一方面，绝大部分安全专家实际对于App开发也不够了解，双方的鸿沟得以形成。这甚至使得针对App安全补丁的开发都成为一种挑战，此事如果再加上企业组织内部的其他组成部分，安全问题的解决将变得更为复杂。

诚然双方工作的优先级是有差异的，仍有越来越多的企业组织开始采用合作式的DevOps实践，将App开发的项目管理人员、开发者、运营与信息安全结合起来，并在系统构建和运营间实现责任共担。这才是健康的App开发方式。我们认为，正如前文提到安全性能够成为移动App差异化竞争的优势项，未来越来越多的开发者和企业组织意识到这一点之后，开发和安全的这种鸿沟会随着此类趋势而逐渐弥合。安全本身会因为市场现状成为双方沟通的一种推动力。

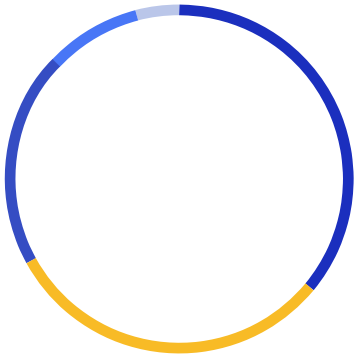
当前App安全最大驱动力仍是合规

从受访的开发者选择为自家App所做安全活动的数据来看，绝大部分开发者、安全专家或企业组织都为App进行过渗透测试，且许多企业内的安全专家将渗透测试（以及安全培训）看做是安全控制和实践有效性的最佳活动[8]。实际上，渗透测试经常作为安全阶段性检查或强制合规的组成部分，且渗透测试在App安全方面具备了相当价值。但开发团队和安全团队如此看重渗透测试，实际上也是他们将安全与开发作切割的客观表现，从源头上并没有形成从移动App设计和构建阶段就加入安全考量的意识。

对App做过哪些安全活动?



对移动App进行安全评估与测试的频率为



36% 仅应用发布（更新 / 升级）之前才进行

31% 基于合规与内部审计周期

20% 发现存在问题时才进行安全测试

9% 首次评估测试后，再也不对App进行安全评估与测试

4% 其它

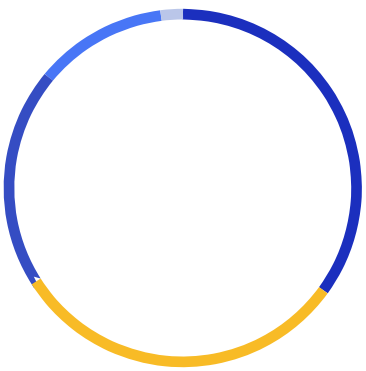
而且绝大部分App开发和安全团队（36%）进行App安全评估与测试时机，仅在应用发布（更新或升级等）之前才进行，更有甚者有部分（20%）是发现安全问题后才作安全评估与测试；9%的开发者在首次应用发布之后就再也不对App作安全评估与测试，这几乎可以认为是对App安全问题的漠视。

从根本上来说，近四成（35%）开发者和安全专家认为，其移动App安全的主要驱动力在于强制合规（或者对于审计结果的响应）——这从安全的角度来说表明国内的移动App开发仍处在初级阶段。无论是渗透测试成为“安全最佳实践”，还是合规审计成为“安全最大驱动力”，都充分表明安全和开发的割裂。

> “作具体规则和标准制定的实体通常滞后于网络犯罪”

合规作为防御方的主要驱动力，能够表现防御方与攻击方的不对等。SANS在报告中提供了有趣的一份数据[8]，其报告测试的19款医疗健康类App是获得FDA（美国食品药品监督管理局）认证批准的，但其测试表明这些App并不比其它普通App更安全。SANS在报告中提到：作具体规则和标准制定的实体通常滞后于网络犯罪。这已经很好地表明了，合规从来不能也不应该作为App安全的主要驱动力，它只为App安全提出最基础的要求。但对国内的开发商而言，真正做到合规仍是第一步，这种投资也是完全有必要的。

应用安全的驱动力和原因主要在于?



35% 合规，或者对于审计结果的响应

31% 对已经发生安全事件的响应

20% 安全事件可能造成经济方面的损失

12% 安全就处在App开发的标准流程中

2% 其它

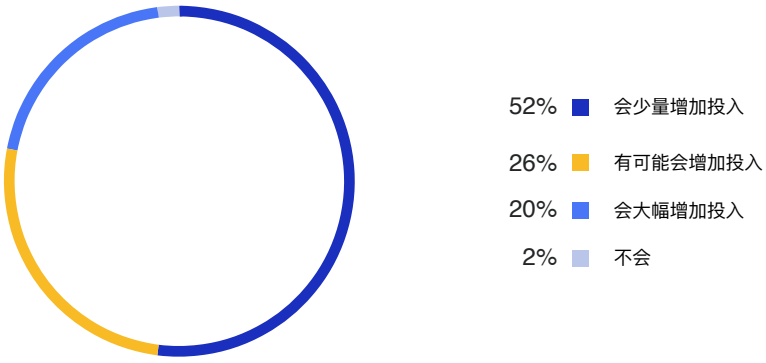
从我们的调研结果来看，仅有12%的开发者回应称其安全就位处移动App开发的标准流程中。这可能是未来很长一段时间内移动App开发需要解决和正视的问题。

App安全投入还会增加

许多开发者及其所在的企业组织都已经意识到了安全培训对于移动App开发的有效性，而且他们中的绝大部分也了解开发与安全作结合的重要性。但大概仍然由于开发者和安全专家在工作优先级上的差异，近五成企业组织从来没有或者很少为开发团队提供安全培训——需要注意的是，这里主要是指对开发团队的安全培训。SANS的报告中提到，安全培训是其受访者认为安全实践有效性评价最高的项目。

统计结果显示，仅25%的开发团队会借由内部安全团队进行App安全开发培训，22%则会邀请第三方安全专家进行培训，极少数团队会针对开发中的不同角色，为其进行强制性的安全认证。就其余很少进行安全培训的团队而言，这个数字还是有极大的提升空间的。

未来一年内，是否会加大App安全方面的投入?



好在过半的企业组织表明，未来一年内会少量增加移动App安全方面的投入；20%则表示会大幅增加投入；26%有可能增加投入。即便这个统计结果可能偏向乐观，移动App安全总体仍是在朝着好的方向迈进的。

4.1 移动App开发安全建议

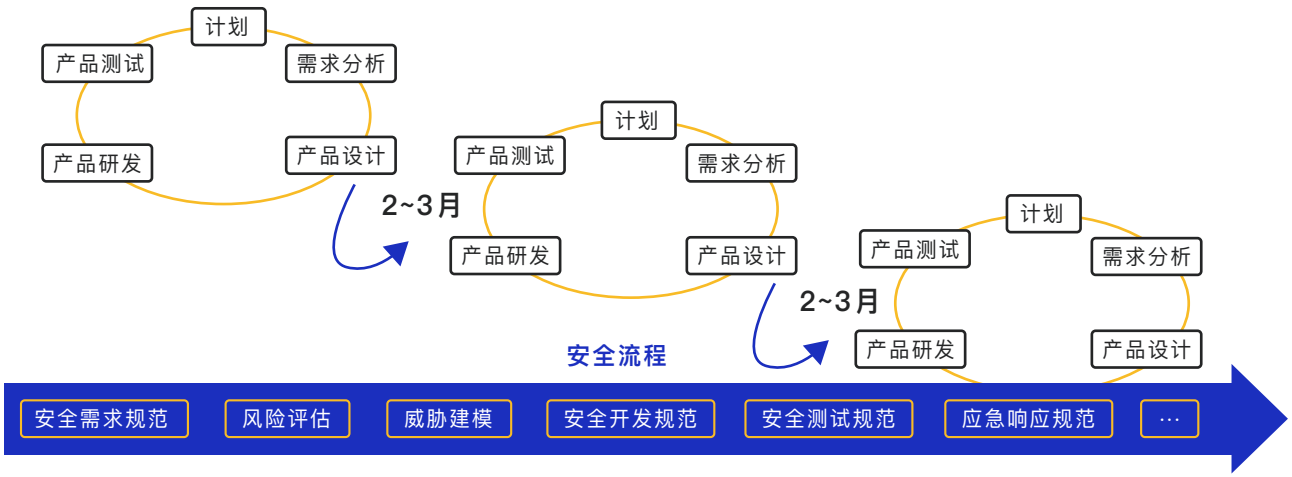
4.1.1 安全开发运营层面

2007年Android系统出现至今，移动App安全走过了几个时代。2012–2014年间，安全加固服务开始崭露头角。不过彼时的安全加固只解决了客户端和代码安全问题，对隐私、业务、通信安全而言并没有很大的帮助；到2015年开始有了移动App安全检测服务，这个阶段的安全加固引入了自动化审计，对通信安全有了一定的帮助，但隐私安全和业务安全也依旧是问题。

就安全部分，移动App安全加固现如今的发展阶段引入了“安全生态链”，所以顺势出现了融入到整个App开发上线周期链中的全套安全服务。这个生态链包含了安全SDK组件、安全编译器、安全检测与风险评估、安全加固、渠道检测和智能云更新。该生态链对行业而言是有价值的。如报告中提到的内存敏感数据即贯穿移动应用产品的整个生命周期，仅仅采取单一的App加固解决方案并不能完全杜绝敏感信息泄露问题。这个“生态链”的本质在于将安全融入到开发周期中，试图解决开发和安全分割的现状。不过，这仍是需要开发团队或项目管理人员，以及配套的安全专家真正建立起足够的安全意识并跨出一步，做出配合方能见效的。

本次报告的前三章内容从移动App安全漏洞、App仿冒、数据泄露等安全问题入手，以统计和测试数据为依托，对这些安全问题的现状进行解读和分析，期望从Android平台移动消费类App客户端安全问题的角度，对移动安全进行管中窥豹，并让所有读者了解移动App安全问题的紧迫性。

面对App应用整个产品生命周期管理各个阶段，操作建议如下：



需求阶段

这个阶段需要将App应用的功能需求统一规划制定出来，而需求文档是整个移动应用开发的指导性文档。文档中需要涵盖客户对安全的需求、企业自身对安全的需求、开发安全需求、测试安全需求等。

产品整体设计阶段

这个阶段可根据企业自身的安全开发规范、安全评估规范进行整体安全设计，其中包括应用安全、源码安全、数据安全、通信安全、服务安全等。

产品开发阶段

这个阶段需要保证需求与设计阶段的落实情况，包括是否遵循企业安全编码规范，是否有质量把控等。

产品测试阶段

产品安全测试阶段主要是对App应用的安全评估工作，以及安全评估规范要求，查验产品安全落实情况。整个评估过程需要符合客观性与公正性原则、经济性和可重用性原则、可重复性和可再现性原则，以及符合性原则。增加有效的测试过程，保证产品上线前的安全性。

产品运维与运营阶段

产品发布过程中需要有安全发布流程，针对App应用发布渠道进行监控，确保发布渠道安全可信、可控、可用。

产品上线后更需有效管理，有必要的监控措施和问题反馈渠道，建立运营管理操作规范。

安全事件处置与应急响应

产品在运营过程中需要进行必要的预案准备，当安全事件发生时，启用预案响应机制进行安全事件处置。对未知事件根据相关规范进行事件分类、定级，制定相关处置措施，必要时成立专家项目组进行应急响应。

应用废止阶段

这是软件生命周期的最后环节，应当保证应用在转移、终止、废弃时，对应用中的敏感数据、核心技术进行保护，确保各个环节的安全性。

4.1.2 企业安全战略布局与行业监督管理层面

除了开发与运营层面的具体实施，中国信息通信研究院安全研究所从企业安全战略布局与行业监督管理层面提出更多建议。相关企业应以合规合法运营为根本，以促进企业持续健康发展为目标，积极转变发展理念。

（1）大力提升安全意识，强化内部安全管理，确保合规合法运营。移动应用安全漏洞频发，数据泄露问题时有发生，严重损害了用户合法权益。《网络安全法》中提出网络运营者开展经营和服务活动，需履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

（2）积极转变发展理念，进行安全战略布局，促进企业持续健康发展。为抢占移动互联网入口，企业各方不遗余力推广与更新自身应用，重用户体验而轻安全保障。但历次数据泄露等安全问题的爆发，无不给企业带来巨大的经济损失和重大不良社会影响。相关企业亟需转变理念，加大安全投入，积极在网络安全上进行战略布局，提升行业安全竞争力，促进企业持续健康发展。

行业管理者可从安全管理机制建立健全、标准体系配套完善、安全意识重点提升方面全面着手，积极引导提升行业安全基准、大力夯实移动App安全防护能力。

（1）强化移动App安全防护能力审查机制，积极引导提升安全基准。我国相关主管部门需积极引导提升移动App安全防护能力水平，增加对企业自主研发移动应用的安全防护能力审查力度。一是将其作为基础电信企业网络与信息安全责任制考核要点，保障安全基线要求，并积极推动相关工作落地实施；二是深入贯彻《国务院关于积极推进"互联网＋"行动的指导意见》，重点开展

“互联网＋”普惠金融、“互联网＋”益民服务、“互联网＋”电子商务、“互联网＋”高效物流等典型互联网企业移动应用安全防护审查试点示范工作，健全行业网络安全防护审查机制。

（2）增强监管标准技术支撑能力，强化平台主体责任。一是完善相关标准体系，积极推动“移动应用开发安全能力技术要求/评估”等标准贯彻实施，为开发实践、安全防护测评提供指导；二是增强监管技术支撑能力，强化事中监管薄弱环节，支持国内第三方检测、评估、认证相关技术手段建设，为行业监管提供有力抓手；三是引入平台治理模式，移动应用分发平台在应用上架前的安全审核中，可增加移动应用安全防护能力测试评估，从分发源头进行安全防控。

（3）引导提升企业安全意识和能力，激励行业安全技术创新。鼓励相关组织机构，一是展开“移动应用安全开发”宣传周活动，推进网络安全文化建设，增强企业安全意识；二是开展APP安全开发培训、竞赛，提高开发者安全开发能力；三是组织产业峰会、学术沙龙，加强技术交流，鼓励行业安全技术创新。

4.2 合规本身是一种投资

为了应用更快捷有效地运行，开发者需要将应用数据存储在本地，这些数据中就有涉及使用者的敏感信息，如：应用软件的登录账户信息；购物软件的个人信息（身份证、家庭住址、交易密码等）。因此，应用中需要可靠的加密措施对这些敏感数据进行保护。然而，基于开发商及开发者对安全认知不足，多数应用采用弱加密或不加密的方式，这种行为会大大降低攻击者破解的难度，导致信息泄露。而移动端的内存敏感数据泄露问题也可以归结到此类别中。

虽然报告在总结移动App安全问题频发的问题时，将其中部分原因归结为近四成开发团队进行App安全实践的驱动力只在于合规。但就国内开发商和开发者现阶段状况而言，合规仍是首先需要迈过的一道门槛，且国内相关规定虽不及发达国家，却也正在发展和完善，对于移动App安全而言具有推动力。

2016年11月中国正式出台了《中华人民共和国网络安全法》，并已经于今年6月1日开始施行；5月2日，国家互联网信息办公室还发布了《网络产品和服务安全审查办法（试行）》。国家未来还会增加更多促进网络安全的相关法律法规，推进网络安全的发展。针对数据泄露相关问题也在部分条款中作了明确说明。如《网络安全法》中：

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

第三十一条、第四十二条、第四十五条对数据泄露都有相关规定。于此，合规是成本还是投资这一问题的答案已经相当明确。《网络安全法》的颁布从大众视角来看，标志着中国互联网安全正式告别蛮荒时代。对企业而言，贯彻落实网络安全法合规性的过程本身就是一种投资。不仅在避免因违规而遭遇处罚的问题上，合规投入有了最为显著的收益，且唯有做到合规，才真正有了安全性可言，业务开展及其连续性才能得到基本保障，这是移动App安全、企业安全乃至整个信息安全领域的第一步。报告中的更多举措建议当不只是呼吁，而理应上升为责任与义务。

附录

参考文献

[1]《Mobile is Eating the World（移动正在吞噬世界）》，ANDREESSEN HOROWITZ，
http://a16z.com/2014/10/28/mobile-is-eating-the-world/

[2]《Smartphones – Statistics & Facts（智能手机：数据与事实）》，Statista，
https://www.statista.com/topics/840/smartphones/

[3]《2017金融行业应用安全态势报告》，FreeBuf，http://www.freebuf.com/news/topnews/128874.html

[4]《Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2016（2016年漏洞总数Top 50产品）》，CVE Details，
http://www.cvedetails.com/top-50-products.php?year=2016

[5]《2016 NowSecure Mobile Security Report（2016 NowSecure移动安全报告）》，NowSecure，
https://www.nowsecure.com/ebooks/2016-nowsecure-mobile-security-report/

[6]《Number of apps available in leading app stores as of March 2017（截至2017年主要应用商店可用App数量）》，Statista，
https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

[7]《5th Annual State of Application Security Report（第五次应用安全年度情况报告）》，Arxan，
https://www.arxan.com/wp-content/uploads/2016/01/State_of_Application_Security_2016_Consolidated_Report.pdf

[8]《State of Application Security: Closing the Gap（应用安全现状：拉近距离）》，SANS，
https://www.sans.org/reading-room/whitepapers/analyst/2015-state-application-security-closing-gap-35942

关于报告

作者

FreeBuf研究院：谢忱、李勇、徐钟豪、曾裕智、张志鹏、朱嘉豪、余桂茗、黄烨锋

启明星辰：姚正宁、刘存

中国信息通信研究院安全研究所：崔涛、于成丽

中国泰尔实验室：杨正军、邓文治、焦四辈、翟世俊

美术设计

孙溪村

更多内容扫描二维码访问FreeBuf

TOPHANT 斗象科技

FREEBUF