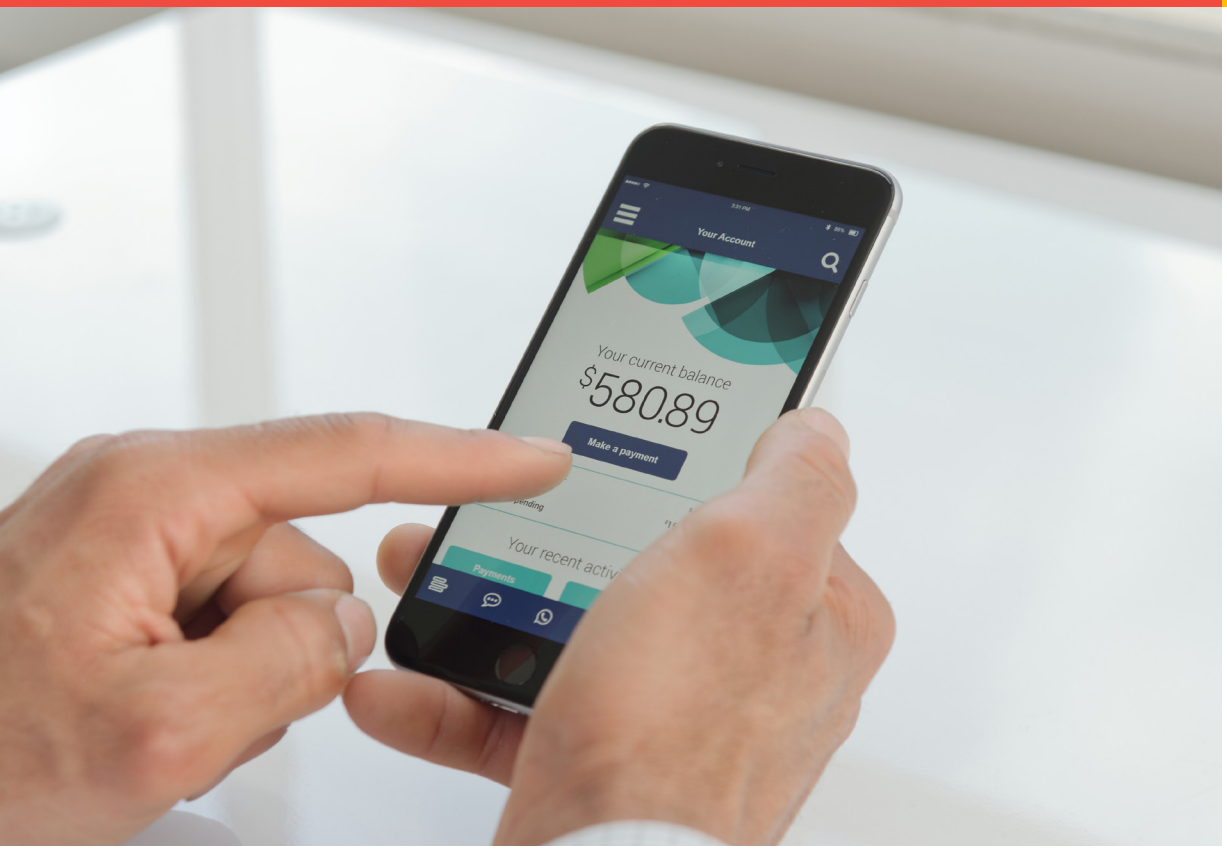
您的数字资产钱包安全吗?

普华永道中国数字资产钱包安全评分体系

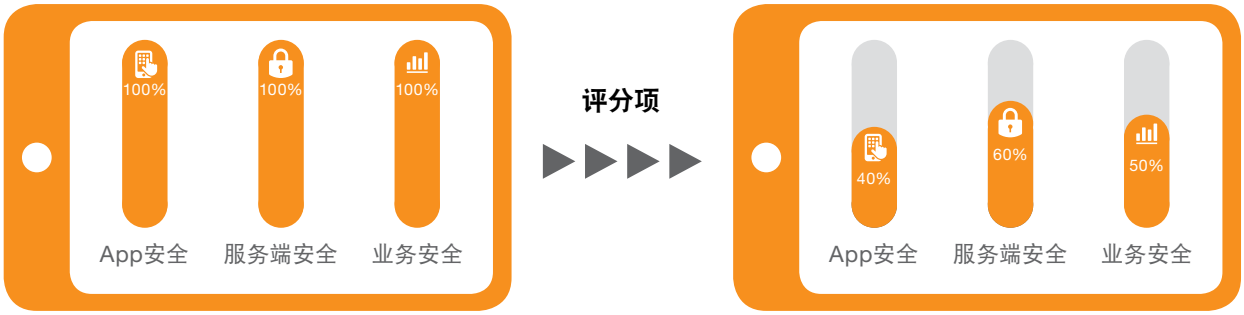
2018年12月



pwc 普华永道

钱包安全评分体系

在之前发布的普华永道中国数字资产钱包安全框架的基础上，我们设计了一套成熟完善的数字资产钱包安全评分体系。普华永道中国数字资产钱包安全评分体系从App安全、服务端安全、业务安全三个方面对钱包进行评分。评分体系采取扣分制，在每个安全方面分别设置了若干评分项，评估每个评分项的漏洞等级和可能性，计算出每个评分项的风险分值。三个安全方面初始分值均为100分，初始分值扣除计算出来的风险分值后得出各个方面的安全评分，最低分值为0分。下文将分别针对评分项、漏洞等级、可能性、风险分值进行详细介绍。



评分项

根据普华永道中国钱包安全研究的经验，在每个安全方面设置了细致的评分项，本文仅在各方向列示了一个评分项作为示例，具体参见下表。

名称	评分项	
App安全	**私钥安全**	私钥的生成算法是否采用可预测的加密因子
	助记词安全	助记词生成过程中是否会以明文形式进行网络传输
	密码安全	交易密码输入过程中是否可以被复制/粘贴
	Keystore安全	keystore是否明文存储在客户端本地缓存
	客户端自身安全	应用进入后台时，是否删除视图中的敏感数据
	本地数据存储安全	是否会将钱包登录密码/手势密码明文保存至本地缓存
服务端安全	**输入安全**	是否存在CSRF跨站请求伪造
	配置安全	是否存在弱口令
	网络传输安全	是否采用不安全的SSL2.0加密传输协议
	网络架构安全	应用所有组件可以被识别且确实需要
业务安全	**业务逻辑安全**	钱包的登陆密码/手势密码是否可以被绕过
	功能设计缺陷	验证创建钱包时需要单独设置密码

漏洞等级

根据评分项对应的漏洞理论上所产生的危害，将漏洞等级分为四个等级，分别为严重（Critical）、高（High）、中（Moderate）、低（Low）。其中严重漏洞分值为50分、高危漏洞分值为20分、中危漏洞分值为10分、低危漏洞分值为5分。如下表所示：

理论上可大规模威胁到网络、操作系统、业务系统的安全性，可直接导致业务中断或敏感信息泄漏，可以使得系统中大规模用户受到攻击，此类风险如高危性质远程缓冲区溢出、重要加密算法破解、远程命令执行、上传getshell、代码执行等。

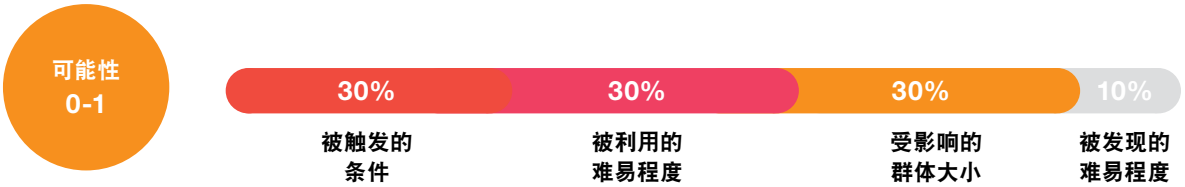
理论上可威胁到网络、操作系统、业务系统的安全性，可能会导致业务中断或敏感信息泄漏。可以使得有限用户受到攻击；此类风险如私钥泄露、助记词泄露、密码泄露、SQL注入、验证绕过、未授权的访问、关键业务弱口令、敏感信息泄漏等。

理论上存在一定的危害性，一经利用即可威胁到操作系统、业务系统的安全性，进而威胁到网络的安全性。此类风险如本地缓冲区溢出、非关键业务弱口令、XSS跨站、敏感信息泄漏等。

理论上仅存在相对较小的危害性，并不直接对系统或应用造成危害。一旦被利用时影响相对较小，在测试中通常会为进一步的渗透产生辅助性作用。此类风险如信息泄漏、非关键业务拒绝服务漏洞等。

可能性

根据每个漏洞被触发的条件、被利用的难易程度、受影响的群体大小和被发现的难易程度四个因素计算其实际发生的可能性。可能性的范围为0-1，四个因素的占比如下：



风险分值

综合考虑漏洞等级及可能性，计算出每一评分项对应的风险分值：

风险分值（Risk）= 漏洞等级（Vulnerability）×可能性（Likelihood）

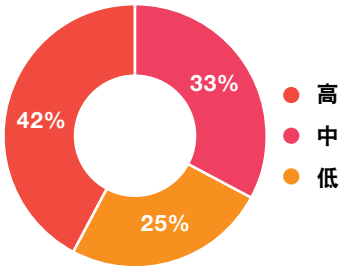
最后由初始分值100分减去所有的风险分值总和，即为其中一个方面的总分，如某一款数字资产钱包在App安全方面的总分如下：

App安全总分 = 100 – ∑（风险分值）

	名称	评分项	漏洞等级	是否存在	可能性（0-1）	风险分值
App安全	私钥安全	私钥的生成算法是否采用可预测的加密因子	严重	不存在		
	助记词安全	助记词生成过程中是否会以明文形式进行网络传输	高	存在	0.5	10
	密码安全	交易密码输入过程中是否可以被复制/粘贴	中	存在	0.3	3
	Keystore安全	keystore是否明文存储在客户端本地缓存	中	不存在		
	客户端自身安全	应用进入后台时，是否删除视图中的敏感数据	低	不存在		
	本地数据存储安全	是否会将钱包登录密码/手势密码明文保存至本地缓存	低	不存在		
	合计总分：App安全总分 = 100 – ∑（风险分值）					87

数字资产钱包黑盒测试

我们的区块链安全研究人员对市场上一些数字资产钱包进行了安全性黑盒测试，对发现的风险进行相关的统计，整体风险分布图如下所示：



静态密钥解密私钥

我们的安全研究人员在测试时发现，有些数字资产钱包，私钥在内存中解密的过程，不是采用主流的交易密码去解密Keystore文件得到私钥的方式，而是采用一个静态的密钥去解密Keystore得到私钥，静态的密钥被写死在代码中，安全研究人员可以通过逆向手段，分析代码流程，找到静态密钥。

代码未进行混淆加固

我们的安全研究人员在测试时发现，有许多的数字资产钱包Android版本的源代码未进行任何的混淆加固，对Android客户端采用反编译的手段可以得到源代码，没有采用任何加固保护，使得攻击者可以很顺利地阅读源代码，从源代码中寻找代码流程方面的漏洞。

无密码转账

我们在测试过程中，还发现有些数字资产钱包在设计流程上也存在一些安全性问题。比如我们发现有些钱包在转账的过程中不需要输入交易密码或者其他任何凭证即可转账成功，这不仅大大降低了攻击者在分析解密私钥时的难度，也使得当用户离开手机的时候，数字资产被攻击者转走的可能性增加。

助记词保护不足

助记词相当于银行卡号+密码，一旦失窃将造成钱包被攻击者窃取。然而我们在测试的过程中发现，多数的数字资产钱包对于助记词的保护不足，可以有多种针对助记词的攻击；有些数字资产钱包将助记词传输至应用日志，攻击者也可以在内存中获取助记词；在输入助记词导入钱包的过程中，许多钱包存在未有效防止键盘记录、截屏等风险。

Keystore本地明文存储

我们区块链安全测试人员发现，有些钱包会将Keystore文件明文存储在本地。这样增加了Keystore文件泄露的风险，Keystore文件一旦被攻击者破解，就相当于私钥的泄露。

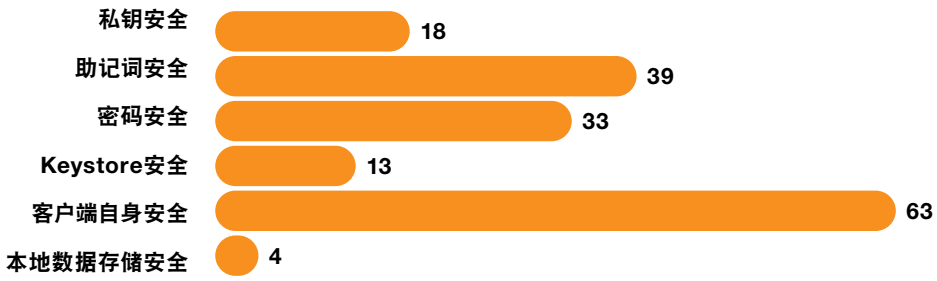
主流数字资产钱包评分

普华永道中国的区块链安全研究人员根据上述数字资产钱包安全评分体系对市场上几款主流的数字资产钱包进行了评分，汇总了各钱包的安全优势和待改进项。选取的主流的6种钱包，在此做了匿名化处理。本次公开的评分仅针对App安全：

操作系统	钱包名称	得分	安全优势	待改进项
Android	钱包A	88	钱包A对代码进行加固，做了反调试、代码注入的保护	助记词安全、密码安全
	钱包B	61	钱包B没有设置私钥和Keystore导入导出功能，一定程度上保护了钱包的私钥和Keystore，且对密码的错误次数做了限制，降低了攻击者暴力破解的风险。	助记词安全、密码安全、客户端自身安全
	钱包C	73	钱包C助记词输入环节采用自主研发的软键盘，降低了助记词在输入过程中被恶意软件记录的风险	客户端自身安全
	钱包D	70	在助记词的保护上，在视图中将助记词用星号代替，降低了攻击者截屏的风险	客户端自身安全
	钱包E	41.5	钱包E可以选择设置锁屏密码，并且每次应用程序退回至后台后，重新切换回来都需要重新输入锁屏密码	私钥安全、助记词安全
	钱包F	62.5	钱包F调用了系统锁屏机制，采用系统锁屏密码解锁钱包	私钥安全、客户端自身安全
iOS	钱包A	78	钱包A增加了指纹登陆的功能，提高了钱包的安全性。	助记词安全、密码安全
	钱包B	暂无	暂无	暂无
	钱包C	86.5	钱包B可以设置指纹解锁和支付，提高了钱包的安全性	客户端自身安全
	钱包D	80	在助记词的保护上，采用输入提示并选择助记词的方式，可以降低攻击者在用户输入的过程中键盘记录、截屏的风险	客户端自身安全
	钱包E	63	钱包E会对锁屏密码的错误次数进行限制，并且做了越狱检测，提示用户越狱之后会有风险	私钥安全、助记词安全
	钱包F	77	钱包F取消了助记词备份恢复钱包，可减少黑客窃取用户钱包的方法	私钥安全、客户端自身安全

经过上述数字资产钱包测评之后，我们的区块链安全团队发现多数钱包在对私钥安全和本地数据存储安全方面做的相对较好，但是对于助记词的保护稍显不足。由于有用户操作的部分参与在内，助记词安全的保护相比私钥要更为复杂，一旦用户操作不当就可能导致助记词的泄露，所以助记词的安全需要引起更多的重视；其次在客户端自身安全性和密码安全也需要进一步加强。

下图为测试中发现的数字资产钱包各类安全问题的数量分布。



后续

在后续的文章中，我们将会给大家带来关于网页钱包、硬件钱包的安全性分析；并且我们已经根据普华永道中国数字资产钱包安全评分体系自主研发了一套数字资产钱包安全的在线检测平台，在后续的文章中将给大家做详细的介绍。

联系我们

我们的团队拥有丰富的数字资产钱包安全评估经验，可以为组织提供专业的数字资产安全评估服务。

网络安全和隐私保护联系人

韦坚信 (Andrew Watkins)
普华永道中国内地及香港首席科技与颠覆技术官

+852 2289 2716
andrew.watkins@hk.pwc.com
Linkedin

中国北区

冼嘉乐
普华永道中国风险及控制服务合伙人

+86 (10) 6533 2937
samuel.sinn@cn.pwc.com
Linkedin

李睿
普华永道中国网络安全和隐私保护合伙人

+86 (10) 6533 2312
lisa.ra.li@cn.pwc.com

中国中区

张俊贤
普华永道中国风险及控制服务合伙人

+86 (21) 2323 3927
chun.yin.cheung@cn.pwc.com
Linkedin

莫威廉 (Ramesh Moosa)
普华永道中国网络安全和隐私保护，咨询服务主管合伙人

+86 (21) 2323 8688
ramesh.moosa@cn.pwc.com
Linkedin

中国南区（包括香港）

黄景深
普华永道中国网络安全和隐私保护，风险及控制服务主管合伙人

+86 (21) 2323 3927
kenneth.ks.wong@hk.pwc.com
Linkedin

颜国定
普华永道中国网络安全和隐私保护合伙人

+852 2289 1935
kok.t.gan@hk.pwc.com
Linkedin

关于我们

普华永道中国网络安全及隐私服务团队凭借其数十年跨行业、地域、技术的实践经验和知识储备，为客户提供端到端组合服务。主要项目包括开展战略性评估、设计、开发和改良网络安全计划等多方面。与此同时，我们与众多企业的相关负责人保持着长期的互信合作关系。

我们的业务可以帮助您开阔网络安全领域的视野，　让您大胆地探索更多可能性。我们将会为您在人才、流程和技术等方面做足准备，应对未来挑战。

pwc 普华永道