黑客瞄上手机银行

随着移动支付的普及，手机银行客户端越来越被用户所认可，很多人觉得，既然是银行的客户端，就应该是非常安全的。然而，事实并非如此。据了解，少数手机银行客户端存在加密机制不完整、不校验服务器身份等安全隐患。不仅如此，我们一直认为最安全的“随机键盘输入密码”也存在不安全的问题。总体而言，银行类手机APP安全状况整体堪忧。

手机银行安全性整体堪忧

作为与支付安全息息相关的环节，手机银行也存在不小的安全隐患。日前，360手机安全中心发布国内首份针对16家主流银行手机客户端(APP)的评测报告——《手机银行客户端安全性测评报告》。经测试发现，少数手机银行客户端存在加密机制不完整、不校验服务器身份等安全隐患。在防范Activity劫持（Activity为安卓系统的一个提供给用户屏幕交互的应用程序组件）、防止进程注入、反盗版/防二次打包以及防止验证短信被劫持等方面，所有16款被检测的手机银行客户端均表现不佳。报告指出，受到安卓系统的体系限制，很多支付安全性问题难以靠手机银行客户端软件单独解决，银行类手机APP整体安全状况堪忧。

手机银行客户端作为网上支付的重要工具，其自身的安全性是网民账户、资金安全的基础。如果手机银行客户端存在安全隐患甚至是安全漏洞，就很有可能被电脑黑客或木马病毒所利用，造成网民银行账户信息泄露和直接财产损失。

报告针对工商银行、建设银行、招商银行、交通银行、中国银行、农业银行等中国16家主流银行的安卓手机客户端展开了一次最全面的安全性评测。测试的主要内容包括：登录机制安全性、键盘输入安全性、Activity组件安全性、进程注入防护、反盗版能力和认证因素安全性的6个主要方面的8项具体测试。

不校验身份或被“攻击”

作为用户使用手机银行客户端的第一步，登录时因为要输入银行账号及密码等敏感信息，安全性尤为重要。在对16款银行客户端的登录机制安全性进行测评的过程中，手机安全专家发现了两类比较严重的安全隐患：一类是加密机制不完整或过于简单，很容易被攻击者劫持或破解；另一类是在通信过程中不对服务端身份进行校验，从而导致登录过程很容易被“中间人攻击”所劫持。其中，有两款手机网银客户端采用了“HTTP+简单加密”的数据传输方式，极易被劫持或破解。

而不论银行客户端使用的是何种登录加密机制，如果客户端在登录过程中不对服务端的身份(证书)进行校验，就有可能“信任”伪装身份的“冒牌服务端”，连接到假冒的银行服务端上，从而导致用户名、密码等信息被窃取，这种假冒服务端身份的攻击，也被称为“中间人攻击”。在测评的16款银行客户端中，共有3款银行客户端(均使用HTTPS加密机制)存在忽略服务端证书校验安全漏洞。

自绘随机键盘并非绝对安全

在键盘输入安全性测试中，安全专家发现，虽然多数手机银行客户端使用了自绘键盘，但自绘随机键盘并未被广泛使用，而且还有两款客户端使用了系统默认的输入法，存在重大的安全隐患。不过，手机安全专家也指出，使用自绘随机键盘虽然能大大提高安全性和黑客攻击的难度，但也并不是万无一失的。如果手机银行客户端被注入了恶意模块，或者系统模块被恶意代码感染等极端恶劣的环境下，攻击者可以通过Hook直接获取到密码明文。

手机银行客户端使用最多的安卓组件是Activity，360手机安全中心对其做了专项安全性测试。在防范Activity劫持、防止进程注入、反盗版/防二次打包以及防止验证短信被劫持等方面，所有16款被检测的手机银行客户端均表现不佳。其中，有一款客户端存在严重的Activity导出风险，另有两款客户端存在Activity导出错误可至系统崩溃的问题。

银行类APP极易被山寨

安卓作为开放平台，攻击者可以较容易地使用逆向分析工具，将银行客户端程序进行反编译，并向反编译结果中加入恶意代码后，发布到一些审核不严格的第三方市场中。这些被二次打包发布的盗版银行客户端软件，对用户的支付安全造成了极其严重的安全威胁。

分析显示，本次测评的16款手机银行客户端均未能完全有效地防范逆向分析和二次打包，虽然一些客户端对自身签名进行了校验，但也很容易在重打包过程中被攻击者轻易篡改，起不到防止二次打包的作用。

测试中还发现，手机银行的认证因素存在一定的安全隐患，16款手机银行客户端软件采用的均是“账号密码+短信验证码”的伪双因素认证体系。这种认证体系在面对具有短信劫持功能的手机木马攻击时，都显得非常脆弱。虽然已经有部分银行开始推广音频盾、蓝牙盾等双因素认证系统，但这些系统的使用不是强制性的，绝大多数用户仍在使用“账号密码+短信验证码”的认证方式。

结合安全软件使用

继银行卡支付，网上支付（PC端）之后，中国消费者已经快速进入了移动支付时代。据CNNIC发布的《第33次中国互联网络发展状况统计报告》数据显示：截至2013年12月，我国手机网民规模达5亿，较2012年底增加8009万人；手机支付用户规模达到1.25亿，同比增长了126.9%，占手机网民总量的25.1%。可见，手机支付用户的增长速度远远高于手机网民规模的增长速度。移动支付的时代已经到来，但安全上的隐患和威胁同样被放大。

针对移动支付面临的种种安全威胁，不少互联网安全企业也与银行展开了安全服务合作，为手机银行客户端提供独立的移动支付安全模块定制服务。该模块被集成到手机银行客户端中，从而全面提升了手机银行客户端的安全性。

手机安全专家指出，目前手机银行客户端有众多安全隐患未能解决，对用户来说，尽量将其与手机安全软件结合使用，以保财产的安全。

延伸：

手机支付病毒暴增

腾讯移动安全实验室日前发布了《2014年上半年手机安全报告》(以下简称“报告”)。报告显示，Android手机病毒在经历了2012~2013年几何式高速增长之后，在2014年上半年逐步趋于平缓，同比增长7.9%。其中，手机支付类病毒进一步蔓延，上半年感染手机支付类病毒用户数达到693.4万，其中可拦截并转发用户支付短信验证码的手机病毒大规模增加，支付类病毒呈现出多种特征融合化发展的趋势。值得注意的是，随着二维码的流行，目前已成为增长最快的染毒渠道，通过二维码传播的病毒，传播比例已达到9%。

此外，随着《中国好声音》第三季的开播，瑞星“云安全”系统监测到了大量仿冒《中国好声音》的中奖类钓鱼网站。瑞星安全专家表示，以热播综艺节目的名义谎称中奖，制作钓鱼网站，是黑客的常用伎俩。一旦网民按照网站上的电话与之联系，骗子就会以“税金”、“快递费”、“保证金”等名目要求网民向其打款，导致用户经济受到损失。

（南方）