基于 3G 网络的手机病毒分析

□ 翁晓奇 李妙旎 于 浚 于 倩

(厦门大学软件学院 福建·厦门 361005)

摘 要：本文介绍了智能手机与手机病毒的发展现状,分析了手机病毒的危害,并结合 3G 网络安全特性,对手机反病毒技术的发展趋势进行论述。

关键词：3G 手机病毒 网络安全

中图分类号：TM93 中图分类号：A 文章编码：1007-3973(2009)09-068-01

伴随着通信产业的不断发展，今天的移动终端已经由原来单一的通话功能向话音、数据、图像综合的方向演变。智能手机以强大的运算储存能力和扩展功能等特点,在 3G 时代进一步得到人们的青睐。然而,伴着手机应用功能的增长,手机操作系统的开放度也随之增大,手机病毒的产生与发展导致信息风险系数增加,已成为不可回避的现实。

1 手机病毒的历史

关于手机病毒的一般定义是以手机为感染对象以手机网络和计算机网络为平台，通过病毒短信等形式对手机进行攻击,造成手机异常的一种新型病毒。第一个真正意义上的手机病毒 Cabir 诞生于 2004 年。Cabir 病毒可以智能地搜索附近已经开启的蓝牙设备，自动建立联系并大量传播病毒副本。在 Cabir 之后,Skull、Commwarrior、Lasco、Locknut、Fontal 等病毒的相继出现,一度引发担忧。随着 3G 市场的放宽,手机病毒的年度增长数量超过过去 10 年的总和。手机所面临的安全威胁很快将超越个人电脑，成为个人信息安全的第一大隐患。

2 手机病毒的危害

手机病毒以手机网络和计算机网络为平台，通过发送短信、彩信、电子邮件,浏览网站、下载,蓝牙设备等方式进行传播并对手机进行攻击。

手机病毒主要带来以下三个方面的危害：

(1)经济方面,通过恶意软件订购 SP 业务、进行恶意的手机支付。感染了病毒的手机会自动拨打声讯台、发送信息、订购增值业务等,造成用户的话费损失。

(2)信息方面,通过通讯录传播病毒,发送恶意信息、不良信息。病毒可以控制用户的手机,调用信息、监听通话、自动联网等,造成用户隐私泄露。

(3)硬件方面,带给手机在硬件方面的损害,使得手机出现死机、运行慢、功能失效等状况。按键失灵、电池耗电量迅速增大,甚至导致手机硬件损坏,致使手机无法使用。

3G 移动通信系统除了提供传统的语音、数据、多媒体业务外,还能支持电子商务、电子支付、股票交易、互联网业务等。涉及了更多的经济利益的同时,也促使了破坏性更大的新型病毒的研制。未来的手机病毒可以利用手机系统漏洞延伸至无线增值服务提供商的后台，通过非法盗取账号信息等手段实现非法盈利。并且当整个行业形成统一的标准的时候,病毒一旦发作就会产生规模效应。

3 3G 网络的安全特性

3G 网络技术主要进行了以下改进：

(1)提供了双向认证。不仅网络对用户进行鉴权,同时用户也对网络进行鉴权，有效防止了伪基站攻击。相对于 2G 的网络单向认证而言,这种双向认证提供了更高的安全性。(2)密钥长度增加至 128 位,并改进了算法。提供了信令信息的完整性保护机制,防止攻击者对信令的篡改。(3)3G 的安全机制具有可拓展性，为将来引入新业务提供安全保护措施;(4)用户可通过安全可视性操作,随时查看自己所用的安全模式及安全级别。

但是,3G 仍存在一定的安全缺陷,面临着复杂多样的安全威胁和攻击。

1)没有建立公钥密码体制,难以实现用户数字签名。密钥产生机制和认证协议有一定的安全隐患。2)网络存在被攻击的可能性。3G 系统的大量数据包括信令、协议认证和密钥交换算法等都是依靠网络传输的，入侵者可能通过各种网络攻击手段来达到窃取的目的。3)终端设备和服务网之间的无线接口存在被窃听、拒绝业务和阻塞业务攻击等风险。

4 手机反病毒技术发展趋势

随着手机病毒的发展，手机反病毒技术的发展将呈现日新月异的变化,主要有以下几种发展趋势：

4.1 手机云安全

手机安全防护面临性能上的限制，这就要求安全防护更具效率。因此相对于运算能力而言,3G 时代的手机安全可以更依赖于网络数据传输。云安全计划融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念,通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息,推送到服务端进行自动分析和处理,再把病毒和木马的解决方案分发到每一个客户端。

4.2 电话防火墙

防火墙在网络网关服务器上运作，在内部网与公共网络之间建立起一个安全网关,保护私有网络资源免遭入侵。可设置不同的拒接情景模式，针对指定类型的联系人设置不同的接听、拒接方案。并可对诸如“响一声”吸费电话等进行识别。

4.3 短信智能过滤

对短信进行黑/白名单或关键字比对。选用黑名单时,短信号码如果在黑名单则直接删除短信，不在黑名单则显示给用户。选用白名单时则进行相反操作。可采用语义特征多层反骚扰引擎技术对垃圾短信进行多层精确过滤，避免黑白名单的缺陷。

4.4 硬件免疫技术

将部分软件和系统集成在一起，存储在只读内部模块中。同时开放一个安全的“沙箱”式的外部运行环境供其他软件的运行,从根本上保证手机硬件以及操作系统的安全。

5 结语

新一代移动通信系统已经到来，如何解决手机病毒所带来的安全问题，怎样提高手机安全防御机制的效率以及对安全机制的有效管理，都将是移动通信系统面临的严峻挑战。基于 3G 网络的手机信息安全,任重而道远。

参考文献：

[1] 刘磊,刘克胜.Symbian 操作系统下手机病毒免疫技术研究[J].应用安全,2006.

[2] 曾勇,舒燕梅.3G 给信息安全带来前景[J].信息安全与通信保密,2009.