浅谈Motorola MPX220手机病毒的攻击方式与防范措施

马 味,曾 科
(西昌学院 信息技术系,四川 西昌 615013)

【摘 要】随着网络技术的快速发展和广泛应用,手机网络的安全正受到严重的挑战。本文分析了Motorola MPX220手机病毒的攻击方式,并给予了有效的防范措施。

【关键词】Web攻击;WAP;蓝牙技术
【中图分类号】TP309.5 【文献标识码】A 【文章编号】1673-1891(2008)03-0089-04

1 引言

Motorola MPX220手机的出现是计算机技术嵌入到手机中的又一产物,跟以往不同的是这次是Windows操作系统的嵌入。Motorola MPX220手机在Windows操作系统的作用下功能更加强大,除了支持Pocket Outlook、Pocket Internet Explorer、MSN Messenger等网络功能外还支持蓝牙技术;简直就是新一代的掌上手机电脑。

然而事物都具有两面性。由于Motorola MPX220手机中某些功能的缺陷及手机网络安全的不健全,导致了攻击者对此款手机的青睐。如Web攻击,主要在手机通过网络浏览页面的过程中链接虚假的页面达到攻击的目的,WAP攻击主要采用类似于邮件炸弹的短信炸弹攻击WAP服务器获取手机内的信息,而蓝牙攻击主要通过猜测并获取PIN码达到攻击的。虽然,这三种攻击都会造成一定的破坏,但只要我们留心并采取一些有效的防范措施就可以化险为夷。从而,充分享受此款手机给我们带来的巨大方便。

2 Motorola MPX220手机病毒

Motorola MPX220手机病毒就是一种类似计算机病毒的病毒,它可以在手机网络上进行传播,也可以通过手机本身的某些功能(如蓝牙功能)进行传播,从而造成通讯网络拥塞,手机内存破坏、收发垃圾短信、窃取用户隐私等[1]。因此Motorola MPX220手机病毒其实就是计算机病毒的另外一种形式,它们都是通过恶意程序攻击手机本身及通讯网络。

3 Motorola MPX220手机病毒的攻击方式与防范

3.1 Wap技术简介

WAP(Wireless Application Protocol无线应用协议)技术已经成为移动终端访问无线信息服务的全球主要标准。它基于Internet中广泛应用的标准(如HTTP、TCP/IP、SSL、XML等),提供一个空中接口和无线设备独立的Internet解决方案。

WAP体系主要由三部分组成:

移动客户端(Client):指安装有微浏览器的无线终端设备,能对WAP网页进行显示、解释、执行;

WAP网关(WAP Gateway):完成HTTP协议向无线Internet传输协议(WSP/WTP)的转换,对无线Internet内容进行压缩和编译。

Web服务器(Web server):与一般的Internet站点类似,区别仅仅是网页编写上采用的语言有所不同,它采用WML(WAP标记语言)语言[2]。

图1 WAP规划模型

根据WAP规划模型,可将Motorola MPX220手机病毒的攻击分为Web攻击、WAP网关攻击及手机自身功能攻击——蓝牙攻击。

3.2 Web攻击与防范

Web攻击是指攻击者建立一个Web站点的拷贝,它具有所有的页面和连接。攻击者控制这个假的Web页,从而使得被攻击对象和真的Web站点之间的所有信息流动都被攻击者所控制。这样攻击者就可以假冒成用户给服务器发送数据,也可以假冒成服务器给用户发送假冒的消息。总之,攻击者可以监视和控制整个过程。

首先,攻击者静态地观察以便获得浏览者所访问的页面以及页面的内容;

其次,实施破坏,即修改来往于浏览者和服务器间的信息;

最后进行攻击,攻击者不会伪装成整个的Web站点,只是采用超文本链接来实现[3]。

攻击的步骤主要分为两步:改写URL和开始攻

收稿日期:2008-06-06
作者简介:马 味(1981-),女,在读硕士,助教,主要从事信息安全方面的教学工作。

击。

第一步,改写URL

攻击者的首要任务是改写某个页面上所有URL,使得这些连接都指向攻击者服务器,而不是真正的服务器。假定攻击者的服务器在机器www.attacker.edu.cn上运行,那么攻击者要在页面上的所有URL前增加http:// www.attacker.edu.cn链接。如原来的URL为http://home.net.com就变成了http://www.attacker.edu.cn或http://home.net.com。

图2给出了当浏览者经过被改写的URL访问页面时发生的情况。因为这个URL以http://www.attacker.edu.cn开始,所以浏览者实际上是请求来自www.attacker.edu.cn的页面,这个URL的后半部分告诉攻击者的服务器去哪里取得真正的文档。

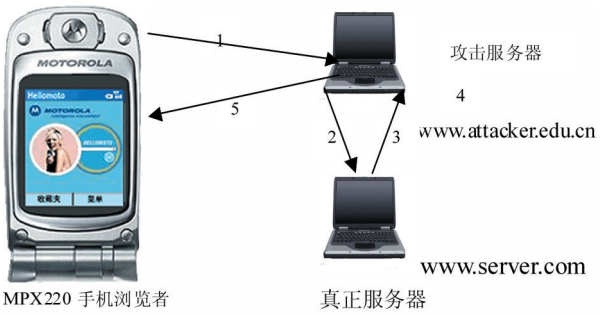

图2 一个Web攻击的例子

①浏览者请求来自攻击服务器的页面;

②攻击服务器请求真正服务器相应页面;

③真正服务器向攻击服务器提供真正的页面;

④攻击服务器重写页面;

⑤攻击服务器向浏览者提供一个经过改写的页面。

第二步,开始攻击

为了开始攻击,攻击者必须诱惑被攻击对象连到攻击者的假的Web上。为了做到这点,攻击者主要采用以下的做法:

攻击者把一个指向假Web页的链接放到一个流行的Web页面(比如www.msn.com)上;此外由于MPX220支持电子邮件系统,那么攻击者也可以向被攻击者对象邮寄一个指向假WAP的指针;或者干脆邮寄给浏览者一页假Web内容。

当浏览者浏览页面时,他实际上是在向攻击服务器询问这个文档,而攻击服务器再去真正的服务器上取回这一文档。一旦攻击服务器从真正的服务器那里得到真正的文档后,它在这份文档的所有URL前加上http://www.attacker.edu.cn来改写该文档,攻击服务器向浏览者提供改写后的文档。从而使得攻击正式开始。这种攻击比较可怕的方面在于只要浏览者激活这个页面上的任何链接,这些链接都会指向攻击者的机器。浏览者于是被陷入攻击者的假Web中,像进入黑洞一样,永远没有逃脱的机会,除非他已经发现被攻击。

虽然这种攻击很有效,但不是很完美。只要浏览者确保地址行总是可见,一旦发现地址不是浏览者要求得到的,就马上关闭Web页面,从而起到防范的作用,此其一。

其二,采用身份验证技术

使用身份验证技术可确保信息的完整性、可控性和保密性。在这里主要通过注册用户名和密码来实现。但要保证注册账户的时效性。不能有死账户,对每个授权的账户(临时用户、员工、管理者等)要有历史记载。另外,密码最好不少于8位、并且采用阿拉伯数字和英语的组合。

其三,加密数据

主要采用非对称加密技术实现。既是公钥加密数据,私钥进行解密,从而达到保护信息的保密性。因为只有公钥的拥有者才能解密,而与该公钥同属一个密钥对的私钥由拥有者安全地保存。

3.3 WAP网关攻击

WAP网关是一个代理服务器,它主要由两部分组成:WAP网关核心子系统和周边子系统。WAP网关核心子系统连接无线网络和因特网,周边子系统提供用户管理与证书认证管理、计费统计、系统日志和网关配置等。

WAP网关攻击就是从WAP网关周边子系统的用户管理模块中获取用户相关信息,通过WAP网关核心子系统实施对用户的攻击。而要想获取用户相关信息就要使用短信炸弹让WAP网关暂时拒绝服务,也就是在很短的时间内连续不断的向WAP网关发送垃圾短信。如同计算机病毒中的邮件炸弹,使得WAP网关在短时间内无法处理大量的短信大量,消耗手机网络资源,导致网络塞车,使大量的手机用户不能正常工作,轻则导致WAP网关的性能下降,重则导致死机或关机[4]。

预防短信炸弹的措施主要有以下的内容:

①WAP网关加入防火墙,可以防止恶意的无线用户对短信服务器进行的破坏活动,实现安全连接。

②采用过滤功能。在短信软件中安装一个过滤器是一种最有效的防范。接收任何短信之前预先检查发送人的资料(先从服务器上下载发送人的手机号码),如果觉得有可疑就直接将它删除,如果收到超过手机短信容量的短信时就自动将它删除。

3.4 手机自身功能攻击——蓝牙攻击与防范

蓝牙技术(bluetooth technology)是一种实现多种设备之间短距离无线连接的协议,通讯速度快,广泛应用于无线设备、图像处理、消费娱乐、汽车产品和家用电器等领域[5]。虽然,蓝牙技术提供了诸如密钥管理、认证和保密等安全机制,但PIN码(个人识别码)长度较短、密码算法简单、IEEE 802.11标准对蓝牙通讯距离的扩展及蓝牙技术的普及,使得蓝牙技术特别容易受到攻击。

蓝牙通讯前双方必须建立连接,这个连接的过程要完成三个步骤:生成初始密钥、生成链路密钥和生成认证密钥。接着,用加密密钥来保护往后的通讯。在建立连接前,需要事先将PIN码输入到蓝牙设备中,PIN是固定不可改变的。如果达到两边PIN匹配则进行通讯。具体过程如表1、表2和表3所示:

表1　A、B设备之间建立连接生成初始密钥

信息	源设备	目的设备	消息	备注
1	A	B	A设备产生的128位随机数IN_RAND	明文传输,并使用E22算法得到初始密钥

表2　A、B设备建立连接生成链路密钥

信息	源设备	目的设备	消息	备注
2	A	B	A设备产生的128位随机数(LK_RANDA)异或初始密钥后的结果	B解开消息得到A设备产生的随机数
3	B	A	B设备产生的128位随机数(LK_RANDB)异或初始密钥后的结果	A解开消息得到B设备产生的随机数
A、B设备分别用E21算法将各自产生的随机数及物理地址进行加密并将结果进行异或得到链路密钥				

表3　A、B设备建立连接生成认证密钥

信息	源设备	目的设备	消息	备注
4	A	B	A设备作为应答方产生的随机数(AU_RANDA)	128位明文传输
5	B	A	B设备作为请求方产生的随机数(AU_RANDB)	128位明文传输
A、B设备都用E1算法将各自得到的随机数和链路密钥及物理地址加密运算生成相同的32位的认证密钥(SRES),连接工作结束				

在这个过程中,我们可以看出,蓝牙技术所用的认证方式属于简单的弱认证方式,其安全性完全依赖于PIN码的保密性。所以,只要破解PIN码就达到攻击的目的。下面就说明如何通过收集必要的消息采用暴力破解方式猜测PIN码的。其步骤如下:

第一步,列举出所有可能的PIN值,如果假定PIN长度为4位,那么可能的PIN取值从0000到9999之间。

第二步,按照顺序取PIN的第一个值,并从消息2中取得B设备的物理地址和IN_RAND,就可以通过E22(注意:E22算法是公开的)算法,计算得到初始密钥。

第三步,根据消息2和消息3,由上面计算得到的初始密钥,反推计算出LK_RANDA和LK_RANDB。

第四步,根据LK_RANDA和LK_RANDB以及两个设备的物理地址等信息,计算得到生成链路密钥。

第五步,由链路密钥和消息4(AU_RANDA),计算得到SRES1同样的,用链路密钥和消息5(AU_RANDB),计算得到SRES2。

第六步,将SRES1和SRES2进行比较,如果相等则给定的PIN是正确的;如果不匹配,回到第二步,取PIN列表的下一个PIN,重复第二步后的步骤,直到找到个正确的PIN为止。

为了避免手机受到蓝牙攻击,可以采用以下方法进行预防。

①关闭手机不必要的蓝牙功能,减少攻击的可能性;

②验证接受的信号,使用复杂的PIN码;

③对设备自身的信息进行加密保护。只允许传送的数据是共享的,其他信息对连接上的所有设备是可见的,但是不可操作的(如复制、修改等)。从而保证了通讯录和存档文件的安全性;

④在通讯的过程中使手机处于隐身状态。

4 结束语

Motorola MPX220手机的出现可以说是手机操作系统的革新,但由于手机网络安全的不健全和手机功能存在的缺陷,导致了严重的安全威胁,故此

款手机的安全防范势在必行。通过本文的讲述，希望大家借鉴Motorola MPX220手机的病毒攻击方式对一般手机的病毒有初步的了解，并有一定的防范意识。

注释及参考文献：

[1]傅建明，彭国军，张焕国. 计算机病毒分析与对抗[M].武汉大学出版社，2004.

[2]张禄林，雷春娟，周彬.WAP技术及其应用[M].北京：人民邮电出版社，2001.

[3]叶丹.网络安全实用技术[M].北京：清华大学出版社，2002.

[4]刘远生，辛一，薛庆水.计算机网络安全[M].北京：清华大学出版社，2006.

[5]严紫建，刘元安.蓝牙技术[M].北京邮电出版社，2001.

An Insight to the Attacking Actions and Precautionary Measures of Motorola MPX220 Mobile Phone Virus

MA Wei，ZENG Ke

（Department of Information Technology，Xichang College，Xichang，Sichuan 615013）

Abstract: With fast development and extensive application of the network technology，the security of the mobile phone network is receiving serious challenge. This article analyzed the attacking actions of Motorola MPX220 mobile phone virus and gave the effectively precautionary measures.

Key words: Web attacking；WAP；Bluetooth technology

（上接85页）

注释及参考文献：

[1]阎菲.实用软件工程教程[M].北京：中国水利水电出版社，2006.

[2]杜义华，张亚.网站信息管理发布系统设计与应用[J].计算机系统应用，2005.

[3]温明等著.ASP 网站建设实录[M].北京：红旗出版社，2005.

The Construction of Enterprise Website

ZENG Ke，MA Wei，LI Jian-jiang

（Department of Informtion Technology，Xichang College，Xichang，Sichuan 615013）

Abstract: With the wide popularization of the computer and Internet，many enterprises have been awared of the importance of the enterprise website to an enterprise's image, marketing and its culture. Gradually, they could provide convenient and fast products information service to customers with the enterprise website. This paper is mainly explaining the whole construction process of an enterprise website.

Key words: Asp；Database；Access