QQ登录协议安全性研究与分析

俞凯[1]，张怡[2]，王勇军[3]
（1.国防科大计算机学院 2.国防科大计算机学院 3.国防科大计算机学院）

【摘要】QQ是国内使用最广泛的即时通信工具，其安全性对于用户安全和网络安全具有重要影响。本文通过捕包分析给出了QQ2008正式版的登录流程，并在此基础上对登录过程中的安全性进行了分析和研究，从中找出了一处比较严重的安全隐患。最后利用该安全隐患，设计了一个有效的攻击方法，并进行了验证。
【关键词】QQ2008 登录协议 登录令牌 密码密钥 会话密钥

在国内即时通信（IM）软件中，腾讯QQ占有IM市场使用用户的90%以上，是目前国内被使用最多的Internet通讯工具。做为IM软件，个人隐私保护是必然要面对的一个问题，所以其安全性也必须要得到充分保证的。本文对QQ（指QQ2008正式版，下同）登录协议的安全性进行了研究，QQ通信协议本身是不开放的，我们参考QQ以前版本的分析资料，采用捕包分析的方法，给出了QQ2008协议登录流程，在此基础上着重分析了QQ协议在登录过程中的安全性。登录过程涉及QQ密码验证和QQ聊天会话密钥的分配与获取，是QQ协议中重要而且关键的一环，该环如果安全可靠则全局的安全就有了强有力的保证，如果该环失效，则牵一发而动全身，洞门大开，基本上没有什么安全性可言。

本文第1部分简单定义涉及到的术语；第2部分阐述了QQ通信协议的格式；第3部分对QQ登录协议进行“黑盒”分析，详细介绍了QQ协议的登录过程，并分析讨论了在登录过程中可能存在的安全隐患，然后利用这些安全隐患的具体攻击实现；第4部分通过实验验证了该攻击实现；第5部分对本文加以总结。

1 术语

首先，本文定义QQ通信协议登录过程中涉及到的主要术语如下：

qqUID：QQ号码，即QQ用户在使用QQ之前，在线在腾讯服务器上申请到的一组阿拉伯数字，这个是识别用户的标志，两个QQ用户进行聊天活动时分别用2个不同的QQ号码作为其个体的标识。目前QQ号码已经申请使用到第10位。

qqPWD：QQ密码。在每一个QQ号码登录到QQ服务器时需要用一个密码来判断该用户的合法身份，在QQ登录时需要输入该QQ密码，QQ服务器会在线验证该QQ密码的合法性，合法则登录成功，动态为该用户分配一个唯一的会话密钥，用于此次QQ活动的加解密过程。

qqTEA：QQ的TEA填充交织算法[8]，QQ采用了标准的16轮TEA（Tiny Encryption Algorithm）算法[1][4]，QQ首先对待加密的明文进行某种方式的填充，结果会在明文的最后生成一定数量的0x00以保证整个长度为8字节的倍数，接着QQ消息被分为多个加密单元，每一个加密单元都是8字节，使用TEA进行加密，加密结果再作为下一个单元的密钥。

M2P：QQ密码密钥。其为QQ密码（qqPWD）进行2次MD5[2][5]后的值，为16字节（M代表MD5，2代表2次，P代表qqPWD）。此密码密钥很重要，用于对服务器发来的包的解密，从而获得会话密钥。

PVS：QQ密码验证串。它是用QQ密码（qqPWD）的2次MD5值（M2P）作为密钥，用qqTEA算法对空字符串进行加密后的值，为16字节。它是客户端发给服务器用于对客户端身份的确认信息，服务器会对该串进行解密，如果解密成功，则为合法的客户端。

PVS'：另外一个QQ密码验证串。它是用QQ密码（qqPWD）的2次MD5值（M2P）作为密钥，用qqTEA算法对“qqPWD的1次MD5后的密文加上4字节的随机字符”进行加密后的值，为32字节。

RandKey：QQ随机密钥。一般由客户端生成，用其加密一段明文后随密文一同发给服务器端，服务器接收后解密得到明文，再发送用该随机密钥加密回应信息给客户端。该随机密钥为16字节。

LoginToken：QQ登录令牌。QQ在登录时需要从服务器上获得一个登录令牌，该令牌为32字节，用于向服务器申请本次QQ活动的临时会话密钥。

SessionKey：QQ会话密钥。此会话密钥极为重要，QQ本次会话的所有信息都用本密钥进行加密和解密，所以本密钥一旦失密，则QQ的聊天信息等就毫无秘密可言，在网络上相当于明文传输。本会话密钥长度为16字节，由服务器生成并发出，客户端需用M2P进行解密才能获得。

2 QQ通信协议格式

QQ的通信协议是腾讯自己开发的一套基于二进制数据的应用层网络协议，QQ通信协议采用了固定的格式，客户端与服务器发送的报文格式上仅有一点点区别。QQ基本通信协议支持udp和tcp两种基本协议方式，两种方式的数据结构基本是一样的，只是tcp包多了一个描述长度的头部。QQ采用了UDP和TCP协议结合的方式来完成QQ的各种任务，大部分情况下QQ

使用的是UDP协议，TCP协议作为其一种补充方式在某些情况下也可被使用。它们的结构如图2.1和2.2所示：

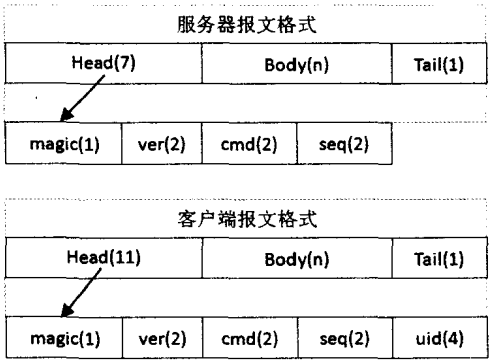


图2.1 基于UDP的QQ通信协议格式

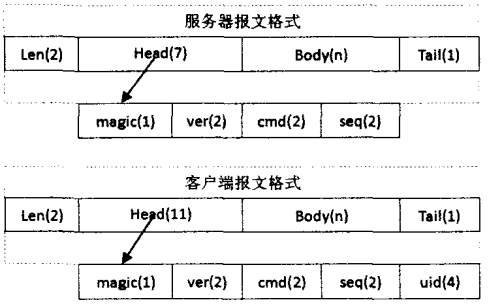


图2.2 基于TCP的QQ通信协议格式

基于TCP的QQ通信协议比基于UDP的只多一个长度域Len，其占用2个字节，指明QQ协议应用层的总长度，单位为字节，我们主要以UDP为例说明QQ的通信协议。基于UDP的QQ通信协议在应用层分为三个域，分别为协议头Head，信息体Body和协议尾Tail。信息体Body根据包的不同内容会有所不同，协议尾Tail占用一个字节，内容固定为0x03，而协议头Head格式分为服务器和客户端二种，格式固定，服务器端的格式分为四个子域，分别为：标志子域magic，版本子域ver，命令子域cmd和序列号子域seq。标志子域magic占用一个字节，内容固定，登录时为0x02，版本子域ver指明QQ的版本，占用2个字节，命令子域cmd占用2个字节，指明本包的作用，序列号子域seq也占用2个字节，指明本包的序列号。客户端的协议头Head格式在服务器端的基础上增加了一个uid子域，占用4个字节，指明客户端登录时使用的QQ号码。

3 QQ通信协议登录过程及其安全性分析

QQ通信协议的登录过程是一个复杂的过程，其中涉及多种算法的运用和各种密钥的转换，最终目的是QQ服务器协商分配一个临时会话密钥给QQ客户端使用，用于QQ客户端本次QQ会话的加解密活动。

QQ通信协议的登录过程是从用户输入QQ号码和密码后点击“登录”按钮后开始的，从先到后按命令子域cmd可以分为以下几个过程：Touch过程、PreLoginToken过程、LoginToken过程、PreSessionKey过程、SessionKey过程，其命令子域值分别为：0x0091、0x0062、0x00ba、0x00dd、0x0022。每个过程又分为Request（由客户端发出）和Respond（由服务器发出）2个子过程。

(1)Touch_Request：客户端先产生一随机密钥RandKey1，然后用此密钥加密15字节的0x00，将RandKey1和加密后的密文封装在QQ报文的Body域中发送给服务器。

(2)Touch_Respond：服务器接受到Touch_Request后，用客户端产生的随机密钥RandKey1加密2个字节的0x00作为信息主体，放入Body域，封装好后发回给客户端，表示Touch成功。

(3) PreLoginToken_Request：客户端用1个字节的0x00作为信息主体填入Body域后发送到服务器，表示请示一个QQ预先登录令牌。

(4) PreLoginToken_Respond：服务器接受到QQ预先登录令牌请求后，生成一个24字节长的QQ预先登录令牌PreLoginToken，在其前面放上2字节的长度信息(0x0018)，整个作为信息主体填入到Body域后发因给客户端。

(5) LoginToken_Request：接着客户端生成一新的随机密钥RandKey2，然后加该随机密钥加密上一步得到的PreLoginToken和一些附加信息，将RandKey2和加密后的密文作为信息主体Body发送给服务器，作为对QQ登录令牌的请求。

(6) LoginToken_Respond：服务器接受到请求后，生成一个QQ登录令牌LoginToken，用RandKey2加密该登录令牌和一些附加信息后发回给客户端，作为对客户端请求的响应。

(7) PreSessionKey_Request：客户端收到服务器的回应后解密获得LoginToken，然后随机生成一个随机密钥RandKey3，再用RandKey3加密LoginToken、密码验证串PVS’以及一些附加信息，将RandKey3和加密后的密文作为信息主体Body，封装好后发送给服务器，作为QQ预先会话密钥PreSessionKey的请求。

(8) PreSessionKey_Respond：服务器接收到请求后，随机生成一个QQ预先会话密钥PreSessionKey，然后用QQ用户的M2P加密该密钥和一些附加信息，再发回给客户端。

(9) SessionKey_Request：客户端收到回应后用M2P解密回应报文得到PreSessionKey，然后用PreSessionKey加密QQ密码验证串PVS和一些附加信息，将密文填充至Body域后发送到服务器，表示对SessionKey的请求。

(10) SessionKey_Respond：服务器接收到请求后，先用PreSessionKey解密报文，得到密码验证串PVS，然后用M2P对PVS进行解密，如果解密成功，则生成一个随机的会话密钥SessionKey，用M2P加密该会话密钥和一些附加信息后填入Body域发送到客户端。

由此可以看出，QQ的盾做得足够坚固，但世界上没有戳不破的盾，QQ也不例外。仔细分析可以发现，QQ登录过程的致命伤来自第7步，即PreSessionKey_Request这个过程。RandKey3是和用RandKey3加密后的密文一起发送的，即密钥和密文在同一个报文中。所以我们可以先用这个密钥RandKey3来对密文进行解密，得到相应的明文：LoginToken和PVS’及一些附加信息。根据对PVS’的描述，PVS’是用M2P作为密钥，使用qqTEA算法进行加密后的一段密文信息。分析一下qqTEA算法可以得出：通过qqTEA的解密过程可以来判断解密密钥是

否正确。而且不仅如此，最致命的是qqTEA可以不用真正等用密钥解密完密文才可以判断密钥的正确与否，只需以密文中倒数第2个8字节为密钥用16轮的TEA解密一下密文的最后8字节，判断解密后的内容中是否存在一定数量的0x00就可以知道该密钥是否是正确的，即可以提前返回错误，这大大加快了判断密钥是否正确这一进程的速度，从而给暴力破解制造机会。

至此，我们可以对QQ通信协议的登录过程构造一个有效的攻击方法：字典暴力攻击。攻击过程描述如下：

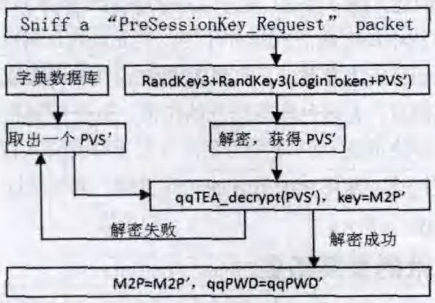
（1）构造一个字典数据库[11]。库中表只有两个数据域，qqPWD和M2P，qqPWD的数据内容为常用的QQ密码，这个可以通过统计得到，M2P的数据内容为qqPWD的2次MD5后的值

（2）通过进行网络监听获得QQ用户登录的PreSessionKey_Request过程数据包。这个可以通过局域网监听或者做个QQ代理等方式获得；

（3）用RandKey3解密PreSessionKey_Request数据包，获得32字节的PVS'；

（4）从数据库中取出每个M2P作为密钥，利用qqTEA算法对PVS'进行解密，如果是错误的密钥立即返回（不用全部解密完），换下一个密钥重新解密，直至解密成功为止。如果解密成功，则攻击成功，从数据库中即可获得用户的QQ密码qqPWD。

攻击过程示意图如图所示：



QQ通信协议登录过程攻击示意图

4 QQ协议攻击实验

为了验证以上攻击方法的可行性，设计组建了一个实验环境。该实验攻击环境如图4.1所示：

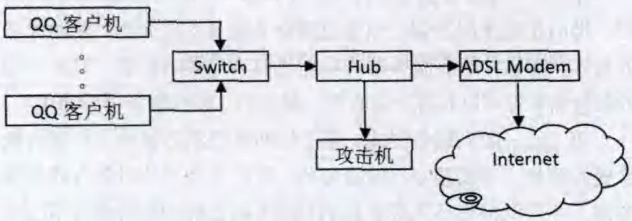


图4.1 攻击环境示意图

需要说明的是，因为在交换机上不能捕获到局域网内其它机器的数据包，故在交换机和上网的ADSL Modem间串接一个Hub，然后在Hub上接上攻击机器，用于实时捕获其它机器的数据包。

攻击计算机配置为：操作系统为Windows XP，CPU为AMD Athlon 3200+，512M内存，80G硬盘，安装的软件有：winPcap4.1，MySql5.0和VS2005。首先，采用了MySql5.0制作生成一个字典数据库，然后，用VS2005和winpcap4.1编写了一个捕包攻击软件安装于攻击机器上，实现自动捕包分析并产生攻击，攻击成功后，在线监控QQ客户机的聊天内容。实验结果令人满意。对于简单的QQ密码（如生日数字，手机号码，英文名等）和简单的字母数字组合密码（如123abc等），该攻击方法非常成功；对于密码长度较长的密码（长度在8位以上）和密码强度较强的密码（如d*0&La之类综合大小写字母，数字和标点符号的密码），破解时间会较长，难于即时通过暴力破解得到QQ密码。虽然如此，但由于网络上充斥着大量的QQ弱口令用户，这些QQ用户为了口令的方便好记，往往采用自己的生日，电话号码或将其经过简单的变形后作为QQ密码。所以该攻击方法是有效的，会对QQ协议安全性产生严重的威胁，所以我们对于这个QQ登录协议的安全问题必须给予高度的关注。

5 结束语

本文对QQ通信协议的登录过程进行了较为详细的研究与分析，在研究和分析的基础上，深入探讨了QQ登录过程的安全性，从中找到了一处QQ通信协议在登录过程中可能存在的严重安全隐患，并根据该安全隐患，设计了一种对QQ登录协议的攻击方法。接着，对该攻击方法进行了必要的论述，得到了若干有指导意义的结论，并通过实验对该攻击法进行了必要的验证，最后得出的结论是该攻击方法是正确有效的，确实会对QQ登录的安全造成较大的安全方面的影响。（责编 马华）

参考文献：
[1] 吴世忠 译，应用密码学（协议算法与C源程序），机械工业出版社，2000年1月
[2] 杨晓元 著，计算机密码学，西安交通大学出版社，2007年3月
[3] 邱仲潘 等译，密码学与网络安全，清华大学出版社，2005年09月
[4] Nikolai Shokhirev,TEA Encryption Algorithm Source,2007.02.07
[5] RFC1321,The MD5 Message-Digest Algorithm,MIT Laboratory for Computer Science and RSA Data Security, Inc.,April 1992
[6] Hans Delfs & Helmut Knebl，密码学导引：原理与应用，清华大学出版社，2007年10月
[7] 腾讯QQ安全频道，http://im.qq.com/safe/index.shtml
[8] QQ的TEA填充算法C#实现,Red_angelX,2006-09-19 http://blog.csdn.net/Red_angelX/archive/2006/09/19/1246701.aspx
[9] QQ密码获取及聊天还原分析，team509,2005-06-20 https://www.xfocus.net/bbs/index.php?act=ST&f=3&t=51411
[10] QQ登录协议分析图,rgbsky, 2008-04-07,http://bbs.pediy.com/showthread.php?t=62660
[11] 利用数据库来破解md5,KBUG,2000-02-04 http://www.bitscn.com/hack/article/200607/45437.html
[12] QQ的工作原理及加密方式,dds1999,2008-07-03 http://blog.54master.com/index.php/438198/viewspace-32020

作者简介：俞凯，男，1976年生，硕士研究生，研究方向：网络信息安全；张怡，女，1973年生，副研究员（硕导），研究领域：网络信息安全；王勇军，男，1971年生，研究员（博导），研究领域：网络信息安全。