第 35 卷　第 13 期　　计　算　机　工　程　　2009 年 7 月
Vol.35　No.13　　Computer Engineering　　July 2009
·安全技术·　文章编号：1000—3428(2009)13—0134—03　文献标识码：A　中图分类号：TP393.08

eMule 协议的安全性研究

刘简达，施　勇，薛　质
(上海交通大学信息安全工程学院，上海　200240)

摘　要：研究 eMule 协议在安全性设计方面所存在的缺陷和不足，指出 eMule 软件在用户隐私泄露、用户积分欺诈和恶意代码攻击 3 个方面对用户造成的风险，给出改进方案。针对 eMule 协议在 Ed2k 链接格式上的 2 个漏洞提出一种新的攻击方式，设计攻击流程，并进行模拟攻击实验，实验结果表明该攻击方式的成功率达到 100%。

关键词：安全保密；eMule 协议；网络攻击；P2P 技术

Research on eMule Protocol's Security Characteristic

LIU Jian-da, SHI Yong, XUE Zhi
(School of Information Security Engineering, Shanghai Jiaotong University, Shanghai 200240)

【Abstract】This paper studies the limitation and shortage of eMule protocol's security design. Based on the study, the eMule software can bring risk to users in three aspects such as privacy leaking, credit cheating and malicious code attack. The suggestions for improvement are proposed accordingly. A new attack method which is based on two leaks of the Ed2k link format is established. It designs the attack flow, and an attack simulation experiment is processed, which shows that the success ratio of this attack method is 100%.

【Key words】security and secrecy; eMule protocol; network attack; Peer-to-Peer(P2P) technology

eMule 作为世界上使用者最多、资源最可靠的 P2P 文件共享客户端软件，在全球已经拥有了数千万的用户，对于这样一款广泛使用的软件，人们在关注它的功能性的同时，却往往忽视了其安全性。而 eMule 作为一个开源项目，一旦存在安全隐患，很容易被攻击者发现并利用该隐患开发出相应的攻击手段。本文将从安全分析的角度出发，提出 eMule 可能存在的安全问题，并给出解决这些问题的改进方案。

1　用户隐私泄漏问题

1.1　协议保密性缺陷

当使用 eMule 下载一个文件时，可以看到同时拥有并共享这个文件的用户的列表，而且选择其中一个用户，还可以查询这个用户共享的所有文件的完整列表，如图 1 所示。

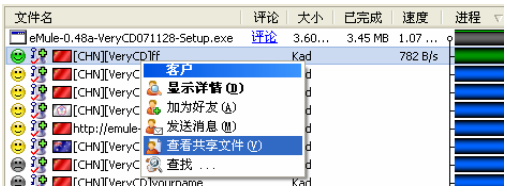

图 1　eMule 下载示意图

事实上，作为一个 P2P 文件共享软件，其基本原则就是所有共享的文件都是用户自愿提供的。当其他用户提出下载一个共享文件的请求时，让他知道这个共享文件是否有资源、是否可以下载是必须的；但是同时告诉他哪些用户拥有此共享文件的副本，这些用户还有哪些其他的文件可以下载，就属于泄漏这些提供共享的用户的个人隐私。

更为严重的一点是，eMule 也没有保护好用户的 IP 地址。当一个用户使用 eMule 下载时，通过“netstat－a”命令就可以查询到正在传送给他文件的其他用户的 IP 地址。这样造成的后果是一旦 eMule 客户端发现安全漏洞(例如在 2003 年曾经发现的 eMule 某些早期版本中的 AttachToAlreadyKnown 模块内存双释放漏洞[1])，攻击者将可以利用这些漏洞有选择地攻击特定的目标，这样造成的危害要大大高于攻击者漫无目的的攻击。由于 eMule 对其他用户提供下载的过程是不受使用用户控制的，因此除非不使用 eMule，不然无法避免将自己的 IP 地址暴露给其他人的情况发生。

上述的这些用户隐私泄漏问题，都是和 eMule 的网络协议设计分不开的。eMule 客户端必须连接到一个服务器来取得网络服务，而服务器使用一个内部数据库来存储关于客户端和文件的信息。服务器本身不存储任何文件，它只为关于文件位置的存储信息作集聚索引。eMule 客户端还需要连接到多个其他的客户端完成文件的上传和下载。eMule 网络结构示意图如图 2 所示。

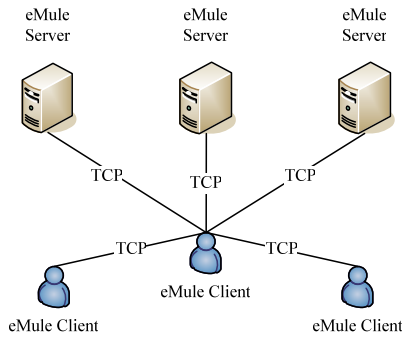

图 2　eMule 网络结构示意图

基金项目：国家“863”计划基金资助项目(2006AA01Z403)
作者简介：刘简达(1985－)，男，硕士研究生，主研方向：网络攻防；施　勇，讲师；薛　质，教授
收稿日期：2008-12-22　**E-mail：**liujianda@gmail.com

eMule 的用户不单单和可信任的服务器发生通信，还要和不可信的其他客户端发生直接通信，这样的网络结构决定了 eMule 不可能很好保护用户的隐私，而这也是现有 P2P 网络的通病。针对这一问题，近年来有人设计了匿名的 P2P 网络，通过中间层，或者加密通信、地址伪装等手段，隐藏客户端用户的信息。目前匿名 P2P 网络的构建主要是基于 Tor, Freenet 以及 I2P 这 3 种网络中间层[2]。使用 BitTorrent 和 Tor, I2P 共同构建的匿名 P2P 网络已经有了实际应用。eMule 也可以增添这方面的功能。当然，事务都有其两面性，匿名的 P2P 网络也是有缺陷的，它对用户来说更加难以使用，并且会使警方在记录非法版权资料的传播时遇到困难，而且匿名 P2P 网络的传输效率肯定比现有的 P2P 网络有所降低。

1.2 间谍服务器攻击

从 2005 年起，eMule 遇到了严重的间谍服务器问题。eMule 网络中突然出现了很多新的服务器，这些服务器的地址一般和一些知名的 eMule 服务器相近。例如某知名 eMule 服务器的 IP 地址是“193.138.231.142”，而一个已知的间谍服务器的 IP 地址是“193.138.231.210”[3]。这些新的 eMule 服务器表面上看起来和普通服务器没什么区别，用户连接上去以后也能实现基本的下载功能，但实际上它们会暗中记录用户的所有行为，包括用户的下载、搜索、共享等。这样一些严重侵犯用户隐私的服务器就被称为“Fake Server”，也即间谍服务器。目前还没有能自动识别间谍服务器的方法，虽然人们也找出了很多间谍服务器不同于普通服务器的特征，但是间谍服务器也会不断地改进自己的策略，使人们无法用自动的手段区别出间谍服务器与普通服务器。而只依赖手动方式的后果是总会有一部分缺乏经验的使用者遭到了间谍服务器的监视。

要想避免遭受间谍服务器的侵害，首先在 eMule 客户端中设置“仅自动连接到静态服务器”，这样会使 eMule 在连接时只连接到某几个指定的服务器。然后在 eMule 的安全设置中，加入一个 IP 过滤列表。这一列表是非官方的，只能由第三方来更新，其中包含了已知的间谍服务器的 IP 地址。有一家名为 bluetack 的英国公司，维护着一个较完备的列表，可以到该公司的网站上下载这一 IP 过滤列表文件。上述的安全措施，都会损害 eMule 的工作效率，而且由于更新过滤列表属于后向性防护，无法做到第一时间的防护，因此还是不能从根本上解决用户的隐私泄漏问题。

2 用户积分欺诈问题

eMule 是一款 P2P 文件共享软件，这就意味着对于某一用户共享的某一文件来说，同一时间可能有多个下载请求，而每个用户的网络带宽和计算能力是有限的，没法全部满足这些下载请求，这就需要一个排队算法来区分满足不同下载请求的先后顺序。为了鼓励更多的上传，使软件得到更广泛的应用，eMule 建立了一套积分系统。当你上传的文件越多时，你的积分就越高，从而当你下载文件时，你在下载排队序列中的排号就越靠前，可以优先下载资源[4]。虽然积分系统是解决下载排队问题的好办法，但是 eMule 的积分系统存在 3 大缺陷：

(1)积分不是所有服务器之间通用的

积分仅仅通用于产生并承认这些积分的服务器和客户。例如一个用户在服务器 A 的上传量很大，那么他在连接到服务器 A 时，下载文件会比较顺利。但是当他转移到服务器 B 时，他之前的那些积分就失效了。

(2)积分不存储于本机

在 eMule 的程序文件夹中，有一个名为“clients.met”的文件，存放的是该用户所承认的所有其他用户的积分，而不是该用户自己的积分。如果删除这个文件，其他用户在下载这一用户的共享文件时，就无法再享受之前的积分了。eMule 为了防止误删“clients.met”文件，专门生成了一个“clients.met.bak”文件作为备份。但是对于蓄意的积分欺诈行为，eMule 就无能为力了。

(3)积分可以不通过安全认证

eMule 使用了一套非对称密钥体系来认证用户的积分，可以保证用户的积分不被冒用或偷窃。但不幸的是，这一安全认证不是强迫执行的，用户在选项设置中可以取消这一认证。虽然在正常情况下，取消这一认证意味着用户之前的积分得不到承认，但是对于试图进行积分欺诈的用户来说，取消这一认证意味着通信流程的简化，使得积分欺诈成为可能。

利用这些缺陷，攻击者在 eMule 开源代码的基础上开发出很多 eMule 的修改版客户端，例如被称作“吸血驴”的 Vagaa 等。这些恶意客户端可以生成多个用户 ID 并假冒不同的 IP 地址和端口下载同一个文件。它们还可以自动生成伪造的热门文件，引诱其他用户下载，虽然之后其他用户会发现他们下载的并不是他们想要的文件，但恶意客户端已经获得了积分。恶意客户端还只上传自己可以交换到对方下载的数据(credit shaping)。

防止这些恶意客户端的攻击，一方面要采取隔离的办法，在 eMule 服务器上禁止这些恶意客户端的登录，在 eMule 客户端上禁止建立与这些客户端的连接。但是恶意客户端也会做出相应的伪装，例如 Vagaa 就把自己伪装成 eMule 0.47a 官方版。另一方面要改进 eMule 的用户积分体系，加强用户身份的安全认证，例如和计算机硬件相关联，并且对共享文件提供一定的预览功能，帮助用户鉴别伪造的文件。

3 恶意代码攻击问题

eMule 的主要功能是下载各种各样的文件，所以，恶意代码的制造者也必然希望能够通过 eMule 来传播他们的恶意代码。例如攻击者通常会给病毒或者木马取一个热门文件的文件名，或者放到一个压缩包里，然后放到 eMule 上来共享。但是这种攻击方式对于那些拥有良好使用习惯的用户来说，还是不起作用的。一个使用习惯良好的用户可以只通过一些信任度较高的网站获得 Ed2k 链接，而且不会盲目下载那些看上去热门的文件。尽管如此，eMule 仍然不是绝对安全的，下面介绍 2 种可能的攻击手段。

(1)利用 eMule 文件校验漏洞攻击

首先介绍一下 eMule 的文件校验体系。在 eMule 网络中共享的文件都要用唯一的 Hash ID 来标识。eMule 对于 Hash ID 的使用包含 2 个方面，它不仅是作为文件的唯一标识，而且在 eMule 下载文件时，还要使用 Hash ID 来校验文件的正确性和完整性。Hash ID 的生成和校验使用的算法是一致的——都是对文件分块(每 9.28 MB 分为一块)进行 MD4 散列运算再组合的结果。

eMule 文件校验体系的缺陷就在于 MD4 散列算法已经不是一种绝对无碰撞的散列算法，而 eMule 仍然在使用它。使用文献[5]中的代码，就可以在有限的时间内用普通的 PC 机计算出一个 MD4 散列的碰撞情况，类似的 MD4 散列碰撞生成器还有很多。这就意味着攻击者完全有机会使一个包含恶

意代码的文件与一个正常的文件拥有相同的 Hash ID 值，或者在一个原本正常的文件中，选择 9.28 MB 大小的一段，替换为一段恶意代码的数据，而不改变文件的 Hash ID。这样一些经过修改的文件，就可以加入原本正在下载这一文件的共享用户集合中，得到快速而无阻碍的传播。

虽然出现这种攻击的可能性较低，但是 eMule 也应该做出针对性的调整。一方面 eMule 可以选择安全性更好的散列算法；另一方面，减小文件分块的长度甚至使用变长的文件分块算法也可以较大地减低遭受此种攻击的可能性。事实上在 eMule 系统中还支持一种叫做根 Hash 的文件校验方法，文件分块大小为 180 KB，使用 SHA-1 散列算法，目前是 eMule 传输协议中的可选部分，不是必需条件，仅用于纠正文件下载时出现的错误。可以考虑逐渐以根 Hash 校验替换原有的 Hash ID 校验。

(2)通过链接欺骗手段攻击

通过找到文件散列的碰撞来实施攻击的可行性可以说还只是停留在理论阶段，而下面将提出一种通过链接欺骗手段的攻击方式，这种攻击方式经过实验证实是切实可行的。

对于任意一个 Ed2k 链接，只修改其中的文件名得到一个新的链接。通过本文的实验证明，eMule 还是可以使用这个新的链接成功地下载到原来的文件，只不过文件在下载到本地后被重命名了。这说明在 Ed2k 链接中，文件名和文件的 Hash ID 并没有建立一个一一对应的关系，而是完全剥离开的。eMule 这样设计 Ed2k 链接的格式，是为了使文件的共享不会因为用户对文件名的改变而受到影响。但是这样的设计却使用户无法从 Ed2k 链接中判断这个文件的真伪，而且 eMule 也没有任何预先验证的机制，留下了极大的安全隐患。例如攻击者可以把木马执行文件的文件名设为“eMule-Setup.exe”这样类似于 eMule 安装文件的文件名，然后通过在各种论坛、公告板发布 Ed2k 链接的方式，传播恶意代码。而且用户在使用 eMule 内建的搜索功能搜索时，也可能误下了含有恶意代码的文件。

如果说上述欺骗手段对于谨慎的用户来说还是可以分辨的话，那么下面这一种欺骗方式用户就很难分辨了。在 0.42 以后的 eMule 版本中，为了提高下载成功率，eMule 在 Ed2k 链接中加入了对 HTTP 链接的支持。如果链接中包含了该文件的 HTTP 地址，eMule 就可以通过 HTTP 协议下载到这个文件。这一设计包含 2 个问题，第一是由于提供下载的一方是 HTTP 服务器，因此 eMule 无法再使用它的分块校验的协议，只能等文件全部下载完后再进行校验；第二是 HTTP 链接本身包含更大的欺骗性，完全可以通过与 DNS 劫持相结合的方式，使用户在误以为可信的情况下，下载到包含恶意代码的文件。

基于上述的 2 种链接欺骗手段，本文设计的攻击流程如下：首先假设用户认为“www.skycn.net”是一个可信任的站点，从而信任给出的包含“www.skycn.net”的 Ed2k 链接，然后对这个用户所在的区域实施 DNS 劫持攻击，把“www.skycn.net”这个域名的解析转移到由本文所架设的 HTTP 服务器上，这样用户将通过本文给出的 Ed2k 链接下载到预先准备的包含恶意代码的文件。整个攻击的示意图如图 3 所示。

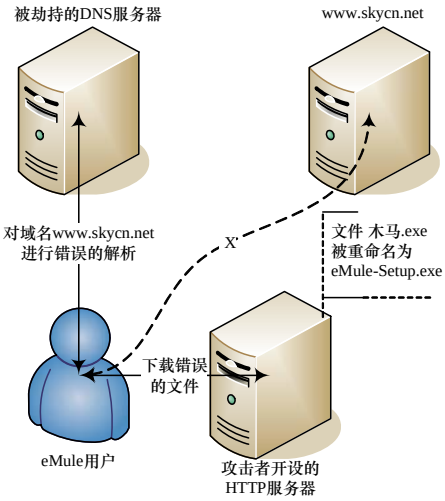

图 3　链接欺骗攻击示意图

在实验室中对此攻击过程进行了模拟。实验结果表明，一旦 eMule 用户选择了下载本文给出的欺骗性链接，下载到本文提供的恶意代码的成功率为 100%。由于 DNS 劫持可以只改变个别域名的解析，因此这一攻击过程用户几乎是无法察觉的。

总体而言，eMule 的下载链接存在较多安全隐患，而且没有为用户提供任何下载前验证来源可靠性的手段。建议在 eMule 中加入第三方的 Hash ID 验证机制，通过建立黑名单的方式为用户提供下载前的安全验证服务。

4　结束语

P2P 技术由于其高效率、低门槛的特点，得到了快速的发展，但当其应用逐渐广泛后，其安全设计不完善的缺点也逐步暴露了出来。希望 P2P 应用的安全问题也能得到越来越多的重视，否则安全问题必将成为 P2P 技术的发展瓶颈。笔者将继续对 eMule 以及其他 P2P 下载软件的安全问题进行深入的研究，并寻求完善其安全性的技术和方法。

参考文献

[1] 绿盟科技. eMule 客户端 AttachToAlreadyKnown 内存双释放漏洞[EB/OL]. (2003-08-22). http://www.nsfocus.net/index.php?act=sec_bug&do=view&bug_id=5313.

[2] Nash A L. Attacking P2P Networks[EB/OL]. (2005-12-16). http://wwwcsif.cs.ucdavis.edu/~nash/235/attacking_p2p_networks.pdf.

[3] eMule-Security. eMule Fakeserver List[EB/OL]. (2008-03-22). http://upd.emule-security.net/fakeservers.txt.

[4] eMule-Project. eMule FAQ[EB/OL]. (2005-06-15). http://www.emule-project.net/home/perl/help.cgi?l=1&cat_id=276.

[5] Stach P. MD4 Collision Generator[EB/OL]. [2008-03-23]. http://www.stachliu.com/md4coll.c.

编辑　任吉慧