FTP安全考虑

本备忘录状态

本备忘录提供了 Internet community 的信息，但不说明任何一种类型的 Internet 标准。发布本备忘录不受限制。

版权声明

概要

文件传输协议（FTP）规范中包含了一些可以缓解网络安全的机制。FTP规范允许一个客户端命令一台服务器给第三方的机器传送文件。这种三方机制，已知的如代理FTP，引起了一个广为人知的安全问题。FTP规范还允许无限次地尝试输入用户密码。这样就允许恶意的“口令猜测”攻击。本文为系统管理员和执行FTP服务器的人提供了一些减少有关FTP的安全问题的意见。

1介绍

文件传输协议规范（FTP）[PR85]提供了一种机制，允许客户端建立FTP控制连接，并在两个FTP服务器之间传输文件。这种“代理FTP”机制能减少网络的流量；客户端命令一台服务器传输一个文件到另一台服务器，比先把文件从第一台服务器传到客户端然后再从客户端传送到第二台服务器要好。当客户端是用很低的速率（比如调制解调器）连接到网络上时这种方法就显得非常有用了。在获得好处的同时，代理FTP带来了一个已知的“跳转攻击” [CERT97:27]的安全问题。另外使用跳转攻击，FTP服务器还会被攻击者恶意地猜测密码。

本文不讨论当FTP和像IP安全这样的强壮安全协议联合使用时的情况。它们也应被编成文档，虽然它们不在本文的讨论范围内。

本文为FTP服务器执行者和系统管理员提供如下信息：第二节讲述了FTP“跳转攻击”。第三节提出了把跳转攻击减小到最少的建议。第四节为基于网络地址有限访问的服务器提出了建议。第五节提供了限制用户恶意“口令猜测”的建议。接着，第六节简要讨论了改善保密性的建议。第七节提供了防止用户身份猜测的建议。第八节讨论了端口盗用。第九节讨论了其它跟软件漏洞有关而跟协议本身无关的FTP安全问题。

2跳转攻击

FTP标准规范[PR85]版中提供了一种攻击已知网络服务器的方法，这使得攻击者很难被跟踪。攻击者发送一个FTP“PORT”指令给FTP服务器，其中包含该主机的网络地址和被攻击的服务的端口号。这样，最初的客户端就能命令FTP服务器发送一个文件到被攻击的服务器。这个文件将包含

被攻击服务器的相关指令（SMTP，NNTP，等等）。命令一台第三方机器连接到服务器，比跟踪直接连接的攻击者要困难，而且攻击者也能绕过基于网络地址访问限制的约束。

举个例子，客户端上传了一个包含SMTP指令的文件到一台FTP服务器。然后，客户端使用一个适当的PORT指令，命令服务器打开一个与第三方服务器的SMTP端口的连接。最后，客户端命令服务器传输那个包含SMTP指令的的文件到第三方服务器。这就允许客户端可以在不进行直接连接时就可以在第三方机器上伪造邮件。这使得跟踪攻击者变得很困难。

3避免跳转攻击

最初的FTP规范[PR85]假定数据连接是通过文件传输协议（FTP）[Pos81]来进行的。0-1023端口号保留给知名的服务，比如邮件，网络新闻组和FTP控制连接[RP94]。FTP规范对数据连接没有限制其端口号。因此，使用代理FTP，用户就可以在任何的机器上获得命令服务器去攻击已知服务器的能力。

为了避免跳转攻击，建议服务器不使用小于1024的端口号进行数据连接。如果服务器收到一个包含小于1024的FTP端口号的PORT指令，建议给出504回应（在[PR85]中定义为“使用该参数指令无法执行”）。注意，这样还是遗留了一些易于受到攻击的不知名服务器（它们使用大于1023的端口号运行）。

一些建议（比如[AOM98]和[Pis94]）提供了允许使用除了TCP以外的其他传输协议来进行数据连接的机制。当使用这些协议时同样要采取预防措施以保护已知的服务。

也要注意跳转攻击一般需要攻击者能够上传一个文件到FTP服务器并稍侯下载它到被攻击的服务器。使用适当的文件保护会预防这种行为。尽管如此，攻击者还是可以通过从远程FTP服务器发送一些随机数据来攻击服务器，以引起某些服务的问题。

为了避免跳转攻击，禁止PORT指令也是一种选择。大多数文件传输可以仅通过PASV指令[Bel94]就可以实现。禁止PORT指令的缺点是失去了代理FTP的功能，但是代理FTP在一些环境下可能是不需要的。

4受限制的访问

对一些FTP服务器来说，限制基于网络地址的访问是必要的。例如，服务器可能要限制确定地域对一些确定的文件的访问（比如，某些文件不能被传送到组织以外）。在这样的情况下，服务器在发送受限的文件之前，应先确认远程主机的控制连接和数据连接地址都在组织之内。通过对这两个连接的检查，就可以避免当控制连接是一个已知的可信任的主机而数据连接却不是的情况。同样地，客户端也应该在接受监听模式下的开放端口连接后，检查远程主机的IP地址，以确保连接是由所期望的服务器建立的。

注意，基于网络地址的限制访问还是遗漏了易于受到“spoof”攻击的服务器。在spoof攻击中，例如，一个用来攻击的组织以外的机器可以伪造组织内的其他机器的地址并下载文件。无论何时，只要在可能的情况下，就应该使用类似于[HL97]中描述的安全鉴别机制。

5保护密码

为了减小通过FTP服务器进行恶意口令猜测的风险，建议服务器限制尝试输入正确口令的次数。在几次（3-5）尝试之后，服务器将关闭与客户端的连接。在关闭连接之前，服务器必须给客户端发送一个421返回码（“服务无效，关闭控制连接。” [PR85]）。另外，建议服务器在回复非法的“PASS”指令之前增加5秒种的延迟，以降低恶意攻击的效率。如果有效，目标操作系统提供的机制可以执行上述建议。

入侵者可以通过在一个服务器上建立多个并行的控制连接来扰乱上述机制。为了抵抗多个并发的连接，服务器可以限制控制连接的总数，或探查会话中的可疑行为并在以后拒绝该站点的连接请求。尽管如此，这两种机制又打开了“服务拒绝”攻击的大门。攻击者可以故意地发起攻击使得合法用户失去访问权限。

标准FTP[PR85]规范中使用“PASS”指令以明文方式发送密码。建议客户端和服务器端使用交互的鉴别机制以避免遭受窃听（IETF公共鉴定技术工作组已经开发了这样一种机制[HL97]）。

6保密性

在标准的FTP规范[PR85]中，所有的数据和控制信息（包括密码）都是不加密地在网络中传输的。为了保证FTP传输信息的保密性，无论何时，只要可能就应该使用强壮的加密机制。在[HL97]中定义了一个这样的机制。

7保护用户名

标准的FTP规范[PR85]中，当用户名非法时为USER命令指定了一个530回应。如果用户名合法但是密码非法则FTP会做出一个331回应。为了防止一个怀有恶意的用户从服务器获取合法的用户名，建议服务器总是为USER指令返回331回应，然后拒绝对无效用户名合并用户名和密码。

8端口盗用

许多操作系统以递增的顺序动态地分配端口号。为了进行一次合法传输，攻击者可能观察服务器当前分配的端口号，并“猜测”下一个将会使用的端口号。攻击者会与这个端口建立连接，这样就剥夺了其他合法用户进行传输的能力。作为选择，攻击者可以盗用合法用户的文件。另外，攻击者还可以在授权用户发出的数据流中插入伪造的文件。通过使FTP客户端和服务器使用随机的本地端口号给数据连接，要求操作系统随机分配端口

号或者使用与依赖于机制的系统都可以减少端口盗用的发生。

9基于软件的安全问题

本文档的重点是和协议有关的安全问题。另外还有一些成文的FTP安全问题是由于不完善的FTP实现造成的。虽然这些类型的问题的细节超出了本文讨论的范围，还是有必要指出以下那些过去曾被误用，应该被未来的执行者们慎重考虑的FTP特性:

匿名FTP

匿名FTP使得客户端以最小的权限连接到FTP服务器并获得公共文件的访问权成为可能。当这样的用户能够访问所有系统中的文件或者建立文件时，就会发生安全问题。[CERT92:09] [CERT93:06]

远程命令的执行

FTP扩展操作“SITE EXEC”允许客户端在服务器上执行任意的命令。这种特性显然需要非常小心地实现。已经有几个成文的例子说明攻击者利用FTP“SITE EXEC”命令可以破坏服务器的安全性。[CERT94:08] [CERT95:16]

调试代码

一些前述的有关危及FTP安全的问题是由于安装了调试特性的软件造成的。[CERT88:01]

本文推荐有这些功能的FTP服务器的执行者，在发布软件之前参阅所有的CERT有关这些攻击以及类似机制的忠告。

10结论

使用上述建议，能够在不丧失现有功能的情况下减少和FTP服务器有关的安全问题。

11安全方面的考虑

本备忘录通篇讨论了安全问题。

感谢

（略——译者注）

参考书目

[AOM98]

Allman, M., Ostermann, S. and C. Metz, “IPv6和NATs的FTP扩展”，RFC 2428，1998年9月。

[Bel94]

Bellovin. S., “防火墙——友好FTP”，RFC 1579，1994年2月。

[CERT88:01]

CERT Advisory CA-88:01. 文件传输服务器软件的弱点， 1988

年12月 ftp://info.cert.org/pub/cert_advisories/

[CERT92:09]

CERT Advisory CA-92:09. AIX 匿名FTP的弱点，1992年4月27日 ftp://info.cert.org/pub/cert_advisories/

[CERT93:06]

CERT Advisory CA-93:06. Wuarchive 文件传输服务器软件的弱点，1997年9月19日， ftp://info.cert.org/pub/cert_advisories/

[CERT94:08]

CERT Advisory CA-94:08. 文件传输服务器软件的弱点， 1997年9月23日， ftp://info.cert.org/pub/cert_advisories/

[CERT95:16]

CERT Advisory CA-95:16. 文件传输服务器软件错误配置的弱点，1997年9月23日， ftp://info.cert.org/pub/cert_advisories/

[CERT97:27]

CERT Advisory CA-97.27. FTP欺骗，1998年1月8日ftp://info.cert.org/pub/cert_advisories/

[HL97]

Horowitz, M. and S. Lunt, “FTP 安全扩展”，RFC 2228, 1997年10月

[Pis94]

Piscitello, D., “FTP 在大地址记录上的操作(FOOBAR)”， RFC 1639, 1994年6月

[Pos81]

Postel, J., “传输控制协议”, STD 7, RFC 793，1981年9月。

[PR85]

Postel, J. and J. Reynolds, “文件传输协议(FTP)”, STD 9, RFC 959, 1985年10月。

[RP94]

Reynolds, J. and J. Postel, “编号的分配”, STD 2, RFC 1700, 1994年10月，参看http://www.iana.org/numbers.html

作者地址

（略——译者注）

完整的版权声明

（略——译者注）

感谢

（略——译者注）

原文：RFC 2577《FTP Security Considerations》
译者：张偶 2002年5月