第33卷 第20期 计 算 机 工 程 2007年10月
Vol.33 No.20 Computer Engineering October 2007
·安全技术· 文章编号：1000—3428(2007)20—0145—03 文献标识码：A 中图分类号：TP31

Windows下RDP协议的安全性

罗 鹏，祝跃飞
(解放军信息工程大学信息工程学院，郑州 450002)

摘 要：微软开发的Windows下的RDP协议暴露出一定的安全问题。介绍了RDP协议的工作原理，分析了RDP采用的安全机制，指出其在协议设计上存在的一些漏洞，从用户使用和协议改进两个方面分别提出了防范措施和修改方案。
关键词：RDP；RSA；安全；中间人

Security of Windows RDP Protocol

LUO Peng, ZHU Yue-fei
(Institute of Information Engineering, PLA Information Engineering University, Zhengzhou 450002)

【Abstract】 The Windows RDP protocol developed by Microsoft Inc. has caused many security problems. The principles of RDP are introduced, and the security-mechanism adopted by RDP is also analyzed. It points out some improper design methods of the protocol. Some security improvement schemes of RDP protocol and advices for using RDP application are both offered.
【Key words】 RDP; RSA; security; man-in-the-middle

微软远程桌面协议(remote desktop protocol, RDP)是一种构建于Windows系列操作系统的终端服务网络通信协议。它采用了典型的C/S架构，共分为两个部分：运行在远程设备上的客户端和运行在服务器上的终端服务器。作为微软公司的一个工业标准，该协议应用于Windows系列服务器，并在Windows XP版本以后的个人操作系统上绑定了其客户端[1~4]。

其广泛的使用性一方面证明了该协议对信息处理的高效率，另一方面也对其安全性有了较高的要求。本文将通过对RDP协议的安全性分析，指出其在应用中暴露出的问题，并给出相应的解决方案。

1 RDP协议概述

RDP协议建立于微软公司内部，与大多数公开细节的网络协议不同，其具体实现过程作为商业机密，目前尚未公开。

该协议定位于TCP/IP协议族的应用层，是在标准协议T120系列协议的基础上发展形成的。在一次使用RDP协议的会话中，客户端的鼠标或者键盘等消息经过加密后传输到远程服务器予以执行，而远端服务器所进行的一系列响应也将以加密消息的形式通过网络回传给客户端，并借助客户端的Win32 GDI API形象地显示出来。

RDP协议的通信功能主要由ISO层与多点通信服务层(multipoint communication service layer)支持，而安全功能则由安全层(secure layer)来保证。

1.1 RDP协议的通信基础

RDP协议采用的是基于连接的传输协议TCP。它在协议族中的位置如下：

RDP layer
secure layer
multipoint communication service layer
ISO layer
TCP layer

ISO层需要完成一个ISO DP 8037连接，其一般的报文结构为：

TPKTversion	TPKT reversed	TPKT length	TPDU data

RDP的实现完整采用了该协议的标准，其version字段目前为0x03，reversed字段为0x00。

多点通信服务层就是T120系列协议。包括T122，T125和T128。其作用主要是支持在任意两个应用实体间通过不同网络类型连接的全双工多点通信。

1.2 安全层

安全层(secure layer)是整个RDP协议的安全保证，它采用RSA认证和RC4流数据加密等机制来完成协议安全功能，其主要任务是：(1)加密套件的磋商；(2)加密密钥的生成；(3)消息认证码的生成；(4)通信数据的加密解密；(5)MAC (message authentication code)值的计算和校验。

2 RDP的安全机制

根据执行任务的不同，一次完整的RDP会话过程可以分为两个阶段：认证连接阶段和数据通信阶段。RDP在不同阶段采取了不同的安全保障，如图1所示。

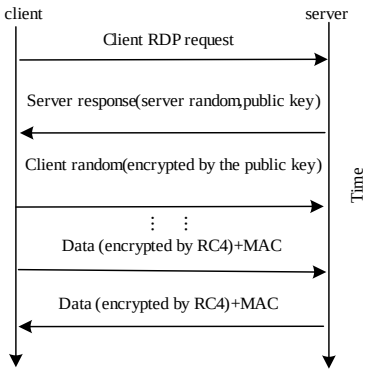


图1 一次RDP会话示意图

作者简介：罗 鹏(1982－)，男，硕士研究生，主研方向：计算机网络安全；祝跃飞，教授、博士生导师
收稿日期：2007-02-27 **E-mail：**boygo1982@gmail.com

2.1 认证连接阶段

在认证连接阶段，RDP 采用的安全策略是服务器端对客户端的单方面认证。其使用的是 RSA 非对称加密算法。

首先，客户端向提供远程桌面服务的服务器发起一个服务请求。请求中包含了客户端的主机信息，自己支持的加密强度和消息认证码算法。

服务器成功接收到请求之后，会立即响应一段应答报文。该应答报文包含一个服务器随机数、一个 RSA 公钥值、一段对该公钥的签名，并提供服务器所支持的加密强度和消息认证码算法。

最后，收到响应的客户端会采用服务器传来的 RSA 公钥加密一个自己当前选择的随机数，并将其发送给服务器端。至此，RDP 会话的认证连接阶段结束。

2.2 数据通信阶段

数据通信阶段的所有通信数据均采用 RC4 对称加密算法，其密钥构建的安全性由认证阶段的操作来保证。服务器和客户端通过认证阶段的操作，相互交换了一对随机数，并同时按照约定的算法，各自独立生成一个 RC4 密钥。由于数据输入和算法相同，双方的 RC4 密钥是等同的。

在数据通信阶段，RDP 协议将使用该 RC4 密钥对所有的通信数据进行加密。数据的加密算法为

$$E_{rc4\_encrypt\_key}(M)+MAC(mac\_key,M)$$

其中，M 是报文数据；mac_key 是消息认证码密值；MAC 表示消息认证码算法。

目前支持的加密长度分为 40 位、56 位和 128 位 3 个等级。具体使用何种强度，在认证阶段通过加密强度的协商信息进行统一。

3 RDP 的协议漏洞分析

RDP 协议在使用的过程中，涉及的敏感数据主要分为两类：一类是登录时用户键入的用户名和密码，另一类是用于加密数据的 RC4 密钥值。针对这两种情况，主要存在以下 3 种普遍的攻击方式：

(1)用户口令猜测。服务器端的 RDP 软件使用客户端提供的用户名和登录密码对其进行认证。用户名并不进行加密，而对口令可以采用穷举、联想甚至社会工程学的方法进行猜测。这种方法并不会引起 RDP 软件的异常现象，但是其花费时间长，且其频繁连接的行为易被安全软件发现。

(2)利用键盘记录的脆弱性。该方法主要是利用了数据通信阶段时，数据封装中使用的 MAC(消息认证码)算法的缺陷。

MAC 算法的具体如下：

$$MAC(mac\_key,M)=MD5(mac\_key||Pading1||SHA1(mac\_key||Pading2||Length(M)||M))$$

其中，Pading1 为以 48 个 0X92 为成员的数组；Pading2 为以 48 个 0X54 为成员的数组；Length(M)为报文的数据长度；MD5、SHA1 为通用的 HASH 值算法。

这种攻击方案并不需要破解 MAC 算法的计算过程，而是利用 RDP 通信数据短小的特点，结合统计的方法来实现。

在上述公式中，可以注意到：参数 Pading1、Pading2 和算法 MD5、SHA1 在任何时候都是固定不变的；而对于当前的一次 RDP 会话而言，mac_key 的数值也是固定的，输入数据中只有一个变量 M 是可变的。为此，用户输入的 M 和加密之后的报文段数据是唯一对应的。

这一特点对于键盘记录数据具备脆弱性。键盘信息的编码相对短小，用户在一次会话中如果有相同的键盘行为，则会生成相同数值的密文。只要收集足够多重复的密文对，就可以破译出用户的键盘记录信息。

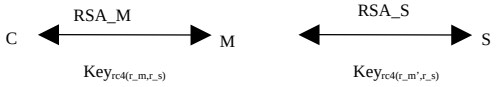
这种攻击方法提供了一种理论上的可行性，但在实际操作中还存在极大的局限性。最大的困难在于这样的一个现实：每一次的 RDP 会话都会生成不同的 RC4 密钥。如果不能在一次特定会话中获取足够的统计信息，则此次的分析结果将无法应用到下一次攻击中。

(3)中间人攻击。中间人攻击的方法利用了 RDP 会话认证阶段单向认证的缺陷。由于客户端既不对服务器发送的 RSA 公钥的身份进行认证，也不验证其完整性，则在会话发生阶段，第三方攻击者可以采用 ARP 地址欺骗、DNS 欺骗等方法伪装成服务器，从而将自己构造的公钥传递给客户端，以建立一个虚假的会话，骗取客户端的敏感信息。根据 RDP 版本的不同，该方法在操作中存在以下两种情况：

1)“钓鱼”攻击。在成功进行欺骗之后，攻击者会构造一个虚假的登录界面，并等待用户将自己的用户名和登录密码输入。因为虚假的攻击者并不能从真正意义上提供完整的 RDP 服务，所以一旦用户执行完登录操作后，该会话会进入无响应阶段。但是攻击者已经顺利地获取了用户足够的信息，具备了登录目标服务器的权限。

该情况多见于客户端安装的是 RDP 低版本 4.0 版的情况下。

2)完整代理窃听。该方法需要分别建立两个 RDP 会话，分别是客户端——攻击者，攻击者——服务器。此时，攻击者需要充当一个代理的身份。设客户端为 C，中间人攻击者为 M，服务器为 S，实例图如下：



在认证阶段，M 向 C 发送自己的 RSA 公钥 RSA_M，以及自己选择的随机数 r_m，而被欺骗的客户端则使用该 RSA_M 加密自己选择的随机数 r_c，并回传给 M。因为 C 与 M 之间的认证使用的是 M 自己的 RSA 公钥匙，则 M 可以用该 RSA_M 对应的私钥解密，从而获取 r_c。拥有了 r_c 和 r_m，C 与 M 将使用相同的 RC4 算法生成通信阶段的加密密钥，则 M 可以完全破解 C 发出的报文信息(RC4 是对称加密算法，其加密密钥与解密密钥相同)。

同理，在 M-S 端，中间人 M 将以客户端的身份建立和服务器 S 的合法连接，认证过程使用服务器的公钥 RSA_S，并通过 M 的随机数 r_m、服务器的随机数 r_s 生成 M-S 端的通信数据加密密钥。

在上面的基础上，中间人将使用$Key_{rc4(r_m,r_s)}$解密来自C的数据，然后再利用$Key_{rc4(r_m',r_s)}$将该数据加密，并转发给服务器S。反之亦然。著名的网络安全工具Cain可以很好地重现该攻击过程。

4 增强 RDP 协议应用安全性的策略

根据现有的 RDP 应用中暴露出来的安全隐患，可以从客户应用和协议改进两方面来增强 RDP 协议的应用安全性。

4.1 客户应用方面

(1)修改 RDP 应用的默认端口

服务器提供 RDP 服务的默认监听端口为 3389。该信息易向黑客暴露用户的当前行为，提示黑客目前正存在一个可利用的 RDP 会话服务，所以最好进行修改。

更改服务端口需要修改服务器的注册表。在注册键

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\rdpwd\Tds\tcp 下，将 Port-Number 的数值修改为新的端口值。

(2)防范中间人攻击

中间人攻击是 RDP 协议安全最大的威胁。防范中间人攻击的实质就是防范不同类型的地址欺骗。其比较直观，且效果明显地就是为本机和服务器维持一个静态地址表项。

无论是 ARP 欺骗，还是 DNS 欺骗，都利用了协议维持信息一致性操作上的缺陷。当初为了动态适应网络变化，协议设计者们力求协议能使网络上的结点通过互相通信来维持地址和时间信息的一致性，这一方便的设计思想也给黑客随意修改主机地址信息提供了机会。

对于结构不经常发生变化的网络，可以采用维持静态地址列表的策略。在终端服务器的 MS-DOS 窗口键入命令行“arp –s IP 地址 MAC 地址”，即可将 IP 地址和 MAC 地址进行绑定。在数据包收发过程中，主机将不再访问动态更新的 ARP 地址缓存，而使用用户设置好的静态信息，是一种有效的防范手段。

4.2 协议改进方面

单向的身份认证使 RDP 协议难以抵抗中间人攻击，所以，协议的改进方向可以从认证的角度入手。使用完整的 SSL (secure socket layer)机制，增加客户端对服务器的认证策略。

安全套接层 SSL 最初是为电子商务开发的，其良好的安全特性为网络安全提供了一种优秀的解决方案。第 1 种方案其实是借鉴了一部分 SSL 的思想，其前提是认为服务器通过用户名和密码能够正确有效地确认客户端的身份。第 2 种方案则是直接在 RDP 协议所处的应用层与 TCP 层之间插入安全套接层，如图 2 所示。

图 2 插入 SSL 之后的协议栈示意图

中间人攻击的第 1 步就是需要中间人向客户端发送一个伪造的服务器公钥，而一旦增加了客户端对服务器的认证措施，则客户端可以识别该公钥的真实性，从而成功杜绝中间人攻击的可能性。

修改方案如下：

(1)对于客户端的 RDP 请求包，修改服务器对其的响应包格式：不再单纯发送一个 RSA 公钥原文，而是将其生成一个证书。将证书内容作为响应内容。

(2)修改客户软件的实现。加入对服务器的认证过程：客户机利用其本地存储的 CA 证书认证该公钥来源。

整个 SSL 的握手规则可以满足上述两个修改方案。在编制软件时，可以采用开源的开发包 Openssl 来实现该机制。

除非攻击者也同样持有一个合法机构颁发的证书，这属于证书制度的管理问题，否则它将很难完成中间人攻击。

5 结束语

RDP 协议在认证阶段采用不完整的身份认证机制，使客户端无法确认服务器的身份合法性；在通信阶段，通信数据的短小一方面有助于其工作效率，但另一方面也带来了其加密的脆弱性。

不同于公开的 TCP/IP 协议栈，作为微软的一款商业软件，RDP 协议的许多细节并未公开，从一定程度上也限制了该软件的改进工作。目前在 Linux 下，已经出现了如 rdpproxy, xrdp,rdesktop 等同类型的软件，相继引用了更多较好的改进措施。但是，作为一种十分强调实时性的远程控制软件，过多的安全策略又容易造成通信上的负担。如何在多种网络环境下使其具备商务网站级别的安全性、并保证快速响应的特点是下一步需要研究的重点。

参考文献

1 Forsberg E. Reverse-engineering and Implementation of the RDP 5 Protocol[EB/OL]. [2006-12-12]. http://efod.se/writings/thesis.pdf.

2 Montoro M. Remote Desktop Protocol, the Good the Bad and the Ugly[EB/OL]. [2006-12-12]. http://www.oxid.it/downloads/rdp-gbu.pdf.

3 Cai Longzheng. Research and Implementation of Remote Desktop Protocol Service over SSL VPN[C]//Proc. of IEEE International Conference on SCC'04. 2004.

4 Whalen S. Cain & Abel v 2.5 Password Cracking via ARP Cache Poisoning Attacks[EB/OL]. [2006-12-12]. http://www.nwcet.org/downloads/cainAbel.pdf.2004.

(上接第 144 页)

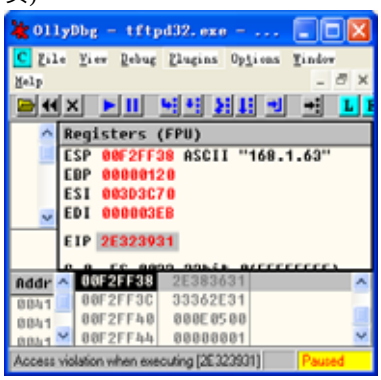


图 7 TFTPD32 版本 2.84 的漏洞调试图

5 结论

利用自主开发的针对 TFTP 服务器的 tftpServerFuzzer，对笔者在互联网上能搜集到的 Windows 平台下的 11 种 TFTP 服务器进行了安全测试，曾经出现在这些版本上的漏洞共 6 个，均能够被 tftpServerFuzzer 发现，另外又发现未曾公布过的新漏洞 7 个。测试结果不仅体现了 tftpServerFuzzer 的实用性、高效性和先进性，更重要的是反映了目前 Windows 平台下 TFTP 服务器存在着的相当大的安全问题。

参考资料

1 FX of Phenoelit. Bug hunting[Z]. (2006-09) http://www.phenoelit.de/stuff/Bugs.pdf.

2 Oehlert P. Violating Assumptions with Fuzzing[J]. IEEE Security & Privacy, 2005, 3(2): 58-62.

3 Sollins K. The TFTP Protocol[Z]. RFC 1350(Revision2), 1992.

4 Howard M, LeBlanc D. 编写安全的代码[M]. 程永敬, 译. 北京: 机械工业出版社, 2002.