校园网络中 SSH 协议的安全改进

罗雅莉 唐宾徽

四川大学锦城学院 四川 成都 611731

【摘要】安全外壳协议（SSH）由互联网工程任务组（IETF）制定，在高校局域网环境中得到了广泛的应用。校园教学课堂一般使用云计算平台进行教学，这种方式虽然减少了学生配置相应学习环境的时间开销，但是在使用 SSH 协议进行身份认证的过程中容易遭受“中间人”攻击（MIM）。本文基于 SSH 协议的口令认证方法，在建立连接时使用网络地址转换（NAT）技术后对登录用户名和 IP 地址进行比对，确认用户是否合法。

【关键词】SSH CRC; 中间人攻击；口令认证；局域网

1 引言

在校园教学局域网中，云计算平台得到了广泛的使用，高校只需要付出一定的运营成本，所需的服务就可以得到快速响应。这种服务十分依赖 TCP/IP 协议，数据的正确传输也是建立在 TCP 协议之上。TCP 协议的建立过程可以简化为三步，首先建立连接，其次数据传输，最后是线路释放。TCP/IP 协议设计之初是为了解决计算机之间的通信问题，在此基础之上，用户和服务器进行数据交换的这个过程更加渴望的是安全。因为 SSH 协议天生对数据是进行加密之后再传输的，所以它被广泛运用在云计算平台的数据传输之中 [1]。

2 相关术语简介

2.1SSH

Secure Shell（安全外壳协议）：利用 TCP 协议提供的端口，对传输的信息进行加密，为文件传输、远程登录等其他网络服务提供安全保障的协议，SSH 协议默认使用 TCP 协议的 22 号端口。

2.1.1 SSH 协议的组成

SSH 协议主要由三个部分组成。第一个是传输层协议（ssh-trans）主要进行传输层基本功能，服务器认证，会话数据加密，数据保密性以及完整性验证。第二个是用户认证协议（ssh-userauth）主要是对客户端请求连接的用户进行鉴定。最后是连接协议（ssh-connect），它提供各种服务通道，是为了向例如 SCP（安全复制）、SFTP（安全文件传送协议）等应用提供服务 [2]。

2.1.2SSH 协议的验证方式

SSH 协议的验证方式共两种，一种是基于口令的验证另外一种是基于密钥的验证。采用口令验证用户只需知道自己的登录用户名、另一台主机的 IP 地址和登录密码，就可以远程登录到另外一台主机，并且在传输数据的过程中所有的数据都会被加密进行传输。客户端首先向请求服务器请求连接，服务器再把生成的公钥（Public Key）发送给客户端，然后在客户端上输入用户的账号和密码并且用服务器端传输过来的公钥进行加密后再回传给服务器，最后服务器使用私钥（Secret Key）对从客户端发来的这条消息进行解密，若此用户在服务器端上存在且输入的该用户密码正确结果正确则允许客户端进行登录。

当采取密钥验证时在用户正在使用的这台主机生成一把成对的公钥和私钥，先把 Public Key 传输给 Server。若要 SSH 连接到 Server 上，Client 先向 Server 发出请求，请求用自己的 Public Key 进行验证。Server 收到请求之后，先在该服务器上该用户的主目录下寻找 Public Key，然后把它和用户发送过来的 Public Key 进行比较。如果两个密钥一致，Server 就对 Public Key 进行 Challenge（质询）即服务器生成一串随机字符并使用 Client 的 Public Key 进行加密然后把它发送给 Client。客户端收到质询之后用自己的 Secret Key 解密后再把它发送给服务器，服务器把收到的这条客户端解密后的消息和之前生成的随机字符进行对比，就可以判断这个用户是不是合法用户。

2.1.3SSH 协议的工作过程

为了实现 SSH 协议的安全连接，客户端和服务器建立连接一共要经历 5 个阶段。

1. 版本号协商阶段

SSH 协议有 SSH1 和 SSH2 两个版本，通信双方通过协商确定要使用的版本。

2. 密钥和算法协商阶段

SSH 协议支持许多种加密算法，比如 DES 这些对称加密算法，也支持像 RSA 这样的非对称加密算法。通信双方根据自己和对方支持的加密算法，确定最终使用的加密算法。但因为对称加密算法使用的加密秘钥和解密秘钥相同，在安全方面存在一些隐患，所以现在大都采用非对称加密算法。因此 RSA 成为了 SSH 协议中使用最为广泛的加密算法，现阶段使用的比较多的是 2048 位的 RSA 加密算法。

3. 认证阶段 [4]

首先 SSH 客户端向 Server 发起认证请求，Server 对 Client 进行认证，认证请求要包含用户名、认证方法等。当 Server 对 Client 进行认证时，如果认证失败，则向 Client 发送一条认证失败的消息，并且这条失败消息中包含了其余可以认证的方法。然后 Client 从其余可以使用的认证方法中挑选一种认证方法再次进行认

证，该过程反复进行。最后，直到认证成功或者认证次数达到上限，Server 就会返回认证成功消息给客户端或者直接关闭这次连接。

4. 会话请求阶段

认证成功后，Client 向 Server 发送会话请求。

5. 交互会话阶段

会话请求通过后，服务器和客户端进行数据传输。

2.2“中间人”攻击 Man-in-the-Middle Attack

攻击者位于客户端和服务器之间，可以窃听、篡改通信数据，但是通信的双方却不知情。数据篡改是指当客户端和服务器通信时都由“中间人”进行“转发”，数据窃听是指“中间人”不修改通信双方所发送的信息，只是备份双方的通信数据，记录双方数据传输时的敏感信息，如：账号、密码等。

2.2.1SSH 连接与 MIM 攻击

其实 SSH 建立时采用口令验证连接的过程理论上是安全的，但是若在客户端发送给服务器登录请求时的这条消息被“中间人”截获，它就可以冒充服务器回复公钥给客户端用户。获得客户端用户的账号密码之后，“中间人”就可以使用这个账号密码登录服务器。因为 SSH 协议没有像 HTTPS 协议这样引入数字证书和数字签名技术，所有的公钥都是由服务器直接发送给客户端的，所以在这个过程中就容易遭受“中间人”攻击。

2.3 IPV6 地址与 IPV4 地址的转换方法

IPV6（Internet protocol version6）是由互联网工程任务组设计出来用于解决 IPV4 地址不够用的问题的下一代 IP 协议。为了实现 IPV4 和 IPV6 的共存，IPV4 地址通常会嵌入 IPV6 地址中。现阶段一共有三种方法实现 IPV6 地址和 IPV4 地址的转换，第一种是双堆栈，即设备同时运行 IPV4 和 IPV6 两种协议栈。第二种是隧道，通过 IPV4 网络传送 IPV6 数据包，把 IPV6 数据包封装在 IPV4 数据包中。最后一种是网络地址转换，允许支持 IPV6 的设备与支持 IPV4 的设备使用类似于 IPV4 中的将内网的私有地址转换为公网上可以使用的公有地址的技术进行通信。把 IPV6 地址转换成 IPV4 地址，或者把 IPV4 地址转换成 IPV6 地址。

3 改进方案

在校园局域网环境中，针对现有 SSH 协议的口令验证报文，使用 NAT 技术，依据 IEFT 制定的 rfc6052 标准[4]把 SSH 的口令验证报文中的 IPV4 地址嵌入 IPV6 地址中。

循环冗余校验（CRC）是经常用在检验传输过程中或保存的数据是否出现错误的一种方法。发送方根据公式计算出一个值并附在传输数据的后方，接收方根据这个接收到的数据再次进行校验，若得出的值和发送方发出的值不同，则证明在传送过程中信息被修改了，则要求发送方进行重新发送。利用循环冗余校验的这种特性，若在信息传输的过程中遭受了“中间人攻击”服务器对从客户端发送来的信息先进行循环冗余校验，就会发现信息在传输过程中被修改了，则要求客户端重新进行验证，因此在一定程度上可以避免“中间人”攻击。

IPV6 地址一共有 128 位，在校园局域网环境中，假设前 48 位表示路由器的前缀，后面的 16 位表示 IPV4 的前 16 位地址，紧接着的 8 位用来分割 IPV4 地址且必须为“0”[4]，后面 16 位表示 IPV4 的低 16 位地址。剩下的 IPV6 后缀使用 CRC-32 循环冗余码进行填充，最后 IPV6 地址还剩 16 位未表示，剩下未使用的位用“0”来补齐。改进前的 IPV6 地址和改进后的 IPV6 地址对比如图 1 所示：

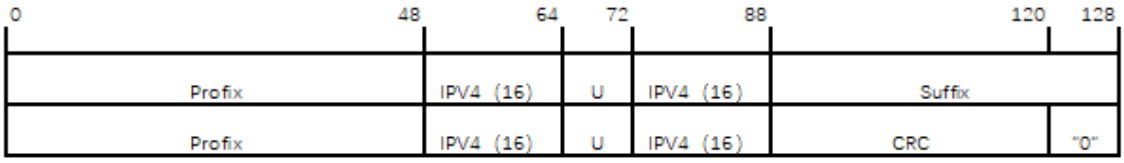

图 1 改进前的 IPV6 地址和改进后的 IPV6 地址对比

改进后的 SSH 连接请求使得 SSH 服务器端收到从客户端发来的 SSH 口令验证请求后，先进行循环冗余码的校验，确认报文在传输过程中有没有被修改。若没有被修改服务器则读取 SSH 连接报文中的 IPV4 地址和用户名且服务器对经过公钥加密的用户名使用自己的私钥解密获得客户端用户的用户名并进行验证。若此用户名在服务器端存在则让客户端用户输入密码，若此用户不存在服务器也不直接拒绝此用户的连接请求，而是根据 SSH 协议工作过程中第二阶段所协商的秘钥和算法，让客户机采用其他加密算法来进行连接请求。因此客户端用户无法分辨是因为加密算法不正确还是因为用户不存在而无法和 SSH 服务器端进行连接，从而在一定程度上保护了用户名不会被泄露。

这种方案其实在 IPV4 和 IPV6 中都同样适用，只是 IPV6 作为下一代的 IP 地址，使这种改进方案更具有意义，所以针对 IVP6 进行讲述。

结语

SSH 协议作为一种在校园局域网中广泛使用的协议，它为网络中数据的传输提供了安全机制，也为其他基于 SSH 协议开发出来的应用提供安全保障，但是 SSH 协议在用户验证过程中仍然有不安全的地方。本文基于 SSH 的两种验证方式其中之一的口令验证方式，对 SSH 连接建立过程中的 IPV4 地址进行改进，利用 NAT 技术使 IPV4 地址映射为 IPV6 地址，增加了循环冗余校验，减少了 SSH 连接建立过程中遭受“中间人”攻击的可能性。

【参考文献】

[1] 吴正挺． 基于 OpenStack 的云管平台的设计与实现 [D]. 东南大学 , 2019.

[2] 林利 . SSH 协议安全性分析及改进 [J]. 电脑与信息技术 , 2010, 18(02):25-28.

[3] 何家方 . 对 SSH 口令认证机制的一种改进方法 [J]. 网络安全技术与应用 , 2010(02):34-36.

[4] https://tools.ietf.org/html/rfc6052#section-2.2

基金项目：201801012040 教育部网络空间安全协同育人项目