第 34 卷 第 20 期 计 算 机 工 程 2008 年 10 月
Vol.34 No.20 Computer Engineering October 2008
·安全技术· 文章编号：1000—3428(2008)20—0187—03 文献标识码：A 中图分类号：TP391.9

一种改进的 TCP 连接迁移安全机制

洪小亮，郭义喜
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：TCP 连接迁移技术使网络可以在主服务器发生故障的情况下稳定地提供服务。该文分析基于椭圆曲线 Diffie-Hellman 密钥协商的连接迁移安全机制中存在的中间人攻击问题，利用改进的 Helsinki 协议进行连接密钥的协商，提出一种新的安全机制。该机制有效地保证了迁移选项的安全，利用安全哈希算法的抗碰撞性和安全性使攻击者难以猜测出连接标志和请求。

关键词：TCP 连接迁移；迁移选项；Helsinki 协议；安全性

Improved TCP Connection Migratory Secure Mechanism

HONG Xiao-liang, GUO Yi-xi
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】The service can be provided steadily when primary server goes wrong by using TCP connection migratory technology. This paper analyzes the problem of man-in-the-middle attack existing in secure mechanism of the connection migratory based on ellipse curve Diffie-Hellman key negotiation. With the improved Helsinki protocol which is applied to negotiate the connection key, a novel secure mechanism is presented. This mechanism can protect the migratory options effectively. The function of resisting collision and the security of hash-algorithm make it hard for attackers to guess the connection symbol and request.

【Key words】TCP connection migratory; migrate options; Helsinki protocol; security

1 概述

随着 Internet 网络规模的不断扩大，网络服务的模型和体系结构发生了很大变化。网络需要提供多种服务并保证端到端的良好性能，尤其是对实时性要求较高的网络应用。网络服务质量保证技术应运而生，可生存性是网络服务质量的重要方面。在系统受到攻击或出现故障的情况下，如何连续稳定地提供高质量服务是目前的一个技术难点。

动态漂移技术[1]实现了在灾难发生时，应用服务由受难节点到备份节点的漂移，即在由多台备份服务器构成的系统中，当正在提供服务的服务器节点发生灾难时，由另一台备份服务器继续提供服务，从而使服务质量不受影响。TCP连接迁移技术[2-4]是目前实现动态漂移技术的一种最新方式，它通过对传统TCP协议进行修改和扩充，获得了高可用性的服务能力。TCP连接迁移的安全机制研究是目前研究的重点和热点之一。

2 TCP 连接迁移技术

TCP 连接迁移技术的主要思想是通过对 TCP 协议的修改(扩充 TCP 选项)使客户端和服务器端可以通过协商的方式完成连接的迁移。由于修改后的 TCP 协议只是对标准 TCP 协议的一个扩充，因此它和标准 TCP 协议具有兼容性，且可以进行互操作。如果客户端和服务器端都加载了新的 TCP 协议，那么整个连接过程就按新协议规定的操作完成，并且此连接具有迁移能力。如果客户端和服务器端有一端没有加载新的 TCP 协议，那么连接过程就按标准 TCP 协议规定的操作完成，此连接不具备迁移能力。

为了实现连接迁移，必须对传统 TCP 进行修改和扩充，因此，在原有 TCP 基础上扩充了一个 TCP 迁移选项，它包含 SYN 字段和一个连接标志。SYN 字段是识别 SYN，并作为先前已建立的连接部分，而不是一个新连接的请求。连接标志标识了先前以相同[地址，端口]对建立的连接。在初始化连接建立时利用迁移许可选项协商该连接标志。当成功协商了一个连接标识后，TCP 连接就能利用传统[源地址，源端口，目的地址，目的端口]或新的[源地址，源端口，连接标志]在每个主机上唯一地标识连接。

迁移过程如图 1 所示。

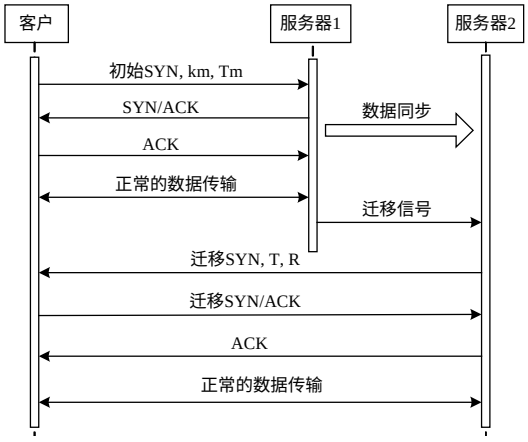

图 1 迁移过程

当主服务器发生故障时，可以从一个备份服务器重新启动先前建立的 TCP 连接。通过发送一个能标识先前连接的迁

作者简介：洪小亮(1981－)，男，硕士研究生，主研方向：网络安全和可生存性；郭义喜，副教授

收稿日期：2008-01-26 **E-mail：**hxl_103@tom.com

移 SYN(其中含有连接标志)，使备份服务器能与客户重新建立同步连接，一个可迁移的连接保持相同的控制块和状态，包括序列号空间。在初始 SYN 交换中协商的任何选项，在连接迁移之后仍具有影响，不需要重新设置迁移 SYN。任何客户接收到的消息通过迁移连接到备份服务器，此时对当前连接应答的迁移 SYN 有一个合适的序列号。类似地，客户提供备份服务器一个应答迁移 SYN/ACK。

3 TCP 连接迁移安全机制分析

迁移选项用于请求一个当前 TCP 连接迁移到一个新地址，以 SYN 字段的形式发送到先前建立了连接的主机，并通过协商迁移许可选项完成。在迁移选项中，有 2 个 64 bit 域，即连接标志和请求；一个 8 bit 序列号域 reqNo。每个新的迁移请求都以单调递增方式发送(序列号允许通信主机确保迁移 SYN 不会重新排序)，如图 2 所示。

Kind	Length	ReqNo
Token		
Token(cont.)		
Request		
Request(cont.)		

图 2　迁移选项

发生 TCP 连接迁移时，如果攻击者能利用迁移选项猜测出连接中使用的序列空间和连接标志，那么攻击者就能完全地劫持该连接。一旦迁移 SYN 已经发出，且在新路径上的主机能猜测出连接标志，就可以利用有效连接标志通过发送伪造的迁移 SYN 发起拒绝服务攻击。因此，必须在连接迁移过程中对该连接迁移标志 T 和迁移请求 R 进行安全性保护。

3.1 原有安全机制

为实现对连接选项的保护，文献[4]提出利用椭圆曲线 Diffie-Hellman密钥交换协议[5]来保护连接密钥，只有得到该连接密钥的主机才能构造连接标志并发出迁移请求，实现了连接标志的不可猜测性。

在椭圆曲线 Diffie-Hellman 密钥交换协议中，设椭圆曲线为 $E(F_q)$；在 Abel 加法群中的阶为 n；点 P_0 为该椭圆曲线上的点；A 和 B 为进行通信的用户。对主机 i 选择一个随机数 $X_i \in [1, n-1]$，并计算

$$k_i = X_i * P_0$$

其中，$*$ 操作是在 F_q 域上的标量乘法。安全连接的关键是保证秘密地协商密钥，因此，X_i 应随机地产生并存储在每个新的连接控制块中。任何需要中继的 SYN 或 SYN/ACK 必须包括迁移选项和时戳选项的值。

收到用迁移许可选项初始化的 SYN 后，在 SYN/ACK 字段中，主机 j 利用一个包括迁移许可选项的相应 TCP 栈。类似地，选择随机 $X_j \in [1, n-1]$ 用于构造公钥 k_j，并以相同的方式发送。

用迁移许可选项和时戳选项初始化主机接收的 SYN/ACK 后，2 台主机能计算出共享秘密的秘密密钥

$$K = k_i * X_j = k_j * X_i$$

秘密密钥 K 用于计算一个连接的有效连接标志。

3.2 原有安全机制的攻击模型

分析表明，在整个协商过程中，上述密钥交换协议不能抵抗来自具有截取、修改或添加数据包能力的主动敌手的攻击，即中间人攻击。若存在攻击者 C 具有截取、修改或添加数据包的能力，他就能利用截获的连接密钥猜测出该连接迁移选项中使用的序列空间和连接标志，并完全劫持该 TCP 连接，进而对服务器发起拒绝服务攻击。其攻击模型如下：

(1)C 选择随机数 $d_C \in [1, n-1]$，并计算 $Q_C = d_C P_0$。

(2)A 选择随机数 $d_A \in [1, n-1]$，并计算 $Q_A = d_A P_0$，$A \to B: Q_A$。

(3)C 中途拦截 Q_A，且 $C \to B: Q_C$。

(4)B 选择随机数 $d_B \in [1, n-1]$，并计算 $Q_B = d_B P_0$，$B \to A: Q_B$。

(5)C 中途拦截 Q_B，且 $C \to A: Q_C$。

在执行椭圆曲线 Diffie-Hellman 密钥交换协议后，A 和攻击者 C 之间建立了秘密密钥 $K_{AC} = d_A Q_C = d_A d_C P_0$，$B$ 和攻击者 C 之间建立了秘密密钥 $K_{BC} = d_B Q_C = d_A d_C P_0$。此时，攻击者 C 得到了 A, B 之间的连接密钥，即中间人攻击方法获得成功。因为攻击者可以成功地让 A 认为自己是合法的客户端，得到了共享密钥使攻击者可以破解 SYN，所以可以利用有效的连接标志通过发送伪造的迁移 SYN 发起拒绝服务攻击，且 A 无法察觉该过程。

为了避免在连接迁移中出现中间人攻击，要有效地保证迁移选项的安全，必须确保用户 A 是在和合法用户 B 交换消息而不是和攻击者 C 交换消息。因此，在密钥建立时，必须对参与者同时进行身份认证。本文提出利用改进的 Helsinki 认证协议进行连接密钥的协商。

4 改进的安全机制

4.1 Helsinki协议[6]的改进

Helsinki 协议是国际标准 ISO/IEC DIS 11770-3 中提出的认证协议。Mitchell 和 Yeun 对 Helsinki 协议进行了改进，能有效防止中间人攻击，并实现通信双方会话密钥的安全共享。该协议过程如下：

(1) $A \to B: \{A, K_a, N_a\}_{PK_b}$

(2) $B \to A: \{B, K_b, N_a, N_b\}_{PK_a}$

(3) $A \to B: N_b$

其中，$\{\}_{PK_a}$ 表示应用用户 A 的公开密钥 PK_a 对大括号内的数据进行加密；N_a 和 N_b 是临时值；K_a 和 K_b 分别是 A 和 B 生成的部分密钥。Helsinki 协议的目标是为 A 和 B 安全地分配一个共享会话密钥 K_{ab}，它最终由 K_a, K_b 和单向函数 f 确定，即 $K_{ab} = f(K_a, K_b)$。该协议建立在公钥密码体制基础上，通过对双方进行交换认证完成密钥的协商，可以有效避免中间人攻击者通过冒充合法用户得到会话密钥。上述协议被形式化证明是安全的，可以利用它对迁移选项进行加密，保证连接密钥的安全。

4.2 基于改进 Helsinki 协议的安全机制

保护连接标志时用到的连接密钥，是在初始化 3 次握手协议时，通过改进的 Helsinki 协议来完成迁移许可选项的协商。其中，迁移许可选项有 2 个变量，即不安全版本长度和安全版本长度，分别为 3 和 20。安全版本需要利用协商连接密钥，并包含一个 8 bit 的主机 ID、一个 8 bit 的临时值 *Num* 和一个 200 bit 的共享密钥域。不安全版本仅包含一个用户 ID(被设置为 0)，它允许 2 台主机跳过密钥协商过程(连接密

钥设置为全 0)。

进行密钥协商时，对主机 i 选择一个临时数 Num_i，利用主机 j 的公开密钥对 ID_i， Num_i 及生成的密钥 K_i 加密，并将该加密过的消息以 SYN 字段的形式发送给主机 j，即

$$i \to j:\{ID_i, K_i, Num_i\}_{PK_j}$$

收到用迁移许可选项初始化的 SYN 后，主机 j 利用一个包含迁移许可选项的相应 TCP 栈，并将其存储在 SYN/ACK 字段中。类似地，主机 j 以同样的方式发送，即

$$j \to i:\{ID_j, K_j, Num_i, Num_j\}_{PK_i}$$

主机 i 将 Num_j 发送给主机 j 进行确认。

用迁移许可选项初始化主机接收 SYN/ACK 后，2 台主机能计算出共享秘密的密钥

$$K_{ij} = f(K_i, K_j)$$

该秘密密钥用于计算一个连接的有效连接标志，即该连接标志 T 通过计算密钥，和初始的序列号 N_i 和 N_j 一起散列化，利用安全哈希算法 *SHA*-1(主机 i 以主动状态发起连接，主机 j 处于被动状态)。

$$T = SHA\text{-}1(N_i, N_j, K_{ij})$$

当迁移许可选项交换计算时，*SHA*-1 产生的 160 bit 哈希数，除了有效的 64 bit，其余的都丢弃。因为 *SHA*-1 具有抗碰撞性，与另一个连接有相同的[地址，端口]对和相同连接标志的可能性很小，所以一个加密的安全 64 bit 连接标志能唯一标识该连接。

请求 R 通过连接的初始序列号 N、迁移 SYN 字段 S、连接密钥 K_{ij} 和请求序列号 I 计算得到 64 bit 的哈希数。

$$R = SHA\text{-}1(N_i, N_j, K_{ij}, S, I)$$

当 SYN 字段包含了上述迁移选项时就进行处理。接收到一个迁移选项的 SYN 包后，支持迁移的 TCP 栈尝试利用此连接标志查找连接的接收端口。每个连接的连接标志是在连接建立时预先计算的，减少了一个哈希查找过程。

如果连接标志有效，则以此[地址，端口]对建立的连接有相同的连接标志，且 reqNo 大于任何先前接收的迁移请求，因此，主机 i 计算 $R = SHA\text{-}1(N_i, N_j, K_{ij}, S, I)$，并和迁移 SYN 中的请求值进行比较：(1)如果比较失败，或连接标志无效，则发送一个消息到发布该迁移 SYN 的地址和端口处，且 SYN 忽略；(2)如果连接标志和请求都有效，但 reqNo 小于先前接收的请求，则 SYN 被认为是次序颠倒并被丢弃；(3)如果连接标志和请求都有效，且 reqNo 大于先前接收的请求，则认为该 SYN 字段有效，接受处理并准备迁移。

4.3 安全性分析

原有基于D-H协议的TCP连接迁移安全机制中存在可能受到中间人攻击的问题，攻击者可能获得 SYN，进而发起拒绝服务攻击。本文利用改进的 Helsinki 协议来协商迁移选项使用的连接密钥，通过对双方身份进行认证，在攻击者能监听的情况下，仍然能保证密钥在合法双方之间共享，有效防止了协商过程中的中间人攻击。

在发生连接迁移的过程中，攻击者要猜测正确的连接标志和请求以劫持该连接，因此，会频繁地产生迁移SYN，并发送到其中一台主机，期望能接收到SYN/ACK响应的一个正确猜测。因为安全哈希算法抗碰撞性和安全性使攻击者难以从 2^{63}SYN字段中成功猜出连接标志和请求，所以在实际中无须考虑上述攻击。

5 性能测试及结果分析

笔者在 Linux 操作系统 2.2.17 内核版本下进行 TCP 连接迁移实验，客户端地址为 25.20.184.208，H 和 O 为实现漂移的服务器节点地址，分别为 25.20.184.209, 25.20.184.210，使用一个 Hub 将其连接起来。一个连接迁移事件的 Tcpdump 跟踪情况如图 3 所示，它的采集是在客户端完成的。

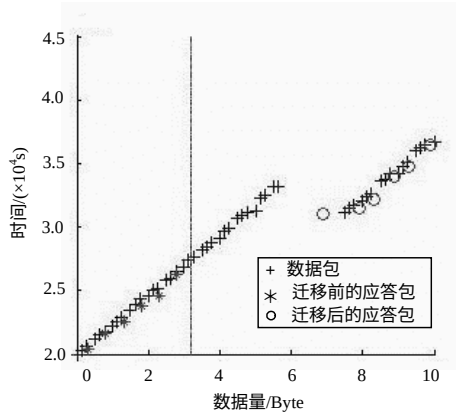

图 3 测试结果

测试开始时，客户端与 H 连接，经过一段时间后，当 t=4.9 s 时，H 出现故障，发出迁移信号 SYN，如图 3 虚线所示。由于已经不再与先前的地址相连，因此所有队列中的分段都在此处丢失。在 t=6.8 s 时，客户端的 SYN/ACK 到达。

由于 TCP 迁移选项没有改变 TCP 的拥塞控制和重传控制机制，因此客户端并不立即重新发送新的数据，而是等待丢失片段的应答信号。到 t=7.8 s 需要进行超时重传时，客户端才重传第 1 个丢失的片断。此时 O 机进行慢启动传输。

笔者进行了多次迁移测试，在整个测试过程中，客户端和服务器都能保持工作，正确发送并接收数据，没有因为出现异常情况而停止工作。可见，本文方案提高了系统安全性且不会影响网络性能。

6 结束语

本文 TCP 连接迁移技术对传统 TCP 协议进行修改，有效地阻止了协商过程中存在的中间人攻击。利用 *SHA*-1 算法对需要保护的连接标志和请求进行散列化，保证了连接迁移的安全性。TCP 连接迁移技术需要进一步探讨和研究，笔者将继续加强安全机制与动态漂移效率等方面的研究。

参考文献

[1] 杨 兵, 黄遵国, 胡光明. 基于高可用性的动态漂移技术研究[J]. 计算机工程与科学, 2004, 26(3): 4-6.

[2] Snoeren A C, Andersen D G, Balakrishnan H. Fine-grained Failover Using Connection Migration[C]//Proceedings of USENIX Symposium on Internet Technologies and Systems. San Francisco, California, USA: [s. n.], 2001.

[3] Sultan F, Srinivasan K. Migratory TCP: Highly Available Internet Services Using Connection Migration[R]. Rutgers, France: Rutgers University, Technical Report: DCS-TR-462, 2001.

[4] Snoeren A C, Balakrishnan H. An End-to-end Approach to Host Mobility[Z]. Cambridge, England: MIT Laboratory for Computer Science, 2000.

[5] Diffie W, Hellman M. New Directions in Cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[6] 卿斯汉. 安全协议[M]. 北京: 清华大学出版社, 2005.