

IKEv2 预共享密钥认证机制的改进算法

高振栋

(无锡科技学院, 江苏 无锡 214028)

摘要: 预共享密钥认证方式作为 IKEv2 中认证方式之一, 具有实施简单等优势, 但是该认证方式下预共享密钥容易被泄露, 从而导致整个认证过程的失败。为了解决以上缺陷, 文中尝试将预共享密钥、密钥恢复、秘密共享中的拉格朗日多项式门限方案等思想和方法结合起来并且提出了一种改进算法, 将认证双方预先共享的密钥进行拆分, 任何一方不能单独恢复预先共享的密钥, 从而降低了预先共享的主密钥泄露的可能性, 也防止了任何一方泄露预共享密钥造成认证失败的后果, 提高了预共享密钥认证方式的安全性。

关键词: IKEv2; 预共享密钥; 算法

中图分类号: TP393.08

文献标识码: A

文章编号: 1005-3751(2006)04-0044-02

Improved Algorithm for Pre-shared Key Authentication Mechanism in IKEv2

GAO Zhen-dong

(Wuxi College of Science and Technology, Wuxi 214028, China)

Abstract: As an authentication mechanism of IKEv2, pre-shared key authentication mechanism has advantages that easy to carry out. But, this kind of authentication mechanism is easy to disclose the pre-shared key, and leads to failure of authentication. To solve the above defects, the article tries to integrate the pre-shared key, key recover, secret share thoughts and methods, and brings up an improved algorithm to take apart the pre-shared key, descends the possibility of the leak the key, and prevents from disclosing the key result in the failure of authentication, enhances the safety of the pre-shared key authentication mechanism.

Key words: IKEv2; PSK; algorithm

0 引言

在现实的网络环境中, 安全问题举足轻重。IKE 协议作为密钥交换协议可以在 VPN 网关之间(不安全的公共网络)建立安全的通讯隧道。IKE 是一种混合型协议, 其复杂性一直受到业界广泛的批评。另外, IKE 还存在易受攻击、功能冗余等不足。目前, IKEv2^[1]作为 IKE 的替代者日益受到业界的普遍关注。

IKEv2 的认证方式可以有以下几种: RSA 数字签名、预共享密钥、DSS 数字签名。数字签名可以很有效地实现身份认证的功能, 但是需要第三方 CA 的认证, 而且系统开销较大。相对而言, 预共享密钥实施简单, 开销较小, 所以得到了广泛应用^[2,3]。但是, 该方式安全性较低, 如果认证任意一方无意或者蓄意泄露预先共享的密钥, 将可能导致认证的失败。文中试图对预共享密钥认证过程作出改进, 以提高该方式的安全性。

1 IKEv2 协商过程中预共享密钥认证方式

IKEv2 协商过程存在初始交换阶段, 主要协商 IKE-SA。在初始交换阶段中协商双方主要进行两次消息交换, 一共 4 条消息交互。第一次消息交换称为 IKE-SA-INIT 交换, 而第二次称为 IKE-AUTH 交换。

IKE-SA-INIT 交换过程如图 1 所示。第一条消息中的 HDR 表示 IKEv2 消息头, SA_i 包含了发起者针对 IKE-SA 的提案建议, 提案中包括加密算法、认证算法、DH 组等内容, KE_i 包含了发起者的 Diffie-Hellman 公开值, N_i 则表示发起者的 Nonce 值。

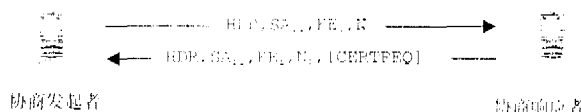


图 1 IKE-SA-INIT 交换过程

响应者接收到发起者发送的消息后在 SA_i 中选择某种提案形成 SA_r, 并且将 KE_r 和 N_r 分别作为响应者的 Diffie-Hellman 公开值以及 Nonce 值发送给发起者。在响应消息中, 响应者还可以包含可选的证书请求载荷发送给发起者。

IKE-SA-INIT 交换完成之后, 协商双方可以计算种

收稿日期: 2005-08-11

基金项目: 江苏省自然科学基金资助项目(BK2004039)

作者简介: 高振栋(1976-), 男, 江苏无锡人, 硕士研究生, 研究方向为计算机网络与安全。

子密钥 SKEYSEED 以便得到 7 个其他秘密:

(1) SK_{-d} 为建立在该 IKE_{-SA} 基础上的各个 CHILD_{-SA} 派生新的密钥材料。

(2) SK_{-ai} 和 SK_{-ar} 分别用于发起者和响应者方向的认证算法。

(3) SK_{-ei} 和 SK_{-er} 分别用于发起者和响应者方向加密后继的交互消息。

(4) SK_{-pi} 和 SK_{-pr} 分别用于发起者和响应者方向的认证载荷的计算。

随后进行的 IKE_{-AUTH} 交换使用前面协商得到的 IKE_{-SA} 中包含的加密、认证算法以及密钥进行保护,并且使用认证载荷对已经结束的 IKE_{-SA} INIT 交换过程进行认证,最终协商得到第一个 CHILD_{-SA},即 IPSec SA。如图 2 所示,IKE_{-AUTH} 交换过程中的 2 条消息是由 IKEv2 消息头 HDR 以及一个加密载荷组成,在这个加密载荷中包含了身份载荷(ID)、可选的证书载荷(CERT)以及证书请求载荷(CERTREQ)、认证载荷(AUTH)、安全关联载荷(SA)、流量选择载荷(TS)等。图 2 中的 SK_{-||} 表示被包含的载荷均被相应方向的 SK_{-e} 和 SK_{-a} 加密和认证保护。IKEv2 协商双方可以在认证载荷中指定认证算法,包括 RSA 数字签名、预共享密钥、DSS 数字签名三种认证方式。在预共享密钥方式下,认证载荷的认证数据计算如下:

$$\text{AUTH} = \text{prf}(\text{prf}(\text{Shared Secret}, \text{"Key Pad for IKEv2"}), \langle \text{msg octets} \rangle)$$

其中 Shared Secret 表示预共享密钥,“Key Pad for IKEv2”表示 17 个 ASCII 字符组成的字符串,⟨msg octets⟩表示消息字节。

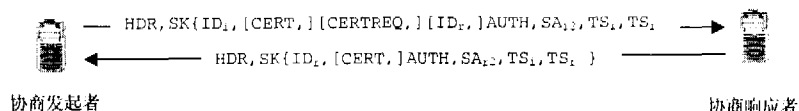


图 2 IKE_{-AUTH} 交换过程

在预共享密钥方式认证方式下,认证载荷中的认证数据是根据预先共享的密钥计算得到的。如果发起者或者响应者由于某种原因泄露了预先共享的密钥,公共网络中潜在的攻击者可以截获没有受到密码学技术保护的 IKE_{-SA} INIT 交换过程中的消息内容,计算出保护 IKE_{-AUTH} 交换过程的相关密钥。由于预先共享的密钥泄露,攻击者可以根据以上公式计算新的认证数据并且替代原有消息的正确数据,从而导致 IKE_{-AUTH} 交换对 IKE_{-SA} INIT 交换过程认证的失败。

2 改进的预共享密钥认证算法

为了解决以上缺陷,文中基于密钥恢复^[3]和秘密共享中的拉格朗日多项式门限方案^[4,5]等思路提出了一种改进型的预共享密钥算法。新的算法将存储在认证双方的预共享密钥进行了“拆分”,在需要进行认证的时候双方通

过数学方法恢复真正的共享密钥。算法主要思路如下:

(1) 假设预先共享的密钥 $K \in Z_p$, 认证双方预先随机选择某条直线表达式: $f(x) = ax + b, f(x) \in Z_p[x]$, 常数 $b = K$ 。认证双方都将 $f(x)$ 作为自己秘密的一部分。

(2) 认证双方在 Z_p 中选择两个非零的、互不相同的元素 x_1, x_2 , 计算 $y_i = f(x_i), 1 \leq i \leq 2$, 将 (x_i, y_i) 分配给认证双方 L_i, y_i 作为认证方 L_i 的秘密, 而 x_i 可以公开。每对数据 (x_i, y_i) 可以看作直线 $f(x) = ax + b$ 的一个点, 由于在平面上任意两点可以唯一确定一条直线, 所以密钥 K 可以由认证双方根据各自的秘密 y_i 重构得出, 而任意一方存储秘密的泄露都不会影响预共享密钥的安全性。

(3) 在实施认证的过程中, 认证方 L_i 利用 IKEv2 协商过程的 IKE_{-SA} INIT 交换中的 Diffie-Hellman 交换生成的临时密钥加密各自的 y_i 得到 Y_i , 然后将 Y_i 包含在 IKEv2 协商消息中发送给认证对方。

(4) 认证双方接收到对方的 Y_i 后使用 Diffie-Hellman 临时密钥进行解密, 利用得到的 y_i 重构共享密钥:

$$K = f(0) = \sum y_i = y_1 + y_2 = b$$

至此, 认证双方都计算出预先共享的密钥 K 。

(5) 认证双方可以利用计算得到的预共享密钥 K 按照传统的方式继续认证过程。

在以上改进后的预共享密钥认证算法中, 认证双方不存储真正的共享密钥, 改为记忆预先选择的直线方程和拆分后的秘密。即使某一方泄露了全部秘密, 攻击者也不能计算出真正的预共享密钥 K , 当然也无法通过认证, 所以改进后的算法大幅度减少了预共享密钥泄露的可能性, 提高了预共享密钥算法的安全性。另外, 如果存在恶意的第三方冒充合法认证一方, 双方在第 4 步重构计算得到的预共享密钥是不同的, 也就无法通过以后的认证步骤。

3 结束语

文中针对预共享密钥认证方式的弱点提出了相应的改进算法, 极大提高了该认证方式的安全性, 从而确保了 IKEv2 协商过程的安全性, 具有广阔的应用前景。

参考文献:

- [1] Kaufman C. RFC 草案 Internet Key Exchange (IKEv2)[S]. draft-ietf-ipsec-ikev2-17.txt, 2004.
- [2] 袁津生, 郭敏哲. 计算机网络安全实用编程[M]. 北京: 人民邮电出版社, 2005.
- [3] 胡向东, 魏琴芳. 应用密码学教程[M]. 北京: 电子工业出版社, 2005.
- [4] Kaufman C, Perlman R, Speciner M. Network Security Private Communication in a Public World(Second Edition)[M]. Beijing: Publishing House of Electronics Industry, 2004.
- [5] 冯登国, 蔡吉人. 网络安全与密码学[M]. 贵阳: 贵州科技出版社, 2004.