第 34 卷 第 2 期 计 算 机 工 程 2008 年 1 月
Vol.34 No.2 Computer Engineering January 2008
·安全技术· 文章编号：1000—3428(2008)02—0100—03 文献标识码：A 中图分类号：TP393.08

基于潜信道的 IPSec 密钥恢复方案

李 蕾，谷大武
（上海交通大学信息安全工程学院，上海 200240）

摘 要：传统密钥恢复协议采取增加密钥恢复字段的方法，恶意攻击者容易辨别具备密钥恢复功能的数据包，并进行过滤阻挠。该文将潜信道密钥恢复与具体协议相结合，提出基于IPSec协议的密钥恢复方案。该方案易于实施，数据包具有不可过滤性，可避免恶意攻击者的过滤阻挠，进行有效的网络监控。

关键词：密钥恢复；潜信道；密钥管理

Key Recovery Scheme of IPSec Based on Subliminal Channel

LI Lei, GU Da-wu
(School of Information and Security Engineering, Shanghai Jiaotong University, Shanghai 200240)

【Abstract】 The key recovery schemes available usually use the method of adding a key recovery field at the end of the protocol packet. So the intruder can easily distinguish the data packet with key recovery functions from the others and filtrate them in order to prevent key recovery. The paper describes an IPSec key recovery scheme based on subliminal channel. The scheme is easy to implement, and the packets are not filterable which can avoid the intruder's filtration. This scheme provides efficient network monitor and control.

【Key words】 key recovery; subliminal channel; key management

随着因特网及行业应用网的发展和通信技术的不断进步，密钥恢复这一课题越来越受关注。其中比较著名的有美国政府曾经使用的EES(Escrow Encryption Standard)，它使用LEAF(Law-Enforcement Access Field)作为附加块，增加在正常数据包的后面。1994 年，Blaze[1]提出了这种框架存在致命的缺陷：由于LEAF数据块的存在，因此拥有密钥恢复功能的数据流是可区分可被过滤的。普通用户可以很容易地察觉是否被监控，并可以方便地使用多种方法对监控进行扰乱。针对这种缺陷，Eu-Jin Goh和Dan Boneh[2]在 2003 年提出了一种基于潜信道机制的密钥托管框架，它与EES的根本区别在于，可恢复密文块并没有明显地附加在数据包后面，而是隐藏在具体的协议中，这样密钥恢复功能的数据流与正常数据流没有区别，唯有密钥恢复机构可以辨别并恢复密钥。本文将潜信道密钥恢复方案与IPSec安全协议相结合，充分利用原协议通信过程，使用潜信道技术实现密钥恢复。在必要的场合，使用这种提供密钥恢复的IPSec协议，可有效地抵御恶意第三方的过滤阻挠，提供高安全性和合法侦听功能。

1 相关协议和概念

1.1 ISAKMP 协议

Internet 安全连接和密钥管理协议(ISAKMP)是 IPSec 体系结构中一种主要协议。该协议结合认证、密钥管理和安全关联(SA)等概念来建立政府、商家和因特网上的私有通信所需要的安全。ISAKMP 定义了程序和信息包格式来建立、协商、修改和删除安全关联，以及密钥交换和认证数据的有效载荷。这些格式为传输密钥和认证数据提供了统一框架，而它们与密钥产生技术、加密算法和认证机制相独立。

1.2 潜信道

潜信道是由Simmons[3]于 1983 年提出，其目的在于证明当时美国用于核查系统中的安全协议的基本缺陷。潜信道是在公开信道中建立的一种实现隐蔽通信的信道，该信道中的潜信息以普通的数字签名信息形式隐藏起来。

将潜信道应用在与协议相结合的密钥恢复方案中，基本思想是：改变原有协议中的随机部分，例如对通信双方传递的随机数或者 nonce 进行替换，改传长度相符的密文。这些密文在不知情的用户看来，与原传递的随机数无异，其明文却可以是会话密钥信息，以便特殊部门得到数据包后，无需很大代价就可以对密钥进行恢复，达到侦听目的。

潜信道为密钥恢复方案带来的优势有两点：

(1)数据包的不可过滤性。潜信道将加密后的信息隐藏在协议中原随机数的部分，不知情的用户以及第三方即便截取到数据包，也无法将带有密钥恢复功能的数据包与正常数据包区分开来。它克服了以往密钥托管或密钥封装中，由于在数据包后面添加密钥恢复字段，而很容易被恶意用户识破的弱点。

(2)实用性。鉴于 IPSec 安全协议的广泛使用，与 IPSec 协议结合的密钥恢复方案有广阔的应用前景。政府部门可以与主要软件企业合作，在一些公用网络设施上，实施有密钥恢复的 IPSec 安全协议，既不会造成用户使用的不惯，又可以达到有效监控的效果。

2 基于潜信道的 IPSec 密钥恢复方案

2.1 主模式阶段

主模式有 6 条消息，具体过程如图 1 所示。涉及密钥交换的主要在第 3 条、第 4 条消息，内有 KE(Key Exchange)载

作者简介：李 蕾(1983－)，女，硕士研究生，主研方向：密钥恢复和网络安全；谷大武，教授、博士生导师

收稿日期：2007-02-10 **E-mail：**dwgu@sjtu.edu.cn

荷和 Nonce 载荷。密钥交换使用 Diffie-Hellman 协议，通信双方共享参数，并互相传递密钥信息后，各自生成共享密钥。

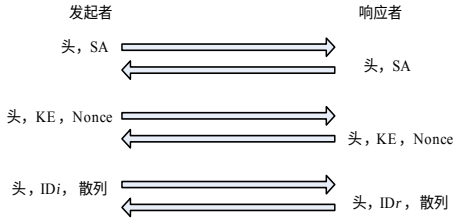

图 1　ISAKMP 主模式过程

假设通信双方为 Initiator 和 Responser，DH 参数为 g 和 p；Initiator 的私钥为 x，传送 g^x (KE)给 Responser；Responser 的私钥为 y，传送 g^y (KE)给 Initiator；那么共享密钥为 g^{xy}。

在第 3 和第 4 个数据包交换完成之后，参与通信的各方会生成如下 4 种秘密：

(1) $SKEYID$ ：后续的所有秘密都建立在它的基础上；

(2) $SKEYID\_d$ ：用于为 IPSec 衍生出加密的材料；

(3) $SKEYID\_a$ ：用来为 IKE 消息保障数据的完整性以及对数据源的身份进行验证；

(4) $SKEYID\_e$ ：用于对 IKE 消息进行加密。

$SKEYID$ 的生成取决于协商好的是何种验证方法。其他所有以 $SKEYID$ 为基础的秘密都以相同的方式衍生出来——无论验证方法是什么。

用以下符号表示一些数据：

(1)发起者 Cookie——$CKY-I$ ；

(2)发起者 nonce——N_i ；

(3)响应者 Cookie——$CKY-R$ ；

(4)响应者 nonce——N_r ；

(5)通信双方共享Diffie-Hellman秘密——g^{xy}。

用||表示连接关系，那么对于数字签名验证来说：

$$SKEYID = PRF(N_i \| N_r, g^{xy})$$

然后

$$SKEYID\_d = PRF(SKEYID, g^{xy} \| CKY-I \| CKY-R \| 0)$$

$$SKEYID\_a = PRF(SKEYID, SKEYID\_d \| g^{xy} \| CKY-I \| CKY-R \| 1)$$

$$SKEYID\_e = PRF(SKEYID, SKEYID\_a \| g^{xy} \| CKY-I \| CKY-R \| 2)$$

另外，为了验证交换中的双方，协议的发起者和响应者要分别产生 $HASH\_I$ 和 $HASH\_R$。

$$HASH\_I = PRF(SKEYID, g^x \| g^y \| CKY\_I \| CKY\_R \| SA_i \| ID_i)$$

$$HASH\_R = PRF(SKEYID, g^y \| g^x \| CKY\_R \| CKY\_I \| SA_i \| ID_r)$$

响应者接收到 $HASH\_I$ 后，按照规则计算出一个散列值，与接收到的 $HASH\_I$ 进行比较，如果相同，则通过验证，并向发起者回复 $HASH\_R$。发起者接收后，采用同样的方法验证。

在正常的协议过程之外，本文方案需要做的额外工作如下：

协议中除通信双方之外，还需存在一个可信第三方(TTP)，且通信双方拥有 TTP 的公钥(定义为 K_{TTP-Pu})，这是一个必要的前提。

用 K_{TTP-Pu} 对 DH 私钥进行加密，并隐藏在潜信道中传递出去。TTP 截取到数据包时，可以对潜信道部分进行解密，进而计算得到 DH 共享密钥。

采用非对称加密算法，用 K_{TTP-Pu} 加密 x 和 y，输出的密文具有伪随机性，与随机数相差无几。同时，在原协议中 Nonce 载荷作为一个伪随机数，恰好可以存放潜信道字段，且协议中对 Nonce 载荷的长度没有限制，这样避免了带宽不够的问题。

$$Nonce^1_{i\to r} = E_{K_{TTP-Pu}}(x)$$

$$Nonce^1_{r\to i} = E_{K_{TTP-Pu}}(y)$$

用 $Nonce^1_{i\to r}$ 替换原协议中的 N_i， $Nonce^1_{r\to i}$ 替换原协议中的 N_r。替换后的协议数据包在不知情的用户或者第三方看来，与正常 IPSec 协议无异。TTP 截获报文后，用私钥解密就可拥有 x 和 y。因此，TTP 通过截取协议数据包获得双方公钥后，可以很容易计算出主模式中的共享密钥 g^{xy}。

主密钥 g^{xy} 同时被通信双方和 TTP 获得，将其记作潜信道加密密钥 K_c。 K_c 可用作后续步骤中的加密密钥。

2.2　快速模式

快速模式有 3 条消息，具体过程如图 2 所示。这 3 条消息均被 ISAKMP 主模式中生成的 SA 所保护，具体来说，由 $SKEYID\_e$ 对消息进行加密，由 $SKEYID\_a$ 对消息进行完整性的保护。在 ISAKMP SA 的保护下，快速模式进行进一步协商，产生 IPSec SA，从而生成真正用来对数据加密的密钥，初始向量等信息。

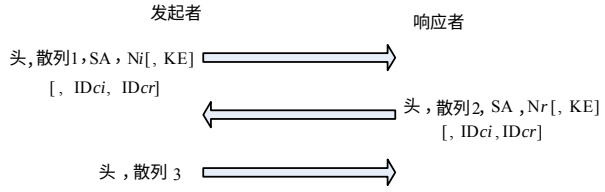

图 2　ISAKMP 快速模式过程

快速模式中提供一个 PFS(Perfect Forward Service)服务选项。如果选择该服务，需要额外一次 DH 密钥交换过程，其意义在于，即使攻击者攻破第 1 阶段的密钥交换(即攻破了 $SKEYID$ 等衍生密钥)，也只能阅读受 ISAKMP SA 保护的信息，却不能阅读受 IPSec SA 保护的信息。

在不提供 PFS 服务，即不包含 KE 载荷的时候，数据加密密钥材料(KEYMAT)的生成规则是

$$KEYMAT = PRF(SKEYID\_d, protocol) \| SPI \| N_i \| N_r)$$

在提供 PFS 服务，即包含 KE 载荷的时候，数据加密密钥材料(KEYMAT)的生成规则是

$$KEYMAT = PRF(SKEYID\_d, g^{ab} \| protocol) \| SPI \| N_i \| N_r)$$

可见，如果不提供 PFS 服务，可信第三方根据已获得的 ISAKMP 阶段共享密钥 K_c (即 g^{xy})，即可进行密钥恢复，得到真正会话密钥。

如果提供 PFS 服务，快速模式中就有另一次的 DH 密钥交换过程，生成新的共享密钥：Initiator 的私钥为 a，传送 g^a (KE)给 Responser；Responser 的私钥为 b，传送 g^b (KE)给 Initiator；那么快速模式中新的共享密钥为 g^{ab}。会话密钥将建立在新的共享密钥基础之上。密钥恢复需要做额外前提工作如下：

用主模式阶段产生的潜信道加密密钥 K_c，对新的 DH 私钥进行加密，并隐藏在潜信道中传递出去。TTP 截取到数据包时，可以对潜信道部分进行解密，进而计算得到新的 DH 共享密钥。

可采用对称算法用 K_c 加密 a 和 b，输出的密文具有伪随机性，与随机数相差无几。同时，在原协议中 Nonce 载荷作

为一个伪随机数，恰好可以存放潜信道字段，且协议中对 Nonce 载荷的长度没有限制，这样避免了带宽不够的问题。

$Nonce^2_{i\to r} = E_{K_C}(a)$

$Nonce^2_{r\to i} = E_{K_C}(b)$

用 $Nonce^2_{i\to r}$ 替换原协议中的 N_i， $Nonce^2_{r\to i}$ 替换原协议中的 N_r。替换后的协议数据包在不知情的用户或者第三方看来，与正常 IPSec 协议无异。

3 TTP 密钥恢复过程

本文以恢复出数据加密密钥材料(KEYMAT)为目标，用 KEYMAT 可以推导出会话密钥。下面依据是否支持 PFS 服务，分成两种情况进行描述。

3.1 无 PFS 服务的密钥恢复

在主模式阶段，通信双方 A 和 B 根据协议进行数据包的传递，且头 4 条消息均为明文。TTP 通过对网络的监听，截取到 A、B 之间的通信数据包是方便的。那么，密钥恢复过程如图 3 所示。

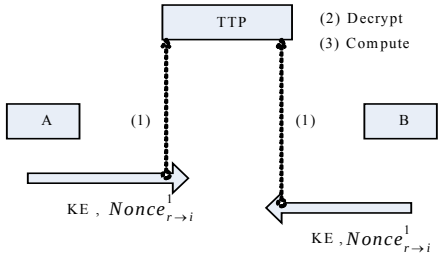

图 3 主模式密钥恢复过程

(1)可信第三方从截获数据包中得到通信双方公钥(g^x 或 g^y),Cookie($CKY-I$ 和 $CKY-R$),替换过的 Nonce($Nonce^1_{i\to r}$ 和 $Nonce^1_{r\to i}$)。

(2)TTP 用私钥对 $Nonce^1_{i\to r}$ 和 $Nonce^1_{r\to i}$ 进行解密，得到 DH 私钥 x 和 y。

(3)TTP 按解密出来的双方私钥 y 或 x，容易计算出 K_C (g^{xy})；并由已知信息计算出 $SKEYID$, $SKEYID\_d$, $SKEYID\_a$,$SKEYID\_e$ 密钥信息。

在快速模式阶段，所有消息均受 ISAKMP SA 保护，因此截获的数据包均为密文。密钥恢复过程如图 4 所示。

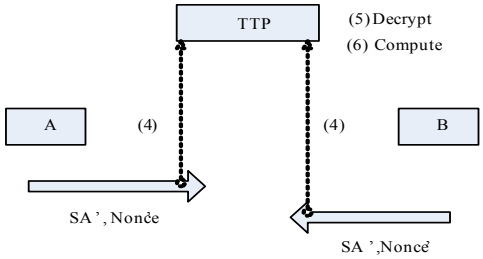

图 4 快速模式密钥恢复过程

(4)可信第三方继续截获 A、B 通信密文数据包。

(5)TTP 可用 $SKEYID\_e$ 对消息解密，得到快速模式的明文。明文中包括双方产生的新 Nonce′以及 SPI(SA 载荷中)等信息。

(6)TTP 拥有了所需的参数，根据规则，可计算出数据加密密钥材料(KEYMAT)：

$KEYMAT = PRF(SKEYID\_d, protocol) \| SPI \| N_i \| N_r)$

3.2 有 PFS 服务的密钥恢复

主模式阶段与 3.1 节中步骤(1)~步骤(3)类似，TTP 计算出 K_C , $SKEYID$, $SKEYID\_d$, $SKEYID\_a$, $SKEYID\_e$ 等密钥信息。

在快速模式阶段，通信数据包是密文，与 3.1 节不同之处在于：存在 KE 载荷进行新一轮的密钥协商，并且新的 Nonce 载荷被用作潜信道隐藏密钥信息。密钥恢复过程见图 5。

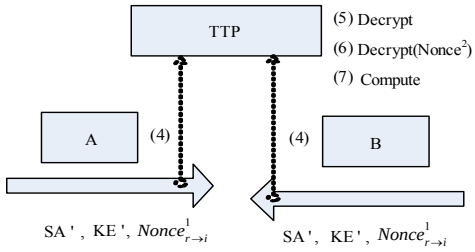

图 5 PFS 快速模式密钥恢复过程

(4)可信第三方继续截取通信双方的密文数据包。

(5)TTP 可用 $SKEYID\_e$ 对消息解密，得到快速模式的明文。明文中包括 SPI(SA 载荷中)、新的交换密钥 KE′(g^a 和 g^b)、被替换过的 $Nonce^2_{i\to r}$ ($= E_{K_C}(a)$)和 $Nonce^2_{r\to i}$ ($= E_{K_C}(b)$) 等信息。

(6)TTP 用潜信道加密密钥 K_C 对 $Nonce^2_{i\to r}$ 或 $Nonce^2_{r\to i}$ 进行解密，得到通信双方的私钥 a 或 b。

(7)TTP 根据解密得到的私钥和截获数据包得到的公钥，计算出快速模式下 DH 共享密钥 g^{ab} ；TTP 拥有了所需的参数，根据规则，可计算出数据加密密钥材料(*KEYMAT*)：

$KEYMAT = PRF(SKEYID\_d, g^{ab} \| protocol) \| SPI \| N_i \| N_r)$

4 方案分析

本文提出的方案，在提供密钥恢复功能的基础上，仍保证协议的高安全性。恶意供给者要想得到数据加密密钥材料(KEYMAT)，根据生成规则，必须得到 g^{ab} 和 $SKEYID\_d$ 等秘密信息，也就是说，恶意攻击者必须得到主模式和快速模式中两个共享密钥 g^{xy} 和 g^{ab} 才能恢复出 *KEYMAT*。鉴于通信双方使用 DH 进行密钥交换，只有通信双方和 TTP 知道共享密钥 g^{xy} 和 g^{ab} 。可见，本文提出的方案保持了原 IPSec 协议的安全性。另外，本文侧重讨论数字签名认证方式的协商过程，当完成了主模式前面 4 条消息的交换以后，第 5 条和第 6 条消息主要用于对已交换的 IKE 消息进行一致性检查并且对对方进行身份验证。发起方和接收方利用协商好的 HMAC 模式的散列算法(或协商好的伪随机算法)，分别使用私钥对 $HASH\_I$ 和 $HASH\_R$ 进行数字签名，得到 SIG_I 和 SIG_R 。数字签名中使用私钥，因此在消息中分别附上了证书 CERT，以便验证运算中使用相对应身份的公钥。实际使用中，使用数字签名认证方式的最后两条消息为：

(5)I->R Header ID*i* CERT SIG_I;
(6)R->I Header ID*r* CERT SIG_R;

采用数字签名认证方式时，中间人攻击者能够获得发起方和接收方的 KE，进而能够获得发起方的身份 ID*i*，但是由于不能得到发起方的签名私钥，不能生成 SIG_I ，不能完成协议，因此中间人攻击无法成功。

可见，本文对原 IPSec 协议进行补充使其具备密钥恢复功能，同时也没有影响到协议的抗攻击性。以后 IPSec 协议

(下转第 110 页)