第35卷 第18期 计 算 机 工 程 2009年9月
Vol.35 No.18 Computer Engineering September 2009
·安全技术· 文章编号：1000—3428(2009)18—0113—03 文献标识码：A 中图分类号：TP393.08

改进的空间网络密钥交换协议

吴 举，杜学绘，钱雁斌，曹利峰
（解放军信息工程大学电子技术学院，郑州 450004）

摘 要：针对空间网络的特点及空间网络对密钥交换的特殊需求，提出一种适用于空间网络的密钥交换协议。该协议以Internet密钥交换协议为基础，通过增加DH循环队列、提高Cookie计算强度的方法增强其抗拒绝服务攻击的能力，给出抵御中间人攻击、选项攻击及反射攻击的修正方法。理论分析表明，该协议具有更高的安全性和较少的交换次数，更适用于空间网络通信环境。

关键词：空间网络；密钥交换协议；Internet密钥交换协议

Improved Key Exchange Protocol for Space Networks

WU Ju, DU Xue-hui, QIAN Yan-bin, CAO Li-feng
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 Aiming at the characteristics of space networks and their special requirements for key exchange, this paper proposes a key exchange protocol for space networks. It is based on the Internet Key Exchange(IKE) protocol, and robust to Denial of Service(DoS) attacks by adding circular DH queue and increasing the calculate intensity of Cookie. Some improved methods are presented in defending man-in-middle attack, option attack and reflect attack. Theoretical analysis shows that the protocol has more security, less exchange messages and it adapts to the space networks.

【Key words】 space networks; key exchange protocol; Internet Key Exchange(IKE) protocol

1 概述

空间网络的通信安全需求一般包括对信息节点之间的认证以及对信息链路的机密性、完整性保护。为了满足上述安全需求，最重要的是实现信息节点之间安全、可靠的密钥交换和身份鉴别。由于空间网络具有时延长、可用带宽低、节点计算能力有限等特点，因此对空间网络密钥交换协议的研究和分析成为空间网络安全问题研究的重点和难点。

Internet密钥交换(Internet Key Exchange, IKE)协议[1]是目前较为通用的一种密钥交换协议，可用于任何需要协商安全信息的场合，该协议在卫星网络和空间网络的密钥管理和交换中被广泛采用。一些研究机构如空间数据系统咨询委员会、美国国家航空和宇宙航行局均建议在其空间通信协议中采用IKE协议的某种模式或其改进形式实现其密钥交换[2]。

2 IKE及其改进协议

2.1 IKE协议

IKE协议由IETF提出，是IPSec服务默认的密钥协商协议，其密钥协商分2个阶段进行：第1阶段建立一个IKE SA；第2阶段使用阶段1产生的IKE SA建立IPSec SA。

IKE协议在设计上存在协商机制过于复杂和交换消息过多的问题。其第1阶段协商分为主模式和野蛮模式，在每种模式下又根据认证方式的不同分为预共享密钥、数字签名、标准公钥加密和修订公钥加密4种不同的交互方式，整个协商过程需主模式6条消息及快速模式3条消息才能完成。IKE协议还易受拒绝服务(Denial of Service, DoS)攻击，攻击方法主要有：通过大量虚假请求使响应方保留大量无用的状态信息而耗尽存储资源；在认证前使响应方计算大量的模数乘法运算或对消息5的验证运算而耗尽CPU资源。同时，其主模式下发起方的身份信息只能抵御被动攻击而不能抵御中间人的主动攻击。其他攻击方式包括选项攻击、反射攻击[3]等。这些缺点在空间网络中尤为突出。

由于野蛮模式速度快且适用于带宽受限的环境，因此有人提出将数字签名认证方式的野蛮模式直接应用于空间网络的密钥交换。而野蛮模式是以牺牲一定的安全性为代价换取速度优势的，它不提供身份保护且不能抵御DoS攻击，并不完全适用于空间网络环境。

2.2 IKEv2协议

由于新的需求和实际应用中的问题不断出现，IETF对IKE协议不合理的部分积极征集修改意见，并于2005年底正式发布了新版本——IKEv2[4]。新版本保留了IKE协议的两阶段协商思想，对协议进行了简化整合，将第1阶段不同的模式、认证方法统一为一种方式，同时减少了交换的消息数，提高了协商效率，并通过改进Cookie技术提高了协议抗耗尽存储资源的DoS攻击的能力。但其仍存在交换消息数不固定、易受耗尽CPU资源的DoS攻击和不能抵抗对发起方身份进行主动攻击等缺点。

2.3 JFK协议

JFK(Just Fast Keying)[5]协议是IETF为代替IKE协议而设计的另一种密钥交换协议。它提出了一种新的密钥交换体制，取消了IKE两阶段的交换思想，只保留了一个阶段，简化了消息交换次数，并采取了有效的方式防止DoS攻击，使协议效率和安全性更高，实现也更为简单。然而其同样存在缺陷，如不能保证完美前向保密(Perfect Forward Secure, PFS)、可能由于发起方不支持响应方提出的算法而使整个通

基金项目：国家“863”计划基金资助项目(2006AA701416, 2007AA701309)

作者简介：吴 举(1982－)，男，硕士研究生，主研方向：网络安全；杜学绘，副教授；钱雁斌、曹利峰，博士研究生

收稿日期：2009-01-17 **E-mail：**Wu_Ju1982@163.com

信无法进行、不能同时为双方身份信息提供抗主动攻击保护。

3 空间网络对密钥交换的要求

由于空间网络具有长延时、可用带宽低、错误率高、节点计算能力有限等特点，因此其密钥交换协议应着重考虑以下 4 个方面的要求：(1)空间网络与地面网络相比更易受攻击和干扰，协议应具有较高的安全性、可靠性及较好的抗 DoS 攻击能力。(2)考虑到空间网络的时延长，协议的消息交换数应尽可能少，且不需要与第三方实时交互，以保证认证效率。(3)对于计算能力有限的空间节点，应尽可能采用开销较少同时能保证安全性的加解密算法。(4)算法尽量采用非对称密钥体制，可在空间节点中预先注入私钥，认证时交换并验证公钥证书，在实现离线认证的同时提高系统的可靠性。

4 改进的空间网络密钥交换协议

本文针对 IKE 协议、IKEv2 协议和 JFK 存在的安全隐患，结合空间网络对密钥交换的具体要求，对 IKE 协议进行了改进，使其适用于空间网络的密钥交换。

4.1 协议的改进思想

在交换阶段仍沿用 IKE 的两阶段交换模式。在两阶段交换模式中，阶段 1 生成 IKE SA 后，可用于生成多个阶段 2 的 SA，更易对现有 SA 重新生成密钥，从整体上提高密钥交换的效率。为了提高协议的利用率、使其更适用于空间网络，可适当延长 IKE SA 的生命周期。

为进一步简化协议，JFK 协议取消了加密认证算法的协商，而是由响应方在第 2 条消息中指定所用的加密和认证算法。这样虽然简化了消息，却可能出现发起方不支持响应方所提出的加密或认证算法而使协商不能正常进行的情况。为了避免这种情况，在消息 1 中分别列出发起方所支持的加密和认证算法，同时将协议提议算法以套件的形式给出，算法套件可以公开获得。在协议中不出现具体的算法，而用指针指向事先设定的算法套件。这样既避免了过多的提议组合，又大大简化了消息长度，符合空间网络低带宽的要求。

为增强协议的抗耗尽存储资源的 DoS 攻击能力，可通过改进的高强度 Cookie 值对发起方进行验证。发起方未经验证前，响应方无须进行代价昂贵的计算，也不需要创建和保留任何状态信息，实现通信双方的无状态交互。针对耗尽 CPU 资源的 DoS 攻击或多个合法用户的连接请求同时到达的情况，原有的 D-H 值计算方式会消耗大量的计算资源且不能满足时效性的要求。在改进协议中增加了一个 D-H 循环队列以及队列指针 *Kp*，对每一个 SA 请求，响应方都从 D-H 队列中取出当前指针 *Kp* 所指的 D-H 值参与协商。若协商成功，则从 D-H 队列中删除使用过的项，并在处理器空闲时计算一组新值存放到队列里；若协商失败，则 D-H 值可以不删除而重新使用。这样既能提高新协议抗 DoS 攻击的能力，又能更好地利用空间节点有限的计算资源，同时保证协议的 PFS。

4.2 对协议的改进

协议涉及的术语[1]有：(1)*HDR*，消息头；(2)*Sax*，由 *x* 提供的安全联盟；(3)*KEx*，*x* 的 Diffie-Hellman 密钥因子；(4)*Nx*，由 *x* 生成的随机数；(5)*IDx*，*x* 的识别符号；(6)*Kir*，由 *KEi* 和 *KEr* 产生的 Diffie-Hellman 密钥；(7)*SIG*，数字签名字段；(8)[*x*]，表示 *x* 字段是可选的；(9)*prf*(*key, msg*)，带密钥的哈希函数；(10)*CKY-I* 和 *CKY-R* 是分别由发起者 *I* 和响应者 *R* 产生的随机数“Cookies”，是为一个密钥、对方的身份以及一个时间计数器值进行综合散列运算而创建的。

为简化协议并满足空间网络对协议算法的要求，改进的协议取消了野蛮模式，只保留数字签名认证方式，除了计算量和安全性方面的考虑外，该方式还可提供不可否认性服务。消息交换都是以包含 Cookie 的 ISAKMP 头开始，发起方先要猜测双方都支持的 D-H 参数群，交换的消息数只有 4 条，改进后的协议传递消息如下：

$$(1)I \rightarrow R: HDR, KEi, Ni, Sai$$

$$(2)R \rightarrow I: HDR, KEr, Nr, Sar, Kp, [CRQ]$$

$$(3)I \rightarrow R: HDR, KEi, Kp, Ni, Nr, Sai, Sar, <HASH(IDi), Sai2, SIGi, [CERTi], [CRQ]>Ke, AUTH$$

$$(4)R \rightarrow I: HDR, <IDr, Sar2, SIGr, [CERTr]>Ke, AUTH$$

消息(1)中包括发起者的 D-H 公共值、随机数 *Ni* 和发起方所支持的阶段 1 的 SA 提议，由响应方从中选择其所支持的算法套件。

消息(2)中包括响应方选择的 SA 提议、D-H 循环队列的当前指针 *Kp* 及其指向的 D-H 公开值 *Ker*、随机数 *Nr*、证书请求 CRQ 和一个改进的高强度的 Cookie。指针 *Kp* 的使用使得发起方不需要将整个 D-H 公钥发回，只需发送一个索引值，从而缩减了消息长度，减少了空间节点的传输负担。改进的 Cookie 值计算公式如下：

$$CKY\text{-}R = prf(Secret, IPi \mid Sar \mid KEi \mid Kp \mid Ni \mid Nr) \quad (1)$$

其中，增加的 *Sar, Kp* 等新元素在几乎不增加空间节点计算量的情况下，增强了 Cookie 的强度，可更好地防止耗尽存储资源的 DoS 攻击和重放攻击；本地密钥 *Secret* 经一定时间间隔后进行变换。由于响应方在发送消息(2)时并不能确认消息(1)是否来自合法的发起方，可能是一个 DoS 攻击的伪造消息，因此响应方不必进行复杂的计算，也不保留任何状态信息，在响应者发出消息 2 后就可以删除所有的连接状态。

消息(3)将发送方的 D-H 公开值 *Kei*、*Ni* 和消息(2)中除 D-H 公开值以外的内容未加密地包括其中，其他内容如发起方身份信息 *IDi* 的哈希值 *HASH*(*IDi*)、发起方证书、对响应方的证书请求、阶段 2 的 SA 请求和发起者的数字签名 *SIGi* 均加密传输。整个消息由 AUTH 进行认证。响应者收到消息(3)后先检查 *Kp* 是否正被使用，若未被使用过，则丢弃消息(3)；若使用过，则从 D-H 循环队列中取出相应的 D-H 值，重新计算 Cookie 值并与收到消息中的 *CKY-R* 比较，验证返回数据的合法性，通过验证则说明消息(1)和消息(3)来自同一个 IP 地址，进一步对加密部分进行解密，验证发起方的数字签名，同时从 D-H 循环队列中删除该使用过的 D-H 值，据此检测和防止“Cookie-jar”型 DoS 攻击，若未通过验证，则将消息(3)丢弃。对消息(3)的这种处理可以保证每一个成功的会话使用不同的 D-H 值，且不为非法的会话计算新的 D-H 值，从而既实现了 PFS，又很好地防止了 DoS 攻击。

由于空间网络的开放性且空间节点身份信息更为敏感，交换过程中节点的身份信息更易受中间人主动攻击。为使发送方的身份信息也能抵御中间人的主动攻击、进一步提高对空间节点身份信息的保护，在消息(3)中用 *HASH*(*IDi*)代替 *IDi*，这样即使主动攻击者解密并获得消息载荷，也不能直接由 *HASH*(*IDi*)得到发送方的身份信息。实现中可预先计算出一个或多个 *HASH*(*ID*)，并将每个 *ID* 与其哈希值绑定在一起。这样在响应方得到 *HASD*(*ID*)后，可根据哈希值及其哈希算法查找到对方的身份。为了增大攻击者暴力破解的难度，用户的 *ID* 信息必须保持一定的长度。

消息(4)在响应方验证发方的数字签名合法后发出，包括响应方的身份信息、数字签名、证书以及对阶段 2 提议的 SA。

整个消息加密发送并由 AUTH 进行认证。发起方通过解密消息验证签名，验证响应方存在并参与了会话，而签名的存在可对整个会话过程提供不可否认性。其加密、认证密钥的生成同 IKE 协议的密钥生成，如下所示：

$$SKEYID = prf(Ni \mid Nr, Kir) \quad (2)$$

$$SKEYID\_d = prf(SKEYID, Kir \mid CKY\text{-}I \mid CKY\text{-}R \mid 0) \quad (3)$$

$$SKEYID\_a = prf(SKEYID, SKEYID\_d \mid Kir \mid CKY\text{-}I \mid CKY\text{-}R \mid 1) \quad (4)$$

$$SKEYID\_e = prf(SKEYID, SKEYID\_a \mid Kir \mid CKY\text{-}I \mid CKY\text{-}R \mid 2) \quad (5)$$

$$AUTH = prf(SKEYID\_a, message) \quad (6)$$

$$SIG = Sig(HASH) \quad (7)$$

为了防止选项攻击和反射攻击，对双方认证的哈希值 *HASH_I* 和 *HASH_R* 的计算方法进行改进，在其中引入 *Sar* 以避免选项攻击；改变 *Sar* 在双方计算公式中的位置，使双方在遭受反射攻击时，能够根据计算得出的 *MAC* 值和收到的 *HASH* 值不同而停止协商，如下所示：

$$HASH\_I = prf(SKEYID, KEi \mid KEr \mid CKY\text{-}I \mid CKY\text{-}R \mid Sai \mid Sar \mid IDi) \quad (8)$$

$$HASH\_R = prf(SKEYID, KEr \mid KEi \mid CKY\text{-}R \mid CKY\text{-}I \mid Sar \mid Sai \mid IDr) \quad (9)$$

5 改进协议的安全性及性能分析

在安全性方面，改进协议通过高强度 Cookie 实现通信双方的无状态连接，以应对耗尽存储资源的 DoS 攻击。通过增加 D-H 循环队列的方法，使每次协商 SA 都使用新的 D-H 值，且只有成功协商 SA 后才重新计算 D-H 值，在实现 PFS 的同时有效防止了耗尽计算资源的 DoS 攻击。用 *HASH*(*IDi*)代替消息(3)中的 *IDi*，增强了发送方身份信息抗中间人主动攻击的能力。在改进的双方认证哈希值的算法中，由于加入了双方的 SA 信息并破坏了其元素排列的对称性，因此能够防止选项攻击和反射攻击。

在性能方面，新协议将 IKE 的 2 种模式、4 种认证方式统一为一种方式，简化了协议的描述。整个协商过程仅需要 2 次交互共 4 条消息即可完成 IKE 协议需主模式和快速模式共 9 条消息才能完成的功能，大大缩减了消息数，降低了通信开销，提高了效率，这些都符合空间网络可用带宽低、时延长的特点。虽然认证哈希值的计算中增加了新的元素，但对于双方来说，由此引入的计算量是微不足道的，而 D-H 循环队列和 *HASH*(*ID*)的存在则会给空间网络节点增加一定的存储负担。

6 结束语

本文协议考虑了空间网络可用带宽低、时延长、节点计算存储资源有限等特点，在保证协议安全性的基础上，简化了交换过程，减少了通信开销。由于空间网络密钥交换是一个较新的研究领域，因此如何实现协议的安全性、复杂性及计算、存储资源的最大优化协调，还需要进一步的研究。

参考文献

[1] Harkins D, Carrel D. The Interact Key Exchange Protocol(IKE)[S]. RFC 2409, 1998.

[2] CCSDS 733.5-O-1 Next Generation Space Internet(NGSI)——End-to-End Security for Space Mission Communications[S]. 2003.

[3] 范　红. 互联网密钥交换协议及其安全性分析[J]. 软件学报, 2003, 14(3): 600-605.

[4] Kaufman C. Internet Key Exchange (IKEv2) Protocol[S]. RFC 4306, 2005.

[5] Aiello W, Bellovin S, Blaze M. Just Fast Keying: Key Agreement in a Hostile Internet[J]. ACM Transactions on Information and System Security, 2004, 7(2): 48-58.

编辑　张　帆

(上接第 112 页)

间服务器获得标准时间，因此，它们存在网络引起的延时(100 ms 以内)。表中最后一列是根据第 4 节提出的时间服务器的精度区间 $\left[(\theta-\frac{\beta-\gamma}{2})-\frac{\delta}{2},(\theta-\frac{\beta-\gamma}{2})+\frac{\delta}{2}\right]$ 计算得出，对照表中的实测数据，二级时间服务器的网络延迟、时钟偏移量较一级时间服务器的要小些。

表 2　部分一级、二级 NTP 服务器测试结果

行号	服务器	级别	精度/ms	根延时/ms	时钟偏移/ms	β/ms	γ/ms	往返延时/ms	$\beta=\gamma$ 精度区间	$\beta\neq\gamma$ 精度区间
1	204.123.2.72	1	1.8E-02	0	940	177	58	520	[680, 1 200]	[620, 1 140]
2	18.26.4.105	1	1.9E-02	0	937	319	166	500	[677, 1 187]	[600, 1 110]
3	133.100.9.2	1	1.8E-02	0	936	158	14	572	[650, 1 222]	[578, 1 150]
4	128.250.36.2	1	1.8E-02	0	924	414	227	540	[654, 1 194]	[560, 1 100]
5	130.149.17.21	1	1.8E-02	0	934	395	230	524	[672, 1 196]	[589, 1 113]
6	142.3.100.15	2	2.0E-02	57	717	935	471	406	[514, 920]	[282, 688]
7	199.240.130.1	2	2.5E-02	99	798	311	111	422	[587, 1 009]	[487, 909]
8	200.144.121.33	2	2.6E-02	31	743	377	264	426	[530, 956]	[473, 899]
9	130.235.20.3	2	2.7E-02	95	769	351	290	442	[548, 990]	[374, 816]
10	129.127.28.4	2	2.1E-02	20	715	175	90	456	[487, 943]	[444, 900]

由于 NPT 算法中的距离是指对应的层数与同步距离的乘积，而同步距离又与网络延迟有关，通过计算得出结论：二级时间服务器置信区间的范围更小，精确度更高；客户端对二级时间服务的同步精度确实要优于一级时间服务器。通过比较表中的最后 2 列可知：$\left[(\theta-\frac{\beta-\gamma}{2})-\frac{\delta}{2},(\theta-\frac{\beta-\gamma}{2})+\frac{\delta}{2}\right]$ 在时间精度区间方面优于 $\left[\theta-\frac{\delta}{2},\theta+\frac{\delta}{2}\right]$。通过对传输时延 γ，β 的深入讨论，可以看出传输时延对精度区间有很大影响，因此，通过精度区间的大小须对时间服务器重新排队。例如在二级时间服务器 $\beta=\gamma$ 的情况下，表 2 中第 10 行的时间精度要好于第 6 行~第 9 行；但是 $\beta\neq\gamma$ 的情况下，第 6 行要好于第 7 行~第 10 行。

5 结束语

本文研究了 NTP 在 TCP/IP 网络中的传输机制，讨论了 NTP 在同步过程中的网络误差。由于网络时间协议在安全性、精确度方面性能较低，因此须对协议进行修改。在安全性问题上，可使用自动钥(Autokey)，把公钥密码算法和一个伪随机钥流结合在一起，以脱机模式签名和验证时间值，同时用钥流来鉴别与签名值有关的分组，而且自动钥是完全自组织的，服务器和客户机可以在任意拓扑结构下配置和再配置，无须人为干预。

参考文献

[1] Mills D L. Network Time Protocol(Version 3) Specification, Implementation[S]. RFC 1305. 1992.

[2] 贺　鹏, 李　菁, 吴海涛. 网络时间同步算法研究与实现[J]. 计算机应用, 2003, 23(2): 15-17 .

[3] 陈　敏. 基于 NTP 协议的网络时间同步系统的研究与实现[D]. 武汉: 华中科技大学, 2005.

[4] 李明国, 宋海娜. 计算机时钟同步技术研究[J]. 系统仿真学报, 2002, 14(4): 477-480.

[5] 赵　龙. 基于 NTP 协议的网络授时研究[D]. 阜新: 辽宁工程技术大学, 2006.

编辑　顾姣健