通用可组合安全的 Internet 密钥交换协议

彭清泉，裴庆祺，杨 超，马建峰
(西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071)

摘要：通过对新一代 Internet 密钥交换协议(IKEv2)进行分析，指出了其初始交换过程中存在发起者身份暴露和认证失败问题.而在无线接入网络环境下，对发起者身份等敏感信息进行主动保护是十分必要的.提出了一种适用于无线网络环境下的 Internet 密钥交换协议，该协议让响应者显式地证明自己的真实身份，实现了对发起者主动身份保护.并通过重新构造认证载荷，有效防止了认证失败问题.在通用可组合安全模型下，证明了该协议达到了通用可组合安全.性能分析和仿真实验表明，该协议具有较少的计算量和通信量.

关键词：Internet 协议安全；密钥交换；Internet 密钥交换协议；可证安全；通用可组合
中图分类号：TP393 **文献标识码**：A **文章编号**：1001-2400(2009)04-0714-07

Universally composable secure Internet key exchange protocol

PENG Qing-quan, *PEI Qing-qi*, *YANG Chao*, *MA Jian-feng*
(Ministry of Education Key Lab. of Computer Network and Information Security, Xidian Univ., Xi'an 710071, China)

Abstract: The new Internet key exchange protocol (IKEv2) is analyzed, and it is found that the protocol can not achieve active identity protection to the initiator and has the security flaw of authentication failure in its initial exchange. However, it is necessary to protect the identity information to the initiator under the environment of a wireless access network. In this paper, a novel key exchange protocol for the wireless network based on IKEv2 initial exchange is proposed, which realizes active identity protection to the initiator by the responder explicitly proving his true identity, and achieves successful authentication by reconstructing the authentication payload. With the Universally Composable (UC) security model, this new protocol is analyzed in detail, with the analytical results showing that it affords provably UC security. Performance analysis and simulation results show that the proposed protocol has less computation and communication overhead.

Key Words: Internet protocol security; key exchange; Internet key exchange protocol; provably secure; universally composable

随着 WLAN，WiMAX 以及 3G 等无线网络技术的日益成熟，人们可以通过各种无线网络方便地接入 Internet.然而无线接入网络带来便利的同时，伴随的安全问题也越来越突出.IPSec 协议是 IP 互联网的网络层安全标准，它能为 IP 数据包提供完整性、机密性、数据源认证等安全服务.Internet 密钥交换协议(IKE)是 IPSec 中的密钥协商协议，用于动态地建立为通信双方协商 IPSec 所需的安全关联(SA)(包括密钥、密码算法、认证算法、密码参数等).虽然 IKEv1[1]得到了广泛应用和支持，但由于其协议轮数较多、过于复杂、协商效率较低并且不能有效地防止拒绝服务攻击(DoS 攻击)和中间人攻击等类型的攻击，IETF 工作组提出了 IKEv2[2]来替代 IKEv1.这两个版本的协议均采用了 SIGMA[3]协议结构.Boyd 等人[4]分析指出：在 IKEv2 协议中和 IKEv1 一样也存在认证失败的问题，如果采用分布式攻击的话，这种安全缺陷容易造成严重的 DoS 攻击.另外，IKEv1 协议在身份保护方面的脆弱性问题，也同样存在于 IKEv2 的初始交换中.而在

收稿日期：2008-11-21
基金项目：国家自然科学基金资助(60633020，60573036，60803150)
作者简介：彭清泉(1980-)，男，西安电子科技大学博士研究生，E-mail：qingquanpeng@sina.com.

用户通过无线接入 Internet 的情况下,用户身份等敏感信息的保密性显得尤为重要,IKE 协议应当对协议发起者提供主动的身份保护. IETF 工作组采用 IKEv2-EAP[5] 的方法来解决这个问题,但协议性能并不理想. 作为互联网安全关键技术之一,对 IKEv2 协议进行深入分析和改进有着重要的意义.

可证明安全方法最早由 Bellare 和 Rogaway[6] 于 1993 年提出来,这是近年来比较流行和公认的安全协议形式化分析与设计方法. 1998 年 Bellare 等人引入模块化的思想,提供了可重用的模块来构造新的可证安全的协议. 这种方法由 Canetti 和 Krawczyk 于 2001 年进一步扩展,称之为 CK 模型[7]. 这些可证明安全模型和方法都只适用于对孤立环境下的协议设计和分析,为此 Canetti 提出了通用可组合安全(Universally Composable Security, UC 安全)模型[8-9],该模型最重要的属性是它能够确保协议在任意的和未知的多方环境中运行时仍然是安全的. 在复杂环境中,协议的安全性可以通过通用可组合定理来得到保证. 通用可组合安全是更高级别的安全定义,它的抽象层次远超过其他模型,在安全协议设计和分析中具有重要的作用[10].

笔者对 IKEv2 协议进行了深入研究,分析了其初始交换过程中存在的两个安全缺陷. 针对无线接入网络特点,在 IKEv2 的基础上,提出了一个改进的 Internet 密钥交换协议. 在通用可组合安全模型下对改进的协议进行了安全性证明,结果表明改进的协议达到了通用可组合安全级别. 在性能方面与相关协议进行了对比分析,并给出了仿真实验结果.

1　通用可组合安全模型

通用可组合安全(UC 安全)模型为密码学协议的安全性定义提供了一种形式化描述方法. 符合 UC 安全定义的协议被称为是通用可组合安全的. 通用可组合安全是现实网络环境中的实际需求,在孤立环境模型中被证明是安全的协议在并发组合情况下并不一定是安全的,仅仅在孤立环境模型中设计和证明安全协议是不够的. 而 UC 安全模型可以用来描述和分析并发组合情况下密码协议的安全性,它能够确保许多协议实例在并发执行时以及同任意的协议组合时的安全. UC 安全模型最重要的性质在于:可以单独设计子协议,只要子协议满足 UC 安全,就可以进行组合构造新的 UC 安全协议,并保证协议并发组合情况下的安全性.

定义 1　令 $n \in N$,$\mathcal{F}$ 是理想函数,π 是 n 方协议,称 π 通用可组合安全实现 $\mathcal{F}$,如果对于任何攻击者 $\mathcal{A}$ 都存在一个理想过程攻击者 S,使得对所有外部环境 $\mathcal{Z}$ 对于分布空间 $\mathrm{REAL}_{\pi,\mathcal{A},\mathcal{Z}}$ 和 $\mathrm{IDEAL}_{\pi,\mathcal{A},\mathcal{Z}}$ 是多项式时间计算不可区分的.

定义 2　令 $\mathcal{F}$,G 是理想函数,π 是在 $\mathcal{F}$- 混合模型中的 n 方协议,ρ 是在 G- 混合模型中安全实现理想函数 $\mathcal{F}$ 的 n 方协议. 那么,在 G- 混合模型中的协议 π^{ρ} 能够仿真在 $\mathcal{F}$- 混合模型中的协议 π. 如果 π 安全实现了 $\mathcal{F}$- 混合模型中的某个理想函数 I,那么 π^{ρ} 能够安全实现 G- 混合模型下的理想函数 I.

2　IKEv2 协议安全性分析

IPSec 在实施密码安全保护时,通信双方必须首先协商出双方的安全关联 SA(包括密钥、密码算法、认证算法、密码参数等),该协商过程由 Internet 密钥交换协议完成,IKEv2 是当前 IPSec 认证密钥交换协议的 IETF 标准. 在 IKEv2 协商过程中建立的安全关联叫 IKE_SA,在 IKE_SA 基础上建立的 AH 和 ESP 的安全关联叫 CHILD_SA. IKEv2 协议通信由请求/响应消息对组成,每一对消息称为一次交换. IKEv2 中定义了 3 种类型的交换,分别为初始交换(Initial Exchange)、协商子 SA 交换(CREATE_CHILD_SA Exchange)和信息交换(Informational Exchange). 初始交换由 4 条消息组成,其交换具体步骤为:

(1) $I \rightarrow R$: HDR_i, SA_i^1, KE_i, N_i.

(2) $R \rightarrow I$: HDR_r, SA_r^1, KE_r, N_r, [CERTREQ].

(3) $I \rightarrow R$: HDR_i, $\mathrm{SK}\{\mathrm{ID}_i$, [CERT], [CERTREQ], AUTH_i, $\mathrm{SA}_i^2\}$.

(4) $R \rightarrow I$: HDR_r, $\mathrm{SK}\{\mathrm{ID}_r$, [CERT], AUTH_r, $\mathrm{SA}_r^2\}$.

其中,前两条消息称为 IKE_SA_INIT 交换,其作用为协商密码算法、一次性随机数、DH 交换公开值,并建立 IKE_SA,导出用于加密和验证后续消息所需的密钥材料;后两条消息称为 IKE_AUTH,其作用是

验证 IKE_SA_INIT 以及交换身份标识和证书,并建立第 1 个 CHILD_SA. 通过 IKE_SA_INIT 交换之后,密钥协商双方可以通过计算 PRF($N_i|N_r$, g^{ir})得到种子密钥 SKEYSEED. 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)等. 其中 SK{MSG}表示用相应的密钥对消息 MSG 进行加密和完整性保护.

IKEv2 并没有选择对 Internet 中用户最关心的发起者身份进行主动保护,而是选择了对身份信息不是很敏感的响应者进行主动身份保护. IKEv2 中发起者的身份被暴露攻击过程如下:

$I\rightarrow R$: HDR_i, SA_i^1, KE_i, N_i.

① $I\rightarrow M$: HDR_i, SA_i^1, KE_i, N_i.

② $M\rightarrow I$: HDR_m, SA_m^1, KE_m, N_m, [CERTREQ].

③ $I\rightarrow M$: HDR_i, SK{ID_i, [CERT], [CERTREQ], QUTH_i, SA_i^2}.

④ Dropped.

以上描述的就是发起者 I 的身份被暴露攻击过程,当 I 发送第一条消息向 R 请求建立 SA 时被攻击者 M 截获,此后 M 就可以假冒 R 和 I 进行协议的交互.

协议攻击运行结束后,发起者 I 以为它和响应者 R 进行了一次不成功的协议交互,而实际上 R 根本没有参与此次协议的执行. 由于 SK 为 I 和攻击者 M 所共享,因此 M 可以解开消息 SK{ID_i, [CERT], [CERTREQ], AUTH_i, SA_i^2},进而得到 I 的身份 ID_i.

Meadows[11]指出:IKEv1 中基于签名的认证模式存在认证失败的问题,而 Boyd 等人[4]则证明了在 IKEv2 中存在同样的安全缺陷,IKEv2 中基于签名认证模式中的认证失败攻击过程如下:

(1) $I\rightarrow R$: HDR_i, SA_i^1, KE_i, N_i.

① $M\rightarrow R$: HDR_i, SA_i^1, KE_i, N_i.

② $R\rightarrow M$: HDR_r, SA_r^1, KE_r, N_r, [CERTREQ].

(2) $M\rightarrow I$: HDR_r, SA_r^1, KE_r, N_r, [CERTREQ].

(3) $I\rightarrow M$: HDR_i, SK{ID_i, [CERT], [CERTREQ], AUTH_i, SA_i^2},

① $M\rightarrow R$: HDR_i, SK{ID_i, [CERT], [CERTREQ], AUTH_i, SA_i^2};

② $R\rightarrow M$: HDR_r, SK{ID_r, [CERT], AUTH_r, SA_r^2}.

(4) Dropped.

该协议攻击运行结束后,R 认为自己和 I 进行了一次协议交互,并且和 I 共享了一致会话密钥;而 I 却认为自己和 M 进行了一次不成功会话. R 被 M 完全欺骗了,它会一直等待 I 发出的服务请求,直到它为 I 建立的 IKE_SA 超时. 实际上 I 并不会同 R 进行任何会话,而 R 却在维护 I 的状态信息,分配和 I 通信所需的资源,并等待随后和 I 的通信. 如果 M 展开分布式攻击的话,那么受到攻击的 R 给其他诚实用户提供服务的能力大大降低,甚至不能提供任何服务. 因此,这种认证失败攻击也可称为是一种“拒绝服务攻击”.

3 改进的 Internet 密钥交换协议

为了克服 IKEv2 协议中存在的缺陷,笔者提出一种改进的 Internet 密钥交换协议(WIKE). 该协议能够解决在无线环境中缺乏对发起者身份保护和认证失败的问题. 改进的协议也采用请求/响应消息模式,协议具体的交换消息如下:

(1) $I\rightarrow R$: HDR_i, SA_i^1, KE_i, N_i, [CERTREQ].

(2) $R\rightarrow I$: HDR_r, KE_r, N_r, SK{ID_r, SA_r^1, [CERT], [CERTREQ], AUTH_r}.

(3) $I\rightarrow R$: HDR_i, SK{ID_i, ID_r, [CERT], SA_i^2, AUTH_i}.

(4) $R\rightarrow I$: HDR_r, SK{ID_i, ID_r, SA_r^2}.

在 WIKE 协议中,前两条消息建立 IKE_SA,用于 DH 交换和协商保护第 1 个 CHILD_SA 的安全策略. 在协议中,响应者选择了自己的 DH 公共值和 nonce 之后,并且已知发起者的 DH 公共值和 nonce,则可

以计算出当前的会话密钥;而在第(2)条消息中对 DH 公共值和 nonce 进行了完整性保护,对 R 的身份进行了加密和完整性保护,这样可以防止 ID_r 被攻击者窃听到,从而实现对响应者 R 的被动身份保护.后两条消息是建立第 1 个 CHILD_SA 阶段,在确认了响应者的身份之后,对第 1 阶段交换的消息进行认证,并建立第 1 个 CHILD_SA,并且后两条消息均在 IKE_SA 的保护下进行交互.其中,第(3)条消息确认了响应者的身份之后,I 向 R 发送用于建立 IPSec_SA 的多个提议,并发送自己身份和身份证明;第(4)条消息响应者 R 从 I 的多个提议中选择一个,协商出共同的 CHILD_SA 来保护以后的通信.

在协议交互完成后,通信双方之间建立了用于保护以后通信的 CHILD_SA,而且实现了对发起者的主动身份保护,对响应者的被动身份保护.同时协议通过重新构造认证载荷,使接收者确信该消息就是给自己的,这样攻击者就无机可乘,从而防止了认证失败问题.因此,新的协议具有以下安全属性:

(1) 对发起者的主动身份保护:在无线接入网络环境下,发起者身份等信息是非常敏感的.在协议中让响应者先显式的证明自己的真实身份,发起者在确认了对方的身份之后再证明自己的身份,从而实现了对发起者的主动身份保护.

(2) 防止认证失败:认证失败是拒绝服务攻击在 IKE 中的一种表现形式,如果攻击者采用分布式攻击手段将产生严重的后果.造成这种安全缺陷的原因是发送的消息中没有用有效的方式说明期望的接受者,因此新的协议通过重新构造认证载荷,使接受者确信该消息就是发送给自己的,这样就能有效防止认证失败问题.

同时,WIKE 协议是可证明安全的,能够达到通用可组合安全(UC 安全).下面对协议的安全性进行证明.

4　协议安全性证明

利用 UC 模型对协议 WIKE 进行安全性证明,经该模型证明安全的协议能保证在实际网络环境中协议组合与并发执行的安全性.证明的基本思路是首先略去协议中不影响安全性的消息,提取出抽象协议 π 及其在理想函数 $\mathcal{F}_{SIG}$[12] 辅助下的混合协议 π_{PKE},证明在 $\mathcal{F}_{SIG}$ 辅助下的混合协议 π_{PKE} 能够安全实现理想函数 $\mathcal{F}_{PKE}$.

4.1　简化后的混合协议 π_{PKE}

忽略协议中不影响安全性的消息和元素,结合理想签名函数 $\mathcal{F}_{SIG}$,可以给出在 $\mathcal{F}_{SIG}$ 辅助下对 WIKE 协议简化抽象后的混合协议 π_{PKE}.令 p 和 q 为大素数,且 $q/p-1$,g 是群 Z_p^* 上的阶为 q 的生成元.协议参与者交互运行混合协议 π_{PKE},执行如下操作:

(1) 一旦收到输入消息(Establish-key, s, I, "init"),该参与方作为发起者随机选取一个 $x \xleftarrow{R} Z_q$,发送协议启动消息(s, g^x),保存会话状态(s, I).I 用"0"·s 激活 $\mathcal{F}_{SIG}$ 的拷贝,发送消息(singer,"0"·s) 给 $\mathcal{F}_{SIG}$;

(2) 当参与方被消息(Establish-key, s, R, "resp")激活时,它作为响应者通过发送消息 (singer,"1"·s) 给 $\mathcal{F}_{SIG}$ 来激活 $\mathcal{F}_{SIG}$ 的拷贝.当收到(s, g^x) 时,R 产生响应消息(s, g^y, R, σ_r, MAC_{k1}("1", s, R)),其中 $y \xleftarrow{R} Z_q$,σ_r 是通过发送(sign,"1"·s, g^x, g^y) 给 $\mathcal{F}_{SIG}$ 签名计算得到,然后记录返回值和 $PRF_{g^{xy}}$(1) 作为 k_1 的值.计算 $PRF_{g^{xy}}$(0) 作为 k_0 的值并保存在内存中,并擦除 y 和 g^{xy};

(3) 一旦收到应答消息 (s, g^y, R, σ_r, t_r),I 首先发送消息(verify,"1"·s, R, (g^x, g^y), σ_r) 给 $\mathcal{F}_{SIG}$ 验证签名 σ_r,同时验证 t_r 是否等于 MAC_{k1}("1"·s, R),此处 k_1 取值为 $PRF_{g^{xy}}$(1),$g^{xy}=(g^y)^x$.若其中一步验证失败,则终止会话并擦除会话状态;如果验证都成功则 I 发送结束消息(s, I, s_i, MAC_{k1}("0", s, I))(其中签名 σ_i 通过发送消息(sign,"0"·s, g^y, g^x) 给 $\mathcal{F}_{SIG}$ 计算得到),并记录获得的值,从而完成会话,输出消息(output, s, R, k_0)(其中 k_0 的取值为 $PRF_{g^{xy}}$(0)),并擦除会话状态;

(4) 一旦收到结束消息 (s, I, σ_i, t_i),通过发送消息(verify,"0"·s, I, (g^y, g^x), σ_i) 给 $\mathcal{F}_{SIG}$ 验证签名,此处 g^y 是在应答消息中接收到的来自 R 的 DH 值,并验证 t_i 是否等于 MAC_{k1}("0", s, I).若其中一步验证失败,则终止会话,否则 R 完成会话,本地输出(output, s, I, k_0)(其中 k_0 的取值为 $PRF_{g^{xy}}$(0)),并擦除会话状态.

4.2 协议安全证明

定理 1 对于任意攻击者而言,在 $\mathcal{F}_{SIG}$ 辅助下的混合协议 π_{PKE} 安全实现了理想函数 $\mathcal{F}_{PKE}$.

证明 令 $\mathcal{A}$ 是与混合协议 π_{PKE} 进行交互的攻击者,构造一个理想过程攻击者 S,使得对于任何环境机 $\mathcal{Z}$ 不能区分是与攻击者 $\mathcal{A}$ 和协议 π_{PKE} 进行交互,还是与攻击者 S 进行交互.

(1) 攻击者 S 的构造 S 模拟的攻击者 $\mathcal{A}$,在其内部对环境机 $\mathcal{Z}$、攻击者 $\mathcal{A}$ 及协议参与者进行仿真,其执行操作如下:

① S 将来自 $\mathcal{Z}$ 的任何输入都转发给 $\mathcal{A}$; $\mathcal{A}$ 的任何输出都拷贝给 S 的输出.

② 一旦接收到 $\mathcal{F}_{PKE}$ 发来的消息$(s,I,\text{“init”})$,S 把消息(s,g^x) 和$(\text{signer},\text{“1”}\cdot s,I)$ 交给 $\mathcal{A}$.

③ 当接收到 $\mathcal{F}_{PKE}$ 发来的消息$(s,R,\text{“resp”})$,S 把消息$(\text{singer},\text{“1”}\cdot s,R)$ 交给 $\mathcal{A}$.

④ 当 $\mathcal{A}$ 传递启动消息(s,α) 给 R 时,S 首先验证它是否收到消息$(s,R,\text{“resp”})$,然后随机选取 y,把消息(s,g^y,R,σ_r,t_r) 交给 $\mathcal{A}$,其中 t_r 的值为 $\text{MAC}_{k1}(\text{“1”},s,R)$,$k_1$ 的值为 $\text{PRF}_{\alpha^y}(1)$,σ_r 是签名值,$\mathcal{A}$ 返回 σ_r.

⑤ 当 $\mathcal{A}$ 传递消息(s,β,P,σ_r,t_r) 给一个未被攻陷的 I 时,S 首先验证 I 之前是否发送了消息(s,g^x),然后模拟签名 σ_r 的验证过程,即仿真当接收到消息$(\text{verify},\text{“1”}\cdot s,I,P,(g^x,\beta),\sigma_r)$ 时的 $\mathcal{F}_{SIG}$ 行为,再验证 t_r 是否等于 $\text{MAC}_{k1}(\text{“1”},s,P)$,其中 k_1 的值为 $\text{PRF}_{\beta^x}(1)$,如果验证都成立,S 就将结束消息$(s,I,\sigma_i,\text{MAC}_{k1}(\text{“0”},s,I))$ 发给 $\mathcal{A}$,其中 σ_i 是在 $\mathcal{F}_{SIG}$ 名义下交给消息$(sign,\text{“0”}\cdot s,\beta,g^x)$ 后 $\mathcal{A}$ 的应答.

⑥ 当 $\mathcal{A}$ 发送结束消息(s,P,σ_i,t_i) 给 R 时,S 首先验证 R 之前是否收到消息(s,α),并已发送应答消息(s,g^y,R,σ_r,t_r),然后仿真签名 σ_r 的验证过程,再验证 t_i 是否等于 $\text{MAC}_{k1}(\text{“0”},s,P)$,其中 k_1 的值为 $\text{PRF}_{\alpha^y}(1)$,如果验证都成立,则在理想过程中,S 发送消息$(\text{output},s,I,(P,k'))$ 给 $\mathcal{F}_{PKE}$,其中 k' 的值为 $\text{PRF}_{\alpha^y}(0)$. 当 $\mathcal{F}_{PKE}$ 发送输出消息给 R,S 就转发该消息.

⑦ 如果 $\mathcal{A}$ 攻陷了 I 或 R,则 S 在理想过程中攻陷相同的参与方,并且把该参与方的内部数据交给 $\mathcal{A}$.

⑧ S 仿真 $\mathcal{A}$ 对 $\mathcal{F}_{SIG}$ 操作,即当 $\mathcal{A}$ 发送消息给 $\mathcal{F}_{SIG}$ 时,S 发送相应的消息给 $\mathcal{F}_{SIG}$; S 同样仿真 $\mathcal{A}$ 和 $\mathcal{F}_{SIG}$ 之间的通信过程.

(2) 真实协议 π_{PKE} 与理想函数 $\mathcal{F}_{PKE}$ 是不可区分的 设 CP 代表参与方在产生输出前被攻陷事件. 证明无论 CP 是否发生,$\mathcal{F}_{PKE}$ 和协议 π_{PKE} 是不可区分的.

① 当 CP 事件发生时,$\mathcal{F}_{PKE}$ 和 π_{PKE} 是不可区分的 当 CP 事件发生时,对于仿真的 $\mathcal{A}$ 而言,S 完美仿真了协议 π_{PKE} 的操作,因此 $\mathcal{F}_{PKE}$ 和 π_{PKE} 是不可区分的.

② 当 CP 事件不发生时,$\mathcal{F}_{PKE}$ 和 π_{PKE} 是不可区分的 当 CP 事件不发生时,构造过度协议 $\mathcal{H}_1$ 和 $\mathcal{H}_2$,依次证明 $\pi_{PKE}\approx\mathcal{H}_1\approx\mathcal{H}_2\approx\mathcal{F}_{PKE}$,其中“$\approx$”代表不可区分性. 过度协议构造如下: $\mathcal{H}_1$ 与 π_{PKE} 的惟一区别在于,当 π_{PKE} 指示 I(或者 R) 用密钥 β^x(或者 α^y) 计算伪随机函数 PRF 时,$\mathcal{H}_1$ 中用一个独立选取的随机数 $r\xleftarrow{R}Z_q$ 计算 PRF,即在 $\mathcal{H}_1$ 中 MAC 的密钥是 k_1,其值为 $\text{PRF}_r(1)$,输出密钥是 k,其值为 $\text{PRF}_r(0)$. $\mathcal{H}_2$ 与 $\mathcal{H}_1$ 惟一的区别是参与方选取的 k_1 和 k 是独立的.

(a) 如果判定性 Diffie-Hellman 假设成立,则有 $\pi_{PKE}\approx\mathcal{H}_1$.

假设存在环境机 $\mathcal{Z}$ 和攻击者 $\mathcal{A}$,使得 $\mathcal{Z}$ 能以不可忽略的概率区分 π_{PKE} 与 $\mathcal{H}_1$. 构造一个算法 D,使得 D 可以攻破 DDH 假设. D 在仿真的交互过程中运行 $\mathcal{Z}$ 的拷贝,使得它与攻击者 $\mathcal{A}$ 和参与者进行交互. 当 I 发送启动消息时,D 把 g^x 换成 g^a; 当 R 发送应答消息时,D 把 g^y 换成 g^b; 当 R(或者 I) 指示运行 $\text{PRF}_{\beta^x}()$(或者 $\text{PRF}_{\alpha^y}()$) 时,D 将其替换成 $\text{PRF}_{g^z}()$; 如果 $\mathcal{Z}$ 在 I 产生输出之前将其攻陷,则算法终止并输出一个随机值; 否则 D 输出 $\mathcal{Z}$ 的输出内容. 在其他情况下 D 扮演环境机 $\mathcal{Z}$ 的角色. 考虑 $z\xleftarrow{R}Z_q$ 并且独立于 a,b,则被仿真的 $\mathcal{Z}$ 的输出与 $\mathcal{H}_1$ 中 $\mathcal{Z}$ 的输出是一样的,这是由于在两个交互过程中,g^x,g^y 及伪随机函数 PRF 的值都是独立随机选取的,而且 $\mathcal{Z}$ 不能得到指数 x 或 y; 考虑 $z=ab$ 的情况,则被仿真的 $\mathcal{Z}$ 的输出与协议 π_{PKE} 的输出是一样的. 综合两种情况,算法 D 能够以不可忽略的概率攻破 DDH 假设,故假设不成立.

(b) 如果 PRF 是安全的伪随机函数族,则有 $\mathcal{H}_1\approx\mathcal{H}_2$.

假设存在环境机 $\mathcal{Z}$ 和攻击者 $\mathcal{A}$,使得 $\mathcal{Z}$ 能以不可忽略的概率区分 $\mathcal{H}_1$ 与 $\mathcal{H}_2$. 利用 $\mathcal{Z}$ 构造一个算法 D,使得 D 可以攻破伪随机函数 PRF 的安全性,即 D 能够访问一个 oracle f,并以不可忽略的概率区分 f 是随机函数

还是伪随机函数 $PRF_r()$. D 在仿真的交互过程中运行 $\mathcal{Z}$ 的拷贝,使得它与 π_{PKE} 中的攻击者 $\mathcal{A}$ 和参与者进行交互. 当参与方被指示计算 k_1 时, D 令 $k_1 = f(1)$; 当参与方被指示产生会话密钥 k 时, D 令密钥 $k = f(0)$; 如果 $\mathcal{Z}$ 在发起者产生输出前攻陷了一个参与方,则算法终止并输出一个随机值; 否则, D 输出 $\mathcal{Z}$ 的输出. 其他情况下 D 扮演环境机 $\mathcal{Z}$ 的角色. 如果 f 是一个随机函数,那么被仿真的 $\mathcal{Z}$ 的输出与 $\mathcal{H}_2$ 中 $\mathcal{Z}$ 的输出是一样的; 如果 f 为 $PRF_r()$,并且 D 没有终止,那么被仿真的 $\mathcal{Z}$ 的输出与 $\mathcal{H}_1$ 中 $\mathcal{Z}$ 的输出相同. 因此,如果 $\mathcal{Z}$ 能够以不可忽略的概率区分 $\mathcal{H}_1$ 与 $\mathcal{H}_2$, D 就能以不可忽略的概率区分伪随机函数和随机函数.

(c) 假设 MAC 是安全消息认证码函数族,则有 $\mathcal{H}_2 \approx \pi_{PKE}$.

假设存在环境机 $\mathcal{Z}$ 和攻击者 $\mathcal{A}$,使得 $\mathcal{Z}$ 能以不可忽略的概率区分 $\mathcal{H}_2$ 与 $\mathcal{F}_{PKE}$. 利用 $\mathcal{Z}$ 构造一个算法 D,使得 D 可以攻破消息认证函数 MAC 抵抗选择消息攻击的安全性,即 D 能访问一个 Oracle $MAC_r()$, 它能以不可忽略的概率产生一个消息 m^* 和一个标记 t^*,使得 t^* 等于 $MAC_r(m^*)$. D 在仿真的交互过程中运行 $\mathcal{Z}$ 的拷贝,使得它与 π_{PKE} 中的攻击者 $\mathcal{A}$ 和参与者进行交互. D 扮演攻击者 $\mathcal{A}$ 和参与方的环境机 $\mathcal{Z}$ 角色. 当参与方被指示对消息 m 计算 $MAC_{k1}(m)$ 时, D 用查询 m 的 Oracle 值进行应答. 如果在发起者的输出中 $P \neq R$,那么 D 输出 m^* 为("1", s, P) 和 t^*; 如果在响应者的输出中 $P \neq I$,那么 D 输出 m^* 为("0", s, P) 和 t^*. 如果在发起者产生输出之前 $\mathcal{Z}$ 攻陷了参与方,那么算法终止并不输出任何消息. 对 D 分析,被仿真的 $\mathcal{Z}$ 的输出与 $\mathcal{H}_2$ 中 $\mathcal{Z}$ 的输出是一样的. D 能以不可忽略的概率成功的伪造一个 MAC 值. 因此,如果 $\mathcal{Z}$ 能以不可忽略的概率区分 $\mathcal{F}_{PKE}$ 与 $\mathcal{H}_2$,那么 D 就能以不可区分的概率伪造 MAC 值,与 MAC 函数的安全性矛盾.

由此得出结论: $\pi_{PKE} \approx \mathcal{H}_1 \approx \mathcal{H}_2 \approx \mathcal{F}_{PKE}$, 证毕.

5　协议性能分析

改进的 WIKE 协议主要针对的是无线网络应用场景,协议发起端的执行效率显得更加重要,因此以客户端的运算量为切入点,对协议性能与相关协议进行对比分析. 表 1 给出了各协议建立一个 CHILD_SA 所需要的运算量和通信量.

表 1　协议运算量和通信量比较

协议	协议中消息条数	模幂运算次数	对称加密次数	签名次数
IKEv1[1]	9	2	5	2
IKEv2[2]	4	2	2	2
IKEv2-EAP[6]	6	2	2	2
WIKE	4	2	3	2

从表 1 中可以看出,4 种协议的模幂运算次数和签名运算次数是一样的. 由于对称加密运算相对于公钥运算是可忽略的,所以协议的性能主要体现在协议中消息条数上. 改进的 WIKE 协议和 IKEv2 协议具有相同的消息条数,但相比 IKEv1 协议要少 4 条消息,所以提出的协议在总体性能上和 IKEv2 相当,和 IKEv1 相比有较明显的优势.

为了能够更直观地反映协议的性能,通过 NS-2 仿真工具对协议性能进行了仿真. 仿真的环境是: 模拟一个具有2 000个节点的无线 IP 网络,其中任意节点之间都是可到达的,并可以自动路由,同时相邻节点之间的链路的延迟是根据当时的网络环境随机产生的. 为了真实反映网络中的通信情况,在网络中随机生成一些数据流来模拟链路上的延迟、阻塞和丢包率等. 然后对每种协议随机选择 50 对节点,在每对节点上运行要仿真的协议,记录每种协议 50 次仿真的结果,其最终的性能比较如图 1 所示.

图 1 中给出了 4 种协议分别在每对节点上执行一次所需要的时间,共进行了 50 次仿真,然后对 50 次仿真的结果取平均值,如图水平线所示. 从图中可以看出仿真结果和理论分析是一致的.

6　结 束 语

新一代 Internet 密钥交换协议 IKEv2 相对于其第一个版本 IKEv1 在安全性和性能上都有了较大的改

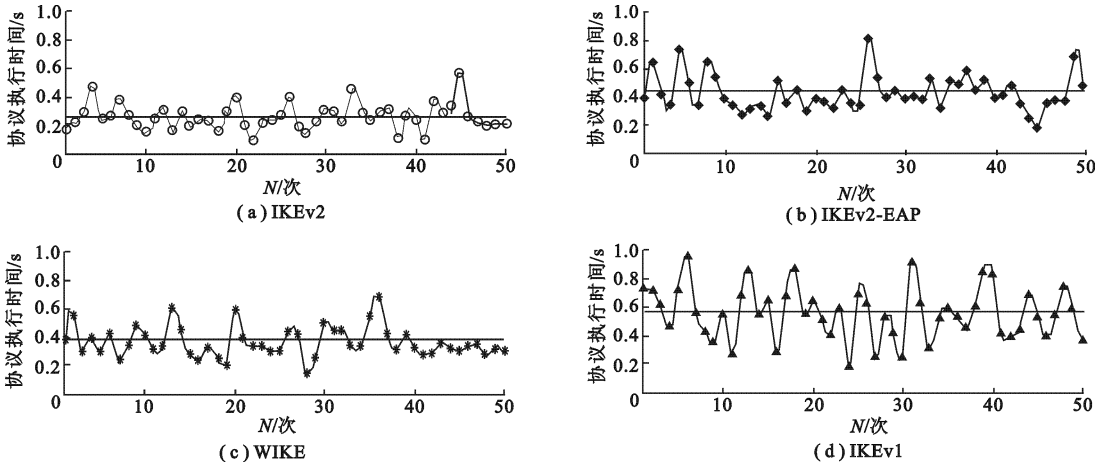

图 1 协议运行时间比较

进,但在其初始交换中同样存在 IKEv1 中在认证失败和身份保护方面的脆弱性问题. 而在用户通过无线接入 Internet 的环境下,用户身份等敏感信息的保密性显得较为重要,IKE 协议应当对发起者提供主动的身份保护. 改进的 Internet 密钥交换协议 WIKE,能够解决 IKEv2 中存在的上述两个安全缺陷,因此能够适用于无线 Internet 环境. 在通用可组合安全模型下对改进的协议进行了安全性证明,分析表明改进的协议能够达到 UC 安全. 通过对比分析和仿真实验,改进的协议在性能上和 IKEv2 相比仅增加了一次对称加密运算,而相对于 IKEv1 和 IKEv2-EAP 具有较明显的优势.

参考文献:

[1] Harkins D, Carrel D. Internet Key Exchange[EB/OL]. [1998-11-11]. http://tools.ietf.org/rfc/rfc2409.txt.

[2] Kaufman C. Internet Key Exchange (IKEv2) Protocol[EB/OL]. [2005-12-25]. http://tools.ietf.org/rfc/rfc4306.txt.

[3] Krawczyk H. SIGMA: the 'SIGn-and-Mac' Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols [C]//Advances in Cryptology-CRYPTO'2003 LNCS 2729. Berlin: Springer-Verlag, 2003: 400-425.

[4] Boyd C, Mao W, Paterson K. Deniable Authentication for Internet Protocols[C]//Proceedings of IWSP'03 LNCS 3364. Berlin: Springer-Verlag, 2003: 137-150.

[5] Tschofenig H, Kroeselberg D, Pashalidis A, et al. EAP IKEv2 Method[EB/OL]. [2007-09-27]. http://tools.ietf.org/id/draft-tschofenig-eap-ikev2-15.txt.

[6] Bellare M, Rogaway P. Entity Authentication and Key Distribution[C]//Advances in Cryptology-Crypto'93 LNCS 773. Berlin: Springer-Verlag, 1994: 232-249.

[7] Canetti R, Krawczyk H. Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels[C]// Advances in Cryptology-Eurocrypt'01 LNCS 2045. Berlin: Springer-Verlag, 2001: 453-474.

[8] Canetti R. Universally Composable Security: a New Paradigm for Cryptographic Protocols[EB/OL]. [2005-12-14]. http://eprint.iacr.org/2000/067.ps.

[9] Canetti R, Dodis Y, Pass R, et al. Universally Composable Security with Pre-Existing Setup[C]//Proceedings of the 4th Theory of Cryptology Conference (TCC) LNCS 4392. Berlin: Springer-Verlag, 2007: 61-85.

[10] 杨超, 曹春杰, 马建峰. 通用可组合安全的 Mesh 网络认证协议[J]. 西安电子科技大学学报, 2007, 34 (5): 814-817.
Yang Chao, Cao Chunjie, Ma Jianfeng. Universally Composable Secure Authentication Protocol for Wireless Mesh Networks[J]. Journal of Xidian University, 2007, 34(5):814-817.

[11] Meadows C. Analysis of the Internet Key Exchange Protocol Using the URL Protocol Analyzer[C]//Proceedings of IEEE Symposium on Security and Privacy'99. Los Alamitos: IEEE, 1999: 216-231.

[12] Canetti R, Krawczyk H. Universally Composable Notions of Key Exchange and Secure Channels[C]//Advances in Cryptology-Eurocrypt'02 LNCS 2332. Berlin: Springer-Verlag, 2002: 337-351.

(编辑: 齐淑娟)