

可信计算环境下的 IKEv2 协议扩展方案

肖跃雷^{1,2,3}, 武君胜¹, 朱志祥^{2,3}

(1 西北工业大学 计算机学院, 陕西 西安 710072; 2 陕西省信息化工程研究院, 陕西 西安 710075;
3 西安邮电大学 物联网与两化融合研究院, 陕西 西安 710061)

摘 要: 在 IKEv2 协议基础上, 利用 ISO/IEC 9798—3:1998/Amd 1:2010 中的认证机制, 提出了一种可信计算环境下的 IKEv2 协议扩展方案, 实现了发起者和响应者之间的双向身份认证和平台认证, 并建立了它们之间的会话密钥, 且与 IKEv2 协议是向后兼容的, 其中可信第三方(TTP)负责它们的身份证书验证、平台证明身份密钥(AIK)证书验证和平台完整性评估, 它们的存储完整性度量日志(SML)被加密传输给可信第三方, 从而有效地解决了现有可信计算环境下 IKE 协议扩展方案所存在的问题。此外, 利用针对可信网络连接协议的串空间模型证明了该 IKEv2 协议扩展方案是安全的。

关键词: 可信计算; 平台认证; 串空间模型; IKEv2

中图分类号: TP309

文献标识码: A

文章编号: 1000—7180(2018)12—0001—07

Extended Internet Key Exchange Protocol Version 2 in Trusted Computing Environment

XIAO Yue-lei^{1,2,3}, WU Jun-sheng¹, ZHU Zhi-xiang^{2,3}

(1 College of Computer Science and Engineering, Northwestern Polytechnical University, Xi'an 710072, China;
2 Shaanxi Provincial Information Engineering Research Institute, Xi'an 710075, China; 3 Institute of
IOT and IT-based industrialization, Xi'an University of Posts & Telecommunications, Xi'an 710061, China)

Abstract: On the basis of the IKEv2, an extended IKEv2 in trusted computing environment based on ISO/IEC 9798—3:1998/Amd 1:2010 is proposed in this paper. It realizes mutual identity authentication and Platform-Authentication between an initiator and a responder, and establishes session keys between them, and is backward compatible with the IKEv2, where a trusted third party (TTP) is responsible for validating the identity and Attestation Identity Key (AIK) certificates of them, and evaluating the platform integrity of them, and the stored integrity measurement logs (SML) of them are encrypted and sent to the TTP. Thus, it is able to solve the problems of the existing extended IKE protocol for trusted computing environment effectively. Moreover, the extended IKEv2 is proved secure based on the strand space model for trusted network connect protocols.

Key words: trusted computing; platform-authentication; strand space model; IKEv2

1 引言

IKE(Internet Key Exchange)协议是 IPSec 的重要组成部分, 在 IP 层执行双向身份认证并建立安全关联(Security Associations, SAs)^[1-2]。目前, IKE

协议已发布了两个版本: IKEv1^[3-5] 和 IKEv2^[2,6-8]。IKE 协议由一系列请求/响应消息对构成, 其中一个请求/响应消息对称为一个消息交换。IKE 协议的头两个消息交换用于建立 IKE 安全关联, 其中第一个消息交换称为 IKE_SA_INIT 交换, 第二个消

息交换称为 IKE_AUTH 交换,两者统称为 IKE 初始交换. IKE 协议后面的消息交换为 CREATE_CHILD_SA 交换或 INFORMATIONAL 交换.

近年来,随着可信计算技术的产生和发展,对 IKEv2 协议又提出了新的安全需求,即文献[9]中所提出来的平台认证,使得 IKEv2 协议不能适用于可信计算环境. 平台认证是由平台身份认证和平台完整性评估两个部分构成的. 为了支持平台认证,已有一些研究者提出将平台认证嵌入在 IKE 协议中,并给出了相应方案^[10-12]. 但是,这些方案仍然存在以下问题:(1)IKE 端点的平台配置隐私泄漏给了其他 IKE 端点;(2)IKE 端点需要具备验证其他 IKE 端点平台完整性的能力,这对 IKE 端点来说是困难的,因为平台完整性验证是较复杂的工作^[9];(3)IKE 端点的身份证书(包括平台身份证书)有效性没有得到验证.

为了解决上述问题,本文利用 ISO/IEC 9798-3:1998/Amd 1:2010 中的认证机制^[13],对 IKEv2 协议进行扩展,提出了一种可信计算环境下的 IKEv2 协议扩展方案. 该扩展方案嵌入了双向平台认证,使得扩展后的 IKEv2 协议能够实现 IP 层的可信网络连接,从而增强了 IPSec 的安全性. 最后,为了分析该扩展方案的安全性,本文基于文献[14]中所提出的针对可信网络接入协议的串空间模型(Strand Space Model,SSM)对该扩展方案进行了安全性分析,结果表明该扩展方案是安全的.

2 可信计算环境下的 IKEv2 协议扩展方案

在本文提出的可信计算环境下的 IKEv2 协议扩展方案中,CREATE_CHILD_SA 交换和 INFORMATIONAL 交换与 IKEv2 协议相同,而 IKE 初始交换由本文扩展后的 IKE 初始交换代替,其中 IKE 初始交换包括两种情形:基于预共享密钥模式和基于证书模式.

2.1 基于预共享密钥模式

针对 IKEv2 协议中 IKE 初始交换的基于预共享密钥模式,本文扩展后的 IKE 初始交换的具体步骤如下:

- (1) $I \rightarrow R: \text{HDR} \parallel \text{SA}_{I,1} \parallel \text{KE}_I \parallel N_I$;
- (2) $R \rightarrow I: \text{HDR} \parallel \text{SA}_{R,1} \parallel \text{KE}_R \parallel N_R \parallel \underline{\text{TTP}_R}$;
- (3) $I \rightarrow R: \text{HDR} \parallel \{ID_I \parallel ID_R \parallel \underline{\text{TTP}_I} \parallel \underline{\text{QUOTE}_I} \parallel \underline{\text{SML}_I} \parallel \underline{\text{AUTH}_I} \parallel \text{SA}_{I,2} \parallel \text{TS}_I \parallel \text{TS}_R\}_{SK_I}$;
- (4) $R \rightarrow T: \underline{N_R^0 \parallel \text{Cert}(\text{AIK}_{pk,a}) \parallel \text{PCR}_a \parallel \{SML_a\}_{K_I} \parallel \{K_I\}_{pk_T} \parallel N_I^0 \parallel \text{Cert}(\text{AIK}_{pk,\beta})}$

$$\parallel \text{PCR}_\beta \parallel \{SML_\beta\}_{K_R} \parallel \{K_R\}_{pk_T};$$

$$(5) T \rightarrow R: \underline{\text{Res}_T} \parallel \sigma_T;$$

$$(6) R \rightarrow I: \text{HDR} \parallel \{ID_R \parallel \underline{\text{QUOTE}_R} \parallel \underline{\text{RESULT}_R} \parallel \underline{\text{AUTH}_R} \parallel \text{SA}_{R,2} \parallel \text{TS}_I \parallel \text{TS}_R\}_{SK_R}.$$

在上述步骤中,新增加的消息和字段是用单下划线标记的,而新扩展的字段是用双下划线标记的. I 为 IKE 协议发起者, R 为 IKE 协议响应者, T 为 IKE 协议可信第三方(Trusted Third Party,TTP), α 为 I 的平台, β 为 R 的平台. N_I^0 是 I 生成的随机数,而 N_R^0 是 R 生成的随机数. PCR_a 是 α 的平台配置寄存器(PCR, platform configuration register)值^[9],而 PCR_β 是 β 的 PCR 值. SML_a 是 α 的存储度量日志(SML, stored measurement log)值^[9],而 SML_β 是 β 的 SML 值. $\text{Cert}(\text{AIK}_{pk,a})$ 是 α 的平台身份证明密钥(AIK, attestation identity key)证书^[9],而 $\text{Cert}(\text{AIK}_{pk,\beta})$ 是 β 的 AIK 证书. $\text{AIK}_{pk,a}$ 和 $\text{AIK}_{pk,\beta}$ 分别为 α 和 β 的 AIK 公钥, K_I 和 K_R 分别为 I 和 R 产生的临时保护密钥, pk_T 和 sk_T 分别为 T 的公私钥对, $\text{Res}_T = N_R^0 \parallel \text{Cert}(\text{AIK}_{pk,a}) \parallel \text{PCR}_a \parallel \text{Re}_{\text{AIK},\alpha} \parallel \text{Re}_{\text{INT},\alpha} \parallel N_I^0 \parallel \text{Cert}(\text{AIK}_{pk,\beta}) \parallel \text{PCR}_\beta \parallel \text{Re}_{\text{AIK},\beta} \parallel \text{Re}_{\text{INT},\beta}$, $\text{Re}_{\text{AIK},\alpha}$ 和 $\text{Re}_{\text{AIK},\beta}$ 分别为 $\text{Cert}(\text{AIK}_{pk,a})$ 和 $\text{Cert}(\text{AIK}_{pk,\beta})$ 的 AIK 证书验证结果, SML_a 和 SML_β 的正确性分别为 PCR_a 和 PCR_β 所验证, $\text{Re}_{\text{INT},\alpha}$ 和 $\text{Re}_{\text{INT},\beta}$ 分别为 SML_a 和 SML_β 的平台完整性评估结果, σ_T 为 T 的签名且 $\sigma_T = \{\text{Res}_T\}_{sk_T}$.

此外, HDR 为 IKE 头, 包含安全参数索引(Security Parameter Indexes, SPIs)、版本号和一些标识信息. ID_I 和 ID_R 分别为 I 和 R 的身份标识负载, 分别包含 I 和 R 的身份标识. N_I 和 N_R 分别为 I 和 R 的随机数负载, 分别包含 N_I^0 和 N_R^0 . $\text{SA}_{I,1}$ 和 $\text{SA}_{R,1}$ 分别为 I 和 R 的 IKE_SA 安全关联负载, 前者包含 I 支持的密码套件, 后者包含 R 选择的密码套件. $\text{SA}_{I,2}$ 和 $\text{SA}_{R,2}$ 分别为 I 和 R 的 CHILD_SA 安全关联负载, 前者包含 I 支持的密码套件, 后者包含 R 选择的密码套件. KE_I 和 KE_R 分别为 I 和 R 的密钥交换负载, 分别包含 g^x 和 g^y , 它们是 Diffie-Hellman 交换的临时公钥. TS_I 和 TS_R 分别为 I 和 R 的通信流量选择负载, 前者包含 I 的一些源地址和目标地址, 后者包含 R 的一些源地址和目标地址. SK_{AI} 和 SK_{AR} 分别为 I 和 R 的完整性保护密钥, SK_{EI} 和 SK_{ER} 分别为 I 和 R 的加密密钥. SK_I 和 SK_R 分别为 I 和 R 的保护密钥, 前者包含 SK_{AI} 和 SK_{EI} , 后者包含 SK_{AR} 和 SK_{ER} . TTP_I 和 TTP_R 分别为 I 和 R 的 TTP 负载, 前者包含 I 选择的 TTP, 后者包含 R 支持的 TTP.

QUOTE_I 和 QUOTE_R 分别为 I 和 R 的 Quote 负载,前者包含 Cert(AIK _{pk_{α}}), PCR _{α} 和 σ_{α} , 后者包含 Cert(AIK _{pk_{β}}), PCR _{β} 和 σ_{β} , 其中 σ_{α} 为 α 的 AIK 签名且 $\sigma_{\alpha} = [\text{prf}(\text{SK}_I, N_R^0) \parallel \text{PCR}_{\alpha}]_{\text{AIK}_{sk_{\alpha}}}$, σ_{β} 为 β 的 AIK 签名且 $\sigma_{\beta} = [\text{prf}(\text{SK}_R, N_I^0), \text{PCR}_{\beta}]_{\text{AIK}_{sk_{\beta}}}$, prf() 为伪随机函数, AIK _{sk_{α}} 和 AIK _{sk_{β}} 分别为 α 和 β 的 AIK 私钥. SKEYSEED 为 I 和 R 的会话密钥种子且 SKEYSEED = prf($g^{xy}, N_I^0 \parallel N_R^0$), SK_D $\parallel$ SK_{AI}

$\parallel \text{SK}_{EI} \parallel \text{SK}_{ER} \parallel \text{SK}_{PI} \parallel \text{SK}_{PR} = \text{prf}^+(\text{SKEYSEED}, N_I^0 \parallel N_R^0 \parallel \text{SPI}_I \parallel \text{SPI}_R)$, 其中 SK_D 为用于 CHILD_SA 安全关联的导出密钥, SK_{PI} 和 SK_{PR} 分别为 I 和 R 用于生成 AUTH_I 和 AUTH_R 的密钥, SPI_I 和 SPI_R 分别为 I 和 R 的安全参数索引, prf⁺() 为基于 prf() 的伪随机输出函数. AUTH_I 和 AUTH_R 分别为 I 和 R 的认证负载, 前者用于认证 I 的身份和保护 IKE_SA_INIT 交换, 后者用于认证 R 的身份和保护 IKE_AUTH 交换, 其中 AUTH_I = prf(prf(K_{pre-shared}, 密钥填充).

HDR $\parallel$ SA _{$I,1$} $\parallel$ KE _{I} $\parallel$ N _{I} $\parallel$ N _{R} ⁰ $\parallel$ prf(SK_{PI}, ID _{I} ^{*})), AUTH_R = prf(prf(K_{pre-shared}, 密钥填充), HDR $\parallel$ SA _{$R,1$} $\parallel$ KE _{R} $\parallel$ N _{R} $\parallel$ TTP _{R} $\parallel$ N _{I} ⁰ $\parallel$ prf(SK_{PR}, ID _{R} ^{*})), ID _{I} ^{*} 和 ID _{R} ^{*} 分别为 ID _{I} 和 ID _{R} 除负载头外的其余部分, K_{pre-shared} 为 I 和 R 之间的预共享密钥. RESULT_R 为 R 的 Result 负载, 包含 Res_T 和 σ_T . SML _{I} 为 I 的 SML 负载, 包含 {SML _{α} }_{K _{I}} 和 {K _{I} }_{pk _{T}} .

2.2 基于证书模式

针对 IKEv2 协议中 IKE 初始交换的基于证书模式, 本文扩展后的 IKE 初始交换的具体步骤如下:

- (1) $I \rightarrow R$: HDR $\parallel$ SA _{$I,1$} $\parallel$ KE _{I} $\parallel$ N _{I} ;
- (2) $R \rightarrow I$: HDR $\parallel$ SA _{$R,1$} $\parallel$ KE _{R} $\parallel$ N _{R} $\parallel$ CERTREQ_R $\parallel$ TTP_R;
- (3) $I \rightarrow R$: HDR $\parallel$ {ID _{I} $\parallel$ CERT _{I} $\parallel$ CERTREQ_I $\parallel$ ID _{R} $\parallel$ TTP_I $\parallel$ QUOTE_I $\parallel$ SML _{I} $\parallel$ AUTH_I $\parallel$ SA _{$I,2$} $\parallel$ TS _{I} $\parallel$ TS _{R} }_{SK _{I}} ;
- (4) $R \rightarrow T$: N _{R} ⁰ $\parallel$ Cert _{i} $\parallel$ Cert(AIK _{pk_{α}}) $\parallel$ PCR _{α} $\parallel$ {SML _{α} }_{K _{I}} $\parallel$ {K _{I} }_{pk _{T}} $\parallel$ N _{I} ⁰ $\parallel$ Cert _{r} $\parallel$ Cert(AIK _{pk_{β}}) $\parallel$ PCR _{β} $\parallel$ {SML _{β} }_{K _{R}} $\parallel$ {K _{R} }_{pk _{T}} ;
- (5) $T \rightarrow R$: Res_T $\parallel$ σ_T ;
- (6) $R \rightarrow I$: HDR $\parallel$ {ID _{R} $\parallel$ CERT _{R} $\parallel$ QUOTE_R $\parallel$ RESULT_R $\parallel$ AUTH_R $\parallel$ SA _{$R,2$} $\parallel$ TS _{I} $\parallel$ TS _{R} }_{SK _{R}} .

在上述步骤中, 新增加的消息和字段是用单下

划线标记的, 而新扩展的字段是用双下划线标记的. Res_T = N _{R} ⁰ $\parallel$ Cert _{i} $\parallel$ Cert(AIK _{pk_{α}}) $\parallel$ PCR _{α} $\parallel$ Re_{CERT, i} $\parallel$ Re_{AIK, α} $\parallel$ Re_{INT, α} $\parallel$ N _{I} ⁰ $\parallel$ Cert _{r} $\parallel$ Cert(AIK _{pk_{β}}) $\parallel$ PCR _{β} $\parallel$ Re_{CERT, r} $\parallel$ Re_{AIK, β} $\parallel$ Re_{INT, β} , Cert _{i} 和 Cert _{r} 分别为 I 和 R 的身份证书, Re_{CERT, i} 和 Re_{CERT, r} 分别为 Cert _{i} 和 Cert _{r} 的身份证书验证结果.

此外, CERTREQ_I 和 CERTREQ_R 分别为 I 和 R 的身份证书请求负载, 分别包含 I 和 R 信任的证书授权机构. CERT_I 和 CERT_R 分别为 I 和 R 的身份证书负载, 分别包含 Cert _{i} 和 Cert _{r} . AUTH_I = [HDR $\parallel$ SA _{$I,1$} $\parallel$ KE _{I} $\parallel$ N _{I} $\parallel$ N _{R} ⁰ $\parallel$ prf(SK_{PI}, ID _{I} ^{*})]_{sk _{I}} , AUTH_R = [HDR $\parallel$ SA _{$R,1$} $\parallel$ KE _{R} $\parallel$ N _{R} $\parallel$ CERTREQ_R $\parallel$ TTP_R $\parallel$ N _{I} ⁰ $\parallel$ prf(SK_{PR}, ID _{R} ^{*})]_{sk _{r}} , 其中 sk _{i} 和 sk _{r} 分别为 I 和 R 的私钥.

3 安全性分析

由于本文扩展后的 IKE 初始交换增加了平台认证, 所以传统的 SSM 不能用来分析其安全性. 为了分析本文扩展后的 IKE 初始交换的安全性, 下面基于文献[14]中所提出的针对可信网络接入协议的 SSM 对本文扩展后的 IKE 初始交换进行安全性分析.

3.1 基于预共享密钥模式

定义 1 基于预共享密钥模式下扩展后的 IKE 初始交换的串空间是以下 4 类串的并集: (1) 发起者串 $s \in \text{Init}[i \cdot \alpha, r \cdot \beta, T, \text{HDR}, \text{ID}_I, \text{ID}_R, N_I, N_R, \text{SA}_{I,1}, \text{SA}_{R,1}, \text{SA}_{I,2}, \text{SA}_{R,2}, \text{KE}_I, \text{KE}_R, \text{AUTH}_I, \text{AUTH}_R, \text{TS}_I, \text{TS}_R, \text{TTP}_I, \text{TTP}_R, \text{QUOTE}_I, \text{QUOTE}_R, \text{SML}_I, \text{RESULT}_R]$, 迹为: $< + m_1, - m_2, + m_3, - m_4 >$, 与这类串相关联的主体为 I , 用 $i \cdot \alpha$ 表示, 是一个双身份协议主体^[14], 其中 i 表示 I 的用户, α 表示 I 的平台; (2) 响应者串 $s \in \text{Resp}[i \cdot \alpha, r \cdot \beta, T, \text{HDR}, \text{ID}_I, \text{ID}_R, N_I, N_R, \text{SA}_{I,1}, \text{SA}_{R,1}, \text{SA}_{I,2}, \text{SA}_{R,2}, \text{KE}_I, \text{KE}_R, \text{AUTH}_I, \text{AUTH}_R, \text{TS}_I, \text{TS}_R, \text{TTP}_I, \text{TTP}_R, \text{QUOTE}_I, \text{QUOTE}_R, \text{SML}_I, \text{RESULT}_R, N_I^0, N_R^0, \text{Cert}(\text{AIK}_{pk_{\alpha}}), \text{Cert}(\text{AIK}_{pk_{\beta}}), \text{PCR}_{\alpha}, \text{PCR}_{\beta}, \text{SML}_{\alpha}, \text{SML}_{\beta}, \text{Re}_{\text{AIK}, \alpha}, \text{Re}_{\text{AIK}, \beta}, \text{Re}_{\text{INT}, \alpha}, \text{Re}_{\text{INT}, \beta}]$, 迹为: $< - m_1, + m_2, - m_3, + M_1, - M_2 + m_4 >$, 与这类串相关联的主体为 R , 用 $r \cdot \beta$ 表示, 是一个双身份协议主体^[14], 其中 r 表示 R 的用户, β 表示 R 的平台; (3) 服务器串 $s \in \text{Serv}[N_I^0, N_R^0, \text{Cert}(\text{AIK}_{pk_{\alpha}}), \text{Cert}(\text{AIK}_{pk_{\beta}}), \text{PCR}_{\alpha}, \text{PCR}_{\beta}, \text{SML}_{\alpha}, \text{SML}_{\beta}, \text{Re}_{\text{AIK}, \alpha}, \text{Re}_{\text{AIK}, \beta}, \text{Re}_{\text{INT}, \alpha}, \text{Re}_{\text{INT}, \beta}]$, 迹为: $< - M_1, + M_2 >$, 与类串相关联的主体为 T ; (4) 入侵者

串 $s \in P$. m_1, m_2, m_3 和 m_4 为 I 和 R 之间的 4 条 IKE 消息, M_1 和 M_2 为 R 和 T 之间的 2 条消息. 此外, SML_α 表明 α 是可信的平台, 而 SML_β 表明 β 是可信的平台.

定理 1 假设 (1) $\sum$ 为基于预共享密钥模式下扩展后的 IKE 初始交换的串空间, C 为 $\sum$ 中的丛, 包含一个发起者串 s , 其迹为 $s \in \text{Init}[i \cdot \alpha, r \cdot \beta, T, \text{HDR}, \text{ID}_I, \text{ID}_R, N_I, N_R, \text{SA}_{I,1}, \text{SA}_{R,1}, \text{SA}_{I,2}, \text{SA}_{R,2}, \text{KE}_I, \text{KE}_R, \text{AUTH}_I, \text{AUTH}_R, \text{TS}_I, \text{TS}_R, \text{TTP}_I, \text{TTP}_R, \text{QUOTE}_I, \text{QUOTE}_R, \text{SML}_I, \text{RESULT}_R]$; (2) $K_{\text{pre-shared}} \notin K_{ep}$ 且 $sk_T \notin K_P$; (3) g^x 和 g^y 唯一产生于 $\sum$ 中, 且 $g^x \neq g^y$. 那么 C 中包含响应者串 $r \in \text{Resp}[i \cdot \alpha, r \cdot \beta, T, \text{HDR}, \text{ID}_I, \text{ID}_R, N_I, N_R, \text{SA}_{I,1}, \text{SA}_{R,1}, \text{SA}_{I,2}, \text{SA}_{R,2}, \text{KE}_I, \text{KE}_R, \text{AUTH}_I, \text{AUTH}_R, \text{TS}_I, \text{TS}_R, \text{TTP}_I, \text{TTP}_R, \text{QUOTE}_I, \text{QUOTE}_R, \text{SML}_I, \text{RESULT}_R, N_I^0, N_R^0, \text{Cert}(\text{AIK}_{pk,\alpha}), \text{Cert}(\text{AIK}_{pk,\beta}), \text{PCR}_\alpha, \text{PCR}_\beta, \text{SML}_\alpha, \text{SML}_\beta, \text{Re}_{\text{AIK},\alpha}, \text{Re}_{\text{AIK},\beta}, \text{Re}_{\text{INT},\alpha}, \text{Re}_{\text{INT},\beta}]$ 和一个服务者串 $t \in \text{Serv}[N_I^0, N_R^0, \text{Cert}(\text{AIK}_{pk,\alpha}), \text{Cert}(\text{AIK}_{pk,\beta}), \text{PCR}_\alpha, \text{PCR}_\beta, \text{SML}_\alpha, \text{SML}_\beta, \text{Re}_{\text{AIK},\alpha}, \text{Re}_{\text{AIK},\beta}, \text{Re}_{\text{INT},\alpha}, \text{Re}_{\text{INT},\beta}]$.

证明由定义 1 和假设 2 可知, $\sigma_T \subset \text{RESULT}_R \subset \text{term}(< s, 4 >)$ 唯一源发于一个服务者串 $t \in \text{Serv}[N_I^0, N_R^0, \text{Cert}(\text{AIK}_{pk,\alpha}), \text{Cert}(\text{AIK}_{pk,\beta}), \text{PCR}_\alpha, \text{PCR}_\beta, \text{SML}_\alpha, \text{SML}_\beta, \text{Re}_{\text{AIK},\alpha}, \text{Re}_{\text{AIK},\beta}, \text{Re}_{\text{INT},\alpha}, \text{Re}_{\text{INT},\beta}]$.

(1) 如果 $K_{\text{pre-shared}} \notin K_{ip}$, 那么由假设 2 可知, $K_{\text{pre-shared}} \notin K_P$, 从而 $\text{AUTH}_R \subset \text{term}(< s, 4 >)$ 唯一源发于一个响应者串 r . 因为 $g^y \subset \text{KE}_R \subset \text{AUTH}_R$, 所以 g^y 唯一源发于这个响应者串 r . 由假设 1 和 3 可知, g^x 唯一产生于 $< s, 1 >$. 因为定义 1 所述的基于预共享密钥模式下扩展后的 IKE 初始交换具有文献[15]中定义的沉默性和保守性, 所以由文献[15]中的定理 9 可知, g^{xy} 不源发于 C 中, 从而 $\text{SK}_I, \text{SK}_R \notin K_P$. 因为 SK_I 和 SK_R 分别用来保护 m_3 和 m_4 , 而 AUTH_I 和 AUTH_R 分别用来保护 m_1 和 m_2 , 所以 $r \in \text{Resp}[i \cdot \alpha, r \cdot \beta, T, \text{HDR}, \text{ID}_I, \text{ID}_R, N_I, N_R, \text{SA}_{I,1}, \text{SA}_{R,1}, \text{SA}_{I,2}, \text{SA}_{R,2}, \text{KE}_I, \text{KE}_R, \text{AUTH}_I, \text{AUTH}_R, \text{TS}_I, \text{TS}_R, \text{TTP}_I, \text{TTP}_R, \text{QUOTE}_I, \text{QUOTE}_R, \text{SML}_I, \text{RESULT}_R, N_I^0, N_R^0, \text{Cert}(\text{AIK}_{pk,\alpha}), \text{Cert}(\text{AIK}_{pk,\beta}), \text{PCR}_\alpha, \text{PCR}_\beta, \text{SML}_\alpha, \text{SML}_\beta, \text{Re}_{\text{AIK},\alpha}, \text{Re}_{\text{AIK},\beta}, \text{Re}_{\text{INT},\alpha}, \text{Re}_{\text{INT},\beta}]$.

(2) 如果 $K_{\text{pre-shared}} \in K_{ip}$, 那么 $\sigma_\beta \subset \text{QUOTE}_R \subset \text{term}(< s, 4 >)$ 唯一源发于一个响应者串 r' (文献[14]中的定理 (1)). 因为 $\sigma_\beta = [\text{prf}(\text{SK}_R, N_I^0),$

$\text{PCR}_\beta]_{\text{AIK}_{pk,\beta}}$, 且 SK_R 是基于 g^y 计算的, 所以 g^y 唯一源发于这个响应者串 r' . 由假设 1 和 3 可知, g^x 唯一产生于 $< s, 1 >$. 因为定义 1 所述的基于预共享密钥模式下扩展后的 IKE 初始交换具有文献[15]中定义的沉默性和保守性, 所以由文献[15]中的定理 9 可知, g^{xy} 不源发于 C 中, 从而 $\text{SK}_I, \text{SK}_R \notin K_P$. 因为 SK_I 和 SK_R 分别用来保护 m_3 和 m_4 , 而 AUTH_I 和 AUTH_R 分别用来保护 m_1 和 m_2 , 所以 $r' = r$.

定理 2 假设 (1) $\sum$ 为基于预共享密钥模式下扩展后的 IKE 初始交换的串空间, C 为 $\sum$ 中的丛, 包含一个响应者串 s , 其迹为: $s \in \text{Resp}[i \cdot \alpha, r \cdot \beta, T, \text{HDR}, \text{ID}_I, \text{ID}_R, N_I, N_R, \text{SA}_{I,1}, \text{SA}_{R,1}, \text{SA}_{I,2}, \text{SA}_{R,2}, \text{KE}_I, \text{KE}_R, \text{AUTH}_I, \text{AUTH}_R, \text{TS}_I, \text{TS}_R, \text{TTP}_I, \text{TTP}_R, \text{QUOTE}_I, \text{QUOTE}_R, \text{SML}_I, \text{RESULT}_R, N_I^0, N_R^0, \text{Cert}(\text{AIK}_{pk,\alpha}), \text{Cert}(\text{AIK}_{pk,\beta}), \text{PCR}_\alpha, \text{PCR}_\beta, \text{SML}_\alpha, \text{SML}_\beta, \text{Re}_{\text{AIK},\alpha}, \text{Re}_{\text{AIK},\beta}, \text{Re}_{\text{INT},\alpha}, \text{Re}_{\text{INT},\beta}]$; (2) $K_{\text{pre-shared}} \notin K_{ep}$ 且 $sk_T \notin K_P$; (3) g^x 和 g^y 唯一产生于 $\sum$ 中, 且 $g^x \neq g^y$. 那么 C 中包含发起者串 $r \in \text{Init}[i \cdot \alpha, r \cdot \beta, T, \text{HDR}, \text{ID}_I, \text{ID}_R, N_I, N_R, \text{SA}_{I,1}, \text{SA}_{R,1}, \text{SA}_{I,2}, \text{SA}_{R,2}, \text{KE}_I, \text{KE}_R, \text{AUTH}_I, \text{AUTH}_R, \text{TS}_I, \text{TS}_R, \text{TTP}_I, \text{TTP}_R, \text{QUOTE}_I, \text{QUOTE}_R, \text{SML}_I, \text{RESULT}_R]$ 和一个服务者串 $t \in \text{Serv}[N_I^0, N_R^0, \text{Cert}(\text{AIK}_{pk,\alpha}), \text{Cert}(\text{AIK}_{pk,\beta}), \text{PCR}_\alpha, \text{PCR}_\beta, \text{SML}_\alpha, \text{SML}_\beta, \text{Re}_{\text{AIK},\alpha}, \text{Re}_{\text{AIK},\beta}, \text{Re}_{\text{INT},\alpha}, \text{Re}_{\text{INT},\beta}]$.

证明由定义 1 和假设 2 可知, $\sigma_T \subset \text{term}(< s, 5 >)$ 唯一源发于一个服务者串 $t \in \text{Serv}[N_I^0, N_R^0, \text{Cert}(\text{AIK}_{pk,\alpha}), \text{Cert}(\text{AIK}_{pk,\beta}), \text{PCR}_\alpha, \text{PCR}_\beta, \text{SML}_\alpha, \text{SML}_\beta, \text{Re}_{\text{AIK},\alpha}, \text{Re}_{\text{AIK},\beta}, \text{Re}_{\text{INT},\alpha}, \text{Re}_{\text{INT},\beta}]$.

(1) 如果 $K_{\text{pre-shared}} \notin K_{ip}$, 那么由假设 2 可知, $K_{\text{pre-shared}} \notin K_P$, 从而 $\text{AUTH}_I \subset \text{term}(< s, 3 >)$ 唯一源发于一个发起者串 r . 因为 $g^x \subset \text{KE}_I \subset \text{AUTH}_I$, 所以 g^x 唯一源发于这个发起者串 r . 由假设 1 和 3 可知, g^y 唯一产生于 $< s, 2 >$. 因为定义 1 所述的基于预共享密钥模式下扩展后的 IKE 初始交换具有文献[15]中定义的沉默性和保守性, 所以由文献[15]中的定理 9 可知, g^{xy} 不源发于 C 中, 从而 $\text{SK}_I, \text{SK}_R \notin K_P$. 因为 SK_I 和 SK_R 分别用来保护 m_3 和 m_4 , 而 AUTH_I 和 AUTH_R 分别用来保护 m_1 和 m_2 , 所以 $r \in \text{Init}[i \cdot \alpha, r \cdot \beta, T, \text{HDR}, \text{ID}_I, \text{ID}_R, N_I, N_R, \text{SA}_{I,1}, \text{SA}_{R,1}, \text{SA}_{I,2}, \text{SA}_{R,2}, \text{KE}_I, \text{KE}_R, \text{AUTH}_I, \text{AUTH}_R, \text{TS}_I, \text{TS}_R, \text{TTP}_I, \text{TTP}_R, \text{QUOTE}_I, \text{QUOTE}_R, \text{SML}_I, \text{RESULT}_R]$.

(2) 如果 $K_{\text{pre-shared}} \in K_{ip}$, 那么 $\sigma_\alpha \subset \text{QUOTE}_I \subset$

$\text{term}(< s, 3 >)$ 唯一源发于一个发起者串 r (文献[14]中的定理 1. 因为 $\sigma_a = [\text{prf}(\text{SK}_I, N_R^a) \parallel \text{PCR}_\alpha]_{\text{AIK}_{\text{sk},a}}$, 且 SK_I 是基于 g^x 计算的, 所以 g^x 唯一源发于这个发起者串 r . 由假设 1 和 3 可知, g^y 唯一产生于 $< s, 2 >$. 因为定义 1 所述的基于预共享密钥模式下扩展后的 IKE 初始交换具有文献[15]中定义的沉默性和保守性, 所以由文献[15]中的定理 9 可知, g^{xy} 不源发于 C 中, 从而 $\text{SK}_I, \text{SK}_R \notin K_P$. 因为 SK_I 和 SK_R 分别用来保护 m_3 和 m_4 , 而 AUTH_I 和 AUTH_R 分别用来保护 m_1 和 m_2 , 所以 $r = r$.

由定理 1 和 2 可知, 基于预共享密钥模式下扩展后的 IKE 初始交换不仅可以抵抗外部攻击者(密钥集为 K_{ep})的攻击, 而且可以抵抗内部攻击者(密钥集为 K_{ip})的攻击. 因此, 基于预共享密钥模式下扩展后的 IKE 初始交换是安全的.

3.2 基于证书模式

定义 2 基于预共享密钥模式下扩展后的 IKE 初始交换的串空间是以下 4 类串的并集: (1) 发起者串 $s \in \text{Init}[i \cdot \alpha, r \cdot \beta, T, \text{HDR}, \text{ID}_I, \text{ID}_R, N_I, N_R, \text{SA}_{I,1}, \text{SA}_{R,1}, \text{SA}_{I,2}, \text{SA}_{R,2}, \text{KE}_I, \text{KE}_R, \text{AUTH}_I, \text{AUTH}_R, \text{TS}_I, \text{TS}_R, \text{TTP}_I, \text{TTP}_R, \text{QUOTE}_I, \text{QUOTE}_R, \text{SML}_I, \text{RESULT}_R, \text{CERT}_I, \text{CERT}_R, \text{CERTREQ}_I, \text{CERTREQ}_R]$, 迹为: $< +m_1, -m_2, +m_3, -m_4 >$, 与这类串相关联的主体为 I , 用 $i \cdot \alpha$ 表示, 是一个双身份协议主体^[14], 其中 i 表示 I 的用户, α 表示 I 的平台; (2) 响应者串 $s \in \text{Resp}[i \cdot \alpha, r \cdot \beta, T, \text{HDR}, \text{ID}_I, \text{ID}_R, N_I, N_R, \text{SA}_{I,1}, \text{SA}_{R,1}, \text{SA}_{I,2}, \text{SA}_{R,2}, \text{KE}_I, \text{KE}_R, \text{AUTH}_I, \text{AUTH}_R, \text{TS}_I, \text{TS}_R, \text{TTP}_I, \text{TTP}_R, \text{QUOTE}_I, \text{QUOTE}_R, \text{SML}_I, \text{RESULT}_R, N_I^0, N_R^0, \text{Cert}(\text{AIK}_{pk,a}), \text{Cert}(\text{AIK}_{pk,\beta}), \text{PCR}_\alpha, \text{PCR}_\beta, \text{SML}_\alpha, \text{SML}_\beta, \text{ReAIK}_\alpha, \text{ReAIK}_\beta, \text{ReINT}_\alpha, \text{ReINT}_\beta, \text{CERT}_I, \text{CERT}_R, \text{CERTREQ}_I, \text{CERTREQ}_R, \text{Cert}_i, \text{Cert}_r, \text{ReCERT}_i, \text{ReCERT}_r]$, 迹为: $< -m_1, +m_2, -m_3, +M_1, -M_2 + m_4 >$, 与类串相关联的主体为 R , 用 $r \cdot \beta$ 表示, 是一个双身份协议主体^[14], 其中 r 表示 R 的用户, β 表示 R 的平台; (3) 服务者串 $s \in \text{Serv}[N_I^0, N_R^0, \text{Cert}(\text{AIK}_{pk,a}), \text{Cert}(\text{AIK}_{pk,\beta}), \text{PCR}_\alpha, \text{PCR}_\beta, \text{SML}_\alpha, \text{SML}_\beta, \text{ReAIK}_\alpha, \text{ReAIK}_\beta, \text{ReINT}_\alpha, \text{ReINT}_\beta, \text{Cert}_i, \text{Cert}_r, \text{ReCERT}_i, \text{ReCERT}_r]$, 迹为: $< -M_1, +M_2 >$, 与类串相关联的主体为 T ; (4) 入侵者串 $s \in P$. m_1, m_2, m_3 和 m_4 是 I 和 R 之间交互的 4 条 IKE 消息, 而 M_1 和 M_2 是 R 和 T 之间交互的 2 条消息. 此外, SML_α 表明 α 是可

信赖的平台, 而 SML_β 表明 β 是可信赖的平台.

定理 3 假设: (1) $\sum$ 为基于证书模式下扩展后的 IKE 初始交换的串空间, C 为 $\sum$ 中的丛, 包含一个发起者串 s , 其迹为: $s \in \text{Init}[i \cdot \alpha, r \cdot \beta, T, \text{HDR}, \text{ID}_I, \text{ID}_R, N_I, N_R, \text{SA}_{I,1}, \text{SA}_{R,1}, \text{SA}_{I,2}, \text{SA}_{R,2}, \text{KE}_I, \text{KE}_R, \text{AUTH}_I, \text{AUTH}_R, \text{TS}_I, \text{TS}_R, \text{TTP}_I, \text{TTP}_R, \text{QUOTE}_I, \text{QUOTE}_R, \text{SML}_I, \text{RESULT}_R, \text{CERT}_I, \text{CERT}_R, \text{CERTREQ}_I, \text{CERTREQ}_R]$; (2) $sk_r \notin K_{ep}$ 且 $sk_T \notin K_P$; (3) g^x 和 g^y 唯一产生于 $\sum$ 中, 且 $g^x \neq g^y$. 那么 C 中包含响应者串 $r \in \text{Resp}[i \cdot \alpha, r \cdot \beta, T, \text{HDR}, \text{ID}_I, \text{ID}_R, N_I, N_R, \text{SA}_{I,1}, \text{SA}_{R,1}, \text{SA}_{I,2}, \text{SA}_{R,2}, \text{KE}_I, \text{KE}_R, \text{AUTH}_I, \text{AUTH}_R, \text{TS}_I, \text{TS}_R, \text{TTP}_I, \text{TTP}_R, \text{QUOTE}_I, \text{QUOTE}_R, \text{SML}_I, \text{RESULT}_R, N_I^0, N_R^0, \text{Cert}(\text{AIK}_{pk,a}), \text{Cert}(\text{AIK}_{pk,\beta}), \text{PCR}_\alpha, \text{PCR}_\beta, \text{SML}_\alpha, \text{SML}_\beta, \text{ReAIK}_\alpha, \text{ReAIK}_\beta, \text{ReINT}_\alpha, \text{ReINT}_\beta, \text{CERT}_I, \text{CERT}_R, \text{CERTREQ}_I, \text{CERTREQ}_R, \text{Cert}_i, \text{Cert}_r, \text{ReCERT}_i, \text{ReCERT}_r]$ 和一个服务者串 $t \in \text{Serv}[N_I^0, N_R^0, \text{Cert}(\text{AIK}_{pk,a}), \text{Cert}(\text{AIK}_{pk,\beta}), \text{PCR}_\alpha, \text{PCR}_\beta, \text{SML}_\alpha, \text{SML}_\beta, \text{ReAIK}_\alpha, \text{ReAIK}_\beta, \text{ReINT}_\alpha, \text{ReINT}_\beta, \text{Cert}_i, \text{Cert}_r, \text{ReCERT}_i, \text{ReCERT}_r]$.

证明 由定义 1 和假设 2 可知, $\sigma_T \subset \text{RESULT}_R \subset \text{term}(< s, 4 >)$ 唯一源发于一个服务者串 $t \in \text{Serv}[N_I^0, N_R^0, \text{Cert}(\text{AIK}_{pk,a}), \text{Cert}(\text{AIK}_{pk,\beta}), \text{PCR}_\alpha, \text{PCR}_\beta, \text{SML}_\alpha, \text{SML}_\beta, \text{ReAIK}_\alpha, \text{ReAIK}_\beta, \text{ReINT}_\alpha, \text{ReINT}_\beta, \text{Cert}_i, \text{Cert}_r, \text{ReCERT}_i, \text{ReCERT}_r]$.

(1) 如果 $sk_r \notin K_{ip}$, 那么由假设 2 可知, $sk_r \notin K_P$, 从而 $\text{AUTH}_R \subset \text{term}(< s, 4 >)$ 唯一源发于一个响应者串 r . 因为 $g^y \subset \text{KE}_R \subset \text{AUTH}_R$, 所以 g^y 唯一源发于这个响应者串 r . 由假设 1 和 3 可知, g^x 唯一产生于 $< s, 1 >$. 因为定义 1 所述的基于证书模式下扩展后的 IKE 初始交换具有文献[15]中定义的沉默性和保守性, 所以由文献[15]中的定理 9 可知, g^{xy} 不源发于 C 中, 从而 $\text{SK}_I, \text{SK}_R \notin K_P$. 因为 SK_I 和 SK_R 分别用来保护 m_3 和 m_4 , 而 AUTH_I 和 AUTH_R 分别用来保护 m_1 和 m_2 , 所以 $r \in \text{Resp}[i \cdot \alpha, r \cdot \beta, T, \text{HDR}, \text{ID}_I, \text{ID}_R, N_I, N_R, \text{SA}_{I,1}, \text{SA}_{R,1}, \text{SA}_{I,2}, \text{SA}_{R,2}, \text{KE}_I, \text{KE}_R, \text{AUTH}_I, \text{AUTH}_R, \text{TS}_I, \text{TS}_R, \text{TTP}_I, \text{TTP}_R, \text{QUOTE}_I, \text{QUOTE}_R, \text{SML}_I, \text{RESULT}_R, N_I^0, N_R^0, \text{Cert}(\text{AIK}_{pk,a}), \text{Cert}(\text{AIK}_{pk,\beta}), \text{PCR}_\alpha, \text{PCR}_\beta, \text{SML}_\alpha, \text{SML}_\beta, \text{ReAIK}_\alpha, \text{ReAIK}_\beta, \text{ReINT}_\alpha, \text{ReINT}_\beta, \text{CERT}_I, \text{CERT}_R, \text{CERTREQ}_I, \text{CERTREQ}_R, \text{Cert}_i, \text{Cert}_r, \text{ReCERT}_i, \text{ReCERT}_r]$.

(2) 如果 $sk_r \in K_{ip}$, 那么 $\sigma_\beta \subset \text{QUOTE}_R \subset \text{term}(<$

$s, 4 \rangle$ 唯一源发于一个响应者串 r' (文献[14]中的定理 1). 因为 $\sigma_\beta = [\text{prf}(\text{SK}_R, N_I^0), \text{PCR}_\beta]_{\text{AIK}_{\mathcal{K}_\beta}}$, 且 SK_R 是基于 g^y 计算的, 所以 g^y 唯一源发于这个响应者串 r' . 由假设 1 和 3 可知, g^x 唯一产生于 $\langle s, 1 \rangle$. 因为定义 1 所述的基于证书模式下扩展后的 IKE 初始交换具有文献[15]中定义的沉默性和保守性, 所以由文献[15]中的定理 9 可知, g^{xy} 不源发于 C 中, 从而 $\text{SK}_I, \text{SK}_R \notin K_P$. 因为 SK_I 和 SK_R 分别用来保护 m_3 和 m_4 , 而 AUTH_I 和 AUTH_R 分别用来保护 m_1 和 m_2 , 所以 $r' = r$.

定理 4 假设: (1) $\sum$ 为基于证书模式下扩展后的 IKE 初始交换的串空间, C 为 $\sum$ 中的丛, 包含一个响应者串 s , 其迹为: $s \in \text{Resp}[i \cdot \alpha, r \cdot \beta, T, \text{HDR}, \text{ID}_I, \text{ID}_R, N_I, N_R, \text{SA}_{I,1}, \text{SA}_{R,1}, \text{SA}_{I,2}, \text{SA}_{R,2}, \text{KE}_I, \text{KE}_R, \text{AUTH}_I, \text{AUTH}_R, \text{TS}_I, \text{TS}_R, \text{TTP}_I, \text{TTP}_R, \text{QUOTE}_I, \text{QUOTE}_R, \text{SML}_I, \text{RESULT}_R, N_I^0, N_R^0, \text{Cert}(\text{AIK}_{\mathcal{K}_{\beta,a}}), \text{Cert}(\text{AIK}_{\mathcal{K}_{\beta,\beta}}), \text{PCR}_\alpha, \text{PCR}_\beta, \text{SML}_\alpha, \text{SML}_\beta, \text{Re}_{\text{AIK},\alpha}, \text{Re}_{\text{AIK},\beta}, \text{Re}_{\text{INT},\alpha}, \text{Re}_{\text{INT},\beta}, \text{CERT}_I, \text{CERT}_R, \text{CERTREQ}_I, \text{CERTREQ}_R, \text{Cert}_i, \text{Cert}_r, \text{Re}_{\text{CERT},i}, \text{Re}_{\text{CERT},r}]$; (2) $\mathcal{K}_i \notin K_{ep}$ 且 $\mathcal{K}_T \notin K_P$; (3) g^x 和 g^y 唯一产生于 $\sum$ 中, 且 $g^x \neq g^y$. 那么 C 中包含发起者串 $r \in \text{Init}[i \cdot \alpha, r \cdot \beta, T, \text{HDR}, \text{ID}_I, \text{ID}_R, N_I, N_R, \text{SA}_{I,1}, \text{SA}_{R,1}, \text{SA}_{I,2}, \text{SA}_{R,2}, \text{KE}_I, \text{KE}_R, \text{AUTH}_I, \text{AUTH}_R, \text{TS}_I, \text{TS}_R, \text{TTP}_I, \text{TTP}_R, \text{QUOTE}_I, \text{QUOTE}_R, \text{SML}_I, \text{RESULT}_R, \text{CERT}_I, \text{CERT}_R, \text{CERTREQ}_I, \text{CERTREQ}_R]$ 和一个服务者串 $t \in \text{Serv}[N_I^0, N_R^0, \text{Cert}(\text{AIK}_{\mathcal{K}_{\beta,a}}), \text{Cert}(\text{AIK}_{\mathcal{K}_{\beta,\beta}}), \text{PCR}_\alpha, \text{PCR}_\beta, \text{SML}_\alpha, \text{SML}_\beta, \text{Re}_{\text{AIK},\alpha}, \text{Re}_{\text{AIK},\beta}, \text{Re}_{\text{INT},\alpha}, \text{Re}_{\text{INT},\beta}, \text{Cert}_i, \text{Cert}_r, \text{Re}_{\text{CERT},i}, \text{Re}_{\text{CERT},r}]$.

证明由定义 1 和假设 2 可知, $\sigma_T \subset \text{term}(\langle s, 5 \rangle)$ 唯一源发于一个服务者串 $t \in \text{Serv}[N_I^0, N_R^0, \text{Cert}(\text{AIK}_{\mathcal{K}_{\beta,a}}), \text{Cert}(\text{AIK}_{\mathcal{K}_{\beta,\beta}}), \text{PCR}_\alpha, \text{PCR}_\beta, \text{SML}_\alpha, \text{SML}_\beta, \text{Re}_{\text{AIK},\alpha}, \text{Re}_{\text{AIK},\beta}, \text{Re}_{\text{INT},\alpha}, \text{Re}_{\text{INT},\beta}, \text{Cert}_i, \text{Cert}_r, \text{Re}_{\text{CERT},i}, \text{Re}_{\text{CERT},r}]$.

(1) 如果 $\mathcal{K}_i \notin K_{ip}$, 那么由假设 2 可知, $\mathcal{K}_i \notin K_P$, 从而 $\text{AUTH}_I \subset \text{term}(\langle s, 3 \rangle)$ 唯一源发于一个发起者串 r . 因为 $g^x \subset \text{KE}_I \subset \text{AUTH}_I$, 所以 g^x 唯一源发于这个发起者串 r . 由假设 1 和 3 可知, g^y 唯一产生于 $\langle s, 2 \rangle$. 因为定义 1 所述的基于证书模式下扩展后的 IKE 初始交换具有文献[15]中定义的沉默性和保守性, 所以由文献[15]中的定理 9 可知, g^{xy} 不源发于 C 中, 从而 $\text{SK}_I, \text{SK}_R \notin K_P$. 因为 SK_I 和 SK_R 分别用来保护 m_3 和 m_4 , 而 AUTH_I 和 AUTH_R 分别用来保护 m_1 和 m_2 , 所以 $r \in \text{Init}[i \cdot \alpha, r \cdot \beta, T, \text{HDR}, \text{ID}_I, \text{ID}_R, N_I,$

$N_R, \text{SA}_{I,1}, \text{SA}_{R,1}, \text{SA}_{I,2}, \text{SA}_{R,2}, \text{KE}_I, \text{KE}_R, \text{AUTH}_I, \text{AUTH}_R, \text{TS}_I, \text{TS}_R, \text{TTP}_I, \text{TTP}_R, \text{QUOTE}_I, \text{QUOTE}_R, \text{SML}_I, \text{RESULT}_R, \text{CERT}_I, \text{CERT}_R, \text{CERTREQ}_I, \text{CERTREQ}_R]$.

(2) 如果 $\mathcal{K}_i \in K_{ip}$, 那么 $\sigma_\alpha \subset \text{QUOTE}_I \subset \text{term}(\langle s, 3 \rangle)$ 唯一源发于一个发起者串 r' (文献[14]中的定理 1). 因为 $\sigma_\alpha = [\text{prf}(\text{SK}_I, N_R^0) \parallel \text{PCR}_\alpha]_{\text{AIK}_{\mathcal{K}_{\alpha,a}}}$, 且 SK_I 是基于 g^x 计算的, 所以 g^x 唯一源发于这个发起者串 r' . 由假设 1 和 3 可知, g^y 唯一产生于 $\langle s, 2 \rangle$. 因为定义 1 所述的基于证书模式下扩展后的 IKE 初始交换具有文献[15]中定义的沉默性和保守性, 所以由文献[15]中的定理 9 可知, g^{xy} 不源发于 C 中, 从而 $\text{SK}_I, \text{SK}_R \notin K_P$. 因为 SK_I 和 SK_R 分别用来保护 m_3 和 m_4 , 而 AUTH_I 和 AUTH_R 分别用来保护 m_1 和 m_2 , 所以 $r' = r$.

由定理 3 和 4 可知, 基于证书模式下扩展后的 IKE 初始交换不仅可以抵抗外部攻击者 (密钥集为 K_{ep}) 的攻击, 而且可以抵抗内部攻击者 (密钥集为 K_{ip}) 的攻击. 因此, 基于证书模式下扩展后的 IKE 初始交换是安全的.

4 结束语

本文在 IKEv2 协议基础上, 利用 ISO/IEC 9798-3:1998/Amd 1:2010 中的认证机制, 提出了一种可信计算环境下的 IKEv2 协议扩展方案. 在该扩展方案中, I 实现了对 R 的身份认证和平台认证, 实现了对 T 的身份认证, 从 T 获得了对 R 的身份证书验证结果, AIK 证书验证结果和平台完整性评估结果. 与此同时, R 实现了对 I 的身份认证和平台认证, 实现了对 T 的身份认证, 从 T 获得了对 I 的身份证书验证结果、 AIK 证书验证结果和平台完整性评估结果. 此外, I 和 R 的 SML 被加密传输给 T , 从而有效保护了 I 和 R 的平台配置隐私. 由于该扩展方案只是增加了一些消息和字段, 以及扩展了一些字段, 所以它与 IKEv2 是兼容的. 最后, 利用针对可信网络连接协议的 SSM 证明了该扩展方案是安全的.

参考文献:

- [1] Kent S, Seo K. RFC 4301. Security architecture for the internet protocol [S]. USA: IETF, 2005.
- [2] Kaufman C, Hoffman P, Nir Y, et al. RFC 7296. Internet key exchange protocol version 2 (IKEv2) [S]. USA: IETF, 2014.

- [3] Piper D. RFC 2407, The internet IP security domain of interpretation for ISAKMP [S]. USA: IETF, 1998.
- [4] Maughan D, Schneider M, Schertler M. RFC 2408, Internet security association and key management protocol (ISAKMP) [S]. USA: IETF, 1998.
- [5] Harkins D, Carrel D. RFC 2409. The internet key exchange (IKE) [S]. USA: IETF, 1998.
- [6] Kaufman C. RFC 4306, Internet key exchange (IKEv2) protocol [S]. USA: IETF, 2005.
- [7] Eronen P, Hoffman P. RFC 4718, IKEv2 clarifications and implementation guidelines [S]. USA: IETF, 2006.
- [8] Kaufman C, Hoffman P, Nir Y, et al. RFC 5996, Internet key exchange protocol version 2 (IKEv2) [S]. USA: IETF, 2010.
- [9] TCG. TCG trusted network communications: TNC architecture for interoperability specification version 1.5 [EB/OL]. (2012-05-07). [2018-04-29]. https://trustedcomputinggroup.org/wp-content/uploads/TNC_Architecture_v1_5_r4.pdf.
- [10] Xia H D, Kanchana J, Brustoloni J C. Enforcement of security policy compliance in virtual private networks [EB/OL]. (2015-11-23). [2018-04-29]. http://people.cs.pitt.edu/~hdxia/papers/ssi2005_xia.pdf
- [11] Sadeghi A R, Schulz S. Extending IPSec for efficient remote attestation [C]//Proceedings of the 14th international conference on financial cryptography and data security. Tenerife: Springer, 2010: 150-165.
- [12] Abd Aziz N, Setapa S, Udzir N I. Mutual remote attestation in IPSec based VPN [J]. International Journal of Cryptology Research, 2013, 4(1): 55-67.
- [13] Lai X L. ISO/IEC 9798-3:1998/Amd 1:2010, Information technology security techniques entity authentication mechanisms - Part 3: Entity authentication using a public key algorithm - Amendment 1 [S]. USA: ISO/IEC, 2010.
- [14] Xiao Y L, Wang Y M, Pang L J. Verification of trusted network access protocols in the strand space model [J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2012, E95-A(3): 665-668.
- [15] Herzog J C. The Diffie-Hellman key-agreement scheme in the strand space model [C]//Proceedings of the 16th IEEE computer security foundations workshop. Pacific, Grove: IEEE Computer Society, 2001, (3): 234-247.

作者简介:

肖跃雷 男, (1979-), 博士后, 副教授. 研究方向为可信计算、安全协议分析与设计、无线网络安全、大数据安全、数据分析与挖掘等. E-mail: xiao_yuelei@163.com.

武君胜 男, (1962-), 博士, 教授. 研究方向为计算方法、科学计算可视化、软件工程等.

朱志祥 男, (1967-), 博士, 教授. 研究方向为网络与信息安全、信息技术和信息化等.