

一种改进的 IKEv2 协议及其形式化验证^{*}

韩明奎, 潘 进, 李 波

(西安通信学院, 西安 710106)

摘 要: 针对 IKEv2 协议在系统开销和发起方身份保护方面的不足, 提出了一种改进协议的方案。新的协议采用基于超椭圆曲线的 Weil 对技术进行数字签名认证, 并且首先认证响应方身份。通过该方案, 改进后的协议降低了系统开销, 实现了对发起方身份的主动保护。最后, 基于应用 π 演算的方法对协议进行了建模, 并定义和分析了协议的安全属性。结果表明, 改进后的协议具有更好的安全性和实用性。

关键词: IKEv2 协议; 身份保护; Weil 对; 应用 π 演算

中图分类号: TP393.08

文献标志码: A

文章编号: 1001-3695(2010)02-0707-05

doi:10.3969/j.issn.1001-3695.2010.02.084

Improved IKEv2 protocol and its formal verification

HAN Ming-kui, PAN Jin, LI Bo

(Xi'an Communications Institute, Xi'an 710106, China)

Abstract: IKEv2 protocol had some flaw in protecting initiator's identity and system requirement, so this paper presented an improved protocol. In the new protocol, used Weil pairing technology, based on hyperelliptic curves, in digital signature authentication, and first authenticated the responder. By those means, the protocol had reduced the system cost and actively protected the initiator's identity. At last, formally analyzed the improved protocol's security property based on applied π calculus. Analysis result shows that the protocol has a better performance in secure and application.

Key words: IKEv2 protocol; identity protection; Weil pairing; applied π calculus

由于 Internet 密钥交换协议 IKEv1^[1] 标准过于复杂、协商效率低、容易受到 DoS 攻击和中间人攻击^[2], IETF 工作组推出了 IKEv2^[3] 协议用于替代 IKEv1。新版本的协议提供了两种认证方式, 即预共享密钥认证和数字签名认证。但这两种认证方式都存在问题。文献[4]指出预共享密钥认证方式存在无法大规模应用、暴力字典破解等问题。文献[5]通过频繁更换预共享密钥的方法抵御离线字典攻击。文献[6]通过修改密钥生成算法解决预共享密钥认证的中间人攻击问题。文献[7]指出数字签名认证依赖于公钥基础设施 PKI, 并且传输、维护、保存、验证证书等造成的巨大开销使该方式不适于实时和低带宽等情况。同时, 两种认证方式都不能保护相对重要的发起方的身份^[8]。作为互联网关键的安全技术之一, 对 IKEv2 协议进行分析和改进有着非常重要的意义。

文献[9,10]提出了一些保护发起方身份的方案, 但不够理想。本文通过基于身份认证的公钥密码体制提出了一个新的改进方案。基于身份认证的公钥密码体制思想最早由文献[11]提出, 在该体制中公钥由用户的身份信息获得, 私钥由可信第三方生成。基于该思想, 相继提出了多个实现方案, 但实用性均不强。2001 年, 文献[12]提出的基于超椭圆曲线的 Weil 对技术是第一个公认有效的方案。本文基于 Weil 对技术改进了 IKEv2 协议, 并且基于应用 π 演算^[13~15] 的方法对改进后协议的安全属性进行了证明。分析结果表明, 在无须部署 PKI 的情况下, 新的协议是安全的, 并且能够保护发起方的身份。

1 IKEv2 协议及其分析

1.1 IKEv2 协议介绍

首先对标志符进行说明。 I 和 R 分别代表发起方和响应方; HDR 为 IKE 消息头部, 用于标志当前会话; SA 为安全关联, 用来协商安全参数; KE 为用于进行 DH(Diffie-Hellman)交换的公共参数; N 为随机数 nonce, 保证密钥和消息的新鲜性; ID 为协议参与方的身份; AUTH 为认证载荷, 用于身份认证和消息完整性保护; CERT/CERTREQ 为证书/证书请求; TS 为流量选择载荷; $sk\{\}$ 表示对内容进行加密和完整性保护。

IKEv2 初始交换协议由四条消息组成, 前两条消息被称做 IKE_SA_INIT 交换, 主要进行密钥算法的协商、nonce 以及 DH 交换, 从而生成用于加密和验证后续交换的密钥材料。后两条消息被称做 IKE_AUTH 交换, 实现对前两条消息的验证, 同时交换身份和证书信息, 并建立第一个 IPSec SA, 除消息头外, IKE_AUTH 交换中的消息都用前面生成的密钥材料进行了加密和完整性保护。当检测到 DoS 攻击时, 增加两条包含 cookie 的消息。协议描述如下:

- 1 $I \rightarrow R$: HDR, SA_{i1} , KE_i , N_i
- 2 $R \rightarrow I$: HDR, SA_{r1} , KE_r , N_r , [CERTREQ]
- 3 $I \rightarrow R$: HDR, $sk\{ID_i, [CERT], [CERTREQ], AUTH, SA_{i2}, TS_i, TS_r\}$
- 4 $R \rightarrow I$: HDR, $sk\{ID_r, [CERT], AUTH, SA_{r2}, TS_i, TS_r\}$

1.2 协议分析

文献[8]指出 Internet 用户(特别是移动 IP 用户)的身份

收稿日期: 2009-06-25; 修回日期: 2009-07-27 基金项目: 国家“863”计划资助项目(2007AA01Z472)

作者简介: 韩明奎(1985-), 男, 河南南阳人, 硕士研究生, 主要研究方向为网络安全(hmktwt@126.com); 潘进(1959-), 男, 教授, 博导, 博士, 主要研究方向为网络安全、信号处理; 李波(1985-), 男, 硕士研究生, 主要研究方向为密码算法。

及位置信息的保密性尤为重要,所以协议应当对发起方提供主动身份保护,然而协议对发起方只提供了被动身份保护。本文采用应用 π 演算与协议分析工具 ProVerif^[16] 相结合的方法验证了文献[9,10]指出的问题。下面过程给出了 ProVerif 输出的攻击者 P 得到发起方 I 身份的过程: I 向 R 发送第一条消息请求建立 SA ,攻击者 P 截获消息并冒充 R 与 I 进行交互。 $P(R)$ 表示攻击者冒充响应方 R , a_1, a_2, a_3 是攻击者生成的符合载荷格式的数据。攻击步骤 4 是指 P 得到包含 I 身份的消息 3 后不再响应或认证失败等导致的协商中断。由于 P 和 I 建立了共享密钥,可以解密消息 3,得到 I 的身份 ID_i 。

- 1 $I \rightarrow R: HDR, SA_{i1}, KE_i, N_i$
- 2 $I \rightarrow P(R): HDR, SA_{i1}, KE_i, N_i$
- 3 $P(R) \rightarrow I: HDR, a_1, a_2, a_3$
- 4 $I \rightarrow P(R): HDR, sk \mid ID_i, AUTH, SA_{i2}, TS_i, TS_r \}$
- 5 交换中断

此外,协议在应用方面存在问题。在 IKEv2 协议的预共享密钥认证方式中,任何两个通信实体之间都要共享一个密钥的要求导致密钥数量会随着通信实体的增加而剧增(如 n 个通信实体需要 $n \times (n-1)/2$ 个密钥)。数字签名认证的前提是部署公钥基础设施 PKI,认证中心 CA 不仅要为通信实体签发证书,还要在网络中维护 PKI;通信实体间证书的传递会导致带宽需求增大,存储对方的证书则需要较大存储空间^[17]。因此,提供一种低开销的数字签名认证方案具有很好的应用价值。

2 基于 Weil 对改进的 IKEv2 协议设计

2.1 Weil 对技术

设 G_1, G_2 分别是阶为 q 的加法循环群和乘法循环群。其中 q 是大素数,且在 G_1, G_2 中离散对数问题都是难解的。设 $\hat{e}$ 是 $G_1 \times G_1 \rightarrow G_2$ 的双线性映射,满足如下性质:

a) 双线性。对任意 $P, Q \in G_1$, 所有 $a, b \in \mathbb{Z}^+$, 满足 $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$; 同时, 对任意 $P_1, P_2, Q \in G_1$, 有 $\hat{e}(P_1 + P_2, Q) = \hat{e}(P_1, Q) \times \hat{e}(P_2, Q)$ 。

b) 非退化性。若 P 是 G_1 的生成元, 则 $\hat{e}(P, P) \in G_2$ 是 G_2 的生成元。

c) 可计算性。存在一个高效的算法计算 $\hat{e}(P, Q), P, Q \in G_1$ 。

通常 G_1 取为有限域 Fe 上的椭圆曲线有理点群的一个加法子群, G_2 取为这个有限域的扩域上的一个乘法子群, 双线性映射 $\hat{e}$ 由椭圆曲线上的 Weil 配对派生得到。 H_1, H_2 是公开的加密用哈希函数, $H_1: \{0, 1\}^* \rightarrow G_1, H_2: \{0, 1\}^* \times G_2 \rightarrow F_q$ 。

构建可信第三方: 私钥生成中心 (private key generator, PKG), PKG 随机选择一个生成元 $P \in G_1$ 和一个整数 $s \in F_p$ 。计算 $Q_a = sP$, 公开 (P, Q_a) , 保密 s 作为系统主密钥。对任一客户端 C , PKG 在验证了用户的身份后计算并安全分发用户的私钥。设 C 的身份由字符串 ID 给出, 则 C 的公钥 $Q_c = H_1(ID)$, 私钥 $S_c = sQ_c$, 密钥对为 (Q_c, S_c) 。

2.2 基于 Weil 对改进的 IKEv2 协议

针对 1.2 节中指出的问题, 本文改进了协议的初始交换部分。一方面, 由于 Weil 对技术实现了基于身份的公钥密码体制, 可以把 Weil 对技术用于 IKEv2 协议的数字签名认证。 I, R

在获得对方身份 ID 之后即可计算其公钥并对签名进行认证, 无须在协议信息中请求和发送证书, 也就不必部署 PKI。另一方面, 为了保证协议的灵活性, 改进后的 IKEv2 协议保留了预共享密钥认证方式, 协议双方可以在 SA 提议中指出具体的认证方式。改进后协议的框架、载荷类型、标志符等与 RFC4306 中定义保持一致, 如下所示:

- 1' $I \rightarrow R: HDR, SA_{i1}, KE_i, N_i$
- 2' $R \rightarrow I: HDR, SA_{r1}, KE_r, N_r, sk \mid ID_r, AUTH_r \}$
- 3' $I \rightarrow R: HDR, sk \mid ID_i, ID_r, AUTH_i, SA_{i2}, TS_i, TS_r \}$
- 4' $R \rightarrow I: HDR, sk \mid ID_i, ID_r, SA_{r2}, TS_i, TS_r \}$

改进后的 IKEv2 初始交换协议由四条消息组成, 为了区别于原有消息记为消息 i' 。当检测到 DoS 攻击时, 采用 cookie 机制增加两条消息。

消息 1': 发起方 I 发起建立连接的请求, 向响应方 R 发送安全关联 SA 提议、 DH 交换值、保证密钥新鲜性和防重放攻击的随机值 N_i 。

消息 2': 响应方 R 选择一个 SA 提议, 并将自己的 DH 交换值、随机值 N_r 以及加密后的身份信息 ID_r 和认证载荷 $AUTH$ 一起发送给发起方 I 。

消息 3': 在验证了响应方的认证载荷之后, I 向 R 发送用于 IPSec SA 的提议, 同时包括自己的身份信息和证明、对方的身份信息以及流量选择符。

消息 4': R 选择一个提议, 并响应 I 的认证消息, 完成初始交互。

采用数字签名认证方式时, 公钥由用户的身份信息 ID 确定, 私钥由 PKG 生成。密钥衍生和认证载荷的计算分别满足式(1)~(4)。 $S\{\}$ 表示使用私钥对内容进行签名。

数字签名方式的密钥衍生满足如下公式:

$$KEYSEED = \text{prf}(N_i \mid N_r, g \mid r) \quad (1)$$

$$\{SK_d \mid SK_ai \mid SK_ar \mid SK_ei \mid SK_er \mid SK_pi \mid SK_pr\} = \text{prf} + (KEYSEED, N_i \mid N_r \mid SPI_i \mid SPI_r) \quad (2)$$

数字签名方式认证载荷的计算满足如下式:

$$AUTH_r = S\{HDR, SA_{r1}, KE_r, N_r, N_i, \text{prf}(SK_pr, ID_r)\} \quad (3)$$

$$AUTH_i = S\{HDR, SA_{i1}, KE_i, N_i, N_r, \text{prf}(SK_pi, ID_i)\} \quad (4)$$

采用预共享密钥认证方式时, 将预共享密钥值散列后参与种子密钥的衍生, 可以抵御中间人攻击、提供发起方身份的主动保护。该认证方式下的密钥衍生和认证载荷的计算满足式(2)和(5)~(7)。

预共享密钥方式的密钥衍生满足下式:

$$KEYSEED = \text{prf}(N_i \mid N_r \mid \text{prf}(\text{shared secret}, "Key Pad for IKEv2"), g \mid r) \quad (5)$$

预共享密钥方式认证载荷的计算满足下式:

$$AUTH_r = \text{prf}(\text{prf}(\text{shared secret}, "Key Pad for IKEv2"), (HDR, SA_{r1}, KE_r, N_r, N_i, \text{prf}(SK_pr, ID_r))) \quad (6)$$

$$AUTH_i = \text{prf}(\text{prf}(\text{shared secret}, "Key Pad for IKEv2"), (HDR, SA_{i1}, KE_i, N_i, N_r, \text{prf}(SK_pi, ID_i))) \quad (7)$$

3 基于应用 π 演算的安全协议证明

基于应用 π 演算分析协议的安全属性是一种新的形式化方法。应用 π 演算是交互、并发系统的理论模型, 提供了相关的概念框架和数学工具, 用于建模、描述系统, 并推导系统的安全性质。基于应用 π 演算的形式化分析方法适合分析并发、分布式的协议, 具有简洁高效的特点^[18,19]。

3.1 应用 pi 演算

3.1.1 应用 pi 演算的语法语义

定义 Σ 为有限函数集合,给定一个 Σ ,应用 pi 演算的项定义如下:

$$L, M, N ::= n \mid x \mid f(M_1, M_2, \dots, M_l) \quad f \in \Sigma$$

其中: n 表示名, x 表示变量, $f(M_1, M_2, \dots, M_l)$ 表示函数项, l 是函数 f 的项数。

应用 pi 演算的普通进程定义如下:

$$P, Q, R ::= 0 \mid P \mid Q \mid !P \mid (vn).P \mid \text{if } M = N \text{ then } P$$

$$\text{else } Q \mid c(x) \bar{c} \langle M \rangle . P$$

其中: 0 表示空进程, $P \mid Q$ 表示并发复合, $!P$ 表示复制, $(vn).P$ 表示范围受限, $\text{if } M = N \text{ then } P \text{ else } Q$ 表示条件, $c(x).P$ 表示输入, $\bar{c} \langle M \rangle . P$ 表示输出。

普通进程增加主动替换 (active substitution) 原语, 可以被扩展为扩展进程。定义如下:

$$A, B, C ::= P \mid A \mid B \mid (vn).A \mid (vx).A \mid M/x$$

其中: P 表示普通进程, $A \mid B$ 表示并发复合, $(vn).A$ 表示名受限, $(vx).A$ 表示变量受限, M/x 表示主动替换。

应用 pi 演算的语义包括用于函数约简的等式理论, 以及扩展进程间的结构等价、内部约简关系等。等式理论是符号集合 Σ 中项集合上的等价关系, 且其在主动替换的条件下封闭; 结构等价“ $\equiv$ ”在名、变量的 α 转换以及评价上下文下封闭; 内部约简用“ $\rightarrow$ ”表示, 是封闭扩展进程集合上最小关系, 并在结构等价, 评价上下文下封闭; 标记操作语义用于进程和与其交互的环境行为的推理。

3.1.2 应用 pi 演算的等价关系

应用 pi 演算使用上下文代表主动攻击者, 上下文不能区分的两个进程满足观察等价, 表示攻击者不能区分进程内容的不同。这一节主要介绍应用 pi 演算的观察等价、框架的静态等价、标记等价, 并说明标记等价与观察等价的一致性, 从而得到证明进程等价的简便方法。

在定义观察等价之前, 需要定义表示进程在通道上可观察的谓词 $\Downarrow$ 。若扩展进程 A 能够在通道 a 上发送消息则称扩展进程 A 在通道 a 上可观察, 记做 $A \Downarrow a$, 即对不限制 a 的上下文有: $A \rightarrow^* C[\bar{a} \langle m \rangle . P]$ 。

定义 1 观察等价 $\approx_o$ 。

观察等价是具有相同域 (domain) 的扩展进程间最大的对称关系, 且 $A R B$ 满足:

- 1) 若 $A \Downarrow a$, 则 $B \Downarrow a$;
- 2) 若 $A \rightarrow^* A'$, 则 $B \rightarrow^* B'$, 且对 $B', A' R B'$ 成立;
- 3) 对所有封闭的评价上下文 $C[_]$, 有 $C[A] R C[B]$ 。

静态等价 ($\approx_s$) 表示两个进程的任何框架不能被任何其他进程所区分。下面给出框架、框架相等的定义, 以便形式化地描述静态等价。框架是一个由 0 和形式如 $\{M/x\}$ 的主动替换通过并发组合或/和限制算子构成的扩展进程, 用 φ 或 ψ 表示; 框架的导出变量是框架在主动替换 $\{M/x\}$ 中而不在限制算子中的变量 x ; $\text{dom}(\varphi)$ 是框架 φ 的域, 是框架 φ 导出变量的集合。

定义 2 项在框架中的相等。

项 M 和 N 在框架 φ 中相等, 记做 $(M = N)_\varphi$, 当且仅当 $\varphi \equiv \bar{vn}.\sigma$, 有 $M\sigma = N\sigma$ 成立, 且对名 $\bar{n}$ 和替换 σ 有 $\{\bar{n}\} \cap (\text{fn}(M) \cup$

$\text{fn}(N)) = \emptyset$ 。

定义 3 框架静态等价。

称封闭框架 φ 和 ψ 静态等价, 记做 $\varphi \approx_s \psi$, 若

- 1) $\text{dom}(\varphi) = \text{dom}(\psi)$;
- 2) 对所有的项 M 和 N 有 $(M = N)_\varphi \Leftrightarrow (M = N)_\psi$ 。

若扩展进程 A, B 的框架满足静态等价, 则它们满足静态等价, 记做 $A \approx_s B$ 。

定义 4 标记互模拟 (labeled bisimulation)。

标记互模拟 $\approx_l$ 是封闭扩展进程集合上最大的对称关系

$R, A R B$ 蕴涵:

- 1) $A \approx_s B$;
- 2) 若 $A \rightarrow^* A'$ 则有 $B \rightarrow^* B'$, 且 $A' R B'$;
- 3) $A \xrightarrow{a} A'$, 其中: $\text{fv}(a) \subseteq \text{dom}(A)$, $\text{bn}(a) \cap \text{fn}(B) = \emptyset$; 则有 B 满足 $B \rightarrow^* B'$, 且 $A' R B'$ 。

标记互模拟满足下面的性质:

定理 1 观察等价是 (is) 标记互模拟, 即 $\approx = \approx_l$ 。

$\approx_l$ 在封闭的评价上下文下封闭, 同时由于 $\approx_l$ 的证明中不包括关于上下文的条件, 标记互模拟的证明比观察等价的证明简单。进程的观察等价一般通过标记互模拟来证明。

3.2 基于应用 pi 演算的协议模型

在协议的形式化描述中, 需要定义它的项如表 1 所示。

表 1 协议的项

$M, T, U, V; :=$	项
$I, R, x_1, x_2, \dots$	变量
$N_i, N_r, sa, TS, c, \dots$	名
$f(U_1, U_2, \dots, U_l)$	函数 $f \in \Sigma$

其中: 函数集 Σ 包括了以下三种类型的函数:

a) 密码相关的函数。 $H_1(x_1)$ 表示公钥生成函数; $H_2(x_1, x_2)$ 表示私钥生成函数; $H\{K\}(x)$ 表示含密钥的单向散列函数; $pk(x)$ 表示公钥; $sk(x)$ 表示私钥; $E\{K\}(x)$ 表示共享密钥加密; $D\{K\}(x)$ 表示共享密钥解密; $S\{sk\}(x)$ 表示私钥签名; $\text{checksign}\{pk\}(x_1, x_2)$ 表示使用公钥验证签名。

b) 消息构造函数。IKEv2 的消息载荷有固定的格式, 四条消息可以定义为 $\text{cons}_1(x_1, x_2, x_3, x_4)$ 、 $\text{cons}_2(x_1, x_2, x_3, x_4, x_5, x_6)$ 、 $\text{cons}_3(x_1, x_2, x_3)$ 、 $\text{cons}_4(x_1, x_2, x_3)$ 。

c) 投影函数。该函数就是选择构造消息函数中的第 j 个消息。包括 $\text{cons}_1.j(\text{cons}_1(x_1, x_2, x_3, x_4))$ 、 $\text{cons}_2.j(\text{cons}_2(x_1, x_2, x_3, x_4, x_5, x_6))$ 、 $\text{cons}_3.j(\text{cons}_3(x_1, x_2, x_3))$ 、 $\text{cons}_4.j(\text{cons}_4(x_1, x_2, x_3))$ 。

由上述函数, 本文定义如下项的代数相等关系:

$$D\{k\} \mid (E\{k\}(x)) = x$$

$$\text{checksign}\{pk(k)\} \mid (S\{sk(k)\}(x), x) = \text{true}$$

$$\text{Tuple}.j(\text{Tuple}(x_1, \dots, x_i)) = x_j \text{ for } j < i, \text{ Tuple} \in \{\text{cons}_1, \text{cons}_2, \text{cons}_3, \text{cons}_4\}$$

在以上定义的项和函数相等关系的基础上, 建立如下协议模型。 I 代表发起方进程, R 代表响应方进程, I, R 共同构成系统进程 S 。

$I = ! \text{init}(sa_{i1}, sa_{i2}). \text{key}_i(sk_i). v \ d_i. v \ N_i. \bar{c} \langle \text{cons}_1(\text{HDR}, sa_{i1}, KE_i, N_i) \rangle. c(\text{cons}_2(\text{HDR}, sa_{r1}, KE_r, N_r, e_{r1}, h_{r1})). \text{let } K_r \text{ in if } h_{r1} = H\{K_{ar}\}(\tau, e_{r1}) \text{ then let } \{ID_r, AUTH_r\} = D\{K_{er}\}(e_{r1}) \text{ in let } ID_r' = H\{K_{pr}\}(ID_r) \text{ in let } PK_r = H_1(ID_r) \text{ in if } \text{checksign}\{PK_r\}(AUTH_r, (\text{HDR}, sa_{r1}, KE_r, N_r, N_i, ID_r')) = \text{true then let } ID_i' = H\{K_{pi}\}(ID_i) \text{ in let AU-}$

$TH_i = S \{ sk_i \} (HDR, sa_{i1}, KE_i, N_i, N_r, ID_i')$ in let $e_i = E \{ K_{ei} \} (ID_i, ID_r, sa_{i2}, AUTH_i, TS_i, TS_r)$ in let $h_i = H \{ K_{ai} \} (i, e_i)$ in $\bar{c} \langle \text{cons}_3 (HDR, e_i, h_i) \rangle \cdot c \langle \text{cons}_4 (HDR, e_{i2}, h_{i2}) \rangle$. if $h_{i2} = H \{ K_{ar} \} (r, e_{r2})$ then let $(= ID_i, = ID_r, sa_{i2}, TS_i, TS_r) = D \{ K_{er} \} (e_{r2})$ in connect $(ID_i, ID_r, sa_{i2}, sa_{r2}, K_d)$
 $R = \text{key}_r (sk_r) \cdot c \langle \text{cons}_1 (HDR, sa_{i1}, KE_i, N_i) \rangle \cdot v \text{dr} \cdot v N_r \cdot v sa_{r1}$. let K_R in let $ID_r' = H \{ K_{pr} \} (ID_r)$ in let $AUTH_r = S \{ sk_r \} (HDR, sa_{r1}, KE_r, N_r, N_i, ID_i')$ in let $e_{r1} = E \{ K_{er} \} (ID_r, AUTH_r)$ in let $h_{r1} = H \{ K_{ar} \} (r, e_{r1})$ in $\bar{c} \langle \text{cons}_2 (HDR, sa_{r1}, KE_r, N_r, e_{r1}, h_{r1}) \rangle \cdot c \langle \text{cons}_3 (HDR, e_i, h_i) \rangle$. if $H \{ K_{ai} \} (i, e_i) = h_i$ then let $(ID_i, = ID_r, sa_{i2}, AUTH_i, TS_i, TS_r) = D \{ K_{ei} \} (e_i)$ in let $ID_i' = H \{ K_{pi} \} (ID_i)$ in let $PK_i = H_1 (ID_i)$ in if check-sign $\{ PK_i \} (e_i, (HDR, sa_{i1}, KE_i, N_i, N_r, ID_i')) = \text{true}$ then $v sa_{i2}$. accept $\langle ID_i, ID_r, sa_{i2}, sa_{r2}, K_d \rangle$. let $e_{r2} = E \{ K_{er} \} (ID_i, ID_r, sa_{i2}, TS_i, TS_r)$ in let $h_{r2} = H \{ K_{ar} \} (r, e_{r2})$ in $\bar{c} \langle \text{cons}_4 (HDR, e_{r2}, h_{r2}) \rangle$
 $S = (v ID_i) (v ID_r) (v s, \text{let } pk_i = H_1 (ID_i) \text{ in let } pk(i) = pk_i \text{ in let } sk_i = H_2 (s, pk_i) \text{ in let } sk(i) = sk_i \text{ in } \text{key}_i \langle sk_i \rangle \cdot \text{let } pk_r = H_1 (ID_r) \text{ in let } pk(r) = pk_r \text{ in let } sk_r = H_2 (s, pk_r) \text{ in let } sk(r) = sk_r \text{ in } \text{key}_r \langle sk_r \rangle) \mid I \mid R$

其中,发起方的密钥值为

$$K_I = \prod_u = Kai, Kei, Kpi, Kar, Ker, Kpr, Kd \{ K_u = H \{ KE_r \} \tilde{d}_i \} (N_i, N_r, u)$$

响应方的密钥值为

$$K_R = \prod_u = Kai, Kei, Kpi, Kar, Ker, Kpr, Kd \{ K_u = H \{ KE_i \} \tilde{d}_r \} (N_i, N_r, u)$$

通道 init、connect、accept 代表协议与主机交互的隐藏信道,环境无法与这些信道进行交互。通道 key_i、key_r 是用来建模私钥生成中心 PKG 与客户端之间传递私钥的安全信道,攻击者不能得到通道内的内容。

3.3 安全属性的形式化验证

本文采用观察等价^[20]和对应性断言^[21]等方法形式化地证明了协议的私密性、认证性和身份保护。部分形式化分析工作是在 ProVerif 的辅助下完成^[22]。

首先考虑私密性。IKEv2 协议用于为 IPSec 协商安全关联、建立共享密钥等参数,当环境无法区分 IKEv2 协商出的不同参数时,说明协议实现了对内容的保护,即满足私密性。因此,有如下定理:

定理 2 协议的私密性。对于攻击者,如果有

$$S(ID_i, ID_r, sa_{i2}, sa_{r2}, K_d) \approx S(ID_i, ID_r, \underline{sa_{i2}}, \underline{sa_{r2}}, K_d)$$

则说明协议满足私密性。记 R 为这两个进程间的最大对称关系。

证明 由协议模型可以定义如下框架:

定义 $\varphi(S(ID_i, ID_r, sa_{i2}, sa_{r2}, K_d))$ 为

$$\{x_1 = (HDR, sa_{i1}, KE_i, N_i)$$

$$\mid x_2 = (HDR, sa_{r1}, KE_r, N_r, E \{ K_{er} \} (ID_r, S \{ sk_r \} (HDR, sa_{r1}, KE_r, N_r, N_i, ID_r')), h_{r1})$$

$$\mid x_3 = (HDR, E \{ K_{ei} \} (ID_i, ID_r, sa_{i2}, S \{ sk_i \} (HDR, sa_{i1}, KE_i, N_i, N_r, ID_i')), TS_i, TS_r), h_i)$$

$$\mid x_4 = (HDR, E \{ K_{er} \} (ID_i, ID_r, sa_{i2}, TS_i, TS_r), h_{i2}) \}$$

定义 $\psi(S(ID_i, ID_r, \underline{sa_{i2}}, \underline{sa_{r2}}, K_d))$ 为

$$\{x_1 = (HDR, sa_{r1}, KE_r, N_r)$$

$$\mid x_2 = (HDR, sa_{i1}, KE_i, N_i, E \{ K_{er} \} (ID_r, S \{ sk_r \} (HDR, sa_{r1}, KE_r, N_r, N_i, ID_r')), h_{r1})$$

$$\mid x_3 = (HDR, E \{ K_{ei} \} (ID_i, ID_r, \underline{sa_{i2}}, S \{ sk_i \} (HDR, sa_{i1}, KE_i, N_i, N_r, ID_i')), TS_i, TS_r), h_i)$$

$$\mid x_4 = (HDR, E \{ K_{er} \} (ID_i, ID_r, \underline{sa_{i2}}, TS_i, TS_r), h_{i2}) \}$$

1) 很显然, $\text{dom}(\varphi) = \text{dom}(\psi)$ 在假设 DH 交换安全的前提下,受密钥保护的安全参数对攻击者而言是不可观察的。根据定义 3 可知: $\varphi \approx_s \psi, S(ID_i, ID_r, sa_{i2}, sa_{r2}, K_d) \approx_s S(ID_i, ID_r, \underline{sa_{i2}}, \underline{sa_{r2}}, K_d)$, 则 $RC \approx_s$ 。

2) 两个进程具有相同的模型,则对于进程 $S(ID_i, ID_r, sa_{i2}, sa_{r2}, K_d)$ 的任意内部动作 τ 和外部动作 α ,进程 $S(ID_i, ID_r, \underline{sa_{i2}}, \underline{sa_{r2}}, K_d)$ 能够做相同的动作,并保持一致的结果。

以上分析表明,进程 $S(ID_i, ID_r, sa_{i2}, sa_{r2}, K_d)$ 、 $S(ID_i, ID_r, \underline{sa_{i2}}, \underline{sa_{r2}}, K_d)$ 满足定义 4,即 $S(ID_i, ID_r, sa_{i2}, sa_{r2}, K_d) \approx_i S(ID_i, ID_r, \underline{sa_{i2}}, \underline{sa_{r2}}, K_d)$ 。由定理 1 可得两个进程满足观察等价,即 $RC \approx$ 。表示发起方和响应方之间协商的信息能够受到有效的保护,攻击者无法获得安全参数。

采用同样的方法可以证明 $S(ID_i, ID_r, sa_{i2}, sa_{r2}, K_d) \approx S(ID_i, ID_r, \underline{sa_{i2}}, \underline{sa_{r2}}, K_d)$,表示攻击者不能区分不同的发起方与同一响应方建立的不同的安全参数。当攻击者采用中间人攻击的方法时,由于获得了响应方身份 ID_r ,则 $S(ID_i, ID_r, sa_{i2}, sa_{r2}, K_d) \neq S(\underline{ID_i}, \underline{ID_r}, \underline{sa_{i2}}, \underline{sa_{r2}}, K_d)$ 。但是,中间人攻击所伪造的消息由于无法通过验证而导致协商失败,双方不建立任何安全参数,不会对系统安全造成影响。改进后的协议具有私密性,能够实现对安全信息的保护。

发起方 I 和响应方 R 的身份是以密文的形式在信道中传递,因此身份保护是协议私密性的拓展。对身份保护的验证可被建模为安全属性查询:攻击者能否获得加密后消息中的内容 ID_i 和 ID_r 。该验证是在自动化工具 ProVerif 的辅助下完成,查询以下事实是否成立。输出结果表明,改进后的协议能够实现对发起方的身份的主动保护;实现对响应方身份的被动保护。

query attacker: ID_i

query attacker: ID_r

定理 3 协议的认证性。对任意迹 $S \xrightarrow{\eta} S', \eta$ 满足条件:

a) R 对 I 的认证性。如果在 η 中存在

$$\text{accept} \langle ID_i, ID_r, sa_{i2}, sa_{r2}, K_d \rangle$$

则在此项之前, η 中必定存在

$$\text{init}(sa_{i1}, sa_{i2}) \text{ and}$$

$$\text{checksign} \{ PK_i \} (e_i, (HDR, sa_{i1}, KE_i, N_i, N_r, ID_i')) = \text{true}$$

b) I 对 R 的认证性。如果在 η 中存在

$$\text{connect} \langle ID_i, ID_r, sa_{i2}, sa_{r2}, K_d \rangle$$

则在此项之前, η 中必定存在

$$\text{accept} \langle ID_i, ID_r, sa_{i2}, sa_{r2}, K_d \rangle \text{ and}$$

$$\text{checksign} \{ PK_r \} (AUTH_r, (HDR, sa_{r1}, KE_r, N_r, N_i, ID_r')) = \text{true}$$

证明 可以用对应性断言 (correspondence assertion) 解释和证明这个定理。 R 对 I 的认证性:如果响应方接收了协商出的安全参数,则发起方必定发起了该协商,并且所声称的身份是真实的; I 对 R 的认证性:如果发起方基于协商出的安全参数建立了安全连接,则响应方已接收协商出的安全参数,并且所声称的身份是真实的。

该定理的证明通过自动化工具 ProVerif 完成。在完成协议模型脚本代码的基础上,查询 (query) 模型是否满足以下对应性断言。输出结果表明协议满足认证性。

$$ev; \text{accept} \langle X_1, X_2, X_3, X_4, X_5 \rangle \Rightarrow (ev; R\text{checksign}I(\text{true}) \Rightarrow ev; \text{init} \langle X_1, X_2 \rangle)$$

$$ev; \text{connect} \langle X_1, X_2, X_3, X_4, X_5 \rangle \Rightarrow (ev; \text{accept} \langle X_1, X_2, X_3, X_4, X_5 \rangle \Rightarrow$$

$ev: IchecksignR(true)$

4 结束语

针对 IKEv2 协议的不足,本文将基于身份认证的公钥密码体制,即 Weil 对技术用于数字签名认证并改进了初始交换协议。改进后的协议降低了系统开销,能够更好地满足实时性和低带宽等条件下的应用。同时,基于应用 π 演算的方法形式化地验证了新协议的安全属性。结果表明改进后的协议满足私密性和认证性,并能够实现对发起方身份的主动保护。因此改进后的协议具有更好的安全性和实用性。

参考文献:

- [1] HARKINS D, CARREL D. RFC 2409, The Internet key exchange (IKE) [S]. United States: RFC Editor, 1998.
- [2] HANDLY M, GREENHALGH A. Steps towards a DoS resistant Internet architecture [C]//Proc of ACM SIFCOMM Workshop on future Directions in Network Architecture. Portland: ACM Press, 2004: 49-56.
- [3] KAUFMAN C. RFC 4306, Internet key exchange (IKEv2) protocol [S]. Washington: IETF, 2005.
- [4] STEVEN M, BELLOVIN, MICHAEL M. Encrypted key exchange: password-based protocols secure against dictionary attacks [C]//Proc of IEEE Symposium on Research in Security and Privacy. Oakland: IEEE Computer Society, 1992: 72-84.
- [5] RAED B H. Enhancing the IKE pre-shared key authentication method [D]. Missouri: Graduate School, University of Missouri-Columbia, 2006.
- [6] 张朝东,徐明伟. 密钥交换协议 IKEv2 的分析与改进 [J]. 清华大学学报:自然科学版,2006,46(7):1274-1277.
- [7] 刘文红. 下一代互联网服务保证关键技术研究 [D]. 北京:北京交通大学,2007.
- [8] 曹春杰,张帆,马建峰. 可证安全的 Internet 密钥交换协议 [J]. 武汉大学学报:理学版,2006,52(5):545-549.
- [9] 沈海峰,薛锐,黄河燕. IKEv2 协议的安全性分析 [J]. 计算机科学,2005,32(11): 59-63.
- [10] 吴昌,肖美华. 基于 SPIN 的 IKEv2 协议高效模型检测 [J]. 计算机工程与应用,2008,44(5):158-161.
- [11] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Advances in Cryptology- Crypto '84, LNCS 196. 1985. Berlin: Springer-Verlag, 1985: 47-53.
- [12] BONEH D, FRANKLIN M. Identity based encryption from the Weil pairings [C]//Advances in Cryptology- Crypto 2001, LNCS 2139. Berlin: Springer-Verlag, 2001: 213-229.
- [13] ABADI M, FOURNET C. Mobile values, new names and secure communication [C]//Proc of the 28th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'01). London: ACM, 2001: 104-115.
- [14] MICHAEL B, CATALIN H, MATTEO M. Automated verification of remote electronic voting protocols in the applied Pi-calculus [C]//Proc of the 21st IEEE Computer Security Foundations Symposium (CSF). Pittsburgh: IEEE Press, 2008: 195-209.
- [15] ABADI M, BLANCHET B. Just fast keying in the pi calculus [J]. ACM Trans on Information and System Security (TISSEC), 2007,10(3):1-59.
- [16] ABADI M, BLANCHET B. Analyzing security protocols with secrecy types and logic programs [J]. Journal of the ACM (JACM), 2005, 52(1):102-146.
- [17] 拾以娟. 基于身份的公钥密码学关键问题研究 [D]. 上海:上海交通大学,2007.
- [18] 廖军,潭浩,刘锦德. 基于 Pi-演算的 Web 服务组合的描述和验证 [J]. 计算机学报,2005,28(4):635-643.
- [19] 袁禄来,曾国荪,王伟. 基于 Pi-演算的信任网络形式化建模 [J]. 系统仿真学报,2008,20(1):57-61.
- [20] BLANCHET B, ABADI M, FOURNET C. Automatic verification of selected equivalences for security protocols [J]. Journal of Logic and Algebraic Programming, 2008, 75(1): 3-51.
- [21] BLANCHET B, FOURNET C. Automatic verification of correspondences for security protocols [C]//Proc of the 20th Annual IEEE Symposium on Logic in Computer Science. Washington: IEEE Computer Society, 2005: 331-340.
- [22] 顾永眼,傅育熙,朱涵. 基于可达关系的安全协议保密性分析 [J]. 计算机学报,2007,30(2):255-261.

(上接第 706 页)水印算法,首先通过置乱,并使用复合混沌二值序列调制水印图案对其加密,增强了水印比特在载体图像分布的均匀性和保密性,然后对水印扩频处理。此外,根据小波系数集确定了量化步长,真正实现了盲嵌入和盲提取,并且充分利用集合中系数相对的不变性,减小了量化步长变化的不确定性。理论分析和实际结果验证了该水印算法具有很好的不可见性、鲁棒性和安全性,特别在抗 JPEG 压缩上算法表现出了较强的健壮性。

参考文献:

- [1] WU C F, HSIEH W S. Digital watermarking using zerotree of DCT [J]. IEEE Trans on Consumer Electronics, 2000, 46(1): 87-94.
- [2] KUTTER M, PETITCOLAS F. Fair evaluation methods for image watermarking system [J]. Journal of Electronic Imaging, 2000, 9(4): 445-455.
- [3] 黄松,张伟,陈军,等. 一个基于 DWT 的自适应数字水印算法 [J]. 计算机科学,2006,33(7):155-157.
- [4] 陈琼,吴祥生. 一种新颖的复合型盲水印算法 [J]. 中国图象图形学报, 2008, 13(3): 415-418.
- [5] FU Yu, WU Xiao-ping, CHEN Ze-mao, et al. A wavelet digital watermarking algorithm based on chaotic mapping [C]//Proc of International Symposium on Electronic Commerce and Security. [S. l.]: IEEE Press, 2008: 886-889.
- [6] LISA M M, CHARLES G B, CHARLES T R. Spread spectrum image steganography [J]. IEEE Trans on Image Processing, 1999, 8(8): 1075-1083.
- [7] COX I J, KILIAN J, LEIGHTON T, et al. Secure spread spectrum watermarking for multimedia [J]. IEEE Trans on Image Processing, 1997, 6(12): 1673-1687.
- [8] 訾鸿,赵岩. 一种双混沌系统加密算法的设计与实现 [J]. 现代电子技术, 2008, 31(19): 88-91.
- [9] 张雪峰,范九伦. 改进的混沌序列产生方法 [J]. 计算机工程与设计, 2007, 28(3): 600-602.
- [10] 丁玮,齐东旭. 基于 Arnold 变换的数字图像置乱技术 [J]. 计算机辅助设计与图形学学报, 2001, 13(4): 338-341.