文章编号:1001 - 9081(2006)09 - 2116 - 05

一种改进的 Woo-Lam 密码协议模型

赵 宇,袁 霖,王亚弟,韩继红
(信息工程大学 电子技术学院,河南 郑州 450004)
(zhaoyn83@ hotmail. com)

摘 要:提出了一种改进的 Woo-Lam 密码协议模型,即 eWoo-Lam 模型。与 Woo-Lam 模型相比,新模型具有以下特点:增强了模型中关于密码学原语操作的描述语法,使得对密码协议主体行为的描述更加精确,提高了模型在检测协议攻击方面的能力;引入了匹配运算机制,保障了模型安全性证明的有效性;提出了七条形式化准则,规范了模型的抽象过程;扩充了模型基于状态迁移的形式语义,使其更加精确合理;重新给出了模型安全性的形式定义,使其更具一般性。

关键词:密码协议模型;语法;形式化语义;安全特性
中图分类号:TP309.07 **文献标识码**:A

Improved Woo-Lam model for cryptographic protocols

ZHAO Yu, YUAN Lin, WANG Ya-di, HAN Ji-hong
(*College of Electronic Technology, Information Engineering University, Zhengzhou Henan* 450004, *China*)

Abstract: An improved Woo-Lam Model for cryptographic protocols, namely eWoo-Lam Model was introduced. Compared with Woo-Lam Model, the new model has such advanced properties as follows: to enhance the syntax of the model for cryptographic primitives, which enables the model to specify the principal actions more precisely and detect the attacks on the protocol more efficiently; to bring in match mechanism, which guarantees the effectiveness for the security analysis of the model; to propose seven formalization principles to normalize the procedure for model abstraction; to extend the state-transition based semantics to make it more rational; to redefine the security properties of the model to make them more generic.

Key words: cryptographic protocol models; syntax; formal semantics; security property

0 引言

密码协议模型是对协议安全特性进行分析和验证的基础和依据,其优劣直接决定了密码协议分析的正确性和可靠性。Thomas Y. C. Woo 和 Simon S. Lam 在文献[6]中提出了一种针对认证协议的形式化语义模型,即 Woo-Lam 模型。在该模型中,Woo 和 Lam 采用自定义的语法和语义对密码协议进行了形式化的描述,定义了一个刻画认证协议执行过程的语义模型,并且首次采用全局状态和迁移来描述密码协议的正确性。但是,从数学的角度来讲,Woo-Lam 模型仍然不够严谨,其中所定义的一些概念是不够完善的[11];另一方面,Woo-Lam 模型中缺乏对解密和解签名等密码学原语的形式化描述,这在某种程度上可能会隐蔽掉密码协议中存在的一些潜在攻击[8]。除 Woo-Lam 模型之外,我们还对其他的一些典型密码协议形式化模型[2~4,7,10~21,23]进行了研究,如 BAN 类模型[2]、Athena 模型[10]、Brutus 模型[11]、NRL 模型[12]等,通过对这些模型的归纳分析,可以得知一个合理的密码协议形式化模型应当具备下述特点:(1)能够对密码协议中的各种原语操作进行精确的形式化描述;(2)具有合理可靠的可证明语义;(3)对密码协议安全特性的定义应当精确合理;(4)便于实现机械化。在以上研究工作的基础上,我们对 Woo-Lam 模型进行了适当改进,提出了一种新的模型,即 eWoo-Lam 模型,该模型在设计过程中重点考虑了上述要求,有效地解决了 Woo-Lam 模型所存在的问题。

1 背景知识

在 eWoo-Lam 模型中,置换和匹配是两种重要的运算机制,具体定义如下:

令 $\mathfrak{X}$ 表示变量的集合,$\mathfrak{F}_n$ 表示 n 元函数标记的集合。

定义 1 项集 $\mathfrak{T}$ 是按照下列规则生成的对象的最小集合:

(1) 若 $x \in \mathfrak{X}$,则 $x \in \mathfrak{T}$;

(2) 若 $t_1, t_2, \cdots, t_n \in \mathfrak{T}, f \in \mathfrak{F}_n$ 则 $f(t_1, t_2, \cdots, t_n) \in \mathfrak{T}$。

定义 2 置换算子 Θ 是从变量 $x_1, x_2, \cdots, x_n$ 到项 $t_1, t_2, \cdots, t_n$ 的绑定的有限集,记为 $\Theta = \{t_1/x_1, t_2/x_2, \cdots, t_n/x_n\}$。$\Theta$ 的结构化定义如下:

(1) 若 $t/x \in \Theta$,则 $\Theta x = t$;

(2) $\Theta f(t_1, t_2, \cdots, t_n) = f(\Theta t_1, \Theta t_2, \cdots, \Theta t_n)$。其中,$f$ 表示函数标记。

定义 3 匹配等式是一个形如 $t \ll t'$ 的合式公式。其中,t 与 t' 均是项。如果存在置换算子 σ,使得 $\sigma t = t'$,则称 σ 为匹配等式的解。匹配系统是一个由若干匹配等式所组成的合取公式。置换算子 σ 是匹配系统 P 的解,当且仅当置换算子 σ 是系统 P 中每个匹配等式的解。记无解的匹配系统为 Ω。图 1 中给出了 eWoo-Lam 模型中用于求解匹配等式的规则。

收稿日期:2006 - 03 - 29;**修订日期**:2006 - 06 - 06

作者简介:赵宇(1983 -),男,山东成武人,硕士研究生,主要研究方向:计算机网络安全、密码协议自动化验证; 袁霖(1981 -),男,河南商丘人,助教,硕士,主要研究方向:计算机网络安全、信息系统安全; 王亚弟(1953 -),男,甘肃兰州人,教授,博士生导师,主要研究方向:计算机网络安全、信息系统安全; 韩继红(1966 -),女,山西定襄人,副教授,主要研究方向:计算机网络安全、信息系统安全.

(S1)	$(f(t_1,t_2,\ldots,t_n)\ll f(t_1',t_2',\ldots,t_n'))\wedge P$	$\rightarrow(\wedge_{i\in\{1,2,\ldots,n\}}\ t_i\ll t_i')\wedge P$
(S2)	$(f(t_1,t_2,\ldots,t_n)\ll g(t_1',t_2',\ldots,t_n'))\wedge P$	$\rightarrow\Omega\mid_{f\neq g}$
(S3)	$(x\ll t)\wedge(x\ll t')\wedge P$	$\rightarrow\Omega\mid_{t\neq t'}$
(S4)	$(f(t_1,t_2,\ldots,t_n)\ll x)\wedge P$	$\rightarrow\Omega\mid_{x\in\chi}$

图 1　eWoo-Lam 模型中匹配等式的求解规则

2　eWoo-Lam 模型

2.1　语法

为了更加清晰准确地对密码协议进行形式化建模,eWoo-Lam模型的基本语法中不仅保留了 Woo-Lam 模型的大部分语法元素,同时增添了新的语法元素,如新的函数标记和动作等。

2.1.1　主体

密码协议系统中的主体类型可以分为三种:(1)合法主体:能够参与协议会话运行且合法拥有或获取协议传输数据的主体;(2)可信第三方:协议运行中用于辅助实现会话密钥的生成、分发、传递或普通协议主体身份认证的区别于协议发起者和响应者的一类特殊合法主体;(3)攻击者:试图以恶意的方式对协议会话实施攻击或利用的危险主体。在 eWoo-Lam 模型中,协议运行过程中涉及到的所有主体构成的集合记为 *NAME*,其中,可信第三方标识为 S;攻击者标识为 A。

2.1.2　消息

根据组成结构不同,可将协议系统中消息项集合 *MESSAGE* 划分为两个不交的集合,即原子项集 *AtomicItems* 和复合项集 *CompoundItems*。

原子项集 *AtomicItems* 由变量集 *Var*、明文集 *Text* 与密钥集 *Key* 构成,即 $AtomicItems = Var \cup Text \cup Key$。其中,明文项集 *Text* 中包含主体名、随机数等;密钥集 *Key* 中包含对称密钥 K_{sym}、公开密钥 K_{pub}、私有密钥 K_{priv} 等。

复合项集 *CompoundItems* 由函数作用于已有消息项获得。eWoo-Lam 模型中,函数集合 $F = \{concat, set, sencrypt, pencrypt, sign, hash, keyowner\}$。其中,$concat(t_1,t_2,\cdots,t_n)$ 表示 n 元项连接函数,简记为 $[t_1,t_2,\cdots,t_n]$;$set(t_1,t_2,\cdots,t_n)$ 表示 n 元集合,简记为 $\{t_1,t_2,\cdots,t_n\}$;$sencrypt(t,k)$ 表示对称密钥加密函数,简记为 $\{t\}_k$;$pencrypt(t,k)$ 表示公钥加密函数,简记为 $\{t\}_{k+}$;$sign(t,k)$ 表示私钥签名函数,简记为 $\{t\}_{k-}$;$hash(t)$ 表示散列函数,简记为 $h(t)$;*keyowner* 表示密钥所有者函数,$keyowner(K) \in 2^{NAME}$。另外,对于密钥 K,若 $keyowner(K) = \{x,y\}, x,y \in NAME\backslash\{A\}$,则也可以将密钥 K 记作 K_{xy}。

2.1.3　动作

eWoo-Lam 模型对 Woo-Lam 模型中关于密码学原语操作的描述进行了增强,引入了加/解密动作、签名/解签名动作等,使得对密码协议执行过程主体行为的形式化描述更加精确,同时增强了模型在检测协议攻击方面的能力;引入了匹配机制,并给出了该机制精确的数学定义,精确的描述了协议运行主体在接收到消息项时所执行的操作,这种机制可以在很大程度上减少协议安全特性证明的过程中的状态迁移数,从而提高证明过程的效率;重定义了 *Begin* 和 *End* 动作,使得关于认证性的形式描述和分析更具一般性;去除了 *GetSecret*、*Accept* 等动作,采用 *OldSecret* 来建模旧密钥攻击,使描述更加简洁有效。

eWoo-Lam 模型将协议运行过程中主体的动作分为两类,即内部动作和外部动作,具体描述如下:

(1) 内部动作

$Begin(t_1,t_2,\cdots,t_n)$ 表示启动一次协议会话的运行。$End(t_1,t_2,\cdots,t_n)$ 表示成功结束一次局部协议会话的运行。其中,*Begin* 和 *End* 中的参数 $t_1,t_2,\cdots,t_n$ 可以为任意项,主要用于数据一致性验证。$NewNonce(n)$ 表示生成随机数并将其绑定到变量 n。$NewSecret(O,s)$ 表示生成秘密并绑定给变量 s,同时指定 s 的合法所有者集合 O,即 $keyowner(s) = O$。$SEncrypt(m,k)$ 表示使用对称密钥项 k 加密消息项 m。$PEncrypt(m,k)$ 表示使用公开密钥项 k 加密消息项 m。$Sign(m,k)$ 表示使用私有密钥项 k 签名消息项 m。$Match(m_1,m_2)$,表示协议主体采用匹配机制来检验数据项 m_1、m_2 之间是否满足模式匹配:若匹配等式 $m_1 \ll m_2$ 有解,则表明满足匹配,协议将继续向后执行,并且建立相关变量的绑定;否则,终止协议运行。该动作仅与 *Receive* 动作连用,用于判定主体所接收到的消息是否是所期望的消息格式。对于攻击者而言,*Match* 的第一个参数总是变量,表示攻击者可以获得网络中的任何消息。$SDecrypt(c,k)$ 表示使用对称密钥项 k 来解密消息项 c。$PDecrypt(c,k)$ 表示使用私有密钥项 k 来解密消息项 c。$CheckSign(sign,k)$ 表示使用公开密钥项 k 来验证签名消息 $sign$。$OldSecret(t)$ 表示协议会话建立过程中当前执行主体部分结束,变量 t 可以表示任意消息项,用于建模已知密钥攻击。

(2) 外部动作

$Send(p,m)$ 表示向主体 p 发送消息项 m,消息项 m 可能遭到攻击者截获而无法达到 p。$Receive(p,m)$ 表示接收来自于主体 p 的消息并将其绑定到变量 m,其后需跟随有匹配动作 *Match* 来检查消息格式是否是所预期的。

2.1.4　形式化准则

利用 eWoo-Lam 模型建模密码协议时,应当遵循以下准则:

变量在使用前应当被绑定;

变量不能被重复绑定;

在生成密钥时,应指定其合法所有者;

可信第三方不能执行 *OldSecret* 动作;

用于解密消息的会话密钥必需已知;

合法主体不能使用其他主体的私钥进行签名;

合法主体不能使用不属于它们的对称密钥进行加解密运算。

2.1.5　协议描述

与 Woo-Lam 模型中不同,eWoo-Lam 模型将密码协议描述为一个对 $< InitialKnowledge, ProtocolsSet >$,使得基于攻击者知识的推理验证显得更加直观。其中,*InitialKnowledge* 表示攻击者初始知识集合;*ProtocolsSet* 表示局部协议的有穷非空集合。

协议语句继承了 Woo-Lam 模型中原有的描述方式,即形如 $label:act$ 的表达式,*label* 表示标记,*act* 表示动作。局部协议是协议语句的有穷序列。对于带有可信第三方的密码协议,局部协议可以分为三种:发起者协议、响应者协议和第三方协议。

根据上述语法定义,Otway-Rees 协议可以形式化地描述为元组 $< InitialKnowledge, \{InitialProtocol, RespondProtocol, ServerProtocol\} >$,如图 2 所示。

$InitialKnowledge=\{k_{AS}\}$	
$InitiatorProtocol=$ (I1) : $NewNonce(m)$ (I2) : $NewNonce(n)$ (I3) : $Begin(m)$ (I4) : $SEncrypt([n,m,i,r],k_{iS})$ (I5) : $Send(r,[m,i,r,\{[n,m,i,r]\}_{kiS}])$ (I6) : $Receive(p,c_1)$ (I7) : $Match([m,\{[n,k]\}_{kiS}],c_1)$ (I8) : $SDecrypt(\{[n,k]\}_{kiS},k_{iS})$ (I9) : $OldSecret(k)$	$ResponderProtocol=$ (R1) : $Receive(i,c_1)$ (R2) : $Match(\{[m,i,r,X],c_1)$ (R3) : $NewNonce(n)$ (R4) : $SEncrypt([n,m,i,r],k_{rS})$ (R5) : $Send(s,m,i,r,X,\{[n,m,i,r]\}_{krS})$ (R6) : $Receive(S,c_2)$ (R7) : $Match([m,Y,\{[n,k]\}_{krS}],c_2)$ (R8) : $SDecrypt(\{[n,k]\}_{krS},k_{rS})$ (R9) : $Send(i,[m,Y])$ (R10) : $OldSecret(k)$ (R11) : $End(m)$
$ServerProtocol=$ (S1) : $Recive(r,c)$ (S2) : $Match([m,i,r,\{[x,m,i,r]\}_{kiS},\{[y,m,i,r]\}_{krS}],c)$ (S3) : $NewSecret(\{i,r\},k)$ (S4) : $SEncrypt([x,k],k_{iS})$ (S5) : $SEncrypt([y,k],k_{rS})$ (S6) : $Send(r,[m,\{[x,k]\}_{kiS},\{[y,k]\}_{krS}])$	

图2 基于 eWoo-Lam 模型对 Otway-Rees 协议的建模

2.2 语义

按照语义学的观点,协议形式化描述可以看作是协议执行过程的符号化表示。也就是说,协议形式化描述的语义实际上就是协议的一系列可能的执行过程。eWoo-Lam 模型重新定义了局部状态、局部迁移、全局状态、全局迁移、协议执行和协议描述等概念,并给出了描述攻击者知识更新的相关规则,使得基于状态迁移的模型形式化语义更清晰准确。

定义 4 事件是指特定协议会话中一条语句,记为 $< run\text{-}id,\ stmt >$。其中,*run-id* 表示当前协议会话的标识符;*stmt* 表示当前执行的协议语句。

定义 5 事件序列的任意首部称为该事件序列的一个前缀。空序列是任意事件序列的前缀。

定义 6 局部协议 $P_i(x_i)$ 的部分实例是指具有相同会话标识 *id* 的事件序列 $\zeta(id)$,并且存在一个基础置换 θ,使得 $\zeta(id)$ 构成 $\theta P_i(x_i)$ 的一个前缀。从直观上看,协议的部分实例是对协议实例部分执行过程建模。

定义 7 协议段是一个由协议事件组成的序列,记为 *frag*。令 X 为协议的合法主体,并且对于任意会话标识 *id*,事件序列 $\zeta(id)$ 总是协议 $P(X)$ 的部分实例,则称 $\zeta(id)$ 为主体 X 的协议段;对于攻击者 A,任意事件序列均可能构成其协议段。

定义 8 局部状态是一个二元组 $(frag,info)$,它从属于协议的某个特定主体。其中,*frag* 表示所属主体的协议段;*info* 为一个消息项的集合,表示所属主体的知识。

定义 9 局部迁移是某个特定主体执行的一条协议语句,常简记为语句中的动作。

令 $(frag,info)$ 是一个局部状态,α 是一个局部迁移,如果下列条件满足,则称局部迁移 α 在局部状态 $(frag,info)$ 处有效:

(1) 存在会话标识 *id*,使得 $frag \parallel < id,\alpha >$ 是主体 X 的协议段。其中,$\parallel$ 是一个连接运算符;

(2) 如果 $\alpha = Send(p,m)$,则有 $m \in info$;

(3) 如果 $\alpha = SEncrypt(m,k)$,则有 $m \in info$,且 $X \in keyowner(k)$;

(4) 如果 $\alpha = PEncrypt(m,k)$,则有 $m \in info$,且 $k \in info$;

(5) 如果 $\alpha = Sign(m,k)$,则 $m \in info$,且 $keyowner(k) = \{X\}$;

(6) 如果 $\alpha = SDecrypt(c,k)$,则 $\exists m \in MESSAGE$,使得 $c = \{m\}_k$,且 $X \in keyowner(k)$;

(7) 如果 $\alpha = PDecrypt(c,k)$,则 $\exists m \in MESSAGE$,使得 $c = \{m\}_k$,且 $keyowner(k) = \{X\}$;

(8) 如果 $\alpha = CheckSign(sign,k)$,则 $k \in info$;

令 $(frag,info)$ 与 $(frag',info')$ 是协议主体 X 的两个局部状态,α 为一个局部迁移,如果满足下列条件,则称状态 $(frag,info)$ 可以经由局部迁移 α 转换为状态 $(frag',info')$,即 $(frag,info) \xrightarrow{\alpha} (frag',info')$:

(1) 局部迁移在状态 $(frag,info)$ 处有效;

(2) 存在会话标识 *id*,使得 $frag' = frag \parallel < id,\alpha >$;

(3) 如果 α 是 *Begin*、*End*、*Send*、*Receive* 等迁移,则 $info' = info$;

(4) 如果 α 是 $NewNonce(n)$、$NewSecret(O,n)$、$OldSecret(n)$ 等迁移,则 $info' = update(info,n)$;

(5) 如果 α 是 $Match(m,n)$ 迁移,则 $info' = update(info,n)$。

其中,*update* 用于表示在获取到新的数据项后协议主体知识的具体更新过程,可用一组规则进行描述。图 3 给出了模型中关于攻击者知识更新的相关规则。

$$(A1)\quad \frac{m \in info}{m \in update(info,n)}$$

$$(A2)\quad \frac{}{n \in update(info,n)}$$

$$(A3)\quad \frac{[m_1,m_2,...,m_n] \in update(info,n)}{m_1 \in update(info,n) \wedge m_2 \in update(info,n) \wedge ... \wedge m_n \in update(info,n)}$$

$$(A4)\quad \frac{\{m\}_{ksym} \in update(info,n) \wedge k_{sym} \in update(info,n)}{m \in update(info,n)}$$

$$(A5)\quad \frac{\{m\}_{k+} \in update(info,n) \wedge k- \in update(info,n)}{m \in update(info,n)}$$

$$(A6)\quad \frac{\{m\}_{k-} \in update(info,n) \wedge k+ \in update(info,n)}{m \in update(info,n)}$$

$$(A7)\quad \frac{m \in update(info,n)}{hash(m) \in update(info,n)}$$

$$(A8)\quad \frac{m \in update(info,n) \wedge k_{sym} \in update(info,n)}{\{m\}_{ksym} \in update(info,n)}$$

$$(A9)\quad \frac{m \in update(info,n) \wedge k+ \in update(info,n)}{\{m\}_{k+} \in update(info,n)}$$

$$(A10)\quad \frac{m \in update(info,n) \wedge k- \in update(info,n)}{\{m\}_{k-} \in update(info,n)}$$

图3 eWoo-Lam 模型中攻击者知识更新规则

定义 10 全局状态是由协议系统中每个主体的局部状态所组成的元组。给定一个全局状态 s,记 s 中属于主体 X 的局部状态为 $s.X$。

定义 11 全局迁移有如下两种形式:

(1) $(X.label,act)$ 表示内部迁移,X 是协议系统中的一个合法主体,$label:act$ 是除 *Send* 和 *Receive* 之外的局部迁移;

(2) $(X.label,Send(Y,M)) \cdot (Y.label',Receive(X,M))$ 表示相继执行的发送迁移 $(X.label,\ Send(Y,\ M))$ 和接收迁移 $(Y.label',\ Receive(X,M))$。

令 s 是一个全局状态,β 是一个全局迁移。如果下列条件之一被满足:

(1) $\beta = (X.label,act)$ 是一个内部迁移,并且局部迁移 $label:act$ 在局部状态 $s.X$ 处有效;

(2) $\beta = (X.label,Send(T,M)) \cdot (Y.label',Receive(V,M)) \cdot (A.label',Receive(V,M))$,并且下列条件成立:

· 局部迁移 $label:Send(T,M)$ 在局部状态 $s.X$ 处有效;

· 局部迁移 $label'$:$Receive(V,M)$ 在局部状态 $s.Y$ 处有效;

· $X = V$ 且 $Y = T$。

则称全局迁移 β 在全局状态 s 处有效。

令 s 和 s' 为两个全局状态,β 是一个全局迁移。如果下列条件满足:

(1) β 在 s 处有效;

(2) 如果 $\beta = (X.label, act)$ 是一个内部迁移,则 $s.X \xrightarrow{label:act} s'.X$ 成立,并且对于所有 $Y \in NAME\backslash\{A\}$ 且 $Y \neq X$,均有 $s.Y = s'.Y$;

(3) 如果 $\beta = (X.label, Send(T,M)) \cdot (Y.label', Receive(V,M)) \cdot (A.label', Receive(V,M))$,则有 $s.X \xrightarrow{label:Send(T,M)} s'.X, s.Y \xrightarrow{label':Receive(V,M)} s'.Y, s.A \xrightarrow{label':Receive(V,M)} s'.A, X = V, Y = T$,并且对于所有 $W \in NAME\backslash\{A, X, Y\}$,均有 $s.W = s'.W$。

则称状态 s 可以经由迁移 β 转换为状态 s',即 $s \xrightarrow{\beta} s'$。

协议的一次执行是一个由全局状态和迁移交替组成的形如 $\xi_{id} = s_1\beta_1 s_2\beta_2\cdots\beta_{n-1}s_n$ 的有限序列,其中的通信迁移均被描述成为顺序执行的发送组件和接收组件。协议的一次执行应当满足下列条件:

(1) 对 $\forall\beta_i, 1 \leqslant i < n$,均有 $s_i \xrightarrow{\beta_i} s_{i+1}$;

(2) 如果 $\beta_i = (X.label, NewNonce(N)) \mid (X.label, NewSecret(O,N))$,$\mid$ 表示逻辑或,则 N 一定是新鲜的;

(3) 如果 k 是出现在 ξ_{id} 中的一个密钥项,则 $keyowner(k) \subseteq NAME$;

协议形式化描述 Π 的语义是所有协议执行过程所组成的集合。当协议描述的上下文环境非常清晰时,通常也将 Π 的语义记为 Π 本身。

命题 1　协议描述的语义在运算上是前缀封闭的。

证明　令 Π 为一个协议描述的语义,ξ 为一次协议执行,$\xi \in \Pi$,

$\psi(\xi)$ 为 ξ 的所有前缀所组成的集合,

根据协议执行过程的定义,对于 $\forall\zeta \in \psi(\xi)$,均有 $\zeta \in \Pi$。

故上述命题成立。

该命题在协议形式化分析过程中非常重要,是包括不变式证明在内的证明方法的基础。

3　安全特性

秘密性和认证性是密码协议的两种基本安全特性。在形式化模型中,如何对这两种安全特性进行精确合理的形式化定义,是至关重要的,也是评价模型优劣的一个重要标准。在 Woo-Lam 模型中,协议秘密性的专用描述部分实质上属于安全性的基本假设,不应当作为安全性的验证目标;认证性描述部分将认证性描述为两个一致性断言,按照 Gavin Lowe 的观点,这只是一种较低级别的认证,存在着缺陷,对数据的一致性的检验不具有一般性。eWoo-Lam 模型则根据新的描述语法对密码协议的安全性进行了重新定义,细粒度更细,更为合理可靠。

3.1　秘密性

密码协议的秘密性目标可以描述为确保协议中的秘密消息在协议运行过程中应当是不能被公开的或被非法攻击者获取的。如果攻击者可以从所截获的消息中推知出某个秘密,则称该秘密被公开了,即协议没有达到预期的秘密性目标。

直观上,如果协议在一次执行结束时攻击者仍然不知道消息 m,则称 m 在该协议执行过程中保持了秘密性。令 $\xi = s_1\beta_1 s_2\beta_2\cdots\beta_{n-1}s_n$ 为协议的一次执行,其中 s_1 表示执行的初始状态,s_n 表示执行的最终状态,则 m 的秘密性可以利用一阶逻辑公式形式地描述为:

$$Secrecy_\xi(m) \cong s_n \vdash \neg(A\ has\ m)$$
$$\cong (frag_n, info_n) = sn.A \wedge m \notin info_n$$

在协议的一次执行结束时,攻击者获得消息 m 的情况有三种可能:

(1) 消息 m 在攻击者的初始知识中;

(2) 攻击者曾经收到过消息 m;

(3) 攻击者根据其初始知识、接收到的消息项及其计算能力推导出消息项 m。

形式化描述如下:

$$sn \vdash (A\ has\ m) \cong (frag_1, info_1) = s1.A \wedge m \in info_1$$
$$\vee\ \exists i, 1 \leqslant i < n, \beta_i = (A.label, Receive(p,m))$$
$$\vee\ \exists i, 1 \leqslant i < n, \beta_i = (A.label, Receive(p,m'))$$
$$\wedge (frag_i, info_i) = si.A \wedge (frag_{i+1}, info_{i+1}) = s_{i+1}.A$$
$$\wedge\ m \in info_i \wedge m \in info_{i+1}$$

3.2　认证性

认证性是密码协议的一个主要安全性目标。在文献[22]中,Gavin Lowe 在对许多关于认证性的定义进行了讨论之后,提出将认证性划分为四个等级:(1) 存在性,即当协议发起方主体 I 完成协议的一次协议的运行时,作为预期响应方的主体 R 确实已经参与了协议的运行;(2) 弱一致性,即在满足存在性的基础上,预期响应方 R 确实是与当前发起者 I 在运行该协议;(3) 非单射一致性,指在满足了弱一致性的基础上,协议发起方与接收方在某一确定的消息集 M 上达成一致;(4) 单射一致性,则是指协议运行在满足了非单射一致性的基础上,协议发起方的一次运行恰好对应于响应方的唯一一次运行。但是,即使协议满足了存在性、弱一致性或非单射一致性,仍然可能遭受各种类型的攻击,典型的如重放攻击等。因此,在研究认证协议的正确性时,讨论最多的是协议的一致性。

在 eWoo-Lam 模型中,协议的一致性需求被描述为一个元组,即 $< e, e' >$。其中 $e = End(t_1, t_2, \cdots, t_n)$ 和 $e' = Begin(t'_1, t'_2, \cdots, t'_n)$ 均为协议描述中的事件。协议的一次执行 $\xi = s_1\beta_1 s_2\beta_2\cdots\beta_{n-1}s_n$ 满足一致性需求 $< e, e' >$,当且仅当对于合法主体 $i, r \in NAME\backslash\{S,A\}$,在协议的一次运行过程中,如果主体 i 执行了语句 e,则主体 r 在此之前必定执行过语句 e',且 $t_1 = t'_1, t_2 = t'_2, \cdots, t_n = t'_n$。上述讨论可以形式化地描述如下($\exists\mid$ 表示存在且唯一):

$$Correspondence_\xi \cong \xi \vdash < e, e' >$$
$$\cong e = \beta_{i\in\{2,\cdots,n-1\}} \Rightarrow \exists\mid \beta_{j\in\{1,\cdots,i\}},$$
$$\beta_j = e' \wedge_{k\in\{1,\cdots,i\}} (t_k = t'_k)$$

4　结语

本文针对 Woo-Lam 密码协议模型中所存在的问题和不足之处,对其进行了改进,提出了一种新的密码协议建模方案,即 eWoo-Lam 模型。新模型对 Woo-Lam 模型中密码学原语的描述语法进行了增强;引入了匹配机制,给出了该机制

精确的数学定义；并提出了七条准则，对密码协议的形式化过程进行规范，使得形式化更加清晰准确。在此基础之上，对密码协议的安全特性重新进行了规范定义，为协议安全特性分析和证明提供了一个合理可靠的基础。

在下一步的工作中，我们将进一步研究基于 eWoo-Lam 模型中的形式化推理机制，分析影响推理过程的各种因素；在此基础上，设计有关该模型的自动化验证算法，并将算法应用于密码协议自动化验证器中。

参考文献：

[1] DOLEV D, YAO AC. On the Security of Public-Key Protocols[J]. IEEE Transactions on Information Theory, 1983, 2(29): 198 - 208.

[2] BRIAIS S, NESTMANN U. A Formal Semantics for Protocol Narrations[A]. Trustworthy Global Computing, International Symposium, TGC 2005[C], Edinburgh, UK, 2005. 163 - 181.

[3] CHEVALIER Y, COMPAGNA L, CUELLAR J, *et al*. A High-Level Protocol Specification Language for Industrial Security — Sensitive Protocols[A]. Proceedings of Workshop on Specification and Automated Processing of Security Requirements(SAPS 2004)[C], 2004.

[4] BOUROULET R, KLAUDEL H, PELZ E. A Semantics of Security Protocol Language Using a Class of Composable High-level Petri Nets [R]. Laboratory of Algorithms, Complexity and Logic of University of Paris, France, 2004.

[5] HALPERN JY, PUCELLA R. Modeling Adversaries in a Logic for Security Protocol Analysis [A]. Formal Aspects of Security, FASec'02[C], 2002.

[6] WOO TYC, LAM SL. A Semantic Model for Authentication Protocols[A]. Proceedings IEEE Symposium on Research in Security and Privacy[C]. Oakland, CA, 1993. 178 - 194.

[7] GUTTMAN JD, HERZOG JC, RAMSDELL JD, *et al*. Programming Cryptographic Protocols[R]. The MITRE Corporation, 2004.

[8] DELAUNE S, JACQUEMARD F. A Decision Procedure for the Verification of Security Protocols with Explicit Destructors[A]. Proceedings of the 11th ACM Conference on Computer and Communications Security[C], 2004. 278 - 287.

[9] 季庆光，冯登国. 对几类重要网络安全协议形式模型的分析[J]. 计算机学报，2005，28(7)：1071 - 1083.

[10] SONG D. Athena: a New Efficient Automatic Checker for Security Protocol Analysis[A]. Proceedings of the 12th IEEE Computer Security Foundations Workshop (CSFW'99)[C], 1999. 192 - 202.

[11] CLARKE EM, JHA S, MARRERO W. Verifying Security Protocols with Brutus[J]. ACM Transactions on Software Engineering and Methodology (TOSEM), 2000, 9(4): 443 - 487.

[12] MEADOWS C. The NRL Protocol Analyzer: an Overview [J]. Journal of Logic Programming, 1996, 26(2): 113 - 131.

[13] DATTA A, DEREK A, MITCHELL JC, *et al*. A Derivation System and Compositional Logic for Security Protocols[J]. Journal of Computer Security (Special Issue of Selected Papers from CSFW-16), 2005, 13(3): 423 - 482.

[14] LOWE G. Casper: A Compiler for the Analysis of Security Protocols [A]. Proceedings of the 1997 IEEE Computer Society Symposium on Research in Security and Privacy[C], 1997. 18 - 30.

[15] STOLLER SD. A Reduction for Automated Verification of Authentication Protocols [R]. Computer Science Department, Indiana University, 1998.

[16] THAYER FJ, HERZOG JC, GUTTMAN JD. Strand spaces: Why is a security protocol correct? [A]. Proceedings of IEEE Symposium on Security and Privacy[C], 1998. 160 - 171.

[17] 刘怡文，李伟琴. 网络支付协议的形式化安全需求及验证逻辑[J]. 通信学报，2004，25(4)：174 - 181.

[18] CREMERS CJF, MAUW S, VINK EP. A Syntactic Criterion for Injective of Authentication Protocols [A]. Proceedings of ARSPA'05 (The Second Workshop on Automated Reasoning for Security Protocol Analysis)[C], 2005.

[19] FOCARDI R, MAFFEI M, PLACELLA F. Inferring Authentication Tags[A]. Proceedings of 2005 IFIP WG 1.7, ACM SIGPLAN and GI FoMSESS Workshop on Issues in the Theory of Security (WITS'05)[C], 2005. 41 - 49.

[20] 胡成军，郑援，吕述望，等. 安全协议的形式化规范[J]. 电子与信息学报，2004，26(4)：556 - 561.

[21] BLANCHET B. An Efficient Cryptographic Protocol Verifier Based on Prolog Rules[A]. 14th IEEE Computer Security Foundations Workshop(CSFW-14), IEEE Computer Society[C]. Los Alamitos, CA, 2001. 82 - 96.

[22] LOWE G. A Hierarchy of Authentication Specifications[A]. Proceedings of the 10th Computer Security Foundations Workshop (CSFW'97)[C]. Rockport, Massachusetts, 1997.

[23] LOWE G, ROSCOE B. Using CSP to Detect Errors in the TMN Protocol[J]. IEEE Transactions on Software Engineering, 1997, 23(10): 659 - 669.

(上接第 2115 页)

1/4，当接受者收到消息后，首先验证 $gcd(x^{p-1/2}, x^2 + mx + c) = x - a$，这里 a 是方程的解，m 和 c 是方程组中选定的参数，含义与(1)，(2) 和(3)，(4) 相同。如果等式不成立，则说明消息被篡改。由于消息 (c_1, c_2) 被成功篡改的可能性是1/4，所以在密钥交换中，有必要利用哈希函数和时间戳的方式来防止篡改。

2) 在实际的系统中，有一些实体可能不是经常参与通信，这时CA 可以不存储它们的会话密钥，而是由实体存储 (c_1, c_2)，通信是临时计算会话密钥，这使得CA 不需要存储任何临时性的信息，而只需要维持一个大的静态数据库，每次收到一个请求发一个响应，然后忘掉所有的一切。这种模式有很多好处，比如可以很容易地实现CA 的备份以及在系统崩溃前不需要保存状态等。

6 结语

本文根据大数分解的困难性，利用同余方程的性质提出了一种新的加密算法，这一算法可以有效地实现会话密钥的交换和加密消息的传输，并且能够防止中间人攻击。

参考文献：

[1] STALLINGS W. 密码编码学与网络安全：原理与实践[M]. 第3版. 刘玉珍，王丽娜，傅建明，译，北京：电子工业出版社，2004.

[2] 潘承洞，潘承彪. 初等数论[M]. 第2版. 北京：北京大学出版社，2003. 155 - 157.

[3] MENEZES AJ, VAN OORSCHOT PC, VANSTONE SA. 应用密码学手册[M]. 胡磊，王鹏，译. 北京：电子工业出版社，2005.

[4] 李子臣，戴一奇. 二次剩余密码体制的安全性分析[J]. 清华大学学报(自然科学版)，2001，41(7)：80 - 82.