移动代理完整性协议形式化分析方法研究

李鹏飞[1,2,3],马恒太[1,2],侯玉文[1,2,4],邱 田[1,2,3]
(1.中国科学院综合信息技术国家级重点实验室,北京 100190; 2.中国科学院软件研究所,北京 100190;
3.中国科学院研究生院,北京 100039; 4.天津大学电子信息学院,天津 300072)

摘 要: 本文给出了移动代理协议数据完整性属性的定义,指出了采用传统认证性属性来分析移动代理数据完整性属性的不足,从而给出了移动代理完整性证明的两个形式化规约:数据完整性规约和序列完整性规约.在此基础上,针对典型协议实例进行CPS建模,并采用阶函数的方法证明了其完整性,验证了完整性规约的正确性和有效性.

关键词: 移动代理; 数据完整性; 形式化方法; 形式化模型
中图分类号: TP309.2 **文献标识码:** A **文章编号:** 0372-2112 (2009) 08-1669-06

Research on Formal Analysis Method of Mobile Agent Data Integrity Protocol

LI Peng-fei[1,2,3], MA Heng-tai[1,2], HOU Yu-wen[1,2,4], QIU Tian[1,2,3]
(1. *National Key Laboratory of Integrated Information System Technology, Bejing* 100190, *China*;
2. *Institute of Software, The Chinese Academy of Sciences, Beijing* 100190, *China*;
3. *Graduate School, The Chinese Academy of Sciences, Beijing* 100039, *China*;
4. *Electronic Information Technical School, Tianjin University, Tianjin* 300072, *China*)

Abstract: This paper gives a formal analysis method of mobile agent data integrity protocol. We pointed out that authentication property is not suit to analysis mobile agent data integrity, and proposed two formal specifications for mobile agent data integrity. We constructed a CSP model for a concrete mobile agent data integrity protocol, checked its integrity using rank function. These works prove formal analysis method is effective in analyzing mobile agent data integrity protocol.

Key words: mobile agents; data integrity; path integrity; formal analysis; formal model

1 引言

移动代理动态数据保护协议针对移动代理动态数据易受攻击的特点,对其私密性、匿名性和完整性等安全属性进行保护.其中,移动代理动态数据完整性保护协议(MADIPP)使用基于密钥的加密或签名等安全机制来实现对移动代理数据的完整性保护.同传统的消息认证协议相比,MADIPP具有很多不同的特点:(1)移动代理协议中正常参与者的数量是不确定的,消息交互的次序也是不确定的;(2)由于移动代理所运行环境的不可确定性,导致协议正常参与者和攻击者之间的界定困难,非可信主机也可成为攻击者[1].

协议形式化分析是通过模型检测和定理证明等手段验证协议是否满足某一安全属性,因此协议安全属性的精确描述是协议形式化分析的基础.通过对协议安全属性的描述和分析,才能清楚认识安全属性要满足的环境要求,确定协议的应用环境.完整性在传统的协议形式化建模理论中曾有所描述[2],但基本局限于文献[2]的表示,即将完整性描述等同于认证性的描述,文献[1,3~6]也沿袭了这一描述.这两种属性在经典的认证协议中也许可认为存在一致,但在MADIPP中将两者等价,就会导致一些缺陷.如:无法分析MADIPP中存在的截断攻击.

本文给出了完整性的新定义,尝试以CSP对Maggi[7]给出的可配置MADIPP进行建模分析,并通过阶函数证明了其在分析MADIPP方面的有效性.

2 可配置的MADIPP

P Maggi[7]给出了一个可配置的MADIPP(PM协议),可以根据安全需求进行配置,保证动态数据的完整性、保密性等安全属性,下面就以该协议为例进行分析.

收稿日期:2008-07-16;修回日期:2009-01-05
基金项目:国家自然科学基金(No.60573042);中国科学院创新基金(No.CXJJ251)

表 1 协议描述符号

i_0	初始主机
$i_0, i_1, i_2, \cdots, i_n, i_0$	代理的漫游路径
Π	代理的静态部分
t	时间戳
$i_j \rightarrow i_k : m$	将数据 m 从主机 i_j 传递到 i_k
$\{m\}_{S_{i_n}^{-1}}$	使用主机 i_n 的私钥对数据 m 签名
$\{m\}_{K_{i_n}^{+}}$	使用主机 i_n 的公钥对数据 m 进行加密
$h(m)$	计算数据 m 的哈希值
$m_1 \parallel m_2$	将数据 m_2 连接到 m_1

协议描述如下：

$i_n \rightarrow i_{n+1} : \Pi_0, \{M_0, \cdots, M_n\}$,

其中 $\Pi_0 = \{\Pi, t\}_{S_{i_0}^{-1}}$, $M_n = D_n \parallel C_n$.

$$D_n = \begin{cases} P_0, & \text{if } i_n = i_0 \\ \{d_n\}_{K_{i_0}^{+}}, P_n, & \text{if } i_n \neq i_0 \end{cases}$$

$$C_n = \begin{cases} (P_0, \Pi_0, i_1)_{S_{i_0}^{-1}}, & \text{if } i_n = i_0 \\ \{(d_n, P_n, \Pi_0, C_{n-1}, i_{n+1})_{S_{i_n}^{-1}}\}_{K_{i_0}^{+}}, & \text{if } i_n \neq i_0 \end{cases}$$

其中 Π_0 包括移动代理自身的可执行程序和时戳 t, M_n 是移动代理在主机 i_n 上执行结果，由两部分数据组成，其中 D_n 包括代理在该主机上的执行结果数据 d_n 和代理的漫游的路径 P_n, C_n 的作用是 D_n 数据的验证，它将数据 d_n、漫游路径 P_n、代理静态部分 Π_0、前一主机的数据封装 C_{n-1} 和下一个要去的主机 i_{n+1} 进行了链接绑定.

3 移动代理数据完整性形式化分析方法

下面用 CSP 对 P Maggi 所给出的协议进行建模，并给出针对完整性属性的形式化规范，以及协议是否符合我们所给出的完整性属性的证明. 限于篇幅这里不对 CSP 的方法及其符号进行介绍，详见文献[2].

3.1 协议形式化模型

(1)可信赖进程描述

在典型的消息交互协议中，协议发起者、协议响应者都属于可信赖的协议主体，即按照协议的规则去正确执行协议，对可信赖协议主体的描述是形式化模型建立的初始步骤. 在移动代理协议中，协议发起者是确定的、可信赖的，而协议响应者的个数是不确定的，不一定可信赖[1]. 下面是协议可信赖进程的描述.

协议发起者为：

$$\text{Initiator}(i_0, \Pi_0) = \square_{i_0, i_1 \in \text{Host}} \text{send}.i_0.i_1.(\Pi_0, M_0) \rightarrow \square_{i_0, i_n \in \text{Host}, \Pi_0 \in \text{Nonce}} \text{receive}.i_n.i_0.(\Pi_0, M_0, \cdots, M_n)$$

协议响应者为：

$$\text{Responder}(i_j, \Pi_0) = \begin{array}{l} \square_{i_{j-1}, i_j \in \text{Host}, \Pi_0 \in \text{Nonce}} \text{receive}.i_j.i_{j-1}.(\Pi_0, M_0, \cdots, M_{j-1}) \rightarrow \text{Responder}(i_j, \Pi_0) \\ \square_{i_j, i_{j+1} \in \text{Host}, \Pi_0 \in \text{Nonce}} \text{send}.i_j.i_{j+1}.(\Pi_0, M_0, \cdots, M_j) \rightarrow \text{Responder}(i_{j+1}, \Pi_0) \end{array}$$

Host 表示所有能够发起和参与该移动代理协议的主机集合，Nonce 表示唯一标识集合，send.a.b.m 表示协议主体 a 发送消息 m 给主体 b，receive.a.b.m 表示 a 从 b 接收消息 m，对消息 m 的各种操作符使用表 1 中的符号.

值得注意的是这里的 i_j 和 i_{j+1} 只是参与者在移动代理漫游路径上的序号，而两者的取值都是能够参与该协议的主机集合，所以两者可以为同一主机，而这种表示也描述了同一轮次协议响应者在数量上的不确定和重复参与同一协议轮次的可能性，同时这是在其它协议模型中所没有描述的.

(2)攻击者进程描述

依据 Dolev-Yao 模型，假设攻击者具有对网络的全面控制能力，能够截获、处理和重发网络中传输的消息. 对消息的处理包括将消息进行删除、合并以及使用所掌握的密钥对消息进行加密和解密. 攻击者描述如下：

$$\text{Intruder}(X) = \text{learn}?\ m : \text{messages} \rightarrow \text{Intruder}(\text{close}(X \cup \{m\}))$$
$$\square \text{say}?\ m : X \cap \text{messages} \rightarrow \text{Intruder}(X)$$

这里采用 learn 和 say 来分别对应协议正常参与者中的 receive 和 send 动作，攻击者能够通过这两个动作获取协议中的消息交互. Close($X \cup \{m\}$)表示将接收到的消息 m 使用密钥操作和字符操作后加入到攻击者所掌握的消息集合 X 中，say 动作所发出的消息 m 是接收到的消息 messages 和所掌握的消息 X 的交集，即攻击者使用所掌握的知识对消息 m 进行处理后所能得到的所有可能消息.

因为 MADIPP 中正常参与者之间往往互相存在竞争关系，是互不信任的，恶意主机参与者的攻击是该类协议必须要考虑的一种攻击形式. 由于攻击者的行为包含恶意参与者的行为，可以将恶意参与者的行为统一用攻击者模型来表示[1,3]，这里只需对攻击者的初始知识进行扩充加入恶意参与者所掌握私钥集合即可.

$$\text{Knowledge}(In) = \text{Knowledge}(In) + S_{i_{malichost}}^{-1}$$

(3)消息集合

为了更好的对协议参与主体及它们的动作进行描述，就必须确认并精确描述参与主体所能够处理的消息[8,9]. 在此，也采用同样方法给出 PM 移动代理协议的消息描述.

通过上面描述，可以给出协议的消息空间，至少包括：移动代理执行标识 Flag、代理漫游主机名 Host、密钥 Key、数据 Data 以及这些内容的组合. 消息集合的语法描述如下：

RAW::= Flag | Host | Key | Data

MESSAGE = RAW | KEY(MESSAGE) | MESSAGE.MESSAGE

(4)协议整体结构

移动代理协议的参与者包括协议的初始发起者、协议的响应者和协议的攻击者. 协议的响应者是移动代理所经过的

各个主机节点.对于 MADIPP,协议响应者的数量是不确定的,文献[1,3~5]在对协议进行形式化分析时都选择了三个响应者作为代表,这种结构也成为 MADIPP 形式分析的常用结构.

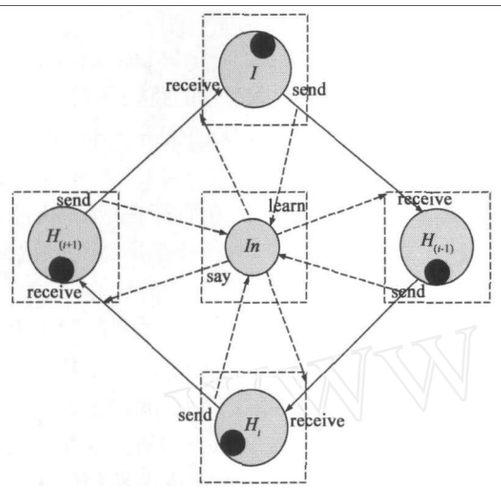

图1　移动代理数据完整性协议模型结构

协议发起者、协议响应者之间的消息交互通过 send 和 receive 信道来完成,为了区分攻击者同协议正常参与者之间的消息信道,可用 learn 和 say 来描述攻击者和消息发起者及响应者之间消息信道,这样整个 MADIPP 结构就可以表示为协议各个组成部分通过设定的信道来并行交互的组合.

$$\text{NETWORK} = \begin{array}{l}(\|\|_{i,j\in \text{Host}}\text{Initiator}_i \,|\, [\text{send},\text{receive}] \,|\, \text{Responder}_j) \\ |\,[\text{learn},\text{say}]\,|\,\text{Intruder}(X)\end{array}$$

3.2　完整性属性

完整性是 PM 协议的主要安全目标.文献[2]认为完整性是认证性的必然结果,即如能保障认证性就能保证完整性,文献[1,3,6,5]对移动代理数据保护协议进行形式化分析时也将完整性的验证转化为对消息的源认证.将完整性转换为认证性,忽略了完整性的一些特点,而这些特点在 MADIPP 中是必须要考虑的.

Karjoth 和 Maggi 在文献[7,10]中将数据完整性划分为转发完整性和抗数据截断完整性,但对完整性定义过于抽象,可操作性不强,不能很好应用于协议分析,对完整性强弱划分不清晰,不能为考核协议的安全性提供依据.我们对移动代理的完整性进行了重新定义.

定义 1　协议发起者 s_0 在一次协议执行完后收到数据为 $\{d_1,\cdots,d_k\}$,该次协议执行的参与主机为 $\{s_1,\cdots,s_k\}$,如 s_0 接收到的任意数据 d_i 确为该次协议执行的参与主机 s_i 所发数据,并且任意该次协议执行参与主机 s_i 所发数据都包括在 s_0 所接收到的数据 $\{d_1,\cdots,d_k\}$ 中,则称数据强完整性被保证.

该完整性的定义过强,在网络不可靠和存在攻击者的环境中是不能够保证的,因为网络或攻击者都有可能丢弃某参与主机 s_i 所发的数据包,造成其所发数据都包括在 s_0 所接收到的数据 $\{d_1,\cdots,d_k\}$ 中,因此下面提出一个较弱的定义.

定义 2　协议发起者 s_0 在一次协议执行完后收到数据为 $\{d_1,\cdots,d_k\}$,该次协议执行的参与主机为 $\{s_1,\cdots,s_k\}$,如 s_0 有证据表明接收到的任意数据 d_i 确为该次协议执行的参与主机 s_0 所发数据,并且如参与主机 s_i 所发数据不包括在 s_0 所接收到的数据 $\{d_1,\cdots,d_k\}$ 中时,s_0 有证据能够发现,则称数据完整性被保证.

对于通常的两方消息协议来说,完整性主要是保证一方发送的消息在被另一方接收到后没有被篡改,这种要求也可以通过发送方和接收方对消息数据 m 达成一致来表示,这就使得在两方消息协议中,消息完整性可以通过消息源认证性来保证[2,11],即 Agreement(receiver, sender, $\{d\}$).目前很多 MADIPP 形式化分析正是基于这一点,而将完整性证明转化为消息源认证性证明.

MADIPP 是一个多方链式协议,消息完整性的保证不仅要满足消息源认证性还要保证协议参与者的完整性,即协议的发起者最终能够得到证据 C,该证据能够证明有唯一确定的一组参与者 $\{s_1,\cdots,s_k\}$ 参与了该协议.

MADIPP 要保证定义 2 给出的完整性需满足下面两个规约:

(1)数据完整性规约

DataIntegrity(Responder, Initiator, $\{D\}$) $\triangleq$

($s_0\in$ Initiator, $\forall\, d_i\in D$)(Signal. Running. Initiator. s_0? s_n? d_i)→($s_i\in$ Responder, $1\leqslant i\leqslant n$)(Signal. Commit. Responder. s_i! s_0! d_i)→STOP

其中 D 为协议初始发起者所接收到的数据的集合,s_0 和 s_i 分别为协议的初始发起者和协议响应者,该规范表明发起者所接收到的任一消息 d_i,必有一协议响应者 s_i 发送该消息 d_i.

(2)序列完整性规约

PathIntegrity(Responder, Initiator, $\{D,P,C\}$) $\triangleq$

(Signal. Running. Initiator. s_0? s_n? D? P? C)→($P\subseteq$ Responder, $s_i\in P, 1\leqslant i\leqslant n$)(Signal. Commit. Responder. s_i! s_0! $c_i(c_i\in C)$) $\wedge$ ($\neg\,\exists\, S(S\neq P)\subseteq$ Responder, $s_j\in S, 1\leqslant j\leqslant n$)(Signal. Commit. Responder. s_j! s_0! $c_i(c_i\in C)$)

其中 P 为初始发起者接收到的参与协议的节点序列,该规约表明初始节点接收到的参与节点序列必须唯一确定,即初始节点在一次协议执行中,根据所接收到的证据能够唯一构造一条协议参与节点序列.攻击者和非可信节点在经过参与节点序列 A 后,不能产生证据 E_A 使得 $E_A=E_B(A\neq B)$,而其中 B 为不等于 A 的节点序列.

3.3　完整性证明

对于数据的完整性规约,可以将其转换为每个响应

者同发起者的认证性规约,因为二者都可以描述为一个事件 T 发生,则必有一个事件 R 发生.因此数据完整性的证明,可以等价为认证性的证明,即证明协议发起者接收到数据 d_i 之前必有一协议响应者发送了该数据 d_i.文献[2]详细描述了如何用阶函数方法来证明认证性属性.本文重点讨论序列完整性的证明,给出了该属性的阶函数证明.

3.3.1 阶函数

阶函数是 Schneider[8]提出的一种协议安全属性证明方法.该方法为协议消息空间中的每个消息设定一个值(也称为阶),根据协议的安全属性给出阶函数应满足的特性,然后根据协议本身、攻击者的知识和能力来寻找一个阶函数的分配方案,在该分配方案下,通过阶函数的证明规则,能够保证只有那些有着严格正阶的消息才能在协议中循环,而保密的消息的阶必须为负.如果该函数存在且满足所需特性,则协议满足该安全属性,否则协议可能存在攻击.

定义 3 阶函数 ρ 就是这样一个 ρ 函数 $\rho(Message)\rightarrow Z$,它把消息映射为一整数.

为了保证只有正阶的消息可以循环,而且只有正阶的信号才能产生,就需要保证每个协议参与者不能够引入非正阶的任何元素.

对于攻击者要检查是否满足下面两个条件:

①所有攻击者知道的消息一定要是正阶的.

②$\vdash$ 关系不影响正阶.也就是只有正阶的消息能够由正阶的消息集合产生.

定义 4 保持正阶(maintains positive ρ)的迹 tr 特性描述如下:

maintains positive $\rho(tr)\Leftrightarrow(\text{send}.a.b.m \text{ in } tr \vee \text{signal}.c.a.b.m \text{ in } tr)\wedge\rho(m)\leqslant 0\Rightarrow\exists$ receive. $a'.b'.m'$ in $tr\cdot\rho(m')\leqslant 0$

上面的定义表示阶为非正的输入消息一定要先于阶为非正的输出消息.

下面给出针对 CSP 操作符的阶函数保持正阶的证明规则:

stop 规则:Stop *sat maintains* ρ

输出规则:$\dfrac{P \textit{ sat maintains } \rho}{\textit{trans}.i.j.m\rightarrow P \textit{ sat maintains } \rho}[\rho(m)\geqslant 1]$

输入规则:$\dfrac{\forall j,x(\rho(f(x))\geqslant 1\Rightarrow(P(j,x) \textit{ sat maintains } \rho}{\textit{rec}.i?\ j?\ f(x)\rightarrow P(j,x) \textit{ sat maintains } \rho}$

选择规则:$\dfrac{\forall j\cdot V_j \textit{ sat maintains } \rho}{W_jV_j \textit{ sat maintains } \rho}$

3.3.2 序列完整性证明

首先给出序列完整性的阶函数证明定理.

定理 1 如果

$R1$:$\forall m\in INIT\cdot\rho(m)\geqslant 1$,*INIT* 是攻击者的初始知识集合.

$R2$:$\forall S,m\cdot((\forall s\in S\cdot\rho(s)\geqslant 1)\wedge S\vdash m\Rightarrow\rho(m)\geqslant 1)$,$S$ 是整个协议的消息集合.

$R3$:$\forall t\in T\cdot\rho(t)\leqslant 0$.

$R4$:$\forall a\in HOST\cdot \text{Responder}_a\rightarrow R$ sat maintains positive ρ,R 为协议运行后产生的路径序列

则对每个 a 有(Network) sat PathIntegrity(Responder, Initiator,$\{D,P,C\}$)

证明 假设 $R1\sim R4$ 成立而存在 Network 不满足 PathIntegrity,则存在迹 tr 产生路径 T 不等路径 R,根据 $R3$ 有 $\rho(t)\leqslant 0$,也就是在 tr 上有一消息的阶小于 0.假设 tr_0 是迹 tr 的前缀,它的最后一个消息的阶小于 0.

那么该消息有两种可能:receive. $i.j.x$ 和 send. $i.j.x$,即 i 从 j 发送和接收消息 x,其中 $\rho(x)\leqslant 0$.

当消息为 receive. $i.j.x$ 时,我们有 tr_0 是攻击者的一个迹.由文献[8]中定理 3.1 知攻击者初始集合$\cup$接收消息集合$\vdash$发送消息集合,也就是能够产生消息 x.而根据假设 tr_0 中除最后一个消息外其它消息阶为正,进一步根据 $R1$,$R2$ 可得 $\rho(x)\geqslant 1$,则同假设矛盾.

当消息为 send. $i.j.x$ 时,我们有 tr_0 是 responder 迹的一部分,且由假设知 send. $i.j.x$ 前有 receive. $i.m$.根据 $R4$ 知 Responder 满足 maintains positive,即$(\forall m\in tr_0\Downarrow rec.i\cdot\rho(m)\geqslant 1)\Rightarrow(\forall m\in tr_0\Downarrow \text{send}.i\cdot\rho(m)\geqslant 1)$,则得到 $\rho(x)\geqslant 1$,同假设矛盾.

因此定理得证.

根据定理 1 可以讨论 PM 协议是否能够保持序列完整性,即希望能够证明:Initiator||Responder||Intruder $\{INIT\}$ sat PathIntegrity($\{D,P,C\}$).这里需要考虑三种情况:

(1)攻击者不掌握响应者密钥

如果攻击者不掌握响应者的密钥,则 $K^{-1}_{responders}\notin INIT$,则要证明在这种情况下攻击者不能够伪造一路径证据,使得该路径证据同另一路径证据相同.因此,可建立下列阶函数.

$\rho(u)=1,u\in HOST$

$\rho(t)=1$

$\rho(\Pi)=1$

$\rho(k_i^+)=1$

$$\rho(s_i^{-1})=\begin{cases}0,\text{if } i\in HOST\\1,\text{otherwise}\end{cases}$$

$$\rho((m)_{s_i^{-1}})=\begin{cases}\rho(m)+1,\text{if } i\in HOST\\\rho(m),\text{otherwise}\end{cases}$$

$\rho(m_1,m_2)=\min\{\rho(m_1),\rho(m_2)\}$

在该阶函数下,验证协议是否能够满足以下几个方面:

■ 所有阶为 0 和更少的消息都不能被攻击者知道.

■ ⊢能够保持正阶.检查协议中所有消息,总能够保证发送非正消息之前必接收一非正消息.

■ 当攻击者采用所掌握的密钥对消息进行签名,试图产生路径证据时,由 $\rho(s_i^{-1})=0$,知其存在 $\rho(t)\leqslant 0$.即该证据不能被协议正常接受.

■ 对应所有的协议参与者检查是否都有 Initator ‖ Responder sat maintains positive ρ,因为根据 CSP 模型中的描述 Initator 执行 send. $i_0.i_1.(\Pi_0,M_0)$或 receive. $i_n.i_0.(\Pi_0,M_0,\cdots,M_n)$,$\Pi_0=(\Pi,t)$和 $\rho(\Pi,t)=1$ 知初始消息为正阶,因为我们这里只考虑完整性,因此对 M_0 中不考虑 D_0,而只考虑 C_0,由 $C_0=(P_0,\Pi_0,i_1)_{S_i^{-1}}$和 $\rho((m)_{s_i^{-1}})=\rho(m)+1$ 知其发送消息为正阶.同理可知响应者使用自身密钥对消息签名都保持正阶,因此发送的消息都为正阶.因此上述条件能够满足.在这种情况下协议的路径完整性能够保持.

(2)攻击者掌握一个响应者密钥

如攻击者掌握了一个协议响应者的密钥,$j\in Responsers$,$K_j^{-1}\in INIT$ 则构造如下的阶函数,在该阶函数下验证以下条件.在该条件下,我们不考虑移动代理两次经过该响应者节点的情况,因为该情况实质上等同于情况(3).

$$\rho(u)=1,u\in HOST$$

$$\rho(t)=1$$

$$\rho(\Pi)=1$$

$$\rho(k_i^+)=1$$

$$\rho(s_i^{-1})=\begin{cases}0,\text{if } i\in HOST,i\neq j\\1,\text{otherwise}\end{cases}$$

$$\rho((m)_{s_i^{-1}})=\begin{cases}\rho(m)+1,\text{if } i\in HOST,i\neq j\\\rho(m)-1,i=j\\\rho(m)\quad,\text{otherwise}\end{cases}$$

$$\rho(m_1,m_2)=\min\{\rho(m_1),\rho(m_2)\}$$

■ 所有阶为 0 和更少的消息都不能被攻击者知道.

■ ⊢能够保持正阶.检查协议中所有消息,总能够保证发送非正消息之前必有接收一非正消息.

■ 当攻击者采用所掌握的密钥对消息进行签名,试图产生路径证据时,由 $\rho(m)-1$,知其存在 $\rho(t)\leqslant 0$.即该证据不能被协议正常接受.

■ 对应所有的协议参与者检查是否都有 Initator ‖ Responder sat maintains positive ρ,因为初始消息都为正阶,此时我们只考虑响应者的情况,或 receive. $i_j.i_{j-1}.(\Pi_0,M_0,\cdots,M_{j-1})$,或 send. $i_j.i_{j+1}.(\Pi_0,M_0,\cdots,M_j)$,当响应者的密钥不被攻击者掌握时,由 $\rho((m)_{s_i^{-1}})=\rho(m)+1$ 知 $\rho(\text{send. } i_j.i_{j+1}.(\Pi_0,M_0,\cdots,M_j))=2$,而当使用泄漏的密钥对消息加密后,由 $\rho((m)_{s_i^{-1}})=\rho(m)-1$ 知其发送消息的阶降 1,$\rho(\text{send. } i_j.i_{j+1}.(\Pi_0,M_0,\cdots,M_j))=1$,但此时响应者仍能够保持阶函数为正.因此这种情况下协议也能够保持路径的完整性.

(3)攻击者掌握两个响应者密钥

如攻击者掌握了两个协议响应者的密钥,$i,j\in Responsers$,$K_i^{-1},K_j^{-1}\in INIT$ 则构造如下的阶函数.该种情况下阶函数类似情况(2),同样在该阶函数下验证以下几种情况:

■ 所有阶为 0 和更少的消息都不能被攻击者知道.

■ ⊢能够保持正阶.检查协议中所有消息,总能够保证发送非正消息之前必有接收一非正消息.

■ 当攻击者采用所掌握的密钥对消息进行签名,试图产生路径证据时,由 $\rho(m)-1$,知其存在 $\rho(t)\leqslant 0$.即该证据不能被协议正常接受.

■ 对应所有的协议参与者检查是否都有 Initator ‖ Responder sat maintains positive ρ,因为初始消息都为正阶,当节点 i 使用泄漏的密钥对消息加密后,由 $\rho((m)_{s_i^{-1}})=\rho(m)-1$ 知其发送消息的阶降 1,$\rho(\text{send. } i_i.i_{i+1}.(\Pi_0,M_0,\cdots,M_i))=1$,当响应者 i 将此消息发送给另一泄漏密钥响应者 j 时,j 再次次使用泄漏的密钥对消息加密后,则 $\rho(\text{send. } i_j.i_{j+1}.(\Pi_0,M_0,\cdots,M_j))=0$,即消息的阶降 0,此时响应者不能够保持阶函数为正.因此这种情况下协议也不能够保持路径的完整性.

在这种情况下,攻击者能够构造一个证据,使得该证据同另外一条路径的证据相同,因此在这种情况下路径的完整性不能够保证,情况(2)在移动代理两次经过密钥泄漏节点时也会产生同样的情况.

4　方法比较

Raja[4,5]尝试使用基于符号迹的形式化方法对 PM 协议进行描述,并使用 STA 工具对该协议进行了分析验证,但没有给出通用的形式化模型,且缺少对非可信协议参与者的描述,因此无法描述和发现合谋攻击情况.Xavier Hannotin 和 Paolo Maggi[1,3]分别使用 CSP 和 SPI 方法对 MADIPP 进行建模,并对数据完整性属性进行了形式化表示,通过分析可以看出,其数据完整性的形式化表示等同于认证性的形式化表示,这对于传统的消息认证协议来说存在一定的合理性,但对于 MADIPP 来说,则会导致很多类攻击无法分析.

文献[6]也使用了基于符号迹的方法进行了形式化分析,但同 Raja 等人一样,该文中没有给出通用形式化模型,对数据完整性的规约也沿袭了传统的认识,从而造成对截断攻击的分析能力不足.

目前 MADIPP 的形式化分析方法还很欠缺,没有对完整性属性这一根本性的问题进行深入的探讨,已有文献所给出的完整性定义都过于含糊和抽象,无法真正应用于实际分析.因此,本文重新给出了数据完整性定义,同时给出了可以应用于具体形式化验证的完整性规约,

这为 MADIPP 的形式化分析打下了基础.此外使用 CSP 方法对 MADIPP 进行了形式化建模,特别对不可信节点和攻击节点的行为及知识进行了形式化描述.在此基础上,对一个具体协议进行了分析,验证了模型及完整性属性的有效性.

参考文献:

[1] X Hannotin, P Maggi, Riccardo Sisto. Formal specification and verification of mobile agent data integrity properties: a case study[A]. Mobile Agents: 5th International Conference[C]. Atlanta, GA, USA, 2001.41.

[2] P Ryan, 等著, 张玉清, 等译. 安全协议的建模与分析[M]. 北京, 机械工业出版社, 2005.
P Ryan, S Schneider, M Goldsmith. Modelling and Analysis of Security Protocols[M]. Addison-Wesley, 2001.

[3] P Maggi, R Sisto. Experiments on formal verification of mobile agent data integrity properties[A]. Workshop on Objects and Agents 2002(WOA2002)[C]. Milano, Italy, 2002.131 - 136.

[4] Raja Al-Jaljouli. A Proposed Security Protocol for Data Gathering Mobile Agents[R]. The University of New South Wales, Report, Sydney, Australia, 2004.

[5] Raja Al-Jaljouli. Formal Methods in the Enhancement of the Data Security Protocols of Mobile Agents[R]. The University of New South Wales, Report, Sydney, Australia, 2005.

[6] 李鹏飞, 卿斯汉, 马恒太, 等. 新颖的移动代理动态数据完整性保护协议[J]. 通信学报, 2007, 28(8): 1 - 10.
Li Pengfei, Qing Sihan, Ma Hengtai. Novel mobile agent dynamic data integrity protection protocol[J]. Journal on Communications, 2007, 28(8): 1 - 10. (in Chinese)

[7] P Maggi, R Sisto. A configurable mobile agent data protection protocol[A]. AAMAS'03[C]. Melbourne, Australia, 2003. 851 - 858.

[8] S A Schneider. Verifying authentication protocols with CSP[J]. IEEE Transactions on Software Engineering. 1998, 24(9): 741 - 758.

[9] S A Schneider. Formal analysis of a non-repudiation protocol [A]. 11th Computer Security Foundations Workshop [C]. Rockport Massachusetts: IEEE Computer Society Press, 1998. 54 - 65.

[10] G Karjoth, N Asokan, C Gulcu. Protecting the computation results of free-roaming agents[J]. Personal and Ubiquitous Computing, 1998, 2(2): 92 - 99.

[11] G Lower. A hierarchy of authentication specification[A]. Proceedings of the 10th IEEE Workshop on Computer Security Foundations[C]. IEEE Computer Society, Washington, DC, USA, 1997.31 - 43.

作者简介:

李鹏飞 男, 1974 年生于河北定州, 博士生, 主要研究方向: 分布式系统安全、移动代理系统及其安全性、安全协议分析.
E-mail: pfli@ios.cn

马恒太 男, 1970 年生于山东临朐, 副研究员, 主要研究方向: 大型网络信息安全、卫星网络安全.