软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(Suppl.(2)):9−16

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

针对移动代理数据完整性保护协议的一种攻击*

马恒太+, 李鹏飞

(中国科学院软件研究所 综合信息系统技术国家级重点实验室,北京 100190)

A Kind of Attack to Free Roaming Mobile Agent Data Integrity Protection Protocol

MA Heng-Tai+, LI Peng-Fei

(National Key Laboratory of Integrated Information System Technology, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

+ Corresponding author: E-mail: hengtai@iscas.ac.cn

Ma HT, Li PF. A kind of attack to free roaming mobile agent data integrity protection protocol. ***Journal of Software***, **2011,22(Suppl.(2)):9−16.** http://www.jos.org.cn/1000-9825/11022.htm

Abstract: This paper focuses on attacking the construction problem and reports research on the colluded attack construction method for free roaming mobile agent data integrity protection protocol with data integrity definition. The formal specification method, and suggests a new attack on Cheng-Wei protocol. In this attack, two colluded hosts can truncate the data collected by using a mobile agent in some probability. This kind of attack is effective on mobile agent data integrity protection protocol based on proof chain.

Key words: security protocol; mobile agent; data integrity protection protocol; attack to data integrity protocol

摘 要: 针对自由漫游移动代理数据完整性协议的攻击构造问题,使用已提出的数据完整性定义和形式化规约方法,研究了移动代理数据完整性保护协议合谋攻击构造方法,提出了一种针对 Cheng-Wei 协议的新型概率攻击方法,该攻击在存在两个合谋攻击节点的情况下,能够在一定概率上形成对数据的截断攻击.该攻击方法对目前采用证据链进行数据完整性保护的移动代理数据完整性保护协议都有效.

关键词: 安全协议;移动代理;数据完整性协议;完整性协议攻击

移动代理技术被认为是未来网络计算发展的一种新的计算模式,特别适合在电子商务领域应用.自由漫游移动代理是指代理在移动过程中能够根据其自身环境来动态确定下一个要移动到的节点.自由漫游移动代理面临两大问题:一是如何防止恶意代理对代理平台的攻击,另一个是如何防止恶意代理平台对移动代理的攻击.前一问题已找到一些有效的解决方案[1−4],并在实际应用中得到验证;后一问题相对难以解决,目前很多研究工作都是针对这一问题,自由漫游移动代理数据保护协议是其中的一种解决方法.

自由漫游代理的动态数据保护协议最初由 Yee 提出,其思想是采用部分结果签名验证机制来对数据进行保护,Karjoth 和 Asokan 等人[5]对 Yee 的思想进行了发展,提出了一个协议族来保证自由漫游代理在运行过程中动态数据的完整性和私密性等安全属性.随后,出现了一系列自由漫游代理数据保护协议[2,6,7],Roth[8,9]对这些协议进行了分析,认为这些协议都存在问题,其主要原因是:没有对协议的执行轮次进行唯一标识.我们分析认为

* 基金项目: 中国科学院国防创新基金(CXJJ-10-M20)
收稿时间: 2011-02-15; 定稿时间: 2011-07-28

导致[9]中攻击方法可行的另一前提是协议中存在合谋节点.如 Roth[9]提出了一个新协议试图解决他发现的问题,但仍存在合谋情况下的数据截断攻击.

2002 年,Cheng 和 Wei[10]提出了一个新协议方案,能够防止对自由漫游移动代理计算结果的截断攻击,特别是能防止两节点合谋的截断攻击,该协议在大多数情况下是有效的.Cheng-Wei 还对 Karjoth 等提出的一些安全属性进行了扩展,对完整性保护的内容进行了细化.Zhou[11]对 Cheng-Wei 提出的协议进行了分析,认为这一协议在一些特殊情况下还存在攻击,如当移动路径出现重复节点时,重复节点同其它恶意节点合谋就能够对代理收集的数据进行截断攻击.文献[13,14]也指出了这种攻击的存在,并分别给出了自己的解决办法.

目前的研究认为[10,11−13],提出的协议能够有效防止两个攻击者对移动代理收集数据的攻击,而在出现多个合谋攻击者时,协议才会失效.我们研究发现该协议在只有两个攻击者时也仍能对已收集的数据进行截断攻击,原因来自于移动代理数据完整性定义.为此,作者在文献[14]中提出了新的完整性定义及两条规约,这两条规约能够覆盖 Kajoth 和 Cheng 等人所提出的完整性保护内容,并提出了基于阶函数的移动代理数据完整性协议的形式化分析方法,以此方法分析了 PM 协议的安全性.该方法的关键在于阶函数构造,阶函数的正确性决定了分析效果,但阶函数的正确性证明是困难的,因此必须对发现的问题进行攻击构造,只有可以构造出有效的攻击过程,才能证明所发现的问题是实际可用的和真实有效的.

本文采用文献[14]的完整性定义及规约,重点研究针对移动代理数据完整性协议的攻击构造方法,以 Cheng-Wei 协议为例,介绍一种新颖的概率攻击构造方法,该攻击深刻揭示了文献[14]的完整性定义所反映的代理数据间的关联意义和完整性规约所反映的证据链关联强度的内涵.本文第 1 节简要介绍 Cheng-Wei 协议.第 2 节介绍采用的数据完整性定义及形式化规约.第 3 节对 Cheng-Wei 的协议进行了分析,给出了该协议中存在的一种新攻击形式.第 4 节是总结.

1 移动代理完整性保护协议

首先简要介绍 Cheng-Wei 协议[10].该协议中,移动代理从主机 S_0 出发在网络上漫游,动态选择要经过的主机 $S_1,\ldots,S_n$,并在这些主机上运行,得到相应的执行结果,然后携带执行结果返回 S_0.该协议主要保证移动代理所收集数据的完整性,为了避免 Roth[9]发现的交错攻击,协议使用联合签名机制来防止对代理收集数据的插入和删除等攻击.联合签名是指一个主机在将移动代理发送到下一个主机前,要将下一主机的标识和自己执行代理所得到的加密数据等一起送给前一主机进行签名,这样将下一主机和本次主机的结果形成一个签名链,这样在返回 S_0 后,发起者就可以根据这个签名链来验证结果集的完整性和主机序列的唯一性.

表 1 是协议所使用的符号语义表.协议包括:代理创建,代理在 S_1 上的迁移和代理在 $S_i(2\leqslant i\leqslant n)$上的迁移.

Table 1 symbol semantics list

表 1 符号语义表

$S_0=S_n+1$	协议的发起者
S_i, $1\leqslant i\leqslant n$	代理执行主机
o_i, $1\leqslant i\leqslant n$	主机平台s_i所提供的数据,s_i的标识在O_i中显式出现
O_i, $1\leqslant i\leqslant n$	主机平台s_i所提供数据的加密结果
h_i, $1\leqslant i\leqslant n$	将O_i和下一跳在一起进行完整性检查的验证值
$O_0,O_1,\ldots,O_n$	对主机平台所提供结果的加密链
r_i	由s_i产生的随机数
$(v_i,\overline{v}_i)$	s_i公私钥对
$(\mu_i,\overline{\mu}_i)$	s_i的临时公私钥对
$Enc_v(m)$	使用s_i的公钥v_i对消息m进行加密
$Sig_{\overline{v}_i}(m)$	使用s_i的私钥$\overline{v}_i$对消息m进行签名
Ver(σ,v)	使用公钥v对签名σ验证的函数
$H(m)$	单向无碰撞的Hash函数
$[m]$	通过加密信道发送消息m
A→B:m	A发送消息m给B

代理创建:

1. 结果封装

S_0:$h_0=H(r_0,s_1)$

S_0:$O_0=Sig_{\bar{v}_0}(Enc_{v_0}(o_0,r_0),I,h_0,\mu_1)$

S_0:$\sigma_0=Sig_{\bar{v}_0}(h_0)$

2. 代理迁移

$S_0\rightarrow s_1$:$O_0,[\bar{\mu}_1,\sigma_0]$

代理在主机S_1上的迁移:

3. 代理验证

s_1:接收$O_0,[\bar{\mu}_1,\sigma_0]$

s_1:Ver(O_0,v_0),并恢复出 I,h_0,μ_1

s_1:Ver(O_0,v_0)

4. 结果交互封装

s_1: $h_1=H(O_0,r_1,s_2)$

$s_1\rightarrow S_0$:$temp_1=Enc_{v_0}(Sig_{\bar{v}_1}(o_1,\sigma_0),r_1),h_1,\mu_2)$

S_0: $O_1=Sig_{v_0}(temp_1)$

$S_0\rightarrow s_1$:O_1

s_1: $Ver(O_0,v_0),\sigma_1=Sig_{\bar{v}_1}(h_1)$

5. 代理迁移

$s_1\rightarrow S_0$: $O_0,O_1,[\bar{\mu}_2,\sigma_0,\sigma_1]$

代理在主机$S_i(2\leqslant i\leqslant n)$上的迁移:

6. 代理验证

s_i:接收$O_0,\ldots,O_{i-1},\bar{\mu}_i,\sigma_{i-2},\sigma_{i-1}$

s_i:Ver(O_0,v_0),并恢复出I,h_0,μ_1

s_i:Ver(O_1,v_0),并恢复出h_1,μ_2

s_i:Ver(O_k,μ_{k-1}),并恢复出$h_k,\mu_{k+1}(2\leqslant k\leqslant i-1)$

s_i:Ver(σ_{i-2},v_{i-2}),Ver(σ_{i-1},v_{i-1})

s_i:验证$S_{i-2}\neq s_{i-1}$

7. 结果交互封装

s_i:$h_i=H(O_{i-1},r_i,s_{i+1})$

$s_i\rightarrow s_{i-1}$:$temp_i=Enc_{v_0}(Sig_{\bar{v}_i}(o_i,\sigma_{i-2},\sigma_{i-1}),r_i),h_i,\mu_{i+1})$

s_{i-1}:$O_i=Sig_{\bar{\mu}_{i-1}}(temp_i)$

$s_{i-1}\rightarrow s_i$:O_i

s_i:$Ver(O_i,\mu_{i-1}),\sigma_i=Sig_{\bar{v}_i}(h_i)$

8. 代理迁移

$s_i\rightarrow s_{i+1}$:$\{O_k|0\leqslant k\leqslant i\},[\bar{\mu}_{i+1},\sigma_{i-1},\sigma_i]$

协议还规定在 s_i 和 s_{i-1} 之间必须要进行相互的认证,且 s_{i-1} 要保存其上执行过的代理的记录,保证对 s_i 一个代理只能执行一次联合签名.同样该协议还要求每个代理所经过的主机 s_i 也应该对消息的链式签名进行验证,并拒绝第 2 次来自 s_{i-1} 的同一代理.

Zhou 等人[11]对以上协议进行了分析,发现当代理在漫游中如果两次经过某一主机 s_i,即存在 s_i 后的某一主机 $s_{i+2}=s_i$,则此时由于 s_i 掌握 s_{i+1} 的临时签名私钥 $\bar{\mu}_{i+1}$,s_i 可以同后面的某一主机 s_w 合谋,截断 s_{i+k} 和 s_w 之间的节点所提供的数据 $O_{i+k+1},\ldots,O_{w-1}$.Zhou 等人在文献[12]中提出了对 Cheng-Wei 协议的改进,但对 Cheng-Wei 协议的整体框架影响不大.因此本文主要针对 Cheng-Wei 协议进行分析.

2 移动代理数据完整性规约

Karjoth[5]将移动代理数据完整性划分为转发完整性,抗插入攻击和抗截断攻击等内容.Cheng-Wei 以及 Zhou 都延用了这种划分,Maggi 在文献[15]中给出了一个移动代理数据完整性的详细定义:假设移动代理实际收集到的数据为$\{d_1,\ldots,d_k\}$,而应该收集到的数据为$\{d'_1,\ldots,d'_k\}$,数据的强完整性表示为:如果 s_0 接到数据后,可以判断是否$\{d_1,\ldots,d_k\}\neq\{d'_1,\ldots,d'_k\}$,并细分为转发完整性和抗数据截断完整性,定义如下:

弱转发完整性:假设 $s_1,\ldots,s_m$ 是移动代理所经过的可信路径,也就是从移动代理发起者到第 1 个恶意节点之间所访问过的节点,则回到代理发起节点 s_0 可以判断是否$\{d_1,\ldots,d_i\}\subseteq\{d_1,\ldots,d_k\}$.

强转发完整性:假设移动代理经过可信节点 s_m,则移动代理的发起者可以判断任何 $d_j(1\leqslant j<m\leqslant k)$是否被修改.

强抗数据截断完整性:当移动代理返回到发起节点后,如果 s_0 可以判断任何对所收集的数据的截断攻击,则数据的强抗数据截断完整性可以保证.也就是当接收到数据$\{d_1,\ldots,d_j,d_{m+1},\ldots,d_k\}(1\leqslant j<m\leqslant k)$,$s_0$ 可以发现数据的完整性被破坏.

弱抗数据截断完整性:假设移动代理经过可信节点 s_j 后,从此可信节点以后的数据被截断,返回到移动代理发起节点 s_0 后,s_0 可以判断数据的完整性被破坏.

上述定义对完整性的强弱划分不清晰,如弱转发完整性考虑的是删除对数据完整性的影响,而强转发完整性考虑的是修改对数据完整性的影响.强转发完整性并不能包括弱转发完整性.强抗数据截断完整性虽然能够完全包括弱抗数据截断完整性,但其定义过于抽象,可操作性不强,难以用于对移动代理完整性进行分析.因此作者在文献[14]中对移动代理的完整性进行了重新定义.

定义协议发起者 s_0 在一次协议执行完后收到数据为$\{d_1,\ldots,d_k\}$,该次协议执行的参与主机为$\{s_1,\ldots,s_k\}$,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$\{d_1,\ldots,d_k\}$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,完整性的保证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,完整性可以通过认证性来保证,即 $Agreement(receiver,sender,\{d\})$,通过文献[16,17]可以清楚地得到这一点,目前很多移动代理完整性的形式化分析正是基于这一点,简单地将证明认证性等同于证明了完整性.

自由漫游移动代理数据保护协议是一个多方链式签名协议,完整性的保证不仅要满足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的一组参与者$\{s_1,\ldots,s_k\}$参与了该协议,并且该证据不可伪造.

移动代理数据协议要保证定义给出的完整性需满足下面两个规约[14],下面是采用 CSP 的形式化描述:

规约 1:数据完整性规约.

$$\mathrm{DataIntegrity}(\mathrm{Responder},\mathrm{Initiator},\{\mathrm{D}\})\mathrm{A}(s_0\in\mathrm{Initiator},\forall\, d_i\in D)(\mathrm{Signal.\ Running.\ Initiator.}\ s_0?s_n?d_i)$$
$$\rightarrow (s_i\in Responder,1\leqslant i\leqslant n)(Signal.\ Commit.\ Responder.\ s_i?s_0?d_i)\rightarrow STOP$$

其中,D 为协议初始发起者所接收到的数据集合,s_0 和 s_i 分别为协议的初始发起者和协议的响应者,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.

规约 2:参与者序列完整性规约.

$$PathIntegrity(Responder,Initiator,\{D,P,C\})\mathrm{A}(Signal.Running.Initiator.\ s_0?s_nD?P?C)$$
$$\rightarrow (P\subseteq Responder,s_i\in P,1\leqslant i\leqslant n)(Signal.Commit.Responder.s_i!s_0!c_i(c_i\in C))$$
$$\wedge(\neg\exists S(S\neq P)\subseteq Responder,s_j\in S,1\leqslant j\leqslant n)(Signal.Commit.Responder.s_j!s_0!c_i(c_i\in C))$$

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 $E_A=E_B(A\neq B)$,其中 B 为不等于 A 的节点序列.

3 攻击构造及分析

根据上述完整性规约,自由漫游移动代理的数据完整性必须要保证主机序列的唯一性,也就是保证只依靠攻击者本身不能够构造主机序列的证据.据此对Cheng-Wei 协议进行分析,可以发现当两个攻击者相邻时,可以合谋对代理漫游路径进行修改,并重构路径的证据,而协议在有些情况下并不能避免和发现路径被修改,因此攻击者能够对代理所收集的数据实施截断攻击.

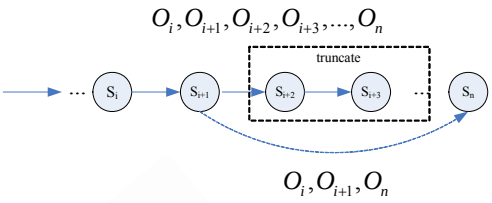

Fig.1 Attack context

图 1 攻击场景

攻击场景如图 1 所示.自由漫游移动代理访问了主机节点 $S_i,s_{i+1},s_{i+2},\ldots,s_n$,得到数据 $O_i,O_{i+1},\ldots,O_n$ 当 S_i,s_{i+1} 两主机节点合谋时,则在有些时候可以将 s_{i+1} 后的某一段数据删除.

未攻击时代理在 s_i 上的执行:

s_i: $h_i=H(O_{i-1},r_i,s_{i+1})$

$s_i\rightarrow s_{i-1}$:$temp_i=$

$Enc_{v_0}(Sig_{\overline{v}_i}(o_i,\sigma_{i-2},\sigma_{i-1}),r_i),h_i,\mu_{i+1})$

s_{i-1}: $O_i=Sig_{\overline{\mu}_{i-1}}(temp_i)$

$s_{i-1}\rightarrow s_i$: O_i

s_i: $Ver(O_i,\mu_{i-1}),\sigma_i=Sig_{\overline{v}_i}(h_i)$

$s_i\rightarrow s_{i+1}$:$\{O_k|0\leqslant k\leqslant i\},[\overline{\mu}_{i+1},\sigma_{i-1},\sigma_i]$

未攻击时代理在 s_{i+1} 上的执行:

s_{i+1}: $h_{i+1}=H(O_i,r_{i+1},S_{i+2})$

$s_{i+1}\rightarrow s_i$:$temp_{i+1}=$

$Enc_{v_0}(Sig_{\overline{v}_{i+1}}(o_{i+1},\sigma_{i-1},\sigma_i),r_{i+1}),h_{i+1},\mu_{i+2})$

s_i: $O_{i+1}=Sig_{\overline{\mu}_i}(temp_{i+1})$

$s_i\rightarrow s_{i+1}$:O_{i+1}

s_{i+1}: $\mathrm{Ver}(O_{i+1},\mu_i),\sigma_{i+1}=Sig_{\overline{v}_{i+1}}(h_{i+1})$

$s_{i+1}\rightarrow s_{i+2}$:$\{O_k|0\leqslant k\leqslant i+1\},[\overline{\mu}_{i+2},\sigma_i,\sigma_{i+1}]$

下面给出具体攻击过程分析,假设移动代理已经过的主机节点为 $...,s_i,s_{i+1},s_{i+2},s_{i+3}...,s_n$,所收集到的数据加密结果为 $...,O_i,O_{i+1},O_{i+2},O_{i+3},...,O_n$,攻击节点为 s_i,s_{i+1},两者在代理所经过的主机节点序列上前后相邻(因为 S_i 可自由选择其后继节点,因此只要存在合谋节点,即可实现相邻),并且根据Dellvo-Yao模型假设攻击者能够对整个网络的公共信道有完全控制的能力,能够任意截获网络信道上传递的数据包.

s_i,s_{i+1} 开始正常执行协议,在自身平台执行代理后,根据代理执行情况选择下一主机节点 s_{i+2},并将代理迁移到该主机,协议正常执行.当攻击者发现代理经过同自身有竞争关系的节点后,就可能发起攻击.这时攻击者要想替换一个能够到达协议发起者 s_0 的消息,则必须要能够破坏协议所提供的对数据完整性规约的保护机制,也就是能够使得 s_0 接收到攻击者所篡改的数据后,认为是攻击者假冒的被攻击者所发送的.证明协议是否满足这一规约可以通过证明 s_0 接收到某消息 m 后,必有协议参与者 s_B 发送了这一消息 m[16].攻击者对参与者序列完整性的攻击会造成将参与协议主机产生的数据截断,要防止这一攻击,需要协议保证参与者序列证据的唯一性,即仅依靠攻击者不能构造出新的参与者序列和证据使得协议发起者不能验证该证据和参与者序列不一致.

分析该协议发现,虽然单独攻击者,或两个不相邻的攻击者合谋时不能随意修改参与者序列并构造证据,但当两个攻击者连续分布时,如 s_i,s_{i+1} 两者合谋,在特定时候就能够产生一条新的参与者序列,并构造一个不可区分的证据为 s_0 接受.

假如移动代理执行到 s_{n-1},并且准备将数据和代理移动到 s_n,这时攻击者要想截断节点 $s_{i+2},\ldots,s_{n-1}$,则 s_i,s_{i+1} 可将 s_{n-1} 发给 s_n 的数据包拦截,并由 s_{i+1} 将自己的下一个要迁移到的节点改为 s_n,并将由 s_i 签名后的消息发送给 s_n.s_i 和 s_{i+1} 在攻击时的执行情况如下:

攻击时代理在 s_i 上的执行:

s_i:$O_{i+1}=Sig_{\overline{\mu}_i}(temp_{i+1})$

$s_i\rightarrow s_{i+1}$:O_{i+1}

攻击时代理在 s_{i+1} 上的执行:

s_{i+1}:$h_{i+1}=h(O_i,r_{i+1},s_n)$

$s_{i+1}\rightarrow s_i$:$temp_{i+1}=Enc_{v_0}(Sig_{\overline{v}_{i+1}}(o_{i+1},\sigma_{i-1},\sigma_i),r_{i+1}),h_{i+1},\mu_{i+2})$

s_{i+1}: $Ver(O_{i+1},\mu_i)$, $\sigma_{i+1}=Sig_{\overline{v}_{i+1}}(h_{i+1})$

$s_{i+1}\rightarrow s_n$:$\{O_k|0\leqslant k\leqslant i+1\},[\overline{\mu}_{i+2},\sigma_i,\sigma_{i+1}]$

虽然 Cheng-Wei 协议规定了前一节点只能对后一节点发来的同一代理的消息进行一次签名,但两个合谋攻击者完全可以不遵守此规定,攻击者 s_i 可以对 s_{i+1} 发送来的消息再次签名.这样节点 s_n 以为收到了 s_{i+1} 的代理及数据包,则按照协议及其自身情况选择下一节点 s_{n+1}.

这时攻击者将先前拦截的 s_{n-1} 发给 s_n 的数据包继续发送,这时 s_n 收到 s_{n-1} 发送的数据包,按照协议是可以继续执行的,这时 s_n 又可以根据其自身情况选择下一节点,假如 s_n 选择的节点还为 s_{n+1},执行如下:

s_n: $h_n=H(O_{n-1},r_n,s_{n+1})$

$s_n\rightarrow s_{n-1}$:$temp_n=Enc_{v_0}(Sig_{\overline{v}_n}(o_n,\sigma_{n-2},\sigma_{n-1}),r_n),h_n,\mu_{n+1})$

s_{n-1}: $O_n=Sig_{\overline{\mu}_n}(temp_n)$

$s_{n-1}\rightarrow s_n$: O_n

s_n:$Ver(O_n,\mu_{n-1}),\sigma_n=Sig_{\overline{v}_n}(h_n)$

$s_n\rightarrow s_{n+1}$:$\{O_k|0\leqslant k\leqslant n\},[\overline{\mu}_{n+1},\sigma_{n-1},\sigma_n]$

根据协议 s_{n+1} 将消息的链式签名进行验证,并拒绝第 2 次来自 s_n 的同一移动代理及其数据包,而此时根据协议 s_n 也不能另选一节点,因为那样将得不到 s_{n-1} 的签名,这样 s_{n-1} 所携带的数据包将被丢弃.这样攻击者 s_i,s_{i+1} 就将根据协议将最初 $s_{i+2},\ldots,s_{n-1}$ 收集的数据完全抛弃掉,然后重新构造一新的数据串 O_i,O_{i+1},O_n,这就造成了对原有数据的截断攻击.

假如 s_n 选择的节点不为 s_{n+1},而是 s_{i+1},则这时 s_i,s_{i+1} 的此次攻击无效,但 s_i,s_{i+1} 还可以继续此次攻击,再次直接将 s_{i+1} 的下一节点选择为 s_{i+1},执行同上描述的动作,则在 s_{i+1} 两次选择同一后继节点的情况下,攻击者就能够完成对原有数据的截断攻击.

攻击者可以重复以上动作,直到 s_i,s_{i+1} 向所有可能节点都发送了数据包后,所有的节点都不再接收来自 s_{i+1} 的数据包,则此时攻击失败.

对上述攻击进一步分析可知,协议存在该攻击的原因在于协议不能满足上节所提到的参与者序列完整性规约.也就是当移动代理经过参与者序列 $P=\langle s_1,\ldots,s_i,s_{i+1},\ldots,s_n,s_{n+1},\ldots\rangle$ 时,其证据 E 包括在数据串为 $O_1,\ldots,O_i,O_{i+1},\ldots,O_n,O_{n+1},\ldots$ 中,协议要保证数据的完整性,应保证攻击者不能构造证据 E',证明协议经过的参与者序列为 P',且 $P\neq P'$.而根据上面所给出的攻击,该协议中攻击者根据协议可以构造证据 $E_A=O_1,\ldots,O_i,O_{i+1},O_n,O_{n+1},\ldots$,该证据对应的参与者序列为 P_A,这就使得协议经过的参与者序列 $P\neq P_A$,而攻击者能够构造 $E=E_A$,这明显违背了参与者序列完整性规约,从而导致数据截断攻击.

4 总 结

文献[13]中我们曾分析,当使用回溯联合签名协议时,向后回溯一位联合签名可以防止两个攻击者的合谋攻击,但不能防止 3 个攻击者合谋攻击,尽管 Zhou[11]提出当出现循环时则会造成两个攻击者合谋能够对协议成

功攻击的情况,但这种情况由于循环两次经过同一节点,因此可认为是 3 个攻击者合谋.采用本文方法分析该协议的路径完整性属性可以发现,该协议仍可采用本文攻击方法进行两攻击者合谋攻击,但此攻击存在一定的成功概率,攻击成功的概率取决于节点在两次接收到同一代理发送的数据包并处理后,选择同一迁移目标节点的概率.在自由漫游情况下,假设攻击节点以后参与协议的不同节点数量为 n,每个节点相邻的可达节点数量为 m,则当攻击者执行一次攻击动作时,成功概率为 $1/m$.如果攻击者重复该攻击,则最大成功概率为 $1-(1-1/m)^{n-1}$.

本文提出了一种针对移动代理数据完整性保护协议的新颖攻击方法,该攻击方法深刻揭示了移动代理数据间关联对完整性保护的重要意义和证据链关联强度的内涵.该文攻击方法对 Cheng-Wei[10],Zhou[11],Xu[12],Li[13]等协议都有效,这些协议之所以不能抵抗这一攻击的原因源于其所参照的数据完整性定义,未能将精确的数据完整性规约有效应用于自由漫游移动代理协议设计.其中移动代理完整性属性的精确规约,及基于数据完整性定义和数据完整性规约,设计可动态配置的移动代理数据保护协议都是值得深入研究的课题.

References:

[1] Lucco S, Sharp O, Wahbe R. Omniware: A universial substrate for web programming. In: Proc. of the 4th Int'l World Wide Web Conf. 1995.

[2] Karnik NM, Tripathi AR. Security in the Ajanta mobile agent system. Technical Report, TR-5-99, Minneapolis: University of Minnesota,. 1999.

[3] Ousterhout J, Levy J, Welch B. The Safe-TCL security model technical reports. Sun Microsystems, 1996.

[4] Tardo J, Valenta L. Mobile agent security and telescript. In: Proc. of the IEEE COMPCON'96. 1996.

[5] Karjoth G, Asokan N, Gulcu C. Protecting the computation results of free-roaming agents. In: Proc. of the 2nd Int'l Workshop on Mobile Agents. 1998. 223−234.

[6] Corradi A, Montanari R, Stefanelli C. Mobile agents protection in the Internet environment. In: Proc. of the 23rd Annual Int'l Computer Software and Application Conference (COMPSAC'99). 1999. 80−85.

[7] Karjoth G. Secure mobile agent-based merchant brokering in distributed marketplaces. In: Kotz D, Mattern F, eds. Proc. of the ASA/MA 2000. LNCS 1882, Berlin, Heidelberg: Springer-Verlag, 2000. 44−56.

[8] Roth V. On the robustness of some cryptographic protocols for mobile agent protection. In: Proc. of the Mobile Agents 2001. LNCS 2240, Springer-Verlag, 2001.

[9] Roth V. Empowering mobile software agents. In: Suri N, ed. Proc. of the 6th IEEE Mobile Agents Conf. LNCS 2535, Spinger-Verlag, 2002. 47−63.

[10] Cheng J, Wei V. Defenses against the truncation of computation results of free-roaming agents. In: Proc. of the 4th Int'l Conf. on Information and Communications Security. LNCS 2513, 2002. 1−12.

[11] Zhou JY, Onieva JA, Lopez J. Analysis of a free roaming agent result-truncation defense scheme. In: Proc. of the Int'l Conf. on E-Commerce Technology. 2004.

[12] Xu DR, Luo JZH. An improved free-roaming mobile agent security protocol against colluded truncation attacks. In: Proc. of the 30th Annual Int'l Computer Software and Applications Conf (COMPSAC 2006). 2006.

[13] Li PF, Qing SH, Ma HT, Deng Y. Novel mobile agent dynamic data integrity protection protocol. Journal on Communications, 2007,28(8):1−10 (in Chinese with English abstract).

[14] Li PF, Ma HT, Hou YW, Qiu T. Research on formal analyses method of mobile agent data integrity protocol. Acta Electronic Sinica, 2009,37(8):1669−1674 (in Chinese with English abstract).

[15] Maggi P, Sisto R. A configurable mobile agent data protection protocol. In: Proc. of the AAMAS 2003. 2003.

[16] Ryan P, Schneider S, Goldsmith M, Wrote; Zhang YQ, Mo Y, Wu JY, Trans. Modelling and analysis of security protocols. Beijing: China Machine Press, 2001 (in Chinese).

[17] Lower G. A Hierarchy of Authentication Specification. IEEE Computer Society Press, 1997. 31−43.

附中文参考文献:

[13] 李鹏飞,卿斯汉,马恒太,邓勇.新颖的移动代理动态数据完整性保护协议,通信学报,2007,28(8):1−10.

[14] 李鹏飞,马恒太,侯玉文,邱田.移动代理完整性协议形式化分析方法研究,电子学报,2009,37(8):1669−1674.

[16] Ryan P, Schneider S, Goldsmith M,著;张玉清,莫燕,吴建耀,译.安全协议建模与分析.北京,机械工业出版社,2005.

马恒太(1970－),山东临朐人,男,博士,副研究员,主要研究领域为卫星组网与信息安全.

李鹏飞(1974－),男,博士,副研究员,主要研究领域为网络安全与信息保密.