基于 Petri 网的密码协议形式化建模

白云莉[1,2] 叶新铭[1]

(内蒙古大学计算机学院 呼和浩特 010021)[1]

(内蒙古农业大学计算机与信息工程学院 呼和浩特 010018)[2]

摘 要 密码协议是安全共享网络资源的机制和规范,是构建网络安全环境的基石,其安全性对整个网络环境的安全起着至关重要的作用。提出了采用 Colored Petri Nets(CPN,着色 Petri 网)分析密码协议的新方法。采用新方法对 TMN 协议的多次并发会话通信进行形式化建模,模型依据会话配置和会话顺序进行功能单元划分,采用 on-the-fly 方法生成攻击路径。采用状态空间搜索技术,发现了该协议的多次并发会话不安全状态,并获得了新的攻击模式。

关键词 密码协议,TMN,CPN,多次并发会话

中图法分类号 TP393.06 **文献标识码** A

Formal Modeling of Cryptographic Protocols Using Petri Nets

BAI Yun-li[1,2] YE Xin-ming[1]

(College of Computer Science, Inner Mongolia University, Hohhot 010021, China)[1]

(College of Computer and Information Engineering, Inner Mongolia Agricultural University, Hohhot 010018, China)[2]

Abstract Cryptographic protocol is secure mechanism for sharing network resources, is the cornerstone to build security network environment. The security of the cryptographic protocol plays a vital role to entire network environment. A new colored Petri nets (CPN) methodology for security analysis of cryptographic protocol was proposed. We applied the new approach to model TMN protocol with multi concurrent session, and the model was categorized based on session configuration and session schedule. And the attack traces were obtained using on-the-fly method. Using the state space search method, several attack states of multi concurrent session were found, and a new attack pattern was obtained.

Keywords Cryptographic protocol, TMN, CPN, Multi concurrent session

1 引言

密码协议是以密码学为基础的消息交换协议,其目的是在网络环境中避免恶意方攻击,从而达到预定安全目标。有很多种密码协议的应用,包括:认证协议、密钥交换协议、电子商务协议、电子银行协议、电子投票协议等。由于与日俱增的攻击能力和应用需求的复杂化,使得设计与分析密码协议越来越困难。大多密码协议的攻击是在使用很多年之后才发现的。因此对密码协议进行形式化建模,对其所存在的攻击进行分析是非常有价值的。常用的形式化分析方法有:BAN 逻辑法、进程代数法、串空间、π 演算和 Petri 网。其中 Petri 网具有异步并发特性,与物理系统极其接近,适合于描述网络体系结构、服务和协议,此外它采用直观的图形表示,具有严密的数学理论和丰富的分析技术,便于进行协议的验证工作。以往基于 Petri 网的密码协议分析与验证工作主要是针对单会话过程进行的。本文提出了一种新的基于 Colored Petri Nets(CPN,着色 Petri 网)的密码协议多并发会话的形式化建模方法,并以密钥交互协议——TMN 协议为例说明了新方法的有效性。我们在模型检测工具 CPN Tools 中实现了新方法,有效地控制了状态空间爆炸,得到了其新的多次并发会话不安全状态,采用 on-the-fly 方法获得了攻击路径。

有很多工作采用 Petri 网对密码协议进行了分析[7,13]。绝大多数的工作主要集中在分析密码协议单会话协议执行过程[9-12]。Al-Azzoni[8]采用 CPN 对密码协议进行了多会话通信分析,但作者没有对整个状态空间进行详细分析,同时主要分析的是两个会话的顺序执行,并且攻击者不能初始化会话,使得攻击能力受到很大影响。

文献[4]采用运行模式分析法对 TMN 协议进行分析,发现该协议包括单会话和多会话 19 个攻击。Lowe 等人[7]采用 CSP 发现和总结了 TMN 协议及改进协议的 10 余种攻击。本文采用具有较强图形化表示和分析能力的 CPN 对 TMN 进行建模分析,获得了不安全状态,并发现了新的多次并发会话攻击模式。

2 Colored Petri Net (CPN) 和 CPN Tools 介绍

定义 1 Colored Petri Net 是一个八元组 $CPN=(P,T,$

到稿日期:2011-10-13 返修日期:2012-02-20 本文受国家自然科学基金项目(61163011),国家重点基础研究发展规划(973)项目(2007CB310702),内蒙古自然科学基金重点项目(20080404ZD20)资助。

白云莉(1977—),博士生,副教授,主要研究领域为计算机网络与网络安全,E-mail:baiyunli@vip.imau.edu.cn;叶新铭(1943—),教授,博士生导师,CCF 高级会员,主要研究领域为计算机网络与分布式系统。

A,C,V,G,E,I),其中,

P:是一个有限库所集合。

T:是一个有限变迁集合,满足 $P\cap T=\emptyset$。

A:$A\subseteq P\times T\cup T\times P$ 是有向弧的集合。

C:是有限非空类型 Color Set 的集合。

V:是有限变量的集合,对所有变量 $v\in V$ 满足 $TYPE[v]\in C$。

G:$T\rightarrow$EXPRv 是防卫表达式,每个变迁有一个防卫表达式,例如:TYPE $[G(t)]$=Bool。

E:$A\rightarrow$EXPRv 是弧表达函数,它为每个弧分配一个表达式,例如:弧 a,Type$[E(a)]=C(p)_{MS}$,p 是与 a 弧连接的位置。

I:$P\rightarrow$EXPR$\emptyset$ 是初始化函数,它给每个位置一个初始化表达式,例如:Type $[I(p)]=C(p)_{MS}$。

CPN 中的颜色集,即集合 C,代表相应库所的数据类型。CPN 的数据类型包含基本数据类型和复合数据类型。基本数据类型有字符串型(string)、整型(int)、布尔型(bool)和单元型(unit)等 4 种。复合数据类型主要有 product 型、列表型(list)、记录型(record)以及联合型(union)等。

Colored Petri Net (CPN) (Jensen,1997)非常适合对同步通信的系统进行建模和验证。CPN 具有的层次建模和标记语言特性适合于对安全协议进行验证分析。CPN Tools[1] 是专门针对 CPN 进行建模和分析开发的工具。作者提出了一种新的基于 CPN 的安全协议多并发会话建模方法,并采用 CPN Tools 对 TMN 协议多会话并发通信进行了建模、模拟、状态空间分析、攻击路径生成等工作。

3 密码协议建模方法

Petri 网作为密码协议分析和设计的典型形式化模型之一,已被广泛采用。使用 Petri 网能够为密码协议的设计与分析提供有力的支持,但即便是一个小的系统,Petri 网也面临状态空间爆炸的问题,难以进一步分析和验证。造成状态空间爆炸的主要原因有,采用基于 Dolev-Yao 模型的攻击者具有较强的能力,可以发送"任意"消息组合,协议参与者的"任意"并发会话导致协议运行的多样性。

攻击者遵循 Dolev-Yao 模型[2],其具备的能力包括:

(1)攻击者具有窃听、篡改、丢包等功能;

(2)攻击者可以初始化会话;

(3)攻击者可以伪装成其他实体;

(4)当知道解密密码时能够解密密文。

本文提出的基于 CPN 的密码协议建模方法有以下几个特点:

(1)攻击者知识分解:在不削减攻击者能力的前提下,将攻击者的知识分解成分解消息、合成消息和原子消息。攻击者只能发送合成消息,从而有效地限制了攻击者的"任意"消息组合操作。

(2)会话设置功能分解:定义密码协议多会话参与模式和会话顺序,将密码协议进行功能单元(Function Unit)分解。一种功能单元分析协议的一类执行情况,从而有效地控制了状态空间。

(3)提出一种简单、有效的 on-the-fly 生成攻击路径的方法。

3.1 攻击者知识分解

将攻击者操作分成两个阶段:消息分解和消息合成。攻击者截获消息后,尽可能地将消息分解,然后再将分解后的消息合成新消息。采用 3 个多重集(Multi Sets,MS)DB、AD 和 CB 取代原有攻击者模型中的消息状态。DB 集用于存储分解和待分解的消息,AB 集用于存储分解过程中得到的原子消息,CB 集用于存储合成和待合成的消息。

攻击者截获消息后,将其添加到 DB 集中开始分解消息。消息被分解成最小的单位后,就可以转移到合成消息 CB 集中。在转移过程中,需要一些过渡规则来限制转移的消息是最小单位。为了使分解合成操作不构成循环,我们首先应用所有可应用的分解规则,然后应用合成规则来合成消息。其中,只有 CB 集中的合成消息才可以发送到通道(channel)上。

$\forall A$:princ　　/*协议实体

$\forall B$:princ　　/*协议实体

$\forall t,t_1,t_2$:msg　　/*通道上的消息

$\forall a$:AB　　/*原子消息

$\forall k,k'$:Key　　/*协议实体的密钥 k'可以解密密钥 k 加密的消息

(1) 分解规则:

channel$(A,t,B)\rightarrow DB(t)$;

channel$(A,t)\rightarrow DB(t)$;

$DB(t_1t_2)\rightarrow DB(t_1)++DB(t_2)$;

$DB(\{t\}k)AB(k')\rightarrow DB(t)AB(k')$。/*$\{t\}k$ 表示采用密钥 k 对消息 t 加密

(2) 合成规则:

$CB(t)\rightarrow$channel(A,t,B);

$CB(t)\rightarrow$channel(A,t);

$CB(t_1)++CB(t_2)\rightarrow CB(t_1t_2)$;

$CB(t)AB(k)\rightarrow CB(\{t\}k)AB(k)$。

(3) 过渡规则:

$DB(a)\rightarrow AB(a)$;

$DB(\{t\}_k)\neg AB(k')\rightarrow CB(\{t\}_k)$。

3.2 会话设置功能分解建模方法

多数密码协议攻击都是在多次并发会话通信过程中进行的。本文针对多次并发会话情况进行建模,以三方参与的密码协议即通信实体 A、B 以及第三方服务实体 J 为例加以说明。模型假设诚实实体 A 和 B 参与并且只参与一次会话,攻击者分别伪装成诚实实体 A 或 B 进行攻击,但不对服务实体 J 进行攻击。

下面给出密码协议多会话参与模式和会话顺序的定义,将密码协议进行模块分解,一种模块分析协议的一类执行情况。

定义 2 密码协议 CPN 模型的会话配置为 colset config=product $Sid_i*I_{11}*I_{12}*\cdots*I_{1n}*I_{21}*I_{22}*\cdots*I_{2n}$,$1\leqslant i\leqslant m$,$m$ 为并发会话的次数,n 为参与密码协议会话的通信实体个数。

其中:

Sid_i:会话标识;/*多次并发会话中的会话标识

$I_{11},I_{12},\cdots,I_{1n}$:实际的会话参与者;

$I_{21},I_{22},\cdots,I_{2n}$:对应的会话参与者采用的身份,即 I_{2i} 对应的会话参与者为 I_{1i},$1\leqslant i\leqslant n$。

定义 3 密码协议 CPN 模型的会话顺序为 colset Step=list st;colset st=product Sid_i*N_j,$1\leqslant i\leqslant m$,$1\leqslant j\leqslant n$,m 为并发会话的次数,n 为密码协议一次会话的步骤总数。

其中：

Sid_i：会话标识；

N_j：会话的步骤数；

st：表示会话的顺序列表。

两次并发会话的顺序可以有很多种组合，但其主要的会话顺序为顺序攻击会话和中间人攻击会话。

顺序攻击会话：

step1=[(1,1),(1,2),…,(1,n),(2,1),(2,2),…,(2,n)]；

中间人攻击会话：

step2=[(1,1),(2,1),(2,2),(1,2),…,(1,$n-1$),(2,$n-1$),(2,n),(1,n)]。

3.3 On-the-fly 攻击路径生成方法

密码协议工作过程通常分为几个步骤执行，即在几个参与会话的诚实实体之间交互消息，从而达到安全目标，例如，分配密钥或通过认证。当分析带有攻击者的密码协议模型的状态空间时，对于存在漏洞的密码协议，可能会得到不安全状态、不安全状态的可达性，以及从初始状态到不安全状态的可达路径，从这个可达路径中提取实体(包括攻击者)之间交互的消息后即可得到攻击路径。CPN Tools 工具中提供 off-the-fly 方式的攻击路径生成方法，即工具可产生状态空间，通过安全属性查询不安全状态，然后采用状态空间搜索法找出每个可达路径，提取攻击路径。本文采用一种简单、有效的 on-the-fly 攻击路径生成方法，它不用搜索整个状态空间，就能将攻击路径的交换消息存放在不安全状态的标记中。采用一个融合库所(Fusion State)将实体之间交互的消息存放在该库所的列表颜色集 trace 中。颜色集 trace 的具体定义如下：

colset msg=union id_1[:name1]+id_2[:$name_2$]+…+id_n[:$name_n$];/*其中 n 为消息类型数，$name_i$ 代表第 i 个消息的类型，$1 \leqslant i \leqslant n$ */

colset trace=list msg。

4 TMN 协议的描述及分析

TMN 协议是由 Tatebayashi. M, Matsuzaki. N 和 Newman. D[3] 设计的密钥交互协议。TMN 协议是针对移动通信系统中两个通信主体(初始发起者、响应者)基于可信第三方(服务者)在公开通道上安全地通信而设计的。通信双方首先要建立一个不能让攻击者知道的安全会话密钥，基于此共享密钥进行加密通信。

协议过程描述如下：

1. $A \rightarrow J$: $(B, ENC_{K_{jp}}(K_{aj})), A$

2. $J \rightarrow B$: A

3. $B \rightarrow J$: $(A, ENC_{K_{jp}}(K_{ab})), B$

4. $J \rightarrow A$: $B, ENC_{K_{aj}}(K_{ab})$

其中，A 为初始发起者，B 为响应者，J 为服务者。

$ENC_{K_{jp}}(K_{aj})$ 是用 J 的公钥 K_{jp} 加密 A 的新鲜密钥 K_{aj}。$A \rightarrow J$: $(B, ENC_{K_{jp}}(K_{aj}))$ 表示 A 向 J 发送消息 $(B, ENC_{K_{jp}}(K_{aj}))$。$K_{ab}$ 为通信双方 A 和 B 建立的安全会话密钥。

对 TMN 协议进行分析后得出，基于两次并发的会话配置主要有如下 4 种：

1. (1,A,B,A,B) & (2,In,In,A,B)；

2. (1,A,In,A,B) & (2,In,B,A,B)；

3. (1,In,B,A,B) & (2,A,In,A,B)；

4. (1,In,In,A,B) & (2,A,B,A,B)。

例如：(1,In,In,A,B)表示会话 1 中攻击者为初始者并且攻击者伪装成诚实实体 A，同时攻击者为响应者并且攻击者也伪装成诚实实体 B。

两次并发会话顺序主要考虑顺序攻击序列和中间人攻击会话，即

顺序攻击会话：

step1=[(1,1),(1,2),(1,3),(1,4),(2,1),(2,2),(2,3),(2,4)]；

中间人攻击会话：

step2=[(1,1),(2,1),(2,2),(1,2),(1,3),(2,3),(2,4),(1,4)]。

5 TMN 协议的 CPN 模型及分析

5.1 TMN 协议的 CPN 模型

图 1 给出了协议模型中的部分数据类型和函数声明。

```
类型声明
colset I=with A|B|In;
colset K=with Kaj|Kjp|Kjpr|Kab|Ki;
colset C=product K*K;
colset M=product I*C;
colset MI=product I*C*I;
colset DB=union cC:C;
colset AB=union ak:K;
colset CB=union crp:C;
colset sid=INT;
colset No=INT;
colset st=product sid*No;
colset Step= list st;
colset config=product sid*I*I*I*I;
colset tr=union b1:MI+b2:I+b3:MI+b4:M;
colset trace=list tr;
函数声明
fun DecryKey(k:K):K
fun SharedKey(i:I):K
```

图 1 TMN 协议模型的声明

TMN 协议顶级 CPN 模型如图 2 所示。模型由 A、B、J 和 $Intruder$(攻击者) 4 个实体组成。攻击者能够截获诚实实体之间的所有会话。模型只考虑一个攻击者的情形，攻击者具备创建、修改以及重放消息等功能。

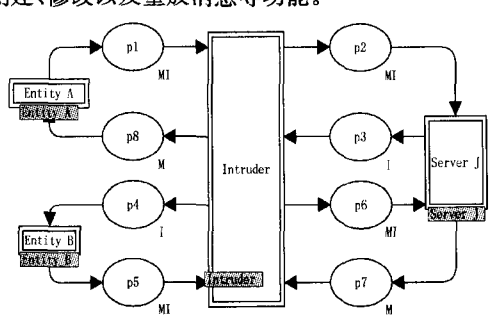

图 2 带攻击者的 TMN 协议顶级 CPN 模型

图 3 显示了实体 A 的模型。变迁 $T1$ 创建协议第一步所要发送的消息。变迁 $T3$ 和 $T4$ 处理协议第四步接收的信息。库所 $c1$ 中存储会话配置，形如(sid_i, i_1, i_2, src, des)。库所 step 中存储会话顺序采用 list(列表)表示，形如 ls=[(1,1),(1,2),(1,3),(1,4),(2,1),(2,2),(2,3),(2,4)]。

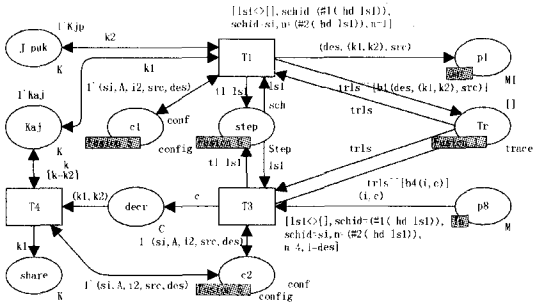

图 3　实体 A 的模型

实体 A 的会话配置中要求实际的初始者为 A。会话顺序当前列表头中的会话标识 schid=(#1(hd ls))，满足：schid=sid_i，其中 sid_i 为会话配置中的会话标识。此外变迁 $T1$ 在会话顺序当前列表头中的会话步骤数为 1 时可以点火，变迁 $T3$ 和 $T4$ 在会话步骤数为 4 时可以点火。

攻击者的功能根据 TMN 协议的 4 个步骤，建立了 4 个页面，其分别对应协议的 4 个步骤。下面以协议第一步为例说明攻击者模型的建模方法。攻击者针对协议第一步的攻击模型如图 4 所示。变迁 $t1$ 截获在协议第一步中传送的消息。库所 dcom 中存储分解和待分解的消息，库所 com 中存储合成和待合成的消息，库所 Atom 中存储原子消息。变迁 $t2$ 将采用攻击者的分解规则后形成的原子消息保存到库所Atom。变迁 $t3$ 将采用攻击者的过度规则无法解密的消息以过度规则保存到库所 com。变迁 $t4$ 采用攻击者的合成规则把原子消息合成后保存到库所 com。融合库所 $c2$ 中存储会话配置。融合库所 step 中存储会话顺序。

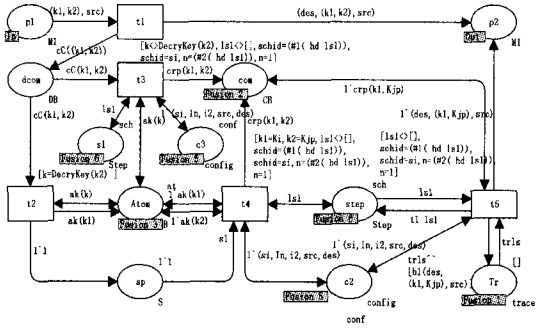

图 4　攻击者-1 的模型

攻击者的协议第一步模型的会话配置中要求实际的初始者为 In。会话顺序当前列表头中的会话标识 schid=(#1(hd ls))，满足 schid= sid_i，其中 sid_i 为会话配置中的会话标识。此外所有变迁在会话顺序当前列表头中的会话步骤数为 1 时可以点火。

5.2　TMN 协议的安全属性验证及分析

状态空间分析工具(State Space)可以对 CPN 模型进行状态空间以及可达性分析，完整的状态空间能够给出模型的所有执行情况。本文基于模型的状态空间，采用时序逻辑 ASKCTL 验证 TMN 协议的安全属性，采用查询语句(query)分析协议的攻击状态(不安全状态)，并对不安全状态通过 on-the-fly 方法得到其攻击序列，分析其真伪性。

(1)安全属性

密钥交互协议的安全属性要求所产生的共享会话密钥满足相等性和保密性。

• 相等性：指协议参与方的相应共享会话密钥，即诚实实体 A 的 $Share_A$ 和实体 B 的 $Share_B$ 相等：$Share_A=Share_B=K_{AB}$；

• 保密性：指诚实实体间的共享会话密钥 K_{AB} 不被攻击者获得：$K_{AB}\notin AB\cup DB\cup CB$。

(2)状态空间报告

本文针对 TMN 两次并发会话的 4 种会话配置和 2 种会话顺序进行了模型的功能单元划分分析。8 种功能单元的状态空间报告如表 1 所列。针对 8 种功能单元的状态空间报告分析得出协议模型没有活锁(Livelocks)和死锁(Deadlocks)。

表 1　状态空间部分分析报告

功能单元	会话顺序	会话配置	节点	弧
1	[(1,1),(1,2),(1,3),(1,4),(2,1),(2,2),(2,3),(2,4)]	(1,A,B,A,B) &(2,In,In,A,B)	3567	6609
2		(1,A,In,A,B) &(2,In,B,A,B)	1575	3169
3		(1,In,B,A,B) &(2,A,In,A,B)	4210	8216
4		(1,In,In,A,B) &(2,A,B,A,B)	2730	6483
5	[(1,1),(2,1),(2,2),(1,2),(1,3),(2,3),(2,4),(1,4)]	(1,A,B,A,B) &(2,In,In,A,B)	51904	124852
6		(1,A,In,A,B) &(2,In,B,A,B)	16415	32550
7		(1,In,B,A,B) &(2,A,In,A,B)	14916	35806
8		(1,In,In,A,B) &(2,A,B,A,B)	1974	4602

(3)TMN 协议的安全属性的 ASKCTL 验证

采用时序逻辑 ASKCTL 验证 TMN 密钥交互协议的安全属性。检验成功攻击，即诚实实体 A 和 B 获得相等的共享会话密钥，同时攻击者也截获到该密钥的 ASKCTL 公式为：

```
use (ogpath^"/ASKCTL/ASKCTLloader.sml");
fun secrecy n=cf(ak(Kab),Mark.step1'Atom 1 n)>0 andalso
              cf(Kab,Mark.Entity_A'share 1 n )>0 andalso
              cf(Kab,Mark.Entity_B's_key 1 n )>0;
fun EndSession n=cf (empty,Mark.Entity_A'step 1 n) > 0;
val sc= NF ("",secrecy);
val SessionEnds=NF ("",EndSession);
val myASKCTLformula=POS (AND(sc,SessionEnds)) ;
eval_node myASKCTLformula InitNode;
```

CPN tools 工具中采用时序逻辑 ASKCTL 检测 TMN 协议的安全属性的结果表明，存在满足相等性但不满足保密性属性的检验结果，即攻击者能够成功攻击的情况。结果表明，当诚实实体 A 和 B 获得了相等的共享会话密钥时，攻击者也同样截获到了该密钥。

(4)查询语句(Query)获得不安全状态

通过查询语句对状态空间中的终止状态(Dead Markings)分析后得出各个功能单元的消息秘密属性存在如下的违背结果。

```
SearchNodes(
  ListDeadMarkings (),
  fn n=> (cf(ak(Kab),Mark.step1'Atom 1 n)>0
  andalso cf(Kab,Mark.Entity_A'share 1 )>0)
  andalso cf(Kab,Mark.Entity_B's_key 1 n )>0,
  NoLimit,
fn n=> n,[],op ;)
```

其中，查询语句给出攻击者与实体 A 同时获得共享密钥 Kab 的不安全终止状态。同样可以查询攻击者与实体 A 同时获得其他共享密钥的不安全终止状态。

查询结果如下：

下面以功能单元 1 为例分析不安全状态及其攻击路径。其中对通过 on-the-fly 生成的攻击路径及采用 TMN 协议的执行过程进行了描述，S_{ij} ($i=1,2;j=1,2,3,4$)代表第 i 次会话的第 j 步。

·初始者 A 共享密钥：Kab；响应者 B 共享密钥：Kab；攻击者获得共享密钥：Kab。

$S_{11}.\ A\rightarrow J:(B,ENC_{K_{jp}}(K_{aj})),A$

$S_{12}.\ J\rightarrow B:A$

$S_{13}.\ B\rightarrow J:(A,ENC_{K_{jp}}(K_{ab})),B$

$S_{14}.\ J\rightarrow A:B,ENC_{K_{aj}}(K_{ab})$

$S_{21}.\ In\rightarrow J:(B,ENC_{K_{jp}}(K_i)),A$

$S_{22}.\ J\rightarrow In:A$

$S_{23}.\ In\rightarrow J:(A,ENC_{K_{jp}}(K_{ab})),B$

$S_{24}.\ J\rightarrow In:B,ENC_{K_i}(K_{ab})$

在功能单元 5 中获得了在文献[4,7]没有提到的新的攻击模式对应的攻击路径如下：

$S_{11}.\ A\rightarrow J:(B,ENC_{K_{jp}}(K_{aj})),A$

$S_{21}.\ In\rightarrow J:(B,ENC_{K_{jp}}(K_i)),A$

$S_{22}.\ J\rightarrow In:A$

$S_{12}.\ J\rightarrow B:A$

$S_{13}.\ B\rightarrow J:(A,ENC_{K_{jp}}(K_{ab})),B$

$S_{23}.\ In\rightarrow J:(A,ENC_{K_{jp}}(K_{ab})),B$

$S_{24}.\ J\rightarrow In:B,ENC_{K_i}(K_{ab})$

$S_{14}.\ J\rightarrow A:B,ENC_{K_{aj}}(K_{ab})$

结束语 随着密码协议的广泛应用，它的正确性和安全性越来越受到关注。形式化建模分析是验证密码协议的一种有效方法。以往的工作大多集中在对密码协议的单会话过程进行分析，本文使用有色 Petri 网对密码协议多次并发会话进行形式化建模和验证，并以 TMN 协议为例进行形式化分析，发现该协议具有多个攻击路径以及新的攻击模式。由于不断增加的密码协议的复杂性以及安全属性的多样性，今后课题组主要针对分析和验证新的安全性质，如非否认性、匿名性、公平性等开展研究工作。

参 考 文 献

[1] Jensen K, Kristensen L, Wells L. Coloured Petri Nets and CPN Tools for modelling and validation of concurrent systems[J]. International Journal on Software Tools for Technology Transfer (STTT), 2007, 9(3): 213-254

[2] Dolev D, Yao A. On the security of public key protocols. Information Theory[J]. IEEE Transactions on Information Theory, 1983, 29(2): 98-208

[3] Tatebayashi M, Matsuzaki N, Jr D B. Key distribution protocol for digital mobile communication systems[M]. Springer-Verlag, 1989: 324-333

[4] Yu-Qing Z, Xiu-Ying L. An Approach to the Formal Analysis of TMN Protocol[M]. Progress on Cryptography, 2004: 235-243

[5] Lowe G, Roscoe B. Using CSP to detect errors in the TMN protocol[J]. Software Engineering, IEEE Transactions on Software Engineering, 1997, 23(10): 659-669

[6] 薛锐，冯登国. 安全协议的形式化分析技术与方法[J]. 计算机学报，2006，29(1)：1-20

[7] Permpoontanalarp Y. On-the-Fly Trace Generation and Textual Trace Analysis and Their Applications to the Analysis of Cryptographic Protocols [M]. Formal Techniques for Distributed Systems, 2010: 201-215

[8] Al-Azzoni I, Down D, Khedri R. Modeling and verification of cryptographic protocols using coloured petri nets and design/CPN[J]. Nordic Journal of Computing, 2005, 12(3): 201-228

[9] 黎波涛，罗军舟. 不可否认协议的 Petri 网建模与分析[J]. 计算机研究与发展，2005，42(9)：1571-1577

[10] Tritilanunt S, Boyd C, Foo E. Using Coloured Petri Nets to Simulate Dos-resistant Protocols[C]// Proceeding of 7th Workshop and Tutorial on Practical Use of Coloured Petri Nets and the CPN Tools. 2006: 261-280

[11] Lee G, Lee J. Petri Net Based Models for Specification and Analysis of Cryptographic Protocols[J]. The Journal of System and Software, 1997, 37: 141-159

[12] Dresp W. Security Analysis of the Secure Authentication Protocol by Means of Coloured Petri Nets[C]// Proceeding of 9th IFIP Communication and Multimedia Security. 2005

[13] Permpoontanalarp Y, Changkhanak A. Security analysis of the TMN protocol by using Coloured Petri Nets: On-the-fly trace generation method and homomorphic property[C]// Computer Science and Software Engineering (JCSSE), 2011 Eighth International Joint Conference. 2011: 63-68

(上接第 58 页)

参 考 文 献

[1] 陈建民. 3G 时代手机病毒的威胁与移动安全[J]. 信息网络安全，2009(09)：19-20

[2] 朱圣军，刘功申，罗俊，等. 智能手机病毒与信息安全[J]. 信息安全与通信保密，2011(05)：96-100

[3] Grant. CNCERT 安全报告：软件漏洞成重大隐患[J]. 网络与信息，2011(04)：57

[4] 马云雷，刘功申，葛克为，等. 基于 Mobile 的手机杀毒软件设计与实现[J]. 信息技术，2011(01)：7-80

[5] 王磊，张玉清. WM 平台下反病毒软件的设计与实现[J]. 计算机工程，2009(21)：144-150

[6] 吴俊军，方明伟，张新访. 基于启发式行为监测的手机病毒防治研究[J]. 计算机工程与科学，2010(01)：35-38

[7] 杨建强，吴钊，李学锋. 增强智能手机安全的动态恶意软件分析系统[J]. 计算机工程与设计，2010(13)：2969-2971

[8] 刘鹏. 云计算[M]. 北京：电子工业出版社，2010：1-3

[9] 杨文志. 云计算技术指南：应用、平台与架构[M]. 北京：化学工业出版社，2010：7-12

[10] 瑞星云安全计划白皮书[EB/OL]. http://sec.chinabyte.com/113/8544113.shtml, 2011-4-20

[11] 趋势科技云安全白皮书[EB/OL]. http://sec.chinabyte.com/458/8546458.shtml, 2011-4-20

[12] 杨磊. 主机入侵防御系统的应用[J]. 计算机安全，2005(4)：20-22