基于 SPIN 的 IKEv2 协议高效模型检测

吴 昌,肖美华
WU Chang,XIAO Mei-hua

南昌大学 信息工程学院,南昌 330031
College of Computer Information and Engineering,Nanchang University,Nanchang 330031,China

WU Chang,XIAO Mei-hua.Effective model checking of IKEv2 protocol based on SPIN.Computer Engineering and Applications,2008,44(5):158-161.

Abstract: This paper first gives a simple introduction of the Internet Key Exchange Protocol IKEv2,then conducts a modeling and analysis of the protocol by using the famous model checking tool SPIN.The author finds the existing modeling method hardly applicable because of the highly complex structure of IKEv2 protocol,and that it can only be used for some simple protocols due to its poor readability,low automatization and verification efficiency.Thus the paper proposes another method of modeling which overcomes all the above mentioned disadvantages and which is particularly useful for complicated protocols.At last,the verification of the IKEv2 protocol model based on SPIN shows that this protocol is incapable of resisting initiative attack.Based on this discovery,two charts are given describing the attack and a personal view is presented to improve IKEv2 protocol's ability to protect the identity of initiator.

Key words: IKEv2;model checking;SPIN;Promela;IP Tunnel

摘 要:论文先简单介绍了互联网密钥交换协议 IKEv2,然后利用著名的模型检测工具 SPIN 对其进行了建模和分析。在建模的过程中,作者发现现有的建模方法很难对结构复杂的协议 IKEv2 进行建模,而且用现有的建模方法建立的模型可读性差、自动化程度不高,验证效率也比较低,因此现有的建模方法只适用于对简单协议进行建模。针对这些不足之处,提出了一种程序可读性、自动化程度及验证效率均较好的建模方法,而且这种建模方法特别适合对复杂的安全协议进行建模。最后利用 SPIN 对 IKEv2 协议的模型进行了验证,发现 IKEv2 协议不能抵御主动攻击,并给出了两个攻击序列图。针对 IKEv2 协议不能保护发起者身份的缺陷,提出了自己的一种改进意见。

关键词:IKEv2;模型检测;SPIN;Promela;IP 隧道
文章编号:1002-8331(2008)05-0158-04 **文献标识码:**A **中图分类号:**TP393.08

1 引言

计算机网络正在为人们提供越来越多的服务,为了保证这些服务的安全性和可靠性,人们需要借助于安全协议。然而,往往非常简单的安全协议也可能存在瑕癖,因此采取一定的方式对协议进行分析验证是必要的。形式化方法由于其准确性、简洁性以及无二义性的特点,已成为安全协议分析的一条可靠途径。目前常用的形式化分析方法有逻辑推证、模型检测及定理证明等,其中模型检测方法以自动化程度高、适用范围广而得到较广泛的应用,而 SPIN 就是一种著名的模型检测器,它非常适合对协议验证[4]。

IKE 是 IPSec 默认的密钥交换协议,它是一种混合协议,它的作用是在 IPSec 通信双方之间建立共享的安全参数以及认证的密钥,即建立安全联盟 SA。但正是由于种混和协议自身的复杂性,不可避免地带来一些安全及性能上的缺陷[1,5-8],导致其成为整个 IPSec 实现中的瓶颈。为此,IETF 一直对 IKE 不合理部分积极征集修改意见,陆续推出了 IKEv2 的草案,并于 2005 年 12 月 26 日正式推出了 IKEv2 的正式版本[2]。

2 IKEv2 简介

IKEv2 协商分为两个阶段,第一阶段称为初始交换(The Initial Exchange),第二阶段为产生子 SA 交换(The Create_Child_SA_Exchange),这两个阶段分别用于协商 IKE_SA 和 CHILD_SA。本文只对初始交换进行分析。初始交换的功能主要是为通信双方建立经过认证的安全信道,包括加密算法、密钥参数及信道的流量等。协议描述如下:

(1)I→R:HDR,SAi1,KEi,*Ni*

(2)R→I:HDR,SAr1,KEr,*Nr*

(3)I→R:HDR,*sk*{IDi,AUTH,SAi2,TSi,TSr}

(4)R→I:HDR,*sk*{IDr,AUTH,SAi2,TSi,TSr}

其中 I 和 R 分别表示发起者和响应者,HDR 表示消息头部,

基金项目:江西省自然科学基金(the Natural Science Foundation of Jiangxi Province of China under Grant No.0411041,No.0611057)。
作者简介:吴昌(1981-),男,硕士生,研究方向:模型检测,协议分析与验证;肖美华(1967-),男,教授,研究方向:软件形式化与可靠性、模型检测,协议分析与验证。
收稿日期:2007-06-05 **修回日期:**2007-08-20

SAi1 和 SAr1 分别表示由发起者提出的 SA 和响应者接受的 SA。KEi 和 KEr 分别表示发起者和响应者 DH(Diffie-Hellman)公共数，*Ni* 和 *Nr* 表示随机数(nonce)。*sk*{…}是消息 1，2 所得出的密钥，IDi 和 IDr 分别表示发起者和响应者的身份。AUTH 载荷数据用来进行认证，对于消息 3，它包括消息 1、*Nr* 和 prf(*sk*，IDi)的签名。对于消息 4，它包括消息 2、*Ni* 和 prf(*sk*，IDr)的签名。SAi2 和 SAr2 用来协商第一个 CHILD_SA。TSi 和 TSr 为通信选择器，用来对 IPSec 服务确定包流向。

3　SPIN 的工作机理

SPIN 是一种著名的用于对并发系统验证模型检测器，它尤其适合对协议验证[4]。它以 Promela 为输入语言，用线性时态逻辑(LTL)公式刻画系统必须满足的性质。验证过程中如果模型不满足 LTL 公式刻画的属性，则说明该协议存在缺陷或攻击，并且 SPIN 会给出一个反例。使用 SPIN 对协议进行验证和分析的过程如图 1 所示。

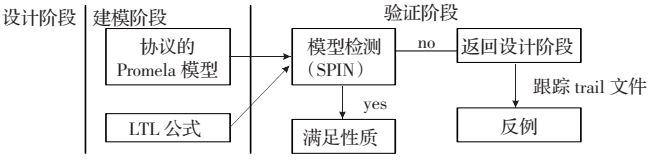


图 1　SPIN 验证模型

4　IKEv2 协议建模及检测结果的分析

4.1　对发起者和响应者建模

在该协议中，将在不安全网络上通信的主体抽象为诚信主体(发起者、响应者)和攻击者。建模的第一步是构造协议名称有限集合，其 Promela 语言描述如下：

mtype ={I，A，R，HDR，SAi1，SAr1，SAa1，KEi，KEr，KEa，*Ni*，Nr，Na，SAi2，SAr2，SAa2，IDi，IDr，IDa，TSi，TSr，TSa}

其中，I 表示发起者，SAi1 表示发起者提出的 SA，KEi 表示发起者的 DH 公共数，*Ni* 表示发起者随机数，SAi2 用来协商第一个 CHILD_SA，IDi 表示发起者的身份，TSi 为通信选择器。其它的协议名称含义类似。此外还需定义密钥和验证载荷的数据结构，根据 DH 算法的特点，采用文献[7]提出的利用交换的 DH 公共数来确定密钥，密钥和验证载荷的数据结构定义如下：

```
typedef DH_SK{
    mtype KE1;/* 发起方的 DH 公共数 */
    mtype KE2;/* 响应方的 DH 公共数 */
}
typedef AUTH{
    mtype N1;/* 发起方的 nonce*/
    mtype N2;/* 响应方的 nonce*/
    DH_SK sk;/* 密钥 */
    …;/* 其它变量 */
}
```

第二步，定义消息通道，由于消息 1、2 和 3、4 分别带有不同的数据结构，因此需定义两个通道，分别用于传递两类消息。其定义如下：

```
chan ca=[0] of {mtype,mtype,mtype,mtype,mtype,mtype};
chan cb=[0] of {mtype,mtype,mtype,mtype,AUTH,mtype,mtype,
mtype};
```

第三步，分别将发起者和响应者定义为一个进程，其模型如下：

```
active proctype PInitiator(){/* 发起者进程 */
    mtype data1,data2,data3,data4,ts;
    AUTH auth;
    atomic{
      if /* 选择通信参与方 */
       ::partnerI=A;ts=TSa /* 发起者 Initiator 希望以攻击者 At-
tacker 通信 */
       ::partnerI=R;ts=TSr /* 发起者 Initiator 希望以攻击者 Re-
sponder 通信 */
       fi;
       ca ! I,partnerI,HDR,SAi1,KEi,Ni;
    }
    atomic{
       ca ? eval (partnerI),eval (I),HDR,data1,data2,data3->
auth.N1=Ni;auth.N2=data3;auth.sk.KE1=KEi;auth.sk.KE2=data2;
       cb ! I,partnerI,HDR,IDi,auth,SAi2,TSi,ts;
    }
    atomic{
       cb ? eval (partnerI),eval(I),HDR,data1,auth,data4,eval
(TSi),eval(ts);
       ((auth.N1==Ni)&& (auth.N2==data3)&& (auth.sk.KE1==
KEi)&&(auth.sk.KE2==data2))->isFinishedI=1;/* 当发起者 Initiator 完
成协议的运行时，isFinishedI=1*/
    }
}
```

考虑到由并发进程相对执行速度的不确定性带来的影响，本文在发起者进程中引入了语句的原子序列 atomic，它表示该语句序列将作为一个不可分割的整体来执行，从而使得模型检测的效率有了一定程度的提高。由于篇幅有限，论文不给出验证结果的效率对比图，在此只给出与验证效率有关的一些数据。在引入了原子序列 atomic 的模型中，对模型的认证性和秘密性进行验证时状态迁移数，分别只需 41 个和 1 626 个，而没有原子序列的模型则分别需要 50 个和 1 734 个。可见引入原子序列 atomic 的模型验证效率比没有原子序列模型的验证效率均有一定程度的提高，而且随着协议结构的复杂性增大，其效率将会更加明显。

响应者进程与发起者进程类似，由于篇幅有限，不给出具体的代码。

4.2　对攻击者建模及验证效率分析

4.2.1　对攻击者建模

攻击者是抽象出来的能对网络和通信进行不良行为的一个主体，它可能存在网络的任何地方，并具有以下能力：

(1)可以在任何通信主体间截获或转发消息；

(2)攻击者可以以自己的身份冒充发起者 Initiator 或响应者 Responder；

(3)根据截获的消息增长自己的知识，以便重组消息；

(4)解密已知密钥的密文(完美加密假设：攻击者不解密不知解密密钥的密文)。

攻击者的模型完整描述如下：

```
active proctype PAttacker(){/* 攻击者进程 */
mtype data1,data2,data3,data4,data5,data6,id,sa,ts1,ts2,ts3,ts4;
  AUTH auth,auth1;
  mtype sender,receiver;
```

```
do
::ca ? sender,receiver,_,data1,data2,data3->
  if /* 存储拦截的数据或者转发消息 1 或消息 2*/
  ::data4=data1;data5=data2;data6=data3
  :: /* 重放数据包或重组数据包 */
    if /* 选择通信双方,I 表示发起者,R 表示响应者,A 表示攻击者 */
      ::sender=I;receiver=R
      ::sender=R;receiver=I
      ::sender=A;receiver=I
      ::sender=A;receiver=R
    fi;
    if
    ::skip /* 重放数据包 */
    ::/* 重组数据包 */
      if
      ::data1=SAi1;data2=KEi;data3=Ni
      ::data1=SAr1;data2=KEr;data3=Nr
      ::data1=SAa1;data2=KEa;data3=Na
      fi
    fi;
    ca ! sender,receiver,HDR,data1,data2,data3
  ::skip /* 丢去所截获的数据包 */
fi
::cb ? sender,receiver,HDR,id,auth,sa,ts1,ts2->
  if /* 存储拦截的数据或者转发消息 3 或消息 4*/
   ::data5 =id;auth1.N1 =auth.N1;auth1.N2 =auth.N2;auth1.sk.KE1=auth.sk.KE1;auth1.sk.KE2=auth.sk.KE2;data6=sa;ts3=ts1;ts4=ts2
   ::((auth.sk.KE1==KEi)&&(auth.sk.KE2==KEr))->
if
 ::((sender==I)&& (receiver==R))-> cb ! sender,receiver,HDR,id,auth,sa,ts1,ts2
 ::((sender==R)&& (receiver==I))-> cb ! A,receiver,HDR,id,auth,sa,ts1,TSa
 ::((sender==I)&&(receiver==A))-> cb ! sender,R,HDR,id,auth,sa,ts1,TSr
 ::((sender==R)&&(receiver==A))-> cb ! sender,I,HDR,id,auth,sa,TSi,TSr
 ::skip
 fi
::/* 重放数据包或重组数据包 */
 if
 ::((auth.sk.KE1==KEi)&&(auth.sk.KE2==KEa))->know_IDi=1
 ::((auth.sk.KE1==KEa)&&(auth.sk.KE2==KEr))->know_IDr=1
 fi;
if/* 选择通信双方,I 表示发起者,R 表示响应者,A 表示攻击者*/
 ::sender=I;receiver=R
 ::sender=R;receiver=I
 ::sender=A;receiver=I
 ::sender=A;receiver=R
fi;
if
::skip /* 重放数据包 */
::/* 重组数据包 */
  if
  ::know_IDi-> id=IDi;sa=SAi2
  ::know_IDr-> id=IDr;sa=SAr2
  ::id=IDa;sa=SAa2
  fi;
  (know_IDi || know_IDr)->
      if
      ::ts1=TSi;ts2=TSr
      ::ts1=TSi;ts2=TSa
      ::ts1=TSa;ts2=TSi
      ::ts1=TSa;ts2=TSr
      fi;
  if
   ::know_IDi->auth.N1=Ni;auth.N2=Na;auth.sk.KE1=KEi;auth.sk.KE2=KEa
    ::know_IDr ->auth.N1 =Na;auth.N2 =Nr;auth.sk.KE1 =KEa;auth.sk.KE2=KEr
    fi
 fi;
 cb ! sender,receiver,HDR,id,auth,sa,ts1,ts2
::skip /* 丢弃所截获的数据包 */
fi
od
}
```

4.2.2 验证效率分析

在整个建模过程中,对攻击者建模是建模的关键,也是建模的难点。作者开始试图采用文献[3]中 Maggi 提出的对攻击者建模的方法,然而在对 IKEv2 协议建模过程中发现,用这种建模方法很难对结构复杂的 IKEv2 协议进行建模,它只适用于对简单协议建模。虽然作者做了大量的工作,但最终未能成功地运用 Maggi 提出的方法对 IKEv2 协议进行建模。从文献[3]中的 NS 协议的模型可知,Maggi 提出的建模方法的程序可读性差、自动化程度不高,验证效率也比较低。针对这些不足之处,提出了一种程序可读性、自动化程度及验证效率均较好的建模方法。提出的建模方法符合程序设计的思维方式,因而程序的可读性好,用户比较容易掌握,而且攻击者截获消息后的行为是由程序自动生成的,因而自动化程度高。两种建模方法的认证性效率如表 1 所示。

IKEv2 协议比 NS 协议复杂得多,但从表 1 可以看到,用提出的方法对它们建模时,验证的复杂度并没明显增加,它并不

表 1 两种建模方法的性能比较

建模方法	建模对象	建模难易程度	可读性	自动化程度	验证效率		适用范围
					存储的状态数(stored states)	状态迁移数(transitions)	
文献[3]中Maggi 提出的方法	NS 协议	较难	差	低	154	335	适用于简单协议
本文提出的方法	NS 协议	易	好	高	23	26	简单协议和复杂协议均适用
	IKEv2 协议	易	好	高	29	41	

会因为协议结构的复杂性增大，而使得对攻击者建模的难度和验证时的复杂度明显增加，因此这种建模方法比较适合对结构复杂的协议进行建模。

4.3　协议性质的 LTL 描述

IKEv2 密钥交换协议需满足通信协议的认证性和秘密性.。认证性是指能够确认对方的真实身份，保证对方的真实身份与消息中声称的身份相一致。秘密性是指保证需要保密的协议消息内容，在传送过程中不被非法窃取。该模型的 LTL 公式描述如下：

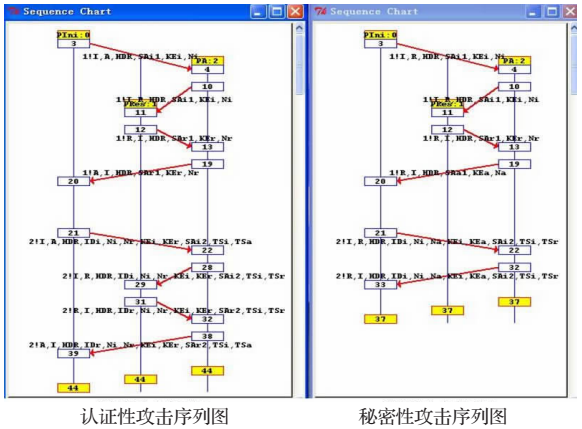
（1）认证性：[]((isFinishedI&& isFinishedR)->((partnerI=R)<->(partnerR=I)))

（2）秘密性：[]((isFinishedI&&(partnerI=R))->(! know_IDi)))&&([]((isFinishedR && partnerR=I)->(! know_IDr)))

其中[]表示一直(always)，->表示蕴含(implication)，<->表示当且仅当(iff)的意思。公式(1)表示发起者 I 和响应者 R 成功地完成了一次协议的运行，那么 I 相信它的通信对象是 R 当且仅当 R 相信它的通信对象是 I。公式(2)表示发起者 I 和响应者 R 成功地完成了一次协议的运行，则攻击者不可以知道 I 的身份 IDi，同样攻击者也不能知道 IDr。

4.4　检测结果与分析

用 SPIN 对上述模型验证之后，发现 IKEv2 协议不满足 LTL 公式刻画的认证性和秘密性。给出用 SPIN 检测出的两个攻击序列，其攻击序列如图 2 所示。



认证性攻击序列图　　秘密性攻击序列图

图 2　攻击序列图

从图 2 的攻击序列图的认证性攻击序列图可以看到，发起者 I 本希望与攻击者 A 进行协议的运行，但 A 收到消息后，冒充 I 转发给 R，这样 R 以为是和 I 在通信，发送消息(2)给 I，但消息(2)被 A 截获作为自己的消息响应给 I，最终 I 和 R 都会通过对方的验证。根据 DH 算法的特点，虽然这对攻击者本身并没有任何好处，但发起者 I 和响应者 R 完全被攻击者 A 欺骗了，它们并未察觉任何攻击的存在。由秘密性攻击序列图可知当 A 截获 R 发给 I 的消息(2)，A 用自己的 nonce、KEa 和 SAa1 篡改了消息(2)，使得 A 能够解密消息(3)而获得发起者的身份 IDi。

5　对基于数字签名的 IKEv2 协议的改进建议

文献[9,10]中说明了 IPSec VPN 三种保护模式中的安全网关与安全网关的隧道模式可以保护主机的身份，这种模式在通信的两个安全网关之间建立一个 IPSec 隧道，利用新的 IP 头对原有 IP 头的封装来保护发起者的身份信息，因此可以利用 IPSec 隧道技术来实现对 IKEv2 中的发起者身份保护。改进后的 IKEv2 协议如下：

（1）I→R：HDR，SAi1，KEi，*Ni*，[CERTREQ 网关]

（2）R→I：HDR，SAr1，KEr，*Nr*，[CERTE 网关]

（3）I→R：HDR，*sk*{pk{IDi}，AUTH，SAi2，TSi，TSr}

（4）R→I：HDR，*sk*{IDr，AUTH，SAi2，TSi，TSr}

上述协议中用响应者的安全网关的公钥 *pk* 来加密 IDi，可以保护身份，防止主动攻击的破坏，只有特定的得到 I 允许的安全网关才能解密并得到 IDi，攻击者由于没有私钥只能得到 *pk*{IDi}。当然这种保护的前提是安全网关的局域网内部是高度可靠的，如果主动攻击出现在局域网内部，那这种保护也将失败。

6　结束语

IKEv2 相对 IKEv1 在安全性和性能上都有很大的改进，其消息结构非常复杂，减少的消息交换回合无疑提高了协议的效率，但也遗留了 IKEv1 中的安全隐患。IKEv1 在身份保护方面的脆弱性同样存在于 IKEv2 的初始交换中。本文利用模型检测工具 SPIN 对 IKEv2 协议进行了检测，然后根据检测出的漏洞，提出对 IKEv2 中的发起者身份进行保护的一种改进建议，改进后的协议实现代价并不大，安全性有了一定程度的提高。

参考文献：

[1] Meadows C.Analysis of the Internet key exchange protocol using the protocol analyzer[C]//Proceedings of S&P'99.Los Alamitos：IEEE Press，1999：216-231.

[2] Kaufman C.Internet Key Exchange(IKEv2) protocol[EB/OL].(2005-12).http://tools.ietf.org/html/rfc4306.

[3] Maggi P，Sisto R.Using SPIN to verify security properties of cryptographic protocols[C]//SPIN'2002 Workshop，2002.

[4] 肖美华，薛锦云.基于 SPIN/Promela 的并发系统验证[J].计算机科学，2004(7)：201-203.

[5] 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.

[6] 陈大伟，董荣胜，郭云川，等.IKEv2 协议的 SPIN 模型检测[J].计算机工程，2006，32(5)：164-166.

[7] 常亮，古天龙，郭云川.互联网密钥交换协议的 SMV 分析[J].计算机工程与应用，2005，41(19)：154-157.

[8] 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.

[9] 李振强，赵晓宇，马严.IPv6 技术揭秘[M].北京：人民邮电出版社，2006.

[10] 周贤伟，薛楠.IPSec 解释[M].北京：国防工业出版社，2006.