广西科学院学报
Journal of Guangxi Academy of Sciences

2008,24(4):307～309
Vol. 24,No. 4 November 2008

基于SPIN的SAS协议和NS公钥协议分析
Study on Analysis of SAS Protocol and NS Protocol Based on SPIN

刘 芳,魏 昭,董荣胜
LIU Fang, WEI Zhao, DONG Rong-sheng

(桂林电子科技大学计算机系,广西桂林 541004)
(Department of Computer Science, Guilin University of Electronic Technology, Guilin, Guangxi, 541004, China)

摘要:给出SPIN模型检测协议的验证步骤,使用其分析验证SAS协议的安全属性和数据流行为属性,以及NS公钥协议的机密性和认证性。结果成功发现SAS协议数据流的缺陷和NS公钥协议的攻击路径。

关键词:协议 模型检测 分析
中图法分类号:TP301.2 **文献标识码**:A **文章编号**:1002-7378(2008)04-0307-03

Abstract: Protocol verification procedures based on model checking technique using SPIN were provided, then these procedures were used to analyze and verify the safty and function property in the SAS protocol, and the security and authentication property in the NS protocol. The results show that the flaw in the data flow of SAS protocol and the attacking path of NS protocol are detected.

Key words: protocol, model checking, analysis

协议是网络的血液和生命,计算机网络的发展是网络协议设计和开发的结果。但是计算机通信与网络技术的发展进一步增强了协议的复杂性,而协议开发过程中任何一点错误和缺陷都将给分布系统的稳定性、可靠性、坚固性、安全性、容错性以及异种系统之间的互通性带来巨大的危害。形式化的分析方法有助于协议设计的早期发现错误,该方法基于严格的数学基础,具有精确的语法和语义,所以能够检测协议中细微的漏洞[1]。模型检测是一种很重要的自动验证技术,在众多的形式化方法中,模型检测以其简洁明了和自动化程度高而引人注目。在硬件分析和验证领域,模型检测取得了巨大的成功。随着形式化方法的日益进步和应用领域的推广,模型检测逐渐应用到安全协议领域[2]。SPIN是常见的模型检测工具之一,它适合于并行系统,尤其适合协议一致性的辅助分析[3]。

本文给出一种模型检测的协议验证步骤,并根据这些验证步骤,使用SPIN模型检测工具对经典的SAS协议和NS公钥协议进行协议分析。

收稿日期:2008-10-12

作者简介:刘 芳(1984-),女,硕士研究生,主要从事网络信息安全技术研究。

1 模型检测的协议验证步骤

用模型检测方法对协议进行验证主要有协议建模、协议性质描述和验证3个步骤。

1.1 协议建模

模型检测的第一步是将协议转换成模型检测工具能接受的形式化模型(用有限状态模型来描述协议),需要使用抽象技术消减无关或不重要的细节。

1.2 协议性质描述

用某种合适的逻辑(通常都是时态逻辑)来描述协议性质要求。在验证前需要声明一个协议必需满足的属性,模型检测提供了一个验证系统满足某种属性的手段,但是它不能确定所给的属性是否覆盖了协议应该满足的所有性质。

1.3 验证

应用模型检验工具对上述有限状态模型和相应的安全性质进行分析。将系统的有限状态模型转化成各自的编程语言,并输入到各自的检测器中,系统地验证有限状态所描述的模型是否满足所需求的性

质。如果系统模型不满足安全性质要求，那么模型检测器会自动生成不满足所需求性质的反例。

2 协议的形式化分析

2.1 基于web服务的SAS协议分析

2.1.1 协议分析

在基于web服务的SAS协议[4]中，有3个参与运行的主体，首先Investor给StockBroker发送Regist消息，该消息由订单号orderid、一系列的股票号stockid和投股资金stockprice构成。如果Regist消息被接收，StockBroker将发送Request消息给ResearchDept，但是每次发送的Request消息中只包含一个stockid，所以从StockBroker发送Request消息到ResearchDept，ResearchDept发送report消息到Investor，Investor发送ack消息到StockBroker之间存在循环。而在循环中Investor有权利发送cancel消息来终止整个交易。若每个stockid都已经被处理，StockBroker将发送bill消息给Investor，最后，StockBroker通过发送消息terminate来终止整个交易。

2.1.2 协议描述

使用SPIN[3~6]建立SAS协议的形式模型，在协议中定义4个主体模块：投股人(Investor)、股东分析服务(StockBroker)、分析部门(ResearchDept)和消息管理机制(msgmanage)，并采用Promela语言描述4个主体模块为：主体I：proctype Investor()；主体S：proctype stockbroken()；主体R：proctype researchdept()；主体M：proctype msg()。

2.1.3 认证属性

对SAS协议的安全属性、数据流行为属性进行认证[4,5]。

(1)安全属性。例如：死锁的检验均采用<>!death格式，结果表明SAS协议不存在死锁；状态的可达性检验，[]<>(terminate.orderID==true)表明系统最终会发送terminate消息来终止运行，该属性是满足的。

(2)数据流行为属性。在SAS协议中，投资者所投的每一个股票号，在投资者不发送取消操作，股东也没有拒绝投资者所投订单的情况下，每一个股票号都要出现在股东到分析部门的请求消息中。用LTL属性[2,7]表示如下：

① []((regin.stockid[0]==2 && flag==1) -> (<> (request.stockid==2)) || <> (cancel.orderid==1) || <>(reject.orderid==1))；

② []((regin.stockid[1]==2 && flag==1) -> (<> (request.stockid==2)) || <> (cancel.orderid==1) || <>(reject.orderid==1))；

③ []((regin.stockid[2]==2 && flag==1) -> (<>(request.stockid==2)) || <>(cancel.orderid==1) || <>(reject.orderid==1))。

实验结果是：属性①认证无误，属性②③认证出错，属性②③的反例为regin.stockid[0]=0，regin.stockid[1]=2，regin.stockid[2]=0和regin.stockid[0]=0，regin.stockid[1]=2，regin.stockid[2]=2。

2.2 NS公钥协议分析

2.2.1 协议分析

NS公钥协议[8]按功能划分为两个部分：获取公开密钥和双方身份认证。这里我们研究其机密性和认证性，协议为

消息1：A→B：{N_a，A}K_b；消息2：B→A：{N_a，N_b}K_a；消息3：A→B：{N_b}K_b。

其中A、B是协议的通信个体，A为协议的发起者，B为协议的响应者。整个协议采用公开密钥系统，K_a、K_b分别是A和B的公开密钥，用于加密消息；N_a，N_b是A和B发布的具有新鲜性的随机数(也称临时值)。协议的运行过程为：首先，发起者A将一个随机数N_a和自己的身份一起用响应者B的公钥K_b加密后发送给B，然后B收到并通过解密获得N_a，B通过检查事先定义好的数据库，将N_a连同自己产生的随机数N_b一起用A的公钥加密后发送给A，A通过比较前后的N_a得到B已经获得自己发送的消息，这样B的身份被A确认。最后，A再次向B发送以B的公钥加密的随机数N_b，这样A的身份也被B确认。

在A与B建立认证的过程中，很可能出现入侵者I，它一方面监听A发往B的消息，并且截获到消息1，然后I可以破坏消息1，对消息进行篡改，扰乱A和B的通信[9]。入侵者是抽象出来的能对网络通信进行不良行为的一个主体，入侵者可能在网络的任何地方，并具有以下能力：(1)可以在任何通信主体间截获消息或转发消息；(2)可以以自己的身份冒充初始者A和响应者B；(3)根据获取的消息可以产生新消息；(4)解密已知密钥加密的消息。

2.2.2 协议描述

我们为NS公钥协议构造有限状态系统模型为

参与协议运行的主体集合：{初始者A，响应

者B，入侵者I)。

其中A和B是诚实主体,他们将严格按照初始者和响应者的身份参与协议运行,并只运行一次NS公钥协议,而入侵者I则不受此限制。

初始者A、响应者B和入侵者I三个主体进程的具体描述如下。

(1) A作为协议发起的初始者,它的第一个通信动作是发送信息1,通信对象可以是B也可以是I,这是两个并发的通信动作,不确定地选择一个通信对象执行。当A接到消息2后,A要检验消息2是否以自己的公钥加密,并且检查消息中是否含有自己发出的临时值Na。否则,A进程将处于阻塞状态。用Pormela语句表示为(key==keyA)&&(data1==nonceA);如果消息2中是它期望的值,就把消息3发给它的通信对象,并认为通信成功。其通信动作包含一次接收和两次发送。

(2)主体B的通信过程和A类似。其通信动作含有两次接收和一次发送。

(3)入侵者I不是固定地按照协议的步骤运行,目的是让SPIN发现协议中可能存在的攻击。我们描述入侵者I的动作是不确定的,以让SPIN选择执行。比如I存在发送和接收两个不确定的动作,如果选择接收动作,则接下来是拦截或接收一条信息,并将拦截的信息存储或者不存储;如果信息是以nonceI加密,则I可以解开并可以获得nonceA或nonceB,定义两个布尔变量knows-nonceA和knows-nonceB表示是否知道这些临时值。如果选择发送动作,则入侵者I又有两个可选择的动作:重放一个拦截的数据包或者从已知的信息中构造一个新的数据包发出去。I作为冒充者,可冒充A的身份,以I(A)参与协议运行。

2.2.3 认证属性

NS公钥协议的目的是在保密状态下确保协议主体的相互鉴别,换言之,如果A和B成功地运行了一次协议,那么A相信它的通信对象是B当且仅当B相信它的通信对象是A。用LTL公式[2,7]表示为G((statusA=ok∧statusB=ok)=>(partnerA=agentB <=> partnerB =agentA))。

根据模型描述和LTL描述,使用SPIN验证之后,通过生成的反例,发现NS公钥协议存在如下的攻击序列:(1)A→I:$\{N_a,A\}_{K_i}$;(2)I(A)→B:$\{N_a,A\}_{K_b}$;(3)B→I(A):$\{N_a,N_b\}_{K_a}$;(4)I→A:$\{N_a,N_b\}_{K_a}$;(5)A→I:$\{N_b\}_{K_i}$;(6)I(A)→B:$\{N_b\}_{K_b}$。

入侵者在第(1)步解密消息,获得N_a,并在第(2)步通过获得的N_a冒充A与B进行通信,第(3)步B与I(B认为是A)进行通信,第(4)步I将B发给它的消息重放给A,第(5)步I解密A发送回来的消息得到N_b,第(6)步I冒充A向B发送得到的N_b。I假冒A成功。这样,B认为是与A建立了认证关系,而实际上一直与B进行通信的是I。

3 结束语

本文给出一种模型检测技术的协议验证步骤,然后用所给的验证步骤分别对SAS协议和NS公钥协议进行分析和验证,最终结果成功发现了这两个协议相应的缺陷。

由于形式化方法是基于数学的方法,具有精确的语法和语义,能够检测到协议中细微的安全漏洞,在下一步工作中,我们将从语义的角度来定义协议的统一分析框架,形式化到描述各类协议,以便精确的验证协议属性。

参考文献:

[1] Catherine Meadows. Formal methods for cryptographic protocol analysis: emerging issues and trends[J]. IEEE Journal on Selected Areas in Communication, 2003,21(1):44-54.

[2] Edmund M Clarke, Jr Orna Grumberg, Doron A Peled. Model checking[M]. Cambridge: MIT Press, 2000.

[3] Holzmann G J. The model checker SPIN[J]. IEEE Transaction on Software Engineering,1997,23(5):279-295.

[4] Audun,Josang. Security protocol verification using spin: proc of the 1th workshop on Automata Theoretic Verification with the SPIN Model Checker SPIN95 [C]. Montreal:Quebee,1995.

[5] Dong Rongsheng,Wei Zhao,Luo Xiangyu. Model checking behavioral specification of BPEL web services [C]. WCE,2008.

[6] Xiang Fu,Tevfik Bultan,Jianwen Su. Model checking interactions of composite web services:UCSB Computer Science Department Technical Report[R]. California: University of California, Santa Barbara,2004.

[7] Needham R M,Schroeder M D. Using encryption for authentication in large networks of computers [J]. Communications of the ACM, 1978, 21(12):993-999.

[8] 张玉清,王磊,肖国镇,等. Needham-Schroeder公钥协议的模型检测分析[J]. 软件学报, 2000,11(10):1348-1352.

[9] 孙守卿,李廉, 章超,等. 基于模型检测工具SPIN的安全协议形式化分析: 2005年全国理论计算机科学学术年会论文集[C]. 秦皇岛:中国计算机学会理论计算机科学专业委员会,2005.

(责任编辑:韦廷宗)