CN 43-1258/TP
ISSN 1007-130X

计算机工程与科学
Computer Engineering & Science

第 37 卷第 11 期 2015 年 11 月
Vol. 37, No. 11, Nov. 2015

文章编号:1007-130X(2015)11-2121-07

运用 SPIN 对开放授权协议 OAuth 2.0 的分析与验证*

程道雷,肖美华,刘欣倩,梅映天,李　伟
(华东交通大学软件学院,江西 南昌 330013)

摘　要:OAuth 2.0 协议是一种开放授权协议,主要用于解决用户账号关联与资源共享问题。但是,其弱安全性导致各网络公司海量用户信息泄露,且 OAuth 2.0 传输数据采用的 https 通道效率低下,成为黑客攻击对象。提出采用 http 通道传输 OAuth 2.0 协议数据,基于 Promale 语言及 Dolev-Yao 攻击者模型对 OAuth 2.0 协议建模,运用 SPIN 进行模型检测。形式化分析结果表明,采用公钥加密体系对 OAuth 2.0 协议进行加密不安全。上述建模方法对类似的授权协议形式化分析有重要借鉴意义。

关键词:OAuth 2.0 协议;信息泄露;公钥加密体系;模型检测
中图分类号:TP309　　**文献标志码**:A
doi:10.3969/j.issn.1007-130X.2015.11.019

Analyzing and verifying an open authorization protocol OAuth 2.0 with SPIN

CHENG Dao-lei, XIAO Mei-hua, LIU Xin-qian, MEI Ying-tian, LI Wei
(School of Software, East China Jiaotong University, Nanchang 330013, China)

Abstract: The OAuth 2.0 is an open authorization protocol which solves the problem of user accounts associating and resources sharing. However, due to its weak security, massive user information of network companies is leaking. Besides, the https channel used by OAuth 2.0 to transmit data is inefficient, making the OAuth 2.0 an attack object of hackers. We propose an open authorization protocol, which transmits the data of the OAuth 2.0 protocol in http channels, model the protocol based on the Promale language and Dolev-Yao attacker model, and employ the SPIN for model checking. The results of formal analysis show that the OAuth2.0 protocol encrypted by the public key encryption system is unsafe. The proposed modeling method has great significance in formal analysis of similar license agreement.

Key words: OAuth 2.0 protocol; information leakage; public key encryption system; model checking

1　引言

OAuth(Open Authorization)[1]作为一种授权标准,用户无需将用户名和密码等信息提交给第三方应用,便能在第三方应用中获取其存储于其它平台的私密资源,该标准主要用于解决账号关联与资源共享问题。OAuth 2.0 是 OAuth 协议的最新版本,不兼容 OAuth 1.0,但降低了 OAuth 协议的编码复杂度,且为各平台的相关应用提供了对应的认证方式。近年来,OAuth 2.0 协议的安全性漏洞引发了许多互联网安全问题,包括 CSDN、facebook、亚马逊、新浪微博在内的众多著名网站遭受黑客攻击。因此,OAuth 2.0 协议形式化分析与验证具有重要社会价值。

Pai S 等[2]运用 Alloy 框架对 OAuth 2.0 进行形式化分析;Sun San-Tsai[3]通过利用基于 OAuth 2.0 的单点登录系统的实例表明 OAuth 2.0 虽然

* **收稿日期**:2015-08-10;**修回日期**:2015-10-10
基金项目:国家自然科学基金资助项目(61163005);计算机软件新技术国家重点实验室开放课题资助项目(KFKT2012B18);江西省自然科学基金资助项目(20132BAB201033);江西省高校科技落地计划项目(KJLD13038);江西省对外科技合作技术资助项目(20151BDH80005);华东交通大学研究生创新计划资助项目(YC2014-X007)
通信地址:330013 江西省南昌市昌北区华东交通大学软件学院(南区)
Address: School of Software, East China Jiaotong University, Changbei District, Nanchang 330013, Jiangxi, P. R. China

内容简单,但不安全;陈伟等[4]运用"数字签名技术"对 OAuth 2.0 进行改进,并基于 Blanchet 演算对其进行安全性分析;王焕孝等[5]运用协议分析工具 SATMC,得出 OAuth 2.0 协议在失去 https 通道保护下的危险状态。由于 OAuth 2.0 协议当前依赖 https 通道传输相关数据,而 https 要运行 SSL(Secure Sockets Layer)对传输数据加密,降低了 https 传输效率。根据相关调查研究,在北上广深以外的中国广大城市,有 20%~25% 的用户都会遇到 https 连接困难,排查发现问题和接入点无关,信号和网络不稳定导致 https 请求很难完成,导致一旦遭遇 ARP(Address Resolution Protocol)攻击或中间人攻击,用户信息将遭窃取或破坏。本文提出使 OAuth 2.0 脱离 https 通道,通过"http+消息加密"的方式传输数据,并将公钥密钥体系运用到该协议上,使用模型检测技术对协议进行安全性验证。

形式化方法主要包括模型检测(Model Checking)[6]与定理证明[7]两个分支。SPIN(Simple Promela INterpreter)[8,9]是一种著名的协议模型检测验证工具。Maggi P 等[10]以 Ndddam-Schroeder 协议为实例,基于 Dolev-Yao 攻击模型[11]的思想,提出一种用于安全协议模型检测的建模方法。本文对该方法进行扩展,运用到包含多主体的授权协议的模型检测上。

由于 OAuth 2.0 是一个崭新的授权协议,可供参考的运用形式化方法对该协议安全性验证研究成果仍然不足,本文探索使用模型检测技术对 OAuth 2.0 协议进行形式化分析与验证。首先,将 OAuth 2.0 协议进行简化,并用形式化方法对其进行描述,再运用公钥加密体系对协议进行加密,在对 OAuth 2.0 协议进行建模后,验证该协议是否能安全用在消息传输中,模型检测实验发现了中间人攻击序列图,因此得出公钥加密体系不能够保证 OAuth 2.0 协议安全的方法。

本文结构安排如下:第 2 节对 OAuth 2.0 协议进行简化及形式化表示,并运用公钥密码体系对协议加密;第 3 节阐述了 OAuth 2.0 协议建模过程;第 4 节运用 SPIN 对 OAuth 2.0 协议进行验证与分析;第 5 节为结束语。

2 OAuth 2.0 协议及形式化表示

OAuth 是一种第三方授权协议。首先,客户端发送 Authorization Request(授权申请),向 Resource Owner(资源拥有者)申请 Access Grant(访问授权);然后,使用 Access Grant 和 Client Credentials(身份证书)与 Authorization Server(授权服务器)交换 Access Token(访问令牌,包含持续时间、作用范围等信息),最后客户端提交 Access Token 至 Resource Owner(资源拥有者)获取受保护资源。具体过程如图 1 所示。

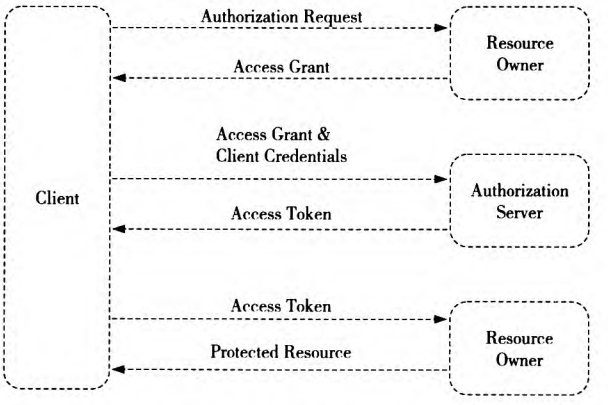

Figure 1 Flow of the abstract protocol

图 1 抽象协议流程

根据图 1 所示的协议流程,将 OAuth 2.0 协议进行形式化表示,获得如下协议:

(1)Client→ Resource Owner: Authorization Request;

(2)Resource Owner→Client:Access Grant;

(3) Client → Authorization Server: Access Grant,Client Credentials;

(4)Authorization Server→Client:Access Token;

(5)Client→Resource Server:Access Token;

(6) Resource Server→Client: Protected Resource。

如果将以上协议中未加密的消息直接通过 http 通道传输数据,所有的信息都将被攻击者轻而易举截获。因此,将 OAuth 2.0 协议简化,并用公钥加密体系对消息进行加密,得到如下 OAuth 2.0 协议:

(1)$C \rightarrow RO:\{A\_r\}PK_{RO}$;

(2)$RO \rightarrow C:\{A\_g\}PK_{C}$;

(3)$C \rightarrow AS:\{A\_g\ ,C\_c\}PK_{AS}$;

(4)$AS \rightarrow C:\{A\_t\}PK_{C}$;

(5)$C \rightarrow RS:\{A\_t\}PK_{RS}$;

(6)$RS \rightarrow C:\{P\_r\}PK_{C}$。

其中,PK_C 表示以 C 的公钥加密,任意经 C 的公钥加密的消息,只有 C 才能通过其私钥解开,其它主体类似。本文将运用模型检测技术对以上协议进

行验证分析。

3 OAuth 2.0 协议建模

将 OAuth 2.0 协议建模分为诚实主体建模和攻击者建模两个部分,其中,攻击者建模以 Dolev-Yao 攻击者模型为指导理论。

3.1 诚实主体建模

OAuth 2.0 协议的诚实主体包括 Client、Resource Owner、Authorization Server 和 Resource Server。结合 Promela 语言性质,我们分别为四个诚实主体定义各自的进程,依次命名为 proctype *PC*()、proctype *PRO*()、proctype *PAS*()和 proctype *PRS*()。由于诚实主体进程的定义方法非常类似,本文将以 proctype *PC*()的定义过程为例进行阐述。

本文所研究的内容为检测协议本身存在的漏洞,因此首先需要对模型做出如下几点假设:

(1)公钥加密算法本身没有漏洞;

(2)只有对应的密钥才能解密加密消息;

(3)攻击者可以是任何主体。

由于攻击者建模遵循 Dolev-Yao 攻击模型,因此诚实主体发送的所有消息都将被攻击者截获,而诚实主体所接收的消息,也全部由攻击者根据已有的知识组合生成或者直接转发截获的消息。依据该思想,建模过程需要借助 Promela 语言中的通道(chan)这一数据结构。将协议中传输的消息根据数据项的数目进行分类,同一类的消息使用同一个通道进行传输,因此,OAuth 2.0 数据传输模拟需要两个参数不同的通道,将其进行如下定义:

chan *ca*=[0] of {mtype,mtype,mtype}

chan *cb*=[0] of { mtype, mtype, mtype, mtype}

其中,协议中的消息(1)、(2)、(4)、(5)、(6)通过通道 *ca* 传输,消息(3)通过通道 *cb* 传输。值得注意的是 *ca* 和 *cb* 所定义的单位元素个数都比所需表示的消息元素多一项,这是因为通道中需要预留一个元素应对会话过程中的优化需要。具体原因如下:由于本文所要构建的是一个并发系统,因此各进程之间的交叉运行所产生的状态迁移量将非常庞大,甚至足以导致状态爆炸[12~15],为了减少状态迁移的数量,在建模过程中,以 *ca* 为例,对通道作如下定义:发送语句 *ca*!*x*1,*x*2,*x*3 中,*x*1 为消息接收者,*x*2 是知识项,*x*3 是对 *x*2 进行加密的公钥。接收语句 *ca*?*eval*(*x*1),*x*2,*eval*(*x*3) 中,*eval* 函数被用作判断知识项是否与预期一致,从左到右依次判断,如果某处不一致,直接拒绝接收该消息。但是,攻击者需要截获所有诚实主体发送的消息,因此不需要通过 *eval* 来判断消息发送方,可直接定义为 *ca*?_,*x*1,*x*2 。如此,可以减少大量无效消息。对 Client 的建模,具体如以下 proctype *PC*() 的详细代码所示:

```
proctype PC(mtype self; mtype party1;mtype party2 ; mtype party3){mtype g1,g2;
atomic{init_start_C_RO(self,party1);ca! party1, nonce ,party1;}
atomic{
  ca ? eval(self),g1,eval(self); init_commit_C_RO(self,party1);
  if
    ::init_start_C_AS(self,party2); cb ! party2, g1,cred,party2;
    ::cb ! HACKER,g2,cred,HACKER;
  fi;
}
atomic{
  ca ? eval(self),g2,eval(self); init_commit_C_AS(self,party2);
  if
    ::init_start_C_RS(self,party3); ca! party3, g2,party3;
    ::ca! HACKER,g2,HACKER;
  fi;
}
atomic{ca? eval(self),eval(P_r),eval(self); init_commit_C_RS(self,party3); }
}
```

在 *PC* 进程中,*self* 表示消息发起者,*party*1、*party*2、*party*3 为消息接收者,*g*1 和 *g*2 为泛型变量,用作表示主体 *C* 接收到的消息中的未知数据项。atomic 为 Promela 语言中用来定义原子序列的语法规则,旨在减少进程交叉运行的次数,达到优化系统的目的。init_start_C_RO、init_commit_C_RO、init_start_C_AS、init_commit_C_AS 和 init_start_C_RS 为模型程序中定义的宏,被用来更新记录原子谓词的变量的值,这些原子谓词被用来表示协议性质。如果主体 *C* 发起对主体 *RO* 的协议会话,表示主体 *C* 参与了主体 *RO* 运行的协议。如果主体 *C* 完成了与主体 *RO* 的会话,则表明主体 *C* 提交了与主体 *RO* 的会话。根据以上原理,模型的每一条性质都需要用一个全局的 Promela 布尔变量表示,它们将在协议运行的特定阶段为真。通过

对协议的分析,定义了如下原子谓词变量:

bit *startCRO*=0; bit *startROC*=0;bit *startCAS*=0; bit *startASC*=0; bit *commitCRS*=0;bit *startCRS*=0; bit *startRSC*=0; bit *commitCAS*=0;bit *commitCRO*=0;

为了将模型中的所有性质运用到 SPIN 工具的仿真过程中,本文将协议性质用 LTL(线性时态逻辑)[16,17]刻画如下:

[]((!! *commitCRO*) ‖ (! *commitCRO*U*startROC*))

[]((!! *startCAS*) ‖ (! *startCAS*U*commitCRO*))

[]((!! *commitCAS*) ‖ (! *commitCAS*U*startASC*))

[]((!! *startCRS*) ‖ (! *startCRS*U*commitCAS*))

[]((!! *commitCRS*) ‖ (! *commitCRS*U*startRSC*))

根据相同的规则,类似地定义主体 RO 的进程 PRO 和主体 AS 的进程 PAS 以及主体 RS 的进程 PRS。

除定义好诚实主体进程之外,还要对初始进程作如下定义:

```
init{
atomic{if
  ::run PC(C,HACKER,A_r,C_c,AS,RS)
  ::run PC(C,RO,A_r,C_c,AS,RS)
  fi;
  run PRO(RO,C,A_g);run PAS(AS,C,A_t);
  run PRS(RS,C,P_r);run H();
  }
}
```

主体 C 作为整个协议的发起者,在协议模型中,他有可能向任意主体发起协议,如主体 RO 和主体 $HACKER$。

3.2 攻击者建模

攻击者建模中,攻击者知识库创建最为关键,其主要由两部分知识项构成:第一部分为攻击者本身的初始知识库;另一部分知识项学习方法如下:攻击者每拦截到一条新消息后,便将学到的知识添加到知识库中。其添加方式分为两种:如截获的消息未经加密,则可直接获取其所有知识项并添加入库;如截获的消息已加密或者部分加密,则未经加密部分或者可以解密部分,直接或者解密后添加入库,如无法解密,将整个密文部分存入知识库中,以备需要时提取使用。

为简化知识项表示,攻击者知识项表示须遵循以下两点原则:(1)不表示攻击者不可能学会的知识项;(2)不表示诚实主体拒绝接受的消息(通过类型检查的方式判断)。基于以上两点,可以计算出需要表示的攻击者知识,如图 2 所示,攻击者潜在能学会的知识和攻击者需要学会的知识的交集为攻击者模型需要表示的知识。

Figure 2 Schematic of the attacker acquiring the knowledge which need to be indicated

图 2 攻击者模型中需要表示的知识项求解示意图

首先求解攻击者可以学会的知识。因为攻击者可以学会的知识,都是通过截获诚实主体发送的消息并对其进行相应处理所得,故可通过对诚实主体的发送消息语句进行分析,获得所需知识。攻击者初始知识库为 $\{C,RO,AS,RS,H,gD,R,PK_H,PK_{RO},PK_{RS},PK_{AS},PK_C\}$,变量 $g1\sim g5$ 的取值范围为 $\{C,RO,AS,RS,H,gD,PK_H,PK_{RO},PK_{RS},PK_{AS},PK_C\}$,因此,可获得如表 1 所示的攻击者可学会的知识。

Table 1 Knowledge elements that the intruder can acquire

表 1 攻击者可学会的知识

潜在的接收到的消息	可学会的知识(不包含初始库)
$\{A\_r\}PK_{RO}$,$\{A\_r\}PK_H$	$\{A\_r\}PK_{RO}$,A_r
$\{C,C\_c\}PK_{AS}$,$\{RO,C\_c\}PK_{AS}$ $\{H,C\_c\}PK_{AS}$,$\{AS,C\_c\}PK_{AS}$ $\{RS,C\_c\}PK_{AS}$,$\{A\_g,C\_c\}PK_{AS}$ $\{A\_t,C\_c\}PK_{AS}$,$\{C\_c,C\_c\}PK_{AS}$ $\{A\_r,C\_c\}PK_{AS}$,$\{P\_r,C\_c\}PK_{AS}$ $\{gD,C\_c\}PK_{AS}$	$\{C,C\_c\}PK_{AS}$,$\{RO,C\_c\}PK_{AS}$ $\{H,C\_c\}PK_{AS}$,$\{AS,C\_c\}PK_{AS}$ $\{RS,C\_c\}PK_{AS}$,$\{A\_g,C\_c\}PK_{AS}$ $\{A\_t,C\_c\}PK_{AS}$,$\{C\_c,C\_c\}PK_{AS}$ $\{A\_r,C\_c\}PK_{AS}$,$\{P\_r,C\_c\}PK_{AS}$ $\{gD,C\_c\}PK_{AS}$
$\{C,C\_c\}PK_H$,$\{RO,C\_c\}PK_H$ $\{H,C\_c\}PK_H$,$\{AS,C\_c\}PK_H$ $\{RS,C\_c\}PK_H$,$\{A\_g,C\_c\}PK_H$ $\{A\_t,C\_c\}PK_H$,$\{C\_c,C\_c\}PK_H$ $\{A\_r,C\_c\}PK_H$,$\{P\_r,C\_c\}PK_H$ $\{gD,C\_c\}PK_H$	C_c,A_g,A_t,A_r,P_r
$\{C\}PK_{RS}$,$\{RO\}PK_{RS}$,$\{H\}PK_{RS}$ $\{AS\}PK_{RS}$,$\{RS\}PK_{RS}$,$\{A\_r\}PK_{RS}$ $\{A\_g\}PK_{RS}$,$\{A\_t\}PK_{RS}$,$\{P\_r\}PK_{RS}$ $\{gD\}PK_{RS}$,$\{C\_c\}PK_{RS}$	$\{C\}PK_{RS}$,$\{RO\}PK_{RS}$,$\{H\}PK_{RS}$ $\{AS\}PK_{RS}$,$\{RS\}PK_{RS}$,$\{A\_r\}PK_{RS}$ $\{A\_g\}PK_{RS}$,$\{A\_t\}PK_{RS}$,$\{P\_r\}PK_{RS}$ $\{gD\}PK_{RS}$,$\{C\_c\}PK_{RS}$
$\{C\}PK_H$,$\{RO\}PK_H$,$\{H\}PK_H$ $\{AS\}PK_H$,$\{RS\}PK_H$,$\{A\_r\}PK_H$ $\{A\_g\}PK_H$,$\{A\_t\}PK_H$,$\{P\_r\}PK_H$ $\{gD\}PK_H$,$\{C\_c\}PK_H$	C_c,A_g,A_t,A_r,P_r
$\{A\_t\}PK_C$,$\{P\_r\}PK_C$,$\{A\_g\}PK_C$ $\{A\_t\}PK_H$,$\{P\_r\}PK_H$,$\{A\_g\}PK_H$	$\{A\_t\}PK_C$,$\{P\_r\}PK_C$,$\{A\_g\}PK_C$ A_t,P_r,A_g

接下来需要求解的是攻击者需学会的知识项。

攻击者需要学会的知识,就是组成攻击者发送给诚实主体的消息的知识项。故可通过对诚实主体的接收消息语句进行分析,根据变量的不同取值,组合得到如表 2 所示的攻击者需要学会的知识。

Table 2 Knowledge elements the intruder needs

表 2 攻击者需要学会的知识项

攻击者潜在发送的消息	需用到的知识项(除初始库外)
$\{C\}PK_C$,$\{RO\}PK_C$,$\{H\}PK_C$ $\{AS\}PK_C$,$\{RS\}PK_C$,$\{A\_r\}PK_C$ $\{A\_g\}PK_C$,$\{A\_t\}PK_C$,$\{P\_r\}PK_C$ $\{C\_c\}PK_C$,$\{gD\}PK_C$	A_r,A_g,A_t,P_r,C_c 或 $\{C\}PK_C$,$\{RO\}PK_C$,$\{H\}PK_C$ $\{AS\}PK_C$,$\{RS\}PK_C$,$\{A\_r\}PK_C$ $\{A\_g\}PK_C$,$\{A\_t\}PK_C$,$\{P\_r\}PK_C$ $\{C\_c\}PK_C$,$\{gD\}PK_C$
$\{C\}PK_{RO}$,$\{RO\}PK_{RO}$,$\{H\}PK_{RO}$ $\{AS\}PK_{RO}$,$\{RS\}PK_{RO}$,$\{A\_r\}PK_{RO}$ $\{A\_g\}PK_{RO}$,$\{A\_t\}PK_{RO}$,$\{P\_r\}PK_{RO}$ $\{C\_c\}PK_{RO}$,$\{gD\}PK_{RO}$	A_r,A_g,A_t,P_r,C_c 或 $\{C\}PK_{RO}$,$\{RO\}PK_{RO}$,$\{H\}PK_{RO}$ $\{AS\}PK_{RO}$,$\{RS\}PK_{RO}$,$\{A\_r\}PK_{RO}$ $\{A\_g\}PK_{RO}$,$\{A\_t\}PK_{RO}$,$\{P\_r\}PK_{RO}$ $\{C\_c\}PK_{RO}$,$\{gD\}PK_{RO}$
$\{C,C\_c\}PK_{AS}$,$\{RO,C\_c\}PK_{AS}$ $\{H,C\_c\}PK_{AS}$,$\{AS,C\_c\}PK_{AS}$ $\{RS,C\_c\}PK_{AS}$,$\{A\_r,C\_c\}PK_{AS}$ $\{A\_g,C\_c\}PK_{AS}$,$\{A\_t,C\_c\}PK_{AS}$ $\{P\_r,C\_c\}PK_{AS}$,$\{C\_c,C\_c\}PK_{AS}$ $\{gD,C\_c\}PK_{AS}$	A_r,A_g,A_t,P_r,C_c 或 $\{C,C\_c\}PK_{AS}$,$\{RO,C\_c\}PK_{AS}$ $\{H,C\_c\}PK_{AS}$,$\{AS,C\_c\}PK_{AS}$ $\{RS,C\_c\}PK_{AS}$,$\{A\_r,C\_c\}PK_{AS}$ $\{A\_g,C\_c\}PK_{AS}$,$\{A\_t,C\_c\}PK_{AS}$ $\{P\_r,C\_c\}PK_{AS}$,$\{C\_c,C\_c\}PK_{AS}$ $\{gD,C\_c\}PK_{AS}$
$\{C\}PK_{RS}$,$\{RO\}PK_{RS}$,$\{H\}PK_{RS}$ $\{AS\}PK_{RS}$,$\{RS\}PK_{RS}$,$\{A\_r\}PK_{RS}$ $\{A\_g\}PK_{RS}$,$\{A\_t\}PK_{RS}$,$\{P\_r\}PK_{RS}$ $\{gD\}PK_{RS}$,$\{C\_c\}PK_{RS}$	A_r,A_g,A_t,P_r,C_c 或 $\{C\}PK_{RS}$,$\{RO\}PK_{RS}$,$\{H\}PK_{RS}$ $\{AS\}PK_{RS}$,$\{RS\}PK_{RS}$,$\{A\_r\}PK_{RS}$ $\{A\_g\}PK_{RS}$,$\{A\_t\}PK_{RS}$,$\{P\_r\}PK_{RS}$ $\{gD\}PK_{RS}$,$\{C\_c\}PK_{RS}$

由表 1 和表 2 的第 2 列求交集,可得到攻击者模型中需要表示的知识项,具体如图 3 所示。

根据以上的研究基础与理论,编写攻击者模型代码,框架如下所示:

```
proctype H( ){
mtype x1=0,x2=0,x3=0; bit k_Ar=0;/* 需要存储的知识 */
do
::ca! (k_Ag→RO:R),A_g,RO;
::cb! (k_C_Cc_AS→AS:R),C,C_c,AS;
::d_step{ca? _,x1,x2;…}
::d_step{cb? _,x1,x2,x3;…}
od
}
```

在 Windows 7 64 位系统、Cygwin 2.510.2.2 以及 SPIN 5.2.0 构建的环境下进行仿真实验,发现了如图 4 所示的 OAuth 2.0 协议的中间人攻击序列。

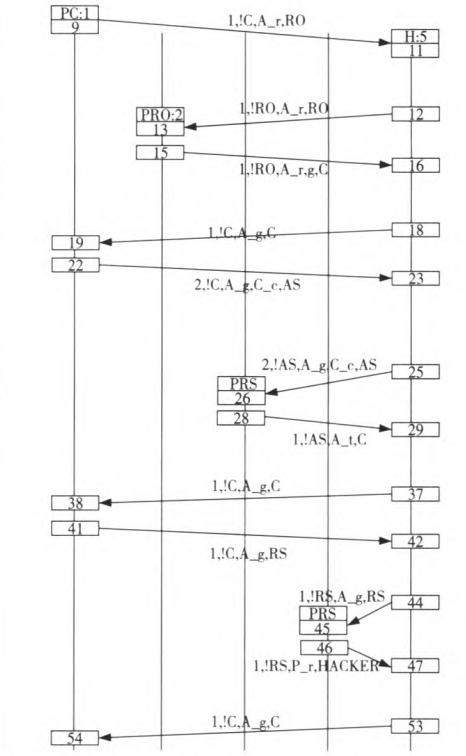

Figure 4 Attack sequence diagram

图 4 攻击序列图

4 实验结果与分析

使用 SPIN 工具,对上述模型进行验证,获得了如图 4 所示的攻击序列,并得到如下攻击过程:

(1)$C \rightarrow HACKER$: $\{A\_r\}PK_{HACKER}$;

$HACKER \rightarrow RO$:$\{A\_r\}PK_{RO}$;

A_r,A_g,A_t,P_r,C_c			
$\{A\_g\}PK_C$,	$\{A\_t\}PK_C$,	$\{P\_r\}PK_C$	
$\{C,C\_c\}PK_{AS}$,	$\{RO,C\_c\}PK_{AS}$,	$\{HACKER,C\_c\}PK_{AS}$	
$\{AS,C\_c\}PK_{AS}$,	$\{RS,C\_c\}PK_{AS}$,	$\{C\_c,C\_c\}PK_{AS}$,	$\{A\_g,C\_c\}PK_{AS}$
$\{A\_t,C\_c\}PK_{AS}$,	$\{A\_r,C\_c\}PK_{AS}$,	$\{P\_r,C\_c\}PK_{AS}$,	$\{A\_r\}PK_{RO}$
$\{gD,C\_c\}PK_{AS}$,	$\{C\}PK_{AS}$,	$\{RO\}PK_{AS}$,	$\{HACKER\}PK_{RS}$
$\{AS\}PK_{RS}$,	$\{RS\}PK_{RS}$,	$\{C\_c\}PK_{RS}$,	$\{A\_g\}PK_{RS}$
$\{A\_t\}PK_{RS}$,	$\{A\_r\}PK_{RS}$,	$\{P\_r\}PK_{RS}$,	$\{gD\}PK_{RS}$

Figure 3 Knowledge elements that need to be indicated in the attacker model

图 3 攻击者模型中需要表示的知识项

(2)$RO \rightarrow HACKER:\{A\_g\}PK_C$;$HACKER \rightarrow C:\{A\_g\}PK_C$;

(3)$C \rightarrow HACKER:\{A\_g,C\_c\}PK_{AS}$;$HACKER \rightarrow AS:\{A\_g,C\_c\}PK_{AS}$;

(4)$AS \rightarrow HACKER:\{A\_t\}PK_C$;$HACKER \rightarrow C:\{A\_t\}PK_C$;

(5)$C \rightarrow HACKER:\{A\_t\}PK_{HACKER}$;$HACKER \rightarrow RS:\{A\_t\}PK_{RS}$;

(6)$RS \rightarrow HACKER:\{P\_r\}PK_{HACKER}$;$HACKER \rightarrow C:\{P\_r\}PK_C$。

协议运行的第(6)步,资源服务器将受保护资源加密发送出来后,被攻击者截获后利用自己的私钥解密,从而窃取受保护资源,而 C 并不知道自己接收到的消息实际是 HACKER 转发而来的。

5 结束语

OAuth 2.0 协议关系到用户账号、密码等个人隐私信息,与人们生活息息相关。本文提出使用 http 通道对 OAuth 2.0 协议数据进行传输,运用模型检测技术,通过 Promela 语言以及 SPIN 工具对经公钥体系加密的 OAuth 2.0 协议运行过程进行仿真,发现一条中间人攻击路径。仿真结果表明,利用公钥加密体系对 OAuth 2.0协议加密并不安全。下一步工作将尝试利用私钥体系对 OAuth 2.0进行加密改进,并对其安全性进行验证。

参考文献:

[1] Hardt D. The OAuth 2.0 authorization framework(draft-ietf-oatuth-v2-31)[EB/OL]. [2012-08-01]. https://tools.ietf.org/id/draft-ieft.org/id/draft-ietf-oauth-v2-31.html.

[2] Pai S, Sharma Y, Kumar S, et al. Formal verification of OAuth 2.0 using Alloy framework[C]// Proc of 2011 International Conference on Communication Systems and Network Technologies (CSNT),2011:655-659.

[3] Sun San-Tsai. Simple but not secure:An empirical security analysis of OAuth2.0-based single sign-on systems[D]. Vancouver:University of British Columbia,2012.

[4] Chen Wei,Yang Yi-tong,Niu Le-yuan. Improved OAuth2.0 protocol and analysis of its security[J]. Computer Systems & Applications,2014,23(3):25-30.(in Chinese)

[5] Wang Huan-xiao,Gu Chun-xiang,Zheng Yong-hui. Formal security analysis of OAuth 2.0 authorization protocol[J]. Journal of Information Engineering University,2014,15(2):141-147.(in Chinese)

[6] Yu Peng,Wei Ou,Han Lan-sheng,et al. Model checking network transmission intervention policies[J]. Journal of Frontiers of Computer Science and Technology,2014,8(8):906-918.(in Chinese)

[7] Xiao M H,Ma C L,Deng C Y,et al. A novel approach to automatic security protocol analysis based on authentication event logic[J]. Chinese Journal of Electronics,2014,23(2):235-241.

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

[9] Hu Liang-wen,Ma Jin-jing,Sun Bo. SPIN-based verification framework for SysML activity diagram[J]. Journal of Frontiers of Computer Science and Technology,2014,8(7):836-847.(in Chinese)

[10] Maggi P,Sisto R. Using SPIN to verify security properties of cryptographic protocols[C]// Proc of the 9th International SPIN Workshop Grenoble,2002:187-204.

[11] Dolev D,Yao A C. On the security of public key protocols [J]. IEEE Transactions on Information Theory,1983,29(2):198-208.

[12] Hou Gang,Zhou Kuan-jiu,Yong Jia-wei,et al. Survey of state explosion problem in model checking[J]. Computer Science,2013,40(z1):77-85.(in Chinese)

[13] Jamal B,Mohamed El-M,Hongyang Q,et al. Communicative commitments:Model checking and complexity analysis [J]. Knowledge-Based Systems,2012,35:21-34.

[14] Yang Yuan-yuan,Ma Wen-ping,Liu Wei-bo. The construction of changeable intruder model in model checking [J]. Journal of Beijing University of Posts and Telecommunications,2011,34(2):54-57.(in Chinese)

[15] Li Xing-feng,Zhang Xin-chang,Yang Mei-hong,et al. Study on modularized model checking method based on SPIN [J]. Journal of Electronics & Information Technology,2011,33(4):902-907.(in Chinese)

[16] Xiao Mei-hua,Xue Jin-yun. Formal description of properties of concurrency system by temporal logic [J]. Journal of Naval University of Engineering,2004,16(5):10-13.(in Chinese)

[17] Salamah S,Ochoa O,Jacquez Y. Using pairwise testing to verify automatically-generated formal specifications[C]// Proc of 2015 IEEE 16th International Symposium on High Assurance Systems Engineering (HASE),2015:279-280.

附中文参考文献:

[4] 陈伟,杨伊彤,牛乐园. 改进的 OAuth2.0 协议及其安全性分析[J]. 计算机系统应用,2014,23(3):25-30.

[5] 王焕孝,顾纯祥,郑永辉. 开放授权协议 OAuth2.0 的安全性形式化分析[J]. 信息工程大学报,2014,15(2):141-147.

[6] 余鹏,魏欧,韩兰胜,等. 模型检测网络传播干预策略[J]. 计算机科学与探索,2014,8(8):906-918.

[9] 胡良文,马金晶,孙博. 基于 SPIN 的 SysML 活动图验证框架[J]. 计算机科学与探索,2014,8(7):836-847.

[12] 侯刚,周宽久,勇嘉伟,等. 模型检测中状态爆炸问题研究综述[J]. 计算机科学,2013,40(z1):77-85.

[14] 杨元原,马文平,刘维博. 模型检测中可变攻击者模型的构造[J]. 北京邮电大学学报,2011,34(2):54-57.

[15] 李兴锋,张新常,杨美红,等. 基于 SPIN 的模块化模型检测方法研究[J]. 电子与信息学报,2011,33(4):902-907.

[16] 肖美华,薛锦云. 时态逻辑形式化描述并发系统性质[J]. 海军工程大学学报,2004,16(5):10-13.

作者简介:

程道雷(1991 -),男,江西上饶人,硕士生,研究方向为软件形式化方法和信息安全。**E-mail**:iamcimon@163.com

CHENG Dao-lei, born in 1991, MS candidate, his research interests include software formal method, and information security.

肖美华(1967 -),男,江西南昌人,博士后,教授,CCF 会员(E200014146s),研究方向为信息安全和软件形式化方法。**E-mail**:xiaomh@ecjtu.edu.cn

XIAO Mei-hua, born in 1967, post doctor, professor, CCF member(E200014146s), his research interests include information security, and software formal method.

刘欣倩(1990 -),女,辽宁营口人,硕士生,研究方向为信息安全和软件形式化方法。**E-mail**:liuxinqianlxq@sina.com

LIU Xin-qian, born in 1990, MS candidate, her research interests include information security, and software formal method.

梅映天(1992 -),女,安徽池州人,硕士生,研究方向为软件形式化方法和信息安全。**E-mail**:meiyingtian@sina.com

MEI Ying-tian, born in 1992, MS candidate, her research interests include software formal method, and information security.

李伟(1993 -),男,江西吉安人,研究方向为信息安全。**E-mail**:macsokolot@gmail.com

LI Wei, born in 1993, his research interest includes information security.