Kerberos 协议的形式分析与 NuSMV 检验

张春永
(盐城工学院 信息工程学院,江苏 盐城 224051)

摘要:NuSMV 是一个基于计算树逻辑的符号化模型检验工具。对 Kerberos 认证协议进行分析,并对其建立有限状态机模型,利用 NuSMV 保密性、认证性和活性等从3个方面进行了验证,指出 Kerberos 协议存在不安全性。

关键词:符号模型检测;计算树逻辑 CTL;NuSMV;Kerberos 协议
中图分类号:TP39 **文献标识码**:A **文章编号**:1671-5322(2009)04-0039-05

Kerberos 协议是给计算机网络提供身份验证的安全协议,其基础是基于信任第三方、集中的进行用户认证和发放电子身份评证。它提供了在开放型网络中进行身份认证的方法,认证实体可以是用户或用户服务,这种认证不需要保证网络上所有主机的物理安全性。本文使用 NuSMV 对 Kerberos 协议的安全性进行了分析。

1 NuSMV 系统

NuSMV 是一个开放的,灵活性强的模型检测工具,它具有良好的结构和详细的开发说明文档。为有利于技术上的交流与合作,NuSMV 力求在设计上符合健壮性、易于修改和接近于工业标准的要求。

NuSMV 提供了3种运行模式,即:批处理模式、命令行交互模式(the interactive shell)和图形用户界面模式。图形用户界面模式是在命令行模式之上开发的,它通过命令行模式来分割进程和与 NuSMV 通信,所以后两种方式本质上是一样的[1]。

NuSMV 输入语言可以用于描述确定的和不确定的系统。相对于 CMU SMV, NuSMV 输入语言扩充了系统规范的表达方式,在 NuSMV 中的属性可以使用 LTL 和不变量来表示。

NuSMV 程序使用 NuSMV 提供的输入语言对系统模型进行描述,使用 CTL 公式和 LTL 公式对系统规范进行描述。

2 Kerberos 认证系统 NuSMV 建模与检验

2.1 Kerberos 协议简介

Kerberos 协议最初是为 MIT 的 Athena 项目而设计的,其主要目的是在服务器和客户之间进行密钥交换和身份认证。出于对用户实现和安全分析的考虑,Kerberos 的认证中心服务任务被分配到两个独立的服务器:AS(认证服务器,它同时连接并维护一个中央数据库存放用户口令、标示等重要信息)和 TGS(票据授权服务器)。因此 Kerberos 系统由4个部分组成:AS、TGS、Client、Server。

Kerberos 系统的基本模型如图1所示:

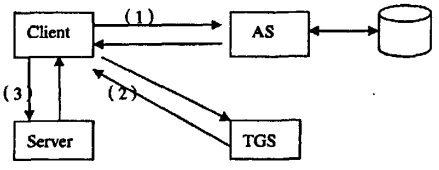

图1 Kerberos 认证过程

Fig. 1 Authentication process of kerberos

Kerberos 工作原理分3个阶段共6个步骤。

阶段1:认证业务交换过程,完成客户向 KDC 请求与 TGS 通信时使用的凭据及其会话密钥的过程。

(1)客户在工作站上向 AS 发送包含有客户方名字(用户名),服务器名字的消息。

收稿日期:2009-02-23
作者简介:张春永(1970-),男,江苏建湖人,讲师,硕士,主要研究方向为计算机软件设计。

消息1 C AS:C,tgs;

(2)AS验证C的真实性和访问权限后,随机生成一个加密密钥Kc,tgs作为下一阶段客户方与TGS通信时使用的会话密钥,构造一个包含客户方,会话密钥及其开始和失效时间等信息的特殊凭据TGT,用TGS的密钥进行加密。AS将新的会话密钥和TGT用客户方的密钥Kc加密回给客户方。

消息2 AS C:{Kc,tgs}Kc,{Tc,tgs}Kc,tgs;

阶段2:授权凭据业务交换过程,是客户方C向TGS请求与最终的应用服务器进行通信所需要的凭据和会话密钥的过程。

(3)客户方向TGS发送包含一个访问TGS用的TGT,需要访问的服务器的名字,以及一个身份认证者Authenticator的消息,Authenticator即用会话密钥签名的客户方信息,这是为了保证这些数据在传输过程中没有被篡改。

消息3 C TGS:{Ac}Kc,tgs,{Tc,tgs}Ktgs;

(4)TGS将客户与服务器之间使用的新的会话密钥和新的服务器凭据用它从客户方发来的TGT中获得的会话密钥Kc,tgs加密后传回给客户方,完成TGS交换。

消息4 TGS C:{Kc,s}Kc,tgs,{Tc,s}Ks;

阶段3:用户/服务器双向认证交换过程,客户方通过递交服务器凭据证明自己的身份的同时,通过一个典型的挑战/响应消息交换服务器向可和证明自己的身份。

消息5 C S:{Ac}Kc,s,{Tc,s}Ks;

消息6 S C:{t}Kc,s;

其中:Tc,tgs={c,tgs,addr,t,life,Kc,tgs}Ktgs

Tc,s={s,c,addr,life,Kc,s}Ks

Ac={c,addr,t}Kc,s

2.2 Kerberos协议建模与NuSMV实现

模型检测技术用于有限状态系统,为此我们为Kerberos协议构造了如下的有限状态系统模型:参与协议运行的主体集合:{初始者A,响应者B,服务器AS,TGS,入侵者I}。其中A,B,S,TGS是诚实的主体,他们将严格按照初始者、响应者、服务器TGS的身份参与协议运行,而入侵者可以以自己身份参与协议运行,不受协议限制。

程序中使用了5个模块Sender、Receiver、Server、TGS、Intruder分别表示消息的发送方、接受方、服务器(AS)、TGS和入侵者。他们之间的通信通过通道实现:

MODULE chan(input)

VAR output: {mess1, mess2, mess3, mess4, mess5, mess6, none};

ASSIGN next(output) := input;

每个模块中有一个状态变量状态,各个状态有各自的状态迁移过程。模块中状态迁移的实现方法为:实体接收到的消息满足状态迁移,那么就使用NuSMV的next()操作,确定模块状态变量的下一刻的值,并使状态迁移。其中初始者的状态迁移过程如图2所示:

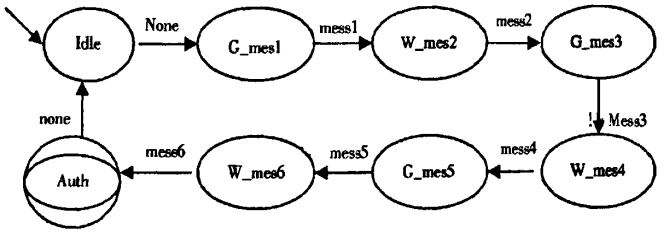

图2 初始者的状态迁移图

Fig.2 Transition graph of the initial status

为了模拟协议运行,服务器S在受到消息1后,我们通过变量initator和responder来记录协议运行的消息的产生者和消息的响应者。初始者A在受到消息2后,通过变量ack_msg记录A得到的消息,当服务器TGS接受到消息3时,通过变量tsg_msg记录得到消息,并为其产生与响应者B的会话密钥Kab;当响应者B接受到消息5后,分别用变量resp_ta,initator记录时间戳ta和协议运行的初始者A。为了便于检验,我们针对不同的主体引入不同的计数器:A_session_B和B_session_A分别表示A(或B)作为初始者(或响应者)和B(或A)开始认证的次数,所有的计数器(包括入侵者的计数器)的初始值均为0。

响应者B、服务器S和TGS的状态迁移和初

始者的状态迁移类似,只要满足消息条件,就将其状态迁移。若进入 Auth,则表示完成一次认证。为了使协议检验更具有实际意义,我们假设入侵者对通道有完全的控制能力,我们用 NuSMV 系统模拟入侵者能够偷听、拦截、存储、转发、重放消息,其协议通信模型如图 3 所示,任何主体之间的通信都要经过入侵者 I[2]。

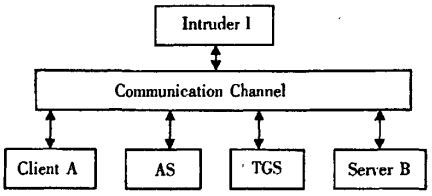

图 3　协议通信模型

Fig. 3　Protocol communication model

入侵者也对应一个非常复杂的有限状态机,它可以以初始者、响应者、服务器 S 和 TGS 身份参与协议运行。其中入侵者作为响应者的有限状态迁移图如图 4 所示[3,4]:

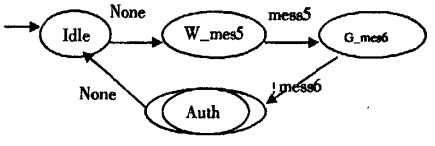

图 4　入侵者作为响应者的状态迁移图

Fig. 4　Status transition graph of intruder as a response

在初始状态时入侵者只拥有自己和服务器方 S 的共享密钥 Kis,随着协议的运行,入侵者拥有的知识逐渐增加,在协议运行的第 1 步入侵者可以截取消息 1,从而获得通信的各方 A 和 B 的消息。协议运行的第 2、3、4、5、6 步,入侵者可以截获消息 2、3、4、5、6。为了记录入侵者拥有和存储的知识,引入了一个一维数组 know_mess,存储入侵者截取到的消息。在程序中,入侵者可以偷听存储消息、重放消息。也可以转发消息、修改消息等。在入侵者引入计数器 I_get_kab 来记录 I 获得 A 和 B 之间的密钥次数。

入侵者 I 的知识获取工作过程:

(1) 将窃听到的由 A、B、S、TGS 发出的消息用自己的密钥解密,若可获取 Kas 或 Kbs,则将 Kas 或 Kbs 加入知识集合;

(2) 将窃听的由 A、B、S、TGS 发出的消息加入相应的一维数组 know_mess 中;

发送消息时进行冒充,I 作为初始者,可冒充 A 的身份,以 I(A)参与协议运行;I 作为响应者时,可冒充 B 的身份,以 I(B)参与协议运行;I 作为服务器时,可冒充 S 和 TGS 的身份,以 I(S)和 I(TGS)参与协议运行。I 在冒充时,根据知识集合可在发出的消息中运用 Kas 或 Kbs,并可重放截取到的消息。

入侵者 I 的攻击目的:

非法获取只有主体 A,B 才能知道的共享密钥 Kab。入侵者 I 获取 Kab 有两种途径:

(1) I 用自己产生的 Ki 来欺骗主体 A,B,使他们认为 Ki 是 Kab;

(2) TGS 产生的密钥 Kab,用 Ki 加密,以{Kab}Ki 的形式出现,I 解密此消息获得 kab;

为了描述 Kerberos 协议中的消息,我们构造了枚举类型 message,其各域为:

Message:{none, mess1, mess2, mess3, mess4, mess5, mess6};消息类型,none, mess1, mess2, mess3, mess4, mess5, mess6 分别对应 Kerberos 协议中的消息 1,2,3,4,5,6,none 表示没有消息。

Initator:{sendID, receiverID, serverID, InstruderID, tgsID};消息的发送者。

Responder:{sendID, receiverID, serverID, InstruderID, tgsID};消息的接受者。

Key:{Kab, Kas, Kbs, Kat};消息的加密密钥

status:{idle, G_mes1, W_mes2, G_mes3, W_mes4, G_mes5, W_mes6, Auth};初始者的状态

status:{idle, W_mes1, G_mes2, auth};服务器 AS 的状态

status:{idle, W_mes3, G_mes4, auth};服务器 TGS 的状态

status:{idle, W_mes5, G_mes6, auth};响应者的状态

status:{eavesdrop, remove, generate, store, send};入侵者的状态

2.3　NuSMV 对 Kerberos 协议属性检验

使用 NuSMV 为系统建立模型后,可用 SPEC 说明来描述系统属性[6]。

2.3.1　认证性

确定对方的真实身份与对方所称的身份是否一致。根据一致性原则,如果 B 要认证 A 的身份,那么在任何情况下 A 作为初始者开始与接受

方B会话次数AcouterB不小于B作为响应者与A完成会话次数,B接受到消息时的次数有两部分组成:couterR和IcounterB,用CTL来描述即为:AG(s. AcouterB >= (r. couterR + i1. IcounterB));如果存在A发送的消息小于B接受到的消息,则说明了入侵者冒充A向B进行认证。同样,我们可以同理来描述初始者对响应者B的身份认证。在认证过程中我们也可以用EF((r. initator = receiverID & i1. responder = instruderID) -> r. RtoI = 1)来判断入侵者能冒充发送方接受到响应方发送的认证消息。

2.3.2 保密性

在Kerberos协议中,保密性就是要求入侵者在任何情况下不能获取会话密钥Kab,用CTL来描述即为:AG(I_get_kab = 0)或AG(i1. responder = instruderID & i1. initator = serverID) -> AF(i1. key = kab),如果入侵者能获取Kab,则协议不具备保密性。

2.3.3 完整性

在Kerberos协议中,如果协议具备保密性,即不会泄漏任何密钥,那么入侵者不会解密消息中内容,不可能删除、更改加密过的任何内容。

2.3.4 活性

协议的活性是指协议运行时一些好的事情会发生,这些好的事情包括:预定的事情会发生、指定的协议状态会到达、应该进行的协议活动会进行等。在这里,Kerberos协议中,每个实体最终都能到达所属的Auth。我们用CTL语言描述初始者的活性为:

EF(s. status = idle -> s. status = Auth),如果为真,则说明协议具有活性。

其中A,G,E,F,→ ,& 都是CTL的符号,含义为:

AG, 所有路径的所有状态;

AF, 所有路径的最后状态;

EF, 最终存在路径到达状态;

→,逻辑蕴含;

&, 逻辑与。

3 检验结果分析

最后使用NuSMV-2.1.2版来运行Kerberos协议的Nusmv程序,发现Kerberos协议并不满足安全性质,对于每种属性均有违背安全性质的反例,这些反例正好时入侵者I对Kerberos协议的攻击。有如下检测结果:

Checking CTL property <0>...

-- specification (AG(s. A_session_B >= (r. B_session_A + i1. I···33counterB))) is false

说明此协议不符合安全协议的要求,经过分析,协议存在如下攻击:入侵者偷听到A向B发送的消息5,并将消息5转发给B,这样B认为A请求了两次会话连接,而实际上A仅有一次会话请求,从而造成了入侵者可以进行重放攻击。

Checking CTL property <1>...

-- specification (AG(I_get_kab = 0)) is false

给出的反例说明协议的不具有保密性。攻击如下:

消息1.1 C I(AS):C,tgs;

此时入侵者I开始第二次Kerberos协议运行:

消息2.1 I AS:I,tgs ;

消息2.2 AS I:I ;

消息2.3 I TGS:I,{Ti,tgs}Ktgs;

消息2.4 TGS I:I,{Ti,tgs}Kai;

攻击中I(AS)表示I冒充AS,整个攻击过程为:入侵者I通过窃听消息1.1知道消息主体C欲和TGS建立会话密钥,则立即开始第二次运行协议,自己和自己运行协议,消息2.1的消息是消息1.1中的消息,服务器AS忠实自己的身份参与协议运行,入侵者I在消息2.3中放入自己产生的Ki,tgs,AS在消息2.4中返回用Ki,tgs加密的Kia,入侵者I在消息1.6中重放消息2.4的加密项。上述协议运行完,主体A认为它与B共享会话密钥Kab(=Kai),实际上它与I共享Kai,I攻击成功。

Checking CTL property <2>...

-- specification EF (s. status = idle -> s. status = Auth) is true

说明此协议满足活性的特点。

4 Kerberos V5的缺点

在Kerberos V5的整个验证过程中有很严格的假设前提和较为受限的验证方法,首先为了能够在客户机和KDC之间安全的传输数据,系统假设二者之间已经存在了一个共享的会话密钥,而这种密钥往往是通过在服务器上设置用户密码,然后在通知用户的做法实现的,显然它的缺点是不易扩展,还有安全级别不高,因为用户往往愿意

设置较为简单的密码。其次就是在作验证是,服务器采用时间戳作为验证方法,这就要求验证的双方服务器的时钟需要同步,但在规模较大的网络中时钟不同步是时有发生的,所有这样影响了验证的正确性。

5 结束语

Kerberos协议自诞生以来已得到广泛的应用,增强了网络通信的安全,但是Kerberos协议本身存在缺陷,本文利用NuSMV提供的模块化和分层描述的特点,为Kerberos协议建立了NuSMV模型,从认证性和保密性两个方面对Kerberos认证系统进行了安全性的验证,认为该协议不满足安全性。

参考文献:

[1] Panti M, Spalazzi L, Tacconi S. Using the NuSMV Model Checker to verify the Kerberos Protocol, Istituto di Informatica [M]. Via Brecce Bianche: University of Ancona, 2001.
[2] 古天龙,蔡国勇. 网络协议的形式化分析与设计[M]. 北京:电子工业出版社,2003:84-120.
[3] Kerberos RFC 1510[EB/OL]. http://www.freesoft.org/CIE/RFC/1510/1.htm.
[4] 张红旗,车天伟,李娜. Kerberos身份认证协议分析及改进[J]. 计算机应用,2002(12):24-28.
[5] 李毅,王道平. Kerberos原理及应用[J]. 应用技术,2004(3):36-41.
[6] 刘峰,李周军,李梦军,等. 基于SMV的安全协议模型检测[J]. 计算机工程与科学,2004(11):27-32.

Form Analysis of Kerberos Protocal and NuSMV Verification

ZHANG Chun-yong
(School of Information Engineering, Yancheng Institute of Technology, Jiangsu Yancheng 224051, China)

Abstract: NuSMV is a symbolic model verification tool based on computation tree logic. The Kerberos authentication protocal was analysed, and the finite state model was set up. The non-security of Kerberos protocol exists which was verifing from security property, authentication and liveness using NuSMV.

Keywords: symbolic model checking; Computation tree logic CTL; NuSMV; Kerberos protocol

(责任编辑:张英健; 校对:沈建新)

(上接第12页)

Effect of Hydrothermal Conditions on the Hydration and Drying Shrinkage of Portland Cement

CAI An-lan
(School of Materials Engineering, Yancheng Institute of Technology, Jiangsu Yancheng 224051, China)

Abstract: In different hydrothermal conditions, the hydration and drying shrinkage properties of Portland cement were studied by measuring strength and drying shrinkage (including reversible portion and irreversible portion), and by using MIP, TG-DSC, NMR analysis. Results show that approximately 2 d time water curing, increasing the temperature (from 20 ℃ to 60 ℃), increases the early (3 d) degree of hydration, the quantity of C-S-H gel, the degree of polymerization of hydrated silicates, the density of cement paste, the 3 d strength of Portland cement, and decreases remarkably 28 d strength and drying shrinkage. The reason that 60 curing has lower drying shrinkage is due to the chemical structure changes of C-S-H gel before drying which decreasing remarkably the irreversible shrinkage.

Keywords: Portland cement; hydration; drying shrinkage; hydrothermal condition; mechanism

(责任编辑:范大和; 校对:沈建新)