基于串空间理论的 Kerberos 协议分析

魏 浩,解争龙,弋改珍
(咸阳师范学院 信息工程学院,陕西 咸阳 712000)

摘 要:在介绍串空间理论基本概念、攻击者模型以及 Kerberos 协议的基础上,利用串空间理论得出 Kerberos 各协议参与主体和攻击者的迹,构造了协议的串空间,给出了 Kerberos 协议的丛图。在证明一个定理的基础上,使用启发式和反证法的思路,证明了认证服务器分配给客户端和应用服务器会话密钥的保密性,即攻击者从现有知识和构造能力无法推导出服务器分配给客户端和应用服务器的会话密钥;证明了客户端和认证服务器以及客户端和应用服务器能够相互认证,得出了 Kerberos 协议正确性的结论。

关键词:串空间;Kerberos 协议;保密性;认证性
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2013)12-0109-04
doi:10.3969/j.issn.1673-629X.2013.12.026

Analysis of Kerberos Protocol Based on Strand Space Theory

WEI Hao, XIE Zheng-long, YI Gai-zhen
(College of Information Engineering, Xiangyang Normal University, Xianyang 712000, China)

Abstract: Based on the theory of the string space, the model of the attacker and the Kerberos protocol, obtain traces of the subject involved in Kerberos protocol and the attacker with string space theory, and establish string space and bundles of the Kerberos protocol. It is proved that the session key of the client and application server assigned by authentication server is confidential by heuristic and reduction to absurdity. The attacker can not obtain the session key from existing knowledge and building capacity. The client and the authentication server and client and application server can be authenticated each other. It is concluded that the Kerberos protocol is correct.

Key words: string space; Kerberos protocol; confidentiality; authenticity

0 引 言

Kerberos 协议[1-4]是一种计算机网络授权访问协议,用来在非信任的网络环境中,以密码学为基础对个人通信以安全的手段进行身份认证。Kerberos 采用单钥密码体制,使用 Needlham-Schroeder 认证协议为基础,由可信赖的服务器为支持,以客户服务器模式实现。它是为 TCP/ IP 网络设计的可信第三方鉴别协议, Kerberos 服务器提供了安全的网络鉴别,允许用户访问网络中的不同服务器。

Fabrega、Herzog 和 Guttman 1998 年建立了串空间模型[5-8],串空间模型属于定理证明方法,它使安全协议的形式化分析技术有了新的发展。形式化分析技术常常因为晦涩复杂受到批评,串空间模型是一种启发式的安全协议证明方法,它具有直观、严谨、简洁等特点。串空间模型的证明依据详细的协议行为,具有更高的可信赖性。

文中介绍了串空间模型的基础理论,并且利用串空间模型对 Kerberos 协议进行分析和验证,证明了该协议的保密性和认证性。

1 串空间模型的基本理论

1.1 基本概念

设 T 和 K 为两个原子项集合,且 T 和 K 不相交。T 是具有原子属性的明文集合,包含如姓名、随机数、时间戳和银行帐号等几种不同类型的原子项信息,A 是协议交互过程当中协议主体可能传递的消息集合,K 是所有密钥集合,集合 A 包含子集 K 和子集 T,且 $K \cap T=\varnothing$。

收稿日期:2013-03-23 **修回日期**:2013-06-25 **网络出版时间**:2013-09-29
基金项目:陕西省科技计划项目(SJ08ZT14-8);陕西省教育自然科学基金项目(08JK481);咸阳师范学院基金项目(06XSYK277)
作者简介:魏 浩(1973-),男,讲师,硕士,研究方向为网络安全;解争龙,教授,硕士,研究方向为网络安全;弋改珍,副教授,研究方向为网络安全和无线网络。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20130929.1521.001.html

在 A 上进一步定义的三种运算:

二元加密运算(encr):$K\times A\rightarrow A$;

一元运算逆运算(inv):$K\rightarrow K$;

二元运算连接(join):$A\times A\rightarrow A$。

encr(K,m)记为$\{m\}_K$,表明了加密运算;inv(K)记为K^{-1},表明了 K 的逆;join(a,b)记为 ab,表明了连接运算。这三种运算代表了安全协议主体构造消息的能力。

1.1.1 串(Strand)和串空间(Strandspace)

串定义为对于诚实的协议参与主体包括发送和接收事件的序列。一个串就对应了一个协议参与者。将一个串映射到有限序列消息集(士 A)*,这个映射称为迹映射,映射的像称为原像的迹,把串的迹也称为串。

串空间是串的集合,包括诚实主体串及攻击串,串空间指一个集合$\sum$,集合$\sum$中的元素就称为串,且满足在这个集合上存在迹映射:tr:$\sum\rightarrow$(士 A)*。

串空间具备如下性质:

(1)设 $s\in\sum$,i 是满足 $1\leqslant i\leqslant$length(tr(s))的任一整数,用二元组<s,i>表示节点,N 是节点集合,节点<s,i>属于串 s;

(2)假如 $n=<s,i>\in N$,则 index(n)= i,strand(n)= s,term(n)= (tr(s))$_i$,n 就是串 s 的迹的第 i 个符号项;

(3)针对 n_A,$n_B\in N$,如果存在一条边 $n_A\rightarrow n_B$,当且仅当 term(n_A)= $+a$ 且 term(n_B)= $-a$,其中 $a\in A$。它表示节点 n_A发送且节点 n_B接收消息 a,表示节点 n_A和节点 n_B间的因果连接;

(4)如果 $n_A=<s,i>\in N$,$n_B=<s,i+1>\in N$,有边 $n_A\rightarrow n_B$存在,这类边表示 n_A是 n_B在串 s 上的直接因果前驱,用 $n_A\rightarrow^+ n_B$表示因果前驱;

(5)当 $t\subset$term(n),无符号项 t 出现在 $n\in N$;令 I 为无符号项集合,节点 $n\in N$ 是集合 I 的进入点,当 term(n)= $+t$, $n'\Rightarrow^+ n$,term(n') $\notin I$;当 n 是集合 $I=\{t':t\subset t'\}$ 的进入点,无符号项 $t\subset$term(n)起源于 $n\in N$;当 t 唯一起源于 $n\in N$,无符号项 t 就是唯一起源。

1.1.2 丛与节点的关系

串空间的丛是节点构成的有向图的一个有限子图,丛高度(c-height)是指丛中节点<s,i>最大的 i 的值。

1.1.3 理 想

如果 $K'\subset K$,$I\subset A$,集合 A 的一个 K'-理想的定义为:对于所有的 $h\subset I$,$g\subset A$ 和 $K\in K'$满足

①hg,$gh\in I$;

②$\{h\}_K\in I$,使用 $I_{K'}[h]$表示包含消息项 h 的最小 K'-理想。

1.2 攻击者模型

安全协议攻击者模型一般假设攻击者具有攻击安全协议设计缺陷的能力,而不具备攻击密码体制的能力,在此假设基础上,不同攻击者模型对攻击者的能力也会有不同的描述。

攻击者能够获得一些消息包括掌握的密钥集合和通过明文传输的信息,攻击者通过拥有的密钥和获得的消息构造新消息。攻击者能力包括:生成文本消息、连接、分离、重放或删除消息、加密等操作,入侵者对协议进行攻击时一般需要把这些原子操作中的某几个结合起来。

$F[g]$. $<-g>$:截获到一个新消息;

$T[g]$. $<-g,+g,+g>$:截获到一个新消息又转发;

$M[t]$. $<+t>$,$t\in T$:发出一个原子项消息;

$C[g,h]$. $<-g,-h,+gh>$:将截获的两个消息连接后发送;

$s[g,h]$. $<-gh,+g,+h>$:将截获的连接消息分拆后发送;

$K[k]$. $<+k>$:发送一个攻击者已知的密钥;

$E[k,h]$. $<-k,-h,+\{h\}_k>$:加密截获到消息并发送,表明了攻击者的加密能力;

$D[k,h]$. $<-k^{-1},-\{h\}^k,+h>$:解密截获到的消息后并发送,表明了攻击者的解密能力。

2 Kerberos 协议

Kerberos 使用两个服务器:鉴别服务器(Authentication Server,AS)、票据授予服务器(Ticket-Granting Server,TGS),它们位于同一服务器 S 上。A 是请求服务的客户,而 B 是被请求的服务器。A 通过 Kerberos 向 B 请求服务[9-10]。Kerberos 需要通过协议以下六个步骤鉴别的确是 A 向 B 请求服务后:

M1 $A\rightarrow S$: A,B

M2 $S\rightarrow A$: $\{K_S,\{A,K_S\}_{K_{Tc}}\}_{K_A}$

M3 $A\rightarrow S$: $\{T\}_{K_S},B,\{A,K_S\}_{K_{Tc}}$

M4 $S\rightarrow A$: $\{B,K_{AB}\}_{K_S},\{A,K_{AB}\}_{K_B}$

M5 $A\rightarrow B$: $\{T\}_{K_{AB}},\{A,K_{AB}\}_{K_B}$

M6 $B\rightarrow A$: $\{T+1\}_{K_{AB}}$

3 Kerberos 串空间

(1)令$\{A,K_S\}_{K_{Tc}}=X$,$\{A,K_S\}_{K_{Tc}}=Y$,$\{A,K_{AB}\}_{K_B}=Z$,集合 Init[$A,B,K_S,X,T,T+1,Y,K_{AB},Z$]中的元素 $s\in\sum$ 且 s 具有如下的迹:

$<+A,-\{K_S,\{A,K_S\}_{K_{Tc}}\}_{K_A},+\{T\}_{K_S},B,\{A,K_S\}_{K_{Tc}},-\{B,K_{AB}\}_{K_S},\{A,K_{AB}\}_{K_B},+\{T\}_{K_{AB}},\{A,K_{AB}$

$\{\!|T_A+1|\!\}_{K_{AB}}>$

和某个 $s \in \text{Init}[A,B,K_S,X,T,T+1,Y,K_{AB},Z]$ 相关联的协议主体是 A。

(2) 集合 $s \in \text{Serv}[A,B,T,K_S,K_{AB},X]$,其中 $K_{AB} \notin K_p$ 且 $K_{AB} \notin \{\!|K_S, K_B: A,B \in T_{\text{name}}|\!\}$ 且 $K_{AB}=K_{AB}^{-1}$,该集合中的元素 $s \in \sum$ 且 s 具有如下的迹:

$<-A,+\{\!|K_S,\{A,K_S\}_{K_{TC}}|\!\}_{K_A},-\{T\}_{K_S},B,\{\!|A,K_S|\!\}_{K_{TC}},+\{B,K_{AB}\}_{K_S},\{\!|A,K_{AB}|\!\}_{K_B}>$

和某个 $s \in \text{Serv}[A,B,T,K_S,K_{AB},X]$ 相关联的协议主体是 S。

(3) 集合 $\text{Resp}[A,B,T,T+1,K_{AB}]$,其中 $K_{AB} \notin K_p$ 且 $K_{AB} \notin \{\!|K_S, K_B: A,B \in T_{\text{name}}|\!\}$ 且 $K_{AB}=K_{AB}^{-1}$,该集合中的元素 $s \in \sum$ 且 s 具有如下的迹:

$<-\{T\}_{K_{AB}},\{\!|A,K_{AB}|\!\}_{K_B},+\{\!|T_A+1|\!\}_{K_{AB}}>$

和某个 $s \in \text{Resp}[A,B,T,T+1,K_{AB}]$ 相关联的协议主体是 B。

$\sum=\text{Init}\cup\text{Resp}\cup\text{Serv}\cup P$,$\sum$ 是 Kerberos 串空间的一个渗入串空间,其中 P 代表侵入者串的集合。

图 1 为 Kerberos 协议串空间模型的丛图。

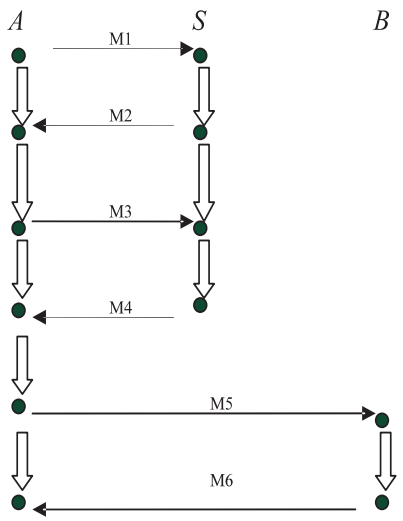

图 1　Kerberos 协议串空间模型的丛图

4　Kerberos 协议正确性证明

定理 1:假设 $K \in K, S \subset A$,任意 $s \in S$,s 宽度为 1,$s \neq \{g\}_K$,如果 $\{h\}_K \in I_{K'}[S], K \in K'$。

证明:假设 $\{h\}_K \in I_{K'}[S], K \notin K'$。集合 $I'=I_{K'}[S]\backslash\{\{h\}_K\}$。因为 S 不包含一个最外层加密密钥为 K 的元素,所以 $S \subset I'$。$I_{K'}[S]$ 是包含 S 最小 K' - 理想,根据最小 K' - 理想定义当 $\{h\}_K \in I_{K'}[S]$ 时,$h \in I_{K'}[S]$。

根据自由加密假设对任意的 $h' \notin I', K' \notin K', \{h'\}_{K'} \notin I'$,因此满足理想定义,$I'$ 是一个包含 S 的 K' - 理想,与 $I_{K'}[S]$ 是包含 S 最小 K' - 理想相矛盾。

4.1　保密性

证明协议的保密性主要是证明服务器 S 为主体 A、B 会话发布密钥 K_{AB} 不会泄露,除非入侵者拥有 K_{AS} 或者 K_{BS},也就是说 K_{AB} 不会被非协议主体所持有的长期密钥加密。

转化成如下命题:

命题 1:假定 C 是 Kerberos 串空间 $\sum$ 中的一个丛;$A,B \notin T_{\text{name}}$;$K_{AB}$ 是唯一起源的;$K_S,K_B \notin K_p$;令 $\{A,K_S\}_{K_{TC}}=X$,$\{\!|A,K_S|\!\}_{K_{TC}}=Y$,$\{\!|A,K_{AB}|\!\}_{K_B}=Z$ 且 $\text{Serv}[A,B,T,K_S,K_{AB},X]$。让 $S=\{\!|K_A,K_S,K_B,K_{TG},K_{AB}|\!\}$,且 $K'=K\backslash S$。对每个节点 $m \in C$,$\text{term}(m) \notin I_{K'}[K_{AB}]$。

证明:利用反证法。假设存在一个正常节点 m 是 $I_{K'}[K_{AB}]$ 的进入点,$\text{term}(m)$ 必是集合 $I_{K'}[K_{AB}]$ 成员,K_{AB} 是 $\text{term}(m)$ 的子项。

根据进入点的定义,m 是某个正常 s 上的一个符号为正的正常节点上,从图 1 可以看出,对于 $K_{AB} \in \text{term}(m)$ 分两种情况:

$s \in \text{Serv}[A,B,T,K_S,K_{AB},X]$ 且 $m=<s,4>$,由于 K_{AB} 唯一起源,所以 $s=s_{\text{serv}}$,$\text{term}(m)=\{B,K_{AB}\}_{K_S}$,或者 $\text{term}(m)=\{\!|A,K_{AB}|\!\}_{K_B}$,由定理 1 推出 $K_S \in K'$ 或 $K_B \in K'$,与假设 $K'=K\backslash S$ 矛盾。

$s \in \text{Init}[A,B,K_S,X,T,T+1,Y,K_{AB},Z]$ 且 $m=<s,5>$,由于 K_{AB} 唯一起源,所以 $s=s_A$,$\text{term}(m)=\{\!|A,K_{AB}|\!\}_{K_B}$,由定理 1 推出 $K_B \in K'$,与假设 $K'=K\backslash S$ 矛盾。

4.2　认证性

4.2.1　A 认证 B 和 S

命题 2:假定 C 是 Kerberos 串空间 $\sum$ 中的一个丛;$A \neq B$;$K_A,K_S,K_B,K_{TG} \notin K_p$;若 $s \in \text{Init}[A,B,K_S,X,T,T+1,Y,K_{AB},Z]$ 且 $C-\text{height}=6$,则 C 中必然存在正常串。

① $s_{\text{resp}} \in \text{Resp}[A,B,T,T+1,K_{AB}]$ 且 $C-\text{height}=2$;

② $s_{\text{serv}} \in \text{Serv}[A,B,T,K_S,K_{AB},X]$ 且 $C-\text{height}=4$。

证明:从图 1 知,s 在 C 中的迹至少包含:$<+A,-\{\!|K_S,\{A,K_S\}_{K_{TC}}|\!\}_{K_A},+\{T\}_{K_S},B,\{\!|A,K_S|\!\}_{K_{TC}},-\{B,K_{AB}\}_{K_S},\{\!|A,K_{AB}|\!\}_{K_B},+\{T\}_{K_{AB}},\{\!|A,K_{AB}|\!\}_{K_B},-\{\!|T_A+1|\!\}_{K_{AB}}>$,$\{\!|T_A+1|\!\}_{K_{AB}}$ 必起源于 C 中的正常节点。从图 1 可知,该正常节点属于串 s_{resp},$s_{\text{resp}} \in \text{Resp}[A,B,T,T+1,K_{AB}]$,该节点为 $<s_{\text{resp}},2>$ 且 $<s_{\text{resp}},2> \in C$,故 $C-\text{height}(s_{\text{resp}})=2$。

从图 1 可知,$\{B,K_{AB}\}_{K_S}$,$\{\!|A,K_{AB}|\!\}_{K_B}$ 起源于 C 中的正常节点,该正常节点属于串 s_{serv},$s_{\text{serv}} \in \text{Serv}[A,B,T,K_S,K_{AB},X]$,该节点 $<s_{\text{serv}},4> \in C$,所以 $C-$

height(s_{serv}) = 4。

当 C - height(s_{init}) = 5 时,C - height(s_{resp}) = 2,C - height(s_{serv}) = 4,由此可见 A 能够认证 B 和 S。

4.2.2 B 认证 A 和 S

命题3:假定 C 是 Kerberos 串空间 $\sum$ 中的一个丛;$A \neq B$;$K_A, K_S, K_B, K_{TG} \notin K_p$;若 $s_{resp} \in$ Resp $[A, B, T, T+1, K_{AB}]$ 且 C - height = 2,则 C 中必然存在正常串。

① $s_{init} \in$ Init $[A, B, K_S, X, T, T+1, Y, K_{AB}, Z]$ 且至少 C - height = 5;

② $s_{serv} \in$ Serv $[A, B, T, K_S, K_{AB}, X]$ 且 C - height = 4。

证明:从图 1 知,s 在 C 中的迹至少包含:$< -\{T\}_{K_{AB}}, \{A, K_{AB}\}_{K_B}, +\{T_A + 1\}_{K_{AB}} >, \{T\}_{K_{AB}}, \{A, K_{AB}\}_{K_B}$ 必起源于 C 中的正常节点。

从图 1 可知,该正常节点属于串 $s_{init}, s_{init} \in$ Init $[A, B, K_S, X, T, T+1, Y, K_{AB}, Z]$,该节点为 $< s_{init}, 5 >$ 且 $< s_{init}, 5 > \in C$,故至少 C - height(s_{init}) = 5。

从图 1 可知,$\{A, K_{AB}\}_{K_B} \subset$ term($< s_{init}, 5 >$) 起源于 C 中的正常节点,该正常节点属于串 $s_{serv}, s_{serv} \in$ Serv $[A, B, T, K_S, K_{AB}, X]$,该节点为 $< s_{serv}, 4 >$ 且 $< s_{serv}, 4 > \in C$,所以 C - height(s_{serv}) = 4。

当 C - height(s_{resp}) = 2 时,能证明 C - height(s_{serv}) = 4,C - height(s_{init}) 至少为 5,$\{T+1\}_{K_{AB}}$ 不能被入侵者替换,也不会起源于入侵者,所以 B 能够认证 S 和 A。

4.2.3 S 认证 A 和 B

命题4:假定 C 是 Kerberos 串空间 $\sum$ 中的一个丛;$A \neq B$;$K_A, K_S, K_B, K_{TG} \notin K_p$;若 $s_{serv} \in$ Resp$[A, B, T, T+1, K_{AB}]$ 且 C - height = 4,则 C 中必然存在正常串。

① $s_{init} \in$ Init$[A, B, K_S, X, T, T+1, Y, K_{AB}, Z]$ 且至少 C - height = 3;

② $s_{resp} \in$ Resp $[A, B, T, T+1, K_{AB}]$ 且至少 C - height = 0。

证明:从图 1 可知,s 在 C 中的迹至少包含:$< -A, +\{K_S, \{A, K_S\}_{K_{TC}}\}_{K_A}, -\{T\}_{K_S}, B, \{A, K_S\}_{K_{TC}}, +\{B, K_{AB}\}_{K_S}, \{A, K_{AB}\}_{K_B} >, \{T\}_{K_S}$ 起源于 C 中的正常节点。从图 1 可知,该正常节点属于串 $s_{init}, s_{init} \in$ Init $[A, B, K_S, X, T, T+1, Y, K_{AB}, Z]$,该节点为 $< s_{init}, 3 >$ 且 $< s_{init}, 3 > \in C$,故至少 C - height(s_{init}) = 3。

从图 1 可知,$s_{serv} \in$ Resp $[A, B, T, T+1, K_{AB}]$ 中的串不起源于 $s_{resp} \in$ Resp $[A, B, T, T+1, K_{AB}]$ 中的串,所以 C - height(s_{init}) 至少为 3,由于 K_S 具有新鲜性,$\{B, K_{AB}\}_{K_S}, \{A, K_{AB}\}_{K_B}$ 不会被入侵者替换,S 能够认证 A。C - height(s_{resp}) 至少是 0,但无法认证 B。

5 结束语

在 Kerberos 协议中,服务器分配给 A、B 会话密钥过程中,会话密钥 K_{AB} 受到 K_A, K_S, K_B, K_{TG} 密钥的保护,而密钥 K_A, K_S, K_B, K_{TG} 不属于入侵者的密钥集,保证了 A、B 会话密钥的 K_{AB} 保密性;A、S 相互认证依赖于它们之间的共享的密钥 K_A,A、B 相互认证依赖于它们之间的共享的会话密钥 K_{AB},为了防止重放攻击在协议中加入时间戳 T,通过串空间理论的证明,A、S 能相互认证,并且 A、B 也能相互认证。Kerberos 协议达到了协议的设计目的,客户端与认证服务器、客户端与应用服务器能相互认证,并为客户端与应用服务器分配了会话密钥。

参考文献:

[1] NEUMANC. The kerberos network authentication service (V5)[S]. RFC 4120,2005.

[2] 文铁华,谷士文. 增强 Kerberos 协议安全性的改进方案[J]. 通信学报,2004,25(6):76-79.

[3] 胡 宇,王世伦. 基于混合体制的 Kerberos 身份认证协议的研究[J]. 计算机应用,2009,29(6):1659-1661.

[4] 杨战海. 基于 Kerberos 协议的用户到用户认证系统的研究[J]. 计算机技术与发展,2010,20(10):180-183.

[5] Thayer F. Strand space: Why is a security protocol correct [C]//Proc of the IEEE symposium on security and privacy. [s. l.]:IEEE Press,1998.

[6] Thayer F. Strand spaces: Proving security protocols correct [J]. Journal of computer security,1999,7(2/3):191-230.

[7] Thayer F, Herzog J C. Authentication tests[C]//Proceedings of the IEEE symposium on security and privacy. Oakland, CA, USA:IEEE Press,2000.

[8] Guttman J D, Thayer F. Authentication tests and the structure of bundles[EB/OL]. 2003-08-12. http://www. mitre. org/work/tech_papers/tech_papers_01/guttma n_bundles/index. html.

[9] 谢希仁. 计算机网络[M]. 第 5 版. 北京:电子工业出版社,2008:295-296.

[10] 王亚弟,束妮娜,韩继红,等. 密码协议形式化分析[M]. 北京:机械工业出版社,2006:169-180.

基于串空间理论的Kerberos协议分析

作者： 魏浩， 解争龙， 弋改珍， WEI Hao， XIE Zheng-long， YI Gai-zhen
作者单位： 咸阳师范学院 信息工程学院,陕西 咸阳,712000

刊名： 计算机技术与发展

ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2013(12)