对改进的无线认证协议 SSM 的分析

郭宇燕[1],魏仕民[2],卓泽朋[3]
GUO Yu-yan[1],WEI Shi-min[2],ZHUO Ze-peng[3]

1.宿州学院 计算机科学与技术系,安徽 宿州 234000
2.淮北煤炭师范学院 计算机科学与技术系,安徽 淮北 235000
3.淮北煤炭师范学院 数学系,安徽 淮北 235000
1.Dept. of Computer Science & Technique,Suzhou University,Suzhou,Anhui 234000,China
2.Dept. of Computer Science & Technique,Huaibei Coal Industry Teachers' College,Huaibei,Anhui 235000,China
3.Dept. of Mathematics,Huaibei Coal Industry Teachers' College,Huaibei,Anhui 235000,China
E-mail:guoyuyan428428@sohu.com

GUO Yu-yan,WEI Shi-min,ZHUO Ze-peng.Analyzing model of amended wireless authentication protocol SSM.Computer Engineering and Applications,2009,45(1):129-130.

Abstract: It is the first time to prove the Liu Xia's modified version of server-specific MAKEP protocol with the theory of strand space which is a rising formal analysis tool.Firstly,its confidentiality is analyzed,and two concepts honest and ideal are used to simplify the process of verification.It indicates that rs,rc are secret.Then its authentication is analyzed,the analysis contains responser's authentication and sponsor's authentication.At last,the result shows that the amended SSM protocol can reach the goal of the protocol.

Key words: SSM protocol;strand space;confidentiality;authentication

摘 要:针对刘霞提出的改进的 Server-specific MAKEP 协议,首次利用一种新兴的形式化分析工具—串空间模型对其进行分析。先对协议的机密性进行分析,并运用"理想"和"诚实"两个概念简化分析协议的步骤,证明了 rs,rc 是保密的,然后对协议的认证性进行分析,分析包括响应者认证和发起者认证。最终结果表明改进的 SSM 协议能够达到协议的安全目标。

关键词:SSM 协议;串空间;机密性;认证性
DOI:10.3778/j.issn.1002-8331.2009.01.040 **文章编号**:1002-8331(2009)01-0129-02 **文献标识码**:A **中图分类号**:TN918.1

1 引言

1998 年由 Thayer Fábrega,Herzog 和 Guttman 等人提出了串空间模型,该模型已经被应用于许多密码协议的安全性分析上面,下面就对串空间模型理论做简单介绍。

1.1 串空间基本概念(详细内容见文献[1])

定义 1(结点和串) 结点 n 是二元组(s,i),其中 $s\in\Sigma$,$(1\leqslant i\leqslant length(tr(s)))$,结点集合记为 N,则称结点$<s,i>$属于串 s。显然每个结点属于唯一的串。若 $n=<s,i>\in N$,则 $index(n)=i$,$strand(n)=s.term(n)$记为$(tr(s))i$,即串 s 路径中的第 i 个消息项。Un_$term(n)$记为$((tr(s))_i)_2$,即串 s 路径中的第 i 个消息项中的无符号部分,称为无符号语句。

定义 2(入点) 令 I 为无符号项集合。节点 $n\in N$ 是 I 的进入点,当且仅当 $term(n)=+a$,其中 $a\in I$,且对所有的 $n'\Rightarrow+n$,$term(n')\notin I$。

定义 3(起源) 无符号项 t 起源于 $n\in N$,当且仅当 $term(n)$ 的符号为正,且对 n 的任何一个前驱节点 n',有 $t\notin term(n')$。无符号项 t 是唯一起源的,当且仅当 t 唯一起源于 n。

1.2 串空间基本理论(详细理论见文献[2])

定理 1 假设 C 是 A 的一个丛,$K=S\cup\kappa^{-1},S\cap Kp=\Phi$。并且不存在这样的结点,此结点是属于 C 的正常结点且是 $I_k[S]$的一个进入点。那么对任何形如$\{g\}_k$ 的消息项(其中 $k\in S$)都不起源于一个入侵者串。

定理 2 假设 C 是 A 的一个丛,$K=S\cup\kappa^{-1}$, 并且 $S\cap Kp=\Phi$。如果存在一个结点 $m\in C$ 使得 $term(m)\in I_k[S]$,则一定存在一个正常结点 $n\in C$,使得 n 为 $I_k[S]$的一个进入点。

定理 3 假设 $k\in K,S\subseteq A$,且对任意 $s\in S$,s 都是简单的,且 s 不是形如$\{g\}_k$ 如果 $k\in K,\{h\}_k\in I_k[S]$,则 $k\in\kappa$。

2 用串空间模型理论分析协议

改进的无线认证协议 Server-specific MAKEP[3]如下:

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60773121);安徽省自然科学基金(the Natural Science Foundation of Anhui Province of China under Grant No.070412052)。

作者简介:郭宇燕(1984-),女,硕士生,研究方向:信息安全;魏仕民(1962-),男,博士,教授,研究方向:网络与信息安全;卓泽朋(1978-),男,讲师,研究方向:信息安全。

收稿日期:2007-12-27 **修回日期**:2008-03-13

$C\rightarrow S:\{rc,ID_C\}_{K_C},ID_C$

$S\rightarrow C:\{rc,rs,ID_s\}_{K_C}$

$C\rightarrow S:\{rs\}_{K_C}$

其中 K_C 是 C 的长期对称密钥;ID_C:用户 C 的身份标识;ID_S:服务器 S 的身份标识。

$T_{name}\subseteq T$, 其中的元素 C,S 是协议主体的名称; 映射 k: $T_{name}\rightarrow K$,且 $K_C=K_C^{-1}$;rc 是 C 产生的随机数,rs 是 S 产生的随机数。

下面用串空间模型对改进的无线认证协议 Server-specific MAKEP 协议进行分析。

2.1 定义协议模型

定义 4 (1)集合 $Init[C,S,rc,rs,ID_C,ID_S,K_C]$中元素 $s\in\sum$ 且 s 具有如下迹:$\langle+\{rcID_C\}_{K_C}ID_C,-\{rcrsID_S\}_{K_C},+\{rs\}_{K_C}\rangle$与某个 $s\in Init[C,S,rc,rs,ID_C,ID_S,K_C]$相关的协议主体是 C。

(2)集合 $Serv[C,S,rc,rs,ID_C,ID_S,K_C]$中元素 $s\in\sum$ 且 s 具有如下迹:$\langle-\{rcID_C\}_{K_C}ID_C,+\{rcrsID_S\}_{K_C},-\{rs\}_{K_C}\rangle$与某个 $s\in Serv[C,S,rc,rs,ID_C,ID_S,K_C]$相关的协议主体是 S。

定理 4 一个无线认证协议 Server-specific MAKEP 的串空间$\sum=Serv\cup Init\cup P$,其中 P 代表侵入者串集合,且 $Serv$,$Init$ 是不相交的。

2.2 保密性分析

首先证明 rs 是保密的。

定理 5 假定 C 是串空间$\sum$中的一个丛,$C,S\in T_{name}$,$K_C\notin K_P$;且 $S_{serv}\in Serv[C,S,rc,rs,ID_C,ID_S,K_C]$,令 $S=\{K_C,rs\}$且 $\kappa=K\backslash S$,则对每个节点 $n\in C$,$term(n)\notin I_\kappa[S]$。

证明:由定理 2,需要证明没有正常节点 n 为 $I_\kappa[S]$的进入点。

(反证法)若 n 为正常节点,并且为 $I_\kappa[S]$的进入点,则 $term(n)\in I_\kappa[S]$,再由文献[1]中子项定义可知 K_C,rc 至少有一项是 $term(n)$的子项,但由定义 4,发起者和响应者节点都不包含 K_C 子项,则 rc 必为 $term(n)$的子项。若 n 符号为正,$rc\subset term(n)$ 则:$s\in Serv$ 且 $n=<s,2>$,由于 rc 在$\sum$中唯一产生,$s=s_{serv}$,因此,$term(n)=\{rcrsIDS\}_{K_C}\in\kappa$,由定理 3 知 $K_C\in\kappa$。此结果与定理假设 $\kappa=K\backslash S$ 相矛盾。故定理得证。

同理可证 rc 是保密的

定理 6 假定 C 是串空间$\sum$中的一个丛,$C,S\in T_{name}$,$K_C\notin K_P$;且 $s_{init}\in Init[C,S,rc,rs,ID_C,ID_S,K_C]$,令 $S=\{K_C,rc\}$且 $\kappa=K\backslash S$,则对每个节点 $n\in C$,$term(n)\notin I_\kappa[S]$。

由上面两个定理可知 rs,rc 是保密的,与文献[3]中协议要求的保密性一致。

2.3 认证性分析

首先证明 C 可以有效认证 S;再证明 S 可以有效认证 C。

定理 6 若$\sum$是 Server-specific MAKEP 协议串空间,C 是其中的一个丛,设 $K_x\notin K_p$,$X\in T_{name}$,则形如$\{h\}_{K_{XS}}$的项不可能产生于 C 中的入侵者结点。

证明:见文献[1]

定理 7 若$\{h\}_{K_{XS}}$产生于正常串 s,则(1)若 $s\in Init$,$H=rc\ ID_C$ 或 rs。(2)若 $s\in Serv$,则 $H=rc\ rs\ ID_S$。

定理 8 若 s 为$\sum$中的一个正常串,那么:(1)若$\{rcID_C\}_{K_C}$起源于 s,则 $s\in Init$,此消息起源于节点<s,1>。(2)若$\{rs\}_{K_C}$起源于 s,则 $s\in Init$,此消息起源于节点<s,3>。(3)若$\{rcrsID_S\}_{K_C}$起源于 s,则 $s\in Serv$,此消息起源于节点<s,2>。

证明:正常串 $s\in Init\cup Serv$,由定理 6 和 7 即得证。

C 认证 S

定理 9 若 C 是串空间$\sum$中的一个丛,在 C 中 rc 是唯一起源的,且 $K_C\notin K_P$,若 $s\in Init[C,S,rc,rs,ID_C,ID_S,K_C]$且 $C\text{-}height(s)=3$,则 C 中一定有一正常串 $s_{serv}\in Serv[C,S,rc,rs,ID_C,ID_S,K_C]$,且 $C\text{-}height(s_{serv})$至少是 2。

证明:由假设知 s 在 C 中迹至少包含$\langle+\{rcID_C\}_{K_C}ID_C,-\{rcrsID_S\}_{K_C},+\{rs\}_{K_C}\rangle$,由定理 6,$\{rcrsID_S\}_{K_C}$起源于 C 中正常节点 n,再由定理 8(3)知,此正常节点 $n\in s_{serv}$,且 $s_{serv}\in Serv[C,S,rc,rs',ID_C,ID_S,K_C]$,由于节点 $n=<s_{serv},2>$,故 $C\text{-}height(s_{serv})$至少是 2。再由定理 6,$term(\langle s_{serv},3\rangle)=\{rs\}_{K_C}$ $term(\langle s_{serv},3\rangle)=\{rs\}_{K_C}$起源于 C 中正常串 s_1,又因为 rs 是由 s 唯一产生的,由定理 8,可得 $s=s_1$,故 $rs=rs'$。从而 $s_{serv}\in Serv[C,S,rc,rs,ID_C,ID_S,K_C]$。

同理可证 S 可有效认证 C。

定理 10 若 C 是串空间$\sum$中的一个丛,在 C 中 rs 是唯一起源的,且 $K_C\notin K_P$,若 $s\in Serv[C,S,rc,rs,ID_C,ID_S,K_C]$且 $C\text{-}height(s)=3$, 则 C 中一定有一正常串 $s_{init}\in Init\ [C,S,rc,rs,ID_C,ID_S,K_C]$,且 $C\text{-}height(s_{init})=3$。

综上所述,此协议经过分析是正确的,与文献[3]中用模型检验分析方法得到的结果一致。

论文首次用串空间对修改后的 Server-specific MAKEP 协议进行分析,结果表明修改后的协议是相对安全的。

参考文献:

[1] Thayer F J,Herzog J C,Guttman J D.Strand spaces:Proving security protocols correct[J].Journal of Computer Security,1999,7(2,3):191-230.

[2] Thayer F J,Herzog J C,Guttman J D.Strand spaces:Honest ideals on strand spaces[C]//Proceedings of the 1998 IEEE Computer Security Foundations Workshop.Los Alamitos:IEEE Computer Society Press,1998:66-77.

[3] 刘霞,古天龙.无线认证协议 Server-specificMAKEP 的一种改进[J].桂林电子工业学院学报,2006,4(26):255-258.