第32卷 第15期 计 算 机 工 程 2006年8月
Vol.32 № 15 Computer Engineering August 2006
·安全技术· 文章编号：1000—3428(2006)15—0137—03 文献标识码：A 中图分类号：TP393

基于Spi演算的密码协议的控制流分析

王全来[1,2]，王亚弟[1]，韩继红[1]
(1. 解放军信息工程大学电子技术学院，郑州 450004；2. 解放军防空兵指挥学院，郑州 450052)

摘 要：基于Spi演算和控制流分析，提出了一个密码协议的新分析方法。随后利用该方法对Beller-Chang-Yacobi MSR协议进行了分析，通过证明该协议已知的漏洞，说明该方法是正确的，并通过更深入的研究和分析，证明了该协议在并行会话攻击下是不安全的，基于此对该协议进一步改进，改进后的协议是安全的。

关键词：Spi演算；认证；并行会话攻击

Control Flow Analysis of Cryptography Protocols Based on Spi Calculus

WANG Quanlai[1,2], WANG Yadi[1], HAN Jihong[1]
(1. Institute of Electronic Technology, PLA University of Information Engineering, Zhengzhou 450004;
2. Air Defense Forces Command College, PLA, Zhengzhou 450052)

【Abstract】 Based on the concepts of the Spi calculus and the control flow analysis, a new technique is presented to analyze the cryptographic protocols. Then it uses the technique to analyze the Beller-Chang-Yacobi MSR protocol. The technique is correct by verifying the known flaws, and through the detailed research and analysis, it proofs the protocol is unsecured under parallel session attack. Based on this, it proves the MSR protocol is secure.

【Key words】 Spi calculus; Authentication; Parallel session attack

密码协议的作用是在一个不可信的环境中实现安全通信，目的在于达成协议本身所期望的安全目标。由于密码协议本身所处的是一个不可信的环境，它自身的安全性又会影响安全目标的达成，因此有必要对密码协议本身进行安全性分析。近年来密码协议的形式化分析已受到很多关注，例如BAN逻辑、Petri网和进程演算等方法。其中进程演算方法是将协议作为一个代数系统模型，通过分析某种状态的可达性，来完成密码协议的安全性分析，例如CSP、Pi演算、Spi演算等[1]。

通过对Spi演算进行深入分析研究，扩展了其语义，并结合控制流分析方法，得到了一个新的分析方法——基于Spi演算的密码协议的控制流分析方法。该分析方法一方面允许描述不同的攻击脚本，而且对协议进行的分析在演算的形式化操作语义上是正确的；另一方面一个简单的分析步骤可以分析不同的性质，而不需要多次重复分析。利用该分析方法对Beller-Chang-YacobiMSR协议[3]进行了分析和改进。

1 相关知识和工作

扩展的Spi演算记为Espi演算，它与Spi演算在两个方面有着本质的区别：一是用全局通信介质的概念代替通道的概念，从而使所有进程都可访问；二是输入和解密的关联测试用模式匹配来表示。

1.1 Espi演算的语法

Espi演算的语法由项和进程组成，其中项用于表示进程中的名字、变量和数据集合，其定义如下：

L,M::=	项标识
n	名字
x	变量
$\{L_1, \dots ,L_k\}_{L_0}$	对称加密
$\{\|L_1, \dots ,L_k\|\}_{L_0}$	非对称加密

其中，名字表示消息或对称密钥等。

进程的定义如下

P,Q::=	进程标识
$<L_1, \dots ,L_k>.P$	输出
$(L_1, \dots ,L_j;x_{j+1},\dots,x_k).P$	输入(带匹配)
P|Q	并行合成
$(\nu\ n)P$	生成名字
$(\nu_{\pm}\ m)P$	生成加解密密钥
0	结束进程标识
case L of $\{L_1, \dots ,L_j;x_{j+1},\dots,x_k\}_{L_0}$ in P	对称解密(带匹配)
case L of $\{\| L_1, \dots ,L_j;x_{j+1},\dots,x_k\|\}_{L_0}$ in P	非对称解密(带匹配)

其中，$(\nu\ n)P$生成一个新名字n，并限定n的范围到进程P上。$(\nu_{\pm}\ m)P$生成两个新名字m^+和m^-，为进程P中的一个密钥对。进程$<L_1,\dots,L_k>.P$输出一个k元组$<L_1,\dots,L_k>$，然后作为P继续。进程$(L_1, \dots ,L_j;x_{j+1},\dots,x_k)P$接收一个k元组$<L_1',\dots,L_k'>$，该输入与前j个项进行模式匹配并且只有在$L_i=L_i$时，匹配才能成功，成功匹配后，变量$x_{j+1},\dots,x_k$被绑定到其余的(k-j)项上。进程case L of $\{L_1, \dots ,L_j;x_{j+1},\dots,x_k\}_{L_0}$ in P为用对称密钥L_0进行解

作者简介：王全来(1970—)，男，博士生，主研方向：密码学，信息安全等；王亚弟，教授、博导；韩继红，副教授

收稿日期：2005-10-11 **E-mail：**wql_lai@126.com

密，只有L为$\{L_1^{`},\dots,L_k^{`}\}_{L_0^{`}}$形式且$L_0^{`}$与L_0相同时，才能解密，如果匹配成功，则进程作为$P[L_{j+1}^{`}/x_{j+1},\dots,L_k^{`}/x_k]$继续。类似地进程case L of $\{|L_1,\dots,L_j;x_{j+1},\dots,x_k|\}_{L_0}$ in P为用非对称密钥L_0进行解密，只有L为$\{|L_1^{`},\dots,L_k^{`}|\}_{L_0^{`}}$形式且$(L_0^{`}, L_0)$是公开密钥和秘密密钥对时，才能解密成功。

1.2 Espi 演算的操作符语义

基于Spi演算，对Espi演算重新定义了两种语义：一是简化语义P→Q，同Spi演算的简化语义；另一个是监控语义$P\rightarrow_M Q$，$M(\lambda,X^{`},\lambda^{`},X)=(\lambda\in X^{`},\lambda^{`}\in X,)$，其作用是确保加密值的密码点在解密时是可接受的(即$\lambda\in X^{`}$)，且解密的密码点对加密是正确的(即$\lambda^{`}\in X$)。当执行解密时，检查箭头上的注释M，如果条件被破坏，则终止执行，更准确地，当加密完成时，相应的解密只能出现在所标明的密码点上，反之亦然。其语义规则如表 1 所示。

表 1 语义规则

$$(\text{并行合成})\ \frac{\prod_{i=1}^{j} L_i=L_i^{`}}{<L_1,\dots,L_k>.P(L_1^{`},\dots,L_j^{`};x_{j+1},\dots,x_k).Q\rightarrow_M P|Q[L_{j+1}/x_{j+1},\dots,L_k/x_k]}$$

$$(\text{解密})\ \frac{\prod_{i=1}^{j} L_i=L_i,(\lambda,X^{`},\lambda^{`},X)}{case\{L_1,\dots,L_k\}_{L_0}^{\lambda}[destX]of\{L_1^{`},\dots,L_j^{`};x_{j+1},\dots,x_k\}_{L_0^{`}}^{\lambda^{`}}[origX]inP\rightarrow_M P[L_{j+1}/x_{j+1},\dots,L_k/x_k]}$$

$$(\text{并发})\ \frac{P\rightarrow_M P^{`}}{P|Q\rightarrow_M P^{`}|Q}\qquad (\text{限定})\ \frac{P\rightarrow_M P^{`}}{(\nu n)P\rightarrow_M(\nu n)P^{`}}\qquad (\text{一致性})\ \frac{P\equiv Q,Q\rightarrow_M Q^{`},Q^{`}\equiv P^{`}}{P\rightarrow_M P^{`}}$$

其中并行合成规则说明输出$<L_1,\dots,L_k>.P$和输入$(L_1^{`},\dots,L_j^{`};x_{j+1},\dots,x_k).P$是匹配的，如果输出和输入的前j个元素两两相同；当匹配成功时，每一个L_i绑定到相应的x_i上。解密规则说明用解密case L of $\{L_1^{`},\dots,L_j^{`};x_{j+1},\dots,x_k\}_{L_0^{`}}^{\lambda^{`}}$ [origX] in P与加密$\{L_1,\dots,L_k\}_{L_0}^{\lambda}$ [destX]的结果匹配，如果匹配成功，则对前j个元素，L_i必须等于$L_i^{`}$且$L_0=L_0^{`}$。其余规则同Spi演算。

1.3 控制流分析

控制流分析是O.Shivers在文献[2]中提出的，用于面向对象语言及具有并发性语言的分析。在Espi演算中，对进程P分析的结果用对(ρ,κ)来表示，并基于流逻辑方法，采用流逻辑的判定形式$(\rho,\kappa)\models P:\psi$作为进程P的分析，其中ρ是抽象环境，它将变量和绑定到变量的值关联起来，即ρ必须包括进程在运行时变量的所有可能值的集合。κ是抽象网络环境，它将名字和在网络中传送的值关联起来，即κ必须包括所有可以在网络上流动的消息序列。ψ是错误分量，它将密码点和值可以出现的位置关联起来，即它是形式为密码点对$(\lambda,\lambda^{`})$的错误消息集合，$(\lambda_A,\lambda_B)\in\psi$说明在密码点$\lambda_A$加密的值在密码点$\lambda_B$错误地解密，即协议是不安全的；相反，如果ψ为空，则协议是正确的。

基于 Espi 演算和控制流分析，设计了一个密码协议的自动验证系统，利用该系统通过对 Needham-Schroeder 协议等的自动分析，可以找到协议中已知的漏洞，说明该系统是有效的。

1.4 MSR 协议

MSR 协议是由 Beller-Chang-Yacobi 提出的，它是基于对称和非对称密码算法相结合的一个密码协议，用于无线网络中移动用户和基站之间的认证。对 MSR 协议，通过分析攻击者的知识集合来确定协议的保密性和消息真实性，具体的对协议的保密性，通过检查任一给定值是否出现在攻击者的知识集合中来判定。消息真实性是通过消息能否在适当的位置结束来决定。为了描述协议的消息真实性，用表示加密和解密所发生的位置的密码点λ和指明已加密消息的源和目标位置的声明来标识它的原文。如加密进程$\{L_1,\dots,L_k\}_{L_0}^{\lambda}$ [destX]或者$\{|L_1,\dots,L_k|\}_{L_0}^{\lambda}$ [destX]，相应的解密进程为 case L of $\{L_1,\dots,L_j;x_{j+1},\dots,x_k\}_{L_0}^{\lambda}$ [origX] in P 或者 case L of $\{|L_1,\dots,L_j;x_{j+1},\dots,x_k|\}$ origX] in P，其中 X 为密码点集合。

2 MSR 协议分析

协议的非形式化描述如图 1 所示。

消息 1 B→A: B，K_B^+	消息 1 B→A: B, $\{|B|\}_{K_U^-}$, K_B^+
消息 2 A→B: $\{|K|\}_{K_B^+}$	消息 2 A→B: $\{|K|\}_{K_B^+}$
消息 3 A→B: $\{A,\{|A|\}_{K_U^-}\}_K$	消息 3 A→B: $\{A,\{|A|\}_{K_U^-}\}_K$

图 1 MSR 协议(左)和 IMSR 协议(右)

MSR 协议依赖于离线的证书机构 U，U 的作用是发布移动用户和基站 ID 的已签名的证书。当移动用户 A 到达基站 B 时，首先发送一个消息来告知基站，进行认证，基站用消息 1 响应并发送它的公开密钥，移动用户生成一个新的会话密钥 K 并和自己的证书一起发送给基站(消息 2 和 3)。MSR 协议和 IMSR 协议的区别仅在于消息 1 中的证书，该证书用于移动用户对基站的认证。

2.1 IMSR 协议的形式化描述

IMSR 协议的形式化描述如下列程序所示。其中A_i(i=1…m)表示移动用户，B_j(j=1…n)表示基站，U表示证书机构。(K^+_j, K^-_j)为B_j的密钥对；(K^+_U, K^-_U)为证书机构的签名密钥对。我们在消息的形式化描述中增加了源和目标地址，其形式为<source,destination,message1,…,messagek>，这确保了所有地址可以在网络中明文发送，使得协议的安全性不依赖于地址的保密性。

```
1   (M, K_U)< K_B^+>|
2   ∏_{i=1}^{m} ∏_{j=1}^{n}! (B_j, A_i, B_j; xC_ij, xK_ij)
3         case xC_ij of {|B_j;|}_{K_U^+}^{a 1 i}  [origb1_j] in
4         (MK_ij)< A_i, B_j,  {|K_ij|}_{x K_ij}^{a 2 i}  [destb2_j]>
5              < A_i, B_j,  {A_i, {|A_i|}_{K_U^-}^{a 3 i}}_{K_ij}^{a 4 i}  [destb3_j]>.0
6   |(ν_{±j=1}^{n} K_j)
7   ∏_{i=1}^{m} ∏_{j=1}^{n}! <B_j, A_i, B_j;  {|B_j|}_{K_U^-}^{b 1 j}, K_j^+>
8         (A_i, B_j; y1_ij)
9         case  y1_ij of  {|; y2_ij|}_{K_j^-}^{b 2 j}  in
10        (A_i, B_j; y3_ij)
11        case  y3_ij of  {A_i; y4_ij}_{y 2 ij}^{b 3 j}  [origa4_i]  in
12        case  y4_ij of  {|A_i;|}_{K_U^+}^{b 4 j}  [origa3_i]  in 0
```

程序中第 1 行说明证书机构将密钥分配给各个角色，2～5 行描述了移动用户进程，6～12 行描述了基站进程。移动用户和基站的进程中的加密和解密的密码点分别用Ki 和Kj 来标识，进程中还包括已加密消息的所期望的目标和源地址，如第 4 行，移动用户 Ai 想和基站 Bj 通话，注释[dest b2j]表明已加密消息希望在基站 Bj 的第 2 个密码点处被解密，且只能在此处；第 5 行，移动用户 Ai 加密的第 2 个消息希望到达基站 Bj 的第 4 个密码点，且只能在此处，其余的依此类推。在解密点加注释，如第 3 行，[orig b1j]指明在此处确认的证

书被认为是来自于 Bj，第 9 行，在基站进行的第 1 次解密处，没有检测消息的源地址，因为基站不希望只有特殊的用户可以使用它的公开密钥。当基站在协议运行的过程中得到更多消息时，它期望的是只有来自于 Ai 的消息可以被解密，如第 11、12 行所示。

2.2 分析结果

利用密码协议自动验证系统，得到 MSR 协议的分析结果，如表 2 所示。

表 2 分析结果

i=1…m，j=1…n	错误分量ψ	攻击者的知识集合
MSR	$(a2_i, \lambda_a)$, $(a4_i, \lambda_a)$, $(\lambda_a, b3_j)$ $(a2_i, b2_j)$, $(a4_i, b3_j)$	n_a , K^+_a , K^-_a ,A_i , B_j K_{ij} , K^+_j , K^+_U
IMSR	$(a2_i, \lambda_a)$, $(a4_i, \lambda_a)$, $(\lambda_a, b3_j)$ $(a2_i, b2_j)$, $(a4_i, b3_j)$	n_a , K^+_a , K^-_a ,A_i , B_j K_{ij} , K^+_j , K^+_U

由表 2 可知，该协议有漏洞，因为错误分量非空且攻击者可以得到所有的会话密钥。检查攻击者的知识集合，可以看到这两个协议均不能提供会话密钥的保密性，如文献[4]所述。文献[4]还描述了一种密钥哄骗攻击，如图 2 左边所示，在协议运行结尾处，A_1认为它在和B_1通话，实际上是和攻击者M通话。

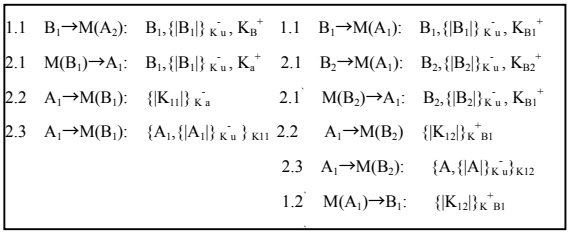

图 2 密钥哄骗攻击(左)和新的并行会话攻击(右)

比较表 2 中错误分量集合和图 2 左边的攻击序列，在攻击序列的最后两行，由A_1加密的东西被攻击者M解密，如表 2 的$(a2_i, \lambda_a)$, $(a4_i, \lambda_a)$。消息 2.2 说明M得到K_{11}，使得M有能力生成形式为第 3 个消息的消息，这就是认证的一个漏洞，文献[4]已给出。$(\lambda_a, b3_j)$说明攻击者加密的东西，在B_j处被错误地解密。元素$(a2_i, b2_j)$和$(a4_i, b3_j)$所表示的含义在文献[4]中没有提及，事实上，它们表示了一个并行会话攻击(图 3 右边所示)，在协议运行结尾处，A_1认为它在和B_2通信，实际上却在和B_1通信。关于MSR协议的这种攻击在相关文献中没有提及。

2.3 安全的 MSR 协议

通过上述分析可知，IMSR 协议不安全的原因在于消息 1 中证书的作用非常小。基于此，对 IMSR 协议进一步改进如下：

消息 1 B→A: $B, K_B^+, P_B^+, \{|H(B, K_B^+, P_B^+)|\}_{K^-u}$

消息 2 A→B: $\{|K_{AB}|\}_{K_B^+}$

消息 3 A→B: $\{A, P_A^+, \{|H(A, P_A^+)|\}_{K^-u}\}_{KAB}$

其中，P_A^+和P_B^+是移动用户和基站的协议密钥的公开密钥。

首先，基站B产生$H(B, K_B^+, P_B^+)$并用K^-_U加密生成它的证书，连同其身份标识符B、K_B^+与 P_B^+一起明传给A。其次，A收到B, K_B^+ , P_B^+ , $\{|H(B, K_B^+, P_B^+)|\}_{K^-u}$ 后，产生会话密钥K_{AB}，并用K_B^+加密传给B。最后，A产生$H(A, P_A^+)$并用密钥K^-_U加密生成自己的证书，连同其身份标识符A、P_A^+用K_{AB}进行加密并发给B。

利用同样的过程对上述协议进行分析，可知攻击者不能得到会话密钥K_{AB}且没有发现其它新的攻击类型，可以证明该协议是安全的。

3 结束语

本文将控制流分析引入到 Spi 演算中，得到一个密码协议的新的形式化分析方法，利用该分析方法对 MSR 协议和 IMSR 协议进行了分析，不仅证实了 MSR 协议已知的所有漏洞，还证明了 IMSR 协议在并行会话攻击下是不安全的，并对 IMSR 协议作了改进。这些研究工作进一步证明了新的分析方法的可行性和有效性。另外，尽管本文所做的分析是基于对称和非对称密码体制，通过深入分析研究，该分析方法还可以应用到更为复杂的密码协议安全性分析中。

参考文献

1 Abadi M, Gordon A D. A Calculus for Cryptography Protocols: the Spi Calculus[J]. Information and Computation, 1999, 148(1): 1-70.

2 Shivers O. Control Flow Analysis in Scheme[C]. Proceedings of the ACM SIGPLAN'88 Conference on Programming Language Design and Implementation, 1988-06.

3 Beller M J, Chang L F, Yacobi Y. Privacy and Authentication on a Portable Communication System[J]. IEEE Journal of Selected Areas in Communication, 1993, 11(6): 821-829.

4 Carlsen U. Optimal Privacy and Authentication on a Portable Communication System[J]. Operating Systems Review, 1994, 28(3): 16-23.

（上接第 122 页）

SWLDRM 模型根据节点作用的不同分为 2 层，将节点聚集为簇，使用远链接与近链接分别提供簇间节点和簇内节点的连接。通过仿真实验表明：SWLDRM 模型较好地符合 P2P 的小世界特性，具有较高的聚类系数和较小的平均跳数，从而比 Chord 模型具有更好的查找性能。

参考文献

1 Napster Homepage[Z]. http://www.napster.com.

2 Stephanos, Stheotokis R, Spinellis D. A Survey of Peer-to-Peer Content Distribution Technologies[J]. Proceedings of ACM Computing Surveys, 2004, 36(4): 335-371.

3 Newman M E J, Jensen I, Ziff R M. Percolation and Epidemics in A Two-dimensional Small World[J]. Physical Review E, 2002, 65(2).

4 Aber r K. An Overview on Peer-to-Peer Information Systems[EB/OL]. http://lsirpeople.epfl.ch/hauswirth/papers/WDAS2002.pdf, 2002.

5 Stoica I, Morris R, Karger D, et al. Chord: A Scalable Peer to Peer Lookup Service for Internet Applications[C]. Proceedings of ACM SIGCOMM, 2001.

6 董 芳. 对等网络 Chord 分布式查找服务的研究[J]. 计算机应用, 2003, 23(11): 25-28.

7 Zhang H, Goel A, Govindan R. Using the Small-world Model to Improve Freenet Performance[C]. Proceedings of the 21st IEEE Infocom Conference, New York, 2002: 40-49.

8 乐光学. 基于 Region 多层结构 P2P 计算网络模型[J]. 软件学报, 2005, 16(6): 1140-1150.