基于 Petri 网的安全协议形式化分析

刘道斌,郭 莉,白 硕
(中国科学院计算技术研究所软件研究室,北京 100080)

摘 要: 本文提出了一种基于 Petri 网的安全协议形式化描述和安全性验证的方法. 该方法的特点是,利用逆向状态分析判定协议运行过程中可能出现的不安全状态,利用 Petri 网的状态可达性分析判断这些不安全状态是否可达. 通过实例,我们证明了这种方法的有效性.

关键词: 安全协议; Petri 网; 可达性分析
中图分类号: TP393.08 **文献标识码**: A **文章编号**: 0372-2112 (2004) 11-1926-04

Formal Analysis of Security Protocols Using Petri Nets

LIU Dao-bin, Guo Li, BAI Shuo
(Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080, China)

Abstract: We propose an approach for the formal modeling and analysis of security properties of cryptographic protocols. Our methodology is based on the idea of backward state analysis and the reachability analysis for Petri nets. By performing the state analysis, we can find out potential insecure states during the run of protocols and determine if these insecure states are reachable by using the state reachability analysis. An example shows that this approach is efficacious.

Key words: security protocol; Petri net; reachability analysis

1 引言

安全协议是一种通信协议,它的主要目的是利用密码技术实现网络通信中的密钥分发和身份认证. 安全协议是任何安全系统的基础,是实现计算机网络安全的关键. 然而,大量事实表明有许多安全协议经过安全专家认真、仔细地分析、设计和实现后仍然存在漏洞,有些甚至在使用多年后才被发现有漏洞. 因此,协议的安全性验证是非常重要的. 近年来,人们主要采用形式化方法验证协议的安全性,在该领域涌现了大量有效的形式化分析方法,其中比较有影响的主要有:BAN 逻辑方法[1]、串空间方法[2]、Petri 网方法[3]、进程代数方法[4]、计算与信息理论方法[5]等.

在本文中,我们提出了一种新的基于 Petri 网[6]状态转换的分析方法. 在传统 Petri 网的状态分析中经常会出现状态空间爆炸问题,在这里由于我们采用了逆向状态可达性分析方法,大大降低了计算的复杂性,使这种方法变得更为高效、实用. 另外,由于着色 Petri 网具有大量的自动化分析工具,我们采用着色 Petri 网作为协议的形式化描述和分析工具,这将使我们的方法易于实现自动化.

2 安全协议分析

这里我们提出一种新的基于 Petri 网的安全协议验证方法,该方法主要采用逆向状态分析以及 Petri 网的可达性分析思想.

我们提出的方法主要分两个阶段进行,第一阶段是不安全状态分析,第二阶段是可达性分析. 不安全状态分析的思想首先在文[7]中提出.

第一阶段:如果试图通过加入入侵模型(如图 1 所示)来分析一个安全协议,我们必须考虑大量的可能情形,这使得分析任务加重. 例如,假设在入侵者模型中有 N 个未加密的变量输入,那么随着 N 的增加,分析步骤将呈 N 指数性增长.

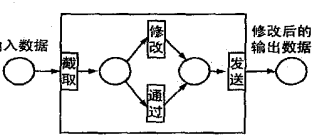

图 1 入侵者攻击模型

为此,我们的想法是找出所有那些不影响合法用户数据接受而又被入侵者修改的输出数据,因为在我们的分析中只需要这些数据. 图 1 模型中的输入数据包括入侵者能修改的未加密数据(假设入侵者只能修改未加密数据)以及合法用户将检测的数据,修改后的输出数据是指既能被攻击者修改同时还能被合法用户接受的数据. 通过这一阶段的分析,我们将确定协议中可能出现的不安全状态并给出相应的攻击模型.

第二阶段:建立状态方程

$$M_n = M_0 + C^T \times \sigma$$

收稿日期:2002-09-10;修回日期:2004-05-28
基金项目:国家"八六三"高技术研究发展计划基金(No. 2001AA142110)

其中 M_0 表示初始状态, M_n 表示不安全的终止状态, C 表示关联矩阵, σ 是变迁实施计数向量,求解方程得向量 σ 的值. 如果方程有解,表明不安全终止状态 M_n 由初始状态 M_0 可达,向量 σ 的值表示由 M_0 到 M_n 的变迁实施序列.

概括起来,我们的方法分以下几步进行:

步 1:给出所要分析协议的着色网模型,确定入侵者可能修改的变量.

步 2:应用不安全状态分析法确定图 1 模型中的修改后输出数据集.

步 3:如果修改后的输出数据集是空集,验证结束. 否则,检查该数据集是否表示协议潜在的漏洞,如果是,在协议模型中加入入侵者攻击模型.

步 4:给出协议攻击模型的初始状态、不安全的终止状态以及关联矩阵.

步 5:建立状态方程,判断不安全终止状态是否由初始状态可达.

3　应用举例

Aziz 和 Diffie 在文[8]中提出了一种用于无线局域网中密钥分发和身份认证的无线通信安全协议(记为:协议 P),这里我们用第三节中提出的方法来验证协议 P,证明它是不安全的,并发现其中存在的安全漏洞.

3.1　协议描述

为便于描述,我们引进如下记号:

A 表示移动终端, B 表示基站, I 表示入侵者, K_x、K_x^{-1} 分别表示主体 x 的公钥、私钥, $K_x()$、$K_x^{-1}()$ 分别表示用 K_x、K_x^{-1} 加密和解密数据, C_x 表示主体 x 的公钥证书.

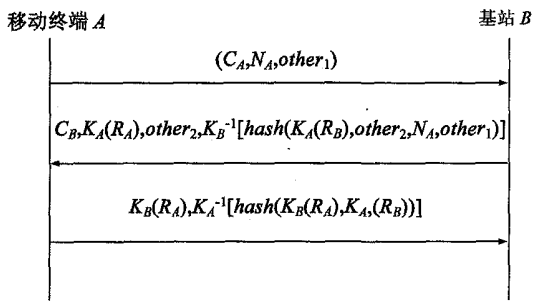

图 2　协议 P 的执行流程

图 2 描述了协议 P 的执行流程,协议 P 的执行分以下几步:

(1) 为建立会话连接,首先移动终端 A 向基站 B 发送会话请求,请求信息中包含 A 的证书 C_A、随机选取的 128 比特数 N_A 以及供 B 选择的密钥算法列表 $other_1$

(2) 基站 B 验证 A 的证书 C_A,若验证通过, B 从 C_A 中抽取 A 的公钥 K_A. 再选取随机数 R_B,用 A 的公钥加密得 $K_A(R_B)$,计算 $[\text{hash}(K_A(R_B), other_2, N_A, other_1)]$(其中 $other_2$ 是 B 选择的密钥算法)并用 B 的私钥加密,然后向移动终端 A 发送响应消息 $C_B, K_A(R_B), other_2, K_B^{-1}[\text{hash}(K_A(R_B), other_2, N_A, other_1)]$

(3) A 验证 B 的证书 C_B,若验证通过, A 从 C_B 中抽取 B 的公钥 K_B,再用它验证 B 的签名. 认证完成后, A 选取随机数 R_A,用 B 的公钥加密得 $K_B(R_A)$,然后向 B 发送消息 $K_B(R_A)$, $K_A^{-1}[\text{hash}(K_B(R_A), K_A(R_B))]$

(4) B 用 A 的公钥解密收到的消息,验证 A 的签名并获取 R_A,最后得到一致的会话密钥 $R_A \oplus R_B$

3.2　协议分析

我们利用第二节中给出的方法来分析协议 P 的安全性,分析步骤如下:

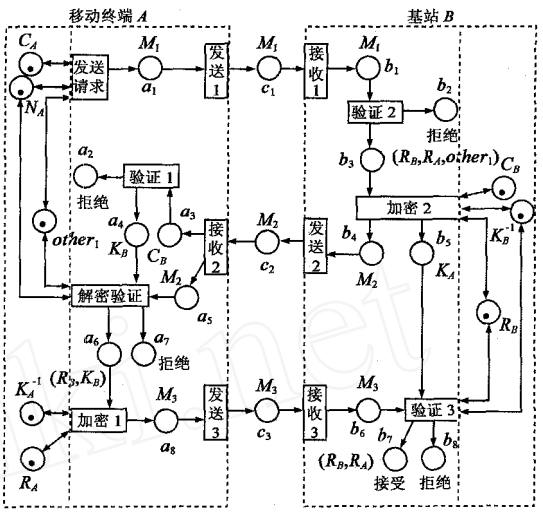

图 3　协议 P 的着色 Petri 网模型

步 1:建立协议 P 的着色网模型,如图 3 所示,其中

$M_1 = \{C_A, N_A, other_1\}$,

$M_2 = \{C_B, K_A(R_B), other_2, K_B^{-1}[\text{hash}(K_A(R_B), other_2, N_A, other_1)]\}$,

$M_2' = \{K_A(R_B), other_2, K_B^{-1}[\text{hash}(K_A(R_B), other_2, N_A, other_1)]\}$,

$M_3 = \{K_B(R_A), K_A^{-1}[\text{hash}(K_B(R_A), K_A(R_B))]\}$.

在图 3 中,变迁表示的动作由变迁方框中的文字说明,比如,加密 1 表示该变迁执行加密信息的动作,数字 1 是该变迁编号,以便同其它加密变迁区别开.

步 2:不安全状态分析. 我们发现基站接受消息 M_1 中的所有信息,只要其中证书属于合法用户;另外,移动终端 A 也接受任何有效的证书,只要证书的公钥能验证消息 M_2 中签名. 这就意味着如果证书没有说明它是属于移动终端的还是基站的,那么一个合法的移动用户就可以冒充成基站把自己的证书(替代基站的证书)发送出去.

步 3:在图 3 中加入入侵者攻击模型(这里假设入侵者是合法用户,拥有有效的证书),如图 4 所示,其中

$M_1 = \{C_A, N_A, other_1\}$, $\widetilde{M}_1 = \{C_I, N_A, other_1\}$

$M_2 = \{C_B, K_I(R_B), other_2, K_B^{-1}[\text{hash}(K_I(R_B), other_2, N_A, other_1)]\}$,

$\widetilde{M}_2 = \{C_I, K_A(R_B), other_2, K_I^{-1}[\text{hash}(K_A(R_B), other_2, N_A, other_1)]\}$,

$M_3 = \{K_I(R_A), K_A^{-1}[\text{hash}(K_I(R_A), K_A(R_B))]\}$,

$\widetilde{M}_3 = \{K_B(R_A), K_I^{-1}[\text{hash}(K_B(R_A), K_I(R_B))]\}$.

步 4:在协议分析过程中,定义不安全状态"入侵者成功获取会话密钥,但移动终端与基站之间仍能正常通信".

步 5: 对图 4 模型进行可达性分析.

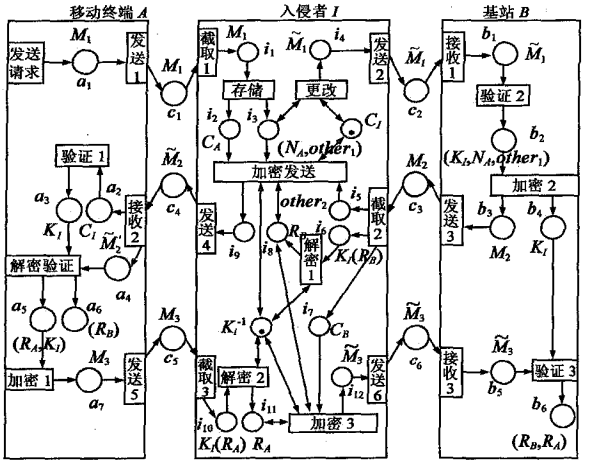

图 4 协议 P 攻击的着色 Petri 网模型

首先给出图 4 中着色网的关联矩阵:

$$C=\begin{bmatrix} C_1 & 0 & 0 \\ 0 & C_2 & 0 \\ 0 & 0 & C_3 \\ C_4 & C_5 & C_6 \end{bmatrix}$$

其中子矩阵 C_1、C_2、C_3、C_4、C_5、C_6 分别由表 1、表 2、表 3、表 4、表 5、表 6 给出. 表中给出的都是符号常量,是图 4 着色网中标记的颜色值,空格处的值为 0

表 1 图 4 模型关联矩阵的子矩阵 C_1

	发送请求	发送 1	接收 2	验证 1	解密验证	加密 1	发送 5
a_1	M_1	$-M_1$					
a_2			C_I	$-C_I$			
a_3				K_I	$-K_I$		
a_4			$\widetilde{M}'_2$		$-\widetilde{M}'_2$		
a_5					(R_A, K_I)	$-(R_A, K_I)$	
a_6					R_B		
a_7						M_3	$-M_3$

表 2 图 4 模型关联矩阵的子矩阵 C_2

	截取 1	存储	更改	发送 2	截取 2	解密 1	加密发送	发送 4	截取 3	解密 2	加密 3	发送 6
i_1	M_1	$-M_1$										
i_2		C_A					$-CA$					
i_3		$(N_A, other_1)$					$-(N_A, other_1)$					
i_4			$\widetilde{M}_1$	$-\widetilde{M}_1$								
i_5					$other_2$		$-other_2$					
i_6					$K_I(R_B)$	$-K_I(R_B)$						
i_7					C_B						$-C_B$	
i_8						R_B						
i_9							$\widetilde{M}_2$	$-\widetilde{M}_2$				
i_{10}									$K_I(R_A)$	$-K_I(R_A)$		
i_{11}										R_A		
i_{12}											$\widetilde{M}_3$	$-\widetilde{M}_3$

表 3 图 4 模型关联矩阵的子矩阵 C_3

	接收 1	验证 2	加密 2	发送 3	接收 3	验证 3
b_1	$\widetilde{M}_1$	$-M_1$				
b_2		$(K_I, N_A, other_1)$	$-(K_I, N_A, other_1)$			
b_3			M_2	$-M_2$		
b_4			K_I			$-K_I$
b_5					$\widetilde{M}_3$	$-\widetilde{M}_3$
b_6						(R_B, R_A)

表 4 图 4 模型关联矩阵的子矩阵 C_4

	发送请求	发送 1	接收 2	验证 1	解密验证	加密 1	发送 5
c_1		M_1					
c_2							
c_3							
c_4			$-\widetilde{M}_2$				
c_5							M_3
c_6							

表 5 图 4 模型关联矩阵的子矩阵 C_5

	截取 1	存储	更改	发送 2	截取 2	解密 1	加密发送	发送 4	截取 3	解密 2	加密 3	发送 6
c_1	$-M_1$											
c_2				$\widetilde{M}_1$								
c_3					$-M_2$							
c_4								$\widetilde{M}_2$				
c_5									$-M_3$			
c_6												$\widetilde{M}_3$

表 6 图 4 模型关联矩阵的子矩阵 C_6

	接收 1	验证 2	加密 2	发送 3	接收 3	验证 3
c_1						
c_2	$-\widetilde{M}_1$					
c_3				M_2		
c_4						
c_5						
c_6					$-\widetilde{M}_3$	

初始状态: $M_0^T = [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]$

不安全的终止状态:

$M_n^T = [0,0,0,0,0,0,R_B,0,0,0,0,0,0,0,0,R_B,0,0,R_A,0,0,0,0,0,(R_B,R_A),0,0,0,0,0,0]$,表示入侵者 I、移动终端 A 和基站 B 都获取会话密钥 (R_A,R_B).

于是可得如下状态方程:

$$M_n = M_0 + C \times \sigma \quad (1)$$

利用线性代数中方程组解的判别方法可判定状态方程(1)有解,说明不安全终止状态 M_n 由初始状态 M_0 可达. 至此,我们就证明了协议 P 是不安全的,存在安全漏洞.

下面对图 4 中描述的入侵者攻击行为进行解释:

(1) 入侵者 I 截取并复制存储信息 M_1,用自己的证书 C_I 替换 A 的证书 C_A,伪造出信息,发送给基站 B

(2) 由于入侵者 I 也是合法用户,所以 B 验证证书有效,从中抽取公钥 K_I,发送 M_2 给 A

(3) 入侵者 I 截取 M_2 并复制存储 B 的证书 C_B,解密 $K_I(R_B)$ 得 R_B,伪造发给 A

(4) A 收到,验证证书有效后,从中抽取公钥 K_I,验证签名有效,然后发送 M_3

(5) 入侵者 I 截取 M_3,解密 $K_I(R_A)$ 得 R_A,这就意味着 I 已获取完整的会话密钥 $(R_A \oplus R_B)$. 由于 I 有 B 的证书,所以 I 用 K_B 加密 R_A,又冒充 A 把 $\tilde{M}_3$ 发给 B

(6) B 知道的公钥是 K_I 而不是 K_A,所以 B 用 K_I 解密 $K_I^{-1}[hash(K_B(R_A), K_I(R_B))]$,验证签名有效,并获取会话密钥.

从以上分析可以看出,入侵者之所以攻击成功,主要是因为它用自己的证书 C_I 替换 A、B 的证书 C_A、C_B 而不被 B、A 所发现. 因此,为防止上述攻击,证书中应包含说明它的所有者是移动终端还是基站的信息,并且至少移动终端 A 应验证这一点.

4 结论

安全协议的形式化分析是信息安全的一个重要研究领域,也是目前的一个研究热点. 本文提出了一种基于 Petri 网的安全协议验证方法,这种方法采用逆向状态可达性分析技术,有效地克服了传统 Petri 网分析过程中经常出现的状态空间爆炸问题. 通过实例分析,我们验证了这种方法的有效性.

参考文献:

[1] M Burrows, M Abadi, R M Needham. A logic of authentication[J]. Proc R Soc Lond, 1989: 233 - 271.

[2] J Thayer, J Herzog, J Guttman. Strand spaces: Why is a security protocol correct[A]? In 1998 IEEE Symposium on Security and Privacy [C]. USA: IEEE Computer Society Press, 1998.

[3] B B Nieh, S E Tavares. Modelling and analyzing cryptographic protocols using Petri nets[A]. Advances in Cryptology-AUSCRYPT '92[C]. volume 718 of LNCS, Springer-Verlag, 1992. 275 - 295.

[4] M Abadi, A Gordon. A calculus for cryptographic protocols: The Spi calculus[A]. Proceedings of the Fourth ACM Conference on Computer and Communications Security[C]. USA: ACM Press, 1997.

[5] R Canetti. Security and composition of multiparty cryptographic protocols[J]. J Cryptology, 2000, 13(4): 143 - 202.

[6] T Murata. Petri nets: Properties, analysis and applications[J]. Proceedings of the IEEE, 1989, 77(4): 541 - 580.

[7] C M Morton. A Modular Approach to Evaluating Cryptographic Protocols using Petri Nets[D]. Kingston, Ontario, Canada: Queen's University, 1993.

[8] A Aziz, W Diffie. A secure communications protocol to prevent unauthorized access: Privacy and authentication for wireless local area networks[J]. IEEE Personal Communications, 1994: 25 - 31.

作者简介:

刘道斌　男,1968 年生于江西,主要研究方向为计算机网络与信息安全、Petri 网、计算机系统性能分析.

郭　莉　女,1969 年生于湖南,主要研究方向为计算机网络与信息安全.

白　硕　男,1956 年生于辽宁,研究员,主要研究方向为网络安全、计算语言学.