串空间代数缺陷到实际攻击的转换

沈海峰[1] 黄河燕[1,2] 陈肇雄[1,2]

(中国科学技术大学计算机科学系 合肥230026)[1] (中科院计算机语言信息工程研究中心 北京100083)[2]

摘 要 根据串空间证明协议安全性的代数结论,可以判断协议是否存在缺陷,但没有给出一个精确的答案:究竟攻击是如何进行的?本文提出四条启发式规则以完成代数缺陷到实际攻击的转换。并结合 Needham-Schroeder 公钥协议、Otway-Rees 对称密钥协议进行了攻击转换分析。实践表明这四条规则在把串空间的代数缺陷转换为实际攻击时非常有效。

关键词 密码协议,串空间,代数缺陷,启发式规则

Converting the Strand Spaces' Algebraic Flaws to Actual Attacks

SHENG Hai-Feng[1] HUANG He-Yan[1,2] CHEN Zhao-Xiong[1,2]

(Dept. of Computer Science ,USTC,Hefei 230026)[1]

(Engineering Research Center of Computer Language Information,CAS, Beijing 100083)[2]

Abstract We can conclude whether a protocol is defective according to the algebraic result after proving the protocol's security. But the algebraic result doesn't tell us explicitly how the actual attack takes place. In this paper, we propose four heuristic rules for converting the algebraic result to actual attack, and use them in Needham-Schroeder public protocol as well as Otway-Rees symmetrical protocol. Practical evidences indicate that these four rules are very efficient in converting Strand Spaces' algebraic flaws to actual attacks.

Keywords Cryptographic protocols,Strand spaces, Algebraic flaw,Heuristic rule

1 引言

串空间(strand spaces)是基于代数理论的密码协议分析模型[1,2,4~6]。它分析协议的基本步骤是:

a. 定义含入侵者的协议代数模型。

b. 给出协议的各种安全目标命题,包括秘密性,认证性和不可否认性。

c. 证明这些命题是否正确,如果正确,则串空间没有发现协议存在安全漏洞,如果错误,则协议存在安全漏洞。

由上面的步骤可以看出,串空间是在协议的代数描述基础上进行分析,其分析结论也是代数形式。当协议被分析出存在代数缺陷时,实际攻击究竟是如何进行的呢?这不是一个显而易见的问题。比如,用串空间理论我们证明了 Needham-Schroeder 公钥协议的一个结论:$S\in Resp[A,B,N_a,N_b]\Rightarrow s'\in Init[A,B',N_a,N_b]$。在这个结论中,响应者和发起者有不同的响应者身份(一个是 B,另一个是 B'),因此,发起者和响应者不能达到单射一致性认证目的[10]。可是这个结论并没有明确告诉我们实际攻击的过程。也就是说,代数缺陷和实际攻击之间还有一道鸿沟。本文的目的是希望提供一些启发式方法以引导我们构建实际的攻击过程。

2 串空间简介

一个串(Strand)是协议参与者的事件序列,即发送、接受消息的序列。一个串空间是串的集合,其中既包括合法参与者的串,又包括入侵者串。设 A 是协议执行中所有可能消息的集合,A 中元素称为项($term$),$t_1\sqsubset t$ 表示 t_1 是 t 的子项。

定义2.1 $\langle\sigma,a\rangle$是有符号项,a 是+或−号,$a\in A$,一个有符号项记为$+t$ 或$-t$,$(\pm A)^*$是全体有符号项的有限序列集合。$(\pm A)^*$中一个典型元素是$\langle\langle\sigma_1,a_1\rangle,\cdots,\langle\sigma_n,a_n\rangle\rangle$。

定义2.2 一个串空间是集合 Σ,并具有一个轨迹(trace)映射 $tr:\Sigma\to(\pm A)^*$。

定义2.3 对一个固定的串空间 Σ,有:

1)结点是$\langle s,i\rangle$,$s\in\Sigma$,i 是整数$1\leqslant i\leqslant length(tr(s))$,结点集合为 N。我们说$\langle s,i\rangle$属于 s,每一个结点都属于唯一的一个串。

2)如果 $n=\langle s,i\rangle\in N$,那么 $index(n)=i$ 且 $strand(n)=i$,定义 s 轨迹的第 i 个有符号项 $term(n)$是$(tr(s))_i$;无符号项 $un_term(n)$是$((tr(s))_i)_2$,即 $term(n)$的无符号部分。

3)如果 $n_1,n_2\in N$,那么 $n_1\rightarrow n_2$意味着 $term(n_1)=+a$,$term(n_2)=-a$,即 n_1发送消息,n_2接受消息。

4)如果 $n_1,n_2\in N$,那么 $n_1\Rightarrow n_2$意味着 n_1、n_2发生在同一个串上,n_1是 n_2的直接前继,有 $index(n_1)=index(n_2)-1$。

5)一个无符号项 t 发生在 $n\in N$,当且仅当 $t\sqsubset term(n)$。

6)一个无符号项 t 起源在 $n\in N$,当且仅当 $term(n)$是正号,$t\sqsubset term(n)$,而且对 n 的任何前继 n'有 $t\not\sqsubset term(n')$。

7)一个无符号项 t 唯一起源在 $n\in N$,当且仅当 t 起源在唯一的结点 $n\in N$。

8)N 加上两种边集合 $n_1\rightarrow n_2$和 $n_1\Rightarrow n_2$就组成一个有向图。

9)$n_1\Rightarrow^+ n_2$表示在同一个串上 n_1经过一个或多个$\Rightarrow$边到达 n_2。

串空间理论还定义了入侵者的行为串。设 K_P 是入侵者的密钥集合,其中包括:所有的公钥,与入侵者共享的对称密钥 K_{PX},丢失或被破解的密钥。

沈海峰 博士生,研究方向密码学与网络安全。黄河燕 教授,博士生导师,主要从事人工智能、形式化方法和计算语言学的研究工作。陈肇雄 教授,博士生导师,主要从事人工智能、网络信息处理的研究工作。

定义2.4 一个入侵者的串轨迹有下列几种：M 文本消息：$\langle +t\rangle, t\in T$；$F$ 接受：$\langle -g\rangle, g\in A$；$T$ 分发：$\langle -g,+g,+g\rangle, g\in A$；$C$ 连接：$\langle -g,-h,+gh\rangle, g,h\in A$；$S$ 分离：$\langle -g,-h,+gh\rangle$；K 密钥：$\langle +K\rangle, K\in K_P$；$E$ 加密：$\langle -K,-h,+\{h\}_K\rangle$；$D$ 解密：$\langle -K^{-1},-\{h\}_k,+h\rangle$。

公理2.5(自由加密假设) $\{m\}_k=\{m'\}_{k'}\Leftrightarrow m=m'\wedge K=K'$。

公理2.6对 $m_0,m'_0,m_1,m'_1\in A,K,K'\in K$：1) $m_0m_1=m'_0m'_1\Rightarrow m_0=m'_0\wedge m_1=m'_1$；2) $m_0m_1\neq\{m'_0\}_k$；3) $m_0m_1\notin K\cup T$；4) $\{m_0\}_k\notin K\cup T$。

定义2.7 设 C 是边的集合，N_C 是依附于 C 的全体结点，称 C 是一个束(bundle)，如果：

1) C 是有限的；2) 如果 $n_1\in N_C$，且 $tem(n_1)$ 是负号，那么有唯一的结点 n_2 满足 $n_2\rightarrow n_1\in C$；3) 如果 $n_1\in N_C$，且 $n_2\Rightarrow n_1$，那么 $n_2\Rightarrow n_1\in C$；4) C 是无环的。

定义2.8 如果 C 是一个束，$s\in\Sigma$，则 s 的束高 $height_C(s)$ 是最大的 $i\leqslant length(tr(s))$，满足 $\langle s,i\rangle\in C$。如果 $height_C(s)=length(tr(s))$，则 C 包含一个完整的 s，或称串 s 包含在束 C 中。

3 Needham-Schroeder 公钥协议的缺陷转换

3.1 协议的代数缺陷

Needham-Schroeder 公钥协议[8]实现 A、B 双向认证，K_a、K_b 分别是 A、B 的公钥，K_S^{-1} 是可信服务器的签名私钥。该协议描述如下：

1. $A\rightarrow S: A,B$
2. $S\rightarrow A: \{K_b,B\}_{KS}^{-1}$
3. $A\rightarrow B: \{N_a,A\}_{Kb}$
4. $B\rightarrow S: B,A$
5. $S\rightarrow B: \{K_a,A\}_{KS}^{-1}$
6. $B\rightarrow A: \{N_a,N_b\}_{Ka}$
7. $A\rightarrow B: \{N_b\}_{Kb}$

其中1、2是 A 向 S 索取 B 的公钥，4、5是 B 向 S 索取 A 的公钥。如果假设 A、B 都已取得对方的公钥，则原协议可简化为只有三条消息的协议，图1是这个简化协议的串空间消息交换图。

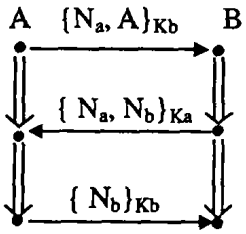


图1 简化的 Needham-Schroeder 公钥协议

定义3.1 简化的 Needham-Schroeder 公钥协议是含入侵者的串空间 (Σ,P)，设 $T_{name}\subseteq T$，(Σ,P) 包含三种串：

1)入侵者串 $S_p\in P$；

2)发起者串 $S_i\in Init[A,B,N_a,N_b], A\in T_{name}, N_a,N_b\in T, N_a\in T_{name}$，串 S_i 的轨迹是 $\langle +\{N_a,A\}_{kb},-\{N_a,N_b\}_{ka},+\{N_b\}_{kb}\rangle$。

3)响应者串 $S_r\in Resp[A,B,N_a,N_b], A\in T_{name}, N_a,N_b\in T, N_b\in T_{name}$，串 S_r 的轨迹是 $\langle -\{N_a,A\}_{kb},+\{N_a,N_b\}_{kb},-\{N_b\}_{kb}\rangle$。

利用文[2]的串空间认证测试理论我们可以证明这个协议存在下面的代数缺陷。

命题3.2 设 C 是 Σ 中的一个束，$s\in Resp[A,N_a,N_b]$ 是一个响应者串，它在 C 上束高是3。假设 $K_a^{-1}\notin K_p$，如果 $N_a\neq N_b$ 且 N_b 唯一起源，则存在一个初始者串 $s'\in Init[A,B',N_a,N_b]$，其在 C 上束高是3。

证明：(证明中的术语和概念请参阅文[2])。$\{N_a,N_b\}_{k_a}$ 是结点 $\langle s,2\rangle$ 中 N_b 的测试成分。边 $\langle s,2\rangle\Rightarrow^+\langle s,3\rangle$ 是 $\{N_a,N_b\}_{K_a}$ 中 N_b 的输出测试。根据认证测试理论，存在常规结点 $m,m'\in C$ 满足 $\{N_a,N_b\}_{K_a}$ 是 m 的一个成分，而且 $m\Rightarrow^+m'$ 是 N_b 的转换边。由于 m 是负常规结点，因此 m 是某个发起者串 $s'\in Init[A',B',N'_a,N'_b]$ 的第二个结点。又因为 $term(\langle s',2\rangle)=\{N_a,N_b\}_{K_a}$，我们可得 $N'_a=N_a,N'_b=N_b,A'=A$，容易看出该串的 C 束高是3。 □

从命题3.2我们只能得到这样的结论：

$s\in Resp[A,B,N_a,N_b]\Rightarrow s'\in Init[A,B',N_a,N_b]$

两个串中有不同的响应者 B 和 B'，这就存在一个认证缺陷：响应者 B 认为他与发起者 A 进行了一次认证，而发起者 A 只认为他是和 B' 完成了一次认证。

3.2 缺陷的实际攻击转换

针对这个代数缺陷，入侵者是如何实施攻击的呢?我们的目的是构造一个完整的含入侵者的串空间消息交换图，使命题3.2成立，同时使 A、B 确信他们都与自己意定的对象完成了一次协议执行。

启发式规则1 在束的约束下，按代数结论分别确定代数结果的前提和后件串轨迹。

于是我们得到下列的响应者和发起者的串空间消息交换图：

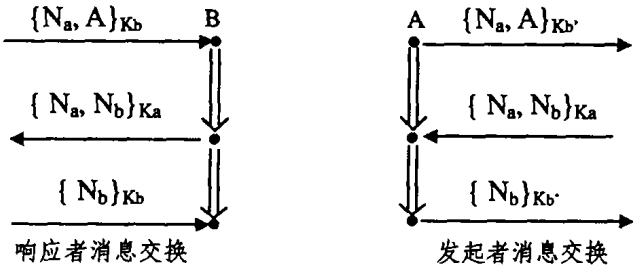


图2

启发式规则2 如果代数结果的前提和后件有不同的主体名，则认为这个不同的主体为入侵者，更改对应的消息交换图。

由于 $B\neq B'$，根据这个规则我们确定 B' 为入侵者，把 $Init[A,B',N_a,N_b]$ 改为 $Init[A,P,N_a,N_b]$，P 是入侵者。从而得到下面的发起者串轨迹。

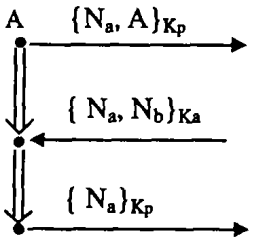


图3 发起者与入侵者的消息交换

启发式规则3 构造协议合法主体之间入侵者的串轨迹，使合法主体认为自己执行了一次完整的协议。

根据这个规则，我们经过以下三个步骤来构造入侵者的行为。

I. A 发出了 $\{N_a,A\}_{K_p}$ 消息，但 B 只收到 $\{N_a,A\}_{Kb}$，这个消息认为由入侵者发出。P 收到 $\{N_a,A\}_{K_p}$ 消息后，由于 K_p^{-1}，$K_b\in K_p$，P 可以构造消息 $\{N_a,A\}_{Kb}$。构造的串轨迹如下：

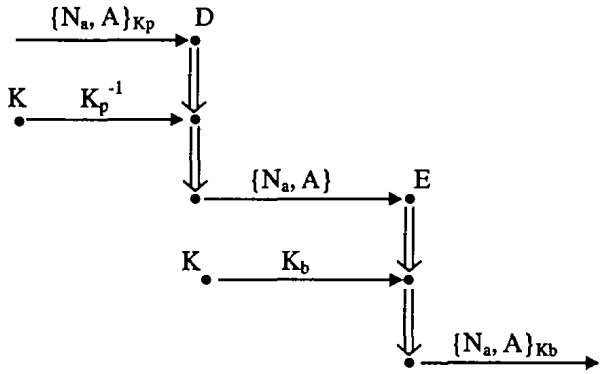


图4 入侵者转换$\{N_a,A\}_{K_P}$为$\{N_a,A\}_{K_b}$

Ⅰ. B 发出消息$\{N_a,N_b\}_{K_a}$，A 也收到了$\{N_a,N_b\}_{K_a}$消息，P 不对这个消息进行分析处理，而是拦截转发。

Ⅱ. A 发出消息$\{N_b\}_{K_P}$，由于 $K_P^{-1},K_b\in K_P$，P 可以构造消息$\{N_b\}_{K_b}$，其串轨迹如下：

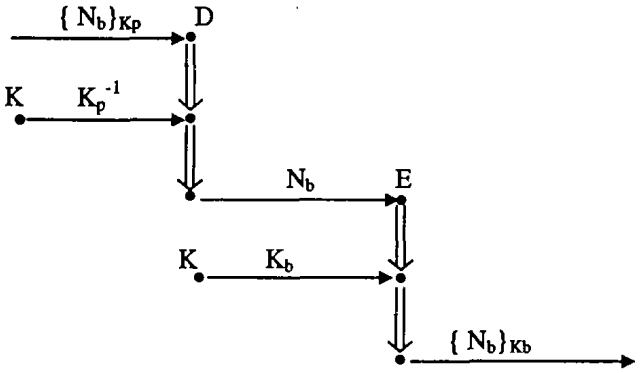


图5 入侵者转换$\{N_b\}_{K_P}$为$\{N_b\}_{K_b}$

结合图2、3、4和5我们已经得到下面一个完整的攻击过程：

3. $A\rightarrow P:\{N_a,A\}_{K_P}$
3'. $P(A)\rightarrow B:\{Na,A\}_{K_b}$
6'. $B\rightarrow P(A):\{N_a,N_b\}_{K_a}$
6. $P\rightarrow A:\{N_a,N_b\}_{K_a}$
7. $A\rightarrow P:\{N_b\}_{K_P}$
7'. $P(A)\rightarrow B:\{N_b\}_{K_b}$

即入侵者 P 利用 A 向自己认证的时机冒充 A 向 B 认证，这正是 G. Lowe 在文[9]中发现的攻击。

4 Otway-Rees 对称密钥协议的缺陷转换

4.1 协议的代数缺陷

Otway-Rees 协议[7]实现 A、B 双向认证，并由密钥服务器为它们分配一个会话密钥 K。该协议的描述是：

1. $A\rightarrow B:M,A,B,\{N_a,M,A,B\}_{K_{AS}}$
2. $B\rightarrow S:M,A,B,\{N_a,M,A,B\}_{K_{AS}},\{N_b,M,A,B\}_{K_{BS}}$
3. $S\rightarrow B:M,\{N_a,K\}_{K_{AS}},\{N_b,K\}_{K_{BS}}$
4. $B\rightarrow A:M,\{N_a,K\}_{K_{AS}}$

定义4.1 Otway-Rees 协议是含入侵者的串空间(Σ,P)，设 $T_{name}\subseteq T$，$A,B\in T_{name}$，$N_a,N_b\in T$，$N_a,N_b\notin T_{name}$，K_{AS}，$K_{BS}\notin K_P$，(Σ,P)包含下列四种串：

1)入侵者串 $s_p\in P$；

2)发起者串 $s_i\in Init[A,B,N_a,M,k]$，s_i 的轨迹是：

$\langle +MAB\{Na,M,A,B\}_{KAS},-M\{Na,K\}_{KAS}\rangle$

3)响应者串 $s_r\in Resp[A,B,N_a,M,K,H,H']$，$H,H'$表示响应者无法处理的消息项，$s_r$ 的轨迹是

$\langle -MABH,MABH\{N_a,M,A,B\}_{K_{BS}},-MH'\{N_b,K\}_{K_{BS}},+MH'\rangle$

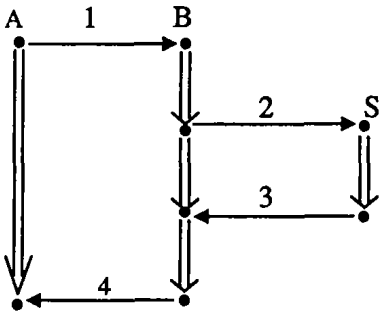


图6 *Otwav-rees* 协议串轨迹

4)服务器串 $S_i\in Serv[A,B,N_a,N_b,M,K]$，$S_i$ 的轨迹是：

$\langle -MAB,\{N_a,M,A,B\}_{KAS}\{N_b,M,A,B\}_{KBS},+M\{N_a,K\}_{KAS}(N_b,K)_{KBS}\rangle$ □

文[6]证明了该协议存在一个微妙缺陷：发起者和响应者不能共享同一个会话密钥。结论是：设 $S_i\in Init[A,B,N_a,M,K]$，$height_C(S_i)=2$，可得到下列两个蕴涵式：

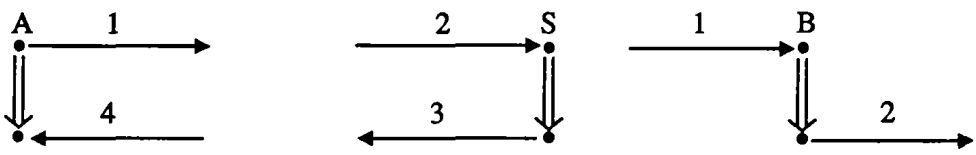
$s_i\in Init[A,B,N_a,M,K]\Rightarrow s_i\in Serv[A,B,N_a,N_b,M,K],height_C(s_i)=2$ ①

$s_i\in Init[A,B,N_a,M,K]\Rightarrow s_r\in Resp[A,B,N_b,N_b,M,**],height_C(s_r)\geqslant 2$ ②

在蕴涵式②中，** 表示任意值，因此不能保证响应者和发起者有共同的会话密钥 K。

4.2 缺陷的实际攻击转换

根据启发式规则1，我们分别确定 *Init*，*Serv* 和 *Resp* 的串执行轨迹。



(a) 发起者 A 的串　(b) 服务器 S 的串　(c) 响应者 B 的串

图7 (a)发起者 A 的串，(b)服务器 S 的串，(c)响应 B 的串

启发式规则4 如果两个主体的束高在串轨迹中和正确束高不匹配，则认为其中插入了入侵者。

由于 $height_C(s_i)=2$，$height_C(s_r)\geqslant 2$，而没有结论 $height_C(s_r)=3$，因此不能确定 S 发出的消息由 B 接受了，可认为被入侵者 P 拦截了。引入 P 的串轨迹是图8。

按照启发式规则3，我们来构造 P 的一系列入侵行为使 B 相信自己完成了一次协议执行。这个过程见图9。

P 利用重放消息2而获得 S 的返回消息3'，B 返回给 A 的消息4' 也被 P 拦截，P 把 A 意定的消息4发给 A(图8)。消息3' 是"$M,\{N_a,K'\}_{K_{AS}},\{N_b,K'\}_{K_{BS}}$"，4' 也自然是"$M,\{N_a,K'\}_{K_{AS}}$"。$B$ 执行的消息1、2、3'、4' 都满足蕴涵式2的后件。至此我们可以得到一个完整的攻击过程描述：

(下转第98页)

之间相互覆盖，因此难以被识别。

当入侵行为是小概率事件时，本方法在较小的误报容忍因子下，能够获得理想的检测率。因此在实际的应用中，本方法存在两种应用模式。

1）用于标识网络特征数据集　作为其它有监督学习方法的中间过程，用本方法辅助标记数据集中的异常数据。如果通过专家逐一标记，工作量记为 $O(n)$。由于数据集分为正常和异常两类数据，假设异常数据的比例为 β，通过本方法筛选候选的异常数据集，工作量将下降为 $O(n*\beta*\alpha)$。以 $\alpha=3$，$\beta=0.01$，那么标记效率提高近30倍。

2）用于入侵检测　其应用的基本思路是：利用前面一段时间的网络特征库作为学习数据集，在此基础上建立入侵检测模式。对于当前网络连接，计算其异常因子，如果值不属于异常值的范围内，就认为该连接正常，否则认为是异常连接。此方法的优点是不需要专家标记大量的学习数据集，因此检测模型可以定期地更新，例如每天更新一次，从而适应不断变化的网络环境。主要的缺点是需要管理人员根据分析的结果不断地调整误报容忍因子，以达到理想的检测率和误报率。

小结　本文提出了采用免疫聚类算法提取数据集的结构特征，然后根据定义的异常因子计算每一次连接的异常度。通过在实际网络特征数据集上的实验表明：新方法能够显著地提高标记异常数据的效率，且对于异常行为发生概率较低的环境中可采用本方法直接检测入侵行为。

参考文献

1 Heady R, et al. The architecture of a network level intrusion detection system: [Technical Report CS90-20]. New Mexico: University of New Mexico, Aug. 1990

2 Pell R J. Multiple outlier detection for multivariate calibration using robust statistical techniques. Chemometrics and Intelligent Laboratory Systems, 2000, 52: 87～104

3 Kollios G. Efficient Biased Sampling for Approximate Clustering and Outlier Detection in Large Data Sets. IEEE Transactions on knowledge and data engineering, 2003, 15(5)

4 Hu T, Sung S Y. Detecting pattern-based outliers. Pattern Recognition Letters, 2003, 24: 3059～3068

5 Ester M, et al. A Density-Based Algorithm for Discovering Clusters in Large Spatial Databases with Noise. In: Proc. of 2nd Intl. Conf. on Knowledge Discovery and Data Mining (KDD-96)

6 Knorr E M, Raymond. Algorithms for Mining Distance-Based Outliers in Large Datasets. In: Proc. of 24th VLDB conf, New York, USA, 1998

7 He Z, et al. Discovering cluster- based local outliers. Pattern Recognition Letters, 2003, 24: 1641～1650

8 钟将，吴中福，吴开贵，欧灵. 基于人工免疫的动态聚类算法. 电子学报，2004(8)：37～41

9 Kim D J, Park Y W, Park D J. A novel validity index for determination of the optimal number of clusters. IEICE Transactions on Information and Systems, vol. E84-D, 2001(2): 281～285

10 KDD99cupdataset. http://kdd. ics. uci. edu /databases/kddcup99/kddcup1999. html, 1999

（上接第92页）

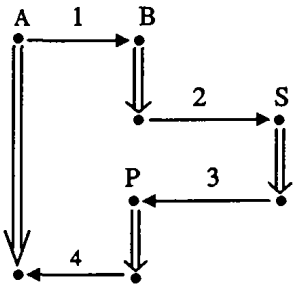


图8　S 发出的消息被 P 拦截

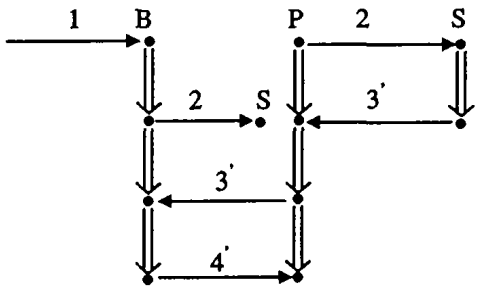


图9　P 的入侵串轨迹

1. $A\rightarrow B: M, A, B, \{N_a, M, A, B\}_{KAS}$
2. $B\rightarrow S: M, A, B, \{N_a, M, A, B\}_{KAS}, \{N_b, M, A, B\}_{KBS}$
3. $S\rightarrow P(B): M, \{N_a, k\}_{KAS}, \{N_b, K\}_{KBS}$
2' $P(B)\rightarrow S: M, A, B, \{N_a, M, A, B\}_{KAS}, \{N_b, M, A, B\}_{KBS}$
3' $S\rightarrow P(B): M, \{N_a, K'\}_{KAS}, \{N_b, K'\}_{KBS}$
3' $P(S)\rightarrow B: M, \{N_a, K'\}_{KAS}, \{N_b, K'\}_{KBS}$
4. $B\rightarrow P(A): M, \{N_a, K'\}_{KAS}$
4' $P(B)\rightarrow A: M, \{N_a, K\}_{KAS}$

攻击结果是 A 得到会话密钥 K，而 B 的会话密钥是 K'。

结论　本文针对串空间理论提出的四条启发式规则在从代数缺陷到实际攻击的转换中非常有效。它们基本上定下了一个攻击转换框架，我们只要在这个框架中填充具体的细节，就可以得到一个实际的攻击描述。但是攻击细节仍然需要我们精心构造，构造的依据是：①遵循代数结论；②根据入侵者的行为模型。

与文[3]不同的是，本文是在人工证明发现缺陷的情况下，启发式的寻找攻击路径。实际转换结果表明本文的启发式规则可以引导我们快速、有效地找到一个攻击过程。这对于研究入侵方法，改造协议是很有帮助的。

参考文献

1 Fábrega F J T, Herzog J C, Guttman J D. Mixed Strand Spaces. In: Proc. of the 12th IEEE Computer Security Foundations Workshop[C], 1999

2 Fábrega F J T, Herzog J C, Guttman J D. Authentication Tests. In: Proc. [C], 2000 IEEE Symposium on Security and Privacy, 2000

3 Song D X, Berezin S, Perrig A. Athena: A novel approach to efficient automatic security protocol analysis. Journal of Computer Security, 2001 (1/2): 47～74

4 Fábrega F J T, Herzog J C, Guttman J D. Honest Ideals on Strand Spaces. In: Proc. of the 11th IEEE Computer Security Foundations Workshop[C], 1998

5 Fábrega F J T, Herzog J C, Guttman J D. Strand Spaces: Why is a Security Protocol Correct. In: Proc. [C], 1998 IEEE Symposium on Security and Privacy, 1998

6 Fábrega F J T, Herzog J C, Guttman J D. Strand Spaces: Proving Security Protocols Correct. Journal of Computer Security[J], 191～230

7 Otway D, Rees O. Efficient and Timely Mutual Authentication. Operating Systems Review[J], 1987, 21(1): 8～10

8 Schroeder N R M. Using Encryption for Authentication in Large Networks of Computers. Communication of the ACM[J], 1978

9 Lowe G. An Attack on the Needham-Schroeder Public-key Authentication Protocol. Information Processing Letters[Z], 1995, 53: 103～107