维普资讯 http://www.cqvip.com

针对猜测攻击的 Athena 方法的扩展*)

李 超 董荣胜
(桂林电子科技大学计算机系 桂林 541004)

摘 要 猜测攻击是安全协议中一类特殊问题,对其进行研究具有现实意义。本文针对猜测攻击,引入了基于串空间模型的 Athena 分析方法,并考虑了攻击者对弱口令的猜测能力。为此,在串空间模型的消息项中引入了可验证项的概念,以描述猜测攻击条件中的验证项,同时扩展了串空间中攻击者的能力,赋予了攻击者对弱口令的猜测能力;为在 Athena 后继函数搜索算法中实现对验证项的关联,以判断猜测攻击,在 Athena 方法的状态表示法中引入猜测验证目标及猜测验证目标绑定的概念,对状态、推理规则进行相应的修改,同时扩展后继状态函数,使扩展后的函数具备分析猜测攻击的能力;最后运用扩展后的 Athena 方法对会话密钥建立协议(key-establishment protocol)进行分析。分析发现,当 pk 为对称密钥时,协议存在猜测攻击,并给出了攻击路径。

关键词 Athena,猜测攻击,串空间,弱口令,认证性

Extensions to Athena for Analyzing Guessing Attack

LI Chao DONG Rong-Sheng
(School of Computer Science, Guilin University of Electronic Technology, Guilin 541004)

Abstract In this paper we extend Athena approach based on strand space, considering the intruder's guessing poorly-chosen password ability for analyzing guessing attack automatically and efficiently. Firstly, we present a new notion and its expression of verifiable term to describe the conditions of guess attacks and enhance the intruder's ability in strand space to endue the intruder's guessing poorly-chosen password talent. Then, in order to relate verifiers in the search process of the next-state function of Athena, two new notions of guessing verifier goal and guessing verifier goal binding are presented. Accordingly, the state expressive way and inference rules are adapted. In addition, next-state functions is extended, so that it is able to analyse guessing attacks. Finally, we analyze the key-establishment protocol using the extended Athena approach, and find a guessing attack when pk is a symmetric key.

Keywords Athena, Guessing attack, Strand space, Poorly-chosen password, Authentication

1 引言

随着互联网技术的广泛应用,安全协议作为网络安全通信的保证变得日益重要。在形式化方法分析安全协议的研究中,Dolev-Yao 模型对密码系统做了一个理想的假设,使协议分析者更专注于分析安全协议内在的安全问题[1]。实际上,密码系统并不是无懈可击的,尤其是人们在安全系统中使用的密钥常常是弱口令的情况下,攻击者可以猜测这些弱口令,并在协议中寻求验证,达到猜测攻击的目的。在研究现实环境下安全协议的安全性时,赋予攻击者猜测攻击的能力是有必要的。正因为这样的原因,不少学者对猜测攻击进行了研究,研究主要集中在设计和分析两个方面。本文的研究重点放在猜测攻击的分析上。

在猜测攻击的分析方面,Gong 提出了一种图论的方法来检查协议的猜测攻击性[2]。但他只考虑了要验证的项是攻击者初始就知道的情况,没有考虑验证项由两种不同方式产生的情况;Ding 和 Horster 针对 Steiner 在 EKE 协议基础上提出的三方认证协议[3],给出了一种非确定在线猜测攻击的方法[4],但其分析方法和大多数文献一样使用的是非形式化的方法;在这方面的研究中,Halevi 和 Krawczyk 最早使用形式化方法证明这类协议的安全性[5],但该方法基于计算复杂性理论,复杂性较高,不能自动分析;之后 Lowe 首次形式化地定义了猜测攻击和猜测攻击验证的方式,使用 CSP 对这种攻击进行建模并用模型检验器 FDR 进行了检测[6],但受模型检验的影响,在分析复杂协议时,无法避免状态空间爆炸的问题。针对以上问题,一个很自然的想法就是利用或改进现有的技术,对猜测攻击进行自动、高效的分析。

经过比较,我们选用了基于串空间的 Athena 分析方法。该方法是一种结合了模型检验和交互式定理证明技术(串空间模型[7])的安全协议分析方法,它消减了状态搜索空间,且能对安全协议任意数量的并发运行进行验证,具有直观、高效、自动的特点[8]。但是,原始的 Athena 分析方法缺乏描述猜测攻击的原语和算法支持,不能分析猜测攻击问题。为此,在本课题现有工作的基础上[9],本文对 Athena 分析方法进行了扩展,使其能自动而高效地分析猜测攻击。

Athena 分析方法中的消息表示以串空间模型为基础,因此本文在串空间模型的消息项中引入了可验证项的概念及表示方法,以描述猜测攻击的条件,同时扩展了串空间中攻击者的能力,以赋予攻击者对弱口令的猜测。在 Athena 方法的状态表示法中引入猜测验证目标及猜测验证目标绑定的概念,并对状态及推理规则中的 Init 和 Final 规则进行相应修改,以使后继函数搜索算法中实现对验证项的关联,以判断猜测攻

*)本文得到广西自然科学基金项目(编号:0542052)的资助。

维普资讯 http://www.cqvip.com

击。再对后继状态函数进行扩展，使扩展后的函数具备分析猜测攻击的能力，最后运用扩展后的 Athena 方法对会话密钥建立协议(key-establishment protocol)进行分析。分析发现，当 pk 为对称密钥时，协议存在猜测攻击，并给出了攻击路径。

2 串空间的扩展

从本节开始，本文将对 Athena 方法进行扩展。由于篇幅，本文对串空间模型及 Athena 的基础知识不进行说明，有关内容可以参见文[7,8]及本文前期工作[9]。

对串空间模型的扩展主要包括两个方面：消息项的扩展和入侵者模型的扩展。

2.1 消息项扩展

用 k_g 表示存在猜测成功可能性的密钥(下文称作可猜测密钥)，即用户的弱口令；

定义 1 可猜测推导密钥集 K_G 是所有可猜测密钥 k_g 以及利用 k_g 可能推导出的密钥 k_d 的集合。

值得指出的是，只有起源于协议正则串的密钥才有可能通过 k_g 推导而得，因此 k_d 必起源于正则串。

猜测攻击之所以能够成功，是因为攻击者能够在协议中寻求到验证项来验证猜测是否正确。因此，在协议分析过程中，如果能找到两种不同方式产生的同一验证项(验证项直接在协议中出现也算一种方式)，则猜测攻击理论上便会发生。为描述可能的验证项，本文引入可验证项的概念。

定义 2 可验证项 t_v 是满足下面条件的项：

(1)$t_v \in \mathcal{T} \cup \mathcal{X}$

(2)$t_v \sqsubset \{h\}_k$

其中 $h \in \mathcal{A}, k \in K_G$。

条件(1)说明 t_v 必须是原子项，条件(2)说明 t_v 必须出现在以可猜测推导密钥加密的项中。可验证项与验证项不同，可验证项是可能成为验证项的项。由可验证项组成的集合称为可验证集，记为 V。

2.2 攻击者模型的扩展

由于引入了攻击者的猜测能力，需要入侵者模型的修改包括两个方面：入侵者初始知识的修改和入侵者角色的修改。

下面先给出协议合法参与者初始知识集合的定义。

定义 3 合法参与者初始知识由下面几个部分组成：

(1)所有主体的姓名；

(2)所有公共密钥、自身的私有密钥以及作为协议运行主体，通过协议规则获得的对称密钥；

在定义 3 的基础上，给出入侵者初始知识的定义。

定义 4 入侵者初始知识定义 init-info(P)如下：

(1)入侵者作为合法参与者获得的初始知识；

(2)协议中的可猜测密钥；

(3)入侵者之间的知识是共享的。

即入侵者 P 的初始知识 init-info(P)包括：主体的名字和入侵者初始密钥集合 Kp。Kp 通常包括公共密钥、所有入侵者的私有密钥、入侵者和其它主体通过运用协议规则分享的对称密钥以及可猜测密钥。

入侵者能够截获消息，并且能够通过初始的知识和截获的消息得到新的知识，构造新的消息。Athena 通过入侵者角色对入侵者动作进行建模。本文在此基础上引入新的入侵者猜测的能力：

$G[k]$ 猜测：$\langle +k \rangle$，这里 $k \in K_G$。

故入侵者角色的集合扩展为：$\Pi = \{M, F, T, V, R, K, E, D, G\}$。

3 Athena 分析方法的扩展

Athena 分析方法的扩展主要包括状态表示法的扩展、推理规则的扩展和后继状态函数的扩展。

3.1 状态表示法的扩展

为在 Athena 后继函数搜索算法中关联验证项，以判断猜测攻击，在 Athena 方法的状态表示法中引入猜测验证目标及猜测验证目标绑定的概念。

定义 5 猜测验证目标是一个二元组 (t_v, n)，这里，sign$(n) = -$，$t_v \in V$。从 C 中的猜测验证目标集合是 C 中所有猜测验证目标的集合，用 $GG(c)$ 来表示。

不难发现，猜测验证目标是一个特殊目标，它的项严格要求为可验证项。

定义 6 称猜测验证目标 (t_v, n)，猜测验证绑定到 n' 上，当且仅当 n' 满足如下条件：

(1)sign$(n') = +$

(2)term$(n') =$ tv

(3)$n \in \sum_{\Pi} \vee n' \in \sum_{\Pi}$

其中，$\sum_{\Pi}$ 表示攻击者串。用 $n \leftrightarrows n'$ 表示猜测验证目标绑定。

猜测验证绑定是可验证项的互绑，作用是将两个不同方式产生的同一个可验证项加以关联，以便寻求进行猜测验证的验证项。

由于引入了猜测验证目标及猜测验证绑定的概念，对状态进行相应的修改。

定义 7 将状态扩展为一个四元组 $(S, G, \twoheadrightarrow, \leftrightarrows)$，

其中：

(1)S 是一个半丛；

(2)G 是 S 中没有绑定的目标集合；

(3)$\twoheadrightarrow$ 是目标绑定的关系；

(4)$\leftrightarrows$ 是猜测验证目标绑定的关系。

注意，G 在此定义中是冗余的，它可以通过 S 和 $\twoheadrightarrow$ 计算出来。

扩展后的状态引入了 $\leftrightarrows$ 关系，使得从状态 l 中不仅能反映出目标绑定的关系，同时还能反映出猜测验证目标绑定的关系。由于这里 $\leftrightarrows$ 的引入只是在状态中引入了对猜测验证目标绑定的关系说明，且猜测验证目标绑定本就是目标绑定中的一类特殊情况，因此 $\leftrightarrows$ 的引入并没有破坏完备性。

3.2 推理规则的扩展

推理规则的扩展包括两方面：Init 规则的扩展和 Final 规则的扩展。

3.2.1 Init 规则的扩展

将验证目标 $(P; \Gamma \vdash \Delta)$ 转换成另外一个形式的序列 $l \vdash \Delta$，这里，l 是一个状态：

$$\frac{l_0(P, \Gamma) \vdash \Delta}{P; \Gamma \vdash \Delta}$$

初始状态 $l_0(P, \Gamma)$ 表示的是任何一个满足下面条件的半丛：它必须满足协议 P 并且包括了 Γ 中的所有串。初始状态 $l_0(P, \Gamma) = \langle S_\Gamma, G_\Gamma, \emptyset, \emptyset \rangle$，这里，$S_\Gamma$ 表示包括了 Γ 的最小半丛，也就是说，S_Γ 是 Γ 用关系 $\Rightarrow$ 构成的回溯闭包(backward closure)；G_Γ 是由 S_Γ 计算出来的。初始状态没有进行目标绑定和猜测验证目标绑定，因此关系 $\twoheadrightarrow$ 和 $\leftrightarrows$ 为空。

从初始状态 $l_0 = l_0(P, \Gamma)$ 的结构以及其语义可以看到它满足下面的性质：

维普资讯 http://www.cqvip.com

$\Gamma \subseteq l_0$

$\forall C.\ \Gamma \subseteq C \Rightarrow C \in \Psi(l_0)$

这条性质显然是可靠并且可逆的。证明省略。

3.2.2 final 规则的扩展

若 $\Delta \cap l \neq \phi$，$l \vdash \Delta$ 称为叶序列(leaf sequent)。当 $l \vdash \Delta$ 称为叶序列的时候，运用 final 推理规则：

$$\frac{\Delta \cap l \neq \emptyset}{l \vdash \Delta}$$

可逆性是很明显的。可靠性证明：对于任何的半丛 C，$C \in \Psi(l)$，那么 C 是 S_l 的超图，又因为 $\Delta \cap l \neq \phi$，则 Δ 与 C 的交集也是非空的。$l \vdash \Delta$ 得证。

若 $G=\phi$，并且 final 规则不能运用，则当前的式子 $l \vdash \Delta$ 是错误的，或者说是悖论。

原因：若 $G=\phi$，则对任何一个正则串 s，$s \in S_l$ 当且仅当 $s \in C$。现在存在一个半丛 C，$C \in \Psi(l)$，因为在 Δ 中没有一个串是在 S_l，那么它也不可能在 C 中，这意味着 $\exists C \in \Psi(l')$。$\Delta \cap l = \phi$，因此 $l \vdash \Delta$ 是错误的。因为所有的规则可逆，那么初始序列也是错误的。这个悖论序列就是一个反例，它展示了针对协议的一次成功攻击。若此时 $\leftrightsquigarrow$ 不为空，则这个悖论序列展示的就是针对协议的一次成功的猜测攻击。因为 $G=\phi$，$\leftrightsquigarrow$ 不为空说明了这个序列中存在两种不同方式产生的可验证项可以通过 $\leftrightsquigarrow$ 联系起来($\leftrightsquigarrow$ 联系的必为两个不同的串)，此时的可验证项即为验证项。如果将验证项直接出现在初始串中也算一种产生方式的话(将文[6]中的条件(4)中第一部分 $S' \vdash_{l'} v$ in $\mathrm{tr} \wedge (S, l) \neq (S', l')$ 和第二部分 $v \in IK \cup \{g\}$ 合为一个条件)，协议可以由两种不同方式产生验证员，于是存在猜测攻击。

3.3 后继状态函数的扩展

计算协议 P 状态 $l=\langle S, G, \twoheadrightarrow, \leftrightsquigarrow \rangle$ 的后继状态，首先选定没有绑定的猜测验证目标 $gg=(t_v, n) \in GG$，执行(ⅰ)；如果状态 l 处不存在猜测验证目标，则选定一个没有绑定的目标 $g \in G$，执行(ⅱ)：

(ⅰ)计算关于可猜测验证项 t_v 的统一替代者集合 $UP(t_v)$，对任意一个项 $u=([r, i], \sigma) \in UP(t_v)$，构造后继状态如下：

(1) 使得 $Su=(\Rightarrow^{-1}) * [\sigma(\langle r, i \rangle)]$ 是一个(可能是部分)串，这个串以 $\sigma(\langle r, i \rangle)$ 为结束节点，并且在 $\Rightarrow$ 上回溯闭包；它包括了 $\sigma(\langle r, i \rangle)$ 节点以及所有 $\sigma(r)$ 的前驱节点。

(2) 对于任意开始于初始状态 l 的串 $s \in S$，若存在一个替代 γ_s 使得 $\gamma_s(Su) \cap \sigma(s) \neq \phi$，即 $\gamma_s(Su)$ 和 $\sigma(s)$ 有相同的节点，那么 $\sigma(s)$ 是 Su 的一个实例化。构造出一个新的状态 $l'=\langle S', G', \twoheadrightarrow', \leftrightsquigarrow' \rangle$，这里：

1) $S'=\sigma(s) \cup \{\gamma_s(Su)\}$；

2) $\twoheadrightarrow' = \sigma(\twoheadrightarrow) \cup \{\langle s', i \rangle \overset{\sigma(t)}{\twoheadrightarrow} \sigma(gg)\}$

(gg 既是可验证目标也是目标，它作为目标被串 s' 的第 i 个节点绑定)；

3) G' 根据上面两条进行更新；

4) $\leftrightsquigarrow' = \sigma(\leftrightsquigarrow) \cup \{\langle s', i \rangle \leftrightsquigarrow \sigma(gg)\}$

(3)将 Su 作为一个新的串，构造了附加的下一个状态 l'' (additional next state)$=\langle S'', G'', \twoheadrightarrow'', \leftrightsquigarrow'' \rangle$，

1) $S''= \sigma(s) \cup Su$；

2) $\twoheadrightarrow'' = \sigma(\twoheadrightarrow) \cup \{\langle Su, i \rangle \twoheadrightarrow \sigma(gg)\}$

(gg 既是可验证目标也是目标，它作为目标绑定在 Su 上的最后一个节点)；

3) G'' 根据上面两条进行更新；

4) $\leftrightsquigarrow'' = \sigma(\leftrightsquigarrow) \cup \{\langle Su, i \rangle \leftrightsquigarrow \sigma(gg)\}$。

(ⅱ)计算关于项 t 的统一者集合 $UP(t)$，对任意一个项 $u=([r, i], \sigma) \in UP(t)$，构造下一个状态如下：

(1) 使得 $Su=(\Rightarrow^{-1}) * [\sigma(\langle r, i \rangle)]$ 是一个(可能是部分)串，这个串以 $\sigma(\langle r, i \rangle)$ 为结束节点，并且在 $\Rightarrow$ 上回溯闭包；它包括了 $\sigma(\langle r, i \rangle)$ 节点以及所有 $\sigma(r)$ 的前驱节点。

(2) 对于任意开始于初始状态 l 的串 $s \in S$，若存在一个替换 γ_s 使得 $\gamma_s(Su) \cap \sigma(s) \neq \phi$，即 $\gamma_s(Su)$ 和 $\sigma(s)$ 有相同的节点，那么 $\sigma(s)$ 是 Su 的一个实例化。构造出一个新的状态 $l'=\langle S', G', \twoheadrightarrow', \leftrightsquigarrow' \rangle$，这里：

1) $S'=\sigma(s) \cup \{\gamma_s(Su)\}$；

2) $\twoheadrightarrow' = \sigma(\twoheadrightarrow) \cup \{\langle s', i \rangle \twoheadrightarrow \sigma(g)\}$

(目标 g 被串 s' 的第 i 个节点绑定)；

3) G' 根据上面两条进行更新；

4) $\leftrightsquigarrow' = \leftrightsquigarrow$。

(3) 将 Su 作为一个新的串，构造了附加的下一个状态 $l''=\langle S'', G', \twoheadrightarrow'', \leftrightsquigarrow'' \rangle$，

1) $S''= \sigma(s) \cup Su$；

2) $\twoheadrightarrow'' = \sigma(\twoheadrightarrow) \cup \{\langle Su, i \rangle (\sigma(g)\}$

(目标 g 绑定在 Su 上的最后一个节点)；

3) G'' 根据上面两条进行更新；

4) $\leftrightsquigarrow' = \leftrightsquigarrow$。

后继状态可能无效，文[8,9]中给出了判断方法。本文仅对其中一点稍加说明，因为它可以有效地避免文[6]中条件 5 的情况。

文[6]条件 5 中引入 undose 关系说明对先前步骤进行简单的反向运算是不可行的。比如，若 v 是验证项，将得到的 v 通过 k 加密得到 $\{v\}_k$，再通过解密 $\{v\}_k$ 得到 v。企图通过这样的方式得到“两种方式产生 v”是不可行的。

在 Athena 中可以很自然地避免这种情况的发生：如果 l' 形成关于 $\twoheadrightarrow$ 和 $\Rightarrow$ 的封闭图形，则 l' 无效。即如果试图通过上面的方法以期产生两个 v，则会产生封闭图形，因此这种情况会在 Athena 的搜索过程中自动地剔出掉。

4 实例分析

文[2]中 Bellovin 和 Merritt 介绍了如下基于弱口令的会话密钥建立协议。这里 pk 是一个非对称密钥，k 是对称的会话密钥。文[6]中 Lowe 运用 Casper/FDR 分析该协议没有发现攻击。而后为考虑 pk 须为非对称密钥的必要性，Lowe 假设 pk 为对称密钥进行分析时，发现了猜测攻击。本文运用扩展后的 Athena 方法进行分析，得出了文[6]中相同的结论。

1. $a \rightarrow b$: $a, \{pk\}_{pab}$
2. $b \rightarrow a$: $\{\{k\}pk\}_{pab}$
3. $a \rightarrow b$: $\{Na\}_k$
4. $b \rightarrow a$: $\{Na, Nb\}_k$
5. $a \rightarrow b$: $\{Nb\}_k$

这里对协议的认证性进行分析。当 pk 为非对称密钥时，协议的认证性是满足的，当 pk 为对称密钥时，Athena 最终的状态图说明由于发生了猜测攻击，其认证性不满足。限于篇幅，本文仅给出 pk 为对称密钥时 Athena 的反例状态图，并给出对应的反例。为使图简洁，在最终状态图中，省略了入侵者角色的参数(注意：在分析过程中由于参数不能确定，参数不能省略)。

(下转第 81 页)

维普资讯 http://www.cqvip.com

一步的研究。

结束语 基于包标记的攻击源追踪技术以其灵活高效的特点，引起业界的广泛注意。研究者提出了很多方案，但存在性能上的差异，本文对目前有代表性的几种方案的性能指标做了深入的探讨，为后续工作的性能优化提供了依据。

参 考 文 献

1 Savage S, Wetherall D. Network support for IP traceback. IEEE/ACM Transactions on Networking, 2001, 9(3): 226～237

2 Song D, Perrig A. Advanced and authenticated marking schemes for IP traceback. In: Proceedings of the IEEE INFOCOM, Anchorage, Alaska USA, 2001, 2: 878～886

3 Peng T, Leckie C, Kotagiri R. Adjusted probabilistic packet marking for IP traceback [A]. In: Proceedings of the Second IFIP Networking Conference (Networking 2002) [C]. Pisa, Italy, May 2002. 697～708

4 Liu J, Lee Z J, Chuang Y C. Efficient dynamic probabilistic packet marking for IP traceback [A]. Networks, ICON2003 [C], 2003. 475～480

5 徐永红，杨云，刘凤玉，等. 基于权重包标记策略的 IP 追踪技术研究[J]. 计算机学报，2003, 26(11): 1598～1603

（上接第 67 页）

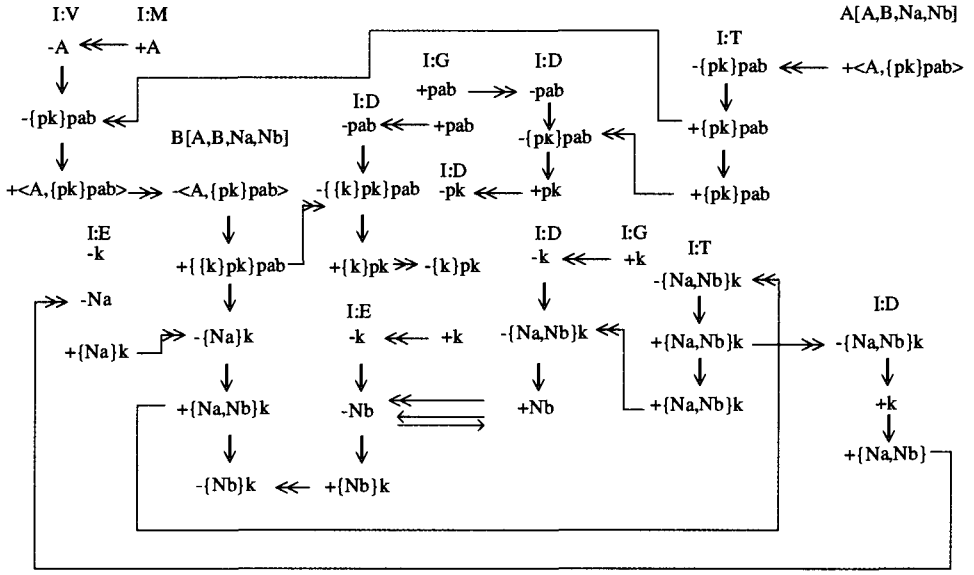

图 1 Athena 分析方法最终状态图

图 1 为运用扩展后的 Athena 方法生成的最后的状态图。因为在这里 $\Delta \cap l = \emptyset$，Final 规则不能运用，且 $G = \emptyset$ 说明认证性不满足。又由 $GG \neq \emptyset$ 可知，存在猜测攻击，所以该状态图为猜测攻击的反例。

$\leftrightarrows$ 两端对应的为两种不同方式产生的验证项 Nb，其生成过程便是猜测攻击的攻击过程：

(1)攻击者截获 $\{pk\}_{pab}$；

(2)猜测弱口令 pab，得到 pk；

(3)截获 $\{\{k\}_{pk}\}_{pab}$；

(4)利用 pab 和(2)中得到的 pk，得到 k；

(5)截获 $\{Na, Nb\}_k$，$\{Nb\}_k$；

(6)利用 k 解密 $\{Na, Nb\}_k$，得到 Nb；解密 $\{Nb\}_k$ 得到 Nb，存在两种不同的方式产生验证元 Nb。

结束语 本文在课题组前期工作的基础上针对猜测攻击对 Athena 分析方法进行了扩展，并运用扩展后的 Athena 方法对协议实例进行了分析，指出其攻击序列。本文进行扩展时对 Lowe 在文[6]中形式化定义的猜测攻击的条件进行了适当简化，假定私钥不可能丢失，因此没有将其条件(4)中第三部分($v \in$ ASYMMETRIC_KEYS $\wedge v^{-1} \in IK$)考虑其中。本文分析实例时猜测攻击之所以发生是由于协议中存在两种不同方法来产生验证元(将验证元直接在协议中出现也视为其中一种方法)。将一个单独运行的不存在猜测攻击的协议置于多协议环境中，由于消息项交互的可能性增加，由两种不同方法产生验证元的可能性也随之增加，即发生猜测攻击可能性会增加。因此将各自独立运行安全的多个协议混合运行，发生猜测攻击也是可能的。

参 考 文 献

1 卿斯汉. 安全协议 20 年研究进展[J]. 软件学报，2003, 14(10): 1740～1752

2 Gong L, Mark T, Lomas A, et al. Protecting poorly chosen secrets from guessing attacks[J]. IEEE Journal on Selected Areas in Communications, 1993, 11(5): 648～656

3 Steiner M, Tsudik G, Waidner M. Refinement and extension of encrypted key exchange[J]. ACM Operating Systems Review, 1995, 29(3): 24～29

4 Ding Y, Horster P. Undetectable on-line password guessing attacks[J]. ACM Operating Systems Review, 2000, 34(4): 12～20

5 Halevi S, Krawczyk H. Public-key cryptography and password protocols[A]. In: ACM Transaction on Information and System Security[C]. New York, USA, ACMPress, 1999, 23: 230～268

6 Lowe G. Analysing protocols subject to guessing attacks[A]. In: Workshop on Issues in the Theory of Security WITS'02[C], January 2002

7 Thayer F J, Herzog J C, Guttman J D. Strand spaces: Why is a security protocol correct? In: Proceedings of 1998 IEEE Symposium on Security and Privacy[C], 1998. 160～171

8 Song D, Perrig A, Berezin S. Athena: a novel approach to efficient automatic security protocol analysis[J]. Journal of Computer Security, 2001, 9(1-2): 47～74

9 吴光伟，董荣胜. 基于串空间的 Athena 分析技术研究[J]. 计算机科学，2006, 33(8): 9～13