认证测试方法在应用中出现的问题及改进*)

李晓乐[1] 董荣胜[1] 郭云川[1,2]

(桂林电子科技大学计算机系 桂林 541004)[1] (中国科学院计算技术研究所 北京 100080)[2]

摘 要 在应用中,当关键原子值发生多次形式转换时,需要进行多次认证测试。鉴于此,本文引入了关键分量(Key Component)的概念,提出了多重认证测试(Multiple Authentication Test)方法。使用该方法重新设计了 Woo-Lam 协议,通过两个"挑战-响应"回合,确保主体角色的非对称性和响应者对发起者的身份认证。设计出的 Woo-Lam 协议不仅避免了原协议经认证测试方法改进后存在的缺少主体标识的缺陷,而且避免了 Abadi 和 Buttyan 等人分别对原协议改进后存在的两个重放攻击。

关键词 认证测试,Woo-Lam 协议,关键分量,多重认证测试,角色非对称性

Improvement of Authentication Test in Application

LI Xiao-Le[1] DONG Rong-Sheng[1] GUO Yun-Chuan[1,2]

(Department of Computer Science, Guilin University of Electronic Technology, Guilin 541004)[1]

(Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080)[2]

Abstract In application, when multiple form transformations of key atomic value occur, there should be multiple authentication tests. With the conception of Key Component, a new method called Multiple Authentication Test is presented. Then the Woo-Lam protocol is redesigned and improved by this method. Through two "challenge-response" runs, the role asymmetry and identity authentication of participants are ensured, not only avoiding the flaw in the protocol improved by Authentication Test, but also avoiding two replay attacks in the protocol improved by informal principles and BSW logic.

Keywords Authentication test, Woo-Lam protocol, Key component, Multiple authentication test, Role asymmetry

认证测试方法(Authentication Test)是 Guttman 等人在 2000 年提出的一种基于串空间的安全协议分析与设计技术[1,2]。它的基本思想是:若协议的一个主体创建并发送了包含某个新值 v 的消息,且在随后收到了改变加密形式后的 v 值,则可推知,存在某个拥有相应密钥的协议主体改变了包含 v 值的这则消息。认证测试方法的优点在于:(1)既可以用于协议的安全性分析,也能用于协议的设计[1~4];(2)与 BAN 逻辑相比,能更加准确地定位协议漏洞,与传统串空间理论中构造集合寻找 M-minimal 元素的方法相比,更为简洁直观。

尽管认证测试方法优点显著,但也存在一定的局限性:Perrig 和 Song 指出,文[1,2]提出的认证定理中存在不允许对测试分量加密的局限[4];Choi 指出,协议参与方之间存在一个通用共享秘密的假设限制了认证测试方法的适用性[5]。

本文则发现,在应用中,当关键原子值发生多次形式转换时,需要进行多次认证测试。鉴于此,引入了关键分量(Key Component)的概念,提出了对多次转换形式的关键分量进行测试的多重认证测试(Multiple Authentication Test)方法。该方法分析关键分量需要发生的形式转换次数,然后以此为依据对关键分量进行相应次数的认证测试,进而确定相关正则主体的行为。以 Woo-Lam 协议的重新设计为例,多重认证测试方法通过两个"挑战-响应"回合实现协议的认证目标:通过 N_b 在 $\{|\cdots N_b\cdots|\}_{Kas}$ 中的入测试 Test1,保证对称环境下主体角色的非对称性;通过 N_b 在 $\{|\cdots N_b\cdots|\}_{Kbs}$ 中的入测试 Test2,保证响应者 B 对发起者 A 的身份认证。设计出的协议不仅避免了原协议经认证测试方法改进后存在的缺少主体标识的缺陷,而且能避免 Abadi 和 Buttyan 等人分别对原协议改进后存在的两个重放攻击[6]。

1 认证测试方法对 Woo-Lam 协议的改进及不足

1.1 针对 Woo-Lam 协议的攻击

Woo-Lam 协议是三方参与的单向认证协议,要求协议响应者 B 认证发起者 A 的存在性。该协议如下:

(1)$A\rightarrow B:A$

(2)$B\rightarrow A:N_b$

(3)$A\rightarrow B:\{N_b\}_{Kas}$

(4)$B\rightarrow S:\{A,\{N_b\}Kas\}_{Kbs}$

(5)$S\rightarrow B:\{N_b\}_{Kbs}$

文[7]指出了针对该协议的两个重放攻击。

攻击 1:

(1)$P(A)\rightarrow B:A$

(2)$B\rightarrow P(A):N_b$

(3)$P(A)\rightarrow B:X$

(4)$B\rightarrow P(S):\{A,X\}_{Kbs}$

(1′)$B\rightarrow P(C):B$

(2′)$P(C)\rightarrow B:P,\{N_b\}_{Kps}$

(3′)$B\rightarrow P(C):\{P,\{N_b\}_{Kps}\}_{Kbs}$

(4′)$P(B)\rightarrow S:\{P,\{N_b\}_{Kps}\}_{Kbs}$

(5′)$S\rightarrow P(B):\{N_b\}_{Kbs}$

*)本文得到广西自然科学基金项目(0542052)的资助。

(5)$P(S)\rightarrow B:\{N_b\}_{Kbs}$

攻击 2:

(1)$P(A)\rightarrow B:A$

(1′)$P\rightarrow B:P$

(2)$B\rightarrow P(A):N_b$

(2′)$B\rightarrow P:N'_b$

(3)$P(A)\rightarrow B:X$

(3′)$P\rightarrow B:\{N_b\}_{Kps}$

(4)$B\rightarrow S:\{A,X\}_{Kbs}$

(4′)$B\rightarrow S:\{P,\{N_b\}_{Kps}\}_{Kbs}$

(5′)

(5)$S\rightarrow B:\{N_b\}_{Kbs}$

1.2 认证测试方法对 Woo-Lam 协议的改进

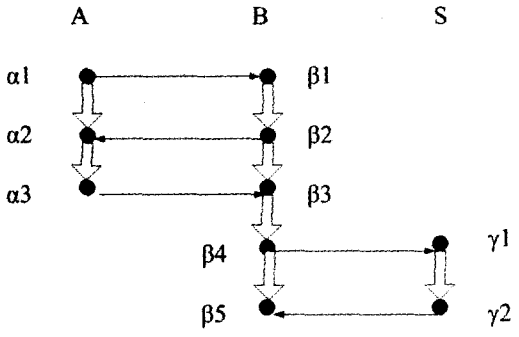

图 1 Woo-Lam 协议的框架

例 1 如图 1 所示,根据文[1,2]中的分析,Woo-Lam 协议目标的实现分为三步:

(1)收到 A 发送的主体标识后,B 在 $\beta 2$ 处生成现时值 N_b,并发起一个针对 N_b 的入测试:

$-\langle\{|A|\}\rangle\Rightarrow+\langle\{|N_b|\}\rangle\Rightarrow\cdots$;

(2)B 在 $\beta 3$ 处收到 A 发出的包含 N_b 的加密分量,在 $\beta 4$ 处将包含该分量的消息项发送给 S:

$\cdots\langle\cdots\{|\cdots N_b\cdots|\}_{Kas}\rangle\Rightarrow+\langle\cdots\{|\cdots N_b\cdots|\}_{Kas}\rangle\Rightarrow\cdots$;

(3)B 在 $\beta 5$ 处收到经 S 处理后的反馈消息,认证 S 在 A 的加密消息中发现了 N_b:

$\cdots-\langle\{|\cdots N_b\cdots|\}_{Kbs}\rangle$。

得到 B 的迹如下:

$-\langle\{|A|\}\rangle\Rightarrow+\langle\{|N_b|\}\rangle\Rightarrow-\langle\cdots\{|\cdots N_b\cdots|\}_{Kas}\rangle\Rightarrow+\langle\cdots\{|\cdots N_b\cdots|\}_{Kas}\rangle\Rightarrow-\langle\{|\cdots N_b\cdots|\}_{Kbs}\rangle$

其中,$\beta 2\Rightarrow^{+}\beta 5$ 是 N_b 在$\{|\cdots N_b\cdots|\}_{Kbs}$中的入测试,以$\cdots\{|\cdots N_b\cdots|\}_{Kas}\Rightarrow\{|\cdots N_b\cdots|\}_{Kbs}$(即 $\gamma 1\Rightarrow\gamma 2$)为相应的转换边。

为了确定唯一的正则转换边,在入测试中,服务器串$\{|\cdots N_b\cdots|\}_{Kbs}$应为$\{|A,N_b|\}_{Kbs}$。

改进后的 Woo-Lam 协议 V1 如下:

(1)$A\rightarrow B:A$

(2)$B\rightarrow A:N_b$

(3)$A\rightarrow B:\{N_b\}_{Kas}$

(4)$B\rightarrow S:A,\{N_b\}_{Kas}$

(5)$S\rightarrow B:\{A,N_b\}_{Kbs}$

1.3 改进后的协议仍存在的缺陷

使用认证测试方法改进后的协议 V1 在(5)中实现了对主体 A 的身份确认,避免了原 Woo-Lam 协议中的两个重放攻击。

但是本文发现,协议 V1 依然存在缺陷。由于(3)中缺少必要的标识信息,无法保证主体 B 和 S 的角色非对称性,导致 V1 中存在另一个重放攻击:

攻击 3:

(1)$P(A)\rightarrow B:A$

(2)$B\rightarrow P(A):N_b$

(1′)$B\rightarrow P(C):B$

(2′)$P(C)\rightarrow B:\{A,N_b\}$

(3′)$B\rightarrow P(C):\{A,N_b\}_{Kbs}$

(3)$P(A)\rightarrow B:X$

(4)$B\rightarrow P(S):A,X$

(5)$P(S)\rightarrow B:\{A,N_b\}_{Kbs}$

所谓角色非对称性,是指扮演不同角色的两个协议主体应生成不同形式的转换项[5]。在攻击 3 中,入侵者利用 B 和 S 可以在不同协议回合中生成相同消息项$\{A,N_b\}_{Kbs}$的漏洞,对 V1 进行多回合重放攻击。

2 多重认证测试方法

在 Woo-Lam 协议中,认证目标的实现围绕原子值 N_b 的形式转换进行。鉴于 N_b 发生了两次形式转换,应对其进行两次认证测试,以确定对转换负责的相关正则主体 A 和 S 的行为。为了对多次转换形式的关键原子值进行测试,本文引入了关键分量的概念,提出了多重认证测试方法,并通过对关键分量 N_b 进行两次认证测试,重新设计了 Woo-Lam 协议。

2.1 关键分量和多重认证测试方法

为便于介绍多重认证测试方法,首先引入关键分量的概念。

关键分量(Key Component):为实现主体认证或密钥分配目标而在协议主体间以不同形式传递的原子值。比如在 Woo-Lam 协议中的 N_b、在 Otway-Rees 协议中的 N_a 和 N_b 等,应围绕此类分量建立并进行认证测试。

在认证测试方法和关键分量概念的基础上,提出了多重认证测试方法。

多重认证测试(Multiple Authentication Test):分析关键分量在协议目标实现过程中需要发生的形式转换次数,然后以此为依据对关键分量进行相应次数的认证测试。

2.2 使用多重认证测试方法重新设计 Woo-Lam 协议

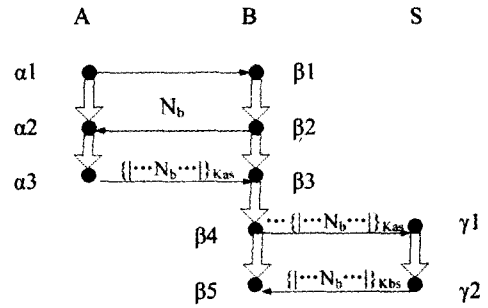

图 2 N_b 的形式转换流程

例 2 如图 2 所示,原子值 N_b 发生的两次形式转换是协议目标实现的关键:A 在边 $\alpha 2\Rightarrow\alpha 3$ 上对 N_b 进行形式转换,将其嵌入到 A 的加密分量$\{|\cdots N_b\cdots|\}_{Kas}$中;$S$ 在边 $\gamma 1\Rightarrow\gamma 2$ 上对 N_b 进行形式转换,将其从$\{|\cdots N_b\cdots|\}_{Kas}$中取出并嵌入到 S 的加密分量$\{|\cdots N_b\cdots|\}_{Kbs}$中。

虽然例 1 以 $\beta 2\Rightarrow^{+}\beta 5$ 为 N_b 在$\{|\cdots N_b\cdots|\}_{Kbs}$中的入测试,确定了唯一的正则转换边 $\gamma 1\Rightarrow\gamma 2$,但是未考虑 N_b 在 $\alpha 2\Rightarrow\alpha 3$ 上的形式转换,没有为其确定唯一的正则转换边 $\alpha 2\Rightarrow\alpha 3$,使"(3)$A\rightarrow B:\{N_b\}_{Kas}$"中缺少必要的主体标识,导致协议 V1 仍存在缺陷。

下面使用多重认证测试方法重新设计 Woo-Lam 协议。首先，与例 1 相同，得到 B 的迹如下：

$-\langle\{|A|\}\rangle\Rightarrow+\langle\{|N_b|\}\rangle\Rightarrow-\langle\cdots\{|\cdots N_b\cdots|\}_{Kas}\rangle\Rightarrow+\langle\cdots\{|\cdots N_b\cdots|\}_{Kas}\rangle\Rightarrow-\langle\{|\cdots N_b\cdots|\}_{Kbs}\rangle$

然后，针对 N_b 在协议中发生两次形式转换，相应地对其进行两次认证测试：

Test1：$\beta2\Rightarrow^{+}\beta3$ 是对于 N_b 在 $\{|\cdots N_b\cdots|\}_{Kas}$ 中的入测试，以 $N_b\Rightarrow\{|\cdots N_b\cdots|\}_{Kas}$ 为相应的转换边；

Test2：$\beta2\Rightarrow^{+}\beta5$ 是对于 N_b 在 $\{|\cdots N_b\cdots|\}_{Kbs}$ 中的入测试，以 $\cdots\{|\cdots N_b\cdots|\}_{Kas}\Rightarrow\{|\cdots N_b\cdots|\}_{Kbs}$ 为相应的转换边。

为确定唯一的正则转换边：

在 Test1 中，发起者串 $\{|\cdots N_b\cdots|\}_{Kas}$ 应为 $\{|B,N_b|\}_{Kas}$；

在 Test2 中，服务器串 $\{|\cdots N_b\cdots|\}_{Kbs}$ 应为 $\{|A,N_b|\}_{Kbs}$。

改进后的 Woo-Lam 协议 V2 如下：

(1)$A\rightarrow B:A$

(2)$B\rightarrow A:N_b$

(3)$A\rightarrow B:\{B,N_b\}_{Kas}$

(4)$B\rightarrow S:A,\{B,N_b\}_{Kas}$

(5)$S\rightarrow B:\{A,N_b\}_{Kbs}$

2.3 对协议 V2 认证性的证明

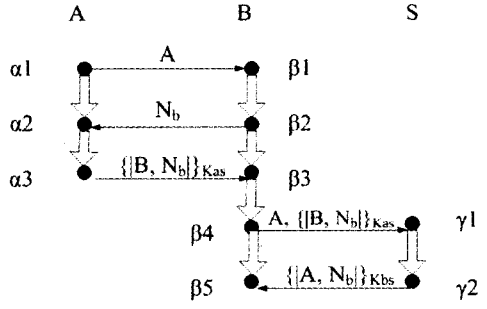

图 3 协议 V2 的丛示意图

如图 3 所示，多重认证测试方法通过两个“挑战-响应”回合实现协议的认证目标：通过 N_b 在 $\{|\cdots N_b\cdots|\}_{Kas}$ 中的入测试 Test1，保证对称环境下主体角色的非对称性；通过 N_b 在 $\{|\cdots N_b\cdots|\}_{Kbs}$ 中的入测试 Test2，保证响应者 B 对发起者 A 的身份认证。因此，为证明协议 V2 实现了认证性目标，需要证明这两次保证的实现。

(1)证明对主体的角色非对称性保证

在协议 V1 中，若 B 在某个回合 x 中扮演发起者，且在另一个回合 y 中扮演响应者，则回合 x 中的 B 可以和回合 y 中的 S 生成相同的消息项 $\{A,N_b\}_{Kbs}$，导致 V1 受到重放攻击。$\beta2\Rightarrow^{+}\beta3$ 上的“挑战-响应”回合，通过对发起者的身份认证，消除了这个漏洞，保证了对称环境下主体角色的非对称性。

假设：C 是协议 V2 串空间 Σ 中的一个丛，C 包含一个响应者串 $\beta\in\mathrm{Resp}[A,B,S,N_b]$，C-height($\beta$)=3，其中 $K_{as}\notin K_p$，$A,B,S\in T_{name}$，$N_b\in T$，$N_b\notin T_{name}$ 且 N_b 是唯一起源的。

需要证明：C 必定包含一个发起者串 $\alpha\in\mathrm{Init}[A,B,S,N_b]$，且 C-height($\alpha$)为 3。

证明：由于 $K_{as}\notin K_p$，N_b 唯一起源于 $\beta2$，$\beta2\Rightarrow^{+}\beta3$ 是 N_b 的被转换边，且 $\{|B,N_b|\}_{Kas}$ 是 N_b 在 $\beta3$ 中的测试分量，因此 $\beta2\Rightarrow^{+}\beta3$ 构成 N_b 在 $\{|B,N_b|\}_{Kas}$ 中的入测试；

根据认证测试定理，存在正则结点 $m,m'\in C$，使 $\{|B,N_b|\}_{Kas}$ 是 m' 的分量，且 $m\Rightarrow+m'$ 是对于 N_b 的转换边；

由于 m' 是一个正的正则结点，且 $\{|B,N_b|\}_{Kas}=\mathrm{term}(m')$，因此 m' 是某个发起者串 $\alpha\in\mathrm{Init}[A',B',S',N'_b]$ 上的 $\alpha3$；既然 $\mathrm{term}(\alpha3)=\{|B,N_b|\}_{Kas}$，因此 $A'=A,B'=B,S'=S,N'_b=N_b$；由此可知，丛 C 包含一个发起者串 $\alpha\in\mathrm{Init}[A,B,S,N_b]$；

由于 $\alpha2\Rightarrow^{-}\alpha3$ 是 N_b 在 C 中的转换边，因此 C-height(α)为 3。

(2)证明响应者 B 对发起者 A 的身份认证

假设：C 是协议 V2 串空间 Σ 中的一个丛，C 包含一个响应者串 $\beta\in\mathrm{Resp}[A,B,S,N_b]$，C-height($\beta$)=2，其中 $K_{bs}\notin K_p$，$A,B,S\in T_{name}$，$N_b\in T$，$N_b\notin T_{name}$ 且 N_b 是唯一起源的。

需要证明：C 必定包含一个服务器串 $\gamma\in\mathrm{Serv}[A,B,S,N_b]$，且 C-height($\gamma$)为 2。

证明过程与(1)类似，在此不加赘述。

2.4 结果分析

由于在(3)和(5)中分别实现了对主体 B 和 A 的身份确认，协议 V2 可以避免原 Woo-Lam 协议中的两个重放攻击和协议 V1 中的一个重放攻击：针对攻击 1，在 V2 的(3′)中，B 向 $P(C)$ 发送“$\{C,P,\{N_b\}_{Kps}\}_{Kbs}$”，使攻击者无法在(4′)中继续执行重放攻击；针对攻击 2，在 V2 的(5)中，S 返回“$\{P,N_b\}_{Kbs}$”，使 B 判断出 N_b 来自协议的另一个回合，从而对 P(而非攻击者希望的 A)进行认证；针对攻击 3，在 V2 的(3′)中，B 向 $P(C)$ 发送“$\{C,A,N_b\}_{Kbs}$”，使攻击者无法得到在(5)中执行重放攻击所必需的“$\{A,N_b\}_{Kbs}$”。

3 多重认证测试方法与其它方法的比较

与非形式化设计原则和 BSW 逻辑相比，多重认证测试方法更加有效。以 Woo-Lam 协议为例，使用多重认证测试方法设计出的新协议避免了 Abadi 和 Buttyan 等人分别对原协议改进后存在的两个重放攻击。

3.1 与非形式化设计原则的比较

在文[8]中，Abadi 等人从显式性的角度分析了 Woo-Lam 协议的缺陷，认为协议消息之间缺乏充分的联系，给出了改进协议 V3：

(1)$A\rightarrow B:A$

(2)$B\rightarrow A:N_b$

(3)$A\rightarrow B:\{N_b\}_{Kas}$

(4)$B\rightarrow S:A,B,\{N_b\}_{Kas}$

(5)$S\rightarrow B:\{A,N_b\}_{Kbs}$

协议 V3 避免了原 Woo-Lam 协议中的两个重放攻击，但是存在另一个重放攻击[6]：

攻击 4：

(1)$P(A)\rightarrow B:A$

(2)$B\rightarrow P(A):N_b$

(1′)$B\rightarrow P(C):B$

(2′)$P(C)\rightarrow B:\{A,N_b\}$

(3′)$B\rightarrow P(C):\{A,N_b\}_{Kbs}$

(3)$P(A)\rightarrow B:X$

(4)$B\rightarrow P(S):A,X$

(5)$P(S)\rightarrow B:\{A,N_b\}_{Kbs}$

在使用多重认证测试方法设计的协议 V2 中，由于“(3)$A\rightarrow B:\{B,N_b\}_{Kas}$”消除了 B 和 S 可以在不同协议回合中生成相同消息项 $\{A,N_b\}_{Kbs}$ 的漏洞，故避免了攻击 4：B 在(3′)中向 P(C)发送“$\{C,A,N_b\}_{Kbs}$”，使攻击者无法得到在(5)中执行重放攻击所需的“$\{A,N_b\}_{Kbs}$”。

3.2 与 BSW 逻辑的比较

在文[9]中，Buttyan 等人使用 BSW 逻辑对 Woo-Lam 协

(下转第 123 页)

4 算法测试及结果

算法的测试数据采用DARPA入侵检测系统评测数据集中第四、第五周的原始数据，测试的结果与Snort port-scan检测结果进行对比(port-scan检测规则设为“如果在3秒内连接数大于6，则报警”)，结果见表1。

表1 性能比较

系统扫描检测算法	检测率	误报率	报警连接数
Scanning Attack Detection	97%	0.07%	870
Snort port-scan	63%	0.15%	11180

由表1可知，基于协议状态有限自动机的系统扫描检测算法与Snort port-scan相比，检测率高，误报率低，报警次数大大减少。这是因为采用基于协议状态有限自动机的系统扫描检测算法对报文序列的状态根据协议状态机进行了检查，能够检测出慢扫描和隐蔽扫描，从而提高了检测率，同时降低了误报率。考虑到实际使用中可只对系统开启的服务端口检测(对连接使用所提出的算法进行合法性检查，如果非法则判断为扫描，对合法的连接的频繁程度采用阈值判别法界定是否发生扫描行为)，对关闭的端口建立连接的企图都界定为扫描，但只报警一次，在测试中对报警进行了合并。因为对外提供服务端口默认为0～1024，测试对0～1024端口进行了检测并报警，同时考虑到有的系统会使用大于1024的端口提供服务，对大于1024的端口以port mod 1024进行检测并报警合并，所以输出的报警数也大为减少。

总结 本文分析了现有检测算法的缺陷，针对现有扫描检测算法对隐蔽扫描、慢扫描无法识别的不足，提出了基于协议状态有限机的检测算法，算法通过对报文序列的状态在协议状态有限机中前后关系进行检查来识别连接的合法性，然后检查非法连接和端口的访问频率(采用现有的阈值判别法)来识别系统扫描。实验测试表明该算法能明显提高系统扫描检测性能，降低误报率和报警次数。

参 考 文 献

1 http://www.snort.org/;

2 Lee W, Nimbalkar R A, Yee K K. A data mining and CIDF based approach for detecting novel and distributed intrusions. In: Proceedings of the Third International Workshop on Recent Advances in Intrusion Detection (RAID 200), Toulouse, France, Oct. 2000

3 Basu R, Cunninghuam R K, Webster S E, et al. Detecting Low-Profile Probes and Novel Denial-of-Service Attacks. In: Proceedings of the 2001 IEEE workshop on information assurance and security, June 2001

4 Porras P A, Neumann P G, Merald E. Event monitoring enabling responses to anomalous live disturbances. In: National Information Systems Security Conference, Baltimore MD, October 1997

5 Stamford S, Hoagland J, Mcalerney J. Practical Automated. Detection of Stealthy Port scans. ACM CCS IDS, Workshop, Athens, Greece, 2000

(上接第105页)

议进行了分析，认为在该协议的最后一则消息中，不能保证A发送过现时值N_b。他们给出了改进协议V4：

(1)$A\rightarrow B:A$

(2)$B\rightarrow A:B,N_b$

(3)$A\rightarrow B:\{B,N_b\}_{Kas}$

(4)$B\rightarrow S:A,\{B,N_b\}_{Kas}$

(5)$S\rightarrow B:\{A,B,N_b\}_{Kbs}$

协议V4避免了原Woo-Lam协议中的两个重放攻击，但是本文发现，该协议中存在另一个重放攻击：

攻击5：

(1)$P(A)\rightarrow B:A$

(2)$B\rightarrow P(A):B,N_b$

(1′)$B\rightarrow P(C):B$

(2′)$P(C)\rightarrow B:A,B,N_b$

(3′)$B\rightarrow P(C):\{A,B,N_b\}_{Kbs}$

(3)$P(A)\rightarrow B:X$

(4)$B\rightarrow P(S):A,X$

(5)$P(S)\rightarrow B:\{A,B,N_b\}_{Kbs}$

在协议V2中，“(3)A→B:$\{B,N_b\}_{Kas}$”消除了B和S可以在不同协议回合中生成相同消息项$\{A,B,N_b\}_{Kbs}$的漏洞，故避免了上述攻击：B在(3′)中向P(C)发送“$\{C,A,B,N_b\}_{Kbs}$”，使攻击者无法得到在(5)中执行重放攻击所需的“$\{A,B,N_b\}_{Kbs}$”。

小结 Abadi和Buttyan等人分别使用非形式化设计原则和BSW逻辑对Woo-Lam协议进行了改进，但是得到的两个新协议V3和V4中仍存在缺陷：V3的“(3)A→B:$\{N_b\}_{Kas}$”中缺少对主体B进行身份确认的标识；V4中，过多的主体标识不仅不能为协议带来更高的安全性保证，反而导致协议受到新的攻击。而使用多重认证测试方法设计出的协议V2，避免了上述缺陷，可以抵抗Abadi和Buttyan等人分别对原协议改进后存在的两个重放攻击。

参 考 文 献

1 Guttman J D, F'abrega F J T. Authentication tests[C]. In: Proceedings of the 2000 IEEE Symposium on Security and Privacy, Los Alamitos, 2000. 96～109

2 Guttman J D, F'abrega F J T. Authentication tests and the structure of bundles[J]. Theoretical Computer Science, 2002, 283(2): 333～380

3 Guttman J D. Security protocol design via authentication tests [C]. In: Proceedings of the 2002 IEEE Computer Security Foundations Workshop, Los Alamitos, 2002. 92～103

4 Perrig A, Song D X. Looking for diamonds in the desert-extending automatic protocol generation to three-party authentication and key agreement[C]. In: Proceedings of the 2000 IEEE Computer Security Foundations Workshop, Los Alamitos, 2000. 64～76

5 Choi Hyun-Jin. Security protocol design by composition [D]. Cambridge, United Kingdom: University of Cambridge, 2006

6 Debbabi M, Mejri M, Tawbi N, et al. A new algorithm for the automatic verification of authentication protocols: From specifications to flaws and attack scenarios[C]. In: DIMACS Workshop on Design and Formal Verifictaion of Security Protocols, 1997

7 Clark J, Jacob J. A survey of authentication protocol literature: Version 1.0[EB/OL]. http://www-users.cs.york.ac.uk/～jac/ under the link \Security Protocols Review, 1997

8 Abadi M, Needham R. Prudent Engineering Practice for Cryptographic Protocols[C]. In: Proceedings of the 1994 IEEE Computer Society Symposium on Security and Privacy, Los Alamitos, 1994. 122～136

9 Buttyan L, Staamann S, Wilhelm U. A simple logic for authentication protocol design[C]. In: Proceedings of the 1998 IEEE Computer Security Foundations Workshop, Los Alamitos, 1998. 153～162