# 对一种身份认证协议的改进及其形式化分析①

何 丽 王立斌 (华南师范大学 计算机学院 广东 广州 510631)

**摘 要:** 基于口令的远程身份认证协议是目前认证协议研究的热点。2005 年，Sung-Woon Lee 等人提出了一个低开销的基于随机数的远程身份认证协议即 Lee-Kim-Yoo 协议，首先分析了此协议中所存在的安全性缺陷，随后构造了一个基于随机数和 Hash 函数，并使用智能卡的远程身份认证协议，最后用 BAN 逻辑对修改后的协议进行了形式化的分析，结果表明修改后的协议能够达到协议的安全目标。

**关键词:** 认证协议;拒绝服务攻击;BAN 逻辑;形式化分析

## Formal Verification and Improvement of an Authentication Protocol

HE Li, WANG Li-Bin (Dept. of Computer Science, South China Normal University, Guangzhou 510631, China)

**Abstract:** Password-based remote user authentication is a hotspot in authentication protocol research. The security of a proposed remote user authentication scheme, the Lee-Kim-Yoo protocol, advanced by Sung-Woon Lee is analyzed, which used nonce random and had very low computational costs. However, this scheme still has many security faults. The weakness of the scheme is demonstrated. This paper proposes an improved scheme, a novel nonce and hash-based remote user authentication scheme using smart cards and analyses the amended protocol with BAN logic. It indicates that the amended protocol can reach the goal of the protocol.

**Keywords:** authentication protocol; Dos attack; BAN logic; formal verification

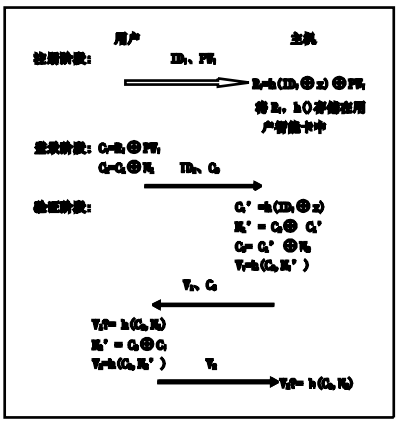
## 1 引言

基于口令的认证机制因其简单有效、易于使用，在分布式环境下被广泛用于身份合法性验证，从而决定是否提供资源的使用授权。但是用户在选择口令的时候，一般都是选择便于自己记忆的口令，这样就会很容易遭到字典攻击。为此许多研究人员从增加安全性和提高效率两方面入手，提出了一系列的协议。大致可以归纳为两类：基于安全 Hash 函数的认证协议以及基于公钥体制的认证协议。前者由于具备开销小、效率高，并结合智能卡自身的安全性与便携性成为近年来研究的热点。

本文主要是对 Sung-Woon Lee 等人所提出的 Lee-Kim-Yoo 协议[1]进行改进，并用 BAN(Burrows,Abadi,Needham)逻辑[2-4]对改进后的协议进行了分析，说明改进后的协议能够完成协议要达到的目标。

## 2 Lee-Kim-Yoo协议

在下面的分析中，全文作如下约定：A 表示合法用户；S 表示系统；E 表示攻击者；$N_*$ →表示随机数；表示不安全信道；⇒ 表示安全信道。Lee-Kim-Yoo 认证协议包括 3 个阶段：注册阶段、登陆阶段、认证阶段。整个过程如下：




① 收稿时间:2009-11-05;收到修改稿时间:2009-12-30

从上述认证过程中不难发现,虽然Lee-Kim-Yoo认证协议能比较有效地完成双边认证，但在用户登录阶段，若攻击者 E 截获消息(IDi、C2)并向远程系统大量发送此消息，由于 IDi 的合法性，使得攻击者 E 可以通过系统检验，以至于远程系统忙于完成后面的计算，从而形成对远程系统的拒绝服务攻击(Dos)。

## 3 改进后的协议

### 3.1 注册阶段

用户 A 通过安全通道向远程系统 S 提交身份 IDi 和密码 PWi，服务器收到该信息后计算：Ri=h(EIDi ⊕x) ⊕PWi,其中 x 是服务器端足够长的密钥，由服务器为所有用户安全保存，EIDi=(IDi ||i)，其中 i 初始值为 1。并将 Ri,h()记入用户的智能卡中。注册完成后，用户智能卡及远程系统保留的信息如下表所示：

| 智能卡 | 系统 |
|---|---|
| $R_1$ | $ID_i$ |
| $ID_1$ | I |
| n=1 | n=② |
| H（） | |

### 3.2 登录认证阶段

(a)用户将智能卡插入读写器，输入自己的用户名($ID_i$)和密码($PW_i$),该设备首先检查用户输入的 $ID_i$ 是否与其保存的 IDi 一致，如果不同则报告错误并停止，否则则开始计算：$y=R_i \oplus PW_i$；$C_1=h(y \oplus n)$;$C_2=y \oplus N_1$，并将 $ID_i$、n、$C_1$、$C_2$ 发送给远程系统，其中 $N_1$ 为随机数。

(b)远程系统在接受到用户发送的消息后，首先检查发送过来的 n 值是否与远程系统保存的 n 值一致，然后计算 $y'=h(EID_i \oplus x)$；$C_1'=h(y' \oplus n)$，比较 $C_1'$ 与收到的 $C_1$ 比较，如果不相等则系统将会放弃后续操作并发送给用户一个出错信息并记录此次认证的结果。否则说明用户是合法用户并通过认证，并计算 $N_1'=y' \oplus C_2$；$V_1=h(C_2,N')$,并将 $V_1$ 发送给用户，同时将 n 值替换成 n+1。

(c)用户接收到远程系统发送的信息后，计算 $V1'=h(C_2,N_1)$,比较 $V_1'$ 与 $V_1$ 是否一致，如果相同则远程系统通过认证，并且将 n 值替换成 n+1。

### 3.3 协议的补充说明

(a)由于 y 值是双方认证过程时依据的一个重要秘密信息，如果被泄露，必须重新设定其值，但是为了保证用户的 ID 和远程系统的 x 不变，所以只需将 i 的值调整为 i+1 即可保证 y 值的改变。

(b)引入 n 值的目的就是抵抗原协议中存在的 Dos 攻击。关键是确保认证双发的同步性。

## 4 基于BAN逻辑的安全协议分析

BAN 逻辑是一种基于信念的模态逻辑[6]，在 BAN 逻辑的推理过程中，参加协议的主体的信念随消息交换的发展而不断变化和发展，本文采用 BAN 逻辑对改进后的协议进行形式化分析，以证明其可达到协议的安全性要求。注：以下所用到的 BAN 逻辑推理规则标识符(如 R1, R2……)均与参考文献[4]一致。

### 4.1 协议理想化模型

M1: $A \rightarrow S: ID_i, PW_i$ from S

M2: $S \rightarrow A: R_i$, h() from A

M3: $A \rightarrow S: ID_i$, n, $C_1$, C2 from A

M4: $S \rightarrow A: V_1$ from S

### 4.2 协议安全性要求

G1: $S|\{$if $h(y \oplus n)=h(y' \oplus n)$ then $S| \equiv h(yn)\}$

G2: $A|\{$if $h(C^2,N_1')=h(C_2,N_1)$ then $A| \equiv h(C2,N1')\}$

### 4.3 协议运行的初始条件

(A1) $A| \equiv \#(N_1)$

(A2) $S| \equiv \#(n)$

(A3) $S| \equiv A|\{ID_i, n, h(y \oplus n), C2\}$

(A4) $A| \equiv S|\{h(C_2,N1')\}$

(A5) $S| \equiv Ah(y \oplus n)$

(A6) $A| \equiv Sh(C_2,N_1')$

### 4.4 协议分析过程

由初始条件(A2)和消息新鲜性规则 R11 得：

$S| \equiv \#\{ID_i, n, h(y \oplus n), C2\}$ (1)

由式(1)、(A3)和随机数验证规则 R4 得：

$S| \equiv A| \equiv \{ID_i, n, h(y \oplus n), C_2\}$ (2)

由式(2)和信念规则 R14 得：

$S| \equiv A|\{h(y \equiv n)\}$ (3)

由式(3)、A5 和管辖规则 R5 得：

$S \equiv |\{h(y \oplus n)\}$ (4)

证明协议满足安全要求 G1。

因为 $N_1' = y' \oplus C_2$、$C_2 = y \oplus N_1$、(A1)和消息新鲜性规则 R11 得:

$$A| \equiv \#(N_1') \quad (5)$$

由式(5)和消息新鲜性规则 R11 得:

$$A| \equiv \#\{h(C_2, N_1')\} \quad (6)$$

由式(6)、(A4)和随机数验证规则 R4 得:

$$A| \equiv S \equiv |\{h(C_2, N_1')\} \quad (7)$$

由式(7)、(A6)和管辖规则 R5 得:

$$A| \equiv h(C_2, N_1') \quad (8)$$

证明协议满足安全要求 G2。

根据协议模型和初始假设推理可知，用户和远程系统相互相信对方拥有和自己相同的哈希值。

## 5 结语

本文首先给出了由 Sung-Woon Lee 等人提出的 Lee-Kim-Yoo 协议，并针对其中存在的 Dos 攻击进行改进，并运用 BAN 逻辑对改进后的协议作了形式化分析。结果表明，改进后的协议能够完成该协议要达到的目标。

**参考文献:**

1 Lee SW, Kmhs, Yoo K Y. Efficient nonce-based remote user authentication scheme using smart cards. Applied Mathematics and Computation, 2005, 167 (1): 335－361.

2 Burrows M， Abadi M, Needham R. A logic of authentication. ACM Transactions on Computer Systems, 1990,8(1):18－36.

3 缪祥华,何大可. Needham-Schroeder 私钥协议的改进.计算机工程, 2006,32(17):32－34.

4 王贵林,卿斯汉,周展飞.Needham-Schroeder 协议的形式化分析.软件学报, 2002,13.

5 张利华,章丽萍,张有光等.基于口令的远程身份认证及密钥协商协议.计算机应用, 2009,29(4):924－927.

6 冯登国.可证明安全性理论与方法研究.软件学报, 2005,16(10):1743－1756.