基于令牌的单点登录协议及其形式化分析

申 婷，李 晖，于明喆
(西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071)

摘要：提出一种新的适用于分布式网络的单点登录协议，利用令牌将身份认证和服务授权结合起来由一个验证服务器实现，授权校验的同时进行密钥分配，实现了用户和应用服务器的双向认证. 令牌使用户只需在登录网络时进行一次身份认证即可接入各应用服务器，从而提高了网络认证效率，同时使验证服务器不需要保存用户的状态，有效提高验证服务器的性能. 采用 BAN 逻辑对该协议进行形式化分析表明，协议达到了认证和密钥分配的目标，具有较强的安全性.

关键词：单点登录；令牌；BAN 逻辑
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1001-2400(2006)05-0792-05

Token-based single sign-on protocol and its formal analysis

SHEN Ting, *LI Hui*, *YU Ming-zhe*
(Ministry of Edu. Key Lab. of Computer Network and Information Security,
Xidian Univ., Xi'an 710071, China)

Abstract: A new single sign-on protocol used for the distributed network is proposed to achieve double-way authentication between user application servers. With a service token, identity authentication and service authorization are implemented by an authentication server, and the key is saved in the token which can be used in the verification process. The token not only makes the user that has been authenticated when it enters the network communicate with any application server, and improves the authentication efficiency of the whole network, but also makes the authentication server unnecessarily save the sate of users, and promotes authentication server's performance. Using the BNA logic, the objective and the security of this protocol are proved by the formal analytical process.

Key Words: single sign-on; token; BAN logic

在分布式网络环境中，认证对于防止恶意攻击，保护合法用户的权益有极其重要的作用. 认证包括两层含义：其一是身份认证，即确认网络中各通信主体身份的真实性；其二是信息完整性认证，即确认信息在传输和存储过程中未被篡改、重放等. 以上两个方面是一个安全认证系统所必须解决的问题.

基于用户名、口令的分散认证机制使用户在进入不同系统时，必须分别提交独立的身份标识来证明身份. 大量的用户名和口令不便于记忆，为此用户往往采用简单信息作为口令或设置相同的口令，带来巨大的安全隐患；对于管理者而言，需要创建多个用户数据库，管理繁琐. 笔者考虑使用公钥证书作为通信主体的身份标识，采用单点登录[1](SSO)机制来设计一个安全认证系统，使用户只需在网络中主动进行一次身份认证，便可访问其被授权的所有网络资源，从而简化网络认证过程，提高认证的安全性和认证效率.

1 基于令牌的单点登录系统

Kerberos[2]系统是常用的单点登录系统，用户在 Kerberos 系统中必须反复向票据发放服务器(TGS)申

收稿日期：2005-12-01
基金项目：国家自然科学基金资助项目(60173056)
作者简介：申 婷(1981-)，女，西安电子科技大学硕士研究生.

请用于接入不同应用服务器的授权票据. 若改由一个验证服务器来实现身份认证和服务授权,采用由验证服务器生成并由其自行校验的服务令牌来替代票据,这样,一个用户只需拥有一个服务令牌便可访问系统中的所有应用服务器. 图 1 表明该单点登录系统的体系结构.

客户接入系统:由用户和代理服务器构成. 代理服务器在认证过程中只起到"透传"的作用,对用户的认证工作在验证服务器上完成.

验证服务器:完成身份认证和服务授权两大功能. 先对用户进行身份认证,之后给通过身份认证的用户发放服务令牌,用户凭借此令牌访问任一应用服务器. 验证服务器生成用户与其共享的会话密钥并保存在令牌上,从而减轻验证服务器维护用户认证状态的负担.

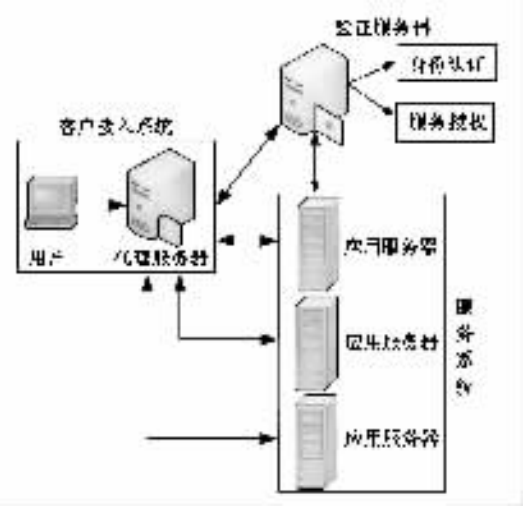

图 1　系统体系结构

应用服务系统:由若干应用服务器组成. 当应用服务器收到用户的服务请求时,将用户的服务令牌送回验证服务器验证. 若验证通过,证明用户为合法用户,验证服务器生成用户和应用服务器的会话密钥. 凭借此会话密钥,应用服务器提供给用户所要求的服务.

2　认证目标和安全性要求

(1) 验证服务器对用户身份进行集中式认证,并且通过验证服务器实现用户和应用服务器的双向认证.

(2) 密钥分配. 在用户和应用服务器之间建立一个共享的会话密钥并且保证会话密钥的机密性. 验证服务器作为可信任的第三方为用户和应用服务器生成会话密钥,传送时分别采用验证服务器和用户的共享密钥、应用服务器的公钥加密来传送给用户和应用服务器[3].

(3) 信息完整性认证. 为防止重放攻击,一是使用一次性随机数代替时戳,同时避免了 Kerberos 中的时钟同步问题;二是在签名消息中加入收方的身份信息,防止收方重放消息[4]. 采用先签名后加密的方法,由于攻击者不知道收方的私钥,不能看到消息内容更不能进行篡改,保证信息完整性.

协议在设计上还必须满足两点安全性要求:信息的机密性和发方的不可否认性.

3　模型和协议描述

基于令牌的单点登录系统的抽象模型如图 2,协议所使用的符号定义如下:

cert_c, cert_a, cert_s:用户、验证服务器、应用服务器的公钥证书;

K_{ca}, K_{ca}^{-1}:证书授权机构的公钥和私钥;K_c, K_c^{-1}:用户的公钥和私钥;K_s, K_s^{-1}:应用服务器的公钥和私钥;K_a, K_a^{-1}:验证服务器的公钥和私钥;

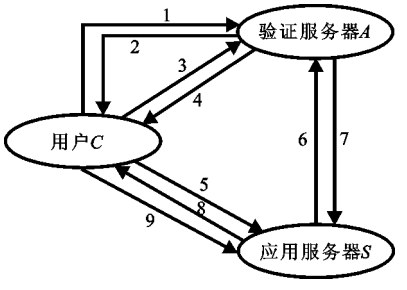

图 2　抽象模型

K:验证服务器的对称密钥;K_{rand}:随机的一次性对称密钥;

$K_{c,s}$:用户和应用服务器的会话密钥;$K_{c,a}$:用户和验证服务器的会话密钥;

Token_c:验证服务器授予用户的服务令牌;$\{M\}_k$:用密钥 K 加密消息 M;

N_c, N_c':用户生成的一次性随机数;N_s, N_s':应用服务器生成的一次性随机数;N_a:验证服务器生成的一次性随机数;

T_a:验证服务器生成的时戳;lifetime:Token_c 的生存期;

$\{M\}_{S_A}$:用 A 的私钥对 M 的数字签名;$\{M\}_{S_C}$:用 C 的私钥对 M 的数字签名;$\{M\}_{S_S}$:用 S 的私钥对 M 的数字签名.

协议流程:

(1) 登录过程. 用户与验证服务器进行相互认证,获得服务令牌.

$M_1: C \rightarrow A: C.$

$M_2: A \rightarrow C: \mathrm{cert}_a, \{N_a, C\}_{S_A}.$

$M_3: C \rightarrow A: A, \{\mathrm{cert}_c, \{N_a+1, N_c, K_{\mathrm{rount}}, A, C\}_{S_C}\}_{K_a}.$

$M_4: A \rightarrow C: \mathrm{Token}_c, \{N_c+1, A, C, K_{c,a}\}_{K_{\mathrm{rand}}}, \mathrm{Token}_c = \{A, C, K_{c,a}, T_a, \mathrm{lifetime}\}_K.$

具体来说,M_1:用户 C 向验证服务器 A 发出认证请求,请求 A 的公钥证书. M_2:验证服务器 A 向用户 C 提供其公钥证书并用其私钥签名挑战信息. C 校验 A 的公钥证书是否已由 CA 或 CA 链签名以及证书是否在其生存期内,这可通过检测周期性更新的证书撤销列表 CRL 或直接向 CA 查询实现. 数字签名可确认消息的发送者是 A,防止攻击者窃取 cert_a 进行假冒攻击. M_3:用户 C 向验证服务器 A 请求服务令牌. 消息先使用 C 的私钥数字签名,再使用 A 的公钥加密[5]. 因此只有 A 才能查看消息并且数字签名认证了 C 的身份. 协议通过挑战响应的方式防止重放攻击,数据域 N_a+1 是对 N_a 的响应,N_c 是 C 对 A 发出的挑战. K_{rand} 是 C 产生的随机的一次性密钥,它将被 A 使用以加密发给 C 的响应消息. 数据域 N_c 用于防止重放攻击[4]. M_4:验证服务器 A 认证用户 C 的身份后,生成其与 C 的会话密钥 $K_{c,a}$,并向 C 提供服务令牌. $K_{c,a}$ 包含在令牌中由用户保存,而验证服务器不保存. 响应消息中加入 A, C 的身份防止攻击[5]. 服务令牌使用仅由 A 知道的对称密钥 K 加密,防止 C 重建令牌. 其中 T_a 用于防止重放攻击. 因为 Token_c 由 A 自行校验,A 将根据自己的时钟校验自己产生的时间戳,故不需要与 C, S 的时钟保持同步.

(2) 授权校验过程. 验证用户的服务令牌,以获得与应用服务器联机的服务.

$M_5: C \rightarrow S: \mathrm{Token}_c, C, N_c'.$

$M_6: S \rightarrow A: \mathrm{cert}_s, \{\mathrm{Token}_c, N_c', S, C, N_s\}_{S_s}.$

$M_7: A \rightarrow S: S, \{\mathrm{cert}_a, \{\{N_c'-1, C, S, K_{c,s}\}_{K_{c,a}}, C, S, N_s+1, K_{c,s}\}_{S_A}\}_{K_s}.$

具体来说,M_5:用户向应用服务器发出服务请求. M_6:应用服务器将用户的服务令牌送回验证服务器校验. 若验证通过,协议转入 M_7;若不通过,协议中止. M_7:验证服务器生成并发放 C, S 的会话密钥 $K_{c,s}$. 消息中的数据域 $N_c'-1, C, S, K_{c,s}$ 采用 C, A 的共享密钥加密,只能由 C 解读,通过 S 转发给 C. 数据域 C, S 表明密钥拥有者,保证密钥真实性[6]. 整条消息采用先签名后加密的方式,保证发方的不可否认性并且防止收方假冒.

(3) 对应用服务器的认证过程.

$M_8: S \rightarrow C: \{N_c'-1, C, S, K_{c,s}\}_{K_{c,a}}, \{N_c'+1, S, C, N_s'\}_{K_{c,s}}.$

$M_9 \rightarrow C^S: \{N'_s+1\}_{K_{c,s}}.$

具体来说,M_8:数据域 $N_c'+1, S, C, N_s'$ 采用 $K_{c,s}$ 加密作为信任状(authenticator)与 S 转发的验证服务器发给用户的消息互相印证来证明应用服务器的身份. M_9:用户对应用服务器的认证响应.

4 形式化分析

基于知识和信仰的 BAN 逻辑[7]是一种已被广泛用于分析安全协议的形式逻辑分析方法. 虽然 BAN 逻辑本身存在缺陷[8],但它简单、易用、直观,适用于分析身份认证和密钥分配协议,故采用 BAN 逻辑对该协议进行形式化分析.

4.1 BAN 逻辑下的认证目标

采用 BAN 逻辑分析该协议要达到的认证目标:$C \mid\equiv C \overset{K_{c,s}}{\longleftrightarrow} S, S \mid\equiv C \overset{K_{c,s}}{\longleftrightarrow} S, C \mid\equiv S \mid\equiv C \overset{K_{c,s}}{\longleftrightarrow} S, S \mid\equiv C \mid\equiv C \overset{K_{c,s}}{\longleftrightarrow} S$,即 C 和 S 都相信 $K_{c,s}$ 是 C 和 S 之间通信的好密钥,且 C 和 S 都相信对方也相信 $K_{c,s}$ 是 C 和 S 之间通信的好密钥.

4.2 协议理想化

由于 M_1, M_5 对协议的逻辑性没有贡献,在协议理想化过程中将其省略.

$M_2: A \rightarrow C: \{\overset{K_a}{\vdash\!\!\rightarrow} A\}_{K_{ca}^{-1}}, \{N_a\}_{K_a^{-1}}$. $M_3: C \rightarrow A: \{\{\overset{K_c}{\vdash\!\!\rightarrow} C\}_{K_{ca}^{-1}}\}, \{N_a, N_c, A \overset{K_{rand}}{\longleftrightarrow} C\}_{K_c^{-1}}\}_{K_a}$.

$M_4: A \rightarrow C: \text{Token}_c, \{N_c, A \overset{K_{c,a}}{\longleftrightarrow} C\}_{K_{rand}}$. $M_6: S \rightarrow A: \{\overset{K_s}{\vdash\!\!\rightarrow} S\}_{K_{ca}^{-1}}, \{\text{Token}_c, N_c', N_s\}_{K_s^{-1}}$.

$M_7: A \rightarrow S: \{\{\overset{K_a}{\vdash\!\!\rightarrow} A\}_{K_{ca}^{-1}}, \{N_s, C \overset{K_{c,s}}{\longleftrightarrow} S, \{N_c', C \overset{K_{c,s}}{\longleftrightarrow} S\}_{K_{c,a}}\}_{K_a^{-1}}\}_{K_s}$.

$M_8: S \rightarrow C: \{N_c', C \overset{K_{c,s}}{\longleftrightarrow} S\}_{K_{c,a}}, \{N_c', N_s', C \overset{K_{c,s}}{\longleftrightarrow} S\}_{K_{c,s}}$. $M_9: C \rightarrow S: \{N_s', C \overset{K_{c,s}}{\longleftrightarrow} S\}_{K_{c,s}}$.

4.3　初始假设

(1) $C \mid\equiv \overset{K_{ca}}{\vdash\!\!\rightarrow} CA$, (2) $A \mid\equiv \overset{K_{ca}}{\vdash\!\!\rightarrow} CA$, (3) $S \mid\equiv \overset{K_{ca}}{\vdash\!\!\rightarrow} CA$, (4) $C \mid\equiv CA \mid\Rightarrow \overset{K_a}{\vdash\!\!\rightarrow} A$,

(5) $A \mid\equiv CA \mid\Rightarrow \overset{K_c}{\vdash\!\!\rightarrow} C$, (6) $A \mid\equiv CA \mid\Rightarrow \overset{K_s}{\vdash\!\!\rightarrow} S$, (7) $S \mid\equiv CA \mid\Rightarrow \overset{K_a}{\vdash\!\!\rightarrow} A$,

(8) $C \mid\equiv C \overset{K_{rand}}{\longleftrightarrow} A$, (9) $A \mid\equiv \overset{K_a}{\vdash\!\!\rightarrow} A$, (10) $S \mid\equiv \overset{K_s}{\vdash\!\!\rightarrow} S$, (11) $A \mid\equiv C \mid\Rightarrow A \overset{K_{rand}}{\longleftrightarrow} C$,

(12) $C \mid\equiv A \mid\Rightarrow A \overset{K_{c,a}}{\longleftrightarrow} C$, (13) $S \mid\equiv A \mid\Rightarrow C \overset{K_{c,s}}{\longleftrightarrow} S$, (14) $C \mid\equiv A \mid\Rightarrow C \overset{K_{c,s}}{\longleftrightarrow} S$,

(15) $C \mid\equiv \#(\overset{K_a}{\vdash\!\!\rightarrow} A)$, (16) $A \mid\equiv \#(\overset{K_c}{\vdash\!\!\rightarrow} C)$, (17) $A \mid\equiv \#(\overset{K_s}{\vdash\!\!\rightarrow} S)$, (18) $S \mid\equiv \#(\overset{K_a}{\vdash\!\!\rightarrow} A)$,

(19) $A \mid\equiv \#(N_a)$, (20) $C \mid\equiv \#(N_c)$, (21) $S \mid\equiv \#(N_s)$, (22) $C \mid\equiv \#(N_c')$, (23) $S \mid\equiv \#(N_s')$.

4.4　逻辑推理

分析过程所用到的 BAN 逻辑推理规则[9]:

$R_1: \dfrac{A \mid\equiv A \overset{K}{\vdash\!\!\rightarrow} B,\ A \triangleleft \{X\}_K}{A \mid\equiv B \mid\sim X}$. $R_2: \dfrac{A \mid\equiv \overset{K}{\vdash\!\!\rightarrow} B,\ A \triangleleft \{X\}_{K^{-1}}}{A \mid\equiv B \mid\sim X}$(**消息含义规则**).

$R_3: \dfrac{A \mid\equiv \#(X),\ A \mid\equiv B \mid\sim X}{A \mid\equiv B \mid\equiv X}$(**一次随机数检验规则**). $R_4: \dfrac{A \mid\equiv B \mid\Rightarrow X,\ A \mid\equiv B \mid\equiv X}{A \mid\equiv X}$(**仲裁规则**).

$R_5: \dfrac{A \mid\equiv \#(X)}{A \mid\equiv \#(X,Y)}$(**新鲜性规则**). $R_6: \dfrac{A \triangleleft (X,Y)}{A \triangleleft X,\ A \triangleleft Y}$. $R_7: \dfrac{A \mid\equiv \overset{K}{\vdash\!\!\rightarrow} A,\ A \triangleleft \{X\}_K}{A \triangleleft X}$(**接收规则**).

$R_8: \dfrac{A \mid\equiv (B \mid\sim (X,Y))}{A \mid\equiv (B \mid\sim X),\ A \mid\equiv (B \mid\sim Y)}$(**曾经说过投射**). $R_9: \dfrac{A \mid\equiv B \mid\equiv (X,Y)}{A \mid\equiv B \mid\equiv X}$(**相互信任投射**).

推理过程如下:

M_2 **结合** R_6 **可得**:$C \triangleleft \{\overset{K_a}{\vdash\!\!\rightarrow} A\}_{K_{ca}^{-1}}, C \triangleleft \{N_a\}_{K_a^{-1}}$. **由** $C \triangleleft \{\overset{K_a}{\vdash\!\!\rightarrow} A\}_{K_{ca}^{-1}}$,**初始假设**(1),(15),(4) **和** R_2, R_3, R_4 **可得**:

$$C \mid\equiv \overset{K_a}{\vdash\!\!\rightarrow} A \quad . \tag{1}$$

M_3 **结合初始假设**(9) **和** R_7, R_6 **可得**:$A \triangleleft \{\overset{K_c}{\vdash\!\!\rightarrow} C\}_{K_{ca}^{-1}}, A \triangleleft \{N_a, N_c, A \overset{K_{rand}}{\longleftrightarrow} C\}_{K_{ac}^{-1}}$.

由 $A \triangleleft \{\overset{K_c}{\vdash\!\!\rightarrow} C\}_{K_{ca}^{-1}}$,**初始假设**(2),(16),(5) **和** R_2, R_3, R_4 **可证得**:

$$A \mid\equiv \overset{K_c}{\vdash\!\!\rightarrow} C \quad . \tag{2}$$

由 $A \triangleleft \{N_a, N_c, A \overset{K_{rand}}{\longleftrightarrow} C\}_{K_c^{-1}}$,**式**(2) **和初始假设**(19),(11) **和** R_2, R_5, R_3, R_9, R_4 **可得**:

$$A \mid\equiv A \overset{K_{rand}}{\longleftrightarrow} C \quad . \tag{3}$$

M_4 **结合** R_6 **可得**:$C \triangleleft \text{Token}_c, C \triangleleft \{N_c, A \overset{K_{c,a}}{\longleftrightarrow} C\}_{K_{rand}}$. **由** $C \triangleleft \{N_c, A \overset{K_{c,a}}{\longleftrightarrow} C\}_{K_{rand}}$,**初始假设**(8),(20),(12) **和** R_1, R_5, R_3, R_9, R_4 **可得**:

$$C \mid\equiv A \overset{K_{c,a}}{\longleftrightarrow} C \quad . \tag{4}$$

M_6 **结合** R_6 **可得**:$A \triangleleft \{\overset{K_s}{\vdash\!\!\rightarrow} S\}_{K_{ca}^{-1}}, A \triangleleft \{\text{Token}_c, N_c', N_s\}_{K_s^{-1}}$. **由** $A \triangleleft \{\overset{K_s}{\vdash\!\!\rightarrow} S\}_{K_{ca}^{-1}}$,**初始假设**(2),(17),(6) **和** R_2, R_3, R_4 **可得**:

$$A \mid\equiv \overset{K_s}{\vdash\!\!\rightarrow} S \quad . \tag{5}$$

M_7 结合假设(10) 和 R_7,R_6 可得:

$$S \lhd \{\overset{K_a}{\vdash\!\!\rightarrow} A\}_{K_{ca}^{-1}} \quad , \quad S \lhd \{N_s, C \overset{K_{c,s}}{\longleftrightarrow} S, \{N_c', C \overset{K_{c,s}}{\longleftrightarrow} S\}_{K_{c,a}}\}_{K_a^{-1}} \quad .$$

由 $S\{\lhd \overset{K_a}{\vdash\!\!\rightarrow} A\}_{K_{ca}^{-1}}$,初始假设(3),(18),(7) 和 R_2,R_3,R_4 可得:

$$S \mid\equiv \overset{K_a}{\vdash\!\!\rightarrow} A \quad . \tag{6}$$

由 $S \lhd \{N_s, C \overset{K_{c,s}}{\dashrightarrow} S, \{N_c', C \overset{K_{c,s}}{\longleftrightarrow} S\}_{K_{c,a}}\}_{K_a^{-1}}$,式(6),初始假设(21),(13) 和 R_2,R_8,R_5,R_3,R_9,R_4 可得:

$$S \mid\equiv C \overset{K_{c,s}}{\vdash\!\!\rightarrow} S \quad . \tag{7}$$

M_8 结合 R_6 可得:$C \lhd \{N_c', C \overset{K_{c,s}}{\longleftrightarrow} S\}_{K_{c,a}}$,$C \lhd \{N_c', N_s', C \overset{K_{c,s}}{\longleftrightarrow} S\}_{K_{c,s}}$.

由 $C \lhd \{N_c', C \overset{K_{c,s}}{\longleftrightarrow} S\}_{K_{c,a}}$,式(4),初始假设(22),(14) 和 R_1,R_5,R_3,R_9,R_4 可得:

$$C \mid\equiv C \overset{K_{c,s}}{\vdash\!\!\rightarrow} S \quad . \tag{8}$$

由 $C \lhd \{N_c', N_s', C \overset{K_{c,s}}{\longleftrightarrow} S\}_{K_{c,s}}$,式(8),初始假设(22) 和 R_1,R_5,R_3,R_9 可得:

$$C \mid\equiv S \mid\equiv C \overset{K_{c,s}}{\vdash\!\!\rightarrow} S \quad . \tag{9}$$

由 M_9 可得:$S \lhd \{N_s', C \overset{K_{c,s}}{\longleftrightarrow} S\}_{K_{c,s}}$,结合式(7),初始假设(23) 和 R_1,R_5,R_3,R_9 可得:

$$S \mid\equiv C \mid\equiv C \overset{K_{c,s}}{\vdash\!\!\rightarrow} S \quad . \tag{10}$$

至此,认证目标已全部证出.

5 结 束 语

通过以上分析可看出,基于令牌的单点登录协议达到了一个安全认证系统的认证目标,并且具有更高的效率和更强的安全性. 下一步的工作是将该协议拓展到多安全域中,实现多个验证服务器环境下的认证和密钥分配,并用更完善的逻辑分析方法对其进行形式化分析,验证其安全性.

参考文献:

[1] Chamberlin N. A Brief Overview of Single Sign-on Technology[EB/OL]. http://www.gitec.org/assets/pdfs, 2005-03-10.

[2] Kohl J, Neuman C. The Kerberos Network Authentication Service(V5)[S]. RFC 1510, 1993.

[3] Abadi M, Needham R. Prudent Engineering Practice for Cryptographic Protocols[J]. IEEE Trans on Software Engineering, 1996, 22(1): 6-15.

[4] 钱 勇,谷大武,除克非,等. 公钥密码体制下认证协议的形式化分析方法研究[J]. 小型微型计算机系统,2002, 23(2): 145-147.

[5] 徐晓东,岳殿武. 密码协议的形式化分析与设计原则[J]. 南京邮电学院学报,2001, 21(3): 28-32.

[6] 卓继亮,蔺慧丽,李先贤. 具有可信第三方的认证协议的安全性[J]. 计算机应用研究,2004, (12): 109-112.

[7] Burrows M, Abadi M, Needham R M. A Logic of Authentication[J]. ACM Trans on Computer Systems, 1990, 8(1): 18-36.

[8] Zhang Yuqing, Li Jihong, Xiao Guozhen. 密码协议分析工具——BAN 逻辑及其缺陷[J]. Journal of Xidian University, 1999, 26(3): 76-78.

[9] 王育民,刘建华. 通信网的安全——理论与技术[M]. 西安:西安电子科技大学出版社,1999.

(编辑: 李维东)