认证协议的一些新攻击方法*

王贵林, 卿斯汉, 周展飞

(中国科学院 软件研究所 信息安全国家重点实验室,北京 100080);
(中国科学院 信息安全技术工程研究中心,北京 100080)
E-mail: glwang@ercist.iscas.ac.cn; qsihan@yahoo.com
http://www.ercist.ac.cn

摘要: 给出了针对3个认证协议的6种新攻击方法,分析了这些攻击产生的原因,并对相关协议作了改进.

关键词: 认证协议;协议攻击;密码协议;密码学
中图法分类号: TP393 **文献标识码**: A

在开放式的网络环境中,认证协议的重要性体现在两个方面:确认主体的身份和为通信主体分发会话密钥.然而,认证协议的设计却是一项非常复杂的工作,要设计出简洁、高效而又能抵抗各种攻击的协议是很困难的.究其原因,首先是各种认证协议的设计背景差别很大,设计目的各异.其次,在同一背景下具有相同目的的各种协议,其报文又不尽相同.再次,符号问题:不同文献中相同的符号可能有不同的含义,不同的符号又可能有相同的含义.众所周知,无论是协议的背景假设,还是所用符号的含义不同,或者交换报文的少许差异,都会导致协议功能上的微妙而又可能是本质性的变化.于是,在近10年中提出了多种研究和分析协议的形式化方法,以检查协议是否具有安全缺陷,能否达到预期的设计目标.但遗憾的是,到目前为止,还没有一种形式化方法能够对协议的正确性给出既充分又必要的判定.以著名的BAN逻辑[1]为例,虽然具有严格的公理体系和推理规则,而且利用BAN逻辑也确实发现了许多协议的安全缺陷.但其理想化过程却是非形式化的、不严格的[2,3].另外,文献[4]还指出,用BAN类逻辑分析表明正确的协议,仍然可能存在安全缺陷(本文中的攻击5也是这种例子).鉴于协议形式化分析研究的这种状况,也有人开始展开对协议的非形式化方法的研究[5],为认证协议的设计提供参考准则,以避免诸多设计错误.

本文给出了我们所发现的对3个协议的6种新的攻击方法,分析了产生这些安全缺陷的原因,并对相关协议作了改进.由于这些攻击的产生原因涉及到认证协议设计中的许多难点问题(身份与临时值(nonce)的使用、加密的目的、服务器的功能、报文格式的重要性以及通信角色的确定等),所以我们相信,由这些具体攻击得出的经验具有一定的代表性,对认证协议的设计、分析和攻击都具有相当的借鉴作用.本文中所发现的6个攻击实例是:对A(0)协议[6]的3种攻击方法;对于对称密码体系版本的Needham-Schroeder协议[7]的一种攻击方法;对Otway-Rees协议[8]及其改进版[5]的攻击方法.

在本文中,用大写英文字母A,B等表示一般主体,用S表示服务器,用I表示攻击者.用$K_{}$,

* 收稿日期: 1999-07-29; 修改日期: 2000-03-13
基金项目: 国家自然科学基金资助项目(60083007)
作者简介: 王贵林(1968-),男,云南大理人,博士,主要研究领域为协议分析,信息安全基础;卿斯汉(1939-),男,湖南邵阳人,研究员,博士生导师,主要研究领域为信息安全理论与技术;周展飞(1969-),男,江苏苏州人,博士后,主要研究领域为密码理论,应用数学.

K_a,K_{ab}等表示加密密钥,而与它们对应的解密密钥分别表示为K^{-1},K_a^{-1},K_{ab}^{-1}等.密钥的下标表示与此密钥相关的主体.例如,K_{ab}表示该密钥与主体A,B有关.这里的密钥可以是对称密码体系(如DES)中的共享密钥,也可以是非对称密码体系(如RSA)中的公开密钥或私有密钥,具体的解释由上下文确定.另外,在描述协议攻击时,将用到与下列式子类似的报文:

1. $I(A)\rightarrow B$: X
2. $B\rightarrow(A)I$: Y

其中的报文1表示,主体I冒充主体A向主体B发送报文X;而报文2则表示,主体B发送给主体A的报文Y被主体I截获.一句话,(A)表示A是某报文的预期发送者(或接收者),但不是该报文的实际发送者(或接收者).

1 A(0)协议

A(0)协议[6]的目的是为通信双方建立共享密钥.选定公开的大素数P及有限域$GF(P)$中的本原元α.在协议开始之前,通信双方A和B各自先选取两个随机整数$\bar{x}$和$\bar{y}$,将计算所得的

$$\bar{R}_a=\alpha^{\bar{x}}(\mathrm{mod}\ P)(\text{对}\ A\ \text{而言}),$$

$$\bar{R}_b=\alpha^{\bar{y}}(\mathrm{mod}\ P)(\text{对}\ B\ \text{而言}),$$

发往认证中心T,以获得各自的公开协商密钥证书(certificate of public key-agreement key).该证书是认证中心T对任一主体C的身份及其公开协商密钥$\bar{R}_c$进行签名的结果.然后,A和B各自选择一随机整数x和y,并计算

$$R_a=\alpha^{x}(\mathrm{mod}\ P)(\text{对}\ A\ \text{而言}),$$

$$R_b=\alpha^{y}(\mathrm{mod}\ P)(\text{对}\ B\ \text{而言}),$$

这里的R_a和R_b可称为A,B的临时公开协商密钥(the fresh part of public agreement key).在此基础上,即可执行A(0)协议,其具体报文如下:

1. $A\rightarrow B$: $A,\bar{R}_a,\{A,\bar{R}_a\}_{K_t^{-1}},R_a$
2. $B\rightarrow A$: $B,\bar{R}_b,\{B,\bar{R}_b\}_{K_t^{-1}},R_b$

其中$\{A,\bar{R}_a\}_{K_t^{-1}}$就是认证中心$T$所签发的、主体$A$的公开协商密钥证书.$B$收到报文1后,通过验证$T$的签名来证实$A$的身份,进而计算出他与$A$之间所建立的共享会话密钥(此后的等式都表示mod P运算):

$$K_{ab}=(\bar{R}_a)^{y}\cdot(R_a)^{\bar{y}}=\alpha^{\bar{x}y}\cdot\alpha^{x\bar{y}}.$$

A也可以类似地验证B的身份,并获得他与B之间的共享会话密钥:

$$K_{ab}=(\bar{R}_b)^{x}\cdot(R_b)^{\bar{x}}=\alpha^{\bar{x}y}\cdot\alpha^{x\bar{y}}.$$

A(0)协议具有一些优点.首先,交换的报文只有两条,内容少而简洁.其次,协议执行的前提条件简单,因为欲建立共享密钥的主体只需要得到认证中心T所签发的公开密钥协商证书就可以执行协议.另外,主体间的共享密钥是通过双方协商产生的,这既体现了公平性,又减轻了认证中心的负担,同时也限制了认证中心的权力.因为从本质上说,对于任一主体A而言,T和其他普通主体一样只知道A的$\bar{R}_a$,并不知道A的$\bar{x}$.

文献[9]中指出了对A(0)协议的一种潜在的攻击方法.攻击者I通过协议的正常执行得到主体A的$\bar{R}_a$以后,把$\bar{R}_a$发往认证中心T,如果T没有检查到$\bar{R}_a$已经是A的公开协商密钥,而给I签发$\{I,\bar{R}_a\}_{K_t^{-1}}$作为其公开协商密钥证书,那么由此可产生一种攻击.但这种攻击与其说是攻击,还

不如说是A(0)协议的缺点.因为只要要求认证中心T保证各主体的公开协商密钥是互不相同的,就可以防止这种攻击.不过,当如果主体很多,而每个公开协商密钥又需要频繁更换时,T的负担就很重.

下面是我们新发现的、对A(0)协议的3种攻击方法.

攻击1. I先与A进行正常通信,然后将A发送来的报文转给B.这样,B认为A欲与其通信,就会给A发送回应报文.A收到B的报文后,便认为是B欲与其通信,自然也会发送回应报文给B,但此报文被I截取.具体报文顺序如下:

$$\alpha.1.\quad I\rightarrow A:\ I,\overline{R}_i,\{I,\overline{R}_i\}_{K_t^{-1}},R_i$$

$$\alpha.2.\quad A\rightarrow I:\ A,\overline{R}_a,\{A,\overline{R}_a\}_{K_t^{-1}},R_a$$

$$\beta.1.\quad I(A)\rightarrow B:\ A,\overline{R}_a,\{A,\overline{R}_a\}_{K_t^{-1}},R_a$$

$$\beta.2.\quad B\rightarrow A:\ A,\overline{R}_b,\{A,\overline{R}_b\}_{K_t^{-1}},R_b$$

$$\beta.2'.\quad A\rightarrow (B)I:\ A,\overline{R}_a,\{A,\overline{R}_a\}_{K_t^{-1}},R'_a$$

攻击结束时,尽管A和B都认为他们之间已共享一个会话密钥,但他们所拥有的密钥并不相同,所以A(0)协议失效.A认为其与B共享的密钥是

$$K'_{ab}=(\overline{R}_b)^{x'}\cdot(R_b)^{\overline{x}}=\alpha^{\overline{x}y}\cdot\alpha^{x'\overline{y}},$$

而B认为其与A共享的密钥是

$$K_{ab}=(\overline{R}_a)^{y}\cdot(R_a)^{y}=\alpha^{xy}\cdot\alpha^{\overline{x}y}.$$

攻击2. 攻击2与攻击1类似.I先分别与A,B进行正常通信,然后将他们发送给I的报文转发给对方.此时,A和B都认为对方欲与其通信,于是他们会互发回应报文,但这些回应报文被I截获.其结果也如同攻击1一样:虽然A和B都认为他们已共享一个会话密钥,但他们所拥有的密钥并不相同.

稍加分析不难看出,产生这两种攻击的原因是,A(0)协议中的两条报文格式是完全相同的,因此不能明确地表明主体在协议中的通信角色——谁是通信的发起者、谁是通信的响应者.

攻击3. I先与A进行正常通信,然后将A发送给I的报文转给B,并将B发给A的报文截获.具体报文顺序如下:

$$\alpha.1.\quad I\rightarrow A:\ I,\overline{R}_i,\{I,\overline{R}_i\}_{K_t^{-1}},R_i$$

$$\alpha.2.\quad A\rightarrow I:\ A,\overline{R}_a,\{A,\overline{R}_a\}_{K_t^{-1}},R_a$$

$$\beta.1.\quad I(A)\rightarrow B:\ A,\overline{R}_a,\{A,\overline{R}_a\}_{K_t^{-1}},R_a$$

$$\beta.2.\quad B\rightarrow (A)I:\ B,\overline{R}_b,\{B,\overline{R}_b\}_{K_t^{-1}},R_b$$

这样,B就会错误地认为其与A之间已享有一个会话密钥

$$K_{ab}=(\overline{R}_a)^{y}\cdot(R_a)^{\overline{y}};$$

而A对此却一无所知,因为他此时只与I共享会话密钥

$$K_{ai}=(\overline{R}_i)^{x}\cdot(R_i)^{\overline{x}}.$$

由于一个主体的公开协商密钥证书会使用较长时间(几个小时或几周),所以攻击3会产生严重的危害:主体B认为他与主体A之间刚刚建立了一个会话密钥,但主体A根本就没有参与会话密钥的建立过程,他甚至可能是离线的.这一攻击表明,还需要进一步交换报文以确定K_{ab}确实是A和B之间的共享密钥.

现在,我们来分析上述攻击产生的原因,并考虑如何改进A(0)协议.

对于任一主体 A 而言,由于他与认证中心 T 之间并没有共享密钥可以利用,也没有私有密钥可以用来签名,所以他只能以明文的方式发送 R_a. 这无疑是上述攻击成功的主要原因. A(0)协议的安全性是基于离散对数问题的,所以通过仔细的观察不难看出,第3方是否知道 R_a 并不重要,关键是要使接收方能认定这一 R_a 确实是由 A 发送出来的. 为此,可以利用刚刚建立起来的共享密钥进行一次关于 R_a 的握手. 对 R_b 存在的同样问题也可类似解决. 这样就可得到A(0)协议的改进形式:

1. $A\rightarrow B$: $A,\overline{R}_a,\{A,\overline{R}_a\}_{K_t^{-1}},R_a$
2. $B\rightarrow A$: $B,\overline{R}_b,\{B,\overline{R}_b\}_{K_t^{-1}},R_b,\{B,R_a,R_b\}_{K_{ab}}$
3. $A\rightarrow B$: $\{A,R_b\}_{K_{ab}}$

2 Needham-Schroeder 协议

根据所用密码体系的不同,Needham-Schroeder 协议[5,7](简称 NS 协议)有对称密码体系和非对称密码体系下的两个版本. 这里,讨论对称密码体系版本的 NS 协议:

1. $A\rightarrow S$: A,B,N_a
2. $S\rightarrow A$: $\{N_a,B,K_{ab},\{K_{ab},A\}_{K_{bs}}\}_{K_{as}}$
3. $A\rightarrow B$: $\{K_{ab},A\}_{K_{bs}}$
4. $B\rightarrow A$: $\{N_b\}_{K_{ab}}$
5. $A\rightarrow B$: $\{N_b-1\}_{K_{ab}}$

这里,假设 S 与 A 和 B 分别享有共享密钥 K_{as} 和 K_{bs}. 其中,前3条报文的作用是主体 A 在服务器 S 的帮助下,进行会话密钥 K_{ab} 的分配. 而后两条报文的目的是使 B 相信 A 现在在线,但不能使 B 相信会话密钥 K_{ab} 是新鲜的. 认识到 NS 协议中的 K_{ab} 对 B 没有新鲜性,Denning 和 Sacco 在文献[10]中指出,攻击者可以利用已经泄露的会话密钥对 B 进行欺骗. 为了使 B 能够识别 K_{ab} 的新鲜性,他们采取用时间戳(timestamp)代替临时值的方法. 解决这一问题的另一方法[11]是,让 B 也向 S 发送一个临时值,然后 S 将 B 的临时值放在给 B 的密钥证书中.

攻击4. 现在,我们指出一种新的攻击方法,即使攻击者没有得到泄露的会话密钥 K_{ab},主体 A 也不能通过报文3,4,5推断出主体 B 知道会话密钥 K_{ab}. 具体的攻击报文顺序如下:

1. $A\rightarrow S$: A,B,N_a
2. $S\rightarrow A$: $\{N_a,B,K_{ab},\{K_{ab},A\}_{K_{bs}}\}_{K_{as}}$
3. $A\rightarrow (B)I$: $\{K_{ab},A\}_{K_{bs}}$
4. $I(B)\rightarrow A$: N_i
5. $A\rightarrow (B)I$: $\{\{N_i\}_{K_{ab}}+\}_{K_{ab}}$

在这一攻击中,攻击者 I 首先将 A 发给 B 的报文3拦截,然后伪装成 B,给 A 发送一个格式与 $\{N_b\}_{K_{ab}}$ 相同的随机数 N_i. 于是 A 就对 N_i 进行所谓的解密,然后再将所得结果与1求和并进行加密后发给 B,但这一报文也被 I 拦截. 攻击结束时,A 认为主体 B 已经知道会话密钥 K_{ab},但实际上 B 更本就没有参加协议的执行过程,B 甚至可能是离线的. 所以,为避免这一攻击,B 应该在报文4中加入主体 A 可识别的消息(比如 B 的身份或临时值 N_a). 另外,为了使 B 得知 K_{ab} 的新鲜性,可由 S 产生一个时间戳 T_s. 由此,我们就可得到对 NS 协议的如下改进形式:

1. $A\rightarrow S$: A,B,N_a
2. $S\rightarrow A$: $\{N_a,B,K_{ab},\{K_{ab},A,N_a,T_s\}_{K_{bs}}\}_{K_{as}}$
3. $A\rightarrow B$: $\{K_{ab},A,N_a,T_s\}_{K_{bs}}$
4. $B\rightarrow A$: $\{N_b,N_a\}_{K_{ab}}$
5. $A\rightarrow B$: $\{N_b\}_{K_{ab}}$

3 Otway-Rees 协议

在 Otway-Rees 协议[8](简称 OR 协议)中,服务器 S 为两个主体 A 与 B 传送新的会话密钥 K_{ab}. 初始条件是 S 分别与 A,B 共享密钥 K_{as},K_{bs}. 具体报文如下:

1. $A\rightarrow S$: $M,A,B,\{N_a,M,A,B\}_{K_{as}}$
2. $B\rightarrow S$: $M,A,B,\{N_a,M,A,B\}_{K_{as}},\{N_b,M,A,B\}_{K_{bs}}$
3. $S\rightarrow B$: $M,\{N_a,K_{ab}\}_{K_{bs}},\{N_b,K_{ab}\}_{K_{bs}}$
4. $B\rightarrow A$: $M,\{N_a,K_{ab}\}_{K_{as}}$

这里,M 是会话识别号;而临时值 N_a 和 N_b 不仅提供了时序信息,还因为在报文 1 和报文 2 中受到了加密保护,所以在报文 4 和报文 5 中这两个临时值作为主体身份的替身出现. S 在检查了报文 2 中两个加密消息内的 M,A,B 相匹配之后,才为 A,B 生成会话密钥 K_{ab},并向 B 发送报文 3. 文献[1]对 OR 协议进行了分析,其结论是:协议正确,但有冗余信息. 但我们发现了一个对 OR 协议的攻击方法(攻击 5). 为了减少冗余,文献[1]提出了 OR 协议的一个修改版:N_a 可省,其作用由 M 代替;报文 2 中的 N_b 不必加密,可用明文传输. 同时,文献[1]还指出,经过修改的 OR 协议与原 OR 协议具有相同的理想化形式,从而就具有相同的逻辑分析结果. 但事实并非如此,Boyd 和 Mao 发现,对文献[1]修改后的 OR 协议存在攻击方法[2]. 此后,Abadi 和 Needham 注意到了这一攻击,于是在文献[5]中提出了 OR 协议的另一个修改版:

1. $A\rightarrow B$: A,B,N_a
2. $B\rightarrow S$: A,B,N_a,N_b
3. $S\rightarrow B$: $\{N_a,A,B,K_{ab}\}_{K_{as}},\{N_b,A,B,K_{ab}\}_{K_{bs}}$
4. $B\rightarrow A$: $\{N_a,A,B,K_{ab}\}_{K_{as}}$

他们认为,将这一修改版与原 OR 协议及文献[1]的修改版相比,更为有效、简洁. 然而,针对文献[5]的这一修改版,我们也发现了一个攻击方法(攻击 6).

攻击 5. 我们发现了对原 OR 协议的如下攻击方法:

α. 1. $A\rightarrow B$: $M,A,B,\{N_a,M,A,B\}_{K_{as}}$

α. 2. $B\rightarrow S$: $M,A,B,\{N_a,M,A,B\}_{K_{as}},\{N_b,M,A,B\}_{K_{bs}}$

α. 3. 1. $S\rightarrow (B)I$: $M,\{N_a,K_{ab}\}_{K_{as}},\{N_b,K_{ab}\}_{K_{bs}}$

β. 2. $I(B)\rightarrow S$: $M,A,B,\{N_a,M,A,B\}_{K_{as}},\{N_b,M,A,B\}_{K_{bs}}$

β. 3. $S\rightarrow (B)I$: $M,\{N_a,K'_{ab}\}_{K_{as}},\{N_b,K'_{ab}\}_{K_{bs}}$

α. 3. 2. $I(S)\rightarrow B$: $M,\{N_a,K_{ab}\}_{K_{as}},\{N_b,K'_{ab}\}_{K_{bs}}$

α. 4. $B\rightarrow A$: $M,\{N_a,K_{ab}\}_{K_{as}}$

其中 B 发送给 S 的报文 α.2 被 I 窃听到并进行了复制,然后 I 在报文 β.2 中简单地将此报文重发给 S. 于是 S 认为 A,B 之间还要建立另一个会话密钥,从而为他们生成密钥 K'_{ab}. 这之后,I 将他所截获的报文 α.3.1 和报文 β.3 进行组合,以生成报文 α.3.2. 攻击完成后,尽管 A 和 B 都得到了会话密钥,但却不是同一个密钥:A 得到的是 K_{ab},而 B 得到的却是 K'_{ab}.

该攻击的成功需要两个关于服务器 S 的假设成立:(1) S 对 A,B 之间时间相隔很短的两次密钥申请不进行限制;(2) S 只对报文 2 中两个加密消息内的会话识别号及主体身份进行匹配检查,而对 A,B 之间密钥分配请求中的 M 不作记录. 我们认为这两个假设是合理的:一方面,本协议的设计者根本没有谈及对服务器 S 是否有这样的要求;另一方面,要加强服务器 S 的功能,从而使这两个假设不成立,这也是困难的.

攻击 6. 对于文献[5]中所提出的 OR 协议修改版的攻击. 在这一攻击中,攻击者 I 将 B 发给 S 的报文 α.2.1 截获,然后把 N_a 和 N_b 分成两次发送给 S,而服务器以为 A 和 B 之间要建立两次会话,所以会给 B 发送两个报文以分发两个密钥. 但是,攻击者 I 将这两个报文截获,并将其组成部分进行组合后发送给 B. 攻击结束时,主体 A 和 B 所拥有的密钥并不相同.

α.1. $A\rightarrow B$: A,B,N_a

α.2.1. $B\rightarrow(S)I$: A,B,N_a,N_b

α.2.2. $I(B)\rightarrow S$: A,B,N_a,N_i

β.2. $I(B)\rightarrow S$: A,B,N'_i,N_b

α.3.1. $S\rightarrow(B)I$: $\{N_a,A,B,K_{ab}\}_{K_{as}},\{N_i,A,B,K_{ab}\}_{K_{bs}}$

β.3. $S\rightarrow(B)I$: $\{N'_i,A,B,K'_{ab}\}_{K_{as}},\{N_b,A,B,K'_{ab}\}_{K_{bs}}$

α.3.2. $I(S)\rightarrow B$: $\{N_a,A,B,K_{ab}\}_{K_{as}},\{N_b,A,B,K'_{ab}\}_{K_{ab}}$

α.4. $B\rightarrow A$: $\{N_a,A,B,K_{ab}\}_{K_{as}}$

攻击 6 攻击的成功也需要关于服务器 S 的如下假设成立:S 对 A,B 之间时间相隔很短的两次密钥申请不进行限制. 但需要 S 对 A,B 之间的临时值作记录的假使,因为报文 α.2.2 和 β.2 中所使用的临时值并不相同.

4 结束语

本文给出了我们所发现的对 3 个认证协议的 6 种新的攻击方法,分析了产生这些安全缺陷的原因,并对相关协议进行了改进. 由于这些攻击的产生原因涉及到认证协议设计中的许多难点问题,所以我们相信,由这些具体攻击实例得出的经验具有一定的代表性,对认证协议的设计、分析和攻击都具有相当的借鉴作用.

References:

[1] Burrows, M., Abadi, M., Needham, R. A logic of authentication. Proceedings of the Royal Society of London, 1989,A(426):233~271.

[2] Boyd, C., Mao, W. On a limitation of BAN logic. In: Helleseth, T., ed. Advances in Cryptology-EUROCRYPT'93. Lecture Notes in Computer Science 765. Berlin: Springer-Verlag, 1993. 240~247.

[3] Nessett, D.M. A critique of the Burrows, Abadi and Needham logic. Operating Systems Review, 1990,24(2):35~38.

[4] Qing, Shi-han. Formal analysis of authentication protocols. Journal of Software, 1996,7:107~114 (in Chinese).

[5] Abadi, M., Needham, R. Prudent engineering practice for cryptographic protocols. IEEE Transactions on Software Engineering, 1996,22(1):6~15.

[6] Matsumoto, T., Takashima, Y., Imai, H. On seeking smart public-key distribution systems. Transactions on IECE Japan, 1986,69(2):99~106.

[7] Needham, R., Schroeder, M. Using encryption for authentication in large networks of computers. Communications of the ACM, 1978,21(12):993~999.

[8] Otway, D., Rees, O. Efficient and timely mutual authentication. ACM Operating Systems Review, 1987,21(1):8~10.

[9] Syverson, P.F., van Oorschot, P.C. A Unified Cryptographic Protocol Logic. 1996.

[10] Denning, D.E., Sacco, G.M. Timestamps in key distribution protocols. Communications of the ACM, 1981,24(8):533~536.

[11] Needham, R., Schroeder, M. Authentication revisited. Operating Systems Review, 1987,21(1):7.

附中文参考文献:

[4] 卿斯汉.认证协议的形式化分析,软件学报,1996,7:107~114.

Some New Attacks upon Authentication Protocols*

WANG Gui-lin, QING Si-han, ZHOU Zhan-fei

(*State Key Laboratory of Information Security, Institute of Software, The Chinese Academy of Sciences, Beijing* 100080, *China*);
(*Engineering Research Center for Information Security Technology, The Chinese Academy of Sciences, Beijing* 100080, *China*)
E-mail: glwang@ercist.iscas.ac.cn; qsihan@yahoo.com
http://www.ercist.ac.cn

Abstract: In this paper, six new attacks upon three authentication protocols are presented. Then the reasons resulting these attacks are analyzed, and the improvement schemas to the related authentication protocols are given.

Key words: authentication protocol; protocol attack; cryptographic protocol; cryptography

* Received July 29, 1999; accepted March 13, 2000
Supported by the National Natural Science Foundation of China under Grant No. 60083007