认证协议的形式化分析*

卿斯汉

(中国科学院软件研究所 北京 100080)

摘要 认证协议的设计是一项十分困难的工作,国际标准化组织(ISO)一直致力于不同环境的认证协议标准的制定.本文研究用BAN逻辑形式化地分析认证协议的方法,指出BAN逻辑分析并非总是推导出正确的结论.在此基础上,本文讨论了认证协议的设计原则以及改进BAN逻辑的设想.

关键词 认证,认证协议,BAN逻辑,密码算法,杂凑函数,数字签名.

近10年来,在计算机网络和分布式系统等应用领域提出了对安全保密的新要求,其中最关键的是认证问题.人们认识到,单纯依靠优良的安全保密算法是不够的,还需要设计基于优良安全算法的优良的密码协议.在分布式系统中,认证是通过协议(称之为认证协议)来实现的.认证协议的主要目的是证实参加协议各方(称之为主体)的身份.此外,许多认证协议还有一个附加的目的,即在主体之间分配密钥或其它各种秘密.然而,设计一个正确的认证协议却是众所周知的一项十分困难的工作.即使参加协议的主体只有2个或3个,在整个协议中交换的报文只有3~5条,迄今所知的许多协议都存在这样或那样的安全缺陷.其原因是多方面的,例如,缺乏正确设计认证协议的指导原则;对认证协议进行非形式化的推理分析;没有考虑到多种攻击类型;对协议施加太强的假设等等.因此,目前的状况大体是:设计出一个认证协议——发现其安全缺陷——改进该协议——发现它不能抵抗另一种形式的攻击——继续改进该协议……

在认证协议的发展史上,最有影响的是Needham-Schroeder协议[1],它们是基于传统密码学(对称密码体制)和公开钥密码学(非对称密码体制)的一系列认证协议.尽管已经发现,上述协议存在着不少不妥之处,但它们是许多近代认证协议和ISO认证协议标准的基础.在设计和分析认证协议的同时,也出现了一系列辅助技术和工具,其中最著名的是BAN逻辑.[2]BAN逻辑将认证协议的非形式化描述转化为一种特殊的形式(称之为理想化形式),并利用逻辑规则去分析它.利用BAN逻辑,可以成功地发现Needham-Schroeder协议等的安全缺陷,并提出相应的改进意见.

但是,本文的研究说明,经BAN逻辑证明正确的协议有时也是有错的,即由于BAN逻辑本身固有的缺陷,会引起错误的结论.因此,我们的忠告是,不能完全相信BAN逻辑分析

---

* 作者卿斯汉,1939年生,研究员,主要研究领域为信息安全保密技术.
本文通讯联系人,卿斯汉,北京100080,中国科学院软件研究所
本文1995-11-03收到修改稿

的结果.

1 基本概念和符号

BAN 逻辑的形式化基础是多种类模态逻辑. 在 BAN 逻辑中区别主体、密钥和公式(也称作语句). 令符号 A,B,C 和 S 表示具体的主体;令 $K_{AB},K_{AC},K_{AS},K_{BS}$ 等表示具体的共享密钥;令 K_A,K_B,K_C,K_S 等表示具体的公开密钥;令 $K_A^{-1},K_B^{-1},K_C^{-1},K_S^{-1}$ 等表示具体的秘密密钥;令 N_A,N_B,N_C,N_S 等表示临时值(Nonce),即一种特殊的语句.

令 P,Q 和 R 表示任意主体;令 X 和 Y 表示任意语句;令 K 表示任意密钥. 我们有以下结构*:

(X,Y)——X 和 Y 链接

$\{X\}_K$——用 K 加密 X 后的结果

$H(X)$——X 的单向杂凑函数

$P\models X$——P 确信 X

$P\lhd X$——P 曾收到 X

$P\propto X$——P 曾发送 X

$P\Rightarrow X$——P 对 X 有管辖权

$\#(X)$——X 是新的

$P\overset{K}{\leftrightarrow}Q$——$P$ 和 Q 可用共享密钥 K 通信

$\overset{K}{\rightarrow}P$——$K$ 是 P 的公开密钥

$P\overset{X}{\rightleftharpoons}Q$——$X$ 是 P 和 Q 间的共享秘密

$(X)_Y$——$(X,Y)\wedge Y$ 是某种秘密

特别地,在本文中,结构 $\{X\}_{K_A^{-1}}$ 表示用 K 对 X 进行数字签名.

以下,我们强调临时值 N 的重要作用. 众所周知,"报文重发型"攻击(攻击者截获合法用户的有效认证报文后,冒充合法用户重发该报文的一种攻击形式)是对认证协议安全的主要威胁. 为了保证所交换的报文是最新的,亦即保证一条报文是最近生成并发送的,而不是一条旧报文的重发,认证协议必须检查报文的"新旧性". 通常,我们使用时间戳、序列号和临时值以及报文链接 4 种方法保证报文的时效性. 基于时间戳的认证协议要求系统使用同步时钟;基于序列号的认证协议要求系统存储附加的信息,即每个主体应用的序列号;基于临时值的认证协议要求在认证过程中交换附加的报文,即主体生成的临时值;报文链接是将最后一次接收到的报文的一段插入到下一条发送的报文之中. 在本文中,我们只讨论采用临时值的认证协议.

对于"请求一响应"这类握手式协议,如果在请求报文中包含一个临时值,则在响应报文中如果再出现此值,就可以保证响应报文的时效性. 因此,临时值必须具有"一次性"的特征. 换言之,应当要求一个主体的临时值只使用 1 次,至少应当要求在该主体的密钥生命周期内临时值只使用 1 次. 为此,系统应该建立一个良好的伪随机数生成器,使临时值具有良好的随机性和不可预测性. 今后,我们认为上述条件已经满足.

2 BAN 逻辑

BAN 逻辑形式化分析工具的目的是解答下述问题:认证协议是否正确;认证协议的目标是否达到认证协议的初设是否合适;认证协议是否冗余.

---

* 因为有些符号排版软件中没有,故文中有些地方没有使用习惯的符号

BAN 逻辑分析的过程是:(1)建立初始假设集合 α;(2)建立理想化协议模型;(3)建立协议预期目标集合 γ;(4)利用初设和逻辑公设推理;(5)推导出协议最终目标集合 Γ;(6)若 $\Gamma\supseteq\gamma$,则协议可行.

以上步骤可能会重复进行,例如,通过分析增加新的初设、改进理想化协议等.

3 成功的例子

利用 BAN 逻辑可以成功地分析下述 Yahalom 协议:

$Y1$　$A\rightarrow B$: A,N_A

$Y2$　$B\rightarrow S$: $B,\{A,N_A,N_B\}_{K_{BS}}$

$Y3$　$S\rightarrow A$: $\{B,K_{AB},N_A,N_B\}_{K_{AS}},\{A,K_{AB}\}_{K_{BS}}$

$Y4$　$A\rightarrow B$: $\{A,K_{AB}\}_{K_{BS}},\{N_B\}_{K_{AB}}$

其中主体 S 是认证服务器.

初设集合 α 是:

$A\models A\overset{K_{AS}}{\leftrightarrow}S$, $B\models B\overset{K_{BS}}{\leftrightarrow}S$, $S\models A\overset{K_{AS}}{\leftrightarrow}S$, $S\models B\overset{K_{BS}}{\leftrightarrow}S$,

$A\models S\not\succ A\overset{K}{\leftrightarrow}B$, $B\models S\not\succ A\overset{K}{\leftrightarrow}B$, $S\models A\overset{K_{AB}}{\leftrightarrow}B$,

$A\models\#(N_A)$, $B\models\#(N_B)$, $S\models\#(A\overset{K_{AB}}{\leftrightarrow}B)$, $B\models A\overset{N_B}{\rightleftharpoons}B$,

$B\models S\not\succ\#(A\overset{K_{AB}}{\leftrightarrow}B)$, $B\models A\not\succ S\models\#(A\overset{K}{\leftrightarrow}B)$, $A\models S\not\succ B\propto N$.

值得注意的是,此处 N_B 不仅是一个临时值,它还是 A 和 B 之间共享的一个秘密(至少 B 如此认为).理想化协议模型是

$Y2$　$B\rightarrow S$: $\{N_A,N_B\}_{K_{BS}}$

$Y3$　$S\rightarrow A$: $\{A\overset{K_{AB}}{\leftrightarrow}B,\#(A\overset{K_{AB}}{\leftrightarrow}B),N_A,N_B,B\propto N_A\}_{K_{AS}},\{A\overset{K_{AB}}{\leftrightarrow}B\}_{K_{BS}}$

$Y4$　$A\rightarrow B$: $\{A\overset{K_{AB}}{\leftrightarrow}B\}_{K_{BS}},\{\langle N_B,A\overset{K_{AB}}{\leftrightarrow}B,S\models\#(A\overset{K_{AB}}{\leftrightarrow}B)\rangle_{N_B}\}_{K_{AB}}$

注意 $Y1$ 被省略了,因为它与 BAN 逻辑分析无关.

协议预期目标集合 γ 是

$A\models A\overset{K_{AB}}{\leftrightarrow}B,B\models A\overset{K_{AB}}{\leftrightarrow}B,A\models B\models N_A,B\models A\models A\overset{K_{AB}}{\leftrightarrow}B.$

换言之,Yahalom 协议设计的目标是分配会话密钥,且每个主体都能证实对方的身份.

以下是逻辑推理过程.

由 $Y2$ 可以推出 $S\models B\propto(N_A,N_B)$.

由 $Y3$ 可以推出 $A\lhd N_B,A\models A\overset{K_{AB}}{\leftrightarrow}B,A\models S\models\#(A\overset{K_{AB}}{\leftrightarrow}B),A\models B\models N_A$.

上述推导中,应用了 BAN 逻辑的"报文含义","临时值校验"和"管辖"法则逻辑公设.

由 $Y4$ 可以推出 $B\models S\propto A\overset{K_{AB}}{\leftrightarrow}B,B\lhd A\overset{K_{AB}}{\leftrightarrow}B$.

值得注意的是,协议在此处要求 B 在证实 K_{AB} 是适当的密钥之前就使用它.为了能处理这类"未校验密钥",我们有必要扩展 BAN 逻辑,即增加下述逻辑公设:

$$\frac{P\vdash R\propto P\overset{K}{\leftrightarrow}Q,P\lhd\{X\}_K}{P\lhd X}$$

由此,我们可以推出 $B\lhd(N_B,A\overset{K_{AB}}{\leftrightarrow}B,S\vdash\#(A\overset{K_{AB}}{\leftrightarrow}B))_{N_B}$.

从而,可得

$B\vdash A\vdash(A\overset{K_{AB}}{\leftrightarrow}B,S\vdash\#(A\overset{K_{AB}}{\leftrightarrow}B)),B\vdash\#(A\overset{K_{AB}}{\leftrightarrow}B),B\vdash A\overset{K_{AB}}{\leftrightarrow}B$.

因此,协议的最终目标集合 Γ 是

$A\vdash A\overset{K_{AB}}{\leftrightarrow}B,\ B\vdash A\overset{K_{AB}}{\leftrightarrow}B,A\vdash B\vdash N_A,\ B\vdash A\vdash A\overset{K_{AB}}{\leftrightarrow}B$.

故 $\Gamma\supseteq\gamma$,即协议可行.

通过 BAN 逻辑的形式化分析,还可以指出改进 Yahalom 协议的方向. 我们发现,协议的初设条件太强了. 诸如 $B\vdash A\overset{N_B}{\rightleftharpoons}B,B\vdash A\not\ni S\vdash\#(A\overset{K}{\leftrightarrow}B)$ 等初设,以及使用"未校验密钥"的条件可否去掉呢? 答案是肯定的. 改进后的 Yahalom 协议如下:

$Y1'$ $A\rightarrow B$: A,N_A

$Y2'$ $B\rightarrow S$: $B,N_B,\{A,N_A\}_{K_{BS}}$

$Y3'$ $S\rightarrow A$: $N_B,\{B,K_{AB},N_A\}_{K_{AS}},\{A,K_{AB},N_B\}_{K_{BS}}$

$Y4'$ $A\rightarrow B$: $\{A,K_{AB},N_B\}_{K_{BS}},\{N_B\}_{K_{AB}}$

在上述协议中,不再使用"未校验密钥". 因为,在 $Y4$ 中临时值 N_B 保证了报文的时效性. 此外,N_B 不再是秘密. 于是,上述协议可以达到与 Yahalom 协议相同的目的,但减少了许多不必要的假设条件.

4 失败的例子 1

认证协议的微妙之处在于,往往一点很小的不起眼的改动,会引起根本性的变化. 例如,一个很好的协议会出现一个很大的安全漏洞. 或者反之,一个很不安全的协议只要改动一点点,就会转变成一个难以攻破的好协议.

下面的协议 Z,很类似前面讲过的 Yahalom 协议,但 Z 协议隐含着一个难以察觉的安全缺陷.

$Z1$ $A\rightarrow B$: $A,\{N_A,A\}_{K_{AS}}$

$Z2$ $B\rightarrow S$: $A,B,\{N_A,A\}_{K_{AS}},\{N_B,B\}_{K_{BS}}$

$Z3$ $S\rightarrow A$: $\{K_{AB},B\}_{K_{AS}},\ \{N_A,N_B,\{K_{AB},A,N_B\}_{K_{BS}}\}_{K_{AB}}$

$Z4$ $A\rightarrow B$: $\{K_{AB},A,N_B\}_{K_{BS}},\{N_B\}_{K_{AB}}$

为简便起见,令 Z 协议的预期目标集合 γ 为: $A\vdash A\overset{K_{AB}}{\leftrightarrow}B,B\vdash A\overset{K_{AB}}{\leftrightarrow}B$.

Z 协议的初始假定集合 α 是标准的,这里不再赘述.

Z 协议的理想化模型如下:

$Z2$ $B\rightarrow S$: $\{N_A\}_{K_{AS}},\{N_B\}_{K_{BS}}$

$Z3$ $S\rightarrow A$: $\{A\overset{K_{AB}}{\leftrightarrow}B\}_{K_{AS}},\ \{N_A,N_B,\{A\overset{K_{AB}}{\leftrightarrow}B,N_B\}_{K_{BS}}\}_{K_{AB}}$

$Z4$ $A\rightarrow B$: $\{A\overset{K_{AB}}{\leftrightarrow}B,N_B\}_{K_{BS}},\{N_B\}_{K_{AB}}$.

如前,$Z1$ 被省略了,因为它不影响 BAN 逻辑的分析结果.

以下是 BAN 逻辑的推理过程.

由 $Z2$ 可以推出 $S \models A \overset{K_{AS}}{\leftrightarrow} N_A, S \models B \overset{K_{BS}}{\leftrightarrow} N_B$.

为了顺利进行下面的逻辑推理,我们对 BAN 逻辑作如下扩展. 设 $F_K(X,Y,\ldots)$ 是具有下述性质的函数:当且仅当知道密钥 K 时,容易计算出 $(X,Y,\ldots)$. 我们增加如下的 BAN 逻辑公设:

$$\frac{P \models P \overset{K}{\leftrightarrow} Q, P \lhd F_K(X,Y,\ldots)}{P \models Q \sim (X,Y,\ldots)}$$

在 $Z3$ 中,我们有 $F_{K_{AS}}(A \overset{K_{AB}}{\leftrightarrow} B, N_A, \ldots) = \{A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{AS}}, \{N_A, \ldots\}_{K_{AB}}$. 因此可以推出

$$A \models S \sim (A \overset{K_{AB}}{\leftrightarrow} B, N_A, \ldots).$$

结合初设 $A \models \#(N_A)$,进而有 $A \models S \models (A \overset{K_{AB}}{\leftrightarrow} B, N_A, \ldots)$ 及 $A \models S \models A \overset{K_{AB}}{\leftrightarrow} B$.

最后,通过初设 $A \models S \Rightarrow A \overset{K}{\leftrightarrow} B$ 可以得到 $A \models A \overset{K_{AB}}{\leftrightarrow} B$.

由 $Z4$ 可以依次推出

$B \models S \sim (A \overset{K_{AB}}{\leftrightarrow} B, N_B)$　　$B \models S \models (A \overset{K_{AB}}{\leftrightarrow} B, N_B)$　　$B \models S \models A \overset{K_{AB}}{\leftrightarrow} B$　　$B \models A \overset{K_{AB}}{\leftrightarrow} B$.

因此,Z 协议的最终目标集合 $\Gamma = \{A \models A \overset{K_{AB}}{\leftrightarrow} B, B \models A \overset{K_{AB}}{\leftrightarrow} B\} = \gamma$.

然而,这个经 BAN 逻辑证明正确的认证协议却存在一个重大的安全缺陷,即它不能承受"报文重发型"的攻击.

假设攻击者 C 存储一条旧报文 $\{K_{AB}, B\}_{K_{AS}}$,并从中破译旧的会话密钥 K_{AB}. 于是,C 对 Z 协议的攻击过程如下.

$Z1$　$A \rightarrow C$: $A, \{N_A, A\}_{K_{AS}}$

说明:C 冒充 B,截获 A 发给 B 的报文 $Z1$.

$Z2$　$C \rightarrow S$: $C, A, \{N_C, C\}_{K_{CS}}, \{N_A, A\}_{K_{AS}}$

说明:C 冒充 A,似乎 C 要求与 A 通信,发报文 $C, \{N_C, C\}_{K_{CS}}$ 给 A. 然后,A 按照协议发报文 $Z2$ 给 S. 这里,C 看不懂截获的 $\{N_A, A\}_{K_{AS}}$ 的内容,只是照原样转发罢了.

$Z3$　$S \rightarrow C$: $\{K_{CA}, A\}_{K_{CS}}, \{N_C, N_A, \{K_{CA}, C, N_A\}_{K_{AS}}\}_{K_{CA}}$

说明:S 误认为是主体 C,A 和 S 之间的正常通信,故根据协议发报文 $Z3$ 给 C.

$Z3'$　$C \rightarrow A$: $\{K_{AB}, B\}_{K_{AS}}, \{N_A, N_C, * * *\}_{K_{AB}}$

说明:C 冒充 S,似乎 S 收到 B 发送的报文后,发以上报文 $Z3'$ 给 A. 值得注意的是:(1) $\{K_{AB}, B\}_{K_{AS}}$ 是 C 存储的旧报文;(2) $* * *$ 可为任何值,因为 $* * *$ 的内容本身对 C 已无关紧要. 但是,$* * *$ 的字符串长度必须遵守协议的规定;(3) 由于 C 通过密码分析已掌握 K_{AB},故 C 可发报文 $\{N_A, N_C, * * *\}_{K_{AB}}$.

$Z4$　$A \rightarrow C$: $\{* * *\}_{K_{BS}}, \{N_C\}_{K_{AB}}$

说明:C 冒充 B,截获 A 根据正常协议发给 B 的报文 $Z4$.

如此,攻击者 C 成功地使 A 相信,A 已经通过 Z 认证协议得到新的一轮会话密钥 K_{AB}. 此后,C 就可以无所顾虑地冒充 B,利用 K_{AB} 和 A 进一步通信,盗取其中的机密了.

显然，BAN 逻辑分析在什么地方出了毛病. 我们认为，这不是形式化分析的过错，毛病出自理想化过程. BAN 逻辑缺乏一种形式化(或符号化)的理想化方法，更无法判断理想协议模型中信息的完整性. 我们只需稍作修改，下述 Z 协议就变得安全了.

$\overline{Z1}$ $A\rightarrow B$: $A,\{N_A,B\}_{K_{AS}}$ $\overline{Z2}$ $B\rightarrow S$: $A,B,\{N_A,B\}_{K_{AS}},\{N_B,B\}_{K_{BS}}$

$\overline{Z3}$ $S\rightarrow A$: $\{K_{AB},B\}_{K_{AS}},\{N_A,N_B,\{K_{AB},A,N_B\}_{K_{BS}}\}_{K_{AB}}$

$\overline{Z4}$ $A\rightarrow B$: $\{K_{AB},A,N_B\}_{K_{BS}},\{N_B\}_{K_{AB}}$

注意到，Z 协议中由 A 经 B 发给 S 的加密信息$\{N_A,A\}_{K_{AS}}$，在 $\overline{Z}$ 协议中变成了$\{N_A,B\}_{K_{AS}}$，只此一点改动而已. 然而，这就是认证协议是否安全的关键. 后者建立了 A 的临时值 N_A 与 A 的通信对象 B 之间的完整性连接，使上述攻击方法不再奏效.

我们提醒读者，上述变更丝毫不影响 BAN 逻辑的分析过程. Z 协议的最终目标集合 $\Gamma=\{A\models A\overset{K_{AB}}{\leftrightarrow}B,B\models A\overset{K_{AB}}{\leftrightarrow}B\}$可以完全相同地推导出来.

5 失败的例子 2

另一个失败的例子是下述使用数字签名的协议 W:

$W1$ $A\rightarrow B$: N_A $W2$ $B\rightarrow A$: $N_B,T_1,\{N_B,N_A,A,T_2\}_{K_B^{-1}}$

$W3$ $A\rightarrow B$: $N'_A,T_3,\{N'_A,N_B,B,T_4\}_{K_A^{-1}}$

其中$\{***\}_{K^{-1}}$表示对 $***$ 进行数字签名.

W 协议与前面的协议不同，它只涉及 2 个主体 A 和 B. 我们假定，A 和 B 分别拥有一对加密(公开)和签名(秘密)密钥 K_A 和 K_A^{-1} 及 K_B 和 K_B^{-1}，并使用相同的数字签名算法，例如 RSA. 我们还假定，数字签名是通过单向杂凑函数 $H(X)$实现的. 所谓单向函数系指，由 X 计算 $H(X)$是计算上容易的，反之由 $H(X)$计算 X 是计算上困难的. 因此，主体 A 对数据项 X 的数字签名$\{X\}_{K_A^{-1}}$应理解为$\{H(X)\}_{K_A^{-1}}$. 同理，我们在校验数字签名$(X,\{X\}_{K_A^{-1}})$时，实际上是校验 $H(X)$与$\{\{H(X)\}_{K_A^{-1}}\}_{K_A}$是否相等. 最后假定，$A$ 和 B 分别拥有对方的公开密钥 K_B 和 K_A.

在 W 协议中，T_1,T_2,T_3 和 T_4 是数据串. 它们的作用是，在相互认证的过程中可以同时实现密钥交换或其它秘密交换. 此外，在某些场合，这些数据串还可以用来传送其它数据信息，例如对报文进行认证校验. 为了进行校验，数据串就必须同时在明文信息和签名信息中出现. 我们很自然地产生疑问，为什么在 W 协议中，T_1 和 T_2 以及 T_3 和 T_4，是不同的数据串呢? 答案是如果令 $T_1=T_2,T_3=T_4$，上述认证协议会面临严重的安全问题. 当然，为了保证合法用户能够校验数字签名的正确性，必须有一种系统的方法使合法用户可以重新构造 T_2(以及 T_4)，使 T_1 和 T_2(以及 T_3 和 T_4)之间可以进行比较.

最后我们注意到，对未经加密的密钥(例如 T_2)进行数字签名，不会冒泄露该密钥的风险. 因为，我们已经假定在进行数字签名之前，所有的数据串都要经过单向杂凑函数的处理.

下面，我们对 W 协议进行 BAN 逻辑分析.

初始假设集合 α 是

$A\models\overset{K_A}{\rightarrow}A$, $B\models\overset{K_B}{\rightarrow}B$, $A\models\overset{K_B}{\rightarrow}B$, $B\models\overset{K_A}{\rightarrow}A$, $A\models B\triangleleft T_2$, $B\models A\triangleleft T_4$, $A\models\#(N_A)$, $B\models\#(N_B)$.

W 协议的理想化模型(不考虑 $W1$)是

$W2$　$B\rightarrow A$: $\{N_B,N_A,T_2\}_{K_B^{-1}}$　　$W3$　$A\rightarrow B$: $\{N'_A,N_B,T_4\}_{K_A^{-1}}$

W 协议的预期目标集合是 $\gamma=\{A\models T_2,B\models T_4,A\models B\models T_2,B\models A\models T_4\}$. 即通过协议 A 和 B 分别得到秘密 T_2 和 T_4,并相互验证对方的存在.

对 W 协议的 BAN 逻辑分析过程如下:

由 $W2$ 可以依次推得

$A\models B\sim(N_B,N_A,T_2)$　　$A\models B\models(N_B,N_A,T_2)$　　$A\models B\models T_2$　　$A\models T_2$.

类似地,由 $W3$ 可以推导出 $B\models A\models T_4$,$B\models T_4$.

因此,$\Gamma=\{A\models T_2,B\models T_4,A\models B\models T_2,B\models A\models T_4\}=\gamma$,故 W 协议可行.

这个经 BAN 逻辑分析认为正确的认证协议也存在重大的安全缺陷. 攻击者 C 对 W 协议的攻击过程如下:

$W1$　$C\rightarrow B$: N_C

说明: C 冒充 A,生成临时值 N_C 后发送给 B,要求与 B 通信.

$W2$　$B\rightarrow C$: $N_B,T_1,\{N_B,N_C,A,T_2\}_{K_B^{-1}}$

说明: B 认为是 A 和 B 之间的正常通信,根据协议发报文 $W2$ 给 C(B 认为 C 是 A).

$W1'$　$C\rightarrow A$: N_B

说明: C 利用刚从 B 收到的 N_B,冒充 B 请求与 A 通信.

$W2'$　$A\rightarrow C$: $N'_A,T'_1,\{N'_A,N_B,B,T'_2\}_{K_A^{-1}}$

说明: A 认为是 B 和 A 之间的正常通信,根据协议发报文 $W2'$ 给 C(A 认为 C 是 B).

$W3$　$C\rightarrow B$: $N'_A,T'_1,\{N'_A,N_B,B,T'_2\}_{K_A^{-1}}$

说明: C 利用刚从 A 收到的报文 $W2'$,原封不动地当成 $W3$ 发给 B,冒充 A 与 B 通信. B 收到 $W3$ 后,相信他和 A 之间进行了一次正常的协议通信.

与上一个例子不同,这次毛病出在认证协议中 $W2$ 与 $W3$ 的格式完全相同,使攻击者 C 有了可乘之机. 因此,对 $W3$ 作如下改动即可万事大吉.

$W3$　$A\rightarrow B$: $N'_A,T_3,\{N'_A,N_A,N_B,B,T_4\}_{K_A^{-1}}$

类似于上一个例子,BAN 逻辑的分析推理并无不妥之处. 毛病仍然出在理想化过程,即 BAN 逻辑机制无法察觉由 2 条格式相同的报文所引起的安全漏洞.

6　结　论

BAN 逻辑自问世以来,作为分析认证协议行之有效的形式化工具受到广泛关注. 人们在充分肯定 BAN 逻辑的价值的同时,也针对它的局限性和缺点作了各种形式的补充和扩展[5~6],我们通称它们为 BAN 类逻辑,然而 BAN 类逻辑仍然无法解决我们在本文中提出的安全问题. 因此,出路只有 2 条. 第 1,进一步改进 BAN 逻辑. 我们认为,改进的方向是:(1) 使理想化过程形式化或符号化;(2) 研究一种新的逻辑分析方法,取消理想化步骤;(3) 在语法分析的同时进行语义分析. 第 2,研究制定认证协议的设计原则. 我们认为这些原则至少应当包括:(1) 确定基本假定集合. 例如,杂凑函数无冲突,主体是诚实的等等. 注意一定要显式地说明,切忌作隐含的假设;(2) 认证协议的非形式化描述一定要简明,各主体的功

能尽量单一，避免复杂化，影响对协议的形式化分析；(3) 列出可能的攻击形式，对协议进行模拟攻击实验；(4) 避免报文格式相同，相关报文之间保持完整性联系，不提供相同的明文密文对，防止“已知明文”的攻击；(5) 利用 BAN 类逻辑对协议进行形式化分析，其推理结果作为改进协议设计的参考. 我们将按上述方向继续工作，有关研究成果另文发表.

参考文献

1 Needham R, Schroeder M. Using encryption for authentication in large networks of computers. C. ACM, 1978, 21 (12): 993～999.

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

3 Gong L, Needham R, Yahalom R. Reasoning about belief in cryptographic protocols. Proc. 1990 IEEE Symp. Security and Privacy, 1990. 234～248.

4 Abadi M. Tuttle M. A semantics for a logic of authentication. Proc. of 10th ACM Symp. on Principles of Distributed Computing, 1991. 201～216.

5 Oorshot P. Extending cryptographic logics of belief to key agreement protocols. Proc. of 1st ACM Conf. on Computer and Communications Security. 1993. 232～243.

6 Syverson P, Oorshot P. On unifying some cryptographic protocol logics. Proc. 1994 IEEE Symp. Security and Privacy, 1994.

FORMAL ANALYSIS OF AUTHENTICATION PROTOCOLS

Qing Sihan

(*Institute of Software The Chinese Academy of Sciences Beijing* 100080)

Abstract The design of authentication protocols is notoriously error—prone. ISO has been working on a variety of authentication protocols standards for some years. This paper explores the approaches to formal analysis of authentication protocols using BAN logic and points out that the BAN logic analysis does not always lead to correct outcome. Finally, this paper discusses the design principles of authentication protocols and the future directions for improvements of the BAN logic.

Key words Authentication, authentication protocol, BAN logic, cryptographic algorithm, hash function, digital signature.