高技术通讯 2010 年 第 20 卷 第 11 期:1108 ~ 1114

doi:10.3772/j.issn.1002-0470.2010.11.002

基于 BAN 逻辑的 SIP 网络认证协议安全性研究①

张兆心② 杜跃进 方滨兴 张宏莉

(哈尔滨工业大学 国家计算机网络与信息安全重点实验室 哈尔滨 150001)

摘 要 利用 BAN 逻辑对会话初始化协议(SIP)网络采用的超文本传输协议(HTTP)摘要认证协议进行了形式化分析和推导。通过严格的逻辑推导,证明 HTTP 摘要认证协议存在不足,以及由此产生的伪装攻击。通过对逻辑推理结果和推导过程的分析,针对 BAN 逻辑提出增加消息抗否认性规则和消息新鲜性传递规则,增强了 BAN 逻辑的逻辑推理能力;针对 HTTP 摘要认证协议提出增加数字签名、公私钥机制、双向认证和密钥协商,提高了 HTTP 摘要认证协议的安全性。

关键词 BAN 逻辑,SIP,HTTP 摘要认证协议,双向认证

0 引 言

在 IP 电话通信网络中,协议安全是整个网络安全的基础,尤其是通信协议的安全。但设计一个符合安全目标的安全通信协议非常困难。一方面安全目标难以明确表述,另一方面协议本身非常复杂,这就使协议的缺陷和漏洞很难被发现。近 20 年来形式化[1]分析方法的采用,发现了协议中以前从未发现的缺陷[2,3],使得这种方法正引起越来越多的关注。在各种形式化分析方法中,基于知识和信仰的模态逻辑方法简单、实用、抽象度高,可以揭示安全协议中的安全缺陷和冗余性,在安全协议验证方面获得了广泛的应用。这一方法所用的 BAN[4] 逻辑成果一项开拓性的成果。BAN 逻辑成功地对 Needham-Schroeder[5],Kerberos 等几个著名的协议进行了分析,找到了其中已知和未知的漏洞。在 BAN 逻辑基础上发展起来的 GNY 逻辑、AT 逻辑、VO 逻辑和 SVO 逻辑等,均是对 BAN 逻辑的扩展[6]。目前,尚未有对会话初始化协议(session initiation protocol, SIP)[7]网络中认证协议的安全性进行分析的文献。本文采用 BAN 逻辑对 SIP 网络中认证协议进行形式化,并对其认证过程进行逻辑推导。通过严格的逻辑推导,证明了超文本传输协议(HTTP)摘要[8]认证协议存在不足,以及由不足产生的伪装攻击。通过对逻辑推导结果和过程的分析,本文针对 BAN 逻辑提出增加消息抗否认性规则和消息新鲜性传递规则,增强了 BAN 逻辑的功能;针对 HTTP 摘要认证协议提出增加采用数字签名[9]、公私钥[10]、双向认证和密钥协商,提高了认证协议安全性,拓展了认证协议的功能。

1 BAN 逻辑

基于推理结构性方法主要是运用逻辑系统从用户接收和发送的消息出发,通过一系列的推理规则和初始假设推证协议是否满足其安全目标。

1.1 基本术语

下面列出了 BAN 逻辑中常用的逻辑符号:

(1) P,Q:主体(principal),指参与协议的各方;

(2) X:观点(formula statement)指协议中的消息;

(3) K:密钥;

(4) $\{X\}_K$:X 用密钥 K 加密;

(5) $\langle X\rangle_Y$:消息 X 和密钥 Y 的级联,Y 的出现证明了使用消息 $\langle X\rangle_Y$ 的主体的身份;

(6) $p \xrightarrow{X} Q$:主体 P 发送消息 X 给 Q;

(7) $P|\equiv X$:P 相信 X;

(8) $P \lhd X$:P 看见过 X;

(9) $P|\sim X$:P 曾经说过 X;

(10) $P|\Rightarrow X$:P 对 X 具有仲裁权;

(11) $\propto (X)$:X 是新鲜的;

① 863 计划(2006AA01Z451,2007AA010503)资助项目。

② 男,1979 年生,博士,副教授;研究方向:计算机网络安全,VoIP 网络安全;联系人,E-mail:heart@hit.edu.cn

(收稿日期:2009-09-07)

(12) $P \xleftarrow{K} Q$: K 是 P,Q 的共享密钥;

(13) $P \xleftarrow{GK} Q$: K 是 P,Q 的良好会话密钥;

(14) $\left|\xrightarrow{K} P\right.$: K 是 P 的公钥;

(15) $P \overset{X}{\rightleftharpoons} Q$: X 是 P,Q 的共享秘密。

1.2 推理规则

BAN 逻辑共有 16 条逻辑规则,分为 7 个小的方面,包括消息意义规则、随机数验证规则、仲裁规则、信仰规则、接收规则、新鲜规则和传递规则。下面列出一些常用的规则。

(1)消息意义规则

该规则的作用是从加密消息所使用的密钥以及消息中包含的秘密来判断发送者的身份(假设 P 和 Q 为不同的主体)。

对于公钥,有

$$P \mid \equiv (P \xrightarrow{GK} Q) \text{ and } P \lhd \{X\}_K \Rightarrow P \mid \equiv (Q \mid \sim X) \quad \text{(规则 1-1)}$$

对于私钥,有

$$P \mid \equiv (\left|\xrightarrow{K} Q\right.) \text{ and } P \lhd \{X\}_K^{-1} \Rightarrow P \mid \equiv (Q \mid \sim X) \quad \text{(规则 1-2)}$$

对于共享秘密,有

$$P \mid \equiv (P \xrightarrow{Y} Q) \text{ and } P \lhd \langle X \rangle_Y \Rightarrow P \mid \equiv (Q \mid \sim X) \quad \text{(规则 1-3)}$$

这三条推理规则表明如果收到一条加密消息,那么只有拥有此加密密钥(或密钥的逆)或非密钥的秘密信息的主体才能够发送这条消息。

(2)仲裁规则

仲裁规则进一步拓展了主体的推知能力,使主体可以在基于其他主体已有的信仰之上推知新的信仰,即

$$P \mid \equiv (Q \mid \Rightarrow X) \text{ and } P \mid \equiv (Q \mid \equiv X) \Rightarrow P \mid \equiv X \quad \text{(规则 2)}$$

此规则表明:如果 P 相信 Q 对 X 是有仲裁权的,并且 P 相信 Q 相信 X,那么 P 相信 X。

(3)新鲜规则

$$P \mid \equiv (\propto (X)) \Rightarrow P \mid \equiv (\propto (X,Y)) \quad \text{(规则 3-1)}$$

$$P \mid \equiv (\propto (X)) \text{ and } P \mid \equiv (Q \mid \sim X) \Rightarrow P \mid \equiv (Q \mid \equiv X) \quad \text{(规则 3-2)}$$

此规则表明:如果 P 相信 X 是新鲜的,那么 P 相信与 X 级联的整个消息也是新鲜的。如果 P 相信 X 是新鲜的,并且 P 相信 Q 曾发送过 X,那么 P 相信 Q 相信 X。

(4)传递规则

$$P \mid \equiv (Q \mid \sim (X,Y)) \Rightarrow P \mid \equiv (Q \mid \sim X) \quad \text{(规则 4)}$$

此规则表明:如果 P 相信 Q 曾发送过整个消息,那么 P 相信 Q 曾发送过消息的子部分。

1.3 基于的假设

BAN 逻辑有三个假设:

(1) 时间假设

协议分析中区分两个时间:past-time 和 current-time。current-time 起始于本次协议运行的开始阶段,而在此之前都是 past-time。如果某一观点在协议开始时是成立的,那么在整个 current-time 中也是成立的,但是在 past-time 中成立的观点在 current-time 中却不一定成立。采用时间区分可以防止消息的重放攻击。

(2) 密钥假设

不拥有适当的密钥则不能解密用此密钥生成的密文,密钥不能从密文中推导出来。

(3) 主体假设

参与协议的主体都是诚实的。

1.4 分析步骤

采用 BAN 逻辑对协议进行分析的一般步骤如下:

(1) 根据 BAN 逻辑的表示方法,对分析目标进行形式化;

(2) 确定安全目标和初始假设,并用逻辑符号表示出来;

(3) 根据逻辑推理规则和初始假设,对各个消息进行推理,若能推出安全目标,则在该方法下是安全的,否则,是不安全的;

(4) 根据推理过程,分析缺陷和冗余性。

2 认证协议的安全性分析

SIP 协议中的认证采用 HTTP 摘要认证方式,摘要认证机制基于挑战/应答方式,应答中包含一个有效的校验和(checksum),即摘要。假定客户方和服务器都知道一个有权使用资源的用户名和密码,当客户方第一次申请资源时,若未提供合适的认证,服务器将在响应中指明一个特有值 nonce。客户方收到 nonce 后,产生一个新的请求,请求头中包括 Digest username,realm,nonce,uri 和 response 消息,其中,response 是对服务器发送 nonce 的响应,是由用户秘密信息和 nonce 杂凑产生的一个 32 位十六进制数编码的摘录值。当服务器再次收到请求时,用同样的

杂凑函数计算出摘录值 response，与请求中的 response 相比，若完全相同，就表明身份已经证实有效。其流程如图 1 所示。

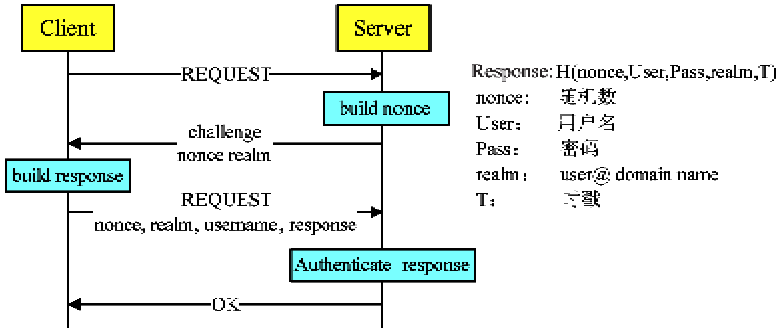

图 1 HTTP 摘要认证协议

由于在 nonce 中加入了时间戳和 uri，使不同时间片中的 nonce 不同，中间窃听者即使原封不动地把 response 照抄下来，也会因时间已过期而不能得逞，即使窃听者能够准确地改回系统时间，也只能访问由 Etag 标识的某一文档，而不能访问其它文档。

2.1 协议形式化

根据 BAN 逻辑对协议的一般分析方法，假设所有的消息都在收到消息后$\triangle T$时间内发出，则 HTTP 摘要认证协议形式化定义如下：

$$A \xrightarrow[X_1]{\Delta T} B:\{A,B,X_1\}$$

$$B \xrightarrow[X_2]{\Delta T} A:\{A,B,X_2,\{T,E_{tag},K_{BS}\}_H\}$$

$$A \xrightarrow[X_3]{\Delta T} B:\ \{A,B,X_3,\ \{U_{ser},P_{ass},R_{ealm},U_{ri},nonce\}_H\}$$

$$B \xrightarrow[X_4]{\Delta T} A:\{A,B,X_4\}$$

2.2 安全目标

BAN 逻辑中安全目标一般形式如下：

$$P|\equiv X, Q|\equiv X, P|\equiv (Q|\equiv X)$$

HTTP 摘要认证协议的最终目的就是认证消息发送者的身份，根据认证协议的目的，其安全目标如下：

(1) $B|\equiv (A \xrightarrow{X_1} B)$

(2) $B|\equiv (A \xrightarrow{X_3} B)$

(3) $A|\equiv (B \xrightarrow{X_2} A)$

(4) $A|\equiv (B \xrightarrow{X_4} A)$

(5) $A|\equiv (\propto (X_2)), B|\equiv (\propto (X_3))$

2.3 初始假设

HTTP 摘要认证协议的基础包含如下三点：(1)认证双方使用的加密算法——H；(2)认证双方的共享秘密——用户密码 K_{AB}；(3)消息的新鲜性——时戳 T。根据以上分析假设如下：

(1) $A|\equiv (A \overset{K_{AB}}{\rightleftharpoons} B), B|\equiv (A \overset{K_{AB}}{\rightleftharpoons} B)$

(2) $B|\equiv (\propto (X_2)), B|\equiv (\propto (X_4)),$
$A|\equiv (\propto (X_1)), A|\equiv (\propto (X_3))$

(3) $A|\Rightarrow (X_1, X_3), B|\Rightarrow (X_2, X_4)$

(4) $A|\equiv (B|\Rightarrow (X_2, X_4)),$
$B|\equiv (A|\Rightarrow (X_1, X_3))$

因为用户 A 密码 K_{AB} 只有 A 与 B 知晓，所以 A 与 B 相信 K_{AB} 是 A 与 B 的共享秘密，即假设条件 1 成立；因为消息 X_1 和 X_3 是由 A 构造发出的，消息 X_2 和 X_4 是由 B 构造发出的，所以 A 相信消息 X_1 和 X_3 是新鲜的，B 相信消息 X_2 和 X_4 是新鲜的；A 对消息 X_1 和 X_3 有仲裁权，B 对消息 X_2 和 X_4 有仲裁权；A 相信 B 对消息 X_2 和 X_4 有仲裁权，B 相信 A 对消息 X_1 和 X_3 有仲裁权。即假设 2,3 和 4 都成立。

2.4 规则拓展

BAN 逻辑的推理能力具有一定的应用范围，有时需要根据具体需求，如待分析的协议，拓展 BAN 逻辑的推理规则，以加强 BAN 逻辑的推理能力。根据 SIP 网络认证协议的特点在此提出两组规则的拓展：消息发送者身份确认规则和消息新鲜性传递规则。

(1)消息抗否认性规则：

在 SIP 网络的认证过程中存在许多信息的交互过程，但 BAN 逻辑并没有给出如何确认消息发送者身份的规则。如 $A \xrightarrow{X} B$，这条形式化语言表示 A 发送消息 X 给 B，但存在岐义。如消息 X 的发送者

不一定是A,消息 X 的接受者不一定是B,或者 B 不是消息的唯一接受者。因此结合 SIP 网络认证协议的特点,需要对消息发送者身份确认,在此提出消息抗否认性规则,规则如下:

$$B\mid\equiv(X)\ \text{and}\ A\xrightarrow{\langle X:\{X_i\}_{K_{PA}^{-1}}\rangle_{K_{AB}}}B\ \text{and}\ B\equiv(A\overset{K_{AB}}{\rightleftharpoons}B)\Rightarrow B\mid\equiv(A\xrightarrow{X}B)$$

(规则 5-1)

$$B\mid\equiv(X)\ \text{and}\ A\xrightarrow{\{X:\{X_i\}_{K_{PA}^{-1}}\}_{PK_{AB}}}B\ \text{and}\ B\equiv(A\xleftarrow{PK_{AB}}B)\Rightarrow B\mid\equiv(A\xrightarrow{X}B)$$

(规则 5-2)

$$B\mid\equiv(X)\ \text{and}\ A\xrightarrow{\{X:\{X_i\}_{K_{PA}^{-1}}\}_{K_{PB}}}B\ \text{and}\ B\equiv(\mid\xrightarrow{K_{PA}}A)\Rightarrow B\mid\equiv(A\xrightarrow{X}B)$$

(规则 5-3)

此规则表明,如果 A 发送消息 X 给 B,B 相信消息 X,且消息 X 中含有采用 A 的私钥加密的部分消息,整个消息 X 使用共享秘密 K_{AB} 或良好会话密钥 PK_{AB} 或 B 的公钥 K_{PB} 加密,B 相信 K_{AB} 是 A 和 B 的共享秘密或 PK_{AB} 是 A 和 B 的良好会话密钥或 K_{PA} 是 A 的公钥,则 B 相信 A 发送消息 X 给 B。但这有一个前提,就是只有拥有这个私有秘密的主体才能发送含有此私有秘密的消息。

(2)消息新鲜性传递规则

消息的新鲜性规则主要是为证明消息的新鲜性,防止消息的重放攻击。有时消息的新鲜性存在着传递关系,而 BAN 逻辑中并不存在这种推理规则。因此结合 SIP 消息的传递机制增加消息新鲜性传递规则:

$$A\mid\equiv(\propto(x))\ \text{and}\ A\xrightarrow{\Delta T}{\scriptstyle X}B\Rightarrow B\mid\equiv(\propto(X))$$

(规则 6)

此规则表明,如果 A 在时刻 T 认为消息 X 是新鲜的,并且 A 在时刻 T 将消息 X 发送给 B,则 B 认为消息 X 在 $T+\triangle T$ 时间内是新鲜的,其中$\triangle T$ 由用户给出。

2.5 推导过程

根据初始假设和推理规则分别对各个安全目标进行推导。

对于安全目标(5):

$$B\mid\equiv(\propto(X_2))\ \text{and}\ B\xrightarrow{\Delta T}{\scriptstyle X_2}A\Rightarrow A\mid\equiv(\propto(X_2))$$

由规则 6 得

$$A\mid\equiv(\propto(X_3))\ \text{and}\ A\xrightarrow{\Delta T}{\scriptstyle X_3}B\Rightarrow B\mid\equiv(\propto(X_3))$$

由规则 6 得

采用新鲜规则,可以有效地防止消息重放攻击。

对于安全目标(2):

$$B\mid\equiv(A\overset{K_{AB}}{\rightleftharpoons}B)\ \text{and}\ B\lhd\langle X_3\rangle_{K_{AB}}\Rightarrow B\mid\equiv(A\mid\sim X_3)$$

由规则 1-3 得

$$A\mid\equiv(\propto(X_3))\ \text{and}\ A\xrightarrow{\Delta T}{\scriptstyle X_3}B\Rightarrow B\mid\equiv(\propto(X_3))$$

由规则 6 得

$$B\mid\equiv(\propto(X_3))\ \text{and}\ B\mid\equiv(A\mid\sim X_3)\Rightarrow B\mid\equiv(A\mid\equiv X_3)$$

由规则 3-2 得

$$B\mid\equiv(A\mid\Rightarrow X_3)\ \text{and}\ B\mid\equiv(A\mid\equiv X_3)\Rightarrow B\mid\equiv X_3$$

由规则 2 得

通过推理可以看出,由于消息 X_3 中不含有其发送者 A 的秘密 K_{SA},因而无法根据规则 5 推出安全目标。并且如果生成应答 response 中时间 T 的作用域过长,那么攻击者 C 窃听了 A 与 B 的通信,在 A 与 B 结束通话后,C 在时间 T 内就可以伪装 A 重新发出请求。即存在伪装 A 的攻击方式,攻击如下:

$$C\xrightarrow{\Delta T}{\scriptstyle X_1}B:\{A,B,X_1\}$$

$$B\xrightarrow{\Delta T}{\scriptstyle X_2}C:\{A,B,X_2,\{T,E_{tag},K_{BS}\}_{H}\}$$

$$C\xrightarrow{\Delta T}{\scriptstyle X_3}B:\{A,B,X_3,\{U_{ser},P_{ass},R_{ealm},U_{ri},nonce\}_{H}\}$$

$$B\xrightarrow{\Delta T}{\scriptstyle X_4}C:\{A,B,X_4\}$$

以安全目标(2)为例,在 T 时间内,进行如下推导:

$$B\mid\equiv(A\overset{K_{AB}}{\rightleftharpoons}B)\ \text{and}\ B\lhd\langle X_3\rangle_{K_{AB}}\Rightarrow B\mid\equiv(A\mid\sim X_3)$$

由规则 1-3 得

推导结果说明,B 相信 A 发送过消息 X_3。但实际上 X_3 是攻击者 C 伪造 A 发出的。

对于安全目标(3):

由于服务器 B 给客户端 A 发送的挑战中虽然含有自己的秘密,但无法用此秘密证明消息发送者的身份,且其传输的内容不含有 A 与 B 的共享秘密或共享密钥或 B 的私钥,所以无法根据规则 1 推出 A 相信 B 发送过消息 X_2。因而 A 无法判断消息 X_2 是否由 B 发送给他,这就存在伪装 B 的攻击方式。同理于安全目标(1)与(4)。如果攻击者 D 窃听了 A 与 B 之间的通信,由于不存在 A 对 B 的认证,那

么存在伪造 B 的如下攻击方式：

$$A \xrightarrow[X_1]{\Delta T} D:\{A,B,X_1\}$$

$$D \xrightarrow[X_2]{\Delta T} A:\{A,B,X_2,\{T,E_{tag},K_{BS}\}_H\}$$

$$A \xrightarrow[X_3]{\Delta T} D:\ \{A,B,X_3,\ \{U_{ser},P_{ass},R_{ealm},U_{ri},nonce\}_H\}$$

$$D \xrightarrow[X_4]{\Delta T} A:\{A,B,X_4\}$$

攻击者 D 不验证 A 的身份，收到消息 X_3 之后，直接发送消息 X_4 给 A。但是 A 并不知道，在 A 看来，攻击者是在与 B 进行通信。如下推导：

$$D \mid \equiv (\propto (X_2)) \text{ and } D \xrightarrow[X_2]{\Delta T} A \Rightarrow$$

$$A \mid \equiv (\propto (X_2)) \qquad \text{由规则 6 得}$$

$$D \mid \equiv (\propto (X_4)) \text{ and } D \xrightarrow[X_4]{\Delta T} A \Rightarrow$$

$$A \mid \equiv (\propto (X_4)) \qquad \text{由规则 6 得}$$

推导结果说明 A 相信消息 X_2 和 X_4 是新鲜的，并且 A 认为消息 X_2 和 X_4 是 B 发出的，但实际上消息 X_2 和 X_4 是攻击者 D 发出的。

2.6 改进

由以上分析可以看出，存在这些安全隐患的根本原因在于认证的单向性与消息发送者身份的无法确认。如增加公钥私钥机制与数字签名结合双方的共享秘密，就可以有效地证明消息发送者的身份，实现双向认证。此外，在认证的过程中，可利用共享秘密进行密钥协商，为通信过程建立密钥，提高通信的安全性。设 K_{PA} 与 K_{PB} 分别表示 A，B 的公钥，K_{SA} 与 K_{SB} 分别表示 A，B 的数字签名，并且通信的双方都存有自己的公私钥与对方的公钥，$B_{challenge}$ 和 $B_{response}$ 分别表示 B 发起的挑战及根据 B 的挑战产生的应答，同理与 $A_{challenge}$ 和 $A_{response}$，$A_{encrypt}$ 表示 A 支持的加密方法，E_M 表示协商后的加密方法。修改后的 HTTP 摘要认证协议如下：

(1) 客户端首先将数据包进行 HASH，然后采用私钥对 HASH 值签名得到 K_{SA}，接着采用 K_{PB} 加密 HASH 值，最后将签名和加密后的数据写入数据包，并发送给服务器端。

(2) 服务器端收到客户端的请求，首先依次验证签名和 HASH 值，如果通过服务器端生成 $B_{challenge}$，然后将含有 $B_{challenge}$ 的数据包进行 HASH，接着采用私钥对 HASH 值签名得到 K_{SB}，采用 K_{PA} 加密 HASH 值，最后将数据依次写入数据包，并发送给客户端。

(3) 客户端收到服务器端的应答，首先依次验证签名和 HASH 值，如果通过客户端生成 $B_{response}$，并生成 $A_{challenge}$，然后将含有 $B_{response}$、$A_{challenge}$ 和 $A_{encrypt}$ 的数据包进行 HASH，接着采用私钥对 HASH 值签名得到 K_{SA}，采用 K_{PB} 加密 HASH 值，最后将数据依次写入数据包，并发送给服务器端。

(4) 服务器端收到客户端的回应，首先依次验证签名和 HASH 值，如果通过服务器端生成 $A_{response}$，然后选择 E_M，并将含有 $A_{response}$ 和 E_M 的数据包进行 HASH，接着采用私钥对 HASH 值签名得到 K_{SB}，采用 K_{PA} 加密 HASH 值，最后将数据依次写入数据包，并发送给客户端。

整个流程如图 2 所示。

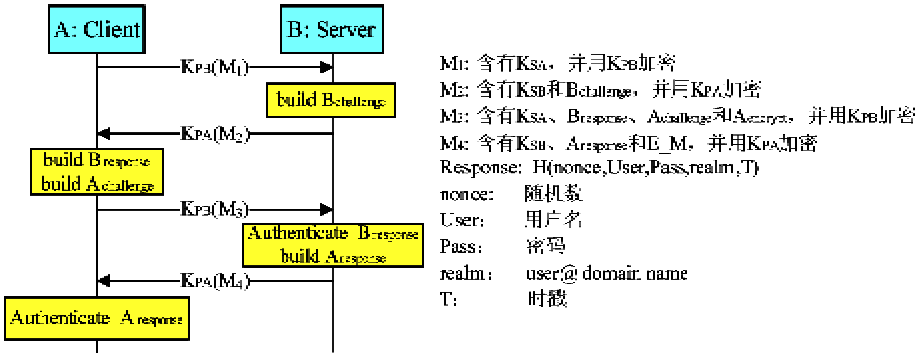

图 2 改进后的 HTTP 摘要认证协议

在此有一点需要说明，客户端和服务器端的公私钥可借助 PKI 体系结构进行分发[11]，这部分内容不是本文研究的重点，故在此忽略。

采用 BAN 逻辑，对改进后的 HTTP 摘要认证协议所设立的安全目标进行形式化分析和推导。改进前后安全目标并未发生变化，但需要增加如下假设：

B 相信 K_{PA} 是 A 的公钥;A 相信 K_{PB} 是 B 的公钥,即

$$B\mid\equiv(\mid\xrightarrow{K_{PA}}A),A\mid\equiv(\mid\xrightarrow{K_{PB}}B)$$

推导过程如下:

对于安全目标(1):

$B\mid\equiv(\mid\xrightarrow{K_{PA}}A)$ and $B\lhd\{X_1\}_{K_{PA}^{-1}}\Rightarrow$

$B\mid\equiv(A\mid\sim X_1)$ 由规则 1-2 得

$A\mid\equiv(\propto(X_1))$ and $A\xrightarrow[X_1]{\Delta T}B\Rightarrow$

$B\mid\equiv(\propto(X_1))$ 由规则 6 得

$B\mid\equiv(\propto(X_1))$ and $B\mid\equiv(A\mid\sim X_1)\Rightarrow$

$B\mid\equiv(A\mid\equiv X_1)$ 由规则 3-2 得

$B\mid\equiv(A\mid\Rightarrow X_1)$ and $B\mid\equiv(A\mid\equiv X_1)\Rightarrow$

$B\mid\equiv X_1$ 由规则 2 得

$B\mid\equiv X_1$ and $A\xrightarrow{\{X_1,\{X_i\}_{K_{PA}^{-1}}\}_{K_{PB}}}B$ and

$B\mid\equiv(\mid\xrightarrow{K_{PA}}A)\Rightarrow B\mid\equiv(A\xrightarrow{X_1}B)$

由规则 5-3 得

对于安全目标(3):

$A\mid\equiv(\mid\xrightarrow{K_{PB}}B)$ and $A\lhd\{X_2\}_{K_{PB}^{-1}}\Rightarrow$

$A\mid\equiv(B\mid\sim X_2)$ 由规则 1-2 得

$B\mid\equiv(\propto(X_2))$ and $B\xrightarrow[X_2]{\Delta T}A\Rightarrow$

$A\mid\equiv(\propto(X_2))$ 由规则 6 得

$A\mid\equiv(\propto(X_2))$ and $A\mid\equiv(B\mid\sim X_2)\Rightarrow$

$A\mid\equiv(B\mid\equiv X_2)$ 由规则 5-2 得

$A\mid\equiv(B\mid\Rightarrow X_2)$ and

$A\mid\equiv(B\mid\equiv X_2)\Rightarrow A\mid\equiv X_2$ 由规则 2 得

$A\mid\equiv X_2$ and $B\xrightarrow{\{X_2,\{X_i\}_{K_{PB}^{-1}}\}_{K_{PA}}}A$ and

$A\mid\equiv(\mid\xrightarrow{K_{PB}}B)\Rightarrow A\mid\equiv(B\xrightarrow{X_2}A)$

由规则 5-3 得

同理,对于安全目标(2)与安全目标(4):增加公私钥机制,攻击者因信息被加密,无法直接通过监听获得会话信息;因增加双向认证,无法实现伪装。

2.7 推导结论

通过以上分析可知,在没有增加数字签名、公私钥机制与双向认证之前,下述三点是肯定的:

(1) 安全目标(1),(3)和(4)无法通过以上规则和初始假设推出。并且推导过程中可推出存在伪装 A 或伪装 B 的攻击。

(2) 安全目标(2)仅能推出 B 相信消息 X_3,却无法推出 A 是消息 X_3 的发送者,即 A 发送消息 X_3 给 B,并且 B 可能不是消息 X_3 的唯一接受者。

(3) SIP 的认证协议中采用的加密方式为 MD5,方法过于单一。因而可能存在伪造信息或窃取信息的攻击方式。

当增加数字签名、公私钥机制和双向认证后,利用初始假设和推理规则可推出全部的安全目标。

根据以上分析和推导过程及推导结论,可对认证协议作如下五点改进:

(1) 交互的个体增加数字签名,利用签名可证明消息发送者的身份,防止伪装攻击。

(2) 采用公私钥机制,以有效防止窃听或伪装攻击。

(3) 利用数字签名和公私钥实现双向认证。

(4) 认证过程中增加密钥协商,通过密钥协商确定认证后通信过程中使用的加密方法,提高通信过程的安全性,防止窃听攻击。

(5) 根据实际情况缩短时间 T 的作用域。

3 结论

IP 电话成为多媒体业务发展的一次革命,IP 电话随着应用的日益广泛,其安全性也日益受到重视。本文采用 BAN 逻辑对 SIP 网络中的 HTTP 摘要认证协议进行了严格的逻辑推导,推导的结果与推导过程证明该认证协议存在多点不足,如无法确认消息发送者身份,存在伪装攻击、窃听攻击,加密方法过于简单。根据以上分析,本文针对 BAN 逻辑提出增加消息抗否认性规则和消息新鲜性传递规则,增强了 BAN 逻辑的功能;针对 HTTP 摘要认证协议提出增加数字签名、公私钥、双向认证和密钥协商,提高了认证协议安全性,拓展了认证协议的功能。改进后协议的效率拟采用模拟的方式进行验证,提高协议的效率是下一步研究的目标。

参考文献

[1] 薛锐, 冯登国. 安全协议的形式化分析技术与方法. 计算机学报, 2006, 29(1):1-20

[2] LOWE G. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. *Software-Concepts and Tools*, 1996, 1055(17):93-102

[3] 王英龙, 王继志, 王美琴. 基于 BAN 逻辑的 ad hoc 移动网络路由协议的安全性分析. 通信学报, 2005, 26(4):125-129

[4] Burrows M, Abadi M, Needham R. A logic of authentication. *ACM Transactions in Computer systems*, 1990, 8(1):18-36

[5] Bruce Schneier 著. 吴世忠等译. 应用密码学. 北京:机械工业出版社, 2000-01,41-42,44

[6] 卿斯汉. 安全协议 20 年研究进展. 软件学报, 2003, 14(10):1740-1752

[7] Rosenberg J, Schulzrinne H, Camanilo G. SIP: Session initiation protocol. Internet RFC 3261, 2002

[8] HTTP authentication: Basic and digest access authentication. Internet RFC 2617,1999

[9] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 1978, 21: 120-126

[10] Hubaux J P, Buttyan L, Capkun S. Self-organized public-key management for mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 2003, 2(1):52-64

[11] Khalili A, Katz J, Arbaugh W A. Towards secure key distribution in truly ad-hoc networks. In: Proceedings of the 13th IEEE Workshop on Security and Assurance in Ad hoc Networks, Orlando, USA, 2003. 342-346

Research on authentication protocol security for SIP networks based on BAN logic

Zhang Zhaoxin, Du Yuejin, Fang Binxing, Zhang Hongli

(Research Center of Computer Network and Information Security Technology, Harbin Institute of Technology, Harbin 150001)

Abstract

The formalized analysis and deduction of the HTTP digest authentication protocol used in session initiation protocol (SIP) networks were conducted by using the BAN logic. The limitations in the HTTP digest authentication protocol and the impersonation attacks caused by the limitations were verified through the strict logic ratiocination. Based on the result of the logic ratiocination and the analysis of the ratiocination process, the message identity validating rule and the message novelty transfer rule were added to the BAN logic, and the ability for logic deduction of the BAN logic was improved. The measures of digital signature, public and private key, two-way authentication, and key negotiation were added to the HTTP Digest authentication protocol, and the security of the protocol was enhanced.

Key words: BAN logic, SIP, HTTP digest authentication protocol, two-way authentication