第 33 卷 第 3 期 计 算 机 工 程 2007 年 2 月
Vol.33 No.3 Computer Engineering February 2007
·安全技术· 文章编号：1000—3428(2007)03—0157—03 文献标识码：A 中图分类号：TP301.6;TP309

一类群组注册协议的设计及其 BAN 逻辑演绎

陆正福，刘吉庆
(云南大学数学系，昆明 650091)

摘 要：MIKEY 是一种可应用于实时的、多媒体通信的群组注册协议的规范。该文分析了 MIKEY 规范中的密钥生成、分发机制，设计了一个符合 MIKEY 规范、基于公钥的群组注册协议，最后应用 BAN 逻辑分析了该协议的安全性。
关键词：MIKEY；密钥管理；注册协议；BAN 逻辑

Design of A Class of Group Registration Protocol and Its BAN Logic Deduction

LU Zhengfu, LIU Jiqing
(Department of Mathematics, Yunnan University, Kunming 650091)

【Abstract】MIKEY is a protocol specification for group registration protocol that can be used for real-time multimedia applications. This paper analyzes the key generation, distribution mechanisms of MIKEY, designs a group registration protocol, MIKEY-PKGRP, based on the public-key mode and MIKEY specification. Finally, it analyzes the security of MIKEY-PKGRP with BAN logic deduction.
【Key words】MIKEY; Key management; Registration protocol; BAN logic

群组安全的核心问题是组密钥管理。文献[1]将组密钥管理结构化地分解为群组注册协议和组密钥更新协议等部分。文献[2]给出了MIKEY(涉及群组通信中初期密钥和其它安全参数的生成和分发)，它属于群组注册协议的范畴。本文基于文献[1,2]分析了MIKEY规范中的密钥生成、分发机制，参照文献[6,7]设计了符合MIKEY规范、基于公钥的群组注册协议，并应用BAN逻辑[3~5]分析了该协议的安全性。

1 MIKEY 的非形式化分析

MIKEY支持基于Internet的一对一、一对多、小规模多对多的交互组等模式。其当前版本[2]基于SRTP。MIKEY定义了与安全协议有关的名词术语：(1) 秘密会话(CS)：由SRTP、IPsec等安全协议承载的单向或双向的数据流。秘密会话集(CSB)：拥有共同TGK等安全参数的秘密会话的全体；(2)TEK，属于会话密钥范畴的数据加密密钥；(3)TGK：TEK生成密钥。TGK是一些由CSB内一方或多方协商形成的位，用于生成认证密钥、TEK等密钥。MIKEY建立CSB及生成TEK的过程如下：(1)通过规定的机制协商TGK等安全参数。MIKEY支持同时为多个安全协议提供密钥和安全参数；(2)为不同的CS生成不同的TEK；(3)TEK及其它一些安全参数作为安全协议的输入参数，来保护CS中的数据流。安全协议可直接使用TEK，也可利用TEK再生成新的会话密钥，这取决于安全协议本身。

MIKEY 规定了安全参数的分发、密钥的生成、协议数据单元的构成等。对 CSB 的更新只是重新执行分发过程。MIKEY 支持 3 种密钥传输/交换方式：预分配，公钥，DH 密钥协商(为选项)。其中的公钥方式适用于大规模的组通信，故下节给出一类基于公钥的群组注册协议的设计。

2 一类基于公钥的群组注册协议的设计

结合文献[1,6]，给出一类符合 MIKEY 规范、基于公钥的群组注册协议的设计，将其简记为 MIKEY-PKGRP。协议设计的前提假设为：(1)GCKS(组控制器/密钥服务器)是可信的，可以是独立的第三方，也可以由发送者兼任；(2)TGK 由 GCKS 生成；(3)基于公钥证书来认证身份；(4)各协议数据单元的构成遵循 MIKEY 规范。

MIKEY-PKGRP的功能目标是：基于公钥方式、通过GCKS、群组用户获得初始的TGK，其消息交互的时序如图 1 所示。步骤如下：(1)用户U_i申请加入一个秘密会话(CS)，发送加入请求和数字证书给GCKS，并用GCKS的公钥加密；(2)GCKS收到加入请求，用自己的私钥解密，将U_i的证书交给认证中心CA验证；(3)CA发送验证结果给GCKS；(4)若U_i未通过验证，则GCKS发送拒绝消息给U_i；若U_i通过验证，则GCKS发送密钥给U_i；(5)若GCKS设定消息需要回复，则U_i发送接收确认消息。

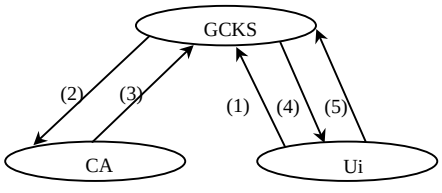

图 1 公钥方式的分发过程

MIKEY-PKGRP 协议数据单元 PDU 的设计参考了文献[2]的第 6 部分：Payload Encoding。该部分以 SRTP 为安全协议，

基金项目：国家自然科学基金资助项目(10561009)；云南省自然科学基金资助项目(2002F0012M)；云南大学理(工)科校级科研重点项目(2003Z010C)；云南大学中青年骨干教师培养计划专项经费资助项目
作者简介：陆正福(1965－)，男，副教授，主研方向：信息安全，协议工程，网络计算等；刘吉庆，硕士生
收稿日期：2006-02-23 **E-mail：**zhflu@ynu.edu.cn

定义了有关的交互消息所形成的负荷编码。负荷编码采用了灵活、可扩展的链式结构，以 next payload 指示字段加以链接。其中最核心的负荷类型是公共头部负荷：HDR，以 HDR 中的 next payload 字段指示其它字段，包括 KEMAC(1，密钥数据传输，可以受 AES/SHA 的保护)、PKE(2，公钥信封数据)、DH(3，DH 数据)、SIGN(4，签名)、T(5，时间戳)、ID(6，标识)、CERT(7，证书)、CHASH(8，证书的散列函数与函数值)、V(9，验证消息－MAC 算法与验证数据)、SP(10，安全策略集)、RAND(11，伪随机位串)、ERR(12，错误指示)、Key Data(20，密钥数据)、General Ext(21，一般扩展)、Last payload(0，指示无后继负荷)。这些已经定义的负荷编码，几乎涵盖了注册协议中可能涉及到的各种类型的负荷，并留有扩展余地。限于篇幅，不能给出所有 PDU 的详细设计，给出消息(1)的 PDU 作为一个示例如图 2 所示。

00000001 00000111 00000110 00000000
00000000 00000000 00000000 00000001
00000001 00000000 00000000 00000000
00000110 00000000 00000000 00010000
二进制的 Ui 的 ID 数据(16B，占 4 行)
00000111 00000000 00000000 00010000
二进制的 GCKS 的 ID 数据(16B，占 4 行)
00010101 00000000 00000000 00000101
二进制的证书数据(5B，占 2 行)
00000000 00000000 00000000 00001000
二进制的公钥数据(8B，占 2 行)

图 2 消息(1)的 PDU 示例

各行分别解释如下：第 1 行的前 8 位表示协议版本为 1，紧接的 8 位表示该消息是用户注册消息，再接下来的 8 位表示下一载荷是ID载荷，后续的 1 位表示发送方是否需要接收方的验证响应消息。最后的 7 位表示密钥生成要采用的伪随机函数。第 2 行为秘密会话集标识。第 3 行的前 8 位表示秘密会话编号，接下来的 8 位表示从秘密会话到安全协议会话唯一的映射，后面的 16 位表明秘密会话需要创建的安全关联。第 4 行前 8 位表示紧接着的下一载荷是ID载荷，接下来的 8 位表示ID类型为URI，最后 16 位表示后续的ID的长度(此处为 16B)。第 5 至第 8 行为U_i的ID(共 16B)。第 9 行前 8 位表示紧接着的下一载荷是CERT证书载荷，接下来的 8 位表示ID类型为URI。后面 16 位表示此ID的长度为 16B。第 10 至第 13 行即为GCKS的ID(共 16B)。

第 14 行前 8 位表示紧接着的下一载荷是承载公钥数据的扩展载荷，接下来的 8 位表示使用的证书类型是 X.509v3，接下来的 16 位表示证书数据的长度为 5B。接下来的两行中，第 1 行和第 2 行前 8 位是二进制的证书数据，其余位为 0。

第 17 行前 8 位表示这一载荷为最后载荷，接下来的 8 位表示使用 RSA 的公钥，接下来的 16 位表示证书数据的长度为 8B。接下来的 2 行是二进制的公钥数据。

从上述负荷可以看出，MIKEY-PKGRP 除了涉及 MIKEY 规范，还涉及其它规范，如 X.509、OCSP 及算法类的规范等。

3 MIKEY-PKGRP 的 BAN 逻辑分析

本节应用 BAN 逻辑考察 MIKEY-PKGRP 的安全性。BAN 逻辑是一类属于信念逻辑范畴的方法，有自己的表达式和推理规则。

3.1 表达式与推理规则

3.1.1 表达式

设 P、Q 表示主体，X 表示消息。

(1)P believes X:表示P相信X是真实的；(2)P sees X:表示P看见X，如P收到含有X的信息；(3)P said X:表示P曾说过X，如P发送过X；(4)P controls X:表示P对X有控制权，如P能生成随机性很好的密钥；(5) fresh(X):表示X是新鲜的；(6) $P \xleftrightarrow{K} Q$:表示K是P和Q之间的通信密钥；(7)$\{X\}_k$:表示用k作为密钥来加密X。

3.1.2 推理规则

规则 1 P believes ($P \xleftrightarrow{K} Q$), P sees $\{X\}_k$, then P believes(Q said X)。

规则 2 P believes (Q has public key K), P sees $\{X\}_k^{-1}$, then P believes(Q said X)。

规则 3 P believes fresh(X), P believes (Q said X), then P believes(Q believes X)。

规则 4 P believes (Q controls X), P believes (Q believes X), then P believes X。

规则 5 P believes fresh(X), then P believes fresh(X,Y)。

规则 6 P believes (P has public key K), P sees $\{X\}_K$, then P sees X。

其中规则 1、规则 2 称为消息意义规则，规则 3 称为随机数验证规则，规则 4~规则 6 称为裁判规则。规则的详细解释可参见文献[3~5,7]。

3.2 BAN 逻辑分析协议的基本过程

运用BAN逻辑分析协议的安全性，涉及的基本过程如下：(1)通过非形式化分析，弄清楚协议中消息的交互；(2)理想化，即用BAN逻辑表达式来表示消息；(3)给出有关协议的假设；(4)根据推理规则，证明协议；(5)得出结论。一般情况下，对于完整的认证协议，可以得出：P believes ($P \xleftrightarrow{K} Q$); Q believes ($P \xleftrightarrow{K} Q$)。有的协议还可进一步得出其它结论[3]。

3.3 MIKEY-PKGRP 协议的安全性分析

3.3.1 理想化

理想化是对协议中的消息传递抽象出必要的部分，形成形式化的模型。下面对公钥方式的密钥传输过程进行理想化。

X_ID表示X的标识，X_pk、X_k分别表示X的公钥和私钥，U_i_C是CA签发的U_i的数字证书，{M}k表示密钥k加密消息M。GCKS可作为sender。

消息(1) $U_i \rightarrow$GCKS:
{U_i_ID,CS_ID,U_i_C,U_i_pk}GCKS_pk
消息(2) GCKS→CA:
{GCKS_ID,U_i_ID,U_i_C}CA_pk
消息(3) CA→GCKS:
{{valid/invalid,U_i_ID}CA_k}GCKS_pk
消息(4) GCKS→U_i：

U_i未通过验证，发送错误消息。Error no表示错误号，当值为 8 时，表示不支持的证书(Invalid Cert)。消息头部的V字段用于标示发送方需不需要接收方的验证响应消息。V=1：需要；V=0：不需要。

{{Error no,CS_ID,T,}GCKS_k}U_i_pk
U_i通过验证，发送公钥方式密钥消息：
{{RAND,{TGK}encr_k,env_k,T}GCKS_k}U_i_pk
消息(5) $U_i \rightarrow$GCKS:

若需回复，则发送公钥方式的验证消息。其中 V 代表验证响应消息载荷。

{{U_i_ID,CS_ID,T,V}U_i_k}GCKS_pk

3.3.2 初始信任集

根据图 1，建立初始信任假设集如下：

假设(1)：U_i believes (U_i has public key U_i_pk)；假设(2)：GCKS believes (GCKS has public key GCKS_pk)；假设(3)：U_i believes (GCKS has public key GCKS_pk)；假设(4)：GCKS believes (CA has public key CA_pk)；假设(5)：GCKS believes CA controls (U_i has public key U_i_pk)； 假设(6)：U_i believes fresh(T)；假设(7)：U_i believes GCKS controls (GCKS $\xleftrightarrow{TEK}$ U_i) 假设(8)：GCKS believes fresh(U_i has public key U_i_pk) 。

假设(1)和假设(2)表示U_i和GCKS都相信它们拥有自己的公钥，假设(3)表示U_i相信GCKS有公钥GCKS_pk，假设(4)表示GCKS相信CA有公钥CA_pk，假设(5)表示GCKS相信CA能生成用户U_i的证书，假设(6)表示U_i相信时间戳T是新鲜的，假设(7)表示U_i相信GCKS与U_i共享的TEK是由GCKS生成的，假设(8)表示U_i的证书是新鲜的。

3.3.3 逻辑演绎过程

由消息(1)知：GCKS sees {{U_i has public key U_i_pk}CA_k}GCKS_pk；再由假设(2)，根据规则 6 得：GCKS sees {U_i has public key U_i_pk}CA_k；再由假设(4)，根据规则 2 得：GCKS believes CA said (U_i has public key U_i_pk)；再由假设(8)，根据规则(3)得：GCKS believes CA believes (U_i has public key U_i_pk)；再由假设(5)，根据规则 4 得：GCKS believes (U_i has public key U_i_pk)；若没有假设(8)，即U_i使用了过期、伪造等不合法的证书来进行通信，将不能通过CA的验证。如果没有假设U_i的证书是新鲜的，或者说如果U_i使用了已泄露密钥的证书来进行假冒通信的话，MIKEY将不能检测出来。

消息(2)是GCKS把用户U_i的证书交给CA验证，消息(3)是CA把验证结果告诉GCKS，我们假设U_i通过了验证。消息(4)中，U_i能够得到RAND和env_k等参数，有能力生成加密TGK的密钥encr_k；另外再加上参数RAND的配合，就可以生成TEK，故U_i接收到的消息可抽象为{{ GCKS $\xleftrightarrow{TEK}$ U_i,T}GCKS_k}U_i_pk。

由消息(4)知：

U_i sees {{GCKS $\xleftrightarrow{TEK}$ U_i,T}GCKS_k}U_i_pk

再由假设(1)，根据规则 6 得：

U_i sees { GCKS $\xleftrightarrow{TEK}$ U_i,T}GCKS_k

再由假设(3)，根据规则 2 得：

U_i believes GCKS said (GCKS $\xleftrightarrow{TEK}$ U_i,T)--(*)

另外，由假设(6)，根据规则 5 得：

U_i believes fresh(GCKS $\xleftrightarrow{TEK}$ U_i,T)

则由(*)式，再根据规则 3 得：

U_i believes GCKS believes (GCKS $\xleftrightarrow{TEK}$ U_i)

由假设(7)，根据规则(4)得：

U_i believes (GCKS $\xleftrightarrow{TEK}$ U_i)

至此，得出结论：

U_i believes (GCKS $\xleftrightarrow{TEK}$ U_i)；

U_i believes GCKS believes (GCKS $\xleftrightarrow{TEK}$ U_i)，

即在密钥分发之后用户U_i相信TEK是GCKS和U_i之间通信的好密钥，并且U_i相信GCKS相信TEK是GCKS和U_i之间通信的好密钥。存在消息(5)时，根据规则(2)，GCKS believes U_i believes (U_i_ID,CS_ID,V)，即GCKS相信U_i相信已经收到密钥。

在这种密钥分发方式中，不能得出

GCKS believes (GCKS $\xleftrightarrow{TEK}$ U_i)；

GCKS believes U_i believes (GCKS $\xleftrightarrow{TEK}$ U_i)，

但在后续的通信中，如果GCKS收到了U_i的加了数据源认证和时间戳的TEK加密消息，GCKS就能确定上述两点。

4 结束语

本文设计了符合 MIKEY 规范的一类群组注册协议，并用 BAN 逻辑分析了协议的安全性。在 BAN 逻辑中，初始假设难以确定，理想化过程是非形式化的，它们对分析结果的正确性是有影响的。因此需要保证的是，协议的设计者和分析者应正确地建立初始信任集合，谨慎地进行非形式化的理想化过程，使用者应合理地选择应用环境。

参考文献

1 Baugher M, Canetti R, Dondeti L, et al. Multicast Security Group Key Management Architecture[S]. RFC4046, 2004.

2 Arkko J, Carrara E, Lindholm F. MIKEY: Multi-media Internet KEYing[S]. RFC3830, 2004.

3 Burrow M, Abadi M, Nneham R. A Logic of Authentication[J]. ACM Transaction in Computer System, 1990, 8(1): 18-36.

4 费定舟, 邓达强. 关于 BAN 逻辑的语义模型的分析与改进[J]. 计算机工程与应用, 2004, 40(15): 17-19,121.

5 王惠芳, 郭金庚. 用 BAN 逻辑方法分析 SSL3.0 协议[J]. 计算机工程, 2001, 27(11): 147-149.

6 陆正福, 叶 锐, 王国栋. 基于移动代理的多播水印协议[J]. 云南大学学报(自然科学版), 2004, 26(4): 306-311.

7 陆正福, 叶 锐, 王国栋. 多播水印协议 MAMWP 的 BAN 逻辑分析[J]. 云南大学学报(自然科学版), 2005, 27(1): 18-21.

（上接第 153 页）

参考文献

1 Gao Xingxin, Xiang Zhe, Wang Hao, et al. An Approach to Security and Privacy of RFID System for Supply Chain[C]//Proceedings of the IEEE International Conference on E-commerce Technology for Dynamic E-business, 2004.

2 Weis S A. Security and Privacy in Radio-frequency Identification Devices[D]. The Department of Electrical Engineering and Computer Science of MIT, 2003.

3 Weis S, Sarma S, Rivest R, et al. Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems[C]//Proc. of Security in Pervasive Computing '04, 2004: 201-212.

4 Ohkubo M, Suzuki K, Kinoshita S. Cryptographic Approach to "Privacy-Friendly" Tags[C]//Proc. of RFID Privacy Workshop, USA MIT, 2003.

5 Henrici D, Müller P. Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices Using Varying Identifiers[C]//Proceedings of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004.