文章编号:1001 - 9081(2009)06 - 1625 - 03

基于公钥的 3G 认证和密钥分配协议

万武南,索 望,陈 运
(成都信息工程学院 信息安全研究所, 成都 610225)
(nan_wwn@ hotmail. com)

摘 要:分析了 3G 认证与密钥协商协议(AKA)的过程和特点,指出了存在的缺陷,提出了一种新的 AKA 改进方案。该方案实现了移动设备(ME)和拜访位置寄存器(VLR)的相互认证,产生的会话密钥对双方都是公正的;该方法避免了双方必须通过资源有限的无线信道传送自己的公钥证书,几乎不需要可信赖第三方参与;同时解决了网络端信息传输的安全性。并对新方案的安全性进行了形式化分析,证明了该协议具有较强的实用性。

关键词:认证与密钥协商协议;3G 安全;认证协议;密钥分配
中图分类号: TP333 **文献标志码**:A

Authentication and key agreement of 3G mobile communication system based on public key

WAN Wu-nan, SUO Wang, CHEN Yun
(*Institute of Information Security, Chengdu University of Information Technology, Chengdu Sichuan* 610225, *China*)

Abstract: The shortcomings to 3G Authentication and Key Agreement (AKA) protocol were described through analyzing its procedure and security. An improved scheme of 3G authentication and key agreement protocol was proposed, which achieve authentication of Mobile Equipment (ME) to Visitor Location Register (VLR) and secure transfer of message between VLR to Home Location Register (HLR). The session key established by the protocol was fair for both side of communication without the third party involved. Finally, the formal analysis results of the improved scheme showed its good practicability.

Key words: Authentication and Key Agreement (AKA); 3G security; authentication protocol; key agreement

0 引言

在移动通信系统中,由于无线信道的公开性,安全问题一直是影响系统性能的关键因素之一,同时也是用户与营运商利益的重要保证。国际组织 3GPP(The Third Generation Partnership Project)在 2G 安全的基础上针对 3G 接入网提出了一系列的安全规范,但由于安全协议和密码体制方面的原因,系统的安全和性能存在如下缺陷[1-4]:

1)3G 信息的加密仍将采用固定的对称密码体制,没有安全灵活协商的途径,密钥产生算法的安全性取决于采用何种密码体制,可扩展性差且不能提供抗抵赖功能。

2)认证和密钥协商协议(Authentication and Key Agreement, AKA)协议中,用户开机注册或初次加入网络,或因特殊情况需要网络无法恢复出用户的 *IMSI*(国际移动用户标识)时,用户将以明文发送 *IMSI*,因而容易泄漏 *IMSI*,而使用户被追踪或遭受伪基站攻击。

3)拜访位置寄存器(Visiting Location Register, VLR)和归属位置寄存器(Home Location Register, HLR)之间的有线通信链路缺乏有效的保护。

4)用户漫游到不同地域时,*VLR* 和用户归属的 *HLR* 相距遥远,归属网络会把认证向量发送到漫游网络,因此认证向量的传输将增加网络负载,易被截获。

5)在 GSM 系统中,身份认证是单向的,基站能够验证用户的身份是否合法,而用户无法确认其所连接的服务网络是否可靠。只有移动设备(Mobile Equipment, ME)对归属环境(Home Environment, HE)和 *VLR* 对 *ME* 的认证,没有 *ME* 对 *VLR* 的认证。

针对上述缺陷,文献[3]在没有增加通讯次数的前提下,增加了 *HLR* 与 *VLR* 之间的共享密钥 K_{HV},实现了 *ME* 对 *VLR* 的认证的方案,但是仍未解决 *ME* 明文传送 *IMSI* 给 *VLR* 的问题,同时文章并没有给出密钥 K_{HV} 产生方法,并且基于对称密码体制的认证方案增加了密钥管理的复杂性,且不能提供防抵赖功能。文献[5]为了避免了从网络链路端泄漏密钥的危险,把认证向量加密。随着移动终端计算能力和存储量的增加,基于公钥体制的认证方法开始应用于 3G 接入安全中。文献[10]采用了在公钥环境下协商加密算法设计认证协议构架。文献[11]提出了基于自验证公钥的认证方案,该方案可使 *ME* 抵抗伪基站攻击并避免鉴别 *VLR* 证书的合法性;在无须传送公钥证书的前提下完成 *ME* 和 *VLR* 的相互认证及会话密钥协商,但是在该认证方案中,*IMSI* 在 *ME* 和 *VLR* 传送次数过多,容易泄露 *IMSI*,同时也未解决 *ME* 明文传送 *IMSI* 给 *VLR* 的问题。

在此基础上,本文提出了一种基于公钥的 AKA 协议,该方案能够满足协议中 *ME* 和 *VLR* 双方进行相互认证的要求,

收稿日期:2008 - 11 - 26;**修回日期**:2009 - 03 - 04。 **基金项目**:国家自然科学基金资助项目(60873216);四川省教育厅青年基金资助项目(07ZB012);现代通信国家重点实验室基金资助项目(9140C1101050705);四川省科技厅应用基础资助项目(2008JY0078);成都信息工程学院人才启动基金资助项目(KYTZ200706)。

作者简介:万武南(1978 -),女,博士,主要研究方向:信息安全、编码理论; 索望(1978 -),男,讲师,主要研究方向:信息安全、3G 通信;陈运(1958 -),女,教授,主要研究方向:密码理论、3G 通信。

避免了双方必须通过资源有限的无线信道传送自己的公钥证书,避免 *ME* 做繁重的签名运算,同时解决了网络端信息传输的安全性,并利用 *BAN* 逻辑对该协议进行形式化安全分析。

1 认证与密钥协商协议(AKA)描述

3G 认证协议(3GAKA) 中参与认证和密钥协商的主体有:用户终端(*ME/ USIM*)、访问网络(*VLR/ SGSN*) 和归属网络(*HE/ HLR*)。3GAKA 协议中,通过用户认证应答(*RES*) 实现 *VLR* 对 *ME* 的认证,通过消息认证码(*MAC*) 实现 *ME* 对 *HLR* 的认证,以及实现了 *ME* 与 *VLR* 之间的密钥分配,同时每次使用的消息认证码 *MAC* 是由不断递增的序列号(*SQN*) 作为其输入变量之一,保证了认证消息的新鲜性,从而确保密钥的新鲜性,有效地防止了重放攻击。3G 认证协议具体步骤如下(如图 1 所示)。

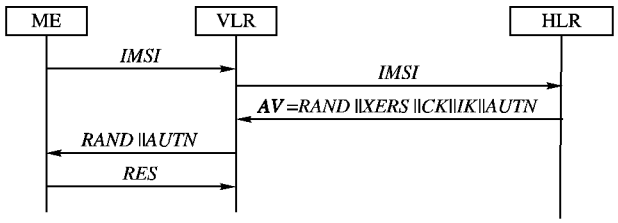

图 1 3G 认证和密钥协商过程(3GAKA)

1) 用户终端(*ME/ USIM*) 向网络发出位置更新或呼叫接入消息,传送用户永久身份认证标识(*IMSI*) 给 *VLR*。

2) *VLR* 收到移动用户的注册请求后,向用户的 *HLR* 发送该用户的永久用户身份标识,请求对该用户进行认证。

3) *HLR* 收到 *VLR* 的认证请求后,生成序列号 *SQN* 和随机数 *RAND*,计算认证向量 ***AV*** 发送给 *VLR*。

其中认证向量(***AV***) 产生方法如下: $\boldsymbol{AV} = RAND \| XRES \| CK \| IK \| AUTN$;*K* 为 *ME* 和 *HLR* 共同拥有的永久性密钥,写入在 *ME* 中的 *SIM* 卡中。各字段计算如下:$XRES = f2_K(RAND)$ 为期望的认证应答;$CK = f3_K(RAND)$ 为加密密钥;$IK = f4_K(RAND)$ 为完整性密钥;$AUTN = SQN \oplus AK \| AMF \| MAC$ 为认证令牌;*SQN* 为序列号;$AK = f5K(RAND)$ 为匿名密钥,用于隐藏序列号;*AMF* 为认证管理域;$MAC = f1_K(SQN \| RAND \| AMF)$ 为消息认证码。这里 *f1*,*f2* 是消息认证函数,*f1* 算法用于产生消息认证码,*f2* 算法用于消息认证中计算期望响应值。*f3*、*f4*、*f5* 是密钥生成函数,*f3* 算法用于产生加密密钥,*f4* 算法用于产生完整性密钥,*f5* 算法用于产生匿名密钥。

4) *VLR* 接收到认证向量后,将 *RAND* 及 *AUTN* 发送给 *ME*,请求用户产生认证数据。

5) *ME* 接收到认证请求后,首先计算 *XMAC*,并与 *AUTN* 中的 *MAC* 比较,若不同,则向 *VLR* 发送拒绝认证消息,并放弃该过程。同时 *ME* 验证接收到的 *SQN* 是否在有效的范围内,若不在有效的范围内,*MS* 则向 *VLR* 发送“同步失败” 消息,并放弃该过程。上述两项验证通过后,*ME* 计算 *RES*、*CK* 和 *IK*,并将 *RES* 发送给 *VLR*。

因为 *ME* 和 *HLR* 都预先知道相同的计算算法,因此 *XMAC* 和 *RES* 计算如下: 消息认证码 $XMAC = f1_K(SQN \| RAND \| AMF)$;用户认证应答 $RES = f2_K(RAND)$。

6) *VLR* 接收到来自 *MS* 的 *RES* 后,将 *RES* 与认证向量 ***AV*** 中的 *XRES* 进行比较,相同则认证成功,否则认证失败。

2 基于自验证公钥的认证和密钥分配协议

通过对3GAKA协议过程分析发现,该协议实现了 *VLR* 对 *MS* 以及 *MS* 对 *HLR* 的认证,而不要求 *MS* 对 *VLR* 进行认证,并且 *IMSI* 明文传送,攻击者可截获的合法用户身份标识。并且没有考虑到网络端的认证与保密通信,若攻击者对 *VLR* 与 *HLR* 之间的信息进行窃听,就可以获得 *HLR* 传给 *VLR* 的认证向量 ***AV***,从而可获得加密密钥 *CK* 与完整性密钥 *IK*。此时,攻击者再假冒该合法用户身份入网,即可实现正常的保密通信,合法用户传送的信息也就失去保密性。在综合考虑协议效率与安全性均衡的基础上,本文提出一种基于公钥的3G认证与密钥协商协议算法。在该协议中,引入可信认证中心(Certificate Authority, CA),*CA* 为 *ME*、*VLR* 和 *HLR* 颁发的公钥证书,系统中的移动用户 *ME* 和 *VLR* 都拥有一对由权威机构分配的公钥和私钥密钥对,并且 *ME*、*VLR* 和 *HLR* 共享:大素数 *p* 和有限域 *Gp* 上的生成元 *g*,*VLR* 和 *HLR* 预先约定的共享密钥 K_{HV}。

1) *ME* 随机选择 $u \in \mathbf{Z}_p^*$,计算 $x = g^u \bmod p$,然后发送:

$ME \rightarrow VLR: E_{PK_V}(x \| IMSI \| ID_v)$

2) *VLR* 用私钥 SK_V 进行解密,获得 *IMSI* 和 *x*,并用 *HLR* 和 *VLR* 的共享密钥 K_{HV} 加密 *IMSI* 加密发送给 *HLR*:

$VLR \rightarrow HLR: E_{K_{HV}}(IMSI)$

3) *HLR* 用共享密钥 K_{HV} 解密,根据 *IMSI* 到认证中心(*HE*) 认证 *ME* 的身份,得到认证之后,并计算生成序列号 *SQN* 和随机数 *RAND*,计算认证向量 $\boldsymbol{AV} = RAND \| XRES \| CK \| IK \| AUTN$,发送给 *VLR*:

$HLR \rightarrow VLR: E_{K_{HV}}(\boldsymbol{AV})$

4) *VLR* 用共享密钥解密得到认证向量 ***AV***,并产生随机数 $r, v \in \mathbf{Z}_p^*$ 和 *TMSI*,计算 $K = H_1(x^y \bmod p, r)$,计算 $y = g^v \bmod p$,$b = H_2(K, r, ID_v)$,随后发送 *ME*:

$VLE \rightarrow ME: E_K(RAND \| \boldsymbol{AV} \| b \| r) \| (y \oplus x')$,其中 x' 为 *x* 的低 128 比特。

5) *ME* 利用 *x* 可以获取到 *y*,然后计算 $K = H_1(y^u \bmod p, r)$,计算接收到的 *b* 是否与自己计算 $b = H_2(K, r, ID_v)$ 一致,若一致,则 *ME* 计算 *RES*,发送如下信息给 *VLR*:

$ME \rightarrow VLR: E_K(RES \oplus r')$

6) *VLR* 接收到来自 *ME* 的消息,利用共享密钥 *K* 进行解密,然后用随机数 *r*,恢复出 *RES* 后,将 *RES* 与认证向量 ***AV*** 中的 *XRES* 进行比较,相同则认证成功,否则认证失败。

3 协议的形式化安全性分析

AKA 协议为三方协议,包括用户终端(*ME/ USIM*)、访问网络(*VLR/ SGSN*) 和归属网络(*HE/ HLR*),其目的是保证三方的身份的相互认证。对改进协议进行形式化安全分析之前,原协议流程描述如下[3]:

1) $ME \rightarrow VLR: IMSI$。

2) $VLR \rightarrow HLR: IMSI$。

3) $HLR \rightarrow VLR: \boldsymbol{AV} = RAND \| XERS \| CK \| IK \| AUTN$。

4) $VLR \rightarrow ME: RAND \| \boldsymbol{AV}$。

5) $ME \rightarrow VLR: RES$。

从上述流程可以看出在,攻击者能够截获第 1 步发送的

信息,获取到 *IMSI*,然后冒充 *ME* 跟 *VLR* 进行密钥协商,然后攻击者截获第 4 步的消息,获取到 $RAND \parallel \boldsymbol{AV}$,然后冒充 *ME* 与 *VLR* 进行密钥协议。另外攻击者同时还能截获第 3 步,*HLR* 发送给 *VLR* 的信息,因为 *HLR* 与 *VLR* 之间是明文传送消息的。改进后的 *AKA* 协议的流程描述如下:

1) $ME \rightarrow VLR$: $E_{PK_V}(x \parallel IMSI \parallel ID_v)$。

2) $VLR \rightarrow HLR$: $E_{PK_H}(IMSI)$。

3) $HLR \rightarrow VLR$: $E_{PK_V}(\boldsymbol{AV})$。

4) $VLR \rightarrow ME$: $E_K(RAND \parallel \boldsymbol{AV} \parallel b \parallel r) \parallel (y \oplus x')$,其中 x' 为 x 的低 128 比特。

5) $ME \rightarrow VLR$: $E_K(RES \oplus r')$。

下面采用 *BAN* 逻辑对基于公钥的认证和密钥分配协议进行认证协议推理。*BAN* 逻辑是一种基于信念的模态逻辑,这一逻辑是一个抽象层次上分析系统中认证协议的安全问题。首先给出 *BAN* 逻辑的基本语法和规则。

1) *BAN* 逻辑语法[12]。

$P \lhd X$:P 收到包含 X 的信息。

$P \mid\sim X$:P 发送 X 信息,并且 P 发送 X 信息时相信 X。

$P \models X$:P 相信 X 是真的。

$P \Rightarrow X$:P 对 X 有控制权;P 是 X 的权威机构。

$\#(X)$:X 是新消息,在这次协议之前没有传送过。

$P \overset{K}{\longleftrightarrow} Q$:$P$ 和 Q 共享密钥 K 通信。

$\mid \overset{K}{\rightarrow} P$:$K$ 是 P 的公钥。

$\{X\}_K$:X 是用密钥 K 进行加密,K 可以是公钥密码也可以是对称密码。

2) *BAN* 逻辑使用的推导规则[12]。

a) *R*1: 若 $P \lhd \{X\}_K, P \models P \overset{K}{\longleftrightarrow} Q$,则 $P \models P \mid\sim X$。

b) *R*2: 若 $Q \lhd \{X\}_K, P \models \mid \overset{K}{\rightarrow} Q$ 或 $Q \models P \overset{K}{\longleftrightarrow} Q$,则 $Q \models P \mid\sim X$。

c) *R*3:若 $P \models Q \models X, P \models Q \Rightarrow X$,则 $P \models X$。

d) *R*4:若 $P \models Q \mid\sim X, P \models \#(X)$,则 $P \models Q \models X$。

e) *R*5:若 $P \models \#(X)$,则 $P \models \#(X, Y)$。

根据 *BAN* 逻辑的语法和规则,验证本文提出的基于公钥的认证和密钥协议实现了 *ME* 与 *VLR*,*ME* 与 *VLR* 之间的相互认证,同时三者之间消息传送的保密性。首先建立 *BAN* 逻辑的初始假设集合,包含如下假设:

a) 协议参与的主体为 *ME*、*VLR*、*HLR* 和 *CA* 四个主体。

b) 协议过程中用到的密钥有:SK_V、PK_V 为 *VLR* 私钥和公钥,K_{HV}、K_{MV} 分别为 *VLR* 和 *HLR*,*ME* 和 *VLR* 之间的共享密钥。

c) 协议中的随机变量包括 *RAND*、*SQR*,另外 x、r、y 和 b 为 *ME* 和 *VLR* 通过随机数产生的用于验证和生成 *HLR* 和 *ME* 的共享密钥的临时值。

d) *ME* 接收到的信息用 *BAN* 逻辑表示为:$ME \lhd \{RAND \parallel \boldsymbol{AV} \parallel b \parallel r\}_{K_{MV}}, y \oplus x'$。

e) *VLR* 接收到的信息用 *BAN* 逻辑表示为:$VLR \lhd \{x \parallel IMSI \parallel ID_v\}_{PK_V}, \{\boldsymbol{AV}\}_{K_{HV}}$。

f) *ME*、*VLR*、*HLR* 相互之间的密钥关系用 *BAN* 逻辑表示为:$VLR \models ME \overset{K_{MV}}{\longleftrightarrow} VLR; ME \models ME \overset{K_{MV}}{\longleftrightarrow} VLR; ME \models \#(x)$。

g) 信息的新鲜性用 *BAN* 逻辑表示为:$VLR \models \#(r)$, $VLR \models \#(y); VLR \models \#(b)$。

利用初始假设集合、*BAN* 逻辑的基本语法和推理,对 *ME* 与 *VLR* 之间的相互认证过程进行形式化分析和证明。下面给出 *ME* 对 *VLR* 认证的 *BAN* 逻辑证明过程。

$$\left.\begin{array}{l} VLR \lhd \{x \parallel IMSI \parallel IDV\}_{PK_V} \\ ME \models \mid \overset{PK_V}{\rightarrow} VLR \end{array}\right\} \overset{R_2}{\Rightarrow} VLR \models ME \models x \qquad (1)$$

根据上面 *BAN* 逻辑推理公式(1)可以得到 $VLR \models ME \models x$,即 *VLR* 相信接收到的 x 消息,*VLR* 相信由 x 计算的 *VLR* 和 *ME* 之间的共享密钥 K_{MV},即 $VLR \models VLR \overset{K_{MV}}{\longleftrightarrow} ME$;再根据 $ME \models ME \mid\sim x, ME \lhd y \oplus x'$($x'$ 为 x 的低 128 位)。因此可以推理出 $ME \models VLR \models y$,然后推理出 $ME \models VLR \overset{K_{MV}}{\longleftrightarrow} ME$,因此可以推理出公式(2):

$$\left.\begin{array}{l} ME \lhd \{RAND \parallel \boldsymbol{AV} \parallel b \parallel r\}_{K_{MV}} \\ ME \models ME \overset{K_{MV}}{\rightarrow} VLR \end{array}\right\} \overset{R_2}{\Rightarrow} ME \models VLR \models b \qquad (2)$$

根据式(2)可知 $ME \models VLR \models b$,若 *ME* 根据计算 $b = H_2(K, r, ID_v)$ 一致,则 *ME* 可以推理出 $ME \models VLR \models x$,即 *ME* 完成对 *VLR* 的认证。

通过上面的 *BAN* 逻辑证明,可以看出改进协议增加了 *ME* 对 *VLR* 的认证,并且 *ME* 对 *VLR* 的认证,并没有验证 *VLR* 的公钥书,但是 *ME* 通过验证 $b = H_2(K, r, ID_v)$,确信与其通信的 *VLR* 知道密钥 x,这样间接验证了 *VLR* 的身份,又减少了 *ME* 的计算量。同时改进协议还具有如下安全特性:

1) 改进方案中增加了 *HLR* PK_H 加密 *IMSI*,实现了 *HLR* 与 *VLR* 之间消息的加密传输,保证了传输信息的机密性,使得窃听者无法获得认证向量,从而防止了假冒 *VLR* 的攻击,同时 *ME* 与 *VLR* 之间的数据传送全部进行加密,保证了 *ME* 与 *VLR* 之间信息传送的机密性。

2) 在 *ME* 和 *VLR* 之间产生的会话密钥 K 得到了双方的确认,并且产生的会话密钥对双方都是公正的、新鲜的,会话密钥由 *ME* 产生的随机数 u 和 *VLR* 产生的随机数 r 共同决定,任何一方都不能单独产生会话密钥。

3) 在移动设备 *ME* 端只进行了一次公钥加密,计算两次签名,其余信息都采用了异或加密和对称加密机制减少移动设备的计算,提高性能。

4　结语

本文基于公钥密码体制对 3GAKA 协议进行了改进,该方案能够满足协议中 *ME* 和 *VLR* 双方进行相互认证的要求,该方法避免了双方必须通过资源有限的无线信道传送自己的公钥证书,避免 *ME* 做繁重的签名运算,同时解决了网络端信息传输的安全性。

参考文献:

[1] 李朔,李方伟,张蓉. 利用密钥更新改进的 3G 认证协议[J]. 现代电信科技,2005(6):45 - 47.

[2] 雷霆. 3G 认证与密钥分配协议的设计[J]. 系统安全,2004(5):33 - 35.

[3] 刘东苏,韦宝典,王新梅. 改进的 3G 认证与密钥分配协议[J]. 通信学报, 2002,23(5):119 - 122.　(下转第 1661 页)

送者)单方面生成用于通信的随机会话密钥,其安全性不高。这样的缺陷不满足密钥交换中的密钥控制安全性原则。

2)存在"非瞬间性"的缺陷。在混合加密体制中,能够强迫接受者出示其私钥的搭线窃听者,就能够恢复所有的有效信息。这个缺点称之为缺乏"前向保密安全性"。所谓前向保密性是指无论通过分析还是强迫,搭线窃听者都不可能由以前发送的密文在将来的时间恢复出明文消息。[9]

3　安全的 Diffie-Hellman 密钥交换协议

综上,提出了一种安全的 Diffie-Hellman 密钥交换协议,即混合加密方案的公钥密码部分采用 Diffie-Hellman 密钥交换协议,就能够克服这两个缺点。在 C 和 S 双方运行的 Diffie-Hellman 密钥交换协议中,共享的会话密钥 $K=g^{ab}$(g 为一个素阶群,a、b 为双方各输入的一个随机数,且满足 $g^a\neq1$,$g^b\neq1$)包含双方的随机输入,假设 C 输入的是 a,S 输入是 b,C(S)能够确信只要对方用了一个随机的整数,从 g^{ab} 推导的共享秘密会话密钥就是随机的。这是因为映射 $g^b\mapsto(g^b)^a$ 和 $g^a\mapsto(g^a)^b$ 在问题中是群的一个置换,所以均匀分布的指数(小于群的阶)把 $g^a(g^b)$ 映射为一个均匀分布的群元素 g^{ab}。这样就能保证生成的会话密钥具有随机性和公平性。使用 Diffie-Hellman 密钥交换协议的混合加密方案就具有前向保密性,会话密钥 g^{ab} 的生成是双方的随机指数生成的。即使一方的私钥泄露,也不能根据其私钥推断得到以前的会话密钥,因为每次的会话密钥中都包含了随机生成的信息,保证了新密钥与其他密钥之间的相互独立,提供了密钥独立性和安全前向保密性。为了谨慎地运行 Diffie-Hellman 密钥交换协议,C 和 S 应该在交换他们的会话密钥,并在协议完成后立即销毁 a 和 b,同时为了正确进行以后的会话通信,C 和 S 还应该在会话结束后销毁他们的会话密钥,并适当地处理他们所通信的明文消息。如果他们遵循这种相当标准的程序,显然强迫手段也不会使搭线窃听者得到 C 和 S 所通信的明文内容。由计算 DH 问题基于离散对数的困难性,此协议具有前向保密性,搭线窃听者的分析也不会成功[9]。并且,该方案还满足已知密钥安全性,即每一次密钥交换产生的密钥是不同的,当一次会话密钥泄露后,其他次产生的密钥不会因此而泄露。

结合上述思想将改进的 Kerberos 认证方案中流程的第 5、6 步改为:

C→S:ST, Authenticator_cc, EKc.s[EKRc(IDc,R,g^a)]

S→C :EKc.s[R3′, EKRs(R′,g^b,K)]

S 收到 C 的报文用 Kc.s 解密后,用 C 的公钥 KUc 验证 C 对 g^a 的签名——EKRc(g^a),若通过验证,S 利用 $K=g^{ab}$ 生成与 C 的两方会话密钥 $K=(g^a)^b$,再发给 C。

当 C 收到 S 的应答报文用 Kc.s 解密后,用 S 的公钥 KUs 验证 S 对 g^b 和两方会话密钥 K 的签名,若通过,C 同样利用 $K=g^{ab}$ 计算得到 $K'=(g^b)^a$,然后与 K 比较,如果相同则说明 K 即为他们间的会话密钥。由于会话密钥 K 每次都是随机产生的,每次皆可能不同,所以保证了一次一密的原则,增强安全性。到此为止,就可以实现 C 和 S 间两方的保密通信了,而 Kerberos 并不知道会话密钥 K 故无法窃听 C 和 S 间的通信内容,从而防止了 Kerberos 系统的内部攻击。

4　结语

改进后的 Kerberos 认证协议安全性较高,但还存在需要进一步完善的地方:该混合体制方案中采用的是 RSA 公钥加密体制和 DES 对称加密体制的组合。然而,采用 RSA 其加解密速度较慢,发送方传输前要加密两次,接收方收到后要解密两次。C 和 S 在使用共享密钥 Kc.s 进行加解密时采用的是 DES 对称加密方式,DES 本身的安全性也较弱。所以,为了提高系统的执行性能,可以考虑使用公钥加密体制中的 ECC(椭圆曲线加密体制)替代 RSA 和对称加密体制中的 AES(Rijndael 算法)替代 DES。还有,Kerberos 目前还不支持用户注册认证,只提供认证服务,至于系统内的访问权限和授权只有通过其他途径来解决。Kerberos 系统的客户之间的通信仍需要事先交换密钥,如果使用环境增大必然会加重网络的负担等。

参考文献:

[1] RFC1510, the kerberos network authentication service (V5) [S]. 1993.

[2] BELLOVIN S M, MERRITT M. Limitation of the Kerberos authentication system [J]. ACM SIGCOMM Computer Communication Review, 1990(5): 119 - 132.

[3] 许先斌,陈凡,苏剑. Kerberos 协议的改进和证明[J]. 计算机工程与应用,2002,38(8):157 - 158.

[4] 姚传茂. Kerberos 认证系统的研究与改进[J]. 安徽建筑工业学院学报:自然科学版,2006,14(2):85 - 87.

[5] 刘克龙,卿思汉,蒙杨. 一种利用公钥体制改进 Kerberos 的方法[J]. 软件学报,2001,12(6):872 - 877.

[6] 张红旗,车天伟,李娜. Kerberos 身份认证协议分析及改进[J]. 计算机应用,2002,(12):25 - 27.

[7] 汤卫东,李为民,周永权. 利用 ElGamal 算法改进 Kerberos 协议[J]. 计算机工程与设计,2006,27(11):2063 - 2065.

[8] 文铁华,谷士文. 增强 Kerberos 协议安全性的改进方案[J]. 通信学报,2004,25(6):76 - 79.

[9] 毛文波. 现代密码学——理论与实践[J]. 北京:电子工业出版社,2004.

(上接第 1627 页)

[4] 袁亚飞,廉玉忠. 3G 认证与密钥分发协议逻辑化分析[J]. 信息工程大学学报,2004,5(4):15 - 17.

[5] 田荣明,李方伟. 一种改进的密钥分配与认证协议[J]. 电讯技术,2004,44(2):68 - 71.

[6] 朱里奇,黄本雄. 3G 认证和密钥分配协议的形式化分析及改进[J]. 电子工程,2004,30(5):21 - 24.

[7] 郑宇,何大可,梅其祥. 基于自验证公钥的 3G 移动通信系统认证方案[J]. 计算机学报,2005,28(8):1327 - 1331.

[8] CHENG SHU - MIN, SHIEH SHIUH - PYNG, YANG WEN - HER. Designing authentication protocols for third generation mobile communication systems [J]. Journal of Information Science and Engineering, 2005,21(2):361 - 378.

[9] 刘锋. 第三代移动通信系统中认证和密钥协商协议的应用研究[D]. 重庆:重庆大学,2005.

[10] 姚惠明,隋爱芬,杨义先. 3GPP 网络 AKA 协议中若干算法的设计[J]. 北京邮电大学学报,2002,25(3):98 - 102.

[11] 刘佳潇,曾光,韩文报. 改进的 3G 认证与密钥协商协议[J]. 信息工程大学学报,2006,7(4):318 - 322.

[12] 杨士平,李祥. BAN 逻辑在协议分析中的密钥猜测分析缺陷[J]. 计算机工程,2006,32(9):126 - 127.