一个无线双向认证和密钥协商协议

邓所云,胡正名,钮心忻,杨义先
(北京邮电大学信息安全中心 126 信箱,100876 北京)

摘 要: 身份认证和密钥协商是无线通信中一个非常重要的安全问题. 本文提出了一个无线双向认证和密钥协商协议,解决了无线通信中的身份认证和密钥协商问题,并使移动网络系统向移动用户提供匿名服务,使得访问网络与非法窃听者无法获知用户的身份信息,保证了用户身份信息和所在位置信息的机密性,高效实用.

关键词: 双向认证; 匿名; 密钥协商; 无线通信; 协议
中图分类号: TP393 **文献标识码**: A **文章编号**: 0372-2112 (2003) 01-0135-04

A Wireless Mutual Authentication and Key Agreement Protocol

DENG Suo-yun, HU Zheng-ming, NIU Xin-xin, YANG Yi-xian
(*Information Security Center, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*)

Abstract: The problem of identity authentication and key agreement is a very important one about security in wireless communications. We propose a wireless mutual authentication and key agreement protocol to resolve this problem. In the protocol, a mobile user can be provided with anonymous service and neither Visited Networks nor wiretappers can get the information of the user's real identity, which guarantees the confidentiality of information of the user's identity and location. This protocol can achieve intended service in an efficient and practical way.

Key words: mutual authentication; anonymity; key agreement; wireless communications; protocol

1 引言

由于移动通信技术的迅速发展,移动通信及其相关应用得到越来越多的重视和推广. 对于移动用户和网络运营商来说,安全依然是其中至关重要的问题. 一旦通过安全手段建立呼叫,就可以利用已经部署好的安全系统提供相应的服务. 毫无疑问,作为呼叫建立过程的一部分,身份认证和密钥协商协议在其中扮演着举足轻重的角色;如果身份认证和密钥协商协议出现安全漏洞,整个会话就没有安全性可言,而且还会危及随后会话的安全性.

双向身份认证和密钥协商协议主要使移动用户和网络运营商能够相互认证对方的合法身份,并协商好会话密钥. 另外,在移动通信中,用户所在位置的信息如果泄漏,不法分子就可以跟踪用户的行踪,用户就没有隐私可言. 所以,用户所在位置的信息也应该得到保护.

2 基本标识符

本文采用如下标识符来描述协议:

$A \rightarrow B : X$: A 向 B 发送消息 X; TID_A: 实体 A 的临时身份标识符; $\{X\}_K$: 用对称密钥 K 对消息 X 进行加密得到的密文; K_{AB}: 在 A、B 之间共享的对称密钥; PK_A, SK_A: A 的公钥/私钥对; $\{X\}_{SK_A}$: 用 A 的私钥对 X 进行签名得到的签名信息; $Cert_A$: 对应于 A 的公钥的证书; M, H, V: 移动用户的真实身份标识、归属网络和访问网络; T_A: 由 A 产生的时间戳; h, h_1, h_2: 三个不同的 HASH 函数.

3 协议

3.1 安全需求

无线双向认证和密钥协商协议因为部署于移动通信环境之中,除了具有有线双向认证和密钥协商协议的安全需求之外,还提出了特殊的安全需求[1,2],如访问网络为用户提供匿名服务等. 我们主要考虑以下安全需求:

® 双向身份认证 指移动用户与网络之间相互认证身份,这是安全通信中最基本的安全需求. 第二代移动通信系统存在很多安全问题[3],其中之一就是缺少用户对移动网络的身份认证.

® 密钥协商和双向密钥控制 指用户与访问网络之间通过安全参数协商确定会话密钥,不能单独由一方确定,保证一次一密. 这一方面是为了防止由于一个旧的会话密钥泄漏而导致的重传攻击;另一方面也是为了防止由通信中的一方指定一特定会话密钥带来的安全隐患.

收稿日期:2001-07-02;修回日期:2002-04-12
基金项目:国家重点基础研究发展规划项目(No. G1999035805);国家杰出青年基金(No. 60073049);国家自然科学基金(No. 60073049)

® 双向密钥确认　移动用户与移动网络系统要进行相互确认,确保对方和自己拥有相同的会话密钥.

® 相关敏感数据的机密性　这特别适用于用户的身份信息,因为有些用户为了防止自己的所在位置信息和行踪泄漏,需要对自己的身份信息进行保护,即身份信息不能以明文形式在网络传输.

为了使移动网络系统为用户提供匿名服务,我们的协议采用临时身份标识符(TID),为了安全起见,TID 需要满足以下安全需求:

® 一次性使用.即用户与移动网络系统之间的每次安全过程都使用不同的 TID.

® TID 之间的不相关性.即用户的各个 TID 之间不存在明显的相关性,非法窃听者不能把他们关联起来,不能找到他们之间的联系.

® 域分离特性.即只要用户的归属网络不泄漏用户的真实身份信息,即使所有的访问网络联合起来,也不能获得用户的身份信息.

3.2　新的双向认证和密钥协商协议

我们的协议需要部署于移动网络通信系统之中. H 和 V 各有一对公/私钥对,并拥有认证中心签发的对应于公钥的数字证书,它们参与通信认证的计算机系统拥有足够的通信和计算资源. H 和 V 之间证书的发布、验证和管理采取有线计算机网络系统成熟的证书管理模式. M 拥有一个移动通信终端,此终端含有一智能卡,其中在用户申请开通移动服务时预先存储 M 的身份信息、认证中心的公钥及其 H 的公钥并具有安全访问控制机和一定的运算功能,M 端的一切运算都在智能卡内进行,M 端的伪随机数也由此智能卡产生. V 与 H 之间相互信任,V 只有获得 H 对 M 的身份合法性确认之后才会向 M 提供网络服务.

下述协议中的乘法运算都是在一个有限乘法群 G 上进行的,G 是一乘法群 Z_p^*(p 是一素数)的子群,G 的阶为素数 q,其生成元为 g. 归属网络 H 的私钥为 SK_H,其对应公钥为 $PK_H = g^{SK_H}$;同样,访问网络 V 的私钥为 SK_V,公钥 $PK_V = g^{SK_V}$.

协议流程如下:

(1) $M \rightarrow V: h(g^{r_M}), g^{r'_M}, TID_M, H$

其中 $TID_M = \{r, g^{r_M}, M \oplus r \oplus g^{r_M}\}_{K_{MH}}$, $K_{MH} = g^{SK_H r'_M}$

(2) $V \rightarrow H: g^{r_V}, h(g^{r_M}), g^{r'_M}, TID_M, \{h(g^{r_V}, h(g^{r_M}), g^{r'_M}, TID_M, V)\}_{SK_V}, T_V, Cert_V$

(3) $H \rightarrow V: g^{r_H}, g^{r_M}, \{\{h(g^{r_H}, M \oplus r \oplus g^{r_M}, H)\}_{SK_H}, \{h(g^{r_V}, g^{r_M})\}_{SK_H}, M \oplus r \oplus g^{r_M}\}_{K_{VH}}, T_H, Cert_H$

其中 $K_{VH} = h_1(g^{r_V r_H}, g^{r_H SK_V})$

(4) $V \rightarrow M: g^{r_V}, \{h(g^{r_V}, g^{r_M})\}_{SK_H}, \{h(g^{r_V}, g^{r_M}, TID'_M, V), T_H\}_{K_{MV}}, T'_V, Cert_V$

其中 $TID'_M = h(g^{r_M r_V}, M \oplus r \oplus g^{r_M})$, $K_{MV} = h_1(g^{r_M r_V}, g^{SK_V r_M})$

(5) $M \rightarrow V: \{h(g^{r_M}, g^{r_V}, T_H, V), T'_V\}_{K_{MV}}$

下面,对上述协议进行详细描述:

(1) 当 M 漫游到 V 时,为了取得网络服务,他必须向 V 证明自己身份的合法性.这个认证过程是通过 H 最终认证 M 的身份来完成的,由于 V 与 H 之间在这方面建立了信任关系,所以也就等于 V 认证了用户的身份,但是 V 并不知道 M 的身份信息. M 首先产生随机数 r、r_M 和 r'_M,计算 $h(g^{r_M})$ 和 $g^{r'_M}$;然后根据 H 的公钥 g^{SK_H} 和 r'_M 计算出 K_{MH},由此计算出 $TID_M = \{r, g^{r_M}, M \oplus r \oplus g^{r_M}\}_{K_{MH}}$,用于向 H 证实自己的身份;最后组成数据流 $h(g^{r_M})$, $g^{r'_M}$, TID_M, H 发送给 V.

(2) 对 M 身份认证是由第二、三条消息来完成的. TID_M 中含有 M 的身份信息,只有 H 才能获得其中的身份信息. V 把接收到的 TID_M 传给 H,由 H 取得其中的身份信息来对用户的身份进行认证,然后再把认证结果通知 V. V 在接收到来自 M 的消息之后,产生一随机数 r_V,计算 g^{r_V},并对 g^{r_V}, $h(g^{r_M})$, $g^{r'_M}$, TID_M 以及身份信息 V 先取摘要值再进行签名,产生时间戳 T_V,并附上自己的数字证书,组成相应消息发送给 H.

(3) H 接收到来自 V 的消息之后,首先验证其中证书的合法性,然后察看 T_V 与当前系统时间的误差是否在一个合理的范围之内. H 从 V 的证书中获取 V 的身份信息,再结合 g^{r_V}、$h(g^{r_M})$、$g^{r'_M}$和 TID_M 利用证书中的公钥验证数字签名的合法性.验证通过之后,H 利用私钥 SK_H 和 $g^{r'_M}$计算出 K_{MH},对 TID_M 进行解密获得用户的身份信息 M,可以进行身份认证;同时也获得了参数 g^{r_M},取其摘要值与 $h(g^{r_M})$ 进行比较.上述验证和比较通过之后,H 生成随机数 r_H,利用 V 的公钥和 g^{r_V}计算出会话密钥 K_{VH},对 H 的签名信息$\{h(g^{r_H}, M \oplus r \oplus g^{r_M}, H)\}_{SK_H}$和$\{h(g^{r_V}, g^{r_M})\}_{SK_H}$以及由解密 TID_M 获得的 $M \oplus r \oplus g^{r_M}$进行加密,然后附上自己的时间戳 T_H、证书 $Cert_H$ 以及参数 g^{r_H}、g^{r_M}组成消息流发给 V.

(4) 协议中的第四、五条消息用于在 M 与 V 之间进行身份认证、密钥协商与确认. V 接收到来自 H 的消息之后,首先验证其中证书的合法性,然后看 T_H 与当前系统时间的误差是否在一个合理的范围之内;计算出 K_{VH},对消息流中密文部分进行解密,然后利用 H 的证书中的公钥进行相应的验证签名;对由 H 处获得的 g^{r_M}取摘要值,与先前由 M 处获得的摘要值比较,看是否一致.上述验证通过之后,V 就可以计算 M 的新的临时身份标识符 $TID'_M = h(g^{r_M r_V}, M \oplus r \oplus g^{r_M})$,并存储起来,为下次与 M 建立会话时使用;计算摘要值 $h(g^{r_V}, g^{r_M}, TID'_M, V)$,根据安全参数计算出与 M 的会话密钥 $K_{MV} = h_1(g^{r_M r_V}, g^{SK_V r_M})$,对此摘要值和 T_H 加密;V 产生时间戳 T'_V,并附上自己的数字证书、安全参数 g^{r_V}和签名信息$\{h(g^{r_V}, g^{r_M})\}_{SK_H}$,组成第四条消息发送给 M. V 可以计算出下次与 M 建立会话时使用的会话密钥 $K'_{MV} = h_2(g^{r_M r_V}, g^{SK_V r_M})$,并存储起来.之所以下次会话密钥采用 K'_{MV}而不采用 K_{MV},主要是因为 K_{MV}已经在本次会话中使用过一次,防止由于 K_{MV}的部分信息的泄漏引起的对下次会话安全性的损害[4,5].

(5) M 接收到第四条消息之后首先验证证书的合法性,然后查看 T'_V 与当前系统时间的误差是否在一个合理的范围之内;利用存储在智能卡里的 H 的公钥验证签名信息

$\{h(g^{r_V}, g^{r_M})\}_{SK_H}$的合法性;利用证书里的公钥、$r_M$ 和 g^{r_V}计算出 K_{MV},对消息中的密文部分进行解密,计算出 TID'_M,验证解密出来的摘要值是否正确,以此判断是否与访问网络拥有相同的会话密钥,并存储 TID'_M,为下次会话使用;验证误差 $T'_V - T_H$是否在一个合理的范围之内. 验证通过之后,M 计算摘要值 $h(g^{r_M}, g^{r_V}, T_H, V)$,用 K_{MV}对此摘要值和 T'_V 加密,组成第五条消息发送给 V. 同样 M 也可以计算出下次与 V 建立会话时使用的会话密钥 $K'_{MV} = h_2(g^{r_M r_V}, g^{SK_V r_M})$. V 收到消息之后可以利用先前计算出 K_{MV}的对消息进行解密,然后验证数据,以此来判断是否与 M 拥有相同的会话密钥.

4　协议分析

下面通过分析协议来说明我们的协议满足第三部分中提出的安全需求.

双向身份认证即 V 和 M 对彼此的身份相互进行认证. M 在表明自己的合法身份时,首先利用随机数计算出临时身份标识符 $TID_M = \{r, g^{r_M}, M \oplus r \oplus g^{r_M}\}_{K_{MH}}$, $K_{MH} = g^{SK_H r'_M}$,虽然 $g^{r'_M}$和 g^{SK_H}为公共参数,但是 r'_M 和 SK_H 分别为 M 和 H 私有,显然 K_{MH}只能由 M 和 H 共享,非法窃听者和 V 都无法获得. 也就是说,只有 H 能够从 TID_M 中获得 M 的身份信息. H 从 V 处获得 TID_M 之后,完成对 M 的身份认证,把认证结果反馈给 V. 由于 V 与 H 在这方面建立了信任关系,从而 V 也就获得了对 M 的身份认证. M 对 V 的身份认证则是通过对协议中第四条消息的验证完成的. M 从 V 的数字证书中提取其身份信息和公钥,计算出会话密钥 K_{MV}对密文进行解密,只要解密出来的明文验证通过,就说明消息确实是由 V 发出的,因为 K_{MV}只有 M 和 V 能够计算出.

密钥协商和双向密钥控制. 由协议知,M 和 V 之间的会话密钥 $K_{MV} = h_1(g^{r_M r_V}, g^{SK_V r_M})$ 和 $K'_{MV} = h_2(g^{r_M r_V}, g^{SK_V r_M})$ 是由 M 和 V 分别给出的安全参数计算得出的. 协议中,g^{r_M}、g^{r_V}以明文形式传输,g^{SK_V}为公钥,两个单向散列函数为公共函数,但是为了计算出 K_{MV}或者 K'_{MV},要么拥有 r_M,要么拥有 r_V 和 SK_V,所以 K_{MV}和 K'_{MV}只在 M 和 V 之间共享,第三者无法计算得出. 而安全参数 r_M 和 r_V 都是每次分别由 M 和 V 随即选取,M 或 V 无法控制密钥的生成,保证了一次一密. 另外,为了保持密钥协商的公平性[6],在 V 给出 g^{r_V}之前,V 并不知道 M 给出的参数 g^{r_M},只知道其摘要值. V 把 g^{r_V}发给 H,H 对 TID_M 解密获得 g^{r_M},然后把 g^{r_M}发给 V,V 可以利用先前收到的摘要值进行验证;而 M 收到 g^{r_V}之后,可以利用 H 的数字签名验证其正确性和合法性,保证了密钥协商的公平性.

双方对会话密钥的确认则是在第四条消息和第五条消息中,数据发送方对数据进行加密,数据接收方对密文进行解密,并验证解密出来的明文是否正确来判断对方是否与自己拥有相同的会话密钥 K_{MH}. 只要拥有了相同的 K_{MH},由 K_{MH}和 K'_{MH}的生成方式知,双方就可以确知拥有相同的 K'_{MH}.

协议显然使移动通信系统为用户提供匿名服务. M 认证自己的身份时,提供的是临时身份标识符 TID_M,由上述讨论知,只有 H 能够从其中获得用户的身份信息,H 在验证用户身份通过之后,只是把验证结果告诉 V,并不泄漏用户的身份信息,虽然 V 得到了用于计算 TID'_M 的 $M \oplus r \oplus g^{r_M}$,由于 r 只有 H 和 M 知道,所以 V 并不能从中获得用户的身份信息,非法窃听者也不可能获得用户的身份信息. 由 TID'_M 的计算方式知,由于每次会话安全参数 r_M 和 r_V 都会随机选取,每次更新,所以每次 TID'_M 都是不同的;由于随机参数的引入,用户的各个 TID 之间不存在明显的相关性. 另外,由于每当用户漫游到一个新的访问网络,在证实身份时,他都会提交一个新的 TID_M,产生新的 TID'_M,同样由于每次引入新的随机参数 r、r_M 和 r_V,各个临时身份标识符之间不存在相关性,所以满足域分离特性.

5　协议优化和改进

在协议中,利用了数字签名进行验证数据的合法性. H 与 V 均需对数据签名一次,分别验证对方签名一次和两次,M 需要验证 H 的签名信息一次. H 与 V 参与通信与认证的计算机系统拥有足够的通信和计算资源,而 M 手持的通信终端由于受到体积等因素的限制,其计算能力受到限制. 因此,在选择签名方案时,应该选取签名时计算较复杂而验证签名时需要计算资源较少的签名方案,如 RSA 等;也可以采用椭圆曲线等在保证相同安全强度的前提下,对存储资源和计算资源要求都很低的签名算法.

在保证满足协议安全性需求的前提下,为了降低 M 对端计算资源和通信资源的要求,我们对上述协议作进一步的改进:H 不再对 $h(g^{r_M}, g^{r_V})$ 进行签名,而用 K_{MH}对 $h(g^{r_M}, g^{r_V}, PK_V)$ 进行加密;V 不再把证书 $Cert_V$ 传给 M,而是把公钥 PK_V 传给 M. 协议的第一、二、五步保持不变,改进后的协议如下:

(1) $M \rightarrow V: h(g^{r_M})$, $g^{r'_M}$, TID_M, H

其中 $TID_M = \{r, g^{r_M}, M \oplus r \oplus g^{r_M}\}_{K_{MH}}$, $K_{MH} = g^{SK_H r'_M}$

(2) $V \rightarrow H$: g^{r_V}, $h(g^{r_M})$, $g^{r'_M}$, TID_M, $\{h(g^{r_V}, h(g^{r_M}), g^{r'_M}, TID_M, V)\}_{SK_V}$, T_V, $Cert_V$

(3) $H \rightarrow V$: $\{\{h(g^{r_H}, M \oplus r \oplus g^{r_M}, H)\}_{SK_H}, \{h(g^{r_V}, g^{r_M}, PK_V)\}_{K_{MH}}, M \oplus r \oplus g^{r_M}\}_{K_{VH}}$, g^{r_H}, g^{r_M}, T_H, $Cert_H$,

其中 $K_{VH} = h_1(g^{r_V r_H}, g^{r_H r = SK_V})$

(4) $V \rightarrow M$: g^{r_V}, $\{h(g^{r_V}, g^{r_M}, PK_V)\}_{K_{MH}}$, $\{h(g^{r_V}, g^{r_M}, TID'_M, V), T_H\}_{K_{MV}}$, T'_V, PK_V

其中 $TID'_M = h(g^{r_M r_V}, M \oplus r \oplus g^{r_M})$, $K_{MV} = h_1(g^{r_M r_V}, g^{SK_V r_M})$

(5) $M \rightarrow V$: $\{h(g^{r_M}, g^{r_V}, T_H, V), T'_V\}_{K_{MV}}$

由前面对协议的讨论得知 K_{MH}只能由 M 和 H 产生,而 M 又信任 H,所以 M 验证$\{h(g^{r_V}, g^{r_M}, PK_V)\}_{K_{MH}}$的合法性与验证$\{h(g^{r_V}, g^{r_M})\}_{SK_H}$的合法性相同,都可以验证 g^{r_V}的合法性,因为 g^{r_V}的合法性已经被 H 验证过,而 M 的计算量大大降低;同样,M 通过验证$\{h(g^{r_V}, g^{r_M}, PK_V)\}_{K_{MH}}$的合法性,可以验证 PK_V 的合法性,因为 PK_V 是 H 经过证书 $Cert_V$ 验证过的,而 M 不必再接收证书 $Cert_V$,通信量也降低. 改进后的协议的其他部分与改进前的部分相同,因此,改进后的协议同样满足本文 3.1 节的安全需求. 而在改进后的协议中,不需要 M 再验证任何数字签名,对 M 的计算资源的要求大大降低,M 与 V 之间

的通信量也随之降低.

另外,本协议中,用户端需要产生三个随机数 r、r_M 和 r'_M,并计算 $h(g^{r_M})$ 和 $g^{r'_m}$. 为了提高协议的效率,在实现本协议时,可以使用户在执行本协议之前的空暇时间,预先选好需要的随机数,并预先计算 $h(g^{r_M})$ 和 $g^{r'_M}$,减少执行本协议所耗费的时间.

6 结论

安全依然是移动通信领域不可忽略的一个方面,身份认证和密钥协商是其中一个至关重要的问题. 本文提出了一个无线双向认证和密钥协商协议,解决了移动用户和网络运营商之间的双向身份认证和密钥协商问题,并使移动网络系统向移动用户提供匿名服务,使访问网络和非法窃听者都不能获得用户的真实身份信息,最大程度保证了用户身份信息和所在位置信息的机密性,移动用户端计算量小,高效实用.

参考文献:

[1] G Horn, B Preneel. Authentication and payment in future mobile systems [A]. In Computer Security ——ESORICS '98 Proceedings [C]. Berlin: Springer-Verlag, 1998.

[2] G Horn, K M Martin, C J Mitchell. Authentication protocols for mobile network environment value added services [EB/OL]. http://isg.rhbnc.sc.uk/cjm/Listofpublications.

[3] A Mehrotra. Mobility and security management in the GSM system and some proposed future improvements [A]. Proceedings of the IEEE [C]. USA: IEEE, 1998.

[4] V Shoup. On formal modules for secure key exchange [R]. IBM Research Report RZ 3120, 1999, http://www.shoup.net/papers

[5] D G Park, C Boyd, S J Moon. Forward secrecy and its application to future mobile communiations security [A]. PKCS2000, LNCS 1751 [C]. Melbourne, Australia: PKCS, 2000.

[6] Mitchell, C J, Ward, M, Wilson, P. Key control in key agreement protocols [J]. Electronics Letters, 1998, 34: 980 - 981.

作者简介:

邓所云 男,1974 年生于山东昌邑,现为北京邮电大学博士生,1996 年于山东大学数学系获得学士学位,1999 年于山东大学计算机系获得硕士学位,主要研究领域:密码学、电子商务和网络安全.

胡正名 男,1931 年生于湖北省江陵,教授,北京邮电大学博士生导师,主要研究领域:密码学、信号与信息处理等.