一种基于 USB Key 的短波通信身份认证方案①

闫宏生, 孟晓锋, 李承泽

(国防信息学院, 武汉 430010)

摘 要: 针对短波网络的窄带特性, 提出了一种基于 USB Key 和 PIN 码的身份认证方案. 方案采用挑战/应答机制, 借鉴了 3G 认证中的五元鉴权思想, 依托 HMAC 算法有效减少了认证过程中的开销, 能够满足短波网络的窄带需求, 并具有较高的安全性.

关键词: 短波; 身份认证; 挑战/应答; HMAC

A Short Wave Communication Scheme Based on USB Key

YAN Hong-Sheng, MENG Xiao-Feng, LI Cheng-Ze

(PLA Academy of National Defense Information, Wuhan 430010, China)

Abstract: Aiming at the narrow-band characteristic of the short wave network, an identity authentication scheme is designed based on USB Key and PIN code. The scheme adopts the challenge/response mechanism, takes the thought of five authentication factors in 3G authentication scheme for reference, and improves the generation mechanism of five authentication factors by using HMAC algorithm. The scheme reduces the data cost in the process of the authentication, meets the bandwidth requirements of the short wave network, and has high security.

Key words: short wave; identity authentication; challenge/response; HMAC

短波通信具有通信距离远、生存能力强、便于机动开设等特点, 使其在最复杂、最困难的情况下, 仍能完成通信保障任务, 被广泛用于军队、气象、林业等部门[1]. 但由于短波网络的固有特性, 短波通信也存在很多缺陷: 传输频带窄、时变特性强、信道容量小, 且易受干扰或截获[2]. 因此, 在短波终端用户接入网络的过程中必须对接入用户的身份进行有效的认证, 防止非法用户对短波资源的占用和干扰. 但是, 在已有的基于对称算法和公钥算法的认证方案中, 认证过程中的数据开销较大, 短波网络的窄带特性很难满足其要求. 如何在对短波网络用户进行身份认证并进可能少的占用短波网络资源, 是短波网络应用中需要解决的一个重要问题.

1 身份认证技术分析

身份认证, 是指以一种安全的方式向计算机系统提交自己的身份证明, 由系统确认用户身份是否属实, 最终拒绝或赋予用户相应权限的过程[3]. 身份认证方式可以分为三种: 基于口令的认证、基于生物特征的认证和基于智能卡的认证. 基于静态口令的安全性较差, 对此种方式的研究主要集中在动态口令认证; 基于生物特征的认证方式具有最高的安全性, 但是开销较大且不够稳定; 基于智能卡的认证方式是当前应用最广的认证方式, 该方式可同动态口令方式和生物特征方式结合, 形成基于双因子或多因子的身份认证方案[4-6].

一个良好的身份认证方案不仅要采取恰当的认证方式, 还需要采用正确的认证机制和认证算法, 才能有效保证系统的安全和认证效率. 目前应用最多的两种认证机制分别为基于挑战/应答的身份认证和基于数字证书的身份认证. 挑战/应答机制中认证服务器通过检验用户对“挑战值”的“应答”来判断用户身份是否

① 收稿时间:2012-11-23;收到修改稿时间:2012-12-24

合法; 后者基于 PKI(公钥基础设施), 通信双方通过数字证书来完成密钥的互换[7].

2 认证方案设计

短波网络的窄带特性是制约认证机制的一个重要因素, 因此在设计中必须减小额外开销, 同时确保认证过程的安全, 做到安全和效率的统一. 以下对认证方式、认证机制、认证算法进行分析, 并在此基础上完成流程设计.

2.1 认证方式

单纯基于用户名/口令的认证方式安全性较差, 很容易受到穷举等网络攻击, 不能满足应急终端用户身份认证的安全需求; 基于生物特征的认证方式成本较高, 且指纹等生物特征的易受环境的影响(如沾上灰渍时很难识别), 限制了其在应急救灾环境下的使用; 基于硬件 USB Key 的身份认证方式结合了现代密码学技术、智能卡技术和 USB 技术, 其安全性能较传统身份认证方式有较大提高, 可实现双因子认证, 且性能稳定. 基于以上分析, 本系统将采用基于 USB Key 和 PIN 码的双因子认证方式.

2.2 认证机制

基于 USB Key 身份认证方式通常同其他先进的认证机制相结合, 目前主要有两种应用模式: 一是基于数字证书的认证模式, 二是基于挑战/应答的认证模式. 数字证书的大小通常在 10kB 以上, 相对于短波网络 75～2400bps 的传输速率来说是很大的开销, 同时公钥算法加密后会使认证数据大量增加. 基于挑战/应答的身份认证是最基础的认证机制, 在无线网络环境下的 GSM 认证协议、3G 认证协议均是在挑战/应答机制的基础上改进形成的. 其中 3G 认证协议是在 GSM 认证协议基础上进行了改进, 从 GSM 的三元鉴权改进为 3G 认证协议的五元鉴权, 克服了 GSM 认证协议存在的缺陷, 实现了用户与网络的互认证, 很好的完成了会话密钥和完整性密钥的协商[8].

系统设计中, 借鉴了 3G 认证中的五元鉴权思想, 引入五元鉴权组: RAND(Random Number, 网络质询随机数)、XRES(Expected Response, 用户应答的期望值)、CK(Cipher Key, 加密密钥)、IK(Integrity Key, 完整性密钥)、AUTN(Authentication Token, 网络身份确认标记). 同时结合短波网络的窄带特性, 对五元鉴权机制进行改进, 减少认证过程中的开销. 五元鉴权组的生成如图 1 所示. 其中, h(PIN)是用户 PIN 码的 Hash 摘要, 存储在 USB Key 和认证服务器中; RAND 是产生的质询随机数. 认证服务器回复 AUTN 和 RAND 给认证客户端, 客户端首先对 AUTN 进行检验, 完成验证后, 生成 RES 回复给认证服务器. 完成互认证后, 客户端根据相应算法产生机密密钥 CK 和完整性密钥 IK, 且二者不在无线链路上传输, 保证了密钥安全.

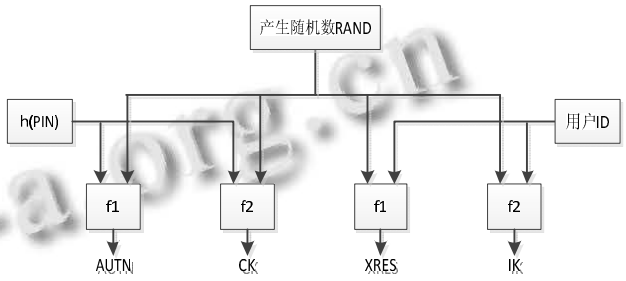

图 1 鉴权向量的生成

2.3 认证算法

身份认证系统的安全在很大程度上依赖于认证算法的安全, 其对网络带宽的需求同样取决于认证算法. 在本系统中, 短波网络的窄带特性是制约系统的一个关键因素, 在保证安全的前提下应尽量减少对带宽的消耗.

RSA 算法是最常用的公钥算法, 其有效密钥长度至少是 1024bit,传输开销较大. ECC 算法在目前已知的公钥算法中具有最高的单比特安全性, 该算法 160bit 长的密钥安全性与 1024bit 的 RSA 密钥相同. 但是该算法额外开销较大, 加密后长度有较大增加, 这制约了它在窄带网络中的应用. DES 算法是最常用的对称算法, 密钥长度为 64bit, 但其安全性较差. 3DES 是其改进算法, 密钥长度达到 168bit, 安全性也有较大提高, 但运算速度极慢. AES 是当前最新的对称算法加密标准, 标准密钥为 128bit, 并可扩展为 192bit 或者 256bit. 以上 3 种对称算法加密后的密文长度同和加密前明文长度相等, 额外开销较少.

Hash 算法具极高的单向安全性, HMAC 是建立在 Hash 函数基础上的算法, 其具有比所依赖的 Hash 函数更高的安全性. 对于 128bit 的散列值来说, 需要得到用同一密钥产生的 264 个分组, 这在 1Gbps 的链路上, 大约需要 150000 年. 在目前的技术水平下, 使用 MD5 和 SHA-1 作为 HMAC 的嵌入 Hash 函数, 安全性是可以得到保证的[9,10].

图 1 中, 采用 SHA-256 加密用户 PIN 码; f1 采用 HMAC-SHA-1 算法, 对 h(PIN)和用户 ID 加密, 生成 160bit 的 AUTN 和 RES; f2 采用 HMAC-MD5 算法, 分别对 h(PIN)和用户 ID 加密, 生成 128bit 的 CK 和 IK. 在认证过程中, 交互的数据包括注册请求中的用户 ID 和时间戳, 网络鉴权响应中的 RAND 和 AUTN, 以及用户鉴权响应 RES. 用户 ID 为 64bit, 时间戳为 128bit, RAND 为 128bit, AUTN 和 RES 为 160bit, 整个认证过程中交互的数据量为 640bit, 短波网络的传输速率为 75～2400bps, 在最极端的情况下完成认证数据交互也只需要 9 秒钟的时间. 对短波网络而言, 这一时延是可以接受的.

2.4 认证流程

系统采用基于 USB Key 的双因子认证方式, 在完成身份审核后, 网管人员为用户分配一个唯一的 ID 号, 初始 PIN 码设为 12345678, 并将用户的身份信息写入本地数据库中, 其中用户 PIN 码以 SHA-256 摘要的形式保存. 同时对 USB Key 进行初始化, 将用户 ID 号、PIN 码的 SHA-256 摘要及认证过程中的相关算法写入 USB Key 中. 其认证流程如图 2 所示.

① 用户插入 USB Key, 打开客户端程序界面, 输入 PIN 码, 提交认证请求.

② 收到请求后, USB Key 生成一个随机数 m, 作为挑战值回复给客户端.

③ 客户端程序对用户 PIN 码进行运算, 并将计算结果同随机数 m 做 HMAC-SHA-1 运算得到 E, 其中: E=H(h(PIN),m), 并将计算结果传给 USB Key.

④ USB Key 将自身存储的 PIN 码摘要同随机数 m 进行 HMAC-SHA-1 运算, 将其计算结果与 E 对比, 若二者一致则说明用户输入 PIN 码正确, 转入步骤 5); 否则说明用户非法, 将结果返回给客户端, 提示 PIN 码输入错误.

⑤ USB Key 发送含用户 ID 和当前时间戳 t 的接入请求.

⑥ 接入基站收到用户接入请求后, 向网络管理中心认证服务器发送 REGISTER 请求.

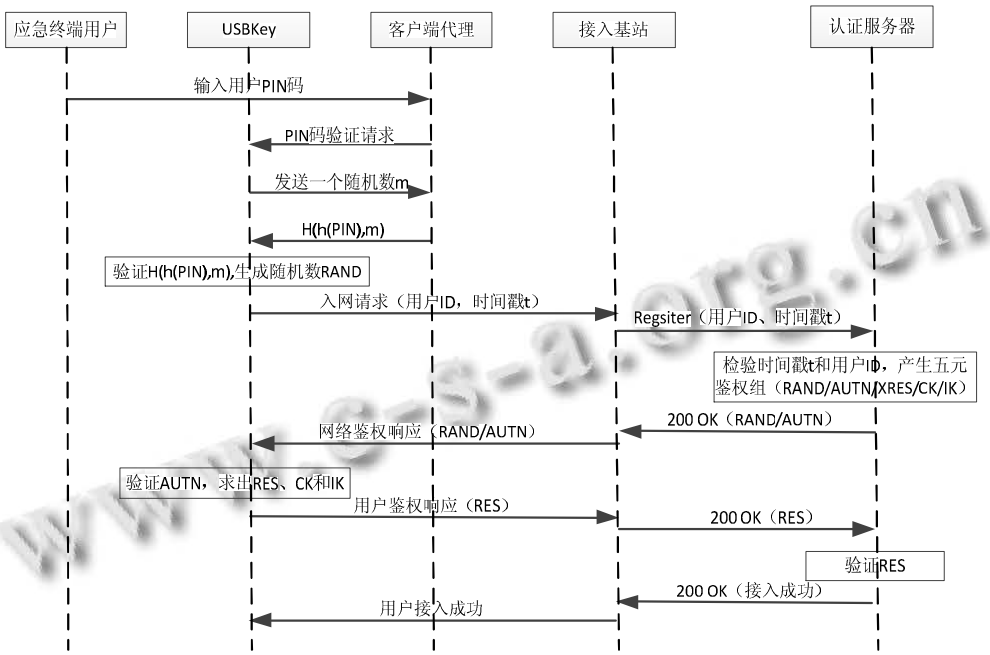

图 2　注册认证流程

⑦ 认证服务器收到请求后, 首先对时间戳 t 进行检验, 需满足 0<t’-t<Δt, 其中 t’为接收时间戳, Δt 为有效时间间隔. 接着检验用户 ID, 若该用户 ID 存在, 则生成五元鉴权组(RAND、AUTN、XRES、CK、IK), 并回复包含 RAND 和 AUTN 的鉴权响应.

⑧ 收到鉴权响应后, USB Key 首先对 AUTN 进行校验. 若验证通过, 则计算出 RES、CK 和 IK, 并回复 RES 给认证服务器; 否则发送“认证拒绝”信息给认证服务器, 放弃该认证过程.

⑨ 认证服务器收到用户鉴权响应后, 将 RES 同

XRES 对比, 若二者相同则说明鉴权成功; 否则鉴权失败.

3 安全性分析

身份认证的目的是为了证明通信双方身份的真实性, 防止非法用户的欺骗. 一个安全的身份认证系统需满足以下三个方面: 认证口令的安全, 认证数据的安全和认证服务器的安全[10]. 对认证口令的攻击主要为口令猜测和口令窃取, 对认证数据的攻击有网络监听和重放, 对认证服务器的攻击为拒绝服务和伪装服务器, 以下分别进行分析.

1) 口令猜测

口令猜测是指恶意用户对用户 PIN 码进行猜测. 由于系统是基于 USB Key 和 PIN 码的双因子认证, 在没有 USB Key 的情况下, 对 PIN 码的验证便无从谈起. 即使非法用户窃取了 USB Key, 因为 USB Key 定义中对用户 PIN 码的输入错误次数进行了设定, 当连续 4 次输入错误时, 系统便会自动锁定.

2) 口令窃取

口令窃取是指非法用户侵入数据库窃取用户 PIN 码. 本系统中, 用户 PIN 码以摘要的形式存储于 USB Key 和认证服务器中. 即使用户窃取了用户 PIN 码的摘要, 由于 SHA-256 单向安全性依然无法推算出用户 PIN 码.

3) 网络监听

网络监听是指通过监听用户会话内容, 从中分析用户 PIN 码等关键认证数据. 在本系统的认证过程中, 用户 PIN 码从不以明文方式传输, 而是以 PIN 的 SHA-256 摘要和随机数进行 HMAC 变换后传输, 即使非法用户成功窃听到认证数据依然无法推算出用户 PIN 码.

4) 重放攻击

重放攻击是指攻击者截获认证数据, 并再次发起认证. 在认证流程中, 认证双方的鉴权响应均是基于随机数 RAND 的运算值, 因为每次的随机数不同, 所以非法用户依靠上一次截获的认证数据无法通过下一次的认证.

5) 拒绝服务攻击

拒绝服务攻击是指非法用户通过大量的认证请求, 引发认证服务器的大量运算. 系统是基于 USB Key 和 PIN 码的双因子认证, 在没有 USB Key 的情况下, 认证请求无法发起.

6) 伪装服务器攻击

伪装服务器攻击是指非法用户伪装为认证服务器, 使用户接入非法网络. 在本系统认证过程中, 不仅实现了服务器对用户的认证, , 也实现了用户对服务器的认证.

参考文献

1 胡中豫.现代短波通信.北京:国防工业出版社,2005.40–43.
2 尤增录.短波通信网.北京:解放军出版社,2010.32–35.
3 王景中,徐小青.计算机通信信息安全技术.北京:清华大学出版社,2006.152–154.
4 Lu R, Cao Z. Efficient remote user authentication scheme using smart card. Computer Networks, 2005,49:65–67.
5 胡鸣.一种新的基于智能卡的身份认证方案.微计算机信息, 2010,26(3):46–48.
6 刘怀兰.改进的基于 USB Key 的动态口令认证方案.华中科技大学学报,2010,11:73–75.
7 荆继武,林璟锵,冯登国.PKI 技术.北京:科学出版社,2008. 142–145.
8 庞韶敏,李亚波.3G UMTS 与 4G LTE 核心网——CS, PS, EPC, IMS.北京:人民邮电出版社,2010.234–137.
9 3GPP TS 33.102 3G security.
10 认证理论及应用.李晓航,王红霞,张文芳.北京:清华大学出版社,2009.37–39.