



文章编号:1001-9081(2017)02-0483-05

DOI:10.11772/j.issn.1001-9081.2017.02.0483

白盒攻击环境下的任务规划系统安全传输方法

崔西宁^{1,2*}, 董星廷³, 牟 明², 吴 娇²

(1. 西安电子科技大学 计算机学院, 西安 710071; 2. 中国航空工业集团公司 西安航空计算技术研究所, 西安 710068;

3. 西安电子科技大学 通信工程学院, 西安 710071)

(* 通信作者电子邮箱 cuixin@126.com)

摘要:针对任务规划系统中的安全传输在白盒攻击环境(WABC)下通信密钥容易被窃取的问题,提出基于修改之后的白盒高级加密标准(白盒AES)的任务规划系统中的安全传输方法。首先,将高级加密标准(AES)拆分成许多查找表,并将密钥嵌入到查找表当中,然后再将查找表按照AES的执行顺序进行合并;其次,在地面按照给出的白盒AES生成算法利用不同的密钥生成不同的白盒AES程序;最后,将这些白盒AES程序嵌入到任务规划系统的安全传输当中,当需要更换密钥时,再在地面将原先的白盒AES程序擦除,生成新的白盒AES。理论分析表明,与传统的任务规划系统中的安全传输相比,修改后的任务规划系统中的安全传输方法可使攻击复杂度提高到 2^{91} ,达到足够的安全强度,可以保护通信密钥。

关键词:白盒攻击环境; 任务规划系统; 安全传输; 白盒AES; 对偶密码

中图分类号: TP309.7 **文献标志码:**A

Secure transmission method of mission planning system in white-box attack context

CUI Xining^{1,2*}, DONG Xingting³, MU Ming², WU Jiao²

(1. School of Computer Science and Technology, Xidian University, Xi'an Shaanxi 710071, China;

2. Xi'an Aeronautical Computing Technique Research Institute, Aviation Industry Corporation of China, Xi'an Shaanxi 710068, China;

3. School of Telecommunications Engineering, Xidian University, Xi'an Shaanxi 710072, China)

Abstract: Concerning the problem that the communication keys in transmission of mission planning system were easily stolen in White-Box Attack Context (WBAC), a new secure transmission method of mission planning system was proposed based on modified white-box Advanced Encryption Standard (white-box AES). First, the Advanced Encryption Standard (AES) was split into many lookup tables and the keys were embedded into these lookup tables, then the lookup tables were merged in accordance with the executing order of the AES. Secondly, on the ground, different white-box AES programs were generated in accordance with the given white-box AES generation algorithms using different keys. In the end, the white-box AES programs were embedded in the security transmission of the mission planning system. When the key needed to be replaced, the original white-box AES program should be erased on the ground to generate a new white-box AES. Theoretical analysis shows that compared with the traditional secure transmission of mission planning system, the modified secure transmission method of mission planning system can make the attack complexity to 2^{91} , which achieves the sufficient security and can protect the communication key.

Key words: White-Box Attack Context (WBAC); mission planning system; security transmission; white-box Advanced Encryption Standard (white-box AES); dual cipher

0 引言

近年来随着科学技术突飞猛进的发展,传统的密码软件使用环境越来越不安全,有的地方密码软件的加解密过程对于攻击者来说(有可能是用户本身)是完全可见的,他们很容易就可以获得密钥。同样,在竞争领域异常激烈的军用密码软件中也存在这样的问题。有可能敌方间谍在使用我方密码软件时很容易获取我方密钥或者对这些软件内部进行更改、观测,这都是我方的损失。任务规划系统是航空领域的重要系统,一旦我国与敌国处于战争状态,任务规划系统的安全管理软件的执行环境就有可能面临这样的环境,使我方的密钥

被敌方抽取,导致航空任务无法完成或被敌方探明。

这种对运行终端非常直接的攻击方法叫作白盒攻击,由Chow等于2002年在文献[1]中提出。他们认为在白盒攻击环境(White-Box Attack Context, WBAC)中,密码分析者对密码终端软件拥有完全的控制能力,与密码软件的执行者拥有同等的权利,攻击者可以对程序进行二进制追踪,读取其内存中的密钥,观察程序执行的中间结果,并且可以对程序进行任意的静态分析以及改变子计算结果,即攻击者可以在终端做任何操作。相比传统的黑盒模型,对攻击者的能力只有很少的限制,这个环境很适合情况复杂多变的战场环境。

在2002年Chow等^[1]提出白盒攻击环境同时,也提出了

收稿日期:2016-08-01;修回日期:2016-10-18。 基金项目:国家重大科技专项(2012ZX01041-006)。

作者简介:崔西宁(1964—),男,陕西咸阳人,研究员,博士,CCF 高级会员,主要研究方向:分布式安全管理、并行分布式系统、实时操作系统、信息安全; 董星廷(1989—),男,山西临汾人,硕士研究生,主要研究方向:密码学、信息安全; 牟明(1973—),男,陕西西安人,研究员,硕士,CCF 会员,主要研究方向:软件工程、软件测试; 吴娇(1987—),女,陕西西安人,工程师,硕士,主要研究方向:嵌入式软件、机载网络。



白盒密码实例——白盒 AES(Advanced Encryption Standard)，通过构造查找表的形式将 AES 分解为小的模块，再通过混淆变换将其混淆。但在 2004 年，Billet、Gilbert 和 Ech-Chabi 提出了 BGE 的攻击^[2]，是一种非常有效的针对白盒 AES 的攻击方法。他们选择某些特定的查找表合并成一个可以用输入输出表示的函数，并使用代数的方法去掉其中的非线性部分，从而能成功提取出隐藏在 T-Box 中的密钥。在这以后，Chow 白盒 AES 的两个改进方案，即 Karroumi^[3]提出的基于对偶 AES 密钥的方案与文献[4]中的 Xiao-Lai 改进方案被提出，其中 Xiao-Lai 改进方案已经被 De Mulder 等在 2012 年攻破^[5]，而 Karroumi^[3]提出的基于对偶 AES 密钥的方案目前还没有攻破。

任务规划系统的原理是利用先进的计算机技术，根据任务需求，从多渠道采集作战需要的各种情报信息，分析战场威胁环境，为任务规划人员制作并提供威胁分布、突防路径评估、数字地形、油量计算、气象、机载武器性能等决策依据，为地面指挥员和作战飞机机组人员制定作战飞机出航航线和返航航线，调度空中作战机群协同攻击计划和时间控制节点，确定武器载荷和武器发射或投掷的时间节点和地点，评估作战效能和出航损伤率，以实现对敌方地面目标的精确打击和低损伤率，是航空兵对地作战指挥系统的核心组成部分。任务规划系统的安全管理软件负责任务规划系统的信息安全。本文基于 Karroumi^[3]修改的 Chow 白盒 AES 来构造在白盒攻击环境下安全的任务规划系统。

1 任务规划系统安全

图 1 为任务规划系统整体框图。安全管理软件为图中安全服务组件，为整个系统提供信息安全服务；最上层为各种应用，通过调用各个组件的接口来获得相应的服务；数据通过最下层的中间件与外部系统进行交换。

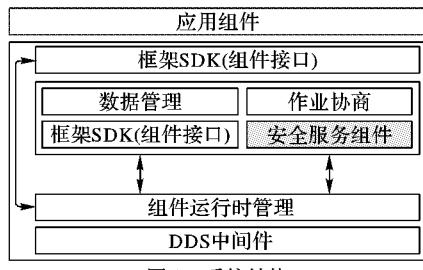


Fig. 1 System structure

整个系统采用 C/S 结构，客户端以对等实体的关系挂接在网络上，同时挂接在网络上的还有认证服务器、数据库服务器、证书授权(Certificate Authority, CA)中心和配置管理服务器。客户端使用 USB Key，负责客户端的数字签名和加解密，也是用户数字证书和私钥的载体。客户端可以使用系统提供的文件访问、文件交互以及数据库访问服务，各个功能由相应的安全控制机制来保证操作与数据的安全性。

安全架构从功能的角度来分层如图 2 所示，最下层为整个系统的最基本的安全支撑——CA 中心。往上一层为登录认证，系统的功能都需要在完成登录认证的基础上才能使用。再上一层为系统的安全访问控制，成功登录的用户所执行的操作都需要经过访问控制组件的检查，只有满足安全策略的操作才能执行。在访问控制之上为系统的四类操作：数据库

操作、消息传输、文件访问和文件交互。其中，消息传输和文件访问需要用到数据安全传输；文件交互操作分为文件在本地和不在本地两种情况，若在本地则直接发送给外域用户，否则需要通过文件访问从文件服务器获取后再发送给外域用户。

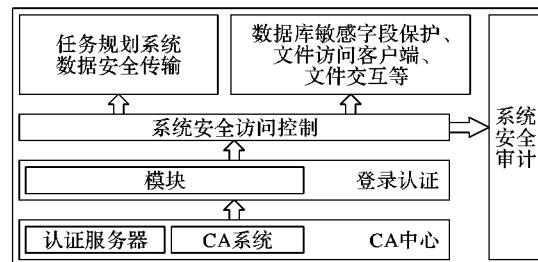


图 2 任务规划系统安全架构

Fig. 2 Security architecture of mission planning system

2 任务规划系统数据安全传输方法

为了保证系统中通信数据的安全性，需要对数据传输进行保护，数据安全传输组件结合数据保护服务、安全协议组和动态安全参数管理三者来实现保护数据包安全和为抵御网络攻击提供防护措施这两个目标，不仅能为通信提供强有力且灵活的保护，而且还能用来筛选特定数据流。数据安全传输组件基于一种端对端的安全模式。

数据安全传输是保护整个安全访问中所有用户通信安全的，它分为发送端和接收端，为应用调用提供的接口，对数据进行相应处理后发送给接收端。数据安全传输是由图 1 中的安全服务组件实现的。

数据安全传输协议首先从系统消息中解析出消息类型，然后对应消息类型从客户端独立线程中取得安全参数对应用数据进行保护，同时在数据封装上增加相应附加信息。

这里所描述的数据安全传输包括发送设计、接收设计、报文设计、加解密设计、哈希校验设计和错误码设计。如图 3 所示为数据安全传输运行流程。

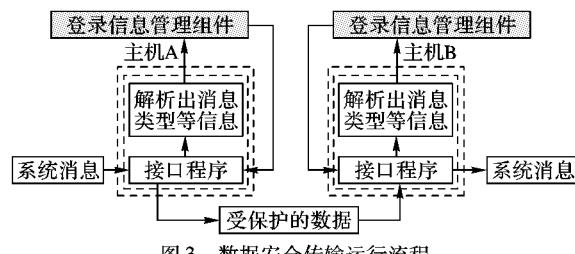


图 3 数据安全传输运行流程

Fig. 3 Security transmission process of data

驱动程序获得系统消息后，解析相应字段，得到消息类型、接收方信息、安全参数标记等信息。

在解析出相应信息后发送端驱动程序执行以下步骤：
1) 从客户端独立线程处获得安全参数；2) 保护应用数据；3) 根据数据封装格式封装数据；4) 将封装好的数据发送出去。

接收端驱动程序执行以下步骤：1) 通过解析接收数据头获取消息类型等信息；2) 按照该信息从客户端独立线程处获取消安全参数；3) 使用获取的安全参数还原数据；4) 将数据递给接收应用程序。

加密完成后的数据封装格式如图 4 所示。其中：消息长度表示整个数据包的长度；消息类型表示是否需要加密；密钥



标识用来从密钥中心获取密钥;接收端消息指真正的接收用户具体信息;序列号表示1~32位递增的数值,唯一地标识了数据包;可变长数据指加了密的密文;哈希认证结果表示前面的数据运用哈希函数作用之后得到的哈希值。



图4 报文格式
Fig. 4 Message format

3 白盒 AES

3.1 白盒 AES 的主要设计思想

白盒攻击环境(WBAC)是这样的一种攻击环境:

1)完全授权的攻击软件和密码软件分享一台主机,攻击者完全接触算法的应用;

2)动态的执行(例如密钥)能被观察;

3)内部算法细节完全可见,并且任意选择。

置乱编码的定义: X 为一个 m 到 n 的转换,选择 m 比特双射 F 和 n 比特双射 G 称 $X = G \circ X \circ F^{-1}$ 为一个 X 的编码版本。其中: F 是输入编码, G 是输出编码。

函数分解:将大的双射表分解为小的双射表的组合,考虑 F_i 的大小为 n_i ,这里 $n_1 + n_2 + \dots + n_k = n$,用 \parallel 来表示向量合成。函数分解 $F_1 \parallel F_2 \parallel \dots \parallel F_k$ 是双射 F 使得

$$\begin{aligned} F(b) &= F_1(b_1, b_2, \dots, b_{n_1}) \parallel \\ &\quad F_2(b_{n_1+1}, b_{n_1+2}, \dots, b_{n_1+n_2}) \parallel \dots \parallel \\ &\quad F_k(b_{n_1+\dots+n_{k-1}+1}, b_{n_1+\dots+n_{k-1}+2}, \dots, b_n) \end{aligned}$$

对于任意的 n 比特向量有 $b = (b_1, b_2, \dots, b_n)$,显然,有 $F^{-1} = F_1^{-1} \parallel F_2^{-1} \parallel \dots \parallel F_k^{-1}$ 。

$Y \circ X$ 的网络编码(即变换 X 执行之后执行变换 Y)是一个编码形式:

$$Y' \circ Y = (H \circ Y \circ G^{-1}) \circ (G \circ X \circ F^{-1}) = H \circ (Y \circ X) \circ F^{-1}$$

注意到双射 F, G, H 被隐藏了。

3.2 白盒 AES 的主要设计方法

白盒AES的设计思路是:首先利用矩阵乘法规则将AES的每一轮拆分成一个个的矩阵,将密钥嵌入到拆分后的矩阵中;然后对每个矩阵的两边乘上置乱矩阵;最后将这些矩阵用查找表的形式表示。在白盒攻击环境中,攻击者最终看到的是乘上置乱矩阵之后的查找表,由于置乱矩阵对攻击者是未知的,所以他无法从中得知有用的信息。

典型的AES由10轮组成,每一轮包括4个部分:SubBytes、ShiftRows、MixColumns和AddRoundKey。在第一轮运行之前先做一个AddRoundKey,而最后一轮没有MixColumns。

白盒AES将AddRoundKey和SubBytes结合起来作为一个T函数,为8bit输入8bit输出,具体定义如下:

$$T'_{i,j} = S(x + K'^{-1}_{i,j}); i, j = 0, 1, 2, 3, r = \{1, 2, \dots, 9\} \quad (1)$$

$$T^{10}_{i,j} = S(x + K^0_{sr(i,j)}) + K^{10}_{sr(i,j)}; i, j = 1, 2, 3 \quad (2)$$

其中:S()是AES的S盒; $K'_{i,j}$ 是AES在 r 轮位置 i, j 的密钥; $sr(i, j)$ 表示在ShiftRow之后在 i, j 处新的位置;+表示比特异或。T盒由SubByte和前一轮的AddRoundKey组成。

紧接着进行MicClouds变换,为避免大的查找表,这时要用到函数分解的思想,利用矩阵分块把列混合矩阵 MC 分解为四块小矩阵;

$$MC = (MC_1, MC_2, MC_3, MC_4)$$

然后再与T变换之后的输出作用,具体见下式:

$$(MC_1, MC_2, MC_3, MC_4) \times$$

$$[T'_{i,0}(x_0) \ T'_{i,1}(x_1) \ T'_{i,2}(x_2) \ T'_{i,3}(x_3)]^T =$$

$$MC_1 \times T'_{i,0}(x_0) + MC_2 \times T'_{i,2}(x_2) +$$

$$MC_3 \times T'_{i,3}(x_3) + MC_4 \times T'_{i,4}(x_4)$$

其中 $MC_i \times T'_{i,j}(x_j)$ 作为查找表二型表,根据置换混淆原则在两边同时插入混合双射 $mb'_{i,j}$ 和 MB_i 得到:

$$MB_i \times MC_i \times T'_{i,j} \times mb'_{i,j}(x_i)$$

此即为置乱编码后的二型表,为8bit输入32bit输出表,如图5所示。

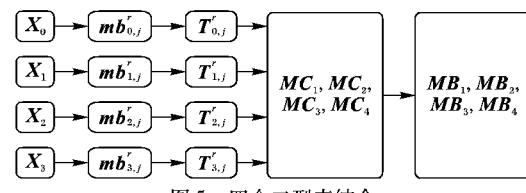


图5 四个二型表结合

Fig. 5 Combination of four two-type tables

接下来制作三型表。三型表要与前面的二型表相结合,根据网路编码原则需要消掉前面的混合双射 MB_i ,又要与下轮的混合双射 mb_i 抵消,所以三型表如下所示:

$$(mb'^{r+1}_{i,j})^{-1} \times MB_i^{-1}$$

为8bit输入32bit输出表。

接下来是四型表。因为在AES中的矩阵有加法操作,但白盒AES中只有各种各样的查找表,所以要将矩阵的加法用查找表的形式表示出来。以上三种类型的查找表都是矩阵的乘法形式转换成的,所以在此应该对矩阵的加法做查找表。查找表的做法是:其中一侧是输入,是两个4bit的列向量;另一侧是输出,是两个输入的和。如图6所示。

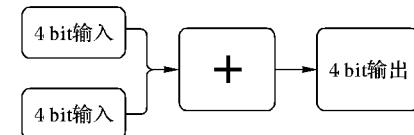


图6 四型表

Fig. 6 Four-type table

一型表是对整个算法进行混淆并且对第一轮的混合双射 mb_1 和最后一轮的 mb_{10} 进行消除,为一个8bit输入128bit输出。

3.3 BGE 攻击

BGE的主要思想是通过对单个查找表观察来回复密钥是困难的,但是通过组合查找表为一轮来分析,恢复密钥信息是比较容易的。

他们将白盒AES的二型表和三型表结合起来考虑:

$$(mb'^{r+1})^{-1} \times MB^{-1} \times MB \times MC \times$$

$$[T'_{i,0} \ T'_{i,1} \ T'_{i,2} \ T'_{i,3}]^T \times mb' \times [x_0 \ x_1 \ x_2 \ x_3]^T =$$

$$(mb')^{-1} \times MC \times [T'_{i,0} \ T'_{i,1} \ T'_{i,2} \ T'_{i,3}]^T \times mb \times$$

$$[x_0 \ x_1 \ x_2 \ x_3]^T =$$

$$\text{diag}((mb_0'^{r+1})^{-1}, (mb_1'^{r+1})^{-1}, (mb_2'^{r+1})^{-1}, (mb_3'^{r+1})^{-1}) \times$$



$$\begin{aligned} & MC \times [T'_{i,0} \quad T'_{i,1} \quad T'_{i,2} \quad T'_{i,3}]^T \times \\ & \text{diag}(\mathbf{mb}'_0, \mathbf{mb}'_1, \mathbf{mb}'_2, \mathbf{mb}'_3) \times [x_0 \quad x_1 \quad x_2 \quad x_3]^T \end{aligned}$$

结合之后 MB 消除掉了, 只剩下混合双射 $(\mathbf{mb}')^{-1}$ 和 \mathbf{mb}' 。令 $P'_i = \mathbf{mb}'_i, Q'_i = (\mathbf{mb}'^{i+1})^{-1}$, 它们可以看成是输入输出置乱编码, 如图 7 所示。

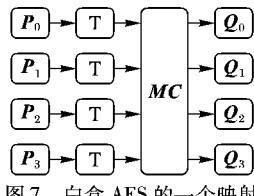


图 7 白盒 AES 的一个映射

Fig. 7 A mapping of white-box AES

攻击的主要步骤如下:1) 把非仿射变换 P, Q 转变为仿射映射;2) 计算出仿射映射 Q ;3) 由 P, Q 计算出隐藏在 T 盒中的密钥。具体过程见参考文献[2], 这里不再详细叙述。

3.4 白盒 AES 的修改

Karroumi^[3]对 Chow 的白盒 AES 进行了修改。

AES 是基于有限域 $GF(2^8)$ 上的简单的代数结构, 如果改变 AES 的所有常量, 包括不可约多项式、矩阵参数、仿射变换, 就构造出新的对偶密码。在文献[8]中有 240 个新的 AES 对偶密码被构造, 在文献[10]中被扩展到了 61 200 个。

AES 和对偶 AES 的输出是有关系的。存在一个线性变换 Δ 将 AES 的比特状态映射到对偶 AES 的比特状态, 即 $X_{\text{对偶}} = \Delta(X)$, 相同的变换还有 $P_{\text{对偶}} = \Delta(P), C_{\text{对偶}} = \Delta(C), K_{\text{对偶}} = \Delta(K)$ 。

每个对偶 AES 代表都被分配一个从 1 到 61 200 的索引, 随机选择 10 个不重复的 $\sigma_r \in \{1, 2, \dots, 61200\}$ ($r = 1, 2, \dots, 10$)。定义 $\Delta_{\sigma_r}: GF(2^8) \rightarrow GF(2^8)$ 为一个线性映射, 将 AES 的一个字节状态映射到 σ_r 对偶映射 Δ_{σ_r} 。能被表示为一个 $GF(2)$ 上的 8×8 的可逆矩阵 M_r , $\Delta_{\sigma_r}^{-1}$ 也可以由 M_r 的逆获得。

字节替换操作为一个代数结构:

$$IS: GF(2^8) \rightarrow GF(2^8), x \rightarrow Ax + b$$

这里 A 是一个矩阵变换, b 是一个常向量。对偶变换变为 $IS^{\sigma_r}(x) = (M_r \times A \times M_r^{-1}) \times x + M_r \times b$, 对偶子密钥为 $K_{i,j}^{\sigma_r} = M_r \times K_{i,j} \circ M_r^{-1}$ 。则新的第 r 轮 T^{σ_r} 盒为:

$$T_{i,j}^{\sigma_r} \triangleq IS^{\sigma_r}(x \oplus K_{i,j}^{\sigma_r}) \oplus K_{i,j}^{\sigma_r}; i, j \in [0, 1, 2, 3]$$

$$T_{i,j}^{\sigma_r} \triangleq IS^{\sigma_r}(x) \oplus K_{i,j}^{\sigma_r};$$

$$r \in [2, 3, \dots, 10], i, j \in [0, 1, 2, 3]$$

其中对于 $i \in \{1, 2, \dots, 10\}$, $K_{i,j}^0 = \Delta_{\sigma_1}(K_{i,j}^{\sigma_r})$, $K_{i,j}^{\sigma_r} = \Delta_{\sigma_1}(K_{i,j}^{\sigma_r})$ 。

在这里用与混合双射相同的原则, 即用矩阵左乘输入向量, 来达到混淆向量的目的。Karroumi^[3]的想法是将 Δ - 编码应用到混合双射当中, 用 $\Delta_r \times \Delta_{r-1}^{-1}$ 来表示上一轮的输出 Δ - 编码和当前轮的输入 Δ - 编码与混合双射 $P_{i,j}^r$ 相结合, 如图 8 所示。

4 本文安全传输方法的设计

任务规划系统对于航空任务的完成至关重要, 因此敌手会用尽其所能的手段来攻击它, 包括在我方安插卧底来了解我方任务规划系统的具体实施流程, 或通过越来越先进的手段比如恶意主机攻击、旁信道攻击^[6]等攻击手段来攻击我方

软件。在面临这种攻击时, 任务规划系统的安全传输的具体执行情况将完全暴露在敌手的眼前, 让他们轻而易举地抽出密钥, 这就是 Chow 提到的白盒攻击环境。所以本文必须想一个办法来对付这样的情况, 即应用白盒加密系统来改善。

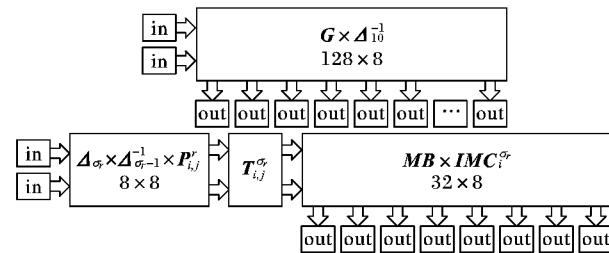


图 8 Mohamed Karroumi 改进的表

Fig. 8 Improved table by Mohamed Karroumi

由于白盒 AES 是把密钥嵌入到加解密算法里面, 生成一些查找表, 在加解密过程中, 通过查找表来生成相应的密文和明文。所以可以设计一个专门用来生成查找表的驱动程序来不断构造查找表, 或者可以生成固定查找表嵌入到传输程序当中。由于驱动程序在生成查找表时会用到密钥, 所以驱动程序生成 AES 查找表的过程应在安全的地方进行。

本文设计了一种可以抵抗白盒攻击环境的安全传输方法。首先在飞机基地用不同类型的密钥通过驱动程序生成不同的查找表, 加密时可以根据需要选择查找表来进行加密。在安全传输中加入一个生成白盒 AES 的驱动程序, 用来根据系统消息的报头来选用相应的白盒 AES。运行流程如图 9 所示。

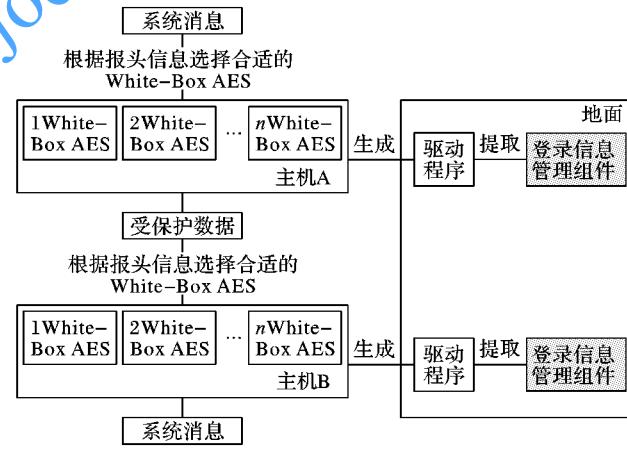


图 9 改进的安全传输

Fig. 9 Improved security transmission

这样, 通过生成 Karroumi^[3]改进的 AES 查找表来设计白盒安全传输应用给发送接口传递消息类型、数据、数据长度和用户信息四个参数。接口根据消息类型判断是否需要加密, 如果需要, 则驱动程序在客户端独立线程获得安全参数, 生成加密 AES 查找表。消息数据输入到改进的白盒 AES, 然后将输出的数据封装成如图 4 所示的报文, 最后将报文利用飞机上的通信协议发送出去。

驱动程序的设计如下:

1) 从客户端独立线程中取出安全参数作为密钥, 通过密钥扩展函数将其扩展为 10 组子密钥。下面以利用 128 位的密钥制作二型表为例来说明查找表的制作过程。128 位的密钥为 3C A1 0B 21 57 F0 19 16 90 2E 13 80 AC C1 07 BD, 通过密钥扩展算法^[7]得出第一轮的子密钥为 45 64 71 B0 12 94 68



A6 82 BA 7B 26 2E 7B 7C 9B。

2)按照3.2节所述进行制表。将子密钥排成一个矩阵

$$\mathbf{K} = \begin{bmatrix} 45 & 12 & 82 & 2E \\ 64 & 94 & BA & 7B \\ 71 & 68 & 7B & 7C \\ B0 & A6 & 26 & 9B \end{bmatrix}$$

由于AES分组矩阵时,每个明文

以128bit分为一组,则明文也排成一个矩阵,设明文为 $\mathbf{P} = \begin{bmatrix} 00 & 01 & 02 & 03 \\ 10 & 11 & 12 & 13 \\ 20 & 21 & 22 & 23 \\ 30 & 31 & 32 & 33 \end{bmatrix}$,取出其中一列 $[01 \ 11 \ 21 \ 31]^T$ 来演

示查找表制作过程。将这列与子密钥矩阵第二列相加为: $\mathbf{P}(2) + \mathbf{K}(2) = [13 \ A5 \ 89 \ D7]^T$ 。 $\mathbf{P}(2)$ 表示矩阵 \mathbf{P} 的第二列, $\mathbf{K}(2)$ 表示矩阵 \mathbf{K} 的第二列。经过S盒变换之后为 $S(\mathbf{P}(2) + \mathbf{K}(2)) = [C7 \ BE \ 46 \ FF]^T$ 。

$$\text{经过列混合即左乘以 } \mathbf{MC} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

将 \mathbf{MC}

划分为 $\mathbf{MC} = (\mathbf{MC}_1 \ \mathbf{MC}_2 \ \mathbf{MC}_3 \ \mathbf{MC}_4)$,则:

$$\mathbf{MC} \times S(\mathbf{P}(2) + \mathbf{K}(2)) =$$

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} C7 \\ BE \\ 46 \\ FF \end{bmatrix} =$$

$$[\mathbf{MC}_1 \ \mathbf{MC}_2 \ \mathbf{MC}_3 \ \mathbf{MC}_4] \times [C7 \ BE \ 46 \ FF]^T = C7 \times \mathbf{MC}_1 \oplus BE \times \mathbf{MC}_2 \oplus 46 \times \mathbf{MC}_3 \oplus FF \times \mathbf{MC}_4 =$$

$$\begin{bmatrix} 95 \\ C7 \\ C7 \\ 52 \end{bmatrix} \oplus \begin{bmatrix} D9 \\ 67 \\ BE \\ BE \end{bmatrix} \oplus \begin{bmatrix} 46 \\ CA \\ 8C \\ 46 \end{bmatrix} \oplus \begin{bmatrix} FF \\ FF \\ 18 \\ E5 \end{bmatrix} = \begin{bmatrix} F5 \\ 95 \\ ED \\ 4F \end{bmatrix}$$

即明文[01]经过上述混合双射后变换后为[95 C7 C7 52]^T,在经过混合双射^[1]和对偶变换^[8]后即为修改后的二型表为 $(01) \rightarrow \Delta_1 \times \mathbf{mb}_1 \times [95 \ C7 \ C7 \ 52]^T \times \mathbf{MB}_1$ 为一个 $P:2^8 \rightarrow 2^{32}$ 的映射,将其输入穷举后也就是256个输入得到256个输出,将这个对应制成查找表如表1。

表1 二型表
Tab. 1 Two-type table

输入	输出
00	BC AB 8E 9D
01	56 CF 8F 2D
...	...
FF	B4 3F 7F 2A

表1所占用的内存空间为 $2^9 = 512$ Byte,白盒AES一轮需要16个这样的表,总共10轮,所以占用的总内存空间为 $160 \times 512 = 81920$ 字节。接下来的一、三、四型表按照同样的思路制作,最后得出整个白盒AES查找表,其需要内存770048 MB^[1]。

3)将查找表按照AES执行顺序进行整理排列,然后将其嵌入到内存当中。以后的加密解密就通过查找表的方式进行,加密完成后,驱动程序将加密AES查找表从内存中擦除。

4)接收端收到消息,并根据报头查看消息是否加密。

5)如果加密,则驱动程序去获得安全参数库里的安全参数,生成解密AES查找表,加密消息通过查找对应的查找表获得相应的明文。

程序运行过程的异常处理方式如下:

- 1)建立连接失败,尝试三次仍然失败,返回错误码给应用;
- 2)发送数据失败,尝试三次仍然失败,返回错误码给应用。

5 方法安全性评估

本文设计的安全性依赖于白盒AES的安全性,其中由Chow等^[1]设计的白盒AES可以被BGE算法^[2]在 2^{30} 攻破,而Karroumi等^[3]利用对偶密码来改造白盒AES,目前暂时未被破解。

在改进的白盒AES中,用到的对偶密码有61200个。这61200个对偶密码中的每一个都可以作用到二型表的改进当中。由于白盒AES每一轮中有四个二型表,每一个二型表都可以与61200个对偶密码中的一个来作用,则可以有 $642000^4 \approx 2^{63}$ 种可能。在白盒攻击环境中,攻击者只能看到输入与对应的输出,无法了解使用的哪一种对偶密码进行作用,只能用穷举的方法,这就使得攻击复杂度有原来的 $4 \times 2^{25} = 2^{27}$ 增加到了 $4 \times 2^{25} \times 2^{63} = 2^{90}$ 。这种改进使得攻击复杂度大大提高,保证了白盒AES的安全可靠。

对于本文设计的新的安全传输方法,由于生成白盒AES是在飞机基地事先秘密完成,而白盒AES在使用过程中被攻破的复杂度很大,所以整个安全传输方法在白盒攻击环境下是安全的。

6 结语

本文介绍了白盒攻击环境下任务规划系统的安全传输方法。首先,对传统的高级加密标准白盒化,使其可以抵抗白盒攻击;其次,按照给出的白盒AES生成算法,利用不同的密钥生成不同的白盒AES程序;最后,将相应的白盒AES程序嵌入到任务规划系统的安全传输当中。经过理论分析,修改后的任务规划系统中的安全传输方法提高了攻击难度,达到足够的安全强度,可以保护通信密钥。

参考文献 (References)

- [1] CHOW S, EISEN P, JOHNSON H, et al. White-box cryptography and an AES implementation [C]// SAC 2002: Proceedings of the 9th Annual International Workshop on Selected Areas in Cryptography, LNCS 2595. Berlin: Springer-Verlag, 2003: 257 - 270.
- [2] BILLET O, GILBERT H, ECH-CHATBI C. Cryptanalysis of a white-box AES implementation [C]// SAC 2004: Proceedings of the 11th Annual International Workshop on Selected Areas in Cryptography, LNCS 3357. Berlin: Springer-Verlag, 2005: 227 - 240.
- [3] KARROUMI M. Protecting white-box AES with dual ciphers [C]// ICISC 2010: Proceedings of the 13th International Conference on Information Security and Cryptology, LNCS 6829. Berlin: Springer-Verlag, 2011: 278 - 291.
- [4] XIAO Y, LAI X. A secure implementation of white-box AES [C]// CSA 2009: Proceedings of the 2nd International Conference on Computer Science and its Applications. Piscataway, NJ: IEEE, 2009: 410 - 415.

(下转第498页)



- trieval: a unified construction [C]// ICALP 2001: Proceedings of the 28th International Colloquium on Automata, Languages and Programming, LNCS 2076. Berlin: Springer-Verlag, 2001: 912–926.
- [8] ITOH T. Efficient Private information retrieval (special section on cryptography and information security [J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 1999, E82-A(1): 11–20.
- [9] ISHAI Y, KUSHILEVITZ E. Improved upper bounds on information-theoretic private information retrieval [C]// STOC '99: Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing. New York: ACM, 1999: 79–88.
- [10] BEIMEL A, ISHAI Y, KUSHILEVITZ E, et al. Breaking the $O(n^{1/(2k-1)})$ barrier for information-theoretic private information retrieval [C]// FOCS '02: Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science. Washington, DC: IEEE Computer Society, 2002: 261–270.
- [11] YANG E Y, XU J, BENNETT K H. Private information retrieval in the presence of malicious failures [C]// COMPSAC '02: Proceedings of the 26th Annual International Computer Software and Applications Conference on Prolonging Software Life: Development and Redevelopment. Washington, DC: IEEE Computer Society, 2002: 805–812.
- [12] 廖干才, 罗守山. 一种基于秘密共享的对称私有信息检索协议 [EB/OL]. (2008-05-05) [2016-03-05]. <http://www.paper.edu.cn/releasepaper/content/200805-65>. (LIAO G C, LUO S S. A protocol of symmetrically private information retrieval based on secret sharing [EB/OL]. (2008-05-05) [2016-03-05]. <http://www.paper.edu.cn/releasepaper/content/200805-65>.)
- [13] BEIMEL A, ISHAI Y, KUSHILEVITZ E. General constructions for information-theoretic private information retrieval [J]. Journal of Computer and System Sciences, 2005, 71(2): 213–247.
- [14] BEIMEL A, STAHL Y. Robust information-theoretic private information retrieval [C]// SCN 2002: Proceedings of the Third International Conference on Security in Communication Networks, LNCS 2576. Berlin: Springer-Verlag, 2003: 326–341.
- [15] DE SANTIS A, DESMEDT Y, FRANKEL Y, et al. How to share a function securely [C]// STOC '94: Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing. New York: ACM, 1994: 522–533.
- [16] BOYLE E, GILBOA N, ISHAI Y. Function secret sharing [C]// EUROCRYPT 2015: Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 9057. Berlin: Springer-Verlag, 2015: 337–367.
- [17] GILBOA N, ISHAI Y. Distributed point functions and their applications [C]// EUROCRYPT 2014: Proceedings of the 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 8441. Berlin: Springer, 2014: 640–658.
- [18] KOMARGODSKI I, ZHANDRY M. Cutting-edge cryptography through the lens of secret sharing [C]// TCC 2016-A: Proceedings of the 13th International Conference on Theory of Cryptography, LNCS 9563. Berlin: Springer, 2016: 449–479.
- [19] 俞志斌, 周彦晖. 基于关键字的云加密数据隐私保护检索 [J]. 计算机科学, 2015, 42(S1): 365–369. (YU Z B, ZHOU Y H. Keyword based privacy-preserving retrieval over cloud encrypted data [J]. Computer Science, 2015, 42(S1): 365–369.)

This work is partially supported by the National Natural Science Foundation of China (U1433130), the Ministry Basic Research Program (Chunhui Program) of China (Z2014045).

YUAN Dazeng, born in 1992, M. S. candidate. Her research interests include security protocol, network security, big data.

HE Mingxing, born in 1964, Ph. D., professor. His research interests include modern cryptographic algorithm, security protocol, key management, electronic commerce/e-government security.

LI Xiao, born in 1972, Ph. D., associate professor. His research interests include information security, cryptography.

ZENG Shengke, born in 1982, Ph. D., associate professor. Her research interests include information security, cryptography.

RSA, DSS, and other systems [C]// CRYPTO 1996: Proceedings of the 16th Annual International Cryptology Conference, LNCS 1109. Berlin: Springer-Verlag, 1996: 104–113.

- [10] BIRYUKOV A, DE CANNIÈRE C, BREAKEN A, et al. A toolbox for cryptanalysis: linear and affine equivalence algorithms [C]// EUROCRYPT 2003: Proceedings of the 2003 International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 2656. Berlin: Springer-Verlag, 2003: 33–50.

This work is partially supported by the National Major Science and Technology Projects (2012ZX01041-006).

CUI Xining, born in 1964, Ph. D., research fellow. His research interests include distributed security management, parallel distributed system, real-time operating system, information security.

DONG Xingting, born in 1989, M. S. candidate. His research interests include cryptography, information security.

MU Ming, born in 1973, M. S., research fellow. His research interests include software engineering, software testing.

WU Jiao, born in 1987, M. S., engineer. Her research interests include embedded software, airborne network.

(上接第 487 页)

- [5] DE MULDER Y, ROELSE P, PRENEEL B. Cryptanalysis of the Xiao-Lai White-Box AES implementation [C]// SAC 2012: Proceedings of the 19th International Conference on Selected Areas in Cryptography, LNCS 7707. Berlin: Springer-Verlag, 2012: 34–49.
- [6] 张效强, 王峰, 高开明. 基于加密算法的数据安全传输的研究与设计[J]. 计算机与数字工程, 2008, 36(5): 107–109. (ZHANG X Q, WANG F, GAO K M. Research and design for secure transmission of data based on encrypt algorithms [J]. Computer and Digital Engineering, 2008, 36(5): 107–109.)
- [7] National Institute of Standards and Technology. Advanced Encryption Standard (AES) (FIPS PUB 197) [S/OL]. Federal Information Processing Standards Publication, 2001 (2001-11-06) [2016-03-06]. <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.
- [8] BARKAN E, BIHAM E. In how many ways can you write Rijndael [C]// ASIACRYPT 2002: Proceedings of the 2002 International Conference on the Theory and Application of Cryptology and Information, LNCS 2501. Berlin: Springer-Verlag, 2002: 160–175.
- [9] KOCHER P C. Timing attacks on implementations of Diffie-Hellman,