车载 ECU 加密通信与身份认证机制研究

吴贻淮，　李　飞*，　覃　周

(成都信息工程大学 信息安全学院，四川 成都　610065)

摘　要：针对车载 ECU 使用明文通信,ECU 固件易被篡改的安全问题提出了一种新的车载 ECU 加密通信与身份认证机制,该机制使用椭圆曲线加密算法(ECC)加密通信密钥,使用对称加密算法加密数据,采用哈希算法来验证 ECU 固件完整性.仿真实验分析表明,该机制具有计算快、安全性高、低成本等优点,能够保证 ECU 间的安全通信,解决 ECU 固件易被篡改的问题.

关键词：车载网络安全；　加密通信；　车载 ECU

中图分类号：TP399　　文献标识码：A　　文章编号：1671-9743(2017)05-0075-03

DOI:10.16074/j.cnki.cn43-1394/z.2017.05.017

1　车载信息系统中的安全问题

车载网络是一个由 ECU (Electronic Control Unit)和总线组成的集自动化控制、通信、计算机等为一体的汽车内部通信网络.随着计算机网络与车载移动通信技术的发展,特别是近年来随着智能交通、车联网等概念的提出，使得汽车与外部网络间的信息交互越来越频繁.人们在享受车联网带来的便利(例如智能导航、智能停车)的同时也面临着巨大的车载信息系统安全问题.例如 2015 年 1 月黑客利用宝马车载系统的安全漏洞,远程攻击安装有该系统的汽车影响涉及 200 万辆宝马汽车.2015 年 2 月 9 日黑客利用安吉星 OnStart 的系统漏洞远程控制汽车.使得车载信息系统安全问题倍受瞩目.

车载 ECU 以总线方式连接,ECU 间的通信是通过将数据包广播到总线上的所有组件,由组件自行决定是否接收该数据包，这样虽然有效的解决了由于 ECU 数量增加而带来的线束增多的问题,然而却也为车载信息系统安全问题带来了巨大的隐患，其中以 CAN(Controller Area Network)网络的安全问题最为突出.由于 CAN 网络作为车载信息系统核心 ECU 的连接网络,通过其传输协议可知,CAN 的数据包不同于传统以太网数据包,CAN 的数据包中只有目的地址没有源地址.这就意味着车载网络中的任意 ECU 都可以访问 CAN 网络中的核心 ECU 例如发动机、转向器等 ECU.所以只要攻击者能获得 CAN 网络的执行权限就能够向 ECU 发送伪造的数据包、修改 ECU 的行为,从而实现对车辆的完全控制.由上可知车载 ECU 的安全直接决定着整个车载信息系统的安全，可以说没有车载 ECU 安全就没有车载信息系统安全.然而由于现行的车载信息系统的数据是以明文方式传输，同时缺少对车载 ECU 的代码完整性校验机制,使得如何保证车载 ECU 代码完整性,维护车载信息系统安全成为难题. 为应对这些安全威胁,Rafael Zalman,Albrecht Mayer[1]引入了 MAC (Message Authentication Code)解决了信息完整性认证问题,但没有解决数据以明文形式传输的问题.Andre Groll,Christoph Ruland[2]在车载网络当中引入 KDC (Key Distribution Centre)解决了数据明文传输问题,但缺少对车载 ECU 身份认证机制.为此本文提出了一种基于 ECC (Elliptic Curves Cryptography)加密算法的 ECU 加密通信机制和 ECU 身份认证方式,能够解决 ECU 间的安全通信和 ECU 被易篡改的问题.

2　ECC 加密算法

在汽车的生命周期当中若车载 ECU 的通信密钥固定不变.攻击者可以通过分析大量的加密数据,从而破译出车载 ECU 的通信密钥. 采用 ECC 加密算法为车载 ECU 的通信传输对称加密所需的通信密钥.能够有效抵抗暴力破解和分析.

ECC 加密算法首先确定一个有限域,这个域只有一个素数 p.

1) 用户 X 在这个有限域中选定一条椭圆曲线 (a,b),并取椭圆曲线上点 G 作为基点.

2) 用户 X 在 1~p-1 之间随机选出一个素数作为私钥 k,并根据加法则,并生公开密钥 $K=kG$.

3) 用户 X 将 $Ep(a,b)$ 和点 K,G 传给用户 B.

4) 用户 Y 接受到消息后,将待传输的明文编码到

收稿日期：2017-03-04

基金项目：四川省科技支撑计划基金资助项目(2016GZ0343).

作者简介：吴贻淮，1991 年生，男，福建宁德人，硕士研究生，研究方向：车载网络信息安全；

* 通信作者：李　飞，1966 年生，男，湖南常德人，教授，硕士研究生导师，研究方向：汽车信息系统安全防护体系.

$Ep(a,b)$ 上一点 M，并产生一个随机整数 r.

5) 用户 Y 将计算点 $C_1=M+rK$；$C_2=rG$.

6) 用户 Y 将 C_1,C_2 传个用户 X.

7) 用户 X 接受到信息后，再进行计算.计算公式：$C_1-kC_2=M+rK-k(rG)=M+rK-r(rG)=M$.

另外 ECC 加密算法与 RSA，Elgamal 相比具有抗攻击性强、计算量小、处理速度快、存储空间占用小、带宽要求低等优点.因而更加适合车载网络这样硬件资源有限的嵌入式环境.

3 车载 ECU 加密通信机制和身份认证方式

车载ECU 进行加密通信可以在一定程度上保证车载信息系统的安全.从密码学的角度出发，实现一次一密的加密通信具有非常高的安全性.然而在车载信息系统这样的嵌入式平台实现一次一密的加密通信，无论是现有的计算资源还是通信带宽都无法承受一次一密加密通信所带来的巨大压力.然而在车辆的每次使用周期当中，使用不同的通信密钥对车载 ECU 的通信进行加密是可以实现.另外对车载 ECU 进行身份认证，有利于保证车载 ECU 在汽车的生命周期当中不被恶意篡改或冒充，进而更加有效的保证车载信息系统的安全.车载 ECU 的加密通信与身份认证具体步骤包括车载 ECU 初始、车载 ECU 身份认证和车载 ECU 加密通信三个部分.

3.1 车载 ECU 初始

车载 ECU 的初始工作是一个由汽车的购买者和 TSP (Telematics Service Provider) 共同参与的一个过程，具体过程如下图 1 所示.

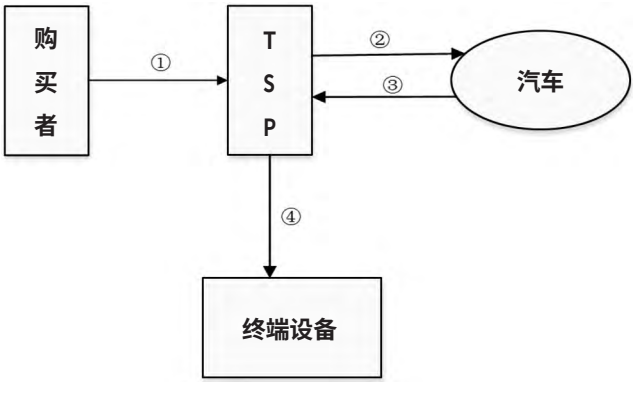

图 1 初化始过程

①购买者→TSP：K

购买者向 TSP 发送一个初始密钥 K，该密钥由购买者和 TSP 共同保留.作为后续车载 ECU 的更新和维修使用.

②TSP→汽车：Mi

TSP 在接受到私钥 K 后，使用 md5 加密 K 得到新的的序列 S. 最后将包含序列 S 的 ECU 可执行文件 Mi 写入车载 ECU 中. 重而保证每辆汽车的 ECU 代码存储区的 hash 特征码具有唯一性.

③汽车→TSP：H(Ni)

汽车在完成 ECU 可执行文件写入完成之后，计算各个 ECU 代码存储区的 hash 特征码 H(Ni) 返回给 TSP.

④TSP→终端设备：H(Ni)

TSP 在获得各个 ECU 代码存储区的 hash 特征码 H(Ni) 后将其写入终端设备当中，终端设备是一种类似于加密狗的具有逻辑处理能力的嵌入式设备.

3.2 车载 ECU 身份认证

中央网关连接着整个车载网络，实现不同网络之间的协议转换，能够实现对整个车载网络的监控.为实现对车载 ECU 的身份认证，在汽车开机自检的时候中央网关必须通过与 ECU 进行会话，从而实现对 ECU 的身份认证.具体认证过程如图 2 所示.

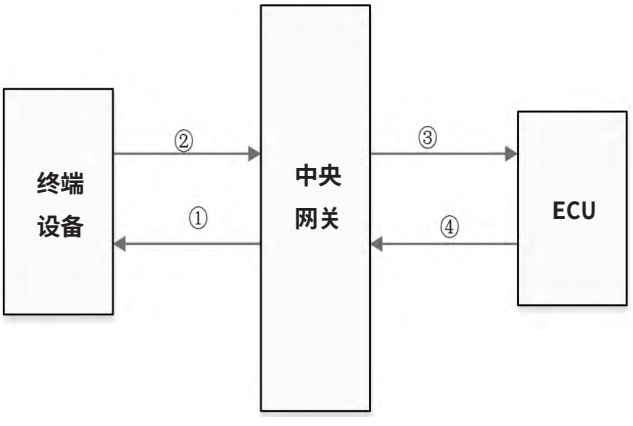

图 2 具体认证过程

①中央网关→终端设：EK[Q||ID||ES||R].

终端设备通过 OBD (On-Board Diagnostics) 接口接入车载网络当中，之后中央网关向终端设备发送获取各个 ECU 代码存储区特征码的请求.该请求包含四个数据项：一是请求码 Q，二是中央网关 ID，ES 对称加密通信密钥，三是随机数 R，该请求通过 ECC 加密算法 EK 加密.

②终端设备→中央网关：ES[SH||H(R)||T]

终端设备对中央网关发出应答，该应答通过对称加密算法 ES 加密传输，应答的内容包括各个 ECU 代码存储区的特征码数组 SH，随机数 R 的 hash 值 H(R) 以及时间戳 T.

③中央网关→ECU：Ek[Q||ID||ES||R||T]

中央网关在获得 ECU 代码存储区的特征码数组 SH 后对各个 ECU 进行身份认证，通过使用 ECC 加密算法 Ek 向各个车载 ECU 发送一个包含求码 Q，需要进行身份认证的 ECU 的 ID，ES 对称加密通信密钥，随机数 R，时间戳 T 的请求.

④ECU→中央网关：ES[H(M)||ID||H(R)]

接受到身份认证请求的车载 ECU，首先进行计算自

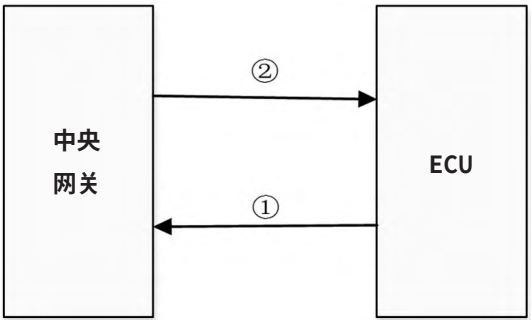

图 3　通信密钥获取

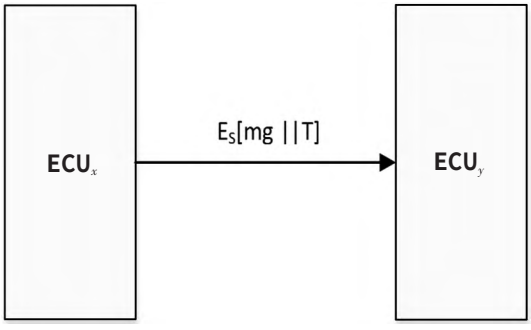

图 4　ECU 之间的加密通信

身代码存储区的硬件 hash 值 H(M)，之后使用对称加密加密算法 ES 加密一个包含 H(M)，自身的 ID 以及随机数 R 的 hash 值 H(R) 的应答.

3.3　车载 ECU 加密通信

车载 ECU 的加密通信主要分为两步：

一通信密钥获取：该过程在发生在汽车启动的时候.由中央网关随机生成一个密钥，该密钥作为整个车载网络的通信密钥.具体步骤如下图 3 所示.

①ECU→中央网关：EK[Q||EN||ID||H(M)||R].

ECU 使用 ECC 加密算法 EK 向中央网关发送一个报文，该报文包含车载网络通信密钥获取请求 Q，对称通信密钥 EN，ECU 的 ID，ECU 代码存储区的硬件 hash 值 H(M) 以及随机数 R.

②中央网关→ECU：ES[EC||T||H(R)].

中央网关通过 ID 和 H(M) 判断当前 ECU 是否合法.对应合法的 ECU 发出应答，应答的内容包括车载网络通信密钥 EC，时间戳 T，随机数 R 的 hash 值 H(R)，其中 ES 为对称加密算法.

二加密通信：该过程发生在所有的车载 ECU 均获得通信密钥之后，该密钥在本次汽车从启动到最后关闭的整个使用过程中均有效，为了抵抗重放攻击，每个通信消息都附上时间戳，于是最终在 CAN 总线上传送的密文为 ES[mg||T]其中 ES 为对称加密算法，mg 为需要发送的消息，T 为时间戳.接受方在接受到密文后使用自己从中央网关获得的通信密钥就可以对密文进行解密，详细流程见图 4.

4　结束语

未来车载信息系统安全将面临越来越严峻的挑战，因此车载信息系统安全也将会被更加重视.本文所提出的车载 ECU 加密通信机制，结合车载信息系统自身特点，能够以较小的代价在一定程度上保证系统的安全性，达到了应用级别.该研究实现车载 ECU 的加密通信与身份认证，在一定程度上能够解决车载 ECU 固件被篡改、假冒攻击、重放攻击等安全问题.

参考文献：

[1]Andre Groll. Christoph Ruland. Secure and authentic communication on existing in-vehicle networks [J]. Intelligent Vehicles Symposium，2009：1931-0587.

[2]Ishtiaq Roufa R M，Mustafaa H，Travis Taylora S O，et al.Security and privacy vulnerabilities of in-car wireless networks：A tire pressure monitoring system case study[C]//19th USENIX Security Symposium，Washington DC，2010：11-13.

[3]许冬琦.车载以太网：下一代联网技术让汽车更智能[J].通信世界，2012，(6)：21-21.

[4]Rafael Zalman.Albrecht Mayer.A secure but still safe and low cost automotive communication technique [C] // 2014 51stACM/EDAC/IEEE Design Automation Conference (DAC)，2014：1-5.

Research on Vehicle ECU Communication Encryption and Identity Authentication Mechanism

WU Yi-huai，　LI Fei*，　QIN Zhou

(*College of Information Security Engineering，Chengdu，Sichuan 610065*)

Abstract：Aiming at the secure problems that the in-Vehicle communication isn't encrypted and ECU's ROM can be easily tampered with，we propose a new ECU identity authentication and encrypted in-Vehicle communication mechanism. It applies symmetry encryption algorithm to encrypt the communication and applies Elliptic Curve Cryptography (ECC) algorithm to encrypt session keys and utilizes the hash algorithm to verify the integrity of firmware ECU. Simulation experimental results shows that the mechanism is low cost，high speed and high safety. It can ensure secure communication between ECUs and maintain the integrity of ECU's firmware.

Key words：in-vehicle network security；　encrypted communication；　vehicle ECU