

针对国产加密技术的信号系统网络捕包解密方案

郝晓平

(郑州地铁集团有限公司, 450018, 郑州 // 高级工程师)

摘要 针对轨道交通信号系统采用的国产密码技术, 提出了信号系统解密网络抓包的方案。介绍了采用网络捕包解密方案的信号系统结构, 详细阐述了在线解密和离线解密的工作流程。通过实验室测试, 验证了网络捕包解密方案的实用性和可行性。

关键词 轨道交通; 信号系统; 国产加密技术; 网络捕包; 解密方案

中图分类号 U231.7

DOI: 10.16037/j.1007-869x.2021.04.022

A Method of Decrypting Network Packet in Encrypted Signaling System Targeting Domestic Cryptographic Technology

HAO Xiaoping

Abstract Targeting domestic cryptographic technology adopted in rail transit signaling system, a method of decrypting network packet in encrypted signaling system is proposed. The signaling system structure that captures network packets is introduced and the workflows of online decryption and offline decryption are expounded. Through laboratory experiments, the applicability and feasibility of network packet decryption solution is verified.

Key words rail transit; signaling system; domestic cryptographic technology; network packet; decryption method

Author's address Zhengzhou Metro Group Co., Ltd., 450018, Zhengzhou, China

采用国产加密技术的信号系统, 通过在既有的信号系统上增设国产加密安全芯片等设备, 用国产加密算法对通信数据进行加密, 使通信数据得到可鉴别性保护、不可否认性保护、机密性保护和完整性保护。这一技术弥补了信号系统内部通信的信息安全漏洞, 实现了信号系统通信的高安全性和高可靠性, 提升了信号系统的信息安全水平。但美中不足的是, 该技术却降低了信号系统的可维护性。

信号系统的一般调试维护是通过通信两侧的数据通信交换机对网络数据进行抓包, 并解析抓包

数据来完成的。而经国产加密技术加密后的网络信息已全部变为密文, 且加密密钥多采用动态协商机制, 只有对已加密的网络捕包进行解密后, 才能与一般的调试维护同步对接。否则, 开发调试人员面对加密数据将无从解析, 也就无法进一步定位问题和分析排查。这给信号系统的调试维护带来了较大的不便和不确定性。

要解密已加密的网络数据, 关键在于如何获取加密密钥, 并将加密密钥与加密报文对应起来。加密密钥采用的点对点动态协商机制, 增大了获取加密密钥的难度。此外, 在解密过程中, 还需保证加密密钥的机密性, 并尽量降低调试维护的操作难度, 以实现与一般的调试维护方式同步对接。

本文针对国产加密技术, 提出了一个网络捕包解密方案, 可对加密的网络数据进行解密。该方案通过系统软件和解密工具的紧密配合, 取得动态协商的密钥, 并将密钥与数据内的报文逐一对应, 从而完成对网络抓包的解密。

1 网络捕包解密方案

1.1 信号系统结构

采用网络捕包解密方案的信号系统, 在既有信号系统上集成了国产加密设备。其系统结构如图 1 所示。在图 1 中, 应用层由 CC(车载控制器)、ZC(区域控制器)、LC(线路控制器)、CI(计算机联锁)、ATS(列车自动监控)、MSS(维护监测系统)等子系统组成, 通信层为 DCS(数据通信系统)。

采用网络捕包解密方案的信号系统在信号系统架构和 PKI(公钥基础设施)模型的基础上增加了证书密钥管理服务器和硬件加密机, 在应用层设备上增加了国产加密安全芯片。通过证书密钥管理系统, 信号系统可以实现保存会话密钥、导出会话密钥及切换模式的操作。

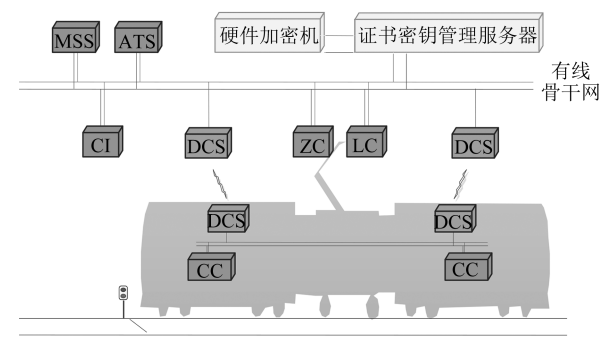


图 1 采用网络捕包解密方案的信号系统结构

1.2 应用场景分析

在信号系统调试维护业务中,网络抓包解密工作按应用场景主要分为在线解密和离线解密。二者的解密对象和解密实时性要求均不一致(见表 1),相应的对解密的设计要求也不相同。总体来说:在线解密主要用于现场调试中,解密对象为当前网络实时捕获的抓包,解密工作需实时完成;离线解密主要用于对正常运营过程中产生问题的分析排查,解密对象为历史网络抓包,解密工作允许延时为分钟级。

表 1 两类网络抓包解密的差异

解密类型	应用场景	解密对象	解密实时性
在线解密	维护调试	实时网络抓包	实时
离线解密	在正常运营期间,对非预期问题的分析排查	已保存的历史网络抓包	分钟级,可接受一定时延

1.3 离线解密

信号系统网络抓包的离线解密工作可分为密钥归集、密钥保存、密钥导出和密钥解密等 4 个阶段。

1.3.1 密钥归集

离线解密的密钥归集过程如图 2 所示。ZC、LC 及 ATS 子系统在与 CC 子系统完成动态密钥协商过程后,主动将已完成协商的动态会话密钥、会话密钥 Hash(哈希)值和会话 ID(标识号)发送至证书密钥管理系统。会话密钥 Hash 值由国产加密芯片根据动态会话密钥生成。

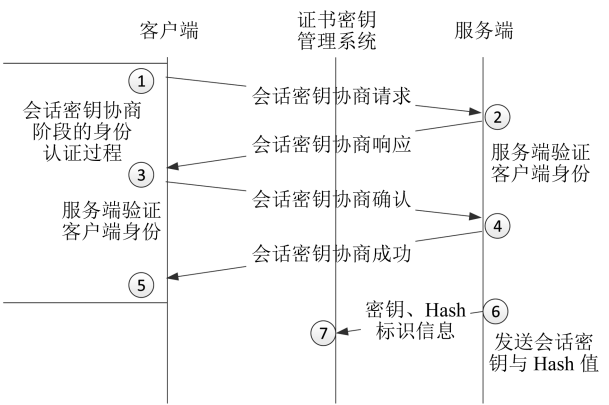


图 2 离线解密的密钥归集过程

在离线解密的密钥归集过程中,只要国产加密芯片产生任何错误,就认为该过程失败,并由 ZC、LC 及 ATS 子系统进行记录。此外,解密网络捕包功能并不影响信号系统以加密通信状态进行日常运营,故离线解密的密钥归集不设置确认重传机制,容许会话密钥在网络传输过程中的可能丢失。

CC、ZC、LC 及 ATS 子系统在发送加密消息时,将会话密钥 Hash 值放入加密消息包头中。

1.3.2 密钥保存

证书密钥管理系统将收到的动态会话密钥、会话密钥 Hash 值和会话 ID 保存在证书密钥管理器内至少 180 d,并在 180 d 后依次删除。

密钥证书管理系统还可提供会话 ID 与更新时间的显示列表。

1.3.3 密钥导出

密钥证书管理系统提供按选择时间(时间精度为 d)导出密钥的操作,可将密钥证书管理器内保存的动态会话密钥及会话密钥 Hash 值按照对应映射关系以加密文件的形式导出到外部设备中。该导出操作需要管理 UKEY(电子钥匙)授权。

1.3.4 密钥解密

密钥解密流程见图 3。操作人员将授权的管理 UKEY 插入待解密的主机设备上,并将导出的加密文件放在同一主机的 C 盘根目录下;Wireshark 插件根据待解密网络抓包中的 Hash 字段,在加密文件中寻找对应的会话密钥进行解密,并将解密后的报文

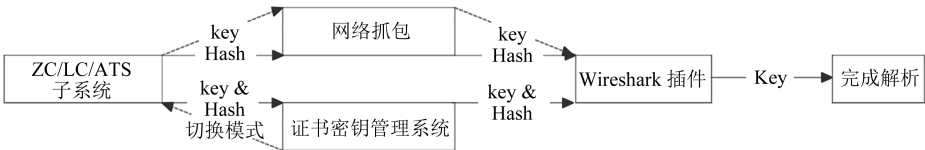


图 3 离线解密与在线解密流程图

显示在 Wireshark 界面上。如果未找到对应会话密钥或解密失败,则报错并显示原始加密报文。

1.4 在线解密

信号系统网络抓包的在线解密工作分为模式切换和密钥解密 2 个阶段。

1.4.1 模式切换

鉴于在线解密的高实时性要求和特殊应用场景,为区别离线解密工作的一般模式,本文将在线解密工作模式定义为调试模式。调试模式将会话密钥直接放入加密消息包头中,以便在密钥解密阶段直接使用会话密钥对实时抓取的网络抓包进行解密。调整后的加密报文消息包头格式如表 3 所示。

表 3 调整后的加密报文消息包头格式

项目	消息包头	
	keyType	Hash
长度	1 B	16 B
赋值说明	1——会话密钥 Hash(正常模式) 2——会话密钥(调试模式)	

密钥证书管理系统提供模式切换操作,可向所有指定的 IP(网际互连协议)地址和端口发送切换模式消息;CC、ZC、LC 及 ATS 子系统收到切换模式消息后转为调试模式,并将会话密钥放入加密消息包头中(如图 4 所示)。切换模式操作需要管理 UKEY 授权。

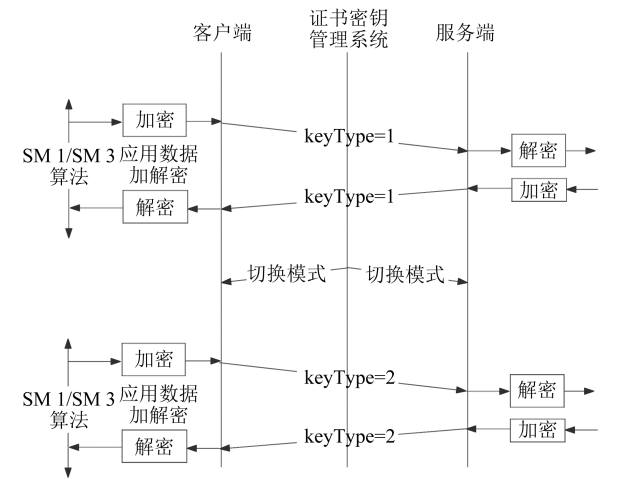


图 4 在线解密的模式切换过程

在模式切换过程中,只要国产加密芯片产生任何错误,都认为该过程失败,并由 CC、ZC、LC 及 ATS 子系统进行记录。此外,解密网络捕包功能并不影响信号系统以加密状态日常运营,故模式切换不设置确认重传机制,容许切换模式消息发送过程中的可能丢失。

如果 CC、ZC、LC 及 ATS 子系统在调试模式下 (keyType=2) 重复收到密钥证书管理系统发送的切换模式消息,则保持 keyType=2 不变。此外,不设置模式回滚机制。当 CC、ZC、LC 及 ATS 子系统收到密钥证书管理系统发送的切换模式消息并成功进行模式切换后,重启相应设备;国产加密芯片初始化后即可按照正常模式 (keyType=1) 运行。

1.4.2 密钥解密

在待解包的主机设备中,Wireshark 插件直接将待解密的实时网络抓包中的 key 字段作为会话密钥进行解密,并将解密后的报文显示在 Wireshark 界面上。如果解密失败,则报错并显示原始加密报文。在线解密流程如图 3 所示。

Wireshark 插件解密网络抓包的过程,具体如下(见图 5):

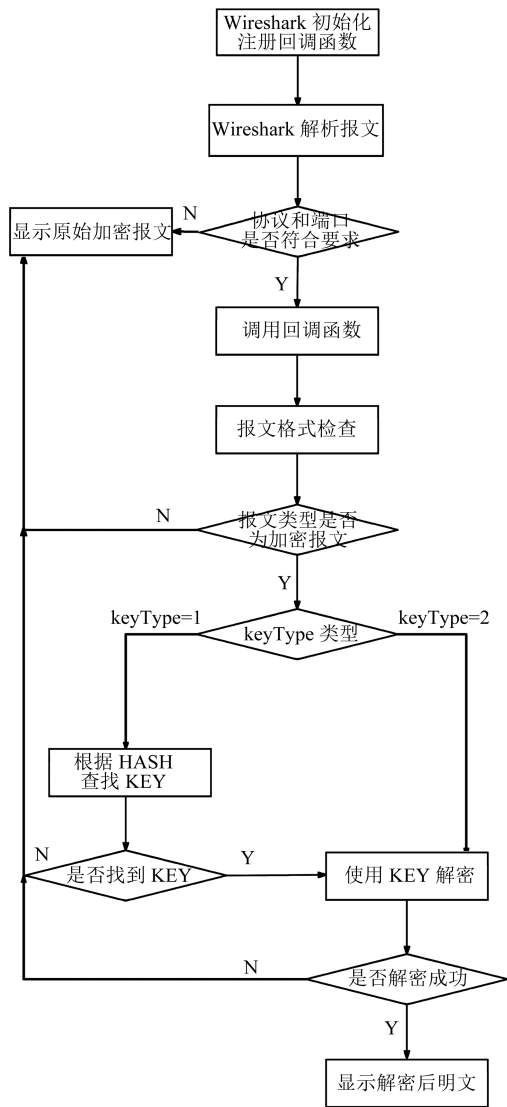


图 5 wireshark 插件解密流程图

1) 判断抓包内的每条二进制码流是否为需要解密的码流。如协议和端口不符合预置则认为该码流并非待解密码流,直接显示原始值;如符合预置的协议和端口则认为该码流为待解密码流。

2) 判断待解密码流是否为具备加密特征的加密码流。如不符合加密特征则认为该码流并非加密码流,直接显示原始值;如符合加密特征则认为该码流为加密码流。

3) 根据 keyType 值对加密码流分别处理。当 keyType=1 时,根据码流中的 Hash 值字段在导出的密钥文件中寻找匹配的密钥。如无法找到密钥,则直接显示原始值;如找到密钥,则进行解密。当 keyType=2 时,直接使用码流中的 Key 字段进行解密。

4) 若解密失败,则直接显示原始值;若解密成功,则显示解密后的明文。

2 应用测试

基于上述解密方案,在实验室搭建信号系统,集成国产加密芯片,进行应用测试。测试过程及结果如下:

1) 信号系统应用设备在启动后进行会话密钥协商;在会话密钥协商成功后,主动发送会话密钥、会话密钥 Hash 值和会话 ID 至证书密钥管理系统;在后续发送加密消息时,将会话密钥 Hash 值放入加密消息包头中。

2) 证书密钥管理系统将收到的密钥信息保存在证书密钥管理服务器内,并可将保存的会话密钥、会话密钥 Hash 值按照对应关系以加密文件形式导出到外部设备中。Wireshark 插件根据待解密的网络抓包报文中的 Hash 字段,在加密文件中寻找对应的会话密钥并进行解密,最终将解密后的报文显示在界面上。

3) 证书密钥管理系统向指定的 IP 地址和端口发送切换模式消息;信号系统应用设备在收到切换模式消息后,随即变更加密报文的组包方式,并将会话密钥放入加密消息包头中。Wireshark 插件直接将待解密的实时网络抓包报文中的 Key 字段作为会话密钥进行解密,并将解密后的报文显示在 Wireshark 界面上。

4) 信号系统应用设备只要在运行过程中收到

一次切换模式消息,就将变更加密报文组包方式,直到该设备关闭或重新启动为止。

3 结语

本文提出了一种在应用国产加密技术的信号系统中,对加密的网络抓包进行解密的方案,使得开发调试人员能够取得动态协商的密钥,并使用密钥完成对加密网络抓包的解密,提升了信号系统的可维护性。

该解密方案不仅适用于信号系统,而且可以用于其他有类似需求的工业自动化控制系统中。实际应用结果表明,与现有技术方案相比,本方案具有以下优点:

1) 针对应用了国产加密技术的信号系统,能取得动态协商的加密密钥,完成对网络抓包的解密,保证了信号系统整体的可维护性,为信号系统后期的运营维护提供了极大的便利。

2) 通过分析设计,可将不同的网络抓包解密需求结合在一起,使用同一套软件处理机制完成。

3) 解密网络抓包所需要的密钥发送消息和切换模式消息发送成功与否,不会影响信号系统应用国产加密技术的正常运行,甚至通信两端可以采取不同的组包方式。

4) 在工作全程中密钥均以加密形式存在,且人员无法直接接触密钥,保证了机密性和安全性。

5) 该方案在保证信号系统既有架构和功能安全等级不受影响的同时,尽可能实现了调试维护的工作方式变化较小。

参考文献

- [1] 卡斯柯信号有限公司. 应用在国产密码加密的信号系统中解析网络捕包的方法:201911100723.8[P]. 2020-02-25.
- [2] 国家密码管理局. 信息系统密码应用基本要求:GM/T 0054—2018[S]. 北京:中国质检出版社,2018.
- [3] 全国信息安全标准化技术委员会. 信息安全技术 证书认证系统密码及其相关安全技术规范:GB/T 25056—2018[S]. 北京:中国标准出版社,2018.
- [4] 全国信息安全标准化技术委员会. 信息安全技术 网络安全等级保护基本要求:GB/T 22239—2019[S]. 北京:中国标准出版社,2019.
- [5] 郭启全. 网络安全法与网络安全等级保护制度培训课程(2018版)[M]. 北京:电子工业出版社,2018.

(收稿日期:2020-08-31)