基于国密算法的安全通信在PLC控制系统应用研究

Research on Application of Security Communication in PLC Control System Based on National Secret Algorithm

★ 楚兵，贾峰，魏敏 宁波和利时信息安全研究院有限公司

摘要： 工业控制系统作为重要的国家关键基础设施，随着工业化与信息化融合的持续深化与发展，把互联网中存在的通信安全威胁带给了工业控制系统。本文从国密算法的应用角度对PLC工业控制系统进行分析，从数据传输保密性、数据存储安全性、通信会话安全性等方面阐述了基于国密算法的信息安全组件的应用研究。

关键词： 国密算法；通信加密；工控系统；数据加密

Abstract: As an important national key infrastructure, industrial control system has brought the communication security threat in the Internet to industrial control system with the continuous deepening and development of the integration of industrialization and informatization. This paper analyzes the PLC industrial control system from the perspective of the application of the national secret algorithm, and expounds the application research of the information security component based on the national secret algorithm from the aspects of data transmission confidentiality, data storage security, communication session security and so on.

Key words: National secret algorithm; Communication encryption; Industrial control system; Data encryption

1 引言

工业控制系统网络架构是依托网络技术，将控制计算节点构建成为工业生产过程控制的技术环境，典型形态包括DCS、PLC等，工业控制系统的建设打破了传统工业“信息孤岛”的弊端缺陷，推动了工业自动化的发展。当前工控系统安全防护比率很低，市场仍面临着产品体系不成熟等问题。调查发现，约80%的企业从来不对工控系统进行升级和漏洞修补，52%的工控系统存在于企业管理系统、内网甚至与互联网连接等问题。

研究基于国密算法在工控系统的应用，对于解决工业控制系统信息安全核心问题、提升整体工业安全防护水平、推进落实国密算法在工业控制领域推广具有重要的意义。

2 国密算法通信技术概览

2.1 国密算法简介

常见的网络安全威胁分类以及受到威胁的特性，对应的密码算法如图1所示。

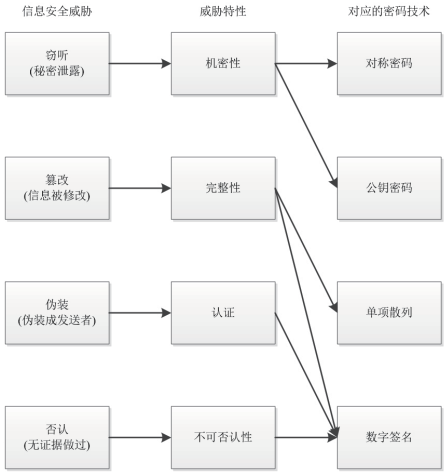

图1 密码算法应用特性

公钥SM2算法：加密和解密使用不同密钥的方式，国密算法中SM2公钥算法呈现出的椭圆曲线

和实际曲线不同，为了防止通信方的否认，SM2签名又称数字签名，是签名者利用数据展开的数字签名，最终通过验证者对签名进行验证。

单向散列SM3算法：国密算法中的SM3算法常应用在密码中，主要包括数字签名与验签过程。应用此技术时，随着生成验证码、验证码应用、产生随机数等过程，保障信息安全。

对称密码SM4算法：加密和解密使用同一密钥，常见的对称密码属于SM4算法，是一种分组密码算法。其分组长度为128bit，密钥长度也为128bit。

2.1 基于国密算法的身份认证技术

身份认证是证实用户的真实身份与其对外的身份是否相符，从而确定用户信息是否可靠，防止非法用户假冒其他合法用户获得一系列相关权限，保证用户信息的安全、合法利益。建立通信双方信任关系，是保障系统安全的第一道防线，也是最重要的一道防线。身份认证的设计目标是利用国密算法技术有效抵御各种网络攻击手段，消除通信双方的安全隐患。

基于国密算法的身份认证的设计要达到以下功能要求：

（1）安全环境下的用户身份进行可信确认，既要保证用户是授权用户，又要保证认证过程的安全，除了用户自身公开的信息以外，秘密信息不能泄漏给任何实体包括认证方。

（2）不同域（组织）之间的用户认证，非本组织用户请求访问资源时，既要确认该用户所属的域是否可信任，还要确认是否为用户本人。若是首次访问，在授权申请、审核之后再给予一定权限。

（3）为不可抵赖性提供证据，确保通信方无法否认的访问行为。

由于历史和计算能力的原因，工控系统通信均采用明码且未进行身份认证，导致数据的保密性无法保障，同时存在对设备进行非授权访问的风险。研究轻量级的国密算法在一体化安全工控系统中身份认证的应用，既能推进密码算法的国产化应用替代，也提高了工控系统的安全保密能力，为保障工业设施的安全提供重要的保障。

3 国密通信在PLC控制系统中应用研究

3.1 基于国密算法安全通信应用方案

基于国密算法通信的控制系统拓扑如图2所示，安全管理中心与安全可信PLC主控、安全可信工程师站与安全可信PLC主控采用基于国密算法的安全通信。

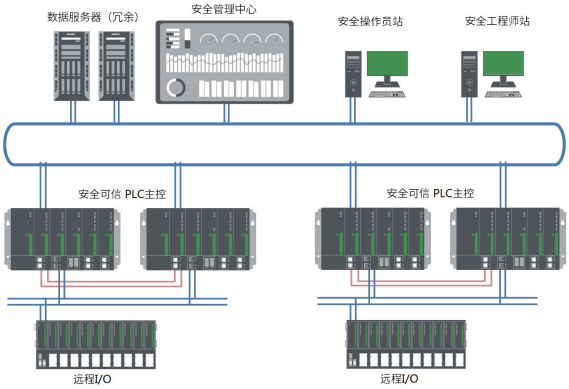

图2 基于国密算法通信的控制系统拓扑

安全可信控制器、安全可信管理平台、安全可信工程师站三者之间通信时采用基于国密算法的公钥基础设施（Public Key Infrastructure，PKI）身份证书，从根本上提高了身份认证的安全强度。针对PLC控制系统的安全通信需求，采用基于国密算法的安全通信组件实现高实时、轻量化的密钥协商和加解密处理能力，具备双向身份证书鉴别、通信加解密功能，实时性高，符合工业系统场景应用。

采用基于国密的SSL安全连接来实施身份认证。安全套接字层协议（Security Socket Layer，SSL），是通信网络上进行保密通信的一个安全协议，其主要目的是保证PLC控制系统之间的通信安全，提供网络上可信赖的服务。该协议采用了多种加密算法，具有保护传输数据以及识别通信机器的功能。

本文以安全可信PLC控制器与安全可信工程师站会话建立为例，说明基于国密算法的安全连接建立过程。在实际使用场景中，PLC作为服务端，工程师站作为客户端进行数据交互，图3为安全可信工程师站示例。

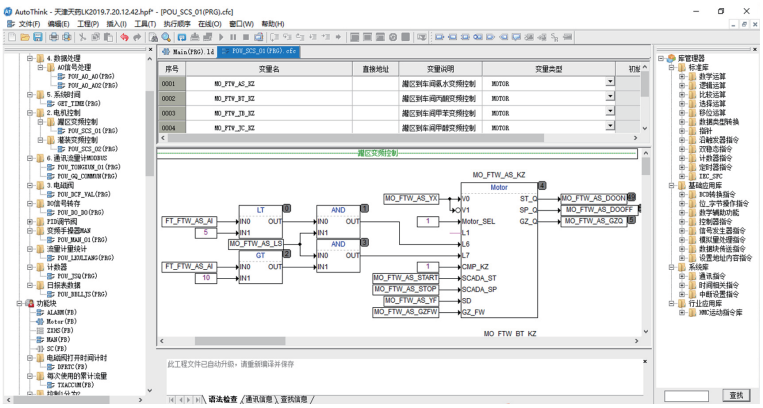

图3 安全可信工程师站

工程师站与PLC控制器中的核心组件RTS进行加密通信之前，需要交换基于国密算法的数字证书。如图4所示。

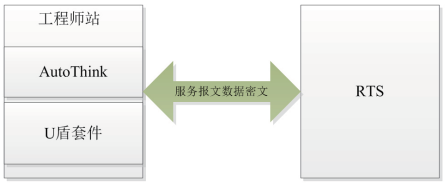

图4 PLC控制器与工程师站互联示意图

具体流程如图5所示，描述如下：

（1）工程师站向RTS发送Client_Hello报文，服务器回应Server_Hello报文，协商好一些安全参数、密文族、压缩方法，同时生成并交换随机数。

（2）RTS需要被认证，RTS将发送基于国密算法的公钥证书工程师站。接下来发送ServerKeyExchange进行密钥交换协商等过程，RTS送Server Hello Done报文，通知客户端，服务器完成了交流过程的初始化。

（3）工程师站同时要发送Certificate，然后发送ClientKeyExchange报文。最后，客户可能发送CertificateVerify报文来校验客户发送的证书。

（4）工程师站发送ChangeCipherSpec报文要求服务器使用加密模式。然后发送Finished报文告诉RTS自身已经准备好安全通信了。RTS响应这两个报文，发送自己的ChangeCipherSpec报文、Finished报文，对工程师站提出相同的要求。握手结束，即可发送应用层数据。

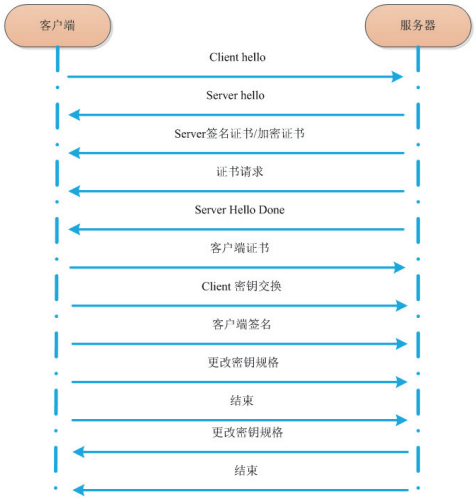

图5 安全连接建立的过程

在握手过程结束时，就使用的加密算法达成一致，并拥有一套与算法匹配的密钥，而且可以确信整个过程攻击者无法干扰。

由网口进入的身份信息的认证过程如图6所示。

图6 进入的身份认证过程图

由网口发出的身份信息的处理过程如图7所示。

图7 发出的身份认证过程图

以上过程是在工程师站与安全可信PLC网络通信中，增加基于国密的安全通信加解密组件，在通信会话建立之前，首先对通信双方的身份进行验证，交换基于国密算法的数字证书，并协商临时通信密钥，会话协商通过后才能进行通信，确保通信双方的身份可信性、网络数据完整性、机密性，可以有效防止常见的网络监听、回放攻击手段。

3.2 测试验证

网络攻击验证环境如图8所示。

3.2.1 非加密网络通信

（1）通过网口监测数据报文，获取数据报文，并解析关键字段，利用恶意软件模拟工程师站下发恶

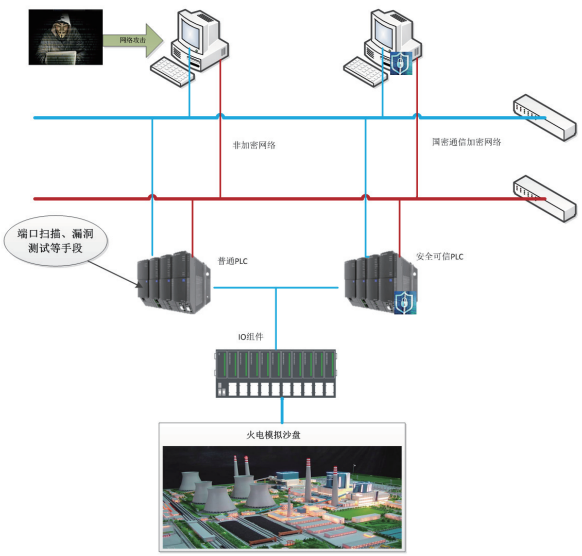

图8 网络攻击验证环境

意指令；

（2）普通PLC与工程师站连接未对客户端的身份进行校验，通信数据也未加密，指令下发后PLC可以执行；

（3）下发恶意指令可以成功，通过I/O组件输出后，到模拟沙盘，可以看到电机停转等较为直观的现象。

3.2.2 基于国密算法的安全通信网络通信

（1）通过网口监测数据报文；

（2）安全可信PLC与工程师站通信中，在端口上增加了安全通信协议，恶意程序无法解析通信数据，即使强制发送，也会数据校验失败，数据被丢弃；

（3）恶意指令下发失败。

3.2.3 测试结果

对于会话连接都要校验身份，且通信的数据加密，恶意进程无法识别数据，且数据帧中包含随机数，可以有效防止网络监听、数据重放攻击。

4 结论

针对工业控制系统存在的网络通信薄弱环节，研究了基于国密算法的安全通信组件，具备数据加密、身份认证等功能，保障了工业控制系统通信数据完整性、保密性、通信身份可信，并搭建了测试环境，通过网络攻击验证了可以有效抵抗常见的网络攻击。本研究对国产密码在工业控制系统推动及应用，具有一定指导价值。AP

作者简介

楚 兵（1982-），男，北京人，中级工程师，硕士，现任宁波和利时信息安全研究院产品技术中心总经理，研究方向为工控信息安全、网络通信、嵌入式系统。

贾 峰（1975-），女，内蒙古包头人，高级工程师，学士，现就职于宁波和利时信息安全研究院有限公司，研究方向为自动化。

魏 敏（1986-），女，河南安阳人，学士，现就职于宁波和利时信息安全研究院有限公司，研究方向为工业信息安全设计与开发。

参考文献：

[1] 王凤娇, 魏军, 郑潇潇, 等. 建立工业控制系统安全认证体系迫在眉睫[J]. 信息安全与通信保密, 2017, (6) : 88 - 95.

[2] 王柯柯. 基于PKI的认证中心的研究与实践[D]. 重庆: 重庆大学, 2004.

[3] 沈昌祥. 用主动免疫可信计算筑牢 "新基建" 网络安全防线[J]. 科学中国人, 2020, 14 : 29-31.

[4] 杨储华, 周航帆, 马军, 等. 基于国密算法的北斗短报文安全防护系统的研究与实现[J]. 计算机与现代化, 2019, (04) : 108 - 113.