基于国产密码算法的数控网络的认证与验证模型研究及安全评估

夏晓峰[①] 向 宏*[①] 肖震宇[②] 蔡 挺[②]

[①](信息物理社会可信服务计算教育部重点实验室 重庆 400044)

[②](重庆大学大数据与软件学院 重庆 400044)

摘 要：该文针对工业控制系统安全，提出面向数控系统(NCS)网络安全保护技术框架，选用国产密码系列算法中的SM2, SM3, SM4算法，设计并建立了数控网络(CNC)认证与验证模型(AUTH-VRF)，分内外两层为数控网络提供安全防护。外层为数控网络设备间通信与传输进行安全认证实现网段隔离，内层验证通信协议完整性以确保现场设备接收运行程序的正确性与有效性；通过基于SM2, SM3, SM4算法设计和部署的外层防护装置，为分布式数控(DNC)设备与数控系统之间的通信提供身份认证与文件加密传输；同时针对工业控制网络的S7Comm工业通信协议数据，通过SM3算法验证专有工业协议数据完整性。通过网络攻击实验证明，AUTH-VRF模型可以为数控网络中工业生产数据提供有效的安全认证和资源完整性保护，为满足我国关键基础设施“国内、国外工业控制系统产品共同安全可控”和“安全技术深入工业控制系统各个层级”的需求提供了实际可行的技术参考方案。

关键词：国产密码算法；数控网络；安全认证；完整性验证

中图分类号：TN918; TP309.2 **文献标识码**：A **文章编号**：1009-5896(2020)08-1846-07

DOI: 10.11999/JEIT190893

Research and Security Evaluation of AUTH-VRF Model for NCS Network Based on Domestic Cryptographic Algorithms

XIA Xiaofeng[①] XIANG Hong[①] XIAO Zhenyu[②] CAI Ting[②]

[①](*Key Laboratory of Dependable Service Computing in Cyber Physical Society*, *Ministry of Education*, *Chongqing* 400044, *China*)

[②](*School of Bigdata and Software Engineering*, *Chongqing University*, *Chongqing* 400044, *China*)

Abstract: For the security of industrial control system, a framework for Numerical Control System(NCS) network security protection technology is proposed. The SM2, SM3 and SM4 algorithms in the domestic cryptographic algorithms are used to design and establish the AUTHentication and VRFfication (AUTH-VRF) model of the Computerized Numerical Control(CNC) network, which provides security protection for both internal and external sides. The external side conducts the security authentication for communication and transmission between CNC network devices to achieve network segment isolation. The internal side verifies communication protocol integrity to ensure that the operating procedures received by the field devices are correct and valid. The external protection device designed and deployed based on the SM2, SM3 and SM4 algorithms provides identity authentication and file encryption transmission for communication between the Distributed Numerical Control(DNC) device and the CNC system. At the same time, for the proprietary industrial communication protocol data in the CNC network, the SM3 algorithm is used to verify its integrity. The network attack experiments prove that the AUTH-VRF model can provide effective security certification and integrity protection for industrial production data in CNC networks. It also provides a practical technical approach to meet the requirements of ‘secure and controllable both for domestic and foreign products’, as well

收稿日期：2019-11-07；改回日期：2020-05-31；网络出版：2020-06-23

*通信作者： 向宏 xianghong@cqu.edu.cn

基金项目：国家重点研发计划(2017YFB0802400)，国家十三五密码发展基金(MMJJ20180211)，重庆市研究生导师团队建设项目，重庆市研究生教育教学改革研究项目(yjg192003)

Foundation Items: The National Key Research and Development Project (2017YFB0802400), The National 13th Five Year Code Development Fund (MMJJ20180211), Chongqing Postgraduate Tutor Team Construction Project, Chongqing Graduate Education and Teaching Reform Research Project (yjg192003)

as ‘applying security technique to all layers of Industrial Control Systems’ for protecting the critical infrastructure.

Key words: Domestic cryptographic algorithm; Computerized Numerical Control(CNC) network; Security certificate; Integrity verification

1　引言

工业控制系统是指包含数据采集与监控系统(Supervisory Control & Data Acquisition, SCADA)、分布式控制系统(Distributed Control System, DCS)、可编程逻辑控制器(Programmable Logic Controller, PLC)、数控系统(Numerical Control System, NCS)等，用于支持工业生产过程中的各种调度与控制的系统，经由工业通信网络协调完成生产任务。

我国大量关键基础设施依靠工业控制系统作业，这些重要行业和领域的工控系统一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全与公共利益。目前我国工业控制系统安全保障工作面临的主要现实问题包括：(1)国外产品主导：占95%以上的PLC产品来自国外，发那科(FANUC)和西门子(SIEMENS)占中高档控制器份额超过80%，国际厂商SCADA产品拥有91%的份额，在DCS分散型数字控制系统占据70%[1]；(2)国产安全技术(密码算法)应用少：国产密码算法应用未深入工业控制系统的控制层和现场层，主要在控制系统外围应用或者在少数专有工业设备，如PLC上有示范性应用；认证和加密应用主要针对工业控制系统的企业层和监控层(信息系统为主)，缺乏对应用广泛的专有工业协议的安全保护，例如西门子S7Comm、施耐德电气Modbus等。

针对工业控制系统中的入侵检测主要有误用检测、异常检测以及综合检测3种方法[2]。工控系统异常行为的入侵检测特征主要考虑通信协议、通信流量、系统工作状态参数等[3]。文献[4]从SCADA审计系统的服务端的I/O值和硬件工作统计值入手，提取入侵检测数据并进行异常行为的入侵检测，同时也提出通过白名单和基于行为协议分析，主动建立入侵检测规则。在抵御侧信道攻击上，文献[5]提出的随机加法链算法比固定加法链算法更加安全有效，但未在工业场景中提供解决方案。针对工业控制系统中的复杂分布式环境，文献[6]采用了一种基于密文策略属性基加密(Ciphertext Policy Attribute Based Encryption, CP-ABE)算法，在保护数据的机密性和完整性的基础上，还提供了细粒度的访问控制办法。

本文针对上述问题，提出一种面向NCS网络的认证与验证模型(AUTH-VRF)。模型外层通过对重要工控设备实现网段隔离，部署外层防护装置，为分布式数控(Distributed Numerical Control, DNC)设备与数控系统之间的通信提供身份认证与文件加密传输；模型内层验证S7Comm专有工业协议完整性，保障设备发往底层硬件的执行指令的安全性。本文工作采用由外至内的主动防护策略，实现网段隔离，以保护重要工控设备外部通信和内部指令收发完整为目标。再通过内层指令通信的验证来防止即使外部攻击的渗入，避免现场设备接收非常规指令而产生物理运行故障。本文第2节提出基于国产密码算法的NCS网络AUTH-VRF模型；第3节详细论述AUTH-VRF模型的实现及安全评估工作；最后总结全文。

2　基于国产密码算法的NCS网络AUTH-VRF模型

基于国产密码算法的NCS网络AUTH-VRF模型分为安全认证和安全验证两部分，其中安全认证子模型实现于NCS网络外层保护装置(Exosphere Protective Device, EPD)；安全验证子模型实现于NCS网络面板控制单元(Panel Control Unit, PCU)、机器控制面板(Machine Control Panel, MCP)。

2.1　AUTH-VRF模型中国密算法简介

SM2算法是我国自主设计的基域为素域和2元扩域的椭圆曲线公钥密码算法，可实现数字签名、密钥协商和数据加密等功能，可满足多种密码应用中身份认证和数据完整性、真实性的安全需求[7]。对于商用密码应用中的密钥交换，可满足通信双方经过2次或可选3次信息传递过程，计算获取一个由双方共同决定的共享会话密钥。在相同安全强度要求下，椭圆曲线密码较其他公钥密码所需的密钥规模要小得多[8–12]。其签名速度与秘钥生成速度皆优于RSA[13]，其使用256 bit长度的密钥获得的安全强度同采用2048 bit密钥长度的RSA算法的相同。SM3杂凑算法用作消息摘要，横向对比MD5算法，常应用于商业密码，通过验证码生成与应用、产生随机数等过程，能适用于多种密码算法以保障信息[14]。输入长度为l (l < 264) bit的消息m, SM3杂凑算法经过填充、迭代压缩和选裁输出3步以生成杂凑值[15]。SM4分组对称加密密码算法适用于无线局域网的安全领域[16]。

2.2 NCS网络AUTH-VRF模型安全认证设计

NCS网络AUTH-VRF模型参考文献[17]中的PGP电子邮件系统模型，使用属性描述协议实体，使用消息摘要、对称密钥加密，以及公钥加密的算法组合，使该模型能同时用于消息加密、身份识别、完整性验证，能够满足机密性与完整性等需求。同时考虑NCS网络的特殊性，本文更接近于文献[18]的Mini PGP模型的方法，同时文献[18]展示了小型PGP的安全性，AUTH-VRF模型的不同在于使用国密SM3来进行消息摘要，SM2完成签名，SM4完成加密功能。AUTH-VRF模型借鉴了文献[19]介绍的信任模型及协议，采用了0kamoto的twisted-PRF技巧，密钥封装方案将由长期私钥与临时对称密钥组合，协议实体将设置多个密钥用于封装密钥的启封。本文借鉴文献[20]的Beth信任模型，采用信任度概念，对待测试传输信道设置可信或不可信两种状态，根据模型工作完成任务的结果对信道定义其信任度。AUTH-VRF模型认为DNC, EPD以及PCU等设备是可信的，模型是针对不完全可信的传输信道来提供解决方法。

NCS安全认证应用的对象为DNC到EPD，其中DNC是发送控制代码文件到NCS的外围设备组合，EPD是为DNC发送到NCS的控制代码文件提供认证服务的外层保护装置。安全认证过程中所用到国产密码算法有SM2, SM3和SM4，其中SM2的签名验签模块负责对文件添加数字签名及验证数字签名，SM2的加密解密模块负责为后面SM4算法所用到的对称密钥进行加密及解密；SM3算法负责产生hash值(消息摘要值)；SM4负责最终传输文件的加解密过程。在上述密码算法中，SM2算法使用的公私钥将根据管理员预先提供的身份信息生成，SM4算法使用的对称密钥将在使用前基于SM2私钥重新生成；因此在加密不同文件时，本模型将使用不同的SM4对称密钥。所有的密钥在生成后都将进入密钥管理系统，该系统使用Token机制对密钥进行保管，1个Token将对应1组用户权限，系统将根据密钥请求方提供的Token判断请求方是否拥有读取某一密钥的权限。管理员将持有最高权限的Root Token，其他任何使用者的Token都将基于Root Token生成，管理员可对任何其他Token进行权限约束、收回等操作。此外，系统在每次关闭后都将进入密封状态，再次使用前需先启封。在第1次密封时，管理员将系统生成N把启封密钥分发给N个可信方，后续启封过程需要其中至少$n(n \le N)$才可启封。整个NCS安全认证的流程如图1。

下文算法描述中使用的“(r, s)(发送的签名)、Z_{A}(关于用户A的可辨别标识、部分椭圆曲线系统参数和用户A公钥的杂凑值)、d_{A}(用户A的私钥)、P_{A}(用户A的公钥)、$Hv(M)$(M的长度为v的杂凑值)”等符号，定义与文献[7–11,15,16]一致。

DNC将GC-file文件(G代码文件，工业生产模型加工文件)的内容Gcode使用SM3算法计算出其hash值，并将该hash值与Gcode本身合并得到GC-file2文件，随后使用SM2签名算法对该文件进行签名得到数字签名(r, s), SM2算法数字签名的输入为：Z_{DNC}(DNC的可辨别标识、部分椭圆曲线系统参数和DNC公钥的杂凑值)、H_v(GC-file2)(GC-file2的长度为v的杂凑值)、P_{DNC}(DNC的公钥)、d_{DNC}(DNC的私钥)，输出为：数字签名(r, s)。之后将(r, s)与GC-file2文件合并得GC-file3，用基于SM2私钥生成的128 bit对称密钥S-key及SM4加密算法对GC-file3进行加密得GC-M-file，同时用P_{EPD}(EPD的公钥)及SM2加密算法对S-key加密得S-M-key。最后将GC-M-file与S-M-key合并得到的AUTH-GC-file文件发送给EPD。

EPD将接受到的AUTH-GC-file′文件后解析出

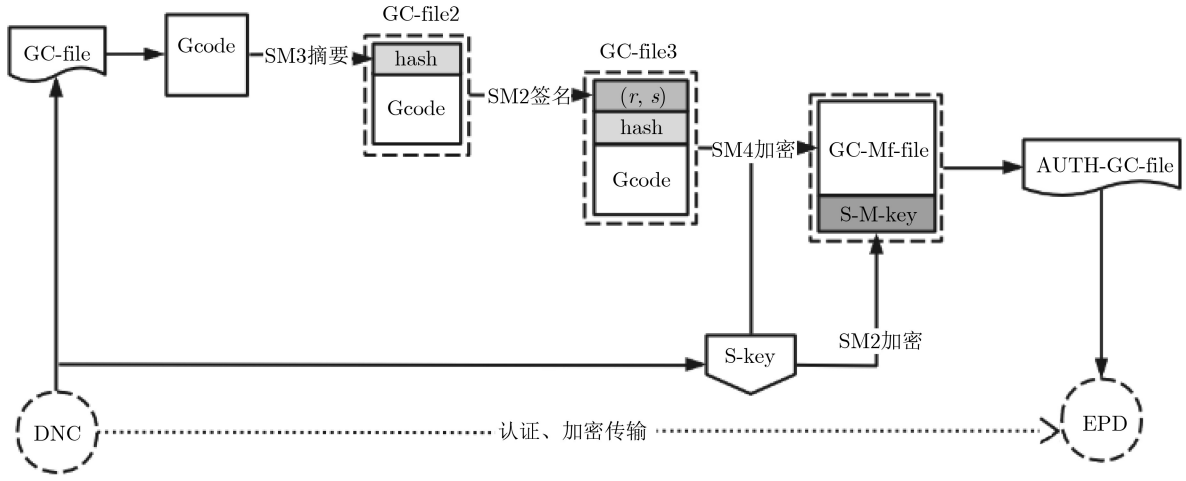

图 1 NCS网络AUTH-VRF模型安全认证流程

GC-M-file′与S-M-key′，使用d_{EPD}(EPD的私钥)及SM2解密算法对S-M-key′解密得S-key′。随后使用S-Key′及SM4解密算法对GC-M-file′进行解密得GC-file3′。对GC-file3′进行解析得GC-file2′与(r', s')，使用d_{EPD}(EPD的私钥)与SM2验签算法对GC-file2′与(r', s')进行验证，若验证失败则说明文件在传输过程中遭到篡改，需要舍弃；若验证成功则证明GC-file2'与GC-file2一致，可进行下一步传输。

2.3 NCS网络AUTH-VRF模型安全验证设计

NCS安全验证的对象为EPD, PCU, MCP到数字控制单元(Numerical Control Unit, NCU)。PCU为NCS的操作面板，MCP是专门为数控机床而配置的，NCU负责数控的所有功能。安全验证所用的算法为SM3，其负责验证经EPD验证后传输给NCU的控制文件。

EPD将认证成功的GC-file2文件发送至PCU, PCU在将接收到的GC-file2′文件发送往NCU前使用SM3算法对文件中的Gcode′代码进行检验，检验过程为PCU对Gcode′使用SM3算法计算出杂凑值hash，若该杂凑值hash与接收到的GC-file2′文件中的杂凑值hash′相等，则检验成功，Gcode′代码文件将作为验证成功的VRF-GC-file文件发往NCU；若不相等，则验证失败，GC-file2′文件将被丢弃。NCS安全验证的流程如图2所示。

3 面向西门子840D数控系统的AUTH-VRF模型实现及安全评估

3.1 AUTH-VRF模型实现

本文所实现的基于国密算法的数控系统AUTH-VRF模型实现场景(图3所示)由以下3部分组成：DNC，西门子840D数控系统及数控机床。实现场景的工作流程为操作者利用局域网设备将控制数控机床运行的文件传输给西门子840D数控系统，经由数控系统处理后在其系统内部通过专用通讯协议S7Comm传输给系统元件CNC(计算机数控)或PLC(可编程逻辑控制器)，最后由CNC或PLC控制数控机床设备完成处理后的指令文件。后续的基于国密算法EPD将基于上述场景进行部署与测试。

3.2 AUTH-VRF模型外层防护的设计与实现

设计工作通过在数控系统与DNC设备间添加

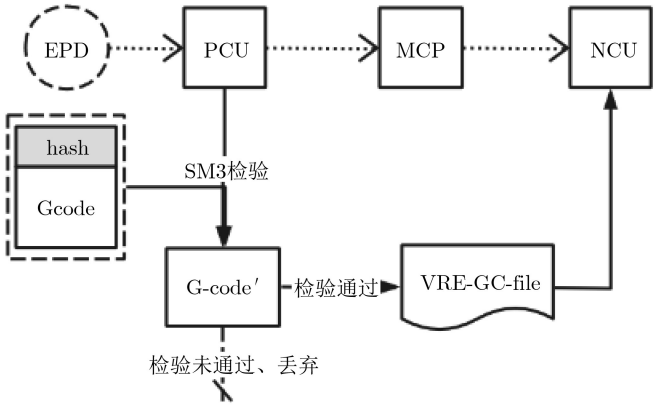

图 2 NCS网络AUTH-VRF模型安全验证流程

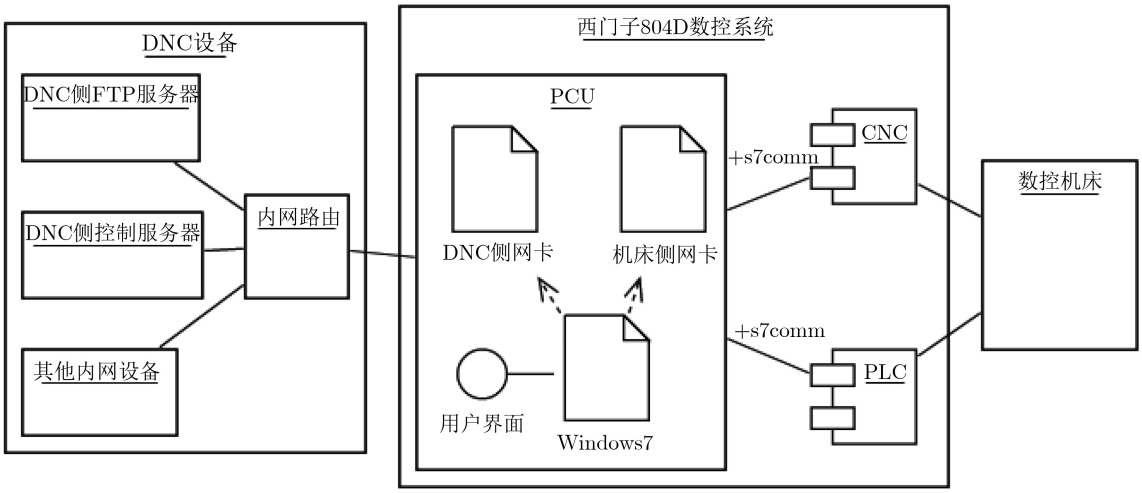

图 3 AUTH-VRF模型实现场景部署

一台专用传输的FTP服务器和EPD及在DNC控制服务器上部署国产密码算法加解密系统和vault密钥管理系统来实现安全防护。

EPD拥有双网卡配置，在网络拓扑中位于数控系统与DNC设备之间，并通过双网卡分别与二者相连，起到了网段隔离的作用。网段隔离使得DNC设备不能直接与数控系统进行文件传输等通信工作，若要进行通信，则必须通过EPD进行身份验证与加密传输。在具体部署时，EPD通过网卡1(面向DNC的网卡)与DNC服务器相连，以便接受并转发由它发往数控系统的文件，其中DNC的FTP服务器上文件已被加密；另一方面，数控系统的FTP服务器部署于数控系统与EPD之间，用于存储从EPD发向数控系统的文件，其中该FTP服务器上的文件已成功通过EPD的验证并成功解密。

国密算法加解密系统与vailt密钥管理系统部署于DNC中，其中国密算法加解密系统实现了国密算法中的SM2, SM3和SM4算法。任何人或设备访问vault管理系统均需要通过身份验证。vailt密钥管理系统中将存放国密算法加解密系统所需的以及EPD镜像保密性、完整性及真实性验证所需的所有密钥。外层防护装置部署如图4所示。

基于上述外层防护装置场景，传输者通过DNC向数控系统发送的文件将受到安全性防护。

3.3 AUTH-VRF模型内层防护的设计与实现

在验证控制文件之前，首先需要保证控制文件内容中保留有控制文件进入系统前留下hash值，本文通过外层防护装置中的EPD来实现这一步。具体实施步骤为：在EPD验证并解密文件之后，其对解密后的文件使用SM3算法计算出hash值并加在文件之后。

文件验证系统可以拦截完整性验证未通过的控制文件，控制文件在向CNC或PLC传输之前就需要被拦截下来。本文的文件验证系统通过使用Windows7操作系统的Winsock2来完成对数据报的拦截。本文的文件验证系统还为拦截下来的数据报提供了一个存储缓冲区，存储数据报的所有内容，用来解决数据包在传输过程中因为过大而被分包传输的问题。内层防护装置部署如图5所示。

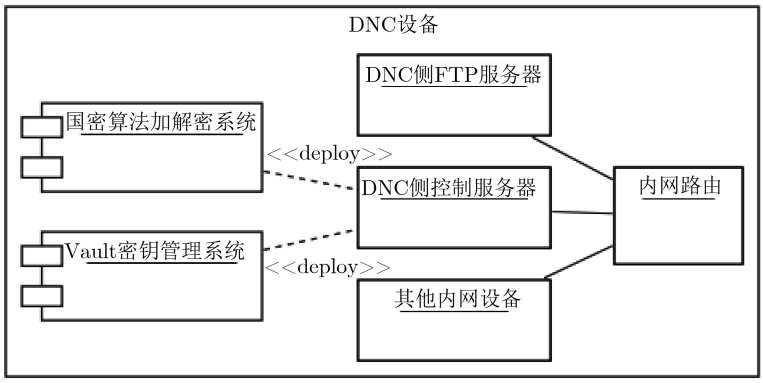

图 4 外层防护装置部署概况

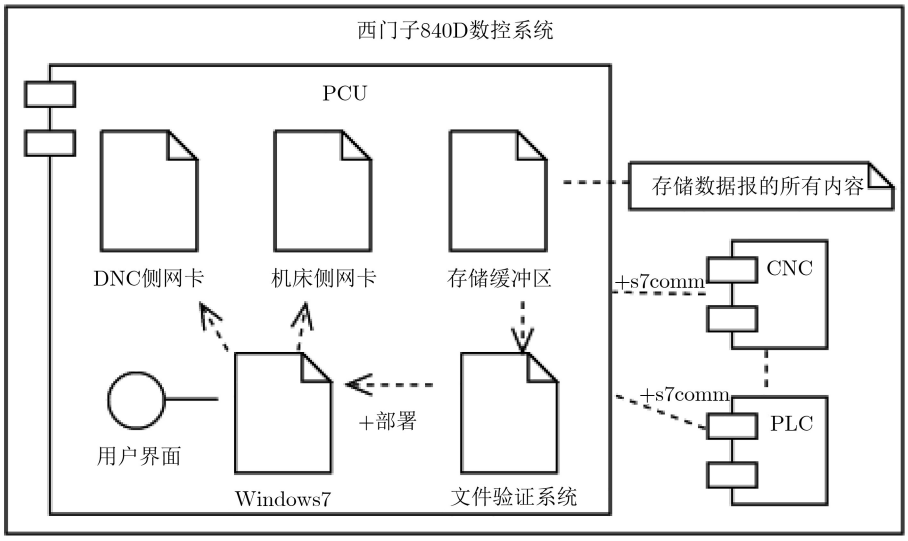

图 5 内层防护装置部署概况

对于成功拦截下来的数据包，文件验证系统基于传输协议S7Comm对数据包的内容进行解析，得出其中的文件内容、hash值部分及接收方的ip地址与端口，然后使用SM3算法计算得出文件本身的hash值与结尾的hash值对比，若一致则读将拦截下来的文件继续发送至接收方处，若不一致则通知系统发生错误。

基于上述成功部署的内层防护装置场景，由数控系统向机床设备发送的文件将受到完整性防护。

3.4 AUTH-VRF模型安全评估

典型的数控网络中各类主机含有敏感的加工模型文件，而这些主机未采取适当的安全措施，比如设备身份认证、接口管控等，重要数字模型文件资源也采取明文传输和存储。因此在数控网络中可以发起篡改攻击，对生产加工模型文件进行窃取和恶意修改，也可以通过非法接入数控网络的主机入侵服务器和操作员站等窃取、修改文件，如图6所示。

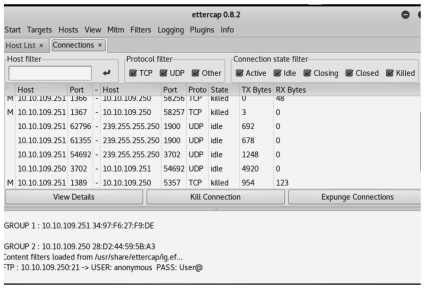

图 6 利用ettercap攻击嗅探NCS网络并劫持未保护的G代码文件

西门子840D数控系统直接与DNC设备相连并接受来自DNC的FTP服务器中的文件。DNC设备同处于同一局域网内，其中的FTP服务器中的文件并未受到加密保护，从而意味着若攻击者连入这一局域网可对FTP服务器上的文件进行查看与修改，亦或是在传输过程中对传输中的文件进行查看与修改。在这一层面上的安全攻击，由于其处于数控系统外部，本文统称为外部攻击。

数控系统内层部署的数控元件主要有PCU，CNC及PLC，其中PCU为连接各元件的核心元件。在PCU上部署了西门子工控系统专用的Windows7操作系统，从整体部署层面上看，由DNC的FTP服务器发往数控系统最终由CNC后PLC执行的控制文件将通过PCU在其Windows7操作系统上处理，其中安全漏洞也易出现在该控制文件处理环节，可能的原因是操作系统本身的不稳定或未处理的系统漏洞。针对这一情况，有必要在Windows7操作系统将控制文件发送到CNC或PLC之前对控制文件进行完整性验证。

面对上述的NCS网络安全漏洞，本文在AUTH-VRF模型实验环境中测试了EPD安全认证功能和PCU/MCU安全验证功能，实验结果表明基于国产密码算法的NCS网络AUTH-VRF模型通过SM2，SM3和SM4算法提供NCS网络设备身份认证与G代码文件加密传输；通过SM3算法验证和保护S7Comm专有工业协议数据完整性。

4 结论

本文选用国产密码算法设计并建立了数控网络AUTH-VRF模型。该模型从数控网络内外两层提供安全认证、加密传输和信息完整性验证。外层为数控网络设备间通信与传输进行安全认证实现网段隔离，内层验证通信协议完整性以确保现场设备接收运行程序的正确性与有效性；通过基于SM2和SM4算法设计和部署的外层防护装置，为DNC设备与数控系统之间的通信提供身份认证与文件加密传输；同时针对数控网络中的专有工业通信协议数据，通过SM3算法验证专有工业协议数据完整性。最后通过网络攻击防御实验证明，AUTH-VRF模型可以为数控网络中工业生产数据提供有效的安全认证和资源完整性保护。

参 考 文 献

[1] 陈清明, 朱少辉. 关于工业控制系统网络安全审查工作的思考[J]. 信息安全与通信保密, 2018(6): 59–67. doi: 10.3969/j.issn.1009-8054.2018.06.011.
CHEN Qingming and ZHU Shaohui. Considerations on the network security censor of industrial control systems[J]. *Information Security and Communications Privacy*, 2018(6): 59–67. doi: 10.3969/j.issn.1009-8054.2018.06.011.

[2] 赖英旭, 刘增辉, 蔡晓田, 等. 工业控制系统入侵检测研究综述[J]. 通信学报, 2017, 38(2): 143–156. doi: 10.11959/j.issn.1000-436x.2017036.
LAI Yingxu, LIU Zenghui, CAI Xiaotian, *et al*. Research on intrusion detection of industrial control system[J]. *Journal on Communications*, 2017, 38(2): 143–156. doi: 10.11959/j.issn.1000-436x.2017036.

[3] 尚文利, 安攀峰, 万明, 等. 工业控制系统入侵检测技术的研究及发展综述[J]. 计算机应用研究, 2017, 34(2): 328–333, 342. doi: 10.3969/j.issn.1001-3695.2017.02.002.
SHANG Wenli, AN Panfeng, WAN Ming, *et al*. Research and development overview of intrusion detection technology in industrial control system[J]. *Application Research of Computers*, 2017, 34(2): 328–333, 342. doi: 10.3969/j.issn.1001-3695.2017.02.002.

[4] YANG Dayu, USYNIN A, and HINES W. Anomaly-based Intrusion Detection for SCADA Systems[C]. The 5th International Topical Meeting on Nuclear Plant

Instrumentation Controls, and Human Machine Interface Technology, Albuquerque, 2006: 797–802.

[5] 黄海, 冯新新, 刘红雨, 等. 基于随机加法链的高级加密标准抗侧信道攻击对策[J]. 电子与信息学报, 2019, 41(2): 348–354. doi: 10.11999/JEIT171211.
HUANG Hai, FENG Xinxin, LIU Hongyu, *et al*. Random addition-chain based countermeasure against side-channel attack for advanced encryption standard[J]. *Journal of Electronics & Information Technology*, 2019, 41(2): 348–354. doi: 10.11999/JEIT171211.

[6] 屠袁飞, 苏清健, 杨庚. 一种适用于工业控制系统的加密传输方案[J]. 电子与信息学报, 2020, 42(2): 348–354. doi: 10.11999/JEIT190187.
TU Yuanfei, SU Qingjian, and YANG Geng. An encryption transmission scheme for industrial control system[J]. *Journal of Electronics & Information Technology*, 2020, 42(2): 348–354. doi: 10.11999/JEIT190187.

[7] 冯登国. 国内外密码学研究现状及发展趋势[J]. 通信学报, 2002, 23(5): 18–26. doi: 10.3321/j.issn:1000-436X.2002.05.005.
FENG Dengguo. Status quo and trend of cryptography[J]. *Journal of China Institute of Communications*, 2002, 23(5): 18–26. doi: 10.3321/j.issn:1000-436X.2002.05.005.

[8] 国家密码管理局. GM/T 0003.1-2012 SM2椭圆曲线公钥密码算法 第1部分: 总则[S]. 北京: 中国标准出版社, 2012.
State Password Administration. GM/T 0003.1-2012 Public key cryptographic algorithm SM2 based on elliptic curves-Part 1: General[S]. Beijing: China Standard Press, 2012.

[9] 国家密码管理局. GM/T 0003.2-2012 SM2椭圆曲线公钥密码算法 第2部分: 数字签名算法[S]. 北京: 中国标准出版社, 2012.
State Password Administration. GM/T 0003.2-2012 Public key cryptographic algorithm SM2 based on elliptic curves-Part 2: Digital signature algorithm[S]. Beijing: China Standard Press, 2012.

[10] 国家密码管理局. GM/T 0003.3-2012 SM2椭圆曲线公钥密码算法 第3部分: 密钥交换协议[S]. 北京: 中国标准出版社, 2012.
State Password Administration. GM/T 0003.3-2012 Public key cryptographic algorithm SM2 based on elliptic curves-Part 3: Key exchange protocol[S]. Beijing: China Standard Press, 2012.

[11] 国家密码管理局. GM/T 0003.4-2012 SM2椭圆曲线公钥密码算法 第4部分: 公钥加密算法[S]. 北京: 中国标准出版社, 2012.
State Password Administration. GM/T 0003.4-2012 Public key cryptographic algorithm SM2 based on elliptic curves-Part 4: Public key encryption algorithm[S]. Beijing: China Standard Press, 2012.

[12] 国家密码管理局. GM/T 0003.5-2012 SM2椭圆曲线公钥密码算法 第5部分: 参数定义[S]. 北京: 中国标准出版社, 2012.
State Password Administration. GM/T 0003.5-2012 Public key cryptographic algorithm SM2 based on elliptic curves-Part 5: Parameter definition[S]. Beijing: China Standard Press, 2012.

[13] STINSON D R, 冯登国, 译. 密码学原理与实践[M]. 2版. 北京: 电子工业出版社, 2003: 131–142.
STINSON D R, FENG D G, translation. Cryptography Theory and Practice[M]. 2nd ed. Beijing: Publishing House of Electronics Industry, 2003: 131–142.

[14] 赵军, 曾学文, 郭志川. 支持国产密码算法的高速PCIe密码卡的设计与实现[J]. 电子与信息学报, 2019, 41(10): 2402–2408. doi: 10.11999/JEIT190003.
ZHAO Jun, ZENG Xuewen, and GUO Zhichuan. Design and implementation of high speed PCIe cipher card supporting GM algorithms[J]. *Journal of Electronics & Information Technology*, 2019, 41(10): 2402–2408. doi: 10.11999/JEIT190003.

[15] 国家密码管理局. GM/T 0004-2012 SM3密码杂凑算法[S]. 北京: 中国标准出版社, 2012.
State Password Administration. GM/T 0004-2012 SM3 cryptographic hash algorithm[S]. Beijing: China Standard Press, 2012.

[16] 国家密码管理局. GM/T 0002-2012 SM4分组密码算法[S]. 北京: 中国标准出版社, 2012.
State Password Administration. GM/T 0002-2012 SM4 block cipher algorithm[S]. Beijing: China Standard Press, 2012.

[17] ZIMMERMANN P R. The Official PGP User's Guide[M]. Cambridge: MIT Press, 1995: 152–188.

[18] KURNIAWAN Y, ALBONE A, and RAHYUWIBOWO H. The design of mini PGP security[C]. 2011 International Conference on Electrical Engineering and Informatics, Bandung, Indonesia, 2011: 6021726.

[19] 李强, 冯登国, 张立武, 等. 标准模型下增强的基于属性的认证密钥协商协议[J]. 计算机学报, 2013, 36(10): 2156–2167.
LI Qiang, FENG Dengguo, ZHANG Liwu, *et al*. Enhanced attribute-based authenticated key agreement protocol in the standard model[J]. *Chinese Journal of Computers*, 2013, 36(10): 2156–2167.

[20] LI Yong, SHA Xuejun, and WANG Kun. Hybrid carrier communication with partial FFT demodulation over underwater acoustic channels[J]. *IEEE Communications Letters*, 2013, 17(12): 2260–2263. doi: 10.1109/LCOMM.2013.102613.131651.

夏晓峰：男，1980年生，副教授，研究方向为信息安全.
向 宏：男，1964年生，教授，研究方向为信息安全.

责任编辑：余 蓉