第 45 卷 第 11 期 计 算 机 工 程 2019 年 11 月
Vol. 45 No. 11 Computer Engineering November 2019

·安全技术· 文章编号：1000-3428(2019)11-0159-07 文献标志码：A 中图分类号：TP309

基于单向传输协议的网间安全交换技术

曾凡毅，经小川，孙运乾

（中国航天系统科学与工程研究院，北京 100048）

摘 要：为解决工业控制系统与涉密工作网络之间信息安全交换的问题，提高信息交换的效率，提出一种基于单向传输协议的数据交换技术。构建数据交换可信验证模型，将业务数据分离成 2 个单向链路，并采用单向隔离设备实现网络的安全隔离和信息单向传输。通过控制信息管理子平台防止高密级信息流向低密级安全域，利用采集信息管理子平台抵御对涉密信息系统的攻击。设计数据安全传输机制，并进行私有协议封装。分析结果表明，该技术可实现工业控制系统与涉密信息系统间的安全互联和数据可信交换。

关键词：工业控制系统；涉密网络；安全隔离；验证模型；单向传输

开放科学（资源服务）标志码（OSID）：

中文引用格式：曾凡毅，经小川，孙运乾. 基于单向传输协议的网间安全交换技术[J]. 计算机工程，2019，45(11)：159-165.

英文引用格式：ZENG Fanyi，JING Xiaochuan，SUN Yunqian. Internetwork security exchange technology based on one-way transmission protocol[J]. Computer Engineering，2019，45(11)：159-165.

Internetwork Security Exchange Technology Based on One-way Transmission Protocol

ZENG Fanyi，JING Xiaochuan，SUN Yunqian

（China Aerospace Academy of Systems Science and Engineering，Beijing 100048，China）

【Abstract】 In order to solve the problem of information security exchange between industrial control systems and confidential working networks，and improve the efficiency of information exchange，a data exchange technology based on one-way transmission protocol is proposed. A data exchange trusted verification model is built to separate the business data into two one-way links，and the one-way isolation device is used to realize network security isolation and one-way information transmission. The information control management sub-platform is used to prevent the flow of high security information to low security domain，and the information collection management sub-platform is used to resist the attack on the classified information system. The data security transmission mechanism is designed，and data is packaged in private protocol. Analysis results show that the proposed technology can realize secure interconnection and data trusted exchange between industrial control system and classified information systems.

【Key words】 industrial control systems；confidential networks；security isolation；verification model；one-way transmission

DOI：10.19678/j.issn.1000-3428.0052658

0 概述

近年来，随着各重点单位生产任务逐渐增多，产品研制要求不断变化，批产质量要求持续提高，在面对不同需求特点的多个任务时，传统制造模式已难以满足其信息交换的需求。各重点单位势必要加快武器装备生产制造数字化的进程，相关工业控制系统的应用研究也将越来越广泛和深入[1]。

按照国家保密标准的相关要求，目前各重点单位的工业控制设备与涉密信息系统之间采取物理隔离和离线交换的方式[2]进行信息交换。信息流转通过人工的方式（利用三合一系统专用涉密介质、光盘等在摆渡点进行信息导入导出）间接进行，其交换流程繁琐，而且效率低下，严重影响科研生产的效率[3]。随着工业控制设备与涉密信息系统之间信息交换的数据量不断增长，离线摆渡操作日益频繁，人

基金项目：广东省科技厅应用型研发基金（2016B010127005）。

作者简介：曾凡毅（1993—），男，硕士研究生，主研方向为工控安全；经小川，研究员、博士生导师；孙运乾，硕士。

收稿日期：2018-09-13 **修回日期：**2018-11-19 **E-mail：**zengfy710@163.com

工管理成本提升,安全保密风险也随之增大。在生产制造过程中,部分任务的实时性要求较高,传统的人工交换方式不能满足业务的实时性需求。

现有研究大多针对互联方案进行,未考虑信息安全问题,也没有从传统的数据分析角度出发对工业控制信息系统和涉密信息系统间传输的数据进行解析以及配置白名单。文献[4]提出一种烧结工控网与办公局域网的组网互联方案,有效提高了生产管理效率。文献[5]提出一种单向安全隔离与交换机制,其克服了单向物理隔离条件下信息交换的不可靠问题,并对潜在的隐蔽通道进行严格控制,以缓解不同安全级网络之间隔离与信息交换之间的矛盾。文献[6]构建一种由内网边界主机模块、隔离交换模块以及工控网边界主机模块组成的"2+1"安全隔离模型,以保证数据在工作内网与工控网络边界上进行安全交换。

为进一步提高信息交换的工作效率和实时性,满足繁重生产任务下大量信息交换的需求,并实时监控工控设备的运行状态,本文在文献[6]的基础上进行改进,提出一种基于单向传输协议的数据交换可信验证模型,以实现工业控制设备与涉密信息系统之间高效、安全、可靠的数据交换。

1 安全交换模型分析

本文采用基于 2 个单向网络边界的防护模式,实现工业控制网络和涉密信息网络之间的边界隔离。同时,按照流向对数据进行剥离,并通过安全交换平台实现 2 个安全域之间数据的单向、可控传输。

1.1 网络渗透攻击分析

本文从实施网络渗透攻击的角度对模型的整体安全性进行分析。网络攻击示意图如图 1 所示。

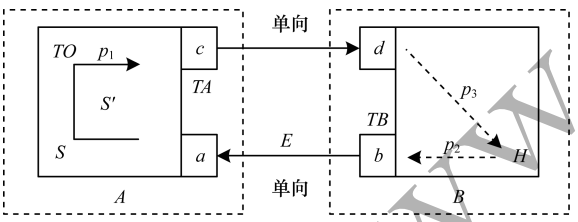

图 1 网络攻击示意图

在图 1 中:A、B 分别表示被攻击网络和攻击者所在网络;H 表示 B 中的一个攻击者;c 和 a 分别表示 A 的边界出口和入口;b 和 d 分别表示 B 的边界出口和入口;E 表示 H 从 b 发出的攻击探测数据集合;S 表示在 A 中从 a 开始的所有网络数据传播路径;S'表示一切可以从 a 到 c 的网络数据传播路径,且 $S'\subseteq S$;函数 $F(E,S)$表示由 H 发出的探测数据得到的响应数据,并沿某一路径传播;TB 表示从 b 发出的探测数据的状态;TA 表示从 c 发出的响应数据的状态;TO 表示响应数据在 A 中的其他状态。TB 到 TA 的状态转换公式为 $TB\xrightarrow{F(E,S)}TA$,TB 到 TO 的状态转换公式为 $TB\xrightarrow{F(E,S-S')}TO$。

在网络 A 和网络 B 中部署防火墙、交换机等网络设备,通过交换机划分虚拟局域网(Virtual Local Area Network,VLAN)并设置 VLAN 之间的访问控制策略,通过防火墙实现安全域间的隔离并进行细粒度的访问控制,使其具有较高的安全性。网络渗透攻击的具体分析如下:

1)攻击失败的可能性证明

假设攻击者 H 发出的探测数据 $\forall e\in E$ 沿着 S 中的任意路径 s 均可形成数据回路并回到 B,即到达 TA 状态,则需要满足状态转换公式 $TB\xrightarrow{F(E,S)}TA$,即满足 $s\in S'$。

由于 s 为任意路径,因此存在 $s\in S-S'$,即存在 $TB\xrightarrow{F(E,S-S')}TO$ 状态转换,从而无法形成回路回到 B。这与假设的前提矛盾,因此,攻击者 H 发出的探测数据 $\forall e\in E$ 沿着任意路径 s 不一定能形成数据回路回到 B。

由上述证明可以看出,攻击者只有沿着特定的路径才能成功实施攻击。

2)攻击成本

攻击者要成功实施一次攻击,至少要先获知攻击路径中各网络节点的 IP 地址和端口。本文假设攻击者已获知被攻击网络的 IP 网段,但各网络节点的端口未知。

以 C 类网段为例,一个网段内共有 253 个可用 IP 地址,每个网络节点又有 65 535 个端口。假设攻击者从 b 开始,沿着从 a 出发的一条路径 s 到达 c,最后经 d 返回。在整个攻击过程中,如果经过网络 A 中的 m 个相同网段的网络节点,则其传播路径总数($total$)的计算如下:

$$\begin{aligned}total=&(253\times65\ 535)\times(252\times65\ 535)\times\cdots\times\\&[(253-m+1)\times65\ 535]=\\&253\times252\times\cdots\times(253-m+1)\times65\ 535^{m}\end{aligned}$$

考虑最简单的情况,a 经过防火墙到达 c,a、c 以及防火墙 3 个网络节点处于同一网段,则在网络 A 中攻击路径的可能性就有 $253\times252\times251\times65\ 535^3$ 种。随着网络复杂性的增加,经过的网络节点数越来越多,网络 A 中传播路径的总数呈指数增长。

设数据沿 S 传播的可能性为 1,沿 S'传播的可能性为 p_1。根据上述分析可以推出 $p_1\ll1$,$L'\ll L$,即 $L'\ll L-L'$,则攻击者 H 发出的探测数据 $\forall e\in E$ 沿着路径 s 形成数据回路回到 B 的可能性很小,可忽略不计。考虑攻击者获得从 H 到 b 的路径的可能性 p_2 和 d 到 H 的路径的可能性 p_3,则从 H 发出,通过 A 再回到 H 的可能性为 $p_1\times p_2\times p_3<p_1\ll1$。

如果攻击者采用穷举的方法试探每一条路径,则需耗费大量时间,攻击没有意义。此外,高密度的

网络探测通过入侵检测系统也可以及时发现攻击者。考虑到攻击的成本,在网络 *A* 较安全的前提下,可以认为攻击者 *H* 很难成功渗透到其中。

1.2　链路安全性分析

互联网络中的涉密网只能向工控网单向下发控制数据,而工控网只能向涉密网单向回传采集数据。涉密网、工控网具有以下属性:

1)涉密网属于高密级网络,工控网属于低密级网络;

2)涉密网属于数据完整性级别较高的网络,工控网属于数据完整性级别较低的网络;

3)控制信息是完整性级别高的文件,只允许由涉密网向工控网单向“写”;

4)采集信息是低密级网络中的数据,只允许由工控网向涉密网单向“写”。

信息传输过程如图 2 所示。在图 2 中,采集信息的回传满足属性 1)和属性 4),即低密级网络中的数据只能由低密级网络向高密级网络单向“写”,可采用 BLP(Bell-Lapadula)模型进行设计。控制信息的下发链路满足属性 2)和属性 3),即完整性要求高的数据只能由完整性级别高的网络向完整性级别低的网络单向“写”,可采用 Biba 模型进行设计。

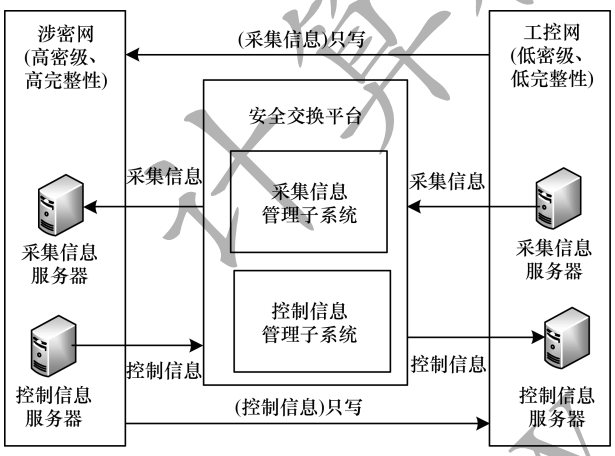

图 2　信息传输示意图

1.2.1　BLP 模型

BLP 模型是 20 世纪 70 年代美国军方提出的用于解决信息安全和保密问题的安全模型,它主要强调信息的保密性控制,限制信息从高密级流向低密级[7]。BLP 模型主要包括主体、客体、访问操作(读、写、读/写)以及安全级别等概念,当主体和客体位于不同的安全级别时,主体对客体就有一定的访问限制[8]。BLP 模型结构如图 3 所示,其访问机制如下:

1)安全级别低的主体访问安全级别高的客体时,主体对客体可写不可读;

2)主体访问同一安全级别的客体时,主体对客体可写可读;

3)安全级别高的主体访问安全级别低的客体时,主体对客体可读不可写。

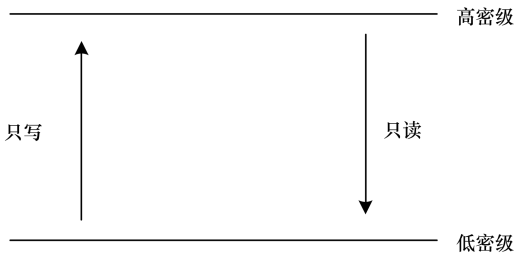

图 3　BLP 模型结构

1.2.2　Biba 模型

Biba 模型是一种用于解决计算机系统信息完整性的安全模型,该模型从保护系统信息完整性的角度进行设计,其访问控制建立在完整性级别上[7]。Biba 模型能够防止数据从低完整性级别流向高完整性级别。Biba 模型的具体结构如图 4 所示,其访问机制如下:

1)完整性级别低的主体访问完整性级别高的客体时,主体对客体可读不可写;

2)主体访问同一完整性级别的客体时,主体对客体可写可读;

3)完整性级别高的主体访问完整性级别低的客体时,主体对客体可写不可读。

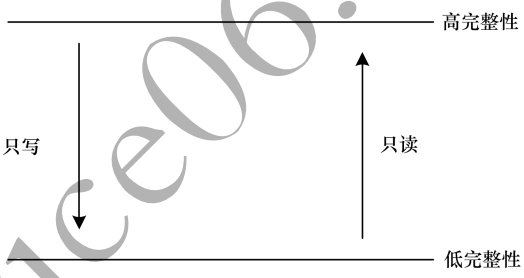

图 4　Biba 模型结构

2　安全交换技术

2.1　安全交换平台

本文依据 BMB17-2006《涉及国家秘密的信息系统分级保护技术要求》和 BMB20-2007《涉及国家秘密的信息系统分级保护管理规范》等保密标准规范[9-10],基于物理隔离、分域防护、流向控制、高可用性、应用扩展性、安全的边界防护、宽进严出的设计原则[11],面向涉密网和工控网之间安全互联、数据可信交换的需要,设计安全交换平台。在平台管理层、数据管理层、数据通信层进行多层次安全防护,实现信息可信、可靠、可控传输[12]。

平台以统一规划的信息资源目录为数据标准,通过灵活配置的抽取和推送链路,实现信息资源全程可监管的安全抽取与推送,打破不同应用系统间的信息壁垒。同时,平台内部采用单向传输链路,降低工业控制系统对涉密信息系统的安全威胁[13]。

一个典型的工业控制网络所涉及的业务信息可分为控制信息和采集信息,2 类信息相互独立,为不同

方向的数据流[14]。平台根据工控系统业务需求和数据流向,将工控系统的业务数据进行剥离,分别通过控制信息管理子平台和采集信息管理子平台实现工控系统中控制数据、采集数据的单向传输和管理。

控制信息管理子平台和采集信息管理子平台在物理结构上均由收集子系统、传输控制子平台和推送子系统 3 个部分组成。这 3 个部分均从子平台管理层、数据管理层和数据通信层 3 个层级进行设计,其中每一层设计都细化为多个具体的功能模块。安全交换平台架构如图 5 所示。

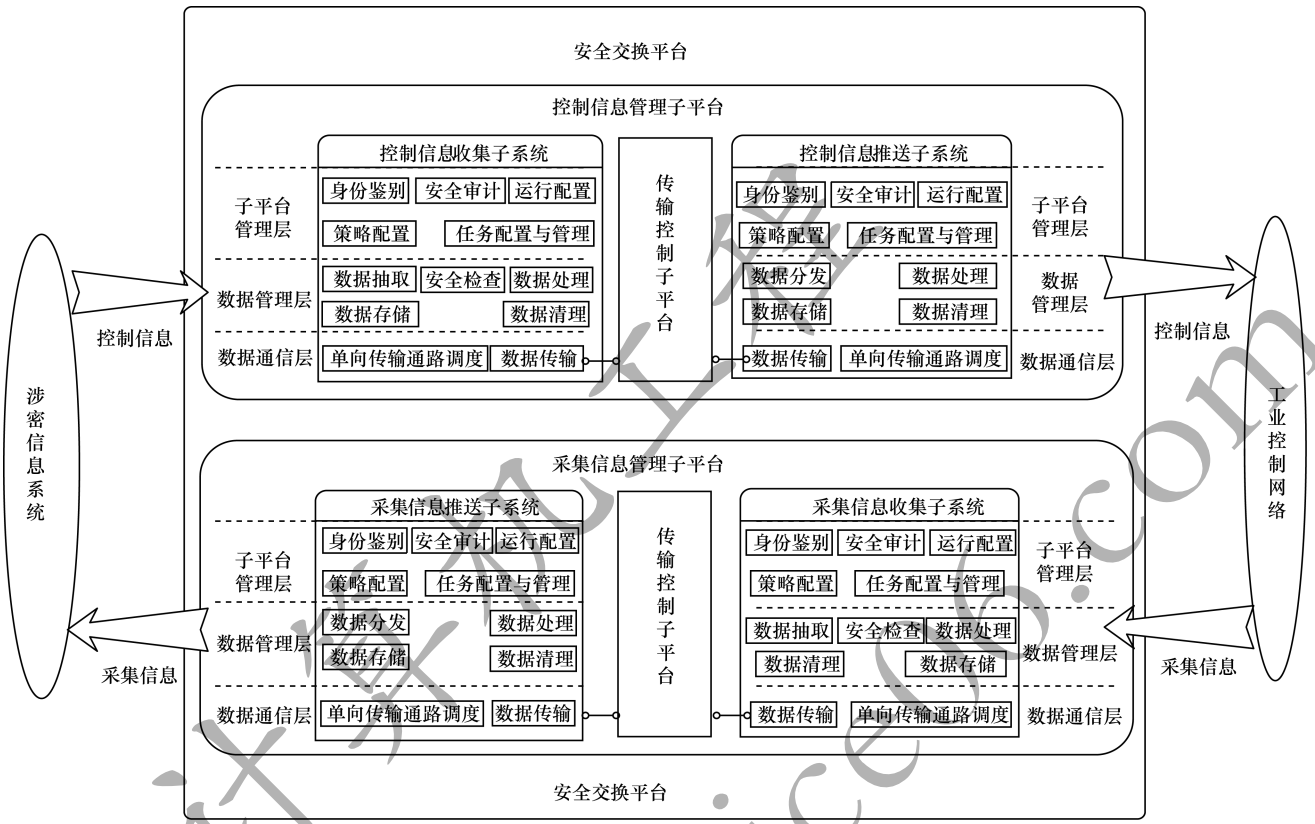

图 5 安全交换平台架构

2.1.1 控制信息管理子平台

对于重点制造单位来讲,数据的完整性尤其重要,细微的差错可能造成重大的损失和影响。控制信息的下发链路参照 Biba 模型进行设计,采用一系列完整性防护机制,确保控制信息只能通过平台从完整性级别高的涉密网向完整性防护级别低的工控网中进行写操作。Biba 模型的应用场景如图 6所示。

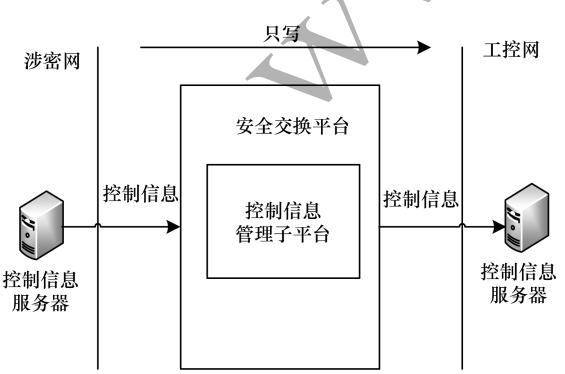

图 6 Biba 模型的应用场景

涉密信息系统为控制信息收集子系统访问涉密系统中业务系统(如 DNC 系统)的数据接口,并按照预先设定的规则抓取数据(如数控程序)。经过一系列安全处理(认证、密级标识、完整性校验处理、深度检查、加密)后,通过传输控制子平台将数据单向传输至控制信息推送子系统。控制信息推送子系统按照预先设定的推送策略,安全地将控制信息推送至工业控制网络中对应的业务系统。深度检查操作包括对数据的属性(如数据类型、大小)和内容的检查。其中,内容检查中包含基于指令集和边界参数的限定,而其他数据检查只需按同样的方式处理即可进行扩展,禁止其他信息传输,以避免高密级信息流向低密级网络。

2.1.2 采集信息管理子平台

采集信息的回传链路参照 BLP 模型进行设计,工控网中的采集信息只能通过平台向涉密网中的采集信息服务器进行写操作,BLP 模型的应用场景如图 7 所示。

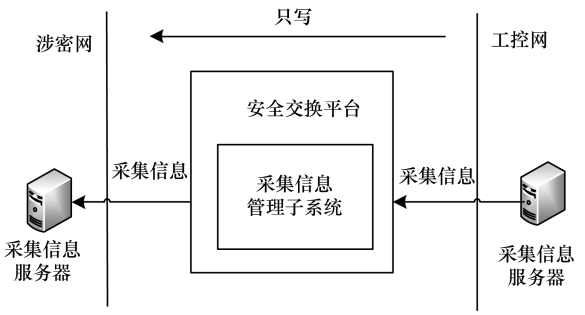

图 7　BLP 模型的应用场景

采集信息收集子系统为访问工业控制网络中业务系统(如 MDC 系统)的数据接口,并按照预先设定的规则抓取数据(如机床的状态信息),经过一系列病毒查杀、转换等处理后,通过传输控制子平台将数据同步至采集信息推送子系统。采集信息推送子系统按照预先设定的推送策略,安全地将采集信息推送至涉密信息系统中对应的业务系统。

2.2　数据安全传输

控制信息管理子平台和采集信息管理子平台的设计原理相同,其主要差异体现在数据的传输方向以及数据的抓取、处理机制等方面。为方便描述,下文将控制信息收集子系统、采集信息收集子系统统称为信息收集子系统进行描述,将控制信息推送子系统、采集信息推送子系统统称为信息推送子系统进行描述。

安全交换平台在数据通信过程中采取数据加密传输的机制。信息收集子系统在应用数据转发之前,先将应用数据拆成数据包,然后创建报文并采用加密措施对应用数据进行加密,以防止数据报文在传输过程中被抓包窃听和还原。

2.2.1　信息收集子系统

信息收集子系统的数据发送模块对抽取的应用数据进行拆包、封装,然后与传输控制子平台的发送机建立可信连接,以传输数据包。

1)应用数据的拆包与封装

信息收集子系统的数据通信层首先将整个应用数据拆分成若干个小的数据包,然后针对每个数据包创建数据报文,具体创建过程如图 8 所示,可分为 2 个步骤:

(1)使用规定的加密算法和密钥对报文中的数据进行加密。

(2)为数据报文加入传输头信息,具体包含信息收集子系统数据通信层、传输控制子平台的发送端之间约定的通信指令。

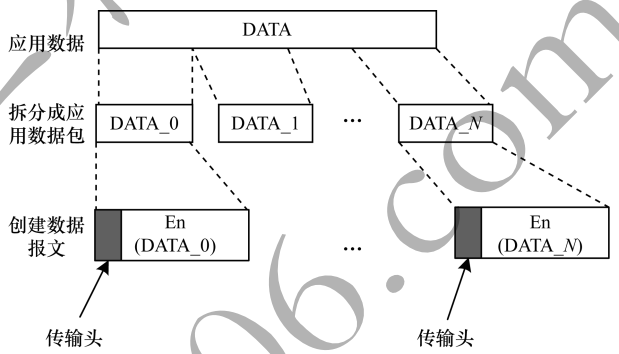

图 8　报文创建过程

2)连接认证

信息收集子系统的数据通信层、传输控制子平台的发送端之间需建立认证机制,采用 Socket 方式确认双方身份可信后才能进行正常通信,其握手认证过程如图 9 所示。

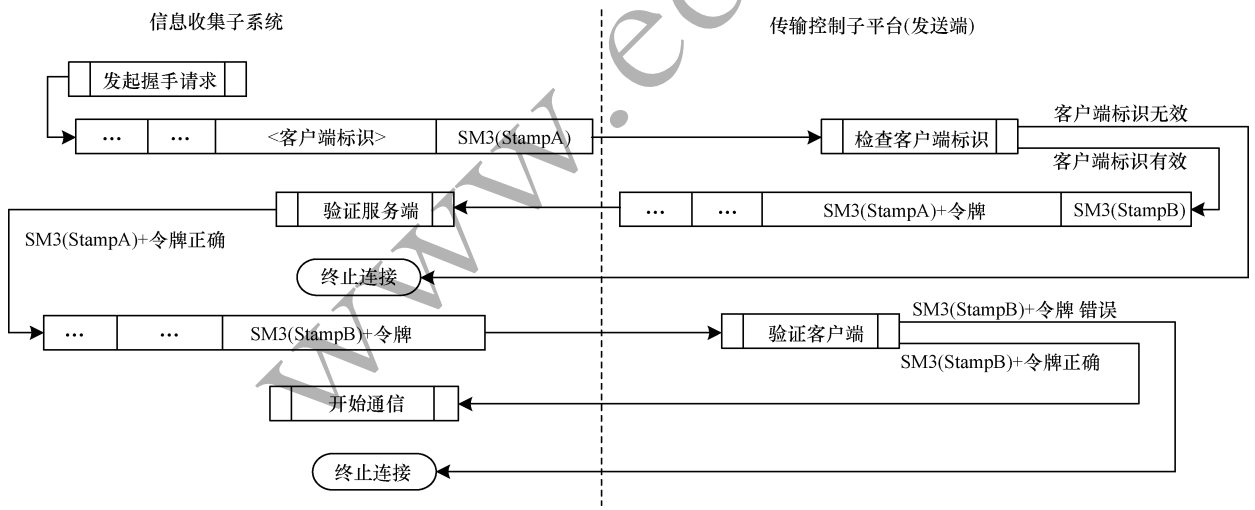

图 9　握手认证过程

握手认证的具体过程如下:

(1)信息收集子系统的数据通信层、传输控制子平台的发送端各产生一个时间戳,分别是 StampA 和 StampB。

(2)信息收集子系统的数据通信层创建 Socket,并连接到传输控制子平台的发送端,同时信息收集子系统发送通信包,其中包含信息收集子系统(客户端)标识以及 StampA 的 SM3 码。

(3)传输控制子平台的发送端检查是否存在客户端,若存在则回发 StampA 的 SM3 码 + 令牌以及 StampB 的 SM3 码,否则判断客户端不合法,终止连接。

(4)信息收集子系统接收到回馈信息后,根据自身 StampA 的 SM3 码和已保存的令牌进行 SM3 计算,然后与传输控制子平台的发送值进行匹配。如果匹配成功则发送 StampB 的 SM3 码 + 令牌,否则终止通信过程。这一步即实现了信息收集子系统对传输控制子平台发送端的认证。

(5)传输控制子平台发送端根据 StampB 的 SM3 码和已保存令牌组合后的 SM3 码,与信息收集子系统发送值进行匹配。如果匹配成功则开始通信,即实现了传输控制子平台发送端对信息收集子系统的认证。

2.2.2 信息推送子系统

信息推送子系统的数据通信层与传输控制子平台的接收端建立可信连接,同时接收所有转发的数据包。在得到所有转发的数据包以后,数据通信层对数据包进行解析,将其还原成原始的数据包。最后,将各个小数据包重组为加密后的应用数据。

1)连接认证

信息推送子系统与传输控制子平台的接收端需要先进行通信认证才能传输数据,具体认证过程参见 2.2.1 节。

2)数据的解析与还原

信息推送子系统的数据通信层在接收到转发的数据报文后,需要对数据进行解析,具体过程如图 10 所示。

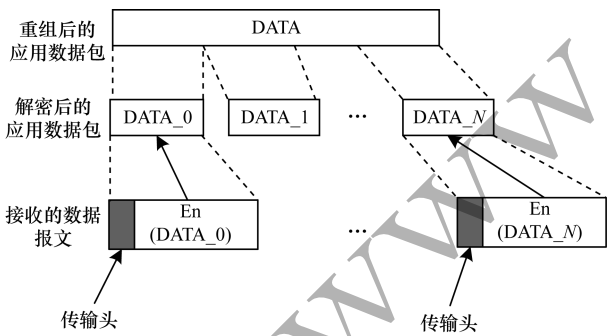

图 10 报文解析过程

数据的解析与还原过程主要分为 2 个步骤:

(1)接收数据报文。对每一个数据报文,使用规定的算法和密钥解密报文里的数据,还原其中的数据包,同时根据数据报文的传输头信息判断是否所有的数据包都传输完毕。

(2)当所有的数据包传输完毕后,对所有小的数据包进行重组,还原得到完整数据。

2.2.3 传输控制子平台

传输控制子平台负责将控制信息收集子系统的数据单向传输至控制信息推送子系统,将采集信息收集子系统的数据单向传输至采集信息推送子系统。通过主流的单向隔离设备,将传输控制子平台与单向隔离设备进行集成,完成绝对单向传输的功能。

传输控制子平台的发送端、接收端的单向传输模块分别与信息收集子系统、信息推送子系统建立连接,具体的连接认证过程参见 2.2.1 节的相关内容。然后采用单向传输通道将信息收集子系统的数据包转发到信息推送子系统。

传输控制子平台采用私有协议实现单向传输,同时直接转发所有的数据包,以存储全部数据信息。传输控制子平台可从硬件上屏蔽所有信号反馈,其没有握手认证机制来保证传输数据完整、可靠。为减少在数据单向传输中的出错概率,传输控制子平台采用基于 RS 算法的前向纠错机制、扰码机制、多冗余通道发送光信号等多种技术进行纠正与检测。

2.3 单向传输协议

安全交换平台的底层数据传输协议采用自定义的私有协议进行传输。信息收集子系统按照私有协议封装数据包,确保经过传输控制子平台转发的数据包只能由信息推送子系统进行解封,如果不能解封,则判断数据为非法数据,可及时丢弃。此外,信息收集子系统与传输控制子平台,传输控制子平台与信息推送子系统之间均采用私有协议进行连接认证,然后才能进行数据传输。

2.3.1 设计思路

本文平台没有反向的控制信息,因此发送端不知道接收端的状态信息。为确保数据传输的完整性,需要制定一套单向的传输协议。发送端不需要确认接收端是否收到数据以及数据是否完整,因此单向传输协议仅通知接收端应用数据的类型、长度等信息即可[15]。

基于以上思路,数据传输应包含以下内容:

1)系统数据的内容。

2)系统数据的相关属性信息,如相关传输需求、应用数据的大小等,接收端接收到数据后,需要将其还原成相应的应用数据。

3)系统数据的 MD5 值,用来检验原始数据是否完整。

4)系统数据、数据块的 ID 标记,用来判断在传输过程中是否遗漏系统数据或数据块。

5)CRC 校验值,对数据块是否完整进行检验。

6)同步信号,对传输通道的状况进行检测。

通过以上内容可以看出,传输的数据类型可以归为 2 类:系统数据的相关内容和同步信号数据,且每一种数据的功能不同。此外,在系统数据传输过程中,仅有一条数据帧并不能实现一段系统数据的完全发送。因此,需将系统数据进行拆分,以小块的数据传输方式进行传输。

2.3.2　数据块类型及传输时序

根据 2.3.1 节的设计思路,数据块可以分为系统数据块(System Data Block,SDB)和信号同步数据块(Synchronous Date Block,SYDB)2 大类。

1)系统数据块用来传输系统数据,依据系统数据传输过程可再分为以下 4 种:

(1)起始数据块(Initial Data Block,IDB):包括系统数据流水号、数据大小、系统数据 MD5 值。

(2)分块数据块(Block Data Block,BDB):用来对系统数据进行分块传输,包括数据分块流水号、数据内容。

(3)FEC 冗余数据块(FEC redundant Data Block,FDB):用来对系统数据分块的 FEC 纠错冗余数据进行传输,主要包括数据分块流水号和 FEC 冗余数据内容。

(4)结束数据块(End Data Block,EDB):用来标记系统数据传输结束。

2)信号同步数据块:发送端通过定时发送 SYDB 检测线路是否发生故障。

系统在数据传输时,数据块的发送顺序如图 11所示。每段系统数据按照 IDB→BDB1→BDB2→…→FDB1→FDB2→…→EDB 的顺序进行发送。安全交换平台通过对协议的封装,能够有效防止无效数据或试探性的网络数据包的传输。

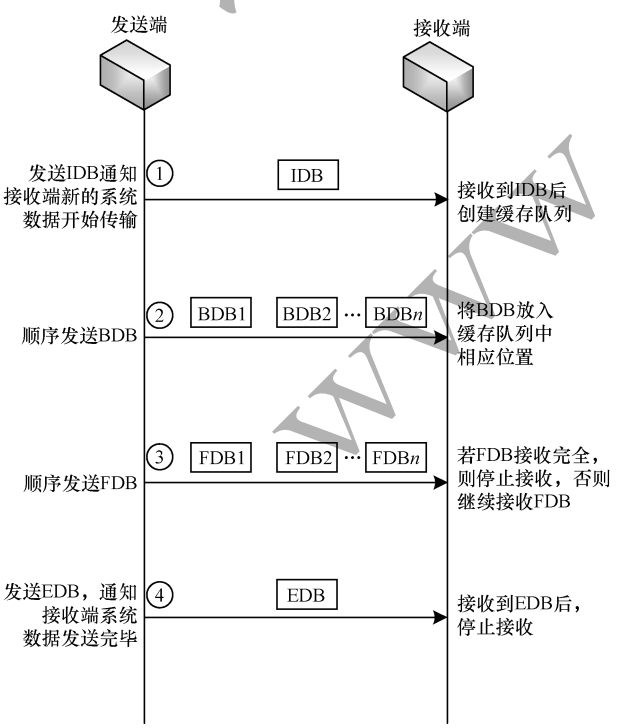

图 11　数据块传输时序

3　结束语

本文提出一种基于单向传输协议的网间安全交换技术。对网络渗透攻击及链路安全性进行分析,在此基础上构建数据交换可信验证模型。将业务数据剥离成 2 个单向链路,设计基于 BLP/Biba 混合模型的安全交换平台,提出数据安全传输机制,并通过单向传输协议对数据进行封装。分析结果表明,该技术可实现安全互联和数据可信交换,是工业控制系统联网交换的一种安全可行的解决方案。下一步将对数据单向传输的效率以及可靠性进行研究。

参考文献

[1] 王会东.构建军工科研生产单位信息安全防护体系[J].中国信息化,2017(8):77-82.

[2] 王婵,黄立峰,裴威.浅析军工企业信息化发展策略[J].中国信息化,2013(12):125.

[3] 赵甫,王琦魁,李昕,等.军工工业控制系统信息安全保密风险与防护方法研究[J].保密科学技术,2016(9):30-33.

[4] 程昌云,管友红.烧结工控网与办公局域网的组网互联[J].冶金设备管理与维修,2012,30(1):6-7.

[5] 陈达,马威,李晓勇,等.一种单向安全隔离与信息交换机制[J].信息网络安全,2014(6):48-52.

[6] 谢梅,刘向东.制造行业工控网与企业内网的安全互联技术研究[C]//全国信息安全等级保护技术大会论文集.沈阳:公安部第一研究所,2014:439-445.

[7] BALAMURUGAN B,SHIVITHA N G,MONISHA V,et al. A honey bee behaviour inspired novel attribute-based access control using enhanced Bell-Lapadula model in cloud computing [C]//Proceedings of International Conference on Innovation Information in Computing Technologies. Washington D. C.,USA:IEEE Press,2016:1-6.

[8] 刘波,陈曙辉.一种基于 Bell-Lapadula 模型的单向传输通道[J].计算机科学,2012,39(10):26-29.

[9] 魏刚.涉密信息系统分级保护[J].电子技术与软件工程,2016(21):203.

[10] 郎静宏,刘昊杰.浅析军工企业信息系统分级保护制度体系的建设[J].保密科学技术,2015(12):52-54.

[11] STIAWAN D,IDRIS M Y,ABDULLAH A H,et al. Cyber-attack penetration test and vulnerability analysis[J]. International Journal of Online Engineering,2017,13(1):125.

[12] 宋卫平.四川省电力公司双网隔离环境下内外网交互平台的设计与实现[D].成都:电子科技大学,2013.

[13] YAO Peisong,XU Feiran,LI Jie. An industrial control system data shunt and one-way transmission security model[C]//Proceedings of the 36th Chinese Control Conference. Washington D. C.,USA:IEEE Press,2017:7559-7563.

[14] 周建宁,季君,彭璇,等.公安内外网数据交换平台的设计研究[J].中国公共安全(学术版),2017(2):73-77.

[15] 杨越.多通道单向传输技术的研究与应用[D].北京:中国航天科工集团第二研究院,2016.

编辑　樊丽娜