iFIX的安全机制及其工控网络三层安全模型

吴志强[1] 卢 刚[2] 谢建辉[2] 赖如清[2] 黄东军[1]
1 中南大学信息科学与工程学院(410083) 2 江西德兴铜矿泗洲选矿厂(334224)

Abstract

This paper introduces and studies the secure mechanism of iFIX in the field of industry control.We analysis the relationship between users,user groups,security areas and application features.We also show some shortcoming of iFIX security mechanism.Based on these studies,we raise the three-layered security model based on iFIX in the industry control network.This model has many advantages such as meeting the industry security requirements well,real-time data transmitting easily and smoothly,scalability,easy deployment,etc.The model has achieved good effects in realistic.

Keywords:iFIX,secure mechanism,three-layered secure model

摘 要

本文介绍和研究了工业控制领域中iFIX的安全机制,分析了用户、用户组、安全域和应用属性及其相互关系,同时阐述了iFIX安全的一些局限性,在此基础上提出了基于iFIX的工业控制网络三层安全模型。该模型具有符合工业安全要求、实时数据通畅可靠、可扩展性好、部署方便等特点,实际应用中取得了良好的效果。本文的工作对于进一步提高iFIX的安全应用具有一定的借鉴意义。

关键词:iFIX,安全机制,三层安全模型

Intellution公司的iFIX软件是完全基于组件对象技术的自动化解决方案,是FIX的升级版。最近推出的iFIX 2.6中文版,降低了掌握iFIX的门槛。由于工控场合特殊的安全需求,加之工业控制网络和企业信息系统实现了互联,而操作系统与应用软件的缺陷或漏洞频繁出现,因此,安全问题越来越受到人们的重视。如何用iFIX构造好一个安全高效,数据通畅,可扩展性好,结构紧凑健壮的网络结构,成为亟待解决的课题。

1 iFIX的安全体系结构

本节阐述和研究iFIX安全的基本概念,这些概念是正确应用iFIX的基础。

(1)iFIX SCADA节点的基本安全需求

SCADA节点是运行数据实时采集、数据管理组件的iFIX节点,用户数目较多而且关系比较复杂,对安全有着特定的需求,对不同的用户有着不同的权限设置。用户一般分为系统管理员,系统操作员,数据录入人员,系统备份人员等。iFIX中的数据块是其实时数据库中的数据项,可以通过I/O DRIVER连接到下位机PLC(可编程逻辑控制器)然后直接对应工业现场中的某个变量,必须针对不同的用户对相应的数据块设定不同的访问权限特别是修改权限,这是工业安全中最基本的需求。iFIX的工作状态分为组态方式和运行方式,运行方式中的程序是以画面文件(.grf)为基本单位的。在实际应用中,一般限制普通用户直接退出到操作系统进行文件的增删改。

(2)iFIX用户、用户组、安全域、应用属性

用户(User):它是iFIX中登录的基本单位,可以属于某个用户组。用户拥有的属性是一些安全域和一些应用属性。用户组(User Group):它也可以拥有某些安全域和某些应用特性,一旦用户属于某个用户组,用户就拥有了用户组的所有安全域和应用特性。安全域(Security Areas)是一个逻辑上的单位,安全域可以按工厂的物理范围或按功能划分。实时数据库中的每个数据块都可拥有不同的安全域,iFIX下的某些其他对象也拥有一些安全域。应用属性(Application Features)是iFIX中对整个工作平台运行环境权限的细分,如能使用数据库管理器,能进行时实数据库保存,能使用配方生成器操作窗口,能退出iFIX运行环境,拥有工作台运行权限等。从逻辑上说,应用属性和安全域是同一层次的概念。使用安全域,可以方便的对不同的工艺变量进行权限设定,可以对变量进行数据的逻辑划分,如报警分域自动打印。图1表示了用户、用户组、安全域和应用属性之间的关系。

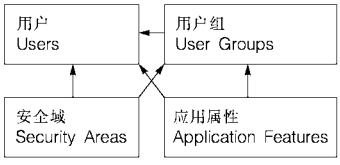

图1 用户、用户组、安全域和应用属性之间的关系

如果用户 USER-A 拥有 A 域权限，并且 iFIX 中的某一些对象也至少拥有 A 域的属性，那么 USER-A 就可以对整个拥有 A 域的对象进行某种操作，这种操作具体到数据块上就是写的操作。拥有安全域的对象包括数据块、运行画面、配方、自动化集对象(DynamoSet object)、计划任务对象(Scheduler object)和用户宏对象(UserGlobals object)等。如 AI(模拟输入)数据块 BLOCK1，标签名为 BLOCK1，若拥有输出的属性，且拥有三个安全域 A，B，C，那么 USER-A 可以在数据库编辑器或者是运行态动态链接输入环境下对 BLOCK1 块进行写操作，对应的操作可以使得 iFIX 通过 PLC 发送写指令使工厂某台电机旋转。如果 USER-B 只拥有 B 域的权限和一些应用属性，那么就无法写 BLOCK1，这在工业安全中是非常重要的。简而言之，用户只要拥有与数据块相同的安全域就可以对数据块进行写的操作。

iFIX 未直接提供限制用户读取实时数据库中数据块的方法，所以对数据块的读取不受直接限制，但在应用属性中具有实时数据库打开编辑的应用属性项，因此在某种程度上对数据的读取可进行间接限制。在实际使用中常常根据不同的工艺流程安全要求设定不同的安全域，以分别对待工厂中不同类型的用户，他们之间可以互不干扰，也可以协同操作，这是国内的一些工控软件所没有的功能。如，组态王，它的实时数据库称为数据字典，数据项对应 iFIX 中的数据块，数据项的权限是用数字表示的；每个用户都拥有不同的权限，它也用数量 0~999 来衡量，只有用户权限比数据项权限大的时候才能对这个数据项进行修改操作。但实际应用中的不同数据项间的修改权限并不仅仅是一个大小的关系，或者根本不存在权限谁大谁小的关系，用数量大小来衡量用户操作数据项的权限是不够的。

(3)iFIX 用户账号与 Windows NT 账号的关系

iFIX 中可以使用 WinNT 上的帐号，但是不能使用 WinNT 上的组。如果使用 WinNT 帐号，同样需要对这个帐号进行安全域和应用属性的配置，配置好后才能访问相应的 iFIX 资源。使用 WinNT 的帐号并不能使登录 WinNT 的同时自动登录 iFIX，同样需要用此帐号登录 iFIX，这一功能称为帐号同步。使用帐号同步的一个优点就是便于对 WinNT 下的 iFIX 进行统一管理，可以高效安全地修改用户口令，可以充分利用一些 Windows 下的安全体系结构，如 Windows 2000 活动目录(Active Directory)安全体系结构，针对不同的用户进行不同的权限配置，方便网络用户的访问，可靠而且高效。使用帐号同步避免了某些用户非法访问或修改操作系统文件，间接对 iFIX 进行数据的复制修改或者破坏，使得 iFIX 的安全与操作系统的安全紧密结合在一起。这也是当前应用软件安全的发展趋势。

(4)iFIX 的脚本编辑环境的安全性

iFIX 下的 VBA (VB Application) 与自带的一些 OLE 控件可以方便的对对象安全域进行操作。VBA 最早应用于 MICROSOFT 的 WORD 等软件中，iFIX 现在集成了 VBA，功能强大，使用简单高效，是其他的一些自动化软件所不能比拟的。VBA 可以十分简单方便地调用各种组件对象模型，可以快速开发出各种工艺流程画面，也可以方便地使用 VBA 通过自动化接口实现安全应用。VBA 与 iFIX 的安全是同一个级别的，iFIX 对 VBA 的执行没有限制，因此，需要程序员直接通过 iFIX 自动化接口操作 VBA 对象的安全属性。

比如获取当前用户状态信息，可以使用 System 对象：

System.FixGetUserInfo (USER_ID,USER_NAME,USER_GROUP);

判断用户有没有访问数据库管理器的权限，也可以使用 System 对象：

System.FixCheckApplicationAccess(DatabaseManager);

iFIX 将安全域进行了统一编号，每一个安全域唯一对应一个数字，这样就更加容易管理。例如，System.FixCheckAreaAccess(11)判断有没有访问第十一号安全域的权限；设定对象的安全域可以使用 Object.SecurityAreas=´A´，其中 A 是安全域标识符，等等。程序员可以方便的开发工艺流程画面的同时实现自己特殊的安全应用。

(5)iFIX 的安全审查文件

安全审查文件记录了每次用户登录的过程，审查跟踪文件 YYMMDD.LOG 驻留在报警路径中。查看审查跟踪，可以获悉：谁登录和注销过 iFIX；何时操作员没有完成的登录过程；何时有人试图进入无访问权限的安全区域或应用特性；何时操作员超出登录的时间。

(6)iFIX 安全机制的局限性

首先，操作系统的某些缺陷让原本安全的安全机制变得不安全。如，我们发现 2000 年就公布的 Windows 2000 输入法漏洞同样在最新版 iFIX2.6 中存在，在运行态时，一个没有任何权限的用户如果找到一个数据输入窗口打开帮助就可以进入操作系统进行文件操作，经过若干操作后也能够成为合法用户。且只要覆盖一些用户配置文件，就可成为 iFIX System Administrators。这对某些企业来说是极大的威胁。

其次，iFIX 的安全机制是组件级的，是建立在 iFIX 自己的某些 OLE 控件安全基础上的。虽然 iFIX 声称拥有安全容器技术，可以防止第三方控件的崩溃，但 OLE 控件的数据封装性使得 iFIX 无法进行安全域的

控制,OLE 控件拥有一切 iFIX 所拥有的权限，程序员使用第三方控件就存在安全问题。

第三,VBA 的所有安全保障都由程序员来实现，这增加了安全的复杂性。安全域并未对 VBA 脚本进行限制。例如,上文中的在 A 域未授权用户 USER-B 可以执行一段代码:FIX32.THISNODE.BLOCK1.F_CV=100000,其结果是跨域非法操作了数据;而一个粗心的程序员就有可能认为未授权的用户不可能执行此命令。

2 iFIX 的网络级安全及其局限性

用 iFIX 可以组成一个分布式网络,程序员只要知道目标节点名,在任何一个 iFIX 节点都可以高效的访问其他节点的数据，一般是访问 SCANDA 节点的数据。网络间的连接对程序员是透明的,使用非常方便而且功能强大。节点名是区分 iFIX 节点的主要标识。图 2 表示了一个 iFIX 网络的结构。

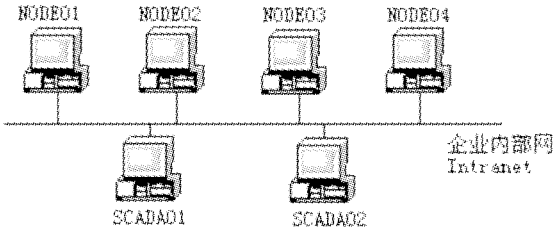

图 2 iFIX 网络结构

iFIX 节点的数据安全分为两个部分，第一是禁用未授权节点的连接，第二是禁止未授权用户远程修改过程数据库。iFIX 的网络安全机制的具体实现是通过配置 Dynamics 子目录下的 NETWORK.INI 文件实现。例如在 SCADA01 结点 NETWORK.INI 文件中写入：

```
[WRITEACCESS]
accept_unauthorized_writes=OFF
writenode1=NODE01
writenode2=NODE02
```

就可以只让 iFIX 节点名为 NODE01 和 NODE02 的计算机进行远程数据库写访问。

在 SCADA02 节点 NETWORK.INI 文件中写入：

```
[TCPIP]
accept_unknown_host=OFF
host1=NODE03
host2=NODE04
```

就可以只让 iFIX 节点名为 NODE03 和 NODE04 的计算机进行远程 TCP/IP 的连接，其他的节点的连接都会被拒绝。默认状态下 accept_unknown_host=ON,是容许未知节点进行 TCP/IP 连接或者是数据库的改写操作,这一点是需要注意的。

显然 iFIX 的网络安全机制是十分有限的,一个恶意的用户在 NODE04 可以将自己改名为 NODEO1 就可以取得 SCADA01 节点的信任。他若有操作系统文件的访问权限，如属于同一个 WinNT 域或者利用 WINDOWS 系统漏洞，就可以通过远程修改 SCADA01 节点的 NETWORK.INI,获得修改 SCADA01 数据库的权限，甚至可以直接覆盖数据库文件 DATABASE.PDB,从而直接控制机器设备的运行。在网络安全方面，应该使用操作系统的安全来为应用软件的安全提供保障。

3 iFIX 工业控制网络的三层安全模型

有鉴于 iFIX 安全域机制的可用性和网络通信安全的某些缺陷,我们根据江西德兴铜矿 iFIX 工业控制信息系统的实践，提出一个安全高效的解决方案。图 3 表示了这个三层模型。

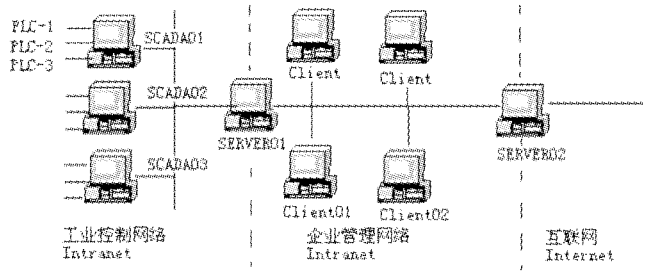

图 3 iFIX 网络的三层模型

企业内部网络分为工业控制网络和企业管理网络。工业控制网络为第一个层次,禁止非授权计算机随意接入。所有 SCADA 节点帐户采用与 WinNT 帐户同步,分系统管理员,系统操作人员,数据录入人员和一般用户，对 NTFS 文件系统访问控制列表进行权限设定,对 iFIX 对象进行安全域的设定。登录 iFIX 时候登录到 WinNT SERVER01 域服务器，可以限制 NT 域外计算机对域内资源的访问。SCADA 节点画面设定相应的安全域，用 VBA 和自带的 OLE 控件对用户进行限制访问,限制一般用户退出 iFIX 运行态而进入操作系统。删除系统目录下的 HELP 目录,解决输入法系统漏洞。由于 Windows NT 对工业软件有着普遍的兼容性能，而且安全可靠，所以工控网络上普遍采用 NT+SP6。工控网上的计算机的安全性由 WinNT 域服务器 SERVER01 提供保障。工业控制网通过 SERVER01 与企业管理网相联。SERVER01 采用双网卡,且禁止 IP 转发，防止外部用户直接进入工业控制网络。SERVERO1 采用 NT4 + SP6 + IIS + iFIX2.6 + i-WebServer ，它一方面负责实时数据的采集处理保存,一方面负责实时数据和历史数据的 Internet 发布。工业控制网络上有权限用户可以查看和修改现场中的实时信息。企业管理网是第二个层次,只有通过 SER-

(下转第 44 页)

彼此合作共享一个 CPU。整个程序本质上就是一个无限循环，每个任务在条件满足的时候才得以执行，否则自我放弃 CPU 的控制权，以便其它就绪的任务得以执行。程序流程图如图 3 所示，程序初始化操作后，打开一个 TCP 端口，和微机建立连接，接收微机发送的数据；如果没有收到数据，则程序转入控制模块，收到数据，就对数据进行解析并加以判断，如果是控制算法，则修改当前的执行机构动作表，如果是其它类型的数据（例如现场数据发送请求等），则根据事先指定的协议执行相应的操作，然后控制器程序进入控制模块，采集现场的数据并进行相应的控制操作，最后，程序进入下一个循环状态。

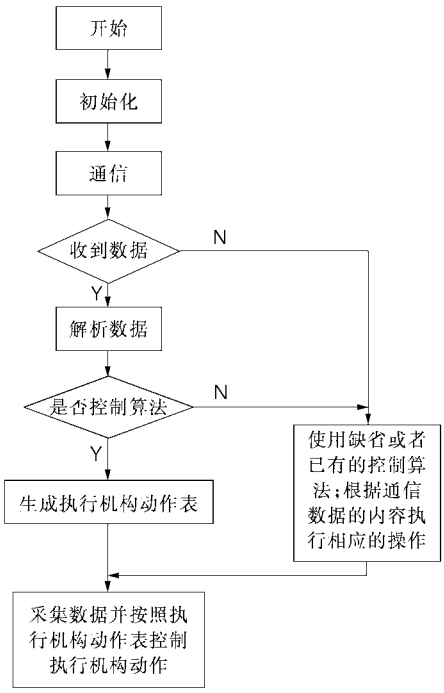

图 3 嵌入式控制器程序流程图

3.3 本系统的特点及存在的问题

本系统采用以太网为通信网络，在计算机端生成系统的控制算法，因此具有较强的灵活性，可以满足不同温室的控制要求。但是，系统还存在一些问题。例如，基于安全性的考虑，没有提供接入因特网的功能，因此不能充分体现以太网作为控制网络的优势。

4 结束语

基于以太网技术构建的通信网络平台，可以广泛应用在各种现场测控网络通信中，具有广阔的应用前景。本文详细说明了组建基于以太网的网络测控系统的方法。类似的系统还可以应用于工业过程控制、桥路收费系统监控、楼宇的智能化监控以及家庭自动化等领域。

参考文献

1 徐皑冬，王宏，杨志家.基于以太网的工业控制网络.信息与控制，2000(4)
2 Geoffrey R.Hendrey Standard Ethernet as an Embedded Communication Network,Project Report for the Degree of Master of Science,April 26,1999
3 Joe Kerkes,real –time Ethernet,Embedded Systems Programming,Feb 26,2001
4 李平.基于 TCP/IP 的多媒体教室系统应用层协议的建立.绍兴文理学院学报，2001(3)

[收稿日期：2002.9.6]

（上接第 28 页）

VER01 上的 iWebServer 才能查看工业实时数据，由于安全性、网络同步和网络延迟等问题，企业管理网上一般不授予工业数据修改的权限。企业管理网上可以利用实时数据进行二次开发。SERVER02 提供 IP 转发的服务，是企业与 Internet 的桥梁，利用防火墙进行 IP 限制和包过滤，为企业管理网提供安全服务。第三个层次为 Internet，访问安全性由 SERVERO1 与 SERVER02 共同完成。HTTP 访问安全性由 IIS(Internet Information System) 的安全性能提供保障。Internet 上用户只有进行登录后才能访问工业数据。

根据不同的实际需求，三层模型结构也可以进行扩展和延伸，例如：增加第三方认证机构，增加故障自动恢复节点，增加数据库服务器等。

4 结束语

本文提出了基于 iFIX 工控网络的三层安全模型。具有符合工业安全要求、实时数据通畅可靠、可扩展性好、部署方便等特点，实际应用中取得了良好的效果。同时，我们认识到，在 iFIX 安全与操作系统安全关系上，还有待更深层次的整合，以使 iFIX 网络通信更可靠、使用更加方便。

参考文献

1 Intellution(中国).iFIX 中文 2.6 版电子文档，2001
2 Intellution (中国).iFIX 在城市输配管网监测控制中的应用，2001
3 Intellution(中国).iFIX 在天津泰达污水处理厂监控系统中的应用，2002
4 北京递杰科进技术开发有限公司.iFIX 软件船舶监控系统，2001

[收稿日期：2002.8.28]