工业控制系统信息安全性分析

Analysis of Information Security for Industrial Control System

彭　杰　刘　力

(南昌大学信息工程学院,江西 南昌　330031)

摘　要:工控系统越来越容易受到信息安全问题的威胁,如计算机病毒、网络病毒、数据操纵,这些威胁会对整个工控系统造成破坏。分析了工控系统信息安全问题及其对控制性能和控制功能的破坏,指出了工业控制系统仍存在的潜在脆弱点,并提出了相应的对策。这些对策包括裁减操作系统、工控用分布式防火墙技术应用以及工控系统安全风险评估。对工业控制系统的信息安全性进行分析,将有助于信息技术在工业控制系统中的应用。

关键词:工业控制　信息安全　安全对策　风险评估　控制网络

中图分类号:TP393　　**文献标志码**:A

Abstract: The industrial control system is increasingly easy to be threatened by information security issues such as computer or network viruses, and data manipulation which may destroy entire control system. The information security of industrial control system and its influence on control performance and functions are analyzed. Other potential vulnerabilities existing in industrial control system are also proposed, and corresponding countermeasures are given. These measures include tailoring the operating system, applying distributed firewall technology for industrial control, and assessing the safety risk for industrial control system. The analysis of information security for industrial control system is helpful to the application of information technology in industrial control system.

Keywords: Industrial control　Information security　Safety countermeasures　Risk assessment　Control network

0　引言

随着 IT 技术快速而广泛地应用于工业自动化系统,工业控制系统遭受网络侵袭已屡见不鲜。工业网络的信息安全问题日益突出,这主要有以下三方面的原因:一是工业控制系统和企业 IT 系统联合得越来越紧密;二是企业 IT 安全措施往往不能直接应用于工业控制系统;三是黑客技术的发展也使蠕虫病毒的破坏力更大。随着以工业以太网为代表的控制网络在监控层占据主流位置,以及实时以太网技术在现场设备层逐步得到应用,对工业控制系统的信息安全风险进行分析研究已经显得十分迫切[1-2]。

1　系统网络化和技术主流化

1.1　“一网到底”

如今的工厂已不再由一系列自动化孤岛组成,为了有效利用自动化资源,通信系统已将其中的各部分连接起来。综合考虑企业范围内的各种需求,工厂网络通信框架一般具有 3 层结构,从低到高分别为现场控制层、监控层和企业管理层。对于监控层,工业以太网技术占据了主流地位,但是对于响应时间要求小于 5 ms 的现场控制层应用,工业以太网也不能胜任。为了满足高实时性能应用的需要,各大公司和标准组织纷纷提出各种提升工业以太网实时性的技术解决方案。这些方案建立在 IEEE 802.3 标准的基础上,通过对其及相关标准的实时扩展提高实时性,并且做到与标准以太网的无缝连接,这就是实时以太网[3-4]。随着实时以太网技术的发展和应用,工控系统逐渐实现“一网到底”。典型的工业网络结构如图 1 所示。

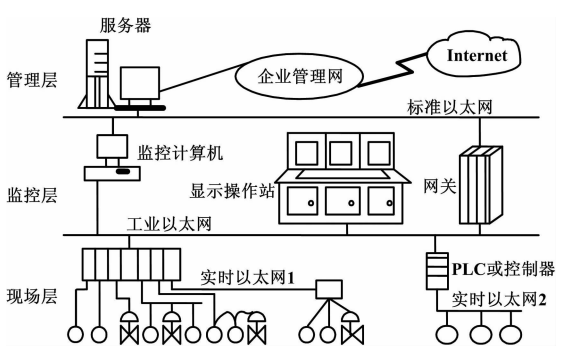

图 1　典型工业网络

Fig. 1　Typical industrial network

1.2　主流信息技术应用

在自动化监控层,不但有用于控制的 PLC 和中央

修改稿收到日期:2012-05-17。

第一作者彭杰(1976-),男,2004 年毕业于上海理工大学热能工程专业,获博士学位,副教授;主要从事控制网络等方面的研究 。

控制器,也有以 Windows 为主流操作系统的操作站、优化系统工作站、先进控制工作站以及 Web 服务器和数据库服务器等设备。系统使用 OPC 技术从不同的数据源得到数据并进行数据交换;数据经常通过工业以太网交换机进行传输等。自动化系统集成和扩展的需要、系统开放互连性的加强,特别是标准 IT 技术在自动化系统组件中的广泛应用,如 FTP 应用、B/S 方式监控、Internet 远程诊断、来自工业现场的视频音频监控数据传输,以及以后有可能实现的 IPv6 在工业控制设备中的应用等,这些都明显体现了工业控制系统作为一个全方位采用主流信息技术的系统特征。

2　工控系统信息安全威胁

工业控制系统所具有的网络化和信息化的特点,使得工控系统除了面对传统的针对商用计算机领域的信息安全威胁,例如病毒、网络安全等以外,还要面对那些会威胁到系统控制性能甚至破坏系统控制功能的信息安全威胁[5-7]。

2.1　对控制性能的威胁

典型的对控制性能的威胁就是控制系统的通信实时性。以在监控层占据主流地位的工业以太网为例。网络响应时间反映了整个工业以太网系统的实时性能。影响网络响应时间的因素主要来自 3 个方面:①本地系统,即源节点的处理;②工业以太网网络,即传输部分;③目的节点系统,即目的节点的处理。

工业以太网响应时间示意图如图 2 所示。此图表明了从源节点向目的节点发送信息所花费的时间,也就是网络响应时间 T_{delay}。总的时间延迟可分为:源节点的时间延迟、网络通道上的时间延迟和目标节点的时间延迟 3 个部分。

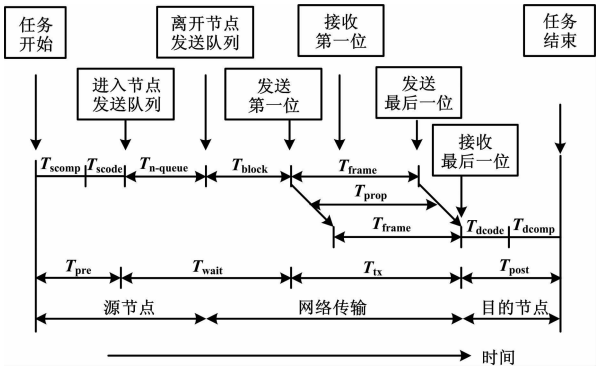

图 2　工业以太网响应时间示意图

Fig. 2　Schematic diagram of response time of industrial Ethernet

源节点的时间延迟包括:①预处理时间 T_{pre},它是计算时间 T_{scomp} 和编码时间 T_{scode} 的总和;②节点内部排队的时间 $T_{n\text{-}queue}$,是等待时间 T_{wait} 的一部分,取决于源节点需传送数据的总和与网络的传送状况。网络时间延迟包括:①传送时间 T_{tx},它是帧发送时间 T_{frame} 和网络的物理传播迟延 T_{prop} 的总和,取决于信息的大小、数据传送率和网络缆线的长度;②网络阻塞时间 T_{block},它是等待时间 T_{wait} 的另外一部分;③目的节点的时间延迟 T_{post} 是数据的后期处理时间,它是目的节点解码时间 T_{dcode} 和目的节点计算时间 T_{dcomp} 的总和。所以总的时间延迟可表示为:

$$\begin{aligned} T_{delay} &= T_{pre} + T_{wait} + T_{tx} + T_{post} = \\ &T_{scomp} + T_{scode} + T_{n\text{-}queue} + T_{block} + \\ &T_{frame} + T_{prop} + T_{dcode} + T_{dcomp} = \\ &T_{pre} + T_{wait} + T_{tx} + T_{post} \end{aligned} \tag{1}$$

式中:$T_{pre} = T_{scomp} + T_{scode}$;$T_{wait} = T_{n\text{-}quene} + T_{block}$;$T_{tx} = T_{frame} + T_{prop}$;$T_{post} = T_{dcode} + T_{dcomp}$。

从图 2 可知,计算机病毒即使不造成操作系统崩溃,也可以通过占用资源,使得源节点的时间延迟和目的节点的时间延迟具有不确定性;局域网病毒或者网络攻击即使不造成以太网瘫痪,也可以通过堵塞造成网络传输的时间延迟具有不确定性。这些不确定性将造成那些具有优先权的工业实时数据的实时性得不到满足,从而破坏系统控制性能。

2.2　对控制功能的破坏

典型的对控制功能的破坏就是破坏和操纵工业控制软件,例如对 OPC 软件或者实时数据库的破坏,但破坏力更强的是对工控软件的操纵。

国家计算机病毒应急处理中心于 2010 年 10 月 3 日发布信息:通过互联网络监测发现,一种利用微软公司漏洞的新型病毒“震网”(也称超级病毒 Stuxnet)出现,提醒用户尤其是大型工业部门小心谨防。该病毒可以通过移动存储介质和局域网进行传播,并且利用西门子公司控制系统(SIMATIC WinCC/Step7)存在的漏洞感染数据采集与监视控制系统(SCADA)。Stuxnet 的目的是通过修改 PLC 来改变工业生产控制系统的行为,包括:拦截发送给 PLC 的读/写请求,以此判断系统是否为潜在的攻击目标;修改现有的 PLC 代码块,并往 PLC 中写入新的代码块;利用 Rootkit 功能隐藏 PLC 感染,躲避 PLC 管理员或程序员的检测。

Step7 软件使用库文件 s7otbxdx. dll 来和 PLC 通信。当 Step7 程序准备进入 PLC 时,它会调用该 DLL 文件中不同的例程。例如,如果一个代码块需要用 Step7 从 PLC 中读出,那么,例程 s7blk_read 就会被调用。s7otbxdx. dll 中的代码会进入 PLC,读出其中的代码,并将它传回 Step7 程序。Stuxnet 运行后,Stuxnet 会

将原始的 s7otbxdx. dll 文件重命名为 s7otbxsx. dll。然后,它将用自身取代原始的 DLL 文件,这样 Stuxnet 就可以拦截任何来自其他程序的访问 PLC 的命令。被 Stuxnet 修改后的 s7otbxdx. dll 文件保留了原来的导出表,导出函数为 109 个,这就使得 Stuxnet 可以应付所有相同的请求。大部分导出命令会转发给真正的 DLL,即重命名后的 s7otbxsx. dll,剩下的 16 种导出命令不会被简单地转发,而是被改动后的 DLL 拦截。被拦截的导出命令为在 PLC 中读、写、定位代码块的例程。通过拦截这些请求,Stuxnet 可以在 PLC 管理员没有察觉的情况下,修改发送至 PLC 或从 PLC 返回的数据。同时,通过利用这些例程,Stuxnet 可以将恶意代码隐藏在 PLC 中。

通过初步分析,确认 Stuxnet 病毒主要存在以下安全威胁:①该病毒针对的目标是用于数据采集与监视控制的专用计算机系统;②此类数据采集与监视控制系统由于其自身功能的特殊性和重要性,往往与互联网隔离,造成无法及时进行安全更新,为病毒传播提供可乘之机;③虽然目前该病毒只是针对西门子公司的数据采集与监视控制系统,但不排除可能出现针对其他专用计算机系统的变种。

2.3　潜在的脆弱点

工业控制系统还存在潜在的脆弱点,这些脆弱点虽然可能还没有立即对控制功能或者控制软件造成损害,但显然增加了系统的安全性威胁。这些潜在的脆弱点包括:①工业控制系统中采用的主流操作系统,如 Microsoft Windows 操作系统存在的安全脆弱点,最近的 Microsoft 远程桌面协议拒绝访问和远程代码执行漏洞;②缓冲区溢出漏洞,例如 ABB 公司就确认在其机器人通信运行软件中存在这类漏洞,通过这个漏洞,攻击者可能具有管理员权限执行远程代码;③控制装置认证机制中存在的脆弱点,例如,西门子公司已经确认在编程和配置客户端软件认证机制中存在潜在的安全弱点。这些机制使用在西门子公司的 SIMATIC S7 PLC 上,其中包括 S7-200、S7-300、S7-400 和 S7-1200。通过这些脆弱点,攻击者有机会接入控制系统的通信链路,截获并破译产品的密码,导致未经授权的更改操作。

3　工控系统信息安全策略

商用系统的信息安全威胁和安全防护一直是矛盾的关系,是动态发展的问题,而基于主流信息技术的发展应用和改造应用的工控系统对此问题的解决显然也是动态的,所以不可能有一成不变的解决方案。因此,应该制定合理的信息安全策略,然后选择可行的防护技术。限于篇幅,本文对此进行初步探讨。

3.1　裁减操纵系统

Stuxnet 蠕虫病毒是利用 Windows 系统和西门子 SIMATIC WinCC 系统的多个漏洞进行攻击。它一共利用了 5 个微软漏洞,其中 4 个在此前均已得到微软官方修复。2010 年 12 月 15 日,微软发布修复的“Windows 计划任务本地权限提升漏洞”(公告编号:MS10-092),是被“超级工厂”病毒利用的最后一个 Windows0day 漏洞。随着第 5 个漏洞的修复,Stuxnet “超级工厂”病毒的危害已经得到解决。但由于操作系统自身存在许多安全漏洞,运行在该系统上的工业软件难免会受到威胁,所以最好能根据应用情况,裁减操纵系统。

3.2　防火墙技术

在主流的分布式防火墙技术基础上,开发和应用适合工控的分布式防火墙技术如图 3 所示。

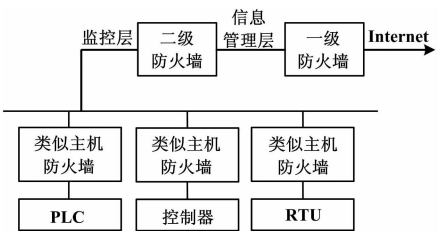

图 3　工控用分布式防火墙

Fig. 3　The distributed firewall for industrial control

与传统边界防火墙相比,分布式防火墙克服了许多传统边界防火墙的缺点,增加了一种用于对内部子网之间的安全防护层;可以针对各个服务对象的不同需要,进行不同配置,配置时能够充分考虑到运行的应用;网络处理负荷分布,克服了传统防火墙因网络规模增大而不堪重负的弊端。

信息网络分布式防火墙的主机防火墙驻留在主机中,负责策略的实施,以及对网络中的服务器和桌面机进行防护。主机防火墙驻留在被保护的主机上,可以针对该主机上运行的具体应用和对外提供的服务来设定针对性很强的安全策略。正如在主流信息网络技术基础上进行适应工业控制特点的改造,这使得现场总线和实时以太网技术一样,可以对应地开发用于工控的类似主机防火墙。两者的不同仅在于这些类似主机防火墙的保护对象是控制器、PLC 和 RTU 等执行控制策略的“主机”。

3.3　信息安全风险评估

对系统的信息安全风险评估有利于采取有针对性

的安全策略,制定事故处理方案。这对类似 Stuxnet 这样破坏控制功能的安全威胁尤其有意义。

目前,国内外关于 IT 系统风险评估的方法有许多种,例如基于概率论方法、层次分析法和模糊逻辑方法。虽然工控系统是一个信息系统,但它更是一个控制系统,这使其在采用风险评估方法中要着重注意保证控制系统正常运行特有的要求。这就使得对工业控制系统的风险评估,要在商用信息系统已经较为成熟的系统风险评估方法和工具应用的基础上,结合控制系统风险特征,例如工业以太网的实时性要求。由于控制系统引发的后果比较严重,所以对风险事件发生后果的影响评价需要更为"保守"。同时,根据技术发展探讨其他可行的策略,例如 VPN、SSL 技术等,许多文献对此已经有诸多研究。

4　结束语

当前工业控制系统与基于 TCP/IP 协议的信息系统已结合得越来越紧密,这使得工控系统容易受到信息安全问题的威胁,例如计算机病毒、网络病毒、数据操纵,从而使整个工业控制系统遭受破坏。

本文针对工业控制系统网络化和信息化的特点,对工业控制系统信息安全问题进行了分析;对威胁到系统控制性能甚至破坏控制功能的信息安全威胁进行了研究;同时指出了工业控制系统还存在的潜在脆弱点,并提出了相应的对策。这些对策包括根据工业控制系统要求来裁减操作系统、研究工控用分布式防火墙技术应用以及进行工控系统安全风险评估。

参考文献

[1] 施晓秋. 计算机网络技术[M]. 北京:高等教育出版社,2006:10 - 189.

[2] 韩东海. 入侵检测系统及实例剖析[M]. 北京:清华大学出版社,2002:18 - 266.

[3] 彭杰,应启戛. 工业以太网的安全性研究[J]. 仪器仪表学报,2004(1):222 - 223.

[4] 康军,戴冠中. 工业以太网控制系统安全性问题研究[J]. 信息与控制,2007,36(2):245 - 249.

[5] Ioannidis S,Keromytis A D,Bellovin S M. Implementing a distributed firewall [C]//Proceedings of Conference on Computer and Communication Security,Athens,Greece,2000:190 - 199.

[6] Miltchev S,Smith J M,Prevelakis V. Decentralized access control in distributed file systems [J]. ACM Computing Surveys, 2008, 40(3):1 - 30.

[7] Burnside M,Keromytis A. Asynchronous policy evaluation and enforcement [C]//Proceedings of the 2nd Computer Security Architecture Workshop (CSAW),Fairfax,VA,2008:5 - 50.

(上接第 35 页)

```
……
void Sreial_int (void) interrupt 5 using 1
                                    //串口数据接收中断程序
{   ……
    i = Receive_data( ); j = 0;
    if (i = =0xD7)      //判断接收的数据是否为包头
    { for (udl_num = Receive_data( );udl > 1;udl - - )
                    //如果为包头,则继续接收后面的数据
        { save_data[j] = Receive_data( );
                    //包括控制字节、电话号码、有效数据
        j + + ;
        } return;
    }
}
```

4　结束语

基于 GSM 模块的远程监控系统现已在多部移动电站上得到了实际应用,用户可通过手机在任何时间、任何地点查询指定编号移动电站的当前运行状态信息,同时也能够在第一时间掌握电站警报情况,甚至可以远程控制移动电站启动/停机,使用效果达到了预期目标。在实际应用中也发现了一些问题,如网络信号较差时,短信收发延时情况较为明显。相信通过 GSM 模块无线发射功率的增强,以及无线网络通信基站覆盖范围的不断加大,这些问题均能得到很大改善。

参考文献

[1] 陈琦,丁天怀, 李成,等. 基于GPRS/GSM 的低功耗无线远程测控终端设计[J]. 清华大学学报:自然科学版,2009,49(2):223 - 225.

[2] 胡金凤,郑萍,吴拥,等. 基于 GSM 的 PLC 车载远程控制系统设计[J]. 自动化仪表,2011,32(4):36 - 39.

[3] 邢娅浪,赵锦成,尹志勇. 基于 W77E58 的电站装备运行记录仪的设计[J]. 移动电源与车辆,2008(2):17 - 19.

[4] 尹志勇,刘洪文,刘金宁. 基于 PM50 语音芯片的电站远程语音提示系统[J]. 移动电源与车辆,2009(2):7 - 10.

[5] 邢娅浪,赵锦成,孙世宇. 基于 STC 系列单片机的 SPWM 波形实现[J]. 国外电子测量技术,2009(12):51 - 53.

[6] 邵天章,谷志峰,尹志勇,等. 移动电站通用控制系统设计[J]. 移动电源与车辆,2009(4):21 - 23.

[7] 马忠梅. 单片机 C 语言应用程序设计[M]. 北京:北京航空航天大学出版社,2003:158 - 164.

[8] 马玉春,孙冰,王建明. GSM 模块的综合应用研究[J]. 计算机应用与软件,2008,25(2):68 - 70.