重中之重:工业控制系统安全的盛世危言

褚 健

浙江大学智能系统与控制研究所,杭州 310027

工业控制系统是国家重要基础设施(如电厂、电网、炼油厂、油气管道、化工厂、城市交通、铁路、船舶、国防等)的“大脑”和“中枢神经”。控制系统一旦崩溃,后果不堪设想。工业控制系统安全已成为安全领域的重中之重。

1　威胁步步逼近

美国电影《虎胆龙威》里面有几个跟控制系统有关的片段:一个是恐怖分子通过接管航空控制信号,劫持并控制了一架战斗机;另一个是恐怖分子控制了城市的信号交通系统,使红绿灯失去作用,整个城市的交通基本瘫痪。电影里被操控的,其实就是工业控制系统。电影拍摄于很多年前,那个时候还有一定的科幻成分,实施起来的可能性比较小,现在来看完全有可能发生,不法分子通过操控工业控制系统来破坏一个城市、一个区域甚至一个国家,是非常容易的,这就是我们当前所面临的问题。

伊朗发生的“震网”(Stuxnet)事件,促使大家开始重视工业控制系统安全。它通过操控应用于铀浓缩离心机和发电汽轮机上的西门子控制系统,将离心机线速度从 1225km/h 提高到 1620km/h,导致约 20%的离心机(2000 多台)失控、直到报废,并使布什尔核电站一再推迟发电计划。科幻电影的情节正在变成现实。

严格来讲,Stuxnet 不是传统意义上的病毒,而是世界上首个专门针对真实世界控制系统的破坏性恶意代码,又叫“超级导弹”、“定向网络武器”,通过操控控制系统,以摧毁设备、甚至引起爆炸。

“震网”具有非常强的针对性,虽然它感染并存在于很多计算机上,但是它只针对伊朗的铀浓缩离心机和核电站。

“震网”还具有非常强的专业性和欺骗性,其开发人员具有丰富的控制系统专业知识,它利用了控制系统软件、硬件漏洞,篡改工业基础设施运行参数,向现场执行机构发送破坏指令,但同时向中央控制室发送“正常”的监视数据,一方面破坏工业基础设施,另一方面却能让操作人员察觉不出。

随着互联网和信息技术的大量应用,工业企业的管理和信息化水平也越来越高,几乎所有的流程工业、制造业企业都直接或间接地连上了互联网。从网络层次上看,一般工业企业的网络由两大部分组成:控制网和企业管理网。企业管理网一般通过防火墙直接跟互联网相连,而控制网一般通过防火墙、网闸等加密设备连接到企业管理网上,但防火墙对一般的病毒或者是黑客可能会有效,对真正的专业人士不一定会有作用。大量企业都逐步应用了 ERP(Enterprise Resource Planning)系统,为了提高经济效益,必须实时通过控制系统了解生产信息,因此断掉网络连接是不可能的。

以 Stuxnet 为例,它首先是散布到互联网,感染计算机和 U 盘,通过这些介质带入到企业内部,传染给控制系统网络;其次,找到西门子控制系统软件“WinCC”后,利用其漏洞,替换原有 S7otbxdx.dll 文件;然后,借助 WinCC 软件,向西门子控制器 PLC 注入恶意控制程序;最后,通过恶意程序利用 PLC 的漏洞向离心机发送破坏控制指令,使其超速,同时向控制室发送欺骗性的“正常”数据。所以,操作员看到屏幕上数据正常,但实际上离心机的运作已经被破坏了。

实际上,Stuxnet 是利用了传统计算机病毒传播方法进行传播,利用控制系统的漏洞使“软件炸弹”得以定点攻击,实现恶意操控,从而实现对基础设施的破坏。类似的这种事件其实很多,以前不知道是何原因引起的,但是有很多案例可以说明,此类事件的发生受到黑客攻击或者其他攻击的可能性比较大。

2　必须承受之重

工业控制系统的应用领域很广,从原油生产、运输到各种燃料、有机材料及其他材料的加工,从矿石开采到五金、稀土材料的生产,到飞机、汽车、生活用品、机械装备等的制造,不管是流程工业还是离散制造业,都要用到工业控制系统。以前工业控制系统主要是国外的产品,现在国内有中控、和利时为代表的自主产品,应用得也非常好。

本文转载自《中国信息安全》2012 年第 3 期,是褚健教授在“工信部中央企业工业控制系统信息安全培训会”上的发言,由《中国信息安全》记者袁胜整理,标题为《中国信息安全》编辑部所加。

作者简介:褚健,教授,研究方向为自动化与仪器仪表、机器人技术,电子信箱:chuj@csc.zju.edu.cn

流程工业对控制系统的安全性和可靠性要求非常高,例如石油化工过程,特点为危险、高耗能、连续运行,是高温高压、易燃易爆、化学反应复杂的过程,安全等级要求极高,要求365天连续24小时运行,甚至10年以上。通常控制系统的生命周期为10—15年,甚至是更长时间,所以对控制系统的可靠性要求极高,不能出一丝一毫的差错。工业控制系统也应用在炼油、石化、电力、冶金、建材、交通、电网、水网、气网、国防等重要领域,这些领域牵涉到国家和社会稳定、经济正常运行,工业控制系统安全就显得尤为重要。

3　有别于传统信息安全

工业控制系统(Industrial Control System,ICS)是一个总称,大到工业生产,小到家庭生活,各种装置都运用了工业控制技术,只是控制规模不同。

工业控制系统一般是由现场设备、控制器、网络和车间监控以及企业监控几部分构成。最初的控制系统不存在任何网络安全问题,因为它是孤立的,只有单回路,没有网络,没有通信,因此是安全的。随着技术不断发展,从20世纪70—80年代开始,工业控制系统使用专有的网络、专有的操作系统,但是没有与以太网和互联网的连接,所以也不存在网络安全的问题。现在以太网、无线设备无处不在,整个控制系统都可以和远程终端进行互联,操作系统用的也大都是通用的操作系统,如Windows和Linux,所以网络安全问题就直接延伸到工业控制系统。一般越大型的工业企业,其控制系统与互联网连接就越紧密,从这个角度来讲,它的控制系统也越脆弱。

工业控制系统与IT系统有一些类似,但是更主要的是差别。IT系统的特点,简单来说是高吞吐量、标准统一的通信协议,设备部署在本地,易于访问,设备生命周期为3—5年。工业控制系统的特点是实时性通信,系统不允许重启,不允许随意更新、打补丁,通信协议多种多样,设备不易访问,设备生命周期为15—20年。为保证操作人员和装备安全,在进行工程实施和安全检查时,不能影响控制系统运行的稳定、可靠与安全。

从性质上看,把Stuxnet病毒叫做"软件炸弹"或者是"超级导弹"更明确,Stuxnet已经不是一般意义的计算机病毒,它不以窃取信息为目的,就是要破坏系统。它可以通过外网输入,也可以事先预埋在系统里,向重要基础设施发布破坏指令,所以称之为"软件炸弹"。"软件炸弹"的主要特点是攻击目标针对性强、能实现"定点"精确攻击。它的隐蔽性很强,平时不破坏装备、不破坏数据、不窃取数据,查毒"查不出"、杀毒"杀不到",难以被"追踪",对于非目标计算机,即使被感染,也不发起攻击。受到触发时,它通过正常网络途径,改变控制指令、改变攻击目标,其破坏性大,造成基础设施失灵、自毁等灾难事故。制造"软件炸弹"需要高技术含量,对恶意软件、工业安全以及特定型号和配置的工业设备十分了解。

所以工业控制系统安全防范有两个方面:一个是网络安全,包括计算机病毒、蠕虫、木马等,另一个就是控制系统安全,也就是"超级导弹"、"软件炸弹"、"定向网络武器"等,这一块以前没有意识到,很少被重视。工业控制系统安全是IT技术延伸必然的结果,需要计算机专家、网络专家、自动化专家联合应对。

4　主要风险漏洞

工业控制系统可能遭到攻击的来源主要有4个方面。一个是黑客,其次是来自于业内人士为了报复而破坏,有时可能是个意外,这种情况也防不胜防。最主要的攻击还是来自恐怖分子和敌对国家,这个威胁一直存在,而且现在防范的意识并不强。

入侵工业控制系统的途径,可以通过办公网络、互联网或者是虚拟的专网、拨号连接、"可信"的第三方连接、无线网络、公共通信设施等。如果现场设备不接入任何网络,是一个"孤岛"的状态,仍有可能受到通过可移动存储和接入设备所传播的恶意软件的攻击。

控制系统恶意代码加上传统病毒途径传播,是工业控制系统被入侵的一般过程。假设一个黑客来攻击工业控制系统,他可以通过互联网渗透到企业网络,然后再到监控网络、现场网络,把恶意的代码带到执行机构上。

恶意的代码要想实现其功能,就要看控制系统是否存在相关的漏洞。控制系统里面的漏洞,特别是硬件和嵌入式软件所存在的漏洞很少有人去分析。控制系统一般与外界隔离,系统软、硬件错误和漏洞不为外人所知,它的数据流、信息流、业务流及其处理流程,普通用户也无法理解和获知。编写控制系统软件和通用软件完全不一样,除非有些系统要按安全系统的标准规范来编写,其他只要功能实现就可以,没有人去关心、也不清楚里面有没有漏洞。只有熟知控制系统各功能块原理、控制方案、数据流程、组态软件等的参与者,才可能发现和利用漏洞。如前面所提的Stuxnet病毒的制造过程,可能就有对相关系统非常熟悉的人参与。

工业控制系统潜在的管理与程序漏洞有很多,如系统本身缺乏安全架构和设计,没有具体或者书面的安全程序,没有存在缺陷工业控制系统设备的安全实施准则,缺乏对行政执法的安全机制,很少有工业控制系统安全审核,没有工业控制系统安全事故与灾难恢复机制与计划,以及缺乏工业控制系统的具体配置变更管理。

实际上还存在潜在的芯片与硬件漏洞。芯片漏洞,主要是指CPU的指令不知道是否存在漏洞,寄存器、堆栈、接口与驱动也可能会有漏洞。在应用环境上,编译软件安全性未经验证,目标码烧录软件安全性未经验证,嵌入式实时操作系统安全性未经验证,都会产生安全风险。

操作站、工程师站软件、嵌入式软件这实际运行的三大系统里,也存在各种各样的安全风险,如安全功能没启用、拒绝服务攻击(DOS)、OPC安全,使用不安全的工控协议、不需

要的服务运行、安全日志与安全事故并不检测、未经保护的文件存储、未经认证和访问控制的配置和编程软件,担心影响控制系统的正常、可靠、稳定运行,从而不安装杀毒软件、不更新操作系统——这些都可能带来安全问题。

在工业通信网络里,也存在一些漏洞。工业通信的实时通信网络不同于互联网,它有自己专用的、多样的现场总线,但它的网络体系结构没有考虑安全性,没有安全验证、认证机制,加解密机制基本不用,安全设备配置不当,密码基本不用或不予关注,访问控制应用不足。总体来说安全性能堪忧。

5　当务之急

首先必须尽快建立工业控制系统安防评估与认证的体系,这个建立起来比较难,目前还没有相关的标准。其次是对工业控制系统进行专业化的漏洞检测工作,但切不可影响控制系统的稳定、可靠与安全运行,否则就容易引起不必要的灾难事故。第三是加快研发工业控制系统安防的技术和产品。

中国现在应用了大量国外的工业控制系统产品,不可能、也没必要换掉这些系统,但防护的意识和措施是要有的,我们可以在重要的基础设施上率先采取一定的防护手段。从长远起见,建议多采用国产的工业控制系统。国产系统在性能上绝不亚于国外的产品,而且安全上更有保障。传统信息安全领域和工业自动化领域需要进行更多的交流与合作,积极主动地来保护中国的工业控制系统,特别是重要基础设施的工业控制系统,为整个国家的国计民生保驾护航。

·学术动态·

“第六届全国水力学及水利信息学大会”征文

“第六届全国水力学及水利信息学大会”将于 2013 年 6 月 8–10 日在北京召开,本次大会由 IAHR 中国分会、水力学专委会和水工水力学专委会主办。

征稿范围:工程水力学(水工水力学与工程安全,江河湖库水力学,冰工程和冷却水水力学,防洪工程与洪水管理,水工模型与仪器);环境与生态水力学(环境与生态水力学,水利水电工程建设与生态环境,城市、河湖水环境及其生态修复,海岸水质、环境与海岸保护修复,雨洪、污水、苦咸水资源化);水利信息学的新进展(数值模拟与仿真技术,复合模型(原观、物模、数模)技术研究,智能算法及其应用,水信息的新兴技术及应用);河口、海岸及海洋工程与极端事件应对(波浪、潮汐及海岸水动力学,海洋新能源开发中的水力学问题,滩涂开发与湿地保护,极端事件与灾害应对中的水动力学问题)。

摘要截稿日期:2012 年 12 月 15 日。

联系电话:13811722697,010-68781126。

电子信箱:qssd2012@vip.163.com。

会议网址:http://www.difut.cn/clientys1/clientys1.asp?conference=C10010。