工控系统安全威胁分析及防护研究

王文宇，刘玉红
（中国软件与技术服务股份有限公司，北京 102200）

[摘 要] 随着信息化的推进，工控系统获得了前所未有的飞速发展。同时，工控系统所面临的安全威胁也越来越严峻。如何解决工控系统安全问题，是当前信息安全领域面临的重大挑战。文中在深入分析工控系统安全威胁的基础上，提出了以基础防护为根本，基于主控系统安全基线的增强防护方法。通过基础防护与增强防护相结合，为工控系统建立全面、系统的安全体系，彻底解除工控系统面临的内外部的威胁，从而为推动工业的信息化、现代化的稳定发展提供保障。

[关键词] 工控系统；基础防护；安全基线
[中图分类号] TP309.2 [文献标识码] A [文章编号] 1009-8054(2012)02-033-02

Analysis and Study of Defense against Security Risk for Industry Control System

WANG Wen-yu，LIU Yu-hong
(China Software and Service Corporation Ltd.，Beijing 102200，China)

[Abstract] With the promotion of-IT technology，the industry control system develops rapidly. Also，the system now faces more serious security risks. How to ensure the security of industry control system is a big challenge for information security. The security risks and protections of the system are analyzed and studied in detail. With fundamental protection as the essence，the enhanced protective method based on security baseline for main control system is proposed. By combining the fundamental protection and enhanced protection，the security system for industry control system is established，thus the inside and outside threats are relieved，and the industrialization and modernization of industry ensured.

[Keywords] industry control system；essential protection；security baseline

0 引言

随着信息化的推动和工业化进程的加速，计算机和网络技术越来越多地应用于工业控制系统，为工业生成带来极大推动的同时，也带来了工业控制系统（简称工控系统）安全性[1]的问题。据权威机构统计，截至2011年底，全球发生了200余起针对工控系统的攻击事件。

工控系统是现代工业基础设施的核心，包括过程控制、数据采集系统、分布式控制系统、程序逻辑控制以及其他控制系统等，广泛应用于核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关的领域，是国家关键基础设施的重要组成部分。

而工业控制系统的安全，更关系到国家的战略安全。如何保证工业控制系统的安全，已引起国家相关部门的高度重视。

2011年，工信部下发了《关于加强工业控制系统信息安全管理的通知》，要求各地区、各有关部门、有关国有大型企业充分认识工业控制系统信息安全的重要性和紧迫性，切实加强工业控制系统信息安全管理，以保障工业生产运行安全、国家经济安全和人民生命财产安全。

1 工控系统面临的安全威胁

信息化和自动化的推进，在为社会带来巨大进步的同时，也使得工控系统所面临的威胁与日俱增。

(1) 网络管理缺失

目前，互联网已成为人们信息交流与共享的核心部分。而接入互联网的用户，一方面有可能成为黑客攻击的重点目标；另一方面，在安全意识淡薄的氛围下，企业信息有可能被用户直接发布到网上。在工控系统中，网络管理的不完善也使得企业的安全面临巨大挑战，如网络间谍侵入企业内网，直接窃取涉密信息，或者植入病毒破坏系统；内部员工通过邮件发送给他人，或者直接发布到公网。

(2) 移动存储介质滥用

移动存储介质作为当前信息传播、交流的重要方式，

收稿日期：2012-01-05
作者简介：王文宇，1980年生，男，工程师，研究方向：网络安全、信息安全；刘玉红，1982年生，女，工程师，方向：网络安全、信息安全。

在为用户提供便捷的同时也给内部系统的安全带来威胁。一方面，可能由于用户个人安全意识淡薄，无意中将企业的涉密信息通过移动存储介质传播出去；另一方面，也有可能是用户所使用的设备感染病毒，信息被非法窃取或破坏。如摆渡木马[2]借助U盘在企业内外网之间传播，并在感染病毒的终端中窃取涉密信息，并通过网络将信息传播出去。

(3) 系统漏洞

工控系统中应用软件或操作系统软件在设计上的缺陷，极易被不法者利用，对系统进行恶意攻击、破坏。系统漏洞虽然可以通过更新系统补丁的方式加以弥补，但系统补丁更新具有一定的滞后性，同时，要对每个终端进行补丁更新，也具有很大的难度，这些因素都给不法分子留下可乘之机，也进一步加剧了工控系统的危险性。

计算机病毒、黑客行为、内部泄密、外部泄密、信息丢失、电子谍报、信息战等各种威胁因素，都给工控系统的安全带来了严峻挑战。目前针对工控系统的安全防护，多集中在传统的IT安全解决方案，如系统升级、病毒查杀等，但这些方案停留在单一的防护方面，具有一定的滞后性，而且没有形成一套完整的安全管理体系，不足以应对工业基础设施领域的全新安全需求。

如以Stuxnet为代表的蠕虫病毒，已给工控系统带来重大的灾难。Stuxnet病毒[3]通过U盘和局域网进行传播，专门针对西门子公司的SIMATIC WinCC监控与数据采集(SCADA)系统进行自毁性破坏。它通过对软件重新编程实施攻击，给机器编一个新程序或输入潜伏极大风险的指令。该病毒能控制关键过程并开启一连串执行程序，最终导致整个系统自我毁灭。Stuxnet蠕虫病毒是世界上第一个可直接破坏现实世界中工业基础设施的恶意代码，此病毒的爆发也让人们更加意识到工控系统安全的重要性。

2 工控系统安全防护

建立系统、健全的安全防护体系，是解除当前工控系统所面临的各种安全威胁的重中之重。文中以基础防护为根本，结合主控系统安全基线，对系统进行增强防护，彻底解决工控系统的安全问题，杜绝各种形式的泄密，防止系统被非法破坏。

2.1 工控系统基础防护方法

工控系统基础方法主要包括失泄密防护、主机安全管理、数据安全管理等。

(1) 失泄密防护

失泄密防护主要对工控系统进行网络控制、应用层控制及外设控制。对网络的控制，指禁用TCP、UDP、ICMP等端口或者在信任前提下允许有条件的使用。应用层控制，则集中在HTTP、FTP、TELNET、SMTP、NETBIOS以及即时通信工具的管理和控制上，如只允许工控系统中的终端访问指定的Web地址；只允许终端向指定的接收方发送数据。通过网络控制及应用层控制，可有效防止内部终端访问网络时被植入病毒，也可防止内部用户将资料传播给非法组织。

失泄密防护中，对外设进行严格的审核和控制，如MODEM、移动存储介质、CD ROM、辅助硬盘、打印机以及外设接口等。以移动存储介质为例，可控制其只读或者禁用，防止摆渡木马病毒窃取终端数据到移动存储介质中。

失泄密防护是工控系统基础防护中的基本防护。通过控制工控系统终端使用网络或外设的权限，达到安全的目的。

(2) 主机安全管理

主机安全管理主要是对工控系统中各分布终端进行统一化的控制。在工控系统中，其终端的数量可能很庞大，单单依靠终端用户的个人安全意识对系统进行防护，并不能切实保障整个系统的安全。主机安全管理对终端进行集中、统一化的管理，主要包括：

1) 系统账户的管理，如账户的密码设置需要通过安全性检查；账户的锁定限制在一定的时间内；是否可共享本终端数据给其他终端等。

2) 防病毒软件的监控和自动更新。

3) 文件的安全删除。

4) 系统补丁的监控和自动更新。

通过主机安全管理，实现了工控系统各分布终端的安全监控，保证终端系统用户的使用安全，同时又对系统进行实时升级，防止因系统漏洞给病毒留下可乘之机。

(3) 数据安全管理

数据安全管理是主要对数据进行加密保护和权限控制，是对工控系统内的核心资料的全面防护。经过加密的数据，即使被系统内部用户无意带走，离开了工控系统的安全域，其数据也无法访问。数据安全管理对于防止内部资料泄露具有得天独厚的优势，也是工控系统防护的重要组成部分。

2.2 基于主控系统安全基线的防护

工控系统基础防护方法可满足工控系统基本的安全防护，对保护工控系统具有重大的意义。同时，基础防护也需要进一步增强，以满足当前工控领域全新的安全需求。基于主控系统安全基线的防护，是工控系统安全的增强。通过此防护方法，一方面彻底杜绝以Stuxnet为代表的病毒攻击，另一方面，也可解除病毒新的变种对系统带来的威胁。

基于主控系统基线的防护，主要包括基线建立、运

行监控、实施防御，如图 1 所示。

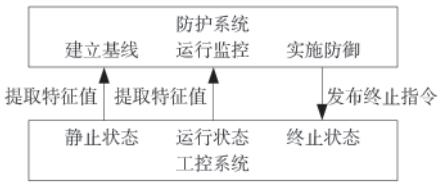

图 1 基于主控系统基线的防护

(1) 基线建立

基线建立是防护的先决条件。在主控系统中，先建立单一的工作环境，该环境未受到任何病毒的感染或疑似威胁的干扰。在此基础上，从环境中提取工控系统的主要文件的特征值 (简称原始特征值) 作为安全基线，如一些关键的 dll、exe 等。文件特征值具有惟一性，即对 dll、exe 进行任何改动，哪怕是极其微小的干扰，被篡改后的文件其特征值将不同于原始特征值。

(2) 运行监控

基线建立以后，该防护系统将对运行中的工控系统进行监控，如在工控系统主要程序启动时，防护系统再次获得其特征值，并与基线中的原始特征值进行比对，以达到实时监控工控系统的目的。

(3) 实施防御

只有被监控终端所运行的程序的特征值与基线的原始特征值一致时，才允许终端正常运作；若当前特征值与原始特征值有差异时，防护系统将产生报警或者使程序异常退出，从而保护工控系统的安全。

以 Stuxnet 为例，其危害工控系统的方式主要是篡改工控系统本来的运行文件，使得原本正常的指令变为毁灭性的指令来破坏系统。而通过安全基线防护，如果运行文件中的指令被篡改，防护系统会在第一时间检测到文件特征值发生了变化，进而由防护系统发挥保护功能，阻止非法程序对系统造成损坏。同理，对于其他相似的病毒或者未来的一些新的病毒变种，基于主控系统安全基线的防护方法，也对其具有强大的防御能力。

3 结语

工控系统安全是关系国计民生的重大战略问题，在当前新形势下，如何对工控系统进行防护，防止来自内部、外部的安全威胁和恶意攻击，是信息安全领域面临的重大挑战。文中在深入分析工控系统安全风险的基础上，提出了以基础防护为根本，基于主控系统安全基线的防护方法。该方法在兼顾控制管理及实时防御的前提下，实现了工控系统全面、系统的安全防护，对于进一步增强工控系统的安全，建立健全的安全防护体系，具有重大的推动作用。

参考文献

[1] GOBLE W M. Control System Safety Evaluation and Reliability[M]. Alexander Drive：ISA，1998：351–357.

[2] 王文宇，刘玉红 . 基于数据二极管技术的摆渡木马防御研究 [J]. 信息安全与通信保密，2011(6)：83–85.

[3] FARWELL J P，ROHOZINSKI Rafal. Stuxnet and the Future of Cyber War[J]. Survival，2011，53(1)：23–40.

(上接第 32 页)

密码研究热点，因此需深入研究量子计算对 ECC 攻击的理论。

ECC 以其安全性高、占用带宽小、计算复杂度高等优点，受到了广大密码学者的关注而得到快速发展，广泛用于无线通信、智能卡等领域。ECC 密码体制的安全性是建立在有限域上椭圆曲线离散对数计算困难性的基础之上的，由于目前没有发现亚指数级破译算法，因此安全强度比较高，是目前安全强度最高的公钥密码。但是自从 2004 年 Chris Monico 破译 109 bit 的 ECC 以来，根据滑铁卢大学和 CertiCom 公司等业内的研究，近年没有新的破译进展。需要考虑量子计算、DNA 计算等新型计算技术对 ECC 攻击的研究。

问题之六：在量子攻击下，究竟怎样评价 ECC 和 RSA 的被破解能力也是需要研究的一个问题。我们认为需要综合考虑 ECC 和 RSA 的加解密速度、认证签名速度等。在电子计算机环境下，163 bit 的 ECC 与 1 024 bit 的 RSA 安全强度等价，但是加解密速度快几倍。在量子计算环境下，1 024 bit 的 RSA 破译时间和 224 bit 的 ECC 等价，但是 224 bit 的 ECC 加解密速度依然快于 1 024 bit 的 RSA 几倍。参照表 1，可以进一步分析得出结论：很难下定义在量子计算机环境下，ECC 是否比 RSA 容易破解。

因此，在量子环境下谈破解，应该综合考虑安全强度、加解密速度和量子位等器件的性能需求和实现技术等。

加拿大商用量子计算机具有广泛的应用前景。近 3 年量子科学领域国际上连续的关键技术突破，可以认为实用化的量子计算机开始浮出水平线，5 到 10 年内百位级通用 Qubit 量子计算机有望问世，相关研究可以此为前提。而加州圣巴巴拉分校通过量子电路成功实现了冯诺依曼结构并能够执行量子傅里叶变换。

量子计算攻击 RSA 密码已经成为实际可能，而不仅仅是理论分析。因此，需要重视并准确评估量子计算机对现代密码体制的影响究竟会有多大，包括通用量子计算机和加拿大商用量子计算机对密码攻击的能力，以及对目前的公钥密码系统等级保护和安全测评的影响。