嵌入式PLC的信息安全策略设计与实现

周 浩 黄 双 黄雄峰 李 科 周纯杰

(华中科技大学控制科学与工程系 武汉 430074)

摘 要 随着工业化和信息化深度融合以及系统网络互联的快速发展,工业嵌入式PLC控制系统中信息安全问题备受关注。针对嵌入式控制系统信息安全问题,设计了两级信息安全恢复控制机制:内环基于攻击特征库检测可识别入侵,并对比安全策略库制定安全策略;外环基于系统模型检测不可识别入侵,使用冗余技术进行处理。在构建的基于CortexA8-Linux的嵌入式PLC平台上,对信息安全策略进行实现并验证。实验结果表明,系统在保证实时性需求的同时,具有良好检测并处理其外部入侵的性能。

关键词 嵌入式PLC,Linux,信息安全,入侵检测,入侵处理

中图法分类号 TP393 **文献标识码** A

Design and Application of Information Security in EPLC

ZHOU Hao HUANG Shuang HUANG Xiong-feng LI Ke ZHOU Chun-jie

(Department of Control Science and Engineering, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract With the deep integration of industrialization and informationization and the rapid development of system network interconnection, the issues of information security in EPLC attract more attention. This paper proposed a two-level control framework to ensure the information security. Detection based on attack signature database is employed to draw up the control schemes for the identifiable instructions at the inner level. And at the external level, redundancy techniques are used to conquer the unidentifiable instructions which are detected based on system models. Finally, a test EPLC platform on CortexA8-Linux was established to realize and verify the proposed approach, and the experimental results show that the EPLC not only could meet the real-time requirement, but also could detect and process those external instructions well.

Keywords Embedded PLC, Linux, Information security, Intrusion detection, Intrusion processing

嵌入式PLC(Embedded Programmable Logic Controller, EPLC)使用嵌入式技术作为平台,发扬PLC梯形图语言优势,具有PC开放性等优点,为解决对象控制问题提供通用开发平台[1]。在目前的自动化控制网络系统中,EPLC已成为首选的主流现场控制设备,其不但负责现场设备控制、数据采集,还需完成与控制管理中心进行相关通信的任务[2,3]。工业技术的发展,要求控制系统的开放性更大。由于构成的控制网络规模越来越大,随之而来的信息安全威胁也越来越多[4],因此EPLC中信息安全问题的有效解决具有重要意义。

目前,国内外相关领域的专家已经对工业自动化控制系统信息安全工作日益重视,并且提出了一些解决办法,如"纵深防御"策略[5]、入侵检测技术[6]、工业防火墙技术[7]等的使用,ISA-99(即IEC62443)等国际标准中也已包含了一系列信息安全方面的标准条例[8]。文献[9]对比传统和现代工业自动化控制系统的特点,分析出信息安全现状,并提出了"纵深防御"等解决办法。文献[10]介绍了一些西门子PLC的故障安全容错方面信息安全的相关策略,从而提高了产品的安全性能。然而,在工业自动化系统中,EPLC的信息安全研究却非常少。

本文设计了两级信息安全恢复控制框架,实现了对入侵的检测,并通过内环入侵处理模块完成了可识别入侵的处理,外环入侵处理模块完成了不可识别入侵的处理。结合最新的CortexA8-Linux处理平台,实现并进行相关实验工作。

1 EPLC的信息安全需求

1.1 EPLC的典型应用系统结构

应用EPLC的工业自动化控制系统可分为4层:企业管理层、本地操作层、现场控制层和现场采集层[11],同时,层与层之间都是由相应的网络进行连接的。结构设计如图1所示。企业管理层的任务一般由核心管理平台完成;本地操作层的功能一般由HMI等监控设备来实现,其与核心管理平台之间通过以太网相连接;现场控制层的任务交由EPLC、变频器等完成,其也是通过以太网与现场控制层、企业管理层的设备相连;现场采集、执行层包含了各种执行器和传感器,如

到稿日期:2012-11-06 返修日期:2013-02-01 本文受国家自然科学基金项目(61272204),华中科技大学自主创新研究基金(2011ts029)资助。

周 浩(1987—),男,硕士生,主要研究方向为工业人机界面、嵌入式系统,E-mail:zhouhao15917@gmail.com;黄 双(1986—),男,博士生,主要研究方向为工业以太网、网络安全;黄雄峰(1980—),男,博士生;李 科(1988—),男,硕士生;周纯杰(1965—),男,教授,博士生导师。

电机和热电偶等。

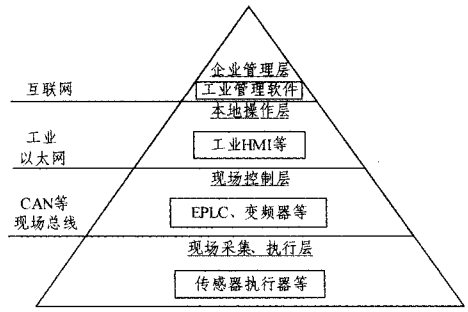

图 1　工业自动化控制系统结构图

工业自动化控制系统中 EPLC 的典型应用系统结构如图 2 所示。基于 EPLC 应用的工业自动化控制系统中，EPLC 主要负责从本地操作层接收数据后发送相应控制命令给执行器，完成与本地操作层 HMI 的通信及对工业现场电机等的控制，同时，对传感器等采集来的数据进行处理；另外，核心管理平台也可以通过以太网和 EPLC 通信，对相连接的执行器进行控制。由此可以看出，EPLC 在工业自动化控制系统中既可以进行现场数据采集、设备控制，又可以进行多个层次间的数据通信，因而其信息安全问题需要得到足够重视，以确保工业自动化控制系统的正常运转。

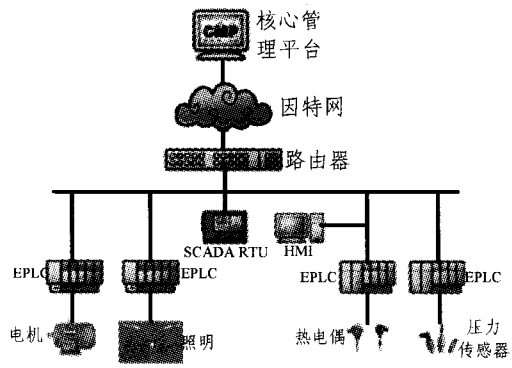

图 2　EPLC 在工业自动化控制系统中经典应用

1.2　EPLC 信息安全问题分析

作为工业自动化控制系统中重要部分的 EPLC，其信息安全问题较为突出。与 IT 信息安全漏洞有所不同，EPLC 可能的威胁有：使用了不充分的访问机制，给予访问者过多或者过少的权限；用户权限窃取，使得低权限用户获得超级用户权限，破坏了 EPLC 系统的核心数据；数据安全审计不够，用户数据容易被篡改、删除、添加；现场总线病毒感染，致使 EPLC 控制命令遭篡改，从而对系统产生毁灭性影响；地线连接混乱，导致 EPLC 发送给执行器的指令错误；核心管理平台受到病毒感染，导致通过 EPLC 连接的现场总线受到攻击；人机界面与系统通信数据未加密，导致 EPLC 受到来自人机界面端的攻击；未使用入侵检测机制及恢复措施，未对入侵行为进行有效防卫、检测和处理等。

2　EPLC 信息安全策略设计

EPLC 系统面对各种各样的攻击，且在工业自动化控制系统中的重要地位决定其信息安全体系结构相比一般的会有所不同，故本文提出了基于两级信息安全控制恢复框架的体系结构，来解决针对 EPLC 信息安全的问题。图 3 所示为 EPLC 信息安全体系结构。

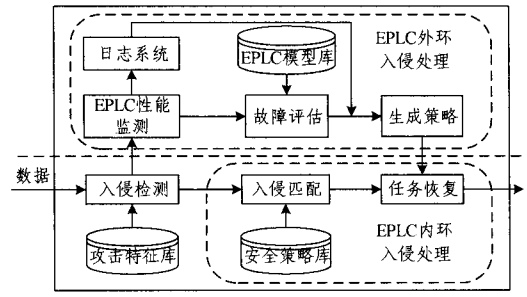

图 3　EPLC 信息安全体系结构

EPLC 的信息安全结构主要包括入侵检测和两级入侵处理功能，内环可以快速处理可识别入侵，外环可以监测系统性能，处理不可识别入侵。“入侵检测”模块借助于“攻击特征库”对相应检测数据进行处理，处理完成后即可判断系统中是否有可识别入侵。EPLC 内环入侵处理模块对可识别入侵进行处理，其使用“安全策略库”进行“入侵匹配”，以完成入侵的快速处理，即发出相应的处理命令；EPLC 外环处理模块对不可识别入侵进行处理，其首先需对系统性能指标进行监测，然后根据模型库中数据对 EPLC 系统的故障进行评估，再选择一个已存储的方案对不可识别入侵进行处理。

EPLC 信息安全体系结构中各个模块的表示：“数据”表示从系统数据流中提取数据用来检测系统是否存在入侵；“EPLC 内环入侵处理”指的是对可识别入侵的处理过程；“攻击特征库”表示特定入侵行为模式的编码而形成的数据库[12]；“入侵检测”指的是使用攻击特征库和系统特征进行匹配，判断系统是否有可识别入侵；“安全策略库”是指用来处理可识别入侵的策略所构成的数据库；“入侵匹配”指使用“安全策略库”对可识别的入侵进行匹配、选择相应的策略的过程；“外环入侵处理”指的是对不可识别入侵的处理过程；“日志系统”用于记录性能检测过程中缠身的数据、参数等；“性能监测”指监测系统中的相关性能参数；“模型库”指系统的机理特征构成的数据库，用于判断系统哪个部分出现故障；“任务恢复”指的是使用选定策略或者故障恢复方案对入侵进行处理并使系统正常执行。

3　EPLC 信息安全策略实现

EPLC 信息安全的实现是在 CortexA8-Linux 平台上，通过将两级信息安全恢复控制框架应用于其软件设计中完成的。

3.1　EPLC 系统平台结构

EPLC 采用 TI 公司的以 CortexA8 为内核的 AM3359 芯片，最高主频可达 1GHz，资源丰富，可帮助 EPLC 实现复杂的功能。图 4 所示为 EPLC 系统硬件结构。EPLC 硬件平台主要包含：CPU 模块、存储模块、通信模块、功能模块、实时时钟模块及备用模块等。

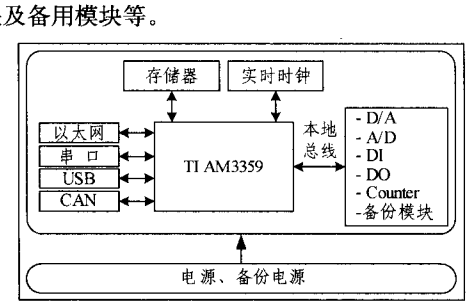

图 4　EPLC 的硬件结构图

EPLC 系统的软件平台的设计是建立在嵌入式 Linux 操作系统基础之上的，其结构如图 5 所示。

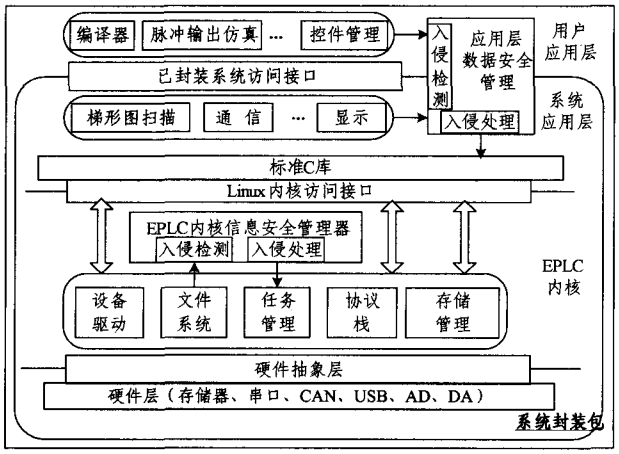

图 5　EPLC 软件平台结构图

EPLC 的软件系统内核（即 Linux 内核）只提供经典的 UNIX 自主访问控制（root 用户），以及部分地支持了 POSIX. 1e 标准草案中的 capabilities 安全机制[13]，这对于 EPLC 内核的信息安全性来说是不够的，因而在内核中添加“ELC 内核信息安全管理器”模块很有必要。EPLC 的应用层和内核之间存在数据交互接口，较容易受到外界的攻击，故应在此接口上添加信息安全管理模块，即“应用层数据安全管理器”模块。

EPLC 系统中上述两个信息安全管理模块都按照两级信息安全恢复控制框架来设计，都包含了入侵检测功能和两级入侵处理功能。

3.2　入侵检测模块实现

EPLC 入侵检测模块主要是通过与攻击特征库[12]进行匹配来判断入侵是否为可识别入侵。首先要对标识特定的入侵行为模式进行编码，建立误用模式库；然后对实际检测过程中得到的数据进行特征匹配，检查是否包含入侵行为的标识。EPLC 入侵检测模块实现流程如图 6 所示。

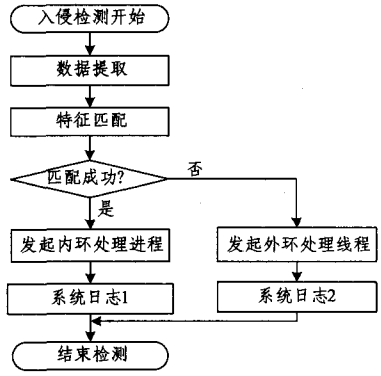

图 6　入侵检测模块实现流程图

“数据提取”后会将相关数据与 EPLC 攻击特征库中的数据进行特征比较，然后判断 EPLC 系统中是否存在可识别的入侵。若发现有可识别的入侵，则发出警告，通过 EPLC 内核任务管理器启动内环处理线程，并将相关入侵信息记录在“系统日志 1”中；若判断出有不可识别入侵存在于系统中，EPLC 内核任务管理器则启动外环处理线程并将相关信息记录在“系统日志 2”中。

若当前所检测出入侵发生在 EPLC 系统内核中，系统需要通过系统日志中的信息向内环处理模块传递较高紧急程度信息，以优先处理该入侵，从而使系统相对更快地恢复正常运行。

3.3　基于匹配技术的可识别入侵处理

EPLC 内环入侵处理模块采用基于匹配技术的入侵处理方式，其在入侵检测模块发起内环入侵处理线程后开始工作。EPLC 内环入侵处理模块借助安全策略库，迅速匹配相应处理策略，对入侵进行快速处理。

只有在策略库及其调用方案设计完成的情况下，入侵处理模块才能发挥其对入侵对象快速、有效处理的特性。故内环入侵处理模块中策略库的设计至关重要。

首先需要设计合适的数据结构。策略库的数据结构不但需要包含与其本身的相关特征信息，还需要包含一些策略调度的信息。安全策略库中策略的数据结构定义如下：

```
struct SecPolicy
{
  struct SecPolicy * chain_head; / * 链式存储头指针 * /
  u_int refent; / * 参考计数器 * /
  struct secpolicyindex spidx; / * 安全策略引擎 * /
  u_int32_t id; / * 进程号 * /
  u_int state; / * 状态 * /
  u_int policy; / * 选择、绕过、应用 * /
  struct secrequest req; / * 处理请求 * /
  u_int degree; / * 策略紧急程度 * /
  struct SecPolicy * chain_Tail; / * 链式存储尾指针 * /
}
```

变量“state”是该策略节点被使用的情况，包括处理、就绪及空闲等状态；变量“policy”指的是该策略节点在策略库中的生命状况，包括丢弃、绕过和应用；变量“degree”指的是当前策略节点对应的入侵需要被处理的紧急程度。

然后，设计一个双向循环链表将策略库中所有策略节点串联起来，以支持快捷地调用其中的策略数据，同时方便地对其包含的安全策略做删减和添加等操作。

数据结构中“ * chain_head”为指向策略库中前一个策略的结构体指针；“ * chain_Tail”为指向策略库中的后一个策略的结构体指针。这样，所有安全策略成员就可以通过双向循环链表构成一个可调度的整体了。

EPLC 内环入侵处理线程通过对系统日志中的数据进行分析，得出用来遍历策略库的特征数据，然后使用策略库成员的策略引擎“spidx”对双向链表进行遍历。当遍历完成后，向处理线程反馈系统应调用哪个策略完成内环入侵处理。最后，线程按照该策略对入侵进行处理。

3.4　基于冗余技术的不可识别入侵处理

EPLC 外环入侵处理采用的是基于冗余技术的处理方式，在入侵检测系统发起外环处理线程后开始工作。EPLC 的外环入侵处理线程首先需对系统性能进行监测。若系统性能正常，那么直接关闭处理线程即可；若此时系统的性能已属于不正常状态，那么该处理线程将结合 EPLC“模型库”判断出 EPLC 系统故障的位置，并采取措施对故障进行评估和处理。对于 EPLC 来说，故障一般可分类为：处理器故障、通信

故障、I/O故障、电源故障。EPLC外环入侵处理模块使用了冗余技术对上述故障进行处理，而冗余技术包括软冗余(soft-redundancy)技术和硬冗余(hard-redundancy)技术[14]。

软冗余技术采用了编程的方式来实现PLC同步、故障切换。外环入侵软冗余故障处理流程如图8所示。

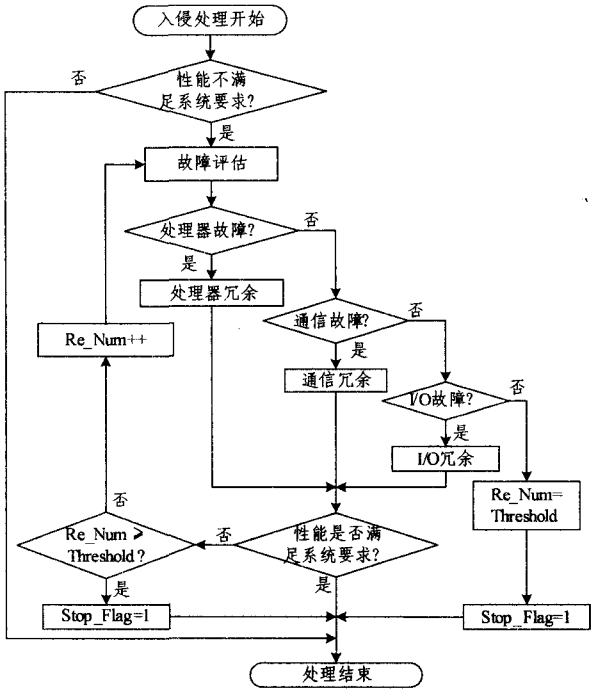

图8 不可匹配入侵处理流程

外环入侵处理开始后，需对EPLC内部的性能进行评估，判断其性能是否满足需求。如果不满足，则其需要对故障进行评估，判断出EPLC系统哪里出现故障。接着处理线程需要针对判断出的故障进行对应的冗余处理。冗余处理结束，继续判断系统性能是否满足需求。若满足需求，则立即关闭入侵处理进程；若不满足需求，则需要继续对故障进行评估并处理。然而，当冗余处理执行次数“Re_Num”达到预定值“Threshold”，严重影响系统实时性能时，设定“Stop_Flag=1”，并向管理员申请安全关闭系统；当系统故障为处理器故障、通信故障及I/O故障以外的故障时，设定“Stop_Flag=1”，并交由下级使用硬件冗余技术处理。

硬冗余技术采用特殊的硬件模块或EPLC中固化的程序来实现EPLC同步、故障切换。当外环入侵处理模块判断出EPLC系统的故障后，若其中一部分模块出现了故障，可以使用硬冗余技术来解决，如I/O设备故障、电源故障等。EPLC系统中增设易出故障模块的备份模块，如备份电源模块、备份I/O模块等，用于硬冗余技术的实施，使得出现故障的EPLC系统通过硬件置换的方式恢复正常运行。当系统故障无法通过硬件冗余技术进行解决时，其会向管理员申请关闭系统。

4 EPLC的信息安全验证实验

4.1 实验平台

实验系统由人机界面、EPLC、路由器、PC机等部分构成。人机界面向EPLC发送正常通信数据，而EPLC通过路由器连接至以太网，并将相关数据上传至PC机进行监测。同时，另一台PC发送模拟攻击至EPLC所在的控制网络中。基本结构如图9所示。

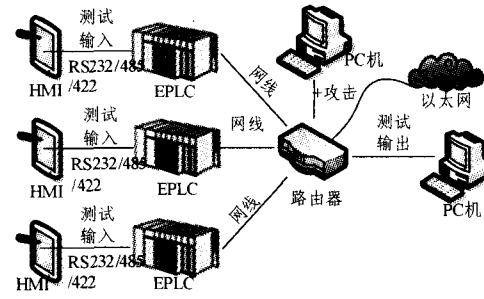

图9 入侵处理实验平台

模拟攻击是从KDDCUP 99入侵数据集[15,16]中提取数据加载到EPLC所在控制系统，该入侵数据集主要分为4大类，它们分别是：拒绝服务DOS、系统漏洞探测Probing、远端超级用户权限获取U2R及远端服务权限获取R2L。

4.2 EPLC信息安全验证实验

EPLC的信息安全体系结构方案验证主要分为3个方面：可识别入侵识别性能、不可识别入侵故障恢复和实时性保障。

(1)可识别入侵检测性能实验

为了满足需求，从KDDCUP 99入侵数据集中提取了8800个记录(800个异常行为记录，8000个正常行为记录)，通过攻击软件加载至系统。另外，使用检测率和误报率对系统入侵检测效果进行评估。实验中使用KDDCUP 99入侵数据集时必须设置一个阈值[17](设置为30)，得到的实验结果如表1所列。

表1 EPLC入侵检测率和误报率

入侵类型	检测率	误报率
DOS	98.22%	4.53%
Probing	99.31%	1.21%
U2R	96.52%	0.67%
R2L	98.78%	3.44%

从实验数据可以看出，入侵类型蟪Probing时，检测率最高；入侵类型为U2R时，误报率最低。系统对可识别入侵的检测体现出较好的可靠性。

(2)不可识别入侵故障恢复实验

这部分实验将DOS、Probing、U2R、R2L互相组合形成攻击源加入系统中。使用系统的故障处理数来检验系统对不可识别入侵故障处理的性能，表2为以下3种情况下1小时内(3600次攻击)故障处理的情况。

Case1 仅内核添加了安全保护模块；

Case2 仅应用层添加了安全保护模块；

Case3 两者皆添加安全保护模块。

表2 EPLC故障处理次数

攻击类型	Case1	Case2	Case3
DOS+Probing	289	3262	3568
Probing+U2R	252	3178	3421
U2R+R2L	263	3235	3518
R2L+DOS	273	3252	3535

由入侵处理验证实验的结果可以看出，当EPLC同时包

含内核信息安全管理模块和应用层信息安全保护模块时，其对不可识别入侵处理的效果很好，最高可达 98.2%。

(3)实时性保障实验

该实验使用实验(1)中的攻击源，且各种攻击出现频率相同，主要针对两方面进行测试：可识别入侵处理和不可识别入侵处理。对于不可识别入侵来说，“Threshold”值大小对系统实时性的影响为实验目标。图 10 为系统实时性在不同信息安全处理条件下的情况。

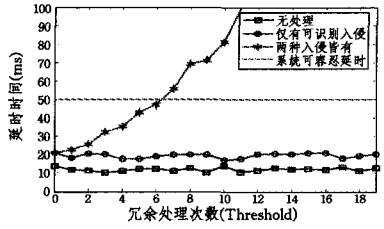

图 10 不同信息安全处理下的系统实时性

由实时性保障验证实验结果可以看出，当系统仅有可识别入侵处理时，其实时性仍可满足需求；而当有不可识别入侵处理且冗余处理次数的阈值设定超过 6 时，系统实时性已经不能满足需求了。故保障系统信息安全的前提应是准确设置软冗余处理的次数阈值。

结束语 为改善工业自动化系统中 EPLC 出现的信息安全问题，本文提出了两级信息安全恢复控制策略，并在基于 CortexA8-Linux 的 EPLC 平台上进行了入侵检测和处理效果验证，通过两级安全防护，其在满足系统实时性要求的同时很好地保证了系统的信息安全。不可识别入侵处理依赖于软冗余处理阈值“Threshold”，构建合理的方法来优化阈值的选择将会进一步提高系统的入侵处理能力，使得系统安全性能进一步提高。

参 考 文 献

[1] 王晓光. 嵌入式 PLC 的设计与研究[D]. 成都：西华大学，2011

[2] 贺无名，余强国. 基于嵌入式软 PLC 的矿井提升机控制系统设计[J]. 煤矿机械，2011，32(6)：244-246

[3] 孟庆春，刘云卿. 应用于 PLC 控制程序的 Petri 网执行模型[J]. 计算机科学，2009，36(10)：150-159

[4] Koopman P. Embedded system security[J]. IEEE Computer，2004，37(07)

[5] 张帅. ICS 工业控制系统安全风险分析[J]. 信息安全与通信保密，2012(3)：15-19

[6] 杨智君，田地，马骏骁，等. 入侵检测技术研究综述[J]. 计算机工程与设计，2006，27(12)：2119-2123，2139

[7] 方来华. 工业控制系统的信息安全[J]. 电气时代，2008(10)：118-121

[8] Stouffer K，Falco J，Scarfone K. Guide to Industrial Control Systems Security[R]. UK：National Institute of Standards and Technology，2011

[9] 唐文. 工业自动化控制系统信息安全研究[J]. 计算机安全，2012(4)：2-7

[10] 田海，崔桂梅，王晓红，等. 西门子 PLC 控制网络的配置策略与应用[J]. 电气传动，2010(01)：76-80

[11] 陈慕宁. 工业自动化控制系统的设计[J]. 电脑编程技巧与维护，2008(16)：27，62

[12] 刘阳. 基于免疫原理的无线传感器网络入侵检测系统研究[D]. 北京：中国科学院研究生院(计算技术研究所)，2008

[13] 刘俊年. 基于 linux 系统的安全策略研究及其实现[D]. 成都：四川大学，2008

[14] 赵中敏. 冗余设计在 PLC 控制系统中的应用[J]. 机床电器，2007(3)：42-45

[15] 白琳. 基于免疫优势克隆网络聚类的入侵检测[J]. 计算机科学，2012，39(07)：82-86，118

[16] Hettich S，Bay S. The UCI KDD Archive[OL]. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. Irvine，CA：University of California，Department of Information and Computer Science，1999

[17] 翟光群，陈向东，胡贵江. 蜜罐与入侵检测技术联动系统的研究与设计[J]. 计算机工程与设计，2009，30(21)：4845-4847，4867

(上接第 124 页)

[6] Miller G A. WordNet：a lexical database for English[J]. Communications of the ACM，1995，38(11)：39-41

[7] 陆汝钤，石纯一，张松懋，等. 面向 Agent 的常识知识库[J]. 中国科学 E 辑，2000，30(5)：453-463

[8] 曹存根，丰强泽，高颖，等. Progress in the Development of National Knowledge Infrastructure[J]. 计算机科学技术学报：英文版，2002，17(5)：523-534

[9] 金芝. 基于本体的需求自动获取[J]. 计算机学报，2000，23(5)：486-492

[10] 钟秀琴，符红光，余莉，等. 基于本体的几何学知识获取及知识表示[J]. 计算机学报，2010，1(33)：167-174

[11] 王前，冯亚军，杨兆民，等. 基于本体的网络攻击模型及其应用[J]. 计算机科学，2010，37(6)：114-117

[12] Peng Ning，Yun Cui，Douglas S. Constructing Attack Scenarios through Correlation of Intrusion Alerts[C]// The 19th ACM Conference on Computer and Communications Security，ACM CCS 2002. Washington：North Carolina State University，2002：245-254

[13] 邓志鸿，唐世渭，张铭，等. Ontology 研究综述[J]. 北京大学学报：自然科学版，2002，38(5)：730-738

[14] Studer R，Benjamins V R，Fensel D. Knowledge Engineering，Principles and Methods[J]. Data and Knowledge Engineering，1998，25(1/2)：161-197

[15] Perez A G，Benjamins V R. Overview of Knowledge Sharing and Reuse Components：Ontologies and Problem-Solving Methods[C]//Proceedings of the IJCAI-99 workshop on Ontologies and Problem-Solving Methods(KRR5). 1999：1-15

[16] 诸葛建伟. 网络攻防技术与实践[M]. 北京：电子工业出版社，2011