电力信息网新型IDS体系设计

张 可[1,3] 吴 瑜[2] 刘乃琦[3] 贾海涛[1]

(电子科技大学电子科学技术研究院 成都 610054)[1] (英特尔公司上海研发中心 上海 201100)[2]

(电子科技大学计算机科学与工程学院 成都 610054)[3]

摘 要 针对目前电力信息网存在的网络安全隐患问题,提出了一种基于IXA架构实现的新型协同入侵检测体系设计,即具有协同人体免疫特性的电力信息网三层防御入侵检测系统。将基于主机的检测和基于网络的检测结合起来,如人体免疫系统一样,为电力信息网提供综合的、多层次的保护。它使用网络处理器作为数据分析引擎,充分利用了Intel IXP网络处理器的可编程高速并行处理特性,使入侵免疫体系具有更强的灵活性和可扩展性。

关键词 电力信息网,入侵检测系统,协同免疫,互连网交换架构,网络处理器

Design of Advanced IDS Architecture for Electricity Information Networks

ZHANG Ke[1,3] WU Yu[2] LIU Nai-qi[3] JIA Hai-tao[1]

(Research Institute of Electronic Science and Technology, University of Electronic Science and Technology of China, Chengdu 610054, China)[1]

(Intel Corp. Shanghai Research Center, Shanghai 201100, China)[2]

(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China)[3]

Abstract For the hidden troubles of current electricity information networks, introduced a design of new architecture of intrusion detection system based on IXA with three protection-layers for electricity information networks. Combining the detections based on hosts and networks, this architecture provided integrative multilayer protection for electricity information networks, just like the biologic immunity system. This architecture uses the network processor as its analysis engine for the high speed and powerful programmable multiprocessing characteristic of Intel IXP. This architecture has more flexible and extensible characteristics.

Keywords Electricity information networks, IDS, Concurrent immunity, IXA, Network processor

1 引言

电力信息网是电力行业的综合业务信息网。它将电力行业的各种相对独立的业务系统,包括各种电力自动化系统、信息管理系统、用电管理系统、通信系统等联网运行,实现各种静态、动态信息的共享。电力信息网经过不断改造和完善,从网络规模、链路质量、运行稳定性上都有了较大的提高,形成了一个覆盖面广、速度快的广域网,提高了企业的工作效率和管理水平[1-3]。

电力信息网的安全性隐患来自方方面面,主要包括系统自身的安全漏洞(可被攻击者利用)、内部人员的不规范操作、来自外部Internet(包括Intranet)的病毒、"黑客"等恶意攻击,以及安全管理的漏洞等。在这些安全隐患当中,来自外部的入侵最为严重,很可能给电力信息网络造成极其巨大的损失。构造有效的入侵检测体系来检测并制止网络中可能导致入侵的行为显得尤为迫切。目前,电力信息网主要采用IDS(入侵检测系统),根据其输入数据的来源可分为两类:基于主机(数据来源于单一主机,通常是主机的审计记录)的入侵检测系统和基于网络(数据来源网络的信息流)的入侵检测系统。这两种IDS都存在数据来源相对单一、信息不能共享、无法有效对付DOS攻击等多个问题。

首先是分布性较差。在大多数电力信息网IDS系统中,中央数据分析器是系统中唯一的数据分析引擎,存在单点失效的问题。一旦该节点被攻破,内部的计算机就无法得到有效的保护,整个电力信息子网都将陷入危险当中。其次是鲁棒性较差。在大多数电力信息网IDS系统中,它们的组件一般都是唯一的。当某种组件遭到多种原因可导致的破坏时,这种破坏将直接影响到整个电力信息网IDS的安全防御性能。最后是适应性较差。当前电力信息网面临的各种攻击手段层出不穷,然而大多数电力信息网IDS系统却不能适应这种变化,对于分布式的DOS等攻击更是显得无能为力。

本文基于IXA架构实现了一种用于电力信息网的新型入侵免疫体系。首先,该体系将基于主机的入侵检测和基于网络的入侵检测结合起来,充分利用了IXP网络处理器强大的可编程并行处理特性,建立如同人体免疫系统一样的新型入侵检测系统,为电力信息网提供协同的、多层次的保护。其

到稿日期:2008-04-16 本文受国家自然科学基金资助项目(60702072)资助。

张 可(1979—),男,助理研究员,博士生,主要研究方向为网络信息安全、网络体系结构,E-mail: kezhang@uestc.edu.cn;吴 瑜(1981—),男,工程师,主要研究方向为Intel IXA架构、信息安全;刘乃琦(1950—),男,教授,主要研究方向为网络与信息安全;贾海涛(1977—),男,助理研究员,博士生,主要研究方向为信息处理技术。

次，该体系不采用单一控制中心设计，整个系统分散存在、协同工作，不存在单点失效问题。再次，该体系实现了数据收集、分析的分布性，极大地提供了系统实时检测和响应入侵的能力，能够有效地检测从电力信息网中发起的 DOS 攻击。最后，该体系使用网络处理器作为数据分析引擎，因为网络处理器所具有的强大可编程高速并行处理特性，所以该体系具有更强的灵活性和可扩展性。

2 IXA 架构与 IXP2350 网络处理器

网络处理器代表了高速网络设备发展的趋势。它兼具 ASIC 的高性能和通用 CPU 可编程的灵活性，以及低成本和低风险。目前所有的网络处理器都采用并行处理机制来提高性能，即通过多个微处理器并行工作来提高系统的吞吐量。

为促进基于下一代 IP 的网络应用的发展，Intel 创建了一种以网络处理器为基础的包处理结构，称为 IXA(Internete Xchange Architecture)。这种架构将 IXA 网络处理器的完全可编程性和强大的高速包处理性能结合起来，以支持智能网络设备的快速开发。IXA 作为一种网络处理架构，是以可编程的网络处理器为核心，包括 3 个主要组成部分：微引擎技术、XScale 技术以及 IXA 可移植架构。

IXP2350[4]是 Intel 公司开发的新一代网络处理器，是英特尔互连网交换架构 IXA 的基础。它具有高性能的数据处理能力，是可适应于多种局域网和远程通讯的产品。

IXP2350 主要包含 4 个 RISC 数据处理器微引擎第二代产品 Microengine version2(MEv2)、1 个 Intel XScale Core、SRAM 控制器、DRAM 控制器、PCI 控制器、SHaC 单元、MSF 单元以及两个 NPE(Network Processor Engine)单元。图 1 为 IXP2350 的内部结构图。

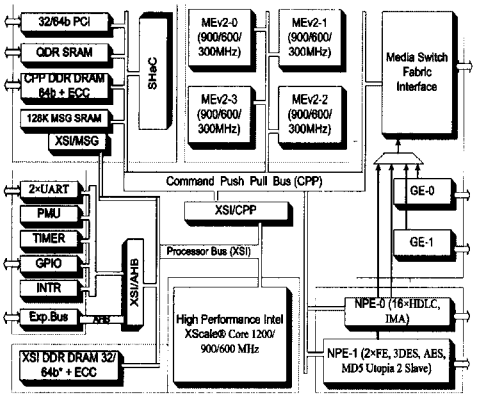

图 1 IXP2350 内部结构图

3 人体免疫生物原理

现代免疫学认为，人体内存在一个负责免疫功能的完整的生理机——免疫系统，它与神经和内分泌等其他系统一样，有着自身的运行机制并可与其他系统相互配合，相互制约，共同维持机体在生命过程中的总体平衡与稳定。免疫系统拥有许多值得借鉴的显著特征，如分布性、多样性、自动应答和自我维护、异常检测等。这些原理为计算机免疫系统的构建提供了多种组织结构。

人体免疫系统从免疫机理和层次的不同，可以分为两类：物理免疫系统和生物细胞免疫系统。前者由皮肤、唾液、鼻毛等一系列人体组织构成，它是这一个免疫体系结构中最外面的层次，也是抵御传统感染的第一道屏障。这个层次的免疫机理是提供如 pH 值或温度等这样不适合某些异己的生命体(即病原体)生存的物理环境，从而达到杀死病原体、保护自己的目的。而后者则存在于人体内部，它可被看作是一个分布式探测系统，该系统主要由白细胞即淋巴细胞组成。它主要是由骨髓和胸腺部位产生的，通过绑定机制来识别一定数量结构相似的抗原细胞。如果在有限的时间内能够绑定到数量超过某一阈值的抗原，那么淋巴细胞就会被启动，以杀死抗原，这称为免疫应答。同时，免疫系统能将侵入抗原反应部分抗体作为记忆细胞保留下来。对于同类抗原的再次侵入时，相应的记忆细胞被激活而产生大量的抗体，缩短了免疫反应时间，这称为免疫记忆。

4 电力信息网协同免疫生物模型

借鉴以上的人体免疫理论，我们为电力信息网构建了一个具有异常检测、免疫应答、免疫记忆的分布式多层防御入侵检测体系。该系统由两部分组成：分析监控器和免疫计算机。分析监控器位于传统的网关节点，执行基于网络的入侵检测，它基于 IXP 网络处理器实现。利用 IXP 网络处理器的分布式数据处理特性，它可以对网络数据流实施两层的分析和监控：首先通过 IXP 网络处理器的微引擎对数据包做轻度检查后，立即高速转发给电力部门子网中的主机；接着，IXP 的核心处理内核 XScale 对数据包做深度的入侵分析，以发现更为隐蔽的入侵。这样，分析监控器在尽量不牺牲数据包转发速率的同时，对电力信息子网中的主机做了最大程度的保护。

将电力信息子网中每台计算机都设为免疫计算机，执行基于主机的入侵检测，构成了整个入侵免疫的第三层防御体系，它类似于人体免疫系统中的生物细胞免疫。在免疫计算机的生物学模拟中，计算机中的活动进程视为有机分子，电力信息网视为有机体组织。对于“细胞”入侵的识别主要根据由授权程序执行的系统调用短序列(类似于肽链)。在系统中，建立类似于淋巴细胞的进程，该进程直接和内核通信，监控其他进程，及时发现程序执行的异常。与免疫系统的判别机制相同，当“淋巴细胞”发现某个进程运行异常时，就认为该进程被破坏或正在受到攻击。如果确定入侵，“淋巴细胞”将减慢、挂起、杀掉或者重启异常进程，并通知位于电力信息网网关位置的分析监控器。免疫计算机的生物学模拟关系如图 2 所示。

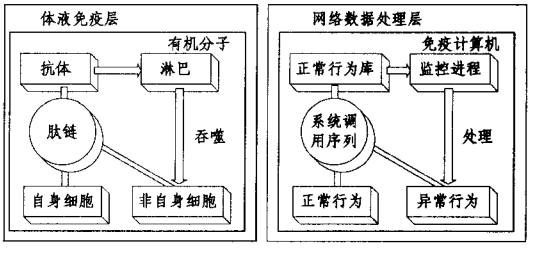

图 2 电力信息网中免疫计算机的生物模拟关系

5 基于 IXA 的电力信息网协同免疫设计

从层次上来看，我们构建的基于 IXA 架构的电力信息网协同免疫体系主要由 3 个层次构成，这 3 个层次的实现分别

位于 Intel IXP 网络处理器的微引擎 MEv2、Xscale Core 以及电力信息子网中的免疫计算机上。它们协同工作，分别模拟了人体免疫系统中免疫机理的不同层次，分别实现了类似物理免疫系统和生物细胞免疫系统的功能。该基于 Intel IXA 架构的协同免疫体系的具体防御层次如图 3 所示。

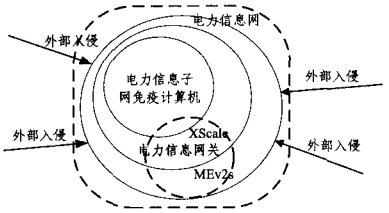

图 3　基于 IXA 的协同免疫 IDS 系统的具体防御层次

整个系统的开发分为两个部分：用 IXP2350 网络处理器实现分析监控器和开发免疫计算机上的入侵检测程序。整个系统的结构如图 4 所示。

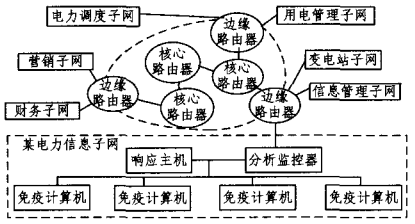

图 4　基于 IXA 的电力信息网协同免疫 IDS 结构图

下面将介绍这 3 个层次分别位于 Intel IXP 网络处理器的微引擎 MEv2、Xscale Core 以及电力信息子网中免疫计算机上的 IDS 系统具体实现。

5.1　电力信息网第一层防御实现

根据 IXP 网络处理器的特点以及软件设计的要求，整个系统采用模块化划分，保持了各个模块的独立性，以有利于扩展和维护。整个设计分为 3 层：数据平面、控制平面、通信子层。

IXP 的微引擎实现数据平面的功能，主要完成数据包的接收、分类、转发等操作。在分析监控器的具体实现中，微引擎有 3 个任务：接受并发送网络数据包、对数据包进行规整（轻度检查）和维持免疫计算机与 XScale 核之间的通信。其中，对数据包进行规整是非常重要的。它有 3 个方面的作用：第一，可以对数据包做预处理，如协议分析等，以便 XScale 做深度的入侵分析。第二，避免了攻击者利用协议的漏洞和不完备性进行系统探测和攻击的可能，可以对电力信息网内部的计算机提供第一层保护。第三，消除了网络数据包的二义性，增强了入侵检测的能力。具体的规整算法可参见文献[10]。

微引擎上的程序开发设计，我们采用 PPS 模式。PPS（Packet Processing Stage）是对应用程序在逻辑层面上划分的可并行执行的一系列功能单元[5,6]，也是 IXP 网络处理器的编程功能单元。根据网络包处理的天然特性，网络应用程序在逻辑上能够划分为多个相对独立的模块，即对应于 IXP 编程中的多个 PPS。PPS 包括初始化代码和一个无条件循环体。PPS 之间的通讯是通过 Pipe 这种数据结构实现的。编译器保证 Pipe 的 PUT 和 GET 操作的同步互斥，支持 Abstract Pipe，NN Pipe 和 Scratch Pipe 3 种。对于 Abstract Pipe，编译器将根据性能需求、资源情况等因素自动选择 Pipe 的实际类型。多个 PPS 及 Pipe 采用 Autopartitioning 模式按照优化处理及通信功能需求分配到 IXP 网络处理器上执行相关功能。

该设计中运行在 MEv2 上的 Inbound Pipeline 包含了如下的 PPSes：Packet Receive，Packets Processing，Classify 和 Coordinate，Scheduler 以及 Packet Transmit，其中 Packets Processing 为核心处理 PPS。图 5 是该 Inbound Pipeline 的 packet processing stages 设计。

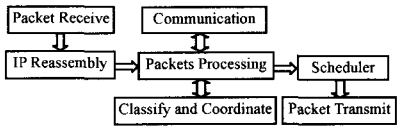

图 5　Inbound 的 PPSes 设计

5.2　电力信息网第二层防御实现

电力信息网第二层防御功能由位于控制平面的 XScale 核完成，其主要任务包括建立和维护正常行为知识库，全局分析整个电力信息子网数据流，进行入侵检测分析，做出入侵决策，根据接种疫苗规则集更新入侵记忆库并与相应主机以及各个免疫计算机进行交互，实时克隆更新各个免疫计算机的免疫特征信息库。为了减轻 XScale 的负担，加强它的处理能力，我们充分利用 IXP2350 内部的两个 NPE（Network Processor Engine）[4]，让它参与完成一部分固定的工作。分析监控器的模块结构如图 6 所示。

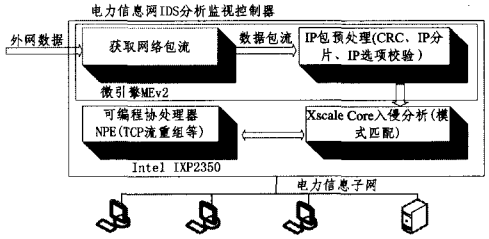

图 6　分析监控器的模块结构图

为了实现 XScale 上的入侵检测，我们选择在文献[11]中提出的 DAIS 算法（Detection Algorithm based on Immunology and Sequential Pattern）。它结合了免疫学和序列模式分析的理论。该算法的显著特点是：

1）根据数据的不同来源，采用了不同的手段，降低了系统的误报率；

2）在正常行为特征上，DAIS 监控特权进程的行为，不受用户行为变化的限制；

3）引入系统调用参数，提高检测精度，降低漏报率；

4）获取数据包和网络流量的规律，实时监控各个连接进出流量及其流速和流速变化率的变化；

5）由于正常行为数据库是根据操作经验产生的，而且该数据库与本地操作环境有关，因此每个站点的数据库均不同，对入侵检测有较为理想的预警、防范作用。

由于电力信息子网内部免疫计算机不能直接和位于电力信息网关位置的分析监控器核心处理器进行通信，而且 IXP 网络处理器目前对微引擎和 XScale 之间的通信机制的提供不够完善，为此我们专门设计了通信子层，负责免疫计算机与

（下转第 287 页）

映射模型，给出了详细的设计与实现方案。仿真结果表明，本文所建立的模型可以支持 Flow Label 与 DSCP 值的映射，以区分更细粒度的 QoS 等级。同时，基于 Flow Label 识别单流的特性，它可以更好地保证具有不同 QoS 策略的自治域间统一的服务等级，实现 QoS 的端到端映射。这给 Flow Label 在 QoS 保障方面的研究提供了强大的支持。

参 考 文 献

[1] Rajahalme J, Conta A, Carpenter B E. Steve Deering: IPv6 Flow Label Specification. RFC 3697, IETF, 2004

[2] Nichols K, Blake S, Baker F, et al. Black: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. RFC2474, December 1998

[3] Robert W. McAuliffe: QoS at the Differv Network Edge. Spring, 2003

[4] Dogar F R, Zartash A. Uzmi: DiffServ Architecture: Impact of scheduling on QoS

[5] Hardy W C. QoS Measurement and Evaluation of Telecommunications quality of service. Wiley, 2001

[6] OPNET Technologies, Inc. http://www.opnet.com/

[7] 李馨，叶明. OPNET Modeler 网络建模与仿真. 2006：87-97

(上接第 283 页)

XScale、微引擎和 XScale 之间的信息交换。

5.3 电力信息网第三层防御实现

电力信息网第三层防御机制由位于电力信息子网内部的免疫计算机提供，这些免疫计算机入侵检测原理主要依据正常行为模式数据库，它通过监控自己感兴趣的应用程序，形成每台计算机特有的正常行为数据库。在计算机程序执行过程中，实时提取审计数据，将提取的审计数据转为特定的行为特征模式，供分析模块分析，检测入侵。当不匹配率超过预先设定的阈值，则产生报警。而系统自学习功能类似于生物免疫系统的再次应答，即当免疫计算机检测到新的攻击手段时，不仅产生报警，同时将该入侵的行为特征模式存入系统。当再次采用该方法入侵系统时，系统可直接向用户产生入侵信号，而不需进行入侵分析和报警，模拟生物的初次应答和再次应答，极大地提高了系统的反应速度和可靠性。

6 电力信息网关 IXP 对包的处理过程设计

首先，MSF 从外部电力信息网接收到数据包，然后将数据包交送 MSF 接口中的缓冲区 RBUF。MSF 接口中的缓冲区包括 RBUF 和 TBUF，它们可编程划分为 64，128 或 256B 的单元。一个包的数据通常要占用若干个这样的单元，存储在每个单元中的包数据，就称为一个 mpacket(MPKT)，这里采用 128B 的单元。接着，MSF 从 THREAD_FREELIST 中寻找可用线程，然后 MSF 将接收状态字写入到线程的传输寄存器中并向线程发送信号。该线程在获得信号后开始工作，读取接收信息并且将 mpacket 从 RBUF 直写到 DRAM 内存中去，然后将一个句柄放到 Scratchpad ring 上。

ME 线程检测位于 Scratchpad ring 上的可用包并取下句柄，然后对包进行检测，并取得包中的各种部分传送到 ME 的传输寄存器中。因为该入侵检测系统的各种表以及规则库存都存放在 SRAM 当中，所以它们可以被高速地查找和修改，而在 DRAM 里的数据包也将根据匹配结果被处理。接下来，被修改后的包的句柄将会被放到 SRAM 队列中，等待被调度和传送。

ME 的线程会监视 SRAM 队列中的包的句柄。如果发现已经被更新了数据的需要发送的包，那么该线程就对这些包的句柄进行出队列操作。然后该线程计算出下一个 mpacket 的位置并将它放入下一个可用的 TBUF 单元，采用直接从 DRAM 传送到 MSF。写 TBUF 单元控制字，标明 TBUF 包含有效的数据。如同接收程序，传输程序必须重复地接收 mpacket 并将其组成即将发出的包，MSF 通过 ME 支持的控制字中包含的信息检测包的结束。最后，一旦 MSF 检测到 EOP mpacket，外部设备将发出该包。接下来，IXP 网络处理器将继续处理下一个包。

结束语 本文利用 Intel 公司 IXA 架构为平台，设计了一个具有协同免疫特性的电力信息网入侵检测系统。该系统充分发挥了 IXP 网络处理器强大的分布式数据处理和快速的包转发能力，使得软件和硬件紧密结合，弥补了目前电力信息网 IDS 的不足。同时，由于使用了可编程的网络处理器，对入侵检测系统功能的升级也只需要升级软件而不需要开发硬件设备。另外，基于人工免疫的思想，提出了多层防御检测体系，使得电力信息网内每台计算机不仅仅是受保护的对象，同时参与入侵检测，大大增强了电力信息网整体检测入侵的能力。

参 考 文 献

[1] 马远东，杨文清，张官元. 电力信息网中的 RMON 网络探测器的设计与实现. 电力系统自动化，2004(12)：67-70

[2] 王焱，郑俊辉，曾家智. 一种电力信息网的新型 QoS 机制. 电力系统自动化，2007(10)：73-107

[3] 王焱，郑俊辉，易发盛，等. 电力信息网的服务元体系结构. 电力系统自动化，2007(4)：85-89

[4] Intel Corp. Intel IXP23XX Product Line Hardware Reference Manual. IXP SDK4. 2. 2004：27-195

[5] Intel Corp. Intel C Compiler for Intel Network Processors Autopartitioning Mode Reference. IXP SDK4. 2. 2005：9-25

[6] Intel Corp . Intel IXA Software Example Designs for Intel C Compiler Application Note. IXP SDK4. 2. 2005：6-55

[7] Intel Corp. Intel IXA Software Building Blocks for Intel C Compiler Developers Manual. IXP SDK4. 2. 2005：23-54

[8] Intel Corp. Intel IXP23XX Product Line Programmer's Reference Manual. IXP SDK4. 2. 2004：19-22

[9] Intel Corp. Intel C Compiler for Intel Network Processors Autopartitioning Mode User's Guide. IXP SDK4. 2. 2005：2-13

[10] 肖鸣. 分布式入侵检测系统设计[D]. 成都：电子科技大学，2002

[11] 李千目，张琨，张宏. 一种基于生物免疫学的入侵检测系统. 计算机工程与应用，2003(8)：45-48

[12] Zhang Ke, Liu Naiqi, Chen Yan. Design of Firewall Based on Intel IXP2350 and Autopartitioning Mode C // Lecture Notes in Computer Science. Vol. 3820, 2005：726-731