基于 PKS 体系的网络安全主机解决方案

陆祖宝，田宗秘，张亚坤，余世勇
（北京集智达智能科技有限责任公司，北京 102206）

摘　要： 针对传统网络安全主机普遍采用国外 CPU 及国外的操作系统做为方案，存在后门、漏洞、断供等重大隐患的问题，提出了一种基于 PKS 体系的网络安全主机解决方案，并对不同架构的网络安全主机进行了对比测试，结果显示 PKS 体系网络安全主机能够满足网络安全产品的功能及性能要求，实现网络安全主机可信计算。

关键词： PKS 体系；网络安全；网络安全主机
中图分类号： TN915.08　　**文献标识码：** A　　DOI：10.16157/j.issn.0258-7998.212248

中文引用格式： 陆祖宝，田宗秘，张亚坤，等. 基于 PKS 体系的网络安全主机解决方案[J]. 电子技术应用，2021，47(12)：44-46.
英文引用格式： Lu Zubao，Tian Zhongmi，Zhang Yakun，et al. The solution of network security host machine based on PKS system[J]. Application of Electronic Technique，2021，47(12)：44-46.

The solution of network security host machine based on PKS system

Lu Zubao，Tian Zhongmi，Zhang Yakun，Yu Shiyong
（Beijing Gemotech Intelligent Technology Co.，Ltd.，Beijing 102206，China）

Abstract： In order to solve the problem that traditional network security hosts commonly use foreign CPUs and OS as solutions，which have important hidden dangers such as backdoor，loopholes and interrupted supply，a solution of network security hosts based on PKS system is presented，and the network security hosts of different architectures are compared and tested. The result shows that the PKS system network security host can meet the function and performance requirements of network security products，and realize trusted computing of network security host.

Key words： PKS system；network security；network security host machine

0 引言

网络安全主机是网络信息安全系统的基础，广泛应用于网络入侵检测及防护系统、防火墙系统、安全审计系统、综合威胁探针系统、安全无线防御系统、抗拒绝服务系统、邮件安全网关、安全隔离与信息交换系统、邮件高级防护系统、网络安全高级检测等系统中。

当前这些系统的网络安全主机普遍采用 X86+Windows/开源 Linux 或 NXP QorIQ 通信处理器+开源 Linux 等系统解决方案，硬件、BIOS、OS 都是来自国外厂家，存在“后门”、“漏洞”、“断供”三个致命风险。

研发自主创新的网络安全主机至关重要。在自主 CPU 及操作系统方面，目前可选择的也很多。CPU 方面主要有飞腾、龙芯、海光、兆芯及鲲鹏等，龙芯性能相对弱整体占比小，海光、兆芯主要做服务器端且是 X86 路线，鲲鹏受限供货不足。相较而言飞腾采用 ARM 架构，功耗低，生态较为健全。操作系统方面主要有麒麟、统信 UOS 等。统信 UOS 目前在金融领域有较多应用，在网络安全行业则是麒麟系统占多数。

中国电子集团推出了基于飞腾 CPU+麒麟操作系统的 PKS 体系，可以建立起自主创新安全基座。麒麟操作系统能有效应对“后门”、“漏洞”两大致命风险，而使用国产芯片如飞腾 CPU 正是应对芯片供应链问题的不二选择，它们正是构建网络安全主机的理想选择。

1 网络安全主机的 PKS 体系方案

网络安全主机主要是对以太网数据进行转发及管理，硬件方面主要包括飞腾 CPU、内存、硬盘、TPCM 卡、网卡；软件方面包括麒麟操作系统、DPDK、应用程序。PKS 体系是网络安全主机软硬件的基石，整机框图见图 1。

1.1 采用内置安全的 CPU

研发网络安全主机平台采用 FT-2000/4 或 D2000/8 CPU 两款 CPU，这两款 CPU 支持内置安全机制，支撑系统安全，包括密码加速引擎、可信执行环境、安全存储、固件管理、硬件漏洞免疫、抗物理攻击。在此基础上，网

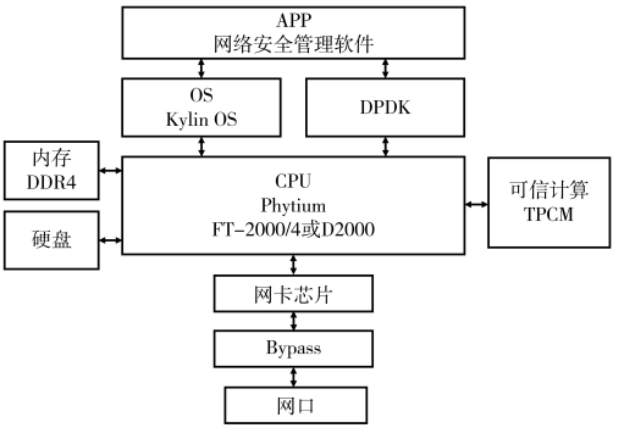

图 1 网络安全主机整体框图

安版还支持安全启动、密钥管理、生命周期管理、量产注入等安全增强机制。

1.2 采用安全操作系统

近几年，国产软硬件不断取得可喜的进步。麒麟软件有着 40 年的研发和 20 年的产业化推广历史，是唯一一个通过 CMMI5 级质量评估的操作系统企业，对 OpenStack 社区的贡献全球第四、中国第一，旗下的银河麒麟操作系统连续 9 年位列中国 Linux 市场占有率第一名，在嫦娥探月、国家电网、北京地铁、航空公司客票系统等都可以看到它的身影，并于 2019 年获得了国家科技进步一等奖。银河麒麟操作系统 V10 拥有六大优势，分别是性能领先、生态丰富、体验提升、云端赋能、融入移动、内生安全。特别是性能方面，官方声称在 UnixBench 2D、3D 测试中，相比同类产品其性能高出 17%，尤其是 3D 方面最高可领先 397%。麒麟操作系统具有高安全、高可靠的优势，符合《GB/T 20272-2006 信息安全技术操作系统安全技术要求》中第四级结构化保护级的要求，是目前我国通过认证的安全等级最高的操作系统，已广泛应用于政府、金融、电力、教育、大型企业等众多领域，为我国的信息化建设保驾护航。

1.3 BIOS 启动

计算机系统中 BIOS 是连接硬件和软件的关键组件，也是系统安全性验证的重要环节，安全主机采用国产 UEFI 并加入可信启动验证，能够确保网络安全主机安全可靠地正常工作及引导系统的工作。

1.4 采用 TPCM 卡可信平台控制模块

FT-2000/4 有网安版的 CPU，可支持可信计算，但是需要专门占用一个 ARM 核来进行可信计算，少一个核对于网络转发及数据处理是很致命的，故采用标准版飞腾 CPU 加上外置可信卡就成为了最好的选择。

可信华泰 TPCM 卡为 M.2 接口，采用 PCIE 进行通信，可以为计算机提供可信根，让可信平台模块具有对平台资源进行控制的功能，具有主动度量功能，实现平台到网络的可信扩展，以确保网络的可信。

1.5 国产化率高

安全主机其他硬件配置方面，电源采用长城 ATX 电源，内存可支持紫光、威捷科等国产 DDR4 内存条，硬盘可选用威捷科、科美、大唐存储等国产硬盘厂家的产品，采用国产高云 FPGA，网卡方面采用的是同样具有自有知识产权北京网迅科技有限公司的以太网控制器，完美支持 DPDK，转发速率可达到线速，在网络安全和网络虚拟化等方面达到较高水平，具有极高的国产化率。

2 网络安全主机设计实施方案

具体的网络安全主机设计方案结构框图如图 2 所示。其中安全主板包括 CPU、内存、TPCM 卡插槽、PCIE 扩展插槽等，安全主板系统设计框图见图 3。

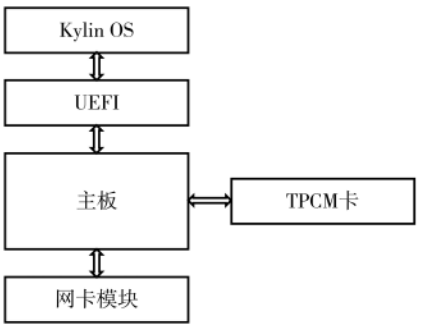

图 2 网络安全主机结构框图

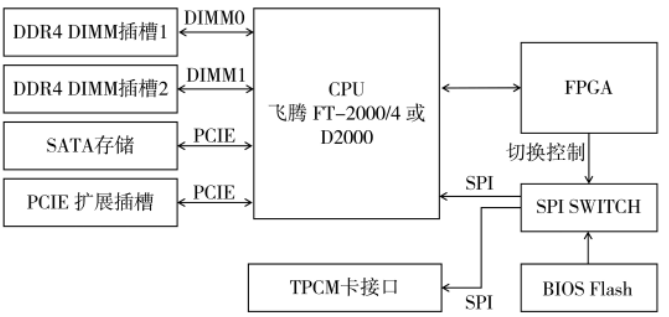

图 3 网络安全主机系统框图

2.1 CPU 模块

CPU 为飞腾公司的 FT-2000/4，主频为 2.6 GHz，支持 ARM v8 64 位指令系统并兼容 32 位指令，支持基于域隔离的安全机制，支持可信启动，集成了 DDR4 内存控制器、PCIE 控制器、SPI/LPC/I²C/UART 等总线接口，集成温度传感器。

2.2 DDR 内存模块

FT-2000/4 支持 2 个 DDR4 通道，最高速率支持 3 200 MT/s。安全主板采用标准的 DDR4 DIMM 条设计，可支持 2 个 DIMM 条，最大支持 64 GB 内存，可以使用 UDIMM 及 RDIMM 内存条。

2.3 SATA 存储模块

安全主板通过 PCIE 转 SATA 芯片，可支持 4 路 SATA 接口。满足客户系统的存储及用户数据的存储，若有需

要加入 RAID 卡后，也可做数据备份。

2.4 可信 TPCM 接口模块

可信 TPCM 模块对安全主机主板的上电控制及启动控制有严格的要求，TPCM 卡的工作流程如下：

(1)安全主机的 FPGA 控制系统上电，并确保 TPCM 卡首先加电同时使 CPU 处于复位状态，TPCM 加电后进行自检，完成状态检查。

(2)FPGA 控制 SPI SWITCH 使得 TPCM 可以读取 BIOS 代码，TPCM 对 BIOS 进行度量，并将度量结果存储在 TPCM 中，在 UEFI 中 CPU 与 TPCM 将会对度量结果进行交互判断。

(3)TPCM 将控制权交给 CPU，TPCM 变为一个控制设备，CPU 通过 PCIE 可以与 TPCM 卡进行高速通信，为计算过程提供密码服务或者可信服务。

为满足这些要求，安全主机主板使用了国产高云 FPGA 对系统电源上电时序及 TPCM 卡进行控制，实现 BIOS 芯片的连接到 TPCM 卡还是 CPU 的切换及 TPCM 卡与 CPU 间通信的逻辑解析。

TPCM 工作流程如图 4 所示。

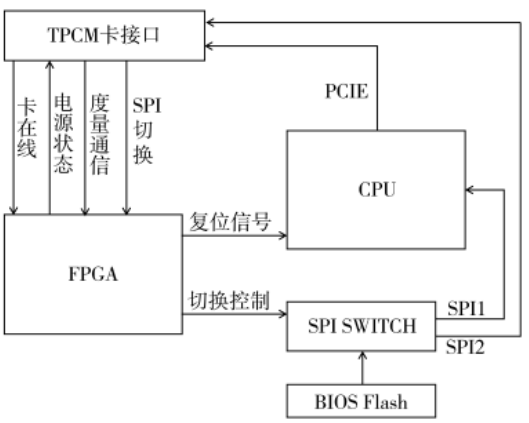

图 4 TPCM 工作流程图

2.5 网卡模块

主板的 PCIE 扩展插槽可以插入网卡模块，网卡模块支持 1 Gb/s、10 Gb/s 等多种不同组合的以太网，采用网讯的 WX1860 及 SP1000A 网络芯片，支持第三代 BYPASS 智能控制。采用标准 PCIE X8 接口定义，客户可以根据现场情况灵活选择网卡型号。

3 网络安全主机性能

网络安全主机的网络性能十分关键，通过对安全主机进行 RFC2544 测试，进行吞吐量、背对背、帧丢失以及帧延迟的网络性能评估，可以验证该方案是否可以满足要求。

我司在多种 CPU 及不同系统平台下，使用网迅 SP1000A 万兆网卡，进行了网络性能对比测试，结果如表 1 所示。

表 1 网络安全主机性能表

CPU	OS	RFC-2544 吞吐量/%					
		64 B	128 B	256 B	512 B	1 024 B	1 518 B
FT-2000/4	Kylin V10	100	100	100	100	100	100
FT-2000/4	UOS Server	90	100	100	100	100	100
Hygon 3230	Kylin V10	93	100	100	100	100	100
INTEL CPU-I7-7700+C236	CentOS-7	100	100	100	100	100	100

由表 1 可见，基于 PKS 体系网络安全主机以太网性能强大，吞吐量都可以到对应速率的 100%，足以满足网络安全行业对以太网的性能要求。

4 结论

综上所述，基本 PKS 体系的网络安全主机方案可应用于网络防火墙、隔离网闸及安全网关等网络安全领域，功能强大，性能强劲，完全满足网络安全主机的要求。

参考文献

[1] 天津飞腾信息技术有限公司.FT-2000/4 系列处理器数据手册(V1.7)[DB/OL].[2021-10-21].https://www.phytium.com.cn/class/122.

[2] 天津飞腾信息技术有限公司.腾锐 D-2000 系列处理器数据手册(V1.2)[DB/OL][2021-10-21].https://www.phytium.com.cn/class/154.

[3] 陈克非，黄征.信息安全技术导论[M].北京：电子工业出版社，2007.

[4] 安葳鹏，刘沛骞.网络信息安全[M].北京：清华大学出版社，2010.

[5] 徐国爱，张淼.网络安全[M].北京：北京邮电大学出版社，2007.

[6] 张玉清.网络攻击与防御技术[M].第二版.北京：清华大学出版社，2011.

[7] 郭帆.网络攻防技术与实战：深入理解信息安全防护体系[M].北京：清华大学出版社，2018.

[8] 王颖.网络与信息安全基础[M].第 2 版.北京：电子工业出版社，2019.

[9] 李冬冬.信息安全导论[M].北京：人民邮电出版社，2020.

[10] 胡俊，沈昌祥，公备.可信计算 3.0 工程初步[M].第 2 版.北京：人民邮电出版社，2018.

[11] GB/T 20976.1-2014 工业控制系统信息安全 第 1 部分：评估规范[S].北京：中国标准出版社，2014.

[12] GB/T 20976.2-2014 工业控制系统信息安全 第 2 部分：验收规范[S].北京：中国标准出版社，2014.

(收稿日期：2021-10-21)

作者简介：

陆祖宝(1986-)，男，本科，高级工程师，主要研究方向：ARM、FPGA 等设计开发。

田宗秘(1983-)，男，本科，主要研究方向：IoT、工业自动化。

张亚坤(1976-)，男，本科，主要研究方向：网络信息安全。

版权声明