Mach-NX：可信系统的基石

首席分析师
Bob Wheeler

2020 年 12 月

www.linleygroup.com

Mach-NX：可信系统的基石

作者：林利（Linley）集团首席分析师 Bob Wheeler

可靠的系统安全机制需要多种方法相结合，并且可信根必须始于安全的引导过程。莱迪思凭借其在该领域的领先地位，推出了新一代 Mach-NX 系列产品，进一步发展了其安全控制平台。这些新器件可以快速应对潜在威胁，保障平台安全，同时简化客户设计。本白皮书由莱迪思赞助，但文中观点和分析均为本文作者所有。

保障系统安全始于固件

为应对当今的各种威胁，复杂的系统需要贯穿整个生命周期的安全机制。这需要从保障供应链安全做起，确保在器件编程、系统制造、运输和安装等过程中系统不会遭到破坏。一旦投入使用，系统还需要安全的 OTA 更新来修补漏洞或更新安全协议。最后，系统还需要安全报废，防止数据丢失。

专注系统安全的传统市场主要包括数据中心、服务提供商和关键基础设施。由于许多攻击可以从系统内部发起，多租户和公共云数据中心的安全机制就变得十分重要，相比之下网络边缘的安全防范就略显过时了。因此，数据中心系统必须能够防御从系统内部发起的软件攻击。攻击目标包括计算服务器、存储系统以及网络交换机和路由器。在服务提供商的网络中，基站、宽带接入设备，路由器和各种网关是也是潜在的攻击目标。即使对用户面数据进行加密，这些攻击也可能危及管理面，从而在系统打开后门。

从广义上讲，工业控制系统包括了那些部署在关键基础设施中的系统，例如国防、公共事业、电网和交通运输等。各国政府很早就采取行动，保护在这些领域中部署的系统的安全，尤其是在恶意攻击者日益猖獗的情况下。然而，网络犯罪分子越来越多地将其他领域的类似系统作为目标以获取经济利益。试想一下勒索软件攻击让工厂陷于停滞将造成多大的损失。另一个攻击目标是汽车，汽车的互连和自动化程度日益提高，许多汽车现在都采取OTA 固件更新。

设备启动的安全性始于固件，而复杂的系统会有多个阶段的启动过程，也形成更大的攻击面。系统固件需要在启动时进行身份验证以及 OTA 更新加密和验证。当系统检测到攻击或故障时，必须能够迅速恢复到稳定和安全的状态。

这些系统中有些采用可信平台模块（TPM）来创建安全地存储加密密钥的可信根（RoT）。但是 TPM 的实现方法差别很大，有的采用专用硬件模块，有的则是基于固件和软件的方法。研究人员已经发现各种实现方式中的漏洞，有些甚至是经过独立认证的方案，并且可 以通过确切的方法利用这些漏洞找到私钥。因此，即便采用 TPM 也无法完全保护所有的系统固件免受损害。

保护、检测和恢复

保护系统固件的方法之一是监控用于读取和写入相关闪存的串行外围设备接口（SPI）信 号。图 1 展示了一个服务器示例，其中南桥（或 PCH）和基板管理控制器（BMC）上都连接了闪存。通过将开关置入 SPI 路径，就可以让可编程逻辑器件（PLD）监控 SPI 信号。PLD 可以根据经授权和未授权访问表来验证指令和地址。检测到未经授权的访问时，它将通过开关阻止指令到达闪存设备。它还可以记录这些活动，便于在 BMC 上运行管理代码。

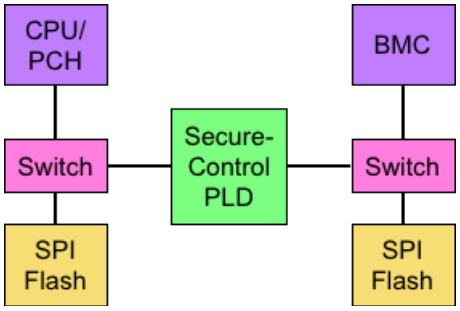

图 1. PFR 系统架构。安全控制 PLD 能够实现 SPI 监控等 PFR 功能和控制功能。

用于保护SPI 访问的PLD 还能实现各类系统控制功能，主要包括电源控制，如上电时序、风扇控制、面板按钮和 LED 以及对功耗、散热以及物理状态的诸多感知功能。由于这些功能大多使用 I2C 接口，PLD 还能为 BMC 缓冲和复用信号。

美国国家标准与技术研究院（NIST）负责开发和制定保障网络和系统安全的算法、协议和框架。该机构最近推出了 NIST SP 800-193 平台固件保护恢复规范（PFR），其核心原则是**保护**平台固件不受损坏，**检测**固件损坏以及将损坏的固件**恢复**到完整状态。

为保护 BMC 和 CPU 的启动镜像，安全控制 PLD 可以在允许关联的主机退出重置状态之前对固件进行验证，包括从闪存读取固件数据、生成摘要、从闪存读取数字签名以及使用适当的非对称加密来验证结果。PFR 规范仅推荐了指定的加密算法，但实际上，由于传统算法需要较长的密钥，因而现在椭圆曲线加密（ECC）成为首选。NIST 的基准要求是等效于 112 位的安全强度，这需要 2048 位 RSA 签名密钥。相比之下，椭圆曲线 DSA（ECDSA）只需 224 位的素数域即可达到相同的加密强度。对于 192 位的等效强度，ECDSA 只需 384 位，而RSA 需要 7680 位。

固件保护还包括经更新验证机制。尽管PFR 规范未做详细规定，但 OTA 更新可以加密进行传输。固件镜像加密采用对称算法，当前的实现则采用高级加密标准（AES）。基准安全强度需要 128 位密钥（AES-128），但如今 256 位密钥在一些对安全性较敏感的应用中更为常见。通过使用AES-256，批量加密超过了 384 位 ECC 哈希（SHA-384）和消息身份验证（HMAC-384）的强度。镜像解密后，可以在写入闪存之前验证其数字签名。

PFR 规范包括了一项可信根检测（RTD）的功能。该功能背后的思路是：对系统固件或关键数据的攻击不应损害 RTD。通过上述 SPI 监控，PLD 不仅能够充当 RTD，还能阻止那些违反预设定的闪存访问规则的攻击。在启动时，它能够通过验证有效的固件镜像检测到入侵。检测到固件受损时，系统优先使用本地存储的固件镜像，恢复到之前经过授权的状态。这里需要注意的是，备份的镜像不能是静态的，因为之前的固件版本可能包括已知的漏洞。

自莱迪思提供实现系统控制功能的 PLD 以来，其芯片、知识产权（IP）和软件快速发展，现在可以将 RoT、系统固件保护以及控制功能集成到单个器件中。新一代 Mach-NX 在久经验证的 MachXO3D 基础上，结合专用 IP、软件和服务，更上一层楼。

Mach-NX 实现强大的加密

为满足安全控制要求，Mach-NX 提供可编程硬核逻辑以及丰富的 I/O。芯片的配置（位流）存储在片上闪存中，该闪存可以管理两个加密的镜像。启动时，主位流在下载到SRAM 的同时会进行验证。如果验证失败，器件可以自动从备份的（黄金版）位流重启。Mach-NX 还包括了通用的用户闪存（UFM），可以用来存储用户的加密密钥。该UFM 大小为 1064Kb 且经过加密，在禁用双引导功能后大小变为 2669 Kb。

安全区域（Secure Enclave）是保障系统安全的重要模块，它可以实现加密协议、真随机数生成器（TRNG）以及为每个器件生成唯一的不可更改的 ID。它还处理包括 ECDSA 和 ECDH 在内的 ECC 协议，最多支持 384 位素域。它还支持使用最大 256 位的密钥进行 AES 批量加密。该区域通过 TRNG 生成公私密钥对，并通过在管理组件传输协议（MCTP）下传输的安全协议和数据模型（SPDM）提供标准的身份验证接口。

如图 2 所示，Mach-NX 添加了一个 RISC-V 硬核来运行管理和控制固件。这一紧凑的 32 位微控制器执行 RV32I 指令集，集成了中断控制器、计时器和 JTAG 调试器。莱迪思此前以软 IP 提供该核，如今采用硬核实现有助于释放可编程逻辑，实现其他功能。Mach-NX 共有 11K 逻辑单元，可用逻辑单元和 UFM 的组合为现场升级提供了空间，满足未来不断发展的安全需求。

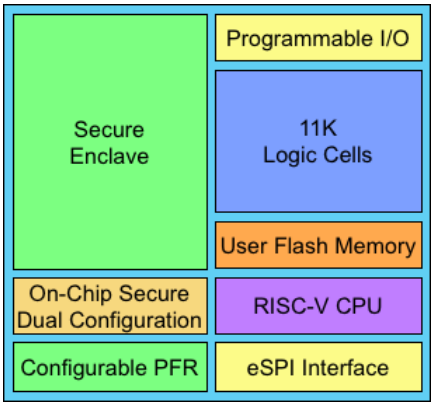

图 2. **Mach-NX 框图。**该芯片包括了硬核 RISC-V CPU、硬核安全模块、闪存、可编程逻辑单元和丰富的 IO。

Mach-NX 的另一个新特性是增强型 SPI（eSPI）接口，它代替了传统的低引脚数（LPC）总线来连接 BMC。eSPI 在 SPI 的电气和时序规范的基础上新增了一层新协议，因此可以向下兼容 SPI。与前代产品一样，新器件包括了实现控制功能的灵活 I/O，最多拥有 379 个引脚，可实现 LVCMOS、LVTTL 和 LVDS 等标准，支持 1.2V 到 3.3V 电压范围。所有封装方案均采用 0.8 mm 引脚间距以简化PCB 布局。

Mach-NX 是基于莱迪思 Nexus 平台的最新产品，采用了三星的 28 nm 全耗尽型绝缘体上硅（FD-SOI）工艺制造。尽管 FD-SOI 以低漏电流著称，但对于大多数安全控制应用而言， 功耗只是次要考量。然而该工艺的另一个好处是大大减少了由辐射引起的软错误。由于器 件配置存储在SRAM 中，因此单粒子翻转（SEU）可能会导致难以恢复的故障。在这种逻辑密度的器件中，FD-SOI 工艺几乎可以杜绝 SEU 的发生。

更加完善的解决方案

为了简化客户的设计，莱迪思通过 IP、软件和各类服务来完善其安全控制平台，实现 PFR 和其他更多解决方案。为了便于使用 PFR IP 来配置 Mach-NX，莱迪思提供了 Propel Builder 这一拖放式的开发工具。PFR 设计中需要的软 IP 包括 SPI 主控、SPI 监控器，I2C 监控器以及 RISC-V CPU 和可编程逻辑之间基于寄存器的接口。SPI 监控器连接外部 SPI 开关，监控 SPI 和闪存之间的访问并阻断未经授权的命令。软核 PFR 模块需要 2.6 K 逻辑单元，剩下的 8.4 K 可用于用户逻辑。

莱迪思还提供在嵌入式 RISC-V 核上运行的固件源代码，作为 Sentry PFR 参考设计的一部分。有三个主要的 PFR 软件组件分别负责安全管理、日志管理和带外通信。每个组件都提供一套应用代码的 API，而低级 API 则提供对软/硬 IP 模块的访问。莱迪思提供了一个应用示例，用于演示保护、检测和恢复功能。Propel SDK 允许客户修改、编译和调试 PFR 固件。

对于生产过程而言， PFR 设计的安全性与供应链息息相关， 因此莱迪思还提供名为SupplyGuard 的安全服务，与 Mach-NX 不可更改的 ID 配合使用。公司为每位客户分配特定的部件号，并使用加密密钥对这些器件进行出厂编程。客户可以使用该密钥以及签名和加密的位流对器件编程。器件的 ID 能够让客户的系统在对合法器件进行编程的同时， 防止对位流的非法读取。这有助于保护位流的完整性以及客户的 IP。如果没有客户专用密钥，就无法对器件重新编程。在这种“锁定”的安全机制下，即便无法确定制造地点的安全性，不无需担心篡改器件的风险。

其他的方案

由于 Mach-NX 的特殊性，它在 PFR 应用中并没有面临正面竞争。如果使用其他厂商的 FPGA，客户就需要获得第三方授权的加密模块作为软 IP。他们需要使用软 IP 实例化 MCU，并将其集成到第三方模块中。大多数FPGA 还需要外部闪存配置存储器。如表1 所示，其他 FPGA 的系统固件认证性能要比 Mach-NX 低得多。验证时间越长，启动时间越长，而启动时间变长会减少系统正常运行时间。许多云服务都包含一项服务水平协议（SLA），规定了系统正常运行的时间。因此启动时间会直接影响 SLA 指标。“五个九”可靠性（99.999%）要求每年的停机时间少于 5.3 分钟，因此系统启动时间在云数据中心十分重要。

	Lattice Mach-NX	其他 FPGAs	BMC
F/W 验证时间*	<5 秒	>15 秒	>10 秒
ECC 支持	硬核 IP	第三方 IP	无
实时 SPI 监控	是	是	否
F/W 恢复时间	<5 微秒	>100 微秒	>100 微秒

表 1. Mach-NX 和其他解决方案的 PFR 功能比较。莱迪思的芯片完美结合了高性能和强大的安全性。* 64 MB 固件镜像和 33 MHz SPI 时钟频率下测得的时间。（数据来源：莱迪思）

当系统固件验证失败时，Mach-NX 可以快速恢复。该器件支持双 SPI 存储器，一个存储主要固件，另一个则可以保存黄金版固件。如果验证失败， Sentry 固件将从主 SPI 切换到副 SPI，继续进行引导过程。然后在后台将经过身份验证的固件镜像复制到主 SPI 闪存中。其他解决方案则必须在引导开始之前复制固件镜像。

另一种 PFR 实现是使用 BMC，但是这种方法有诸多局限。首先，厂商的 BMC 一般不支持椭圆曲线加密，因此它们的验证较弱。其次BMC 依赖于外部闪存，无法规避Mach-NX 和SupplyGuard 可以防止的供应链漏洞。最后，它们不支持SPI 监控，需要使用外部PLD 添加此功能。Mach-NX 可以实现 PFR 以及控制功能，后者在任何情况下都需要 PLD 参与。

最近的一大趋势是客制化的平台安全芯片的发展，但是其中一些是为智能手机设计，如生物识别。谷歌为其云服务器开发了 Titan 安全微控制器。尽管其他的大型云运营商也可以开发类似的芯片，但是多数 OEM 都不愿意承担定制芯片开发所需的巨额资源。莱迪思的客制化解决方案提供了类似的功能，客户无需负担高额的定制芯片开发成本。

结论

莱迪思现在不仅提供 FPGA，还提供全面的安全控制平台，包括优化的芯片、软件、工具和服务。通过在从系统设计到设备报废的整个生命周期内提供安全保护，莱迪思的方案可解决各个阶段出现的漏洞。Mach-NX 基于公司多年的安全控制经验，并在久经验证的MachXO3D 基础上加强了加密功能、升级了 BMC 接口并且提供更多实现自定义功能和现场更新的可编程逻辑。同时，Sentry 参考设计降低了客户对时间和资源的需求，能够快速轻松地将PFR 集成到他们的系统中。

尽管服务器已率先采用了强大的平台安全机制，但随着实时在线的网络连接不断增长，越来越多的系统也暴露在网络攻击之下，安全领域的市场依然在不断扩大。网络和通信设备、工业控制系统、航空航天系统以及自动驾驶汽车等越来越多地成为威胁的目标。莱迪思可以帮助这些领域的客户在从制造到现场升级的整个周期中保障其设计安全。

Bob Wheeler 是林利集团的首席分析师及《微处理器报告》的高级编辑。林利集团为客户提供最全面的微处理器和 SoC 设计方面的分析。我们不仅分析业务战略，还分析技术层面。我们的专题文章涵盖的主题包括嵌入式处理器、移动处理器、服务器处理器、AI 加速器、IoT 处理器、处理器 IP 核和以太网芯片。有关更多信息，请访问我们的官方网站www.linleygroup.com。