全面保障硬件安全

莱迪思半导体白皮书

2019年5月

Jeep被黑客入侵后，140万辆车被召回
FDA召回存在漏洞的心脏起搏器
史上最大规模黑客利用物联网设备的DDOS攻击
至少30亿芯片存在安全漏洞

上述新闻报道有何共同之处？在这些案例中，黑客利用互联网设备存在的漏洞来窃取数据或劫持设备。仅在2018年，超过30亿各类系统的芯片由于硬件攻击，面临数据盗窃、不合法操作和其他安全威胁。未受保护的硬件会威胁系统可靠性和性能，造成不良的客户体验。还会让OEM厂商遭受财务和品牌形象方面的损失，进而影响企业的声誉以及财务状况。

了解更多：

www.latticesemi.com

在线联系我们：

www.latticesemi.com/contact
www.latticesemi.com/buy

目录

OEM厂商通常都有兴趣开发能够解决各类安全威胁（如数据窃取、数据损坏、设备劫持、克隆和设计盗窃）的安全硬件。此外，安全威胁不再局限于使用中的系统。攻击者的目标可能是产品生命周期内任一环节的组件，从最初的组件生产和运送到合同制造商，到系统集成和运行的整个周期都有可能遭到威胁。因此，OEM需要一种能够在系统生命周期的各个阶段保护硬件免受威胁的可靠解决方案。

OEM该如何解决这一难题呢？他们必须使用一个或多个硬件可信根器件作为提供加密功能的平台，保障系统安全。这一过程包括数据加密、数据验证、固件验证、系统验证和代码/配置加密。

可信根器件是保护整个系统的信任链的首要环节。设计人员一旦确认了首个受信任的器件（通常是PLD、FPGA或MCU），它就能作为实现加密功能的基石，保障系统硬件安全。可信根器件必须包含可验证自身配置的硬件，并且应当是首个上电、最后断电的器件。

随着安全威胁的数量和复杂程度与日俱增，系统设计师需要什么样的安全架构呢？首先，任何解决方案都必须足够可靠，以防范现有的或新的固件威胁。为了帮助设计人员评估其解决方案的性能，美国国家标准与技术研究院（NIST）最新定义了一种全新的统一安全机制。NIST SP 800 193平台固件保护恢复准则旨在确保所有的系统固件都有可信根保护。

该标准的开发人员强调以下三个原则：

- 保护：通过访问控制保护非易失性固件存储器
- 检测：加密检测，防止从恶意代码启动
- 恢复：如果遭到破坏，恢复到最新的可信任固件

引擎的选择

理想状况下，实现硬件安全的引擎应当具有功耗低、设计灵活性高、可拓展、物理尺寸小等特点。MCU固然可以提供不错的计算资源，但通常不具备能够帮助其他系统处理器或组件启动所需的全面功能。此外，MCU一旦运行，它就难以监测自身的启动存储器。

现场可编程门阵列（FPGA）相对于MCU有着显著优势。FPGA通常作为首个上电和协调系统启动的器件，并在协调系统关闭后，最后断电。最先上电/最后断电这一特性让FPGA成为快速构建可信根的理想选择。设计人员可以利用FPGA的并行特性来同时检查多个存储器，从而显著缩短启动时间。与MCU不同之处在于，FPGA可以通过实时监控保护非易失性存储器。最后，在系统损坏的情况下，FPGA可提供启动固件恢复所需的逻辑和接口。

莱迪思MachXO3D – 全面保障硬件安全的可信根FPGA

为满足各类应用日益增长的固件安全需求，莱迪思最新宣布推出MachXO3D FPGA，这是首款用于系统控制应用的小尺寸、低功耗FPGA，可以在计算、通信、工业控制和汽车等各类应用中保障系统固件安全。这款新器件通过在产品整个生命周期内实现全面、灵活、可靠的硬件安全系统，帮助OEM防范数据窃取、数据篡改、设计盗窃、产品克隆、过度构建、设备篡改和劫持等问题。

全新的MachXO3D与莱迪思备受欢迎的MachXO3系列（广泛用于各类控制PLD应用）引脚兼容，将成为莱迪思产品系列中实现安全固件应用的重要控制PLD选择。

简化集成

确保轻松实现固件安全是设计MachXO3D时的重点考虑因素。莱迪思的设计师希望设计人员能够方便地使用这款新器件。由于超过50%的通信系统和服务器都采用基于MachXO架构的控制PLD，所以该新款器件经专门设计，与原有架构引脚兼容。这有助于让开发人员对现有的控制解决方案进行改进或增添新的安全功能。目前对于这些全新安全特性的需求正不断增长，且MachXO架构也早已普及，已有超过五家领先的服务器OEM开始与莱迪思合作，着手进行MachXO3D的相关设计。由于开发人员经常使用MachXO3器件作为最先上电和最后断电的组件，他们可以快速建立信任根和信任链，不必担心其他组件是否先于莱迪思PLD之前启动。

实现灵活的安全机制并保持系统完整性

- 关键基础设施的大多数控制PLD都采用MachXO架构开发
- MachXO3和MachXO3D引脚兼容
- MachXO3D是用于简单信任链实现的最先上电和最后断电的器件
- 5家服务器OEM已着手采用MachXO3D设计

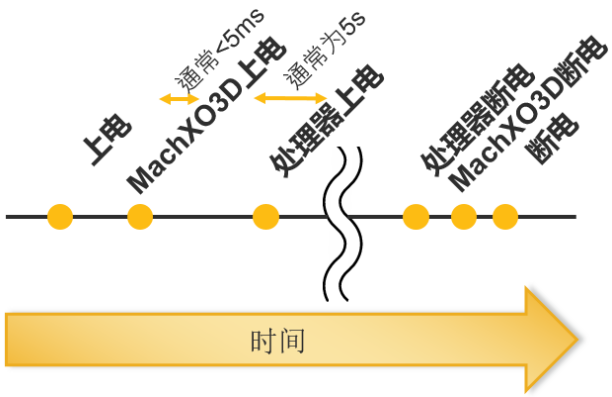

图 1

全面保障安全

为应对日益严峻的硬件安全问题。莱迪思增强了MachXO3D FPGA的控制PLD功能，其中的嵌入式安全模块提供了开发人员解决多种安全威胁所需的硬件可信根和硬件加密功能。

- MachXO3D对位流进行加密，确保设计安全性，防范IP盗窃。
- 为保护OEM的营收和品牌声誉，该器件新增了安全ID，可以与其他安全功能配合，进行器件/平台验证。
- 椭圆曲线加密、公钥/私钥功能和AES加密/解密能有效防止数据盗窃。
- 椭圆曲线验证和签名生成提供验证固件和通用数据的基石。

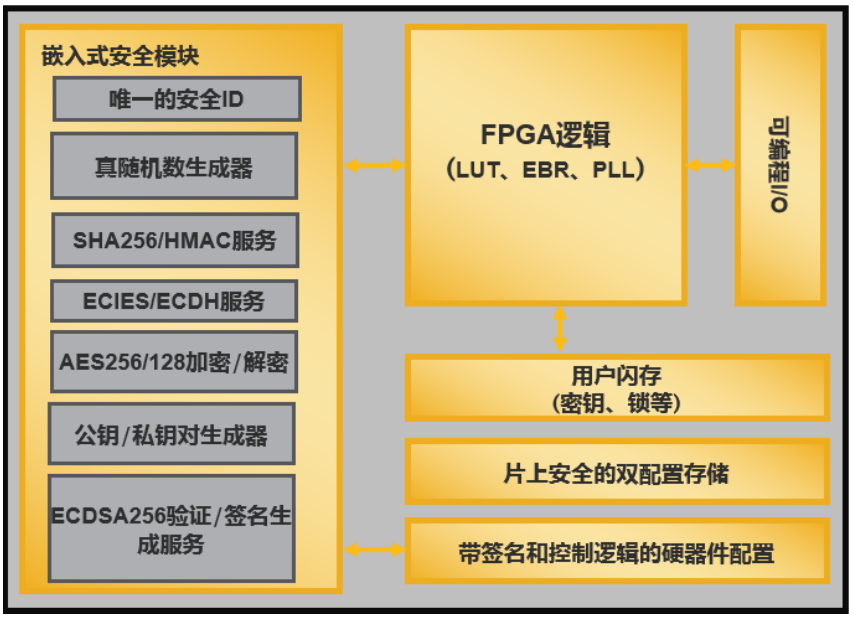

图2：MachXO3D 架构

符合NIST标准的可靠设计

MachXO3D设计非常可靠，是业界首款符合NIST SP 800 193平台固件保护恢复（PFR）准则的控制FPGA。该器件可通过访问控制保护非易失性存储器，加密检测并防止从恶意代码启动，且在固件遭到破坏时能恢复到最新的可信任固件。此外，MachXO3D随时可以动态重新配置I/O端口，从而最小化系统的攻击面。

灵活的设计实现

设计灵活性也是一个关键考虑要素。莱迪思的大多数客户都希望在设备部署完毕后，在XO架构上实现升级。这种可重新编程的特性有助于动态控制攻击面，还能让用户轻松地更新FPGA，应对最新的固件攻击。因此，莱迪思的设计人员希望在提供可靠安全性能的同时，保证可编程特性。

为了应对这种多样化的需求，MachXO3D新增了两个关键特性。作为硬件化的配置引擎的一部分，该器件支持代码验证，确保了每个载入的配置都有合法的数字签名。与此同时，MachXO3D额外增添了片上闪存，可以随时存储器件的两套配置。这种双引导功能能让系统在出现问题时默认使用备份配置。

典型应用

MachXO3D旨在满足多个市场的各类应用需求。潜在应用包括5G无线通信设备，如交换机和路由器、服务器和企业计算机、工厂自动化和工业IoT设备。

下列框图描述了MachXO3D在安全服务器中的典型应用，其中包括了一个基板管理控制器（BMC）、一个主CPU和多个辅CPU或FPGA。通常情况下，一片被称之为控制PLD的小型FPGA管理板上的所有复位和电源控制。所有的处理器从SPI或Quad SPI存储器启动。开发人员现可以使用MachXO3D作为上述小型FPGA，并新增开关，实现服务器安全升级。这种配置允许FPGA自行启动，然后验证每个SPI存储器，随后释放这些组件开始启动（假设存储器正常且签名合法）。如果SPI存储器出现问题，MachXO3D可以根据用户偏好进行下一步操作，如关闭系统或尝试从其他来源重新配置。系统启动后，MachXO3D还会监控对各个SPI存储器的访问，防止未经授权的写入。

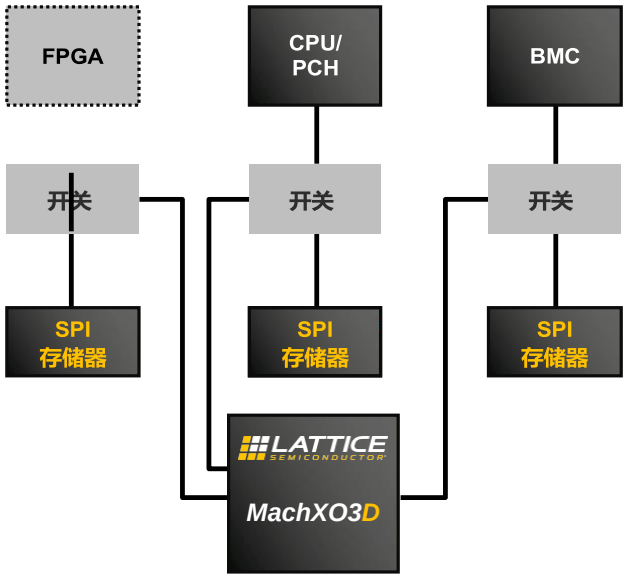

图 3

整个生命周期内的安全保障

为满足产品整个生命周期内日益增长的安全需求，莱迪思优化了其器件生产时的测试集成流程，以支持使用公钥加密技术在未受保护的环境中对器件进行安全编程，让每个器件在其整个生命周期内都能保证安全。这一新功能确保了客户的器件从离开莱迪思工厂直到报废的整个过程都将保持安全。

结论

如今的数字系统面临着前所未有的攻击。黑客会利用系统漏洞来窃取数据和设计、篡改、劫持或克隆产品。这些攻击出现在产品的整个生命周期。仅在2018年，对未受防护的固件进行的攻击就导致计算、通信、工业控制和汽车系统中高达数十亿IC面临安全威胁。最终，容易遭到入侵的硬件就会对OEM厂商的财务状况和品牌声誉产生不良影响。

设计人员如何解决这一威胁，保护他们的系统呢？答案就是使用硬件可信根和信任链技术实现全面、灵活、可靠的安全系统。莱迪思全新的MachXO3D FPGA具有的硬件可信根和双引导特性可以帮助他们增强安全控制功能，同时，该款器件可极大简化安全解决方案的实现，在整个生命周期保障组件安全。

了解更多：

www.latticesemi.com

在线联系我们：

www.latticesemi.com/contact
www.latticesemi.com/buy