企业服务器固件安全保障的新方法

莱迪思半导体白皮书

2018年11月

根据新的NIST SP 800 193标准、在硬件上使用基于FPGA的可信根器件来实现平台硬件保护和恢复 (PFR)，可让服务器固件免受网络攻击，保护性能更上一层楼。莱迪思全新PFR开发工具套件能够简单快速实现基于FPGA的PFR解决方案。

了解更多：

www.latticesemi.com/PFR

在线联系我们：

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

公司地址：

Lattice Semiconductor
111 5th Ave., Suite 700
Portland, Oregon 97204
United States

Phone: 1 (503) 268-8000

版本 1.0 WP0016C

目录

概述

典型的企业服务器包含多个处理组件，每个组件使用各自的非易失性SPI Flash缓存来保存其固件（即上电后处理组件立即启动所需的软件）。尽管使用闪存很方便现场升级和修复问题，但同时也容易遭受恶意攻击。黑客可以未经授权就访问固件，在组件的闪存中植入恶意代码。这些代码能够轻易躲过标准的系统检测手段，即便是进行更新或更换硬盘也无法解决，从而对系统造成永久性破坏。

为解决这一问题，一些处理组件采用集成在芯片上的硬件电路来检测未经授权的固件修改。然而，电路板上其他未采用此种方案的处理组件还是缺乏有效保护，整个服务器仍然易受攻击。美国国家标准与技术研究所（NIST）最近发布了2018年NIST SP 800 193标准，定义了一种标准的安全机制，称为平台固件保护恢复（PFR），它主要基于以下三个指导原则：

保护

保护固件免受攻击

检测

检测SPI闪存中受损的固件

恢复

使用已知完好的固件版本替代受损的版本进行恢复

PFR功能主要依赖外部的硬件（芯片）带有“可信根”（RoT）的器件。使用基于FPGA的RoT器件实现PFR解决方案比使用基于MCU的可信根器件更安全、扩展性更好、系统可靠性更高。莱迪思推出的全新PFR开发套件能让服务器的原始设备制造商快速为其现有设计增加PFR功能，并充分利用这一强大的安全技术带来的优势。系统架构师和系统集成商如今可以更为方便地设计、实现和维护符合PFR标准的FPGA RoT器件，而无需拥有专门的安全专业知识。

易受网络攻击的服务器固件

预计到2021年，网络攻击犯罪造成的损失将达到6万亿美元[1]。网络黑客不断寻找规避安全措施的新方法，旨在：

- 偷看或窃取存储在服务器上的专有数据（信用卡号、公司知识产权等）
- 绕过服务器偷看或窃取数据
- 劫持服务器，对其他目标进行DDoS攻击
- 通过让服务器的一个或多个硬件组件无法运行，从而对其造成破坏（称之为“变砖头”）

由于操作系统和应用会定期更新，以便加入新功能或修复漏洞，它们很容易成为黑客入侵服务器的最大目标。于是，组织的安防资源和战略一般会倾向于保护操作系统和应用软件。然而，入侵服务器还有另外一个较少为人所知的攻击载体：固件。

固件是指服务器组件（即CPU、网络控制器，片上RAID解决方案等）率先上电后立即执行的第一个启动代码。组件的处理器假定固件为一个有效可靠的起点，从中启动并根据服务器的配置使用它来分阶段验证和加载更高级别的功能。在某些情况下，处理组件在其整个运行周期内使用固件执行所需的功能。

国际信息系统审计协会（ISACA）2016年的一份调查显示，在那些声称将硬件安全视作组织头等大事的受访者中，超过半数“报告了至少一起受恶意软件影响的固件被引入公司系统的事件”，并且17%的受访者表示“这些事件造成了实质性影响。[2]”

固件安全状态

服务器固件可能在供应链的各个不同阶段遭到入侵，包括：

- **在原始设备制造商处：**在生产过程中操作人员恶意植入受感染的固件
- **在系统集成商处：**在根据客户要求配置服务器时安装未经授权的固件
- **转运到客户的过程中：**黑客可以打开服务器包装，通过线缆下载未经授权的固件，将恶意代码植入组件的SPI存储器中
- **现场运行过程中：**黑客可以利用固件的自动更新，将可绕过任何现有保护机制的伪造固件替代正常的更新

典型的服务器主板目前都使用至少两种标准的固件实例：统一可扩展固件接口（UEFI）和基板管理控制器（BMC）。尽管这些接口能对固件起到一定的保护作用，但也非常有限。

统一可扩展固件接口 (UEFI)

UEFI (之前称为BIOS) 是负责将服务器固件载入操作系统的软件程序。UEFI在生产过程中就已经安装就绪，用于检查服务器有哪些硬件组件、唤醒这些组件并将其交给操作系统[3]。这一标准通过一种称之为安全启动的过程检测未经授权的固件，如果检测到未经授权的固件，该安全机制就会阻止硬件组件启动[4]。然而，安全启动的实现和支持因组件和供应商而异，这会导致组件安全性能出现漏洞，从而被黑客利用。此外，如果非法固件设法绕过了安全启动，UEFI就无法将组件的固件恢复到上一个经授权的版本并继续运行。

基板管理控制器

基板管理控制器是母板上的一种专用微控制器 (MCU)，通过独立的连接与系统管理员通信以及使用传感器来监控 “计算机、网络服务器或其他硬件设备[5]” 。许多BMC会筛查各自的固件安装情况以确保固件的合法性，但是对于其他的服务器固件则无能为力。BMC无法阻止恶意代码攻击电路板上的其他固件。例如，如果恶意代码被植入组件的SPI存储器未使用的分区，那么BMC则无法阻止代码进入服务器的整个代码流。

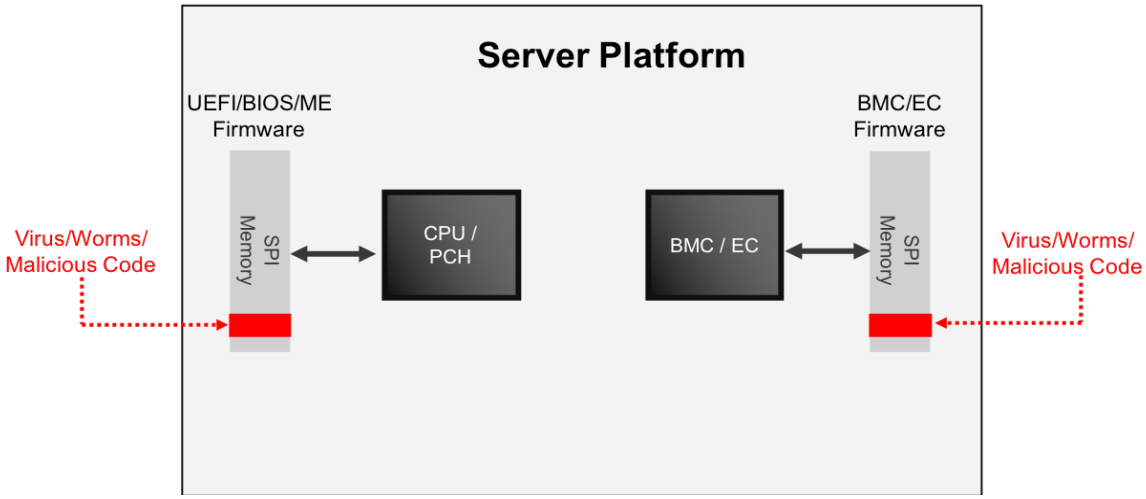

图 1 : 统一可扩展固件接口和基板管理控制器接口只能提供有限的固件保护

平台固件保护恢复 (NIST SP 800 193标准)

为解决当前固件标准的安全问题，美国国家标准技术研究所 (NIST) 于2018年5月发布了一项新标准，为包括UEFI和BMC在内的所有固件提供全面保护。这一被称为PFR的NIST SP 800新标准旨在 “提供技术指导和建议，支持平台固件和数据的恢复，预防潜在的破坏性入侵。[6]” 它提供了一种保护系统中所有固件的统一方法，并且可以配置为对正常系统操作不具有侵入性。一旦确定未经授权的固件正在尝试安装，它则会停止任何相关组件。并且PFR还相对于各个组件可能支持的任何安全功能独立运行。

该标准概括了保护固件的三大关键原则：

- **保护** – 通过阻止对组件SPI存储器的保护区域实施未经授权的写入或者清除全部或部分固件的恶意行为，从而确保组件的固件处于稳定状态。在有些情况下，甚至对保护区的读取的操作也是禁止的。
- **检测** – 在组件的处理器从固件启动之前，可以先验证来自原始设备制造商的固件更新包。若检测到固件有破坏或未经授权，则启动恢复过程。
- **恢复** – 若检测到固件被篡改或被破坏，处理器将从上一个可信固件版本（即“黄金镜像”）启动，或者通过可信进程获得新的固件，启动全系统的恢复。

PFR需要基于硬件的可信根

根据NIST的这一标准，实现安全的PFR功能需要可信根（RoT）器件对服务器的固件执行保护、检测和恢复操作。符合NIST标准的RoT器件必须在启动之前、且不借助任何其他外部组件的情况下对其固件进行以上操作。

硬件RoT解决方案必须拥有以下特点：

- **可扩展** – RoT器件必须通过外部SPI镜像实现保护、检测和恢复功能，同时具备毫微秒级响应速度。这需要专用处理和I/O接口，保证服务器的性能不受影响。
- **不可绕过** – 未经授权的固件不能绕过RoT器件，从而无法从受损的固件启动服务器。
- **自我保护** – RoT器件必须动态地应对不断变化的攻击面（设备或系统中未经授权的用户可以访问的所有节点），保护自身免受外部攻击。
- **自我检测** – RoT器件必须能够使用不可绕过的加密硬件模块检测未授权的固件。
- **自我恢复** – 当设备发现未经授权的固件时，RoT器件必须能够自动切换到上一个黄金固件映像，确保服务器继续运行。

保护	启动前是否检能测有缺陷的固件？	是否能从有缺陷的固件中恢复？	运行期间是否保护所有固件在系统内部更新过程中免受攻击？
UEFI嵌入式方案	是	否	否
BMC嵌入式硬件模块	是	否	否
使用可信根的NIST PFR	是	是	是

图 2：当前的固件标准无法在所有操作阶段保护组件固件

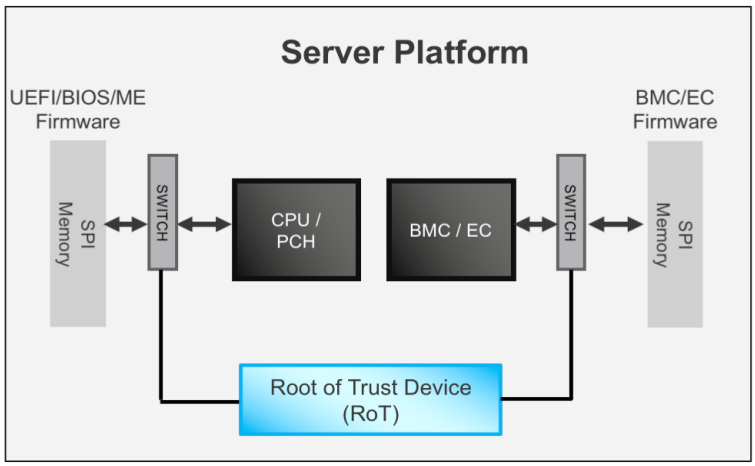

图 3 : NIST SP 800-193标准 : 平台固件保护恢复

如图3所示，RoT器件首先上电，并通过加密方式检查所有组件的固件，以及是否有未经授权的修改。若RoT器件检测到任何破坏，则启动可信固件恢复过程。在极端情况下，若电路板上的所有固件全部受损，RoT器件还可以利用存储在该器件中的可信固件进行全系统恢复（通过BMC）。BMC从可信固件启动后，从系统外部取得已知可信的固件替代被破坏的固件版本。RoT器件随后再次验证所有固件，然后启动电路板的上电程序，在此过程中板上所有组件都将上电，并强制从已知的完好固件镜像中启动，最后开始正常工作。

为保证SPI存储器不再遭受入侵，RoT将主动监测SPI存储器和对应处理器之间的所有活动，发现恶意更新固件的行为后，阻止安装更新。

实现符合NIST标准的PFR解决方案

PLD上实现可信根的难点在于，实现方案的同时不给原始设备制造商带来过大的负担。可信根硬件解决方案（包括基于PLD的解决方案）必须可扩展，也就意味着它能够保护服务器上的所有固件，同时响应时间达到毫微秒级。它还要能够使用不可修改的加密模块，通过加密检测来确定固件是否遭到篡改。将PFR与服务器所有组件完整的启动时序控制功能相结合，RoT就变得不可绕过。最后，解决方案还应能够自动切换回最近的黄金固件镜像，以便在发现当前固件被破坏时服务器可以继续运行。

按照定义，基于硬件的RoT器件自然需要在芯片中实现。在此情况下，最常用的芯片平台即微控制器（MCU）和现场可编程门阵列（FPGA）。在充分考虑到FPGA和MCU的运行特点和特性后，我们发现FPGA在很大程度上更适用于PFR解决方案。

使用MCU实现可信根

MCU过去常在服务器硬件产品中用于构建可信根。简单来说，就是保留MCU层的一部分为可信执行环境。MCU的这一部分与芯片的其他区域保持物理隔离，并持续监控固件，确保其获得授权并正常工作。通常来说，服务器上的PFR功能是通过向现有的硬件架构上添加RoT MCU实现的。

MCU通常难以支持验证服务器中的多个固件实例。这是因为它无法在没有外部设备（如PLD）的帮助下响应对服务器所有固件实例的系统内部攻击（而PLD能实时监控SPI存储器的流量并同步检测和响应入侵行为）。

如图4所示，使用MCU实现PFR的三个组件为：

- **RoT MCU** – RoT MCU执行检测、恢复和保护功能；它是实现RoT的核心组件。
- **保护PLD** – 通过实时监控所有组件处理器与其SPI存储器设备之间的活动，大规模实现PFR，全面保护电路板。
- **控制PLD** – 该器件集成了所有电路板级的上电和复位时序功能，包括风扇控制、SGPIO、I2C缓冲、信号集成和带外通信等启动主板必须的功能。RoT MCU命令控制PLD为电路板上电。若需要在极端情况进行恢复，RoT MCU则命令控制PLD仅为可信恢复过程中使用的部分电路板供电。

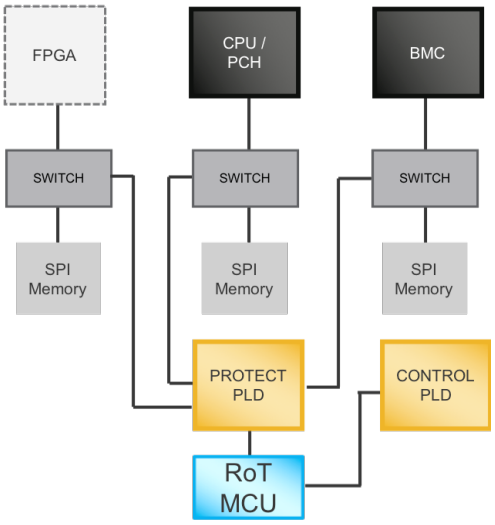

图 4：如果需要各组件同时启动，那么符合PFR标准、使用MCU作为可信根的服务器还需要额外的组件（FPGA）来提供必要的高性能；在大规模的服务器应用场景下，此种解决方案不可扩展

这种基于MCU的PFR方案有诸多限制。例如，图4电路中使用的控制PLD无法保护自身固件，也就意味着这种架构并非完全符合NIST PFR的要求。控制PLD的代码仍有可能被修改，让RoT MCU失效。还有可能受到永久拒绝服务攻击（PDoS），通过删除这些PLD上的信息，让系统无法运行，从而使让服务器无法启动。保护和控制PLD存在的安全漏洞使得组件在运输或者系统集成过程中很难防止对固件的攻击。为了达到NIST SP 800 193标准，RoT MCU必须同时为控制PLD和保护PLD实现PFR功能。而使用MCU在这些器件上实现恢复和保护功能非常困难。最后，基于MCU的方案需要额外的系统级进程来检测试图绕过整个RoT电路的攻击行为。

使用FPGA实现可信根

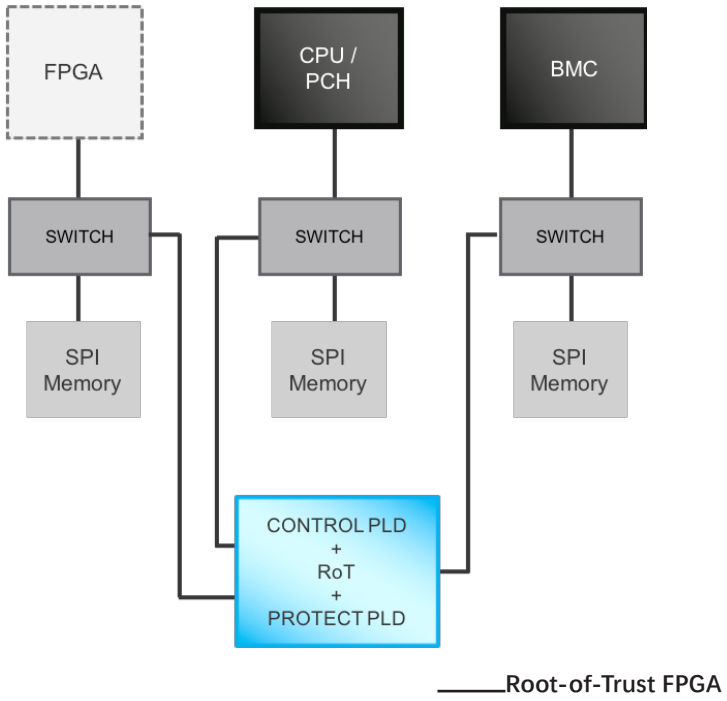

图 5：RoT FPGA解决方案将RoT MCU、控制PLD和保护PLD的功能集成在单个芯片上，不仅可靠、易扩展，而且不可绕过。在拥有符合PFR标准的PLD的服务器上，PLD的性能足以并行监测所有组件的固件而无需使用额外的FPGA

基于可信根FPGA的PFR方案的优势

正如其名，可编程逻辑电路 (PLD) 是一种几乎可以瞬时实现远程重新编程的集成电路，以适应不断变化的场景。PLD可以在硬件层面上改变其电路，因此一旦检测到未经授权的固件，该固件就无法安装。

由于PLD被设计为可重新编程，因此比MCU有更多的I/O接口，这让它们可以并行运行多个功能而非按顺序执行。 因此它们在检测未授权固件时，识别和响应速度更快。

此外，PLD使用了先进的仿真软件，让工程师得以验证其PLD设计的功能。工程师还可以使用这一工具来测试其针对各种固件的网络攻击的设计是否可以保护PLD自身。与PLD相比，MCU的固件更新需要更复杂的测试和验证，因为MCU不能通过仿真支持功能验证。相反，MCU固件的任何更新都必须经过多次回归 (试错过程) 测试，以确保新固件不会对MCU中的其他功能产生不良影响；这一过程远比运行PLD仿真软件繁琐。

当我们对比PLD和MCU的特点时，会发现PLD能提供性能更优、更为可靠的平台实现基于硬件的可信根；它也成为满足PFR标准的必要器件。

应对供应链攻击：MCU vs. FPGA PFR解决方案

如果出现固件攻击，两种不同类型的PFR系统将采取以下应对措施（按照实施顺序）：

RoT MCU	RoT FPGA
检测：RoT MCU对所有的SPI存储器设备按顺序执行加密检测，以检测是否存在未经授权的固件。 遭受入侵的控制PLD（在供应链环节）可以绕过RoT MCU的检测，让BMC从受损的镜像启动。	**检测：**RoT FPGA对所有的SPI存储器设备按顺序执行加密检测，以检测是否存在未经授权的固件。FPGA在其片上非易失性存储器中记录故障情况用于之后的分析。RoT FPGA可保护自身免受来自供应链环节的攻击。
若检测到受损的固件，恢复过程则由管理启动源SPI存储器的保护PLD，或通过控制或保护PLD启动并由RoT MCU监控。	基于FPGA的系统将此功能集成到其硬件中。RoT和Control PLD之间不需要进行外部通信。这使得解决方案更加可靠且不再受外部攻击影响。
服务器完全启动后，保护PLD会主动实时监视所有的SPI活动以阻止后续攻击，并在检测到入侵时通知RoT MCU。	最终的解决方案更简单，完全符合NIST的标准。

PFR开发套件简化FPGA可信根方案的实现

莱迪思现提供一款PFR开发套件，可简化FPGA RoT解决方案的实现。服务器组件的原始设备制造商和系统集成商如今可以快速实现基于FPGA的PFR，满足上市时间的要求。该套件包括一个软件功能库、相关的IP和3个开发板，用于实现PFR（包括保护PLD功能）。用户可以通过Lattice Diamond软件工具将电路板控制PLD功能添加到RoT FPGA设计中。莱迪思PFR开发套件和开发板包括：

- 一个RoT FPGA开发板
- 一块运行Python脚本的ECP5 FPGA板，用于模拟服务器的BMC。开发人员可以通过Python脚本执行命令来模拟对组件SPI存储器的攻击。
- 一个PFR适配卡，用于在SPI存储器中存储BMC代码。在开发板的RoT FPGA中实现的PFR功能可以保护PFR适配卡固件免受攻击（意味着基于FPGA的该解决方案符合NIST PFR标准）。

莱迪思套件让用户能够设计、实现和维护符合NIST标准的自定义PFR方案，而无需专门的安全专业知识。

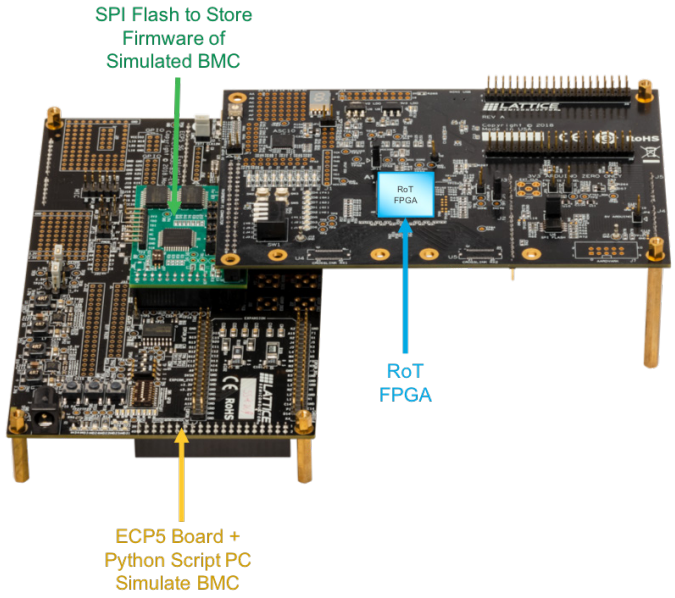

图 6：Lattice FPGA RoT开发套件拥有三块开发板：RoT FPGA开发板，用于模拟服务器BMC的ECP5开发板和用于存储模拟BMC固件的SPI闪存板

小结

对于涉足数字领域的企业和组织而言，网络安全是个至关重要的问题。如今黑客会通过攻击企业服务器固件来获取未经授权访问服务器数据的权限，或者直接让服务器永久瘫痪。而通过基于FPGA的RoT器件实现的PFR则能有效解决这一难题，提供安全可靠、容易扩展、全套完备的方案，在供应链的任何环节保护服务器组件的固件。全新的莱迪思PFR开发套件为加速和简化RoT器件的开发提供了便捷途径，确保你的服务器安全无虞。

---

[i] https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html
[ii] http://www.isaca.org/Knowledge-Center/Research/Documents/CSX-Firmware_whp_eng_1016.pdf?regnum=461390
[iii] https://whatis.techtarget.com/definition/Unified-Extensible-Firmware-Interface-UEFI
[iv] https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot
[v] https://searchnetworking.techtarget.com/definition/baseboard-management-controller
[vi] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf

了解更多：

www.latticesemi.com/PFR

在线联系我们：

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

公司地址：

Lattice Semiconductor
111 5th Ave., Suite 700
Portland, Oregon 97204
United States

Phone: 1 (503) 268-8000