浪潮服务器
安全技术白皮书

浪潮电子信息产业股份有限公司
2021年3月
www.inspur.com

目录

CONTENTS

1 概述

随着云计算、大数据、互联网+、信息安全等先后上升为国家战略，云服务商业模式趋于成熟，机器学习、人工智能、大数据的发展催生了服务器各类应用场景。作为提供计算服务的重要基础设备，服务器自身存在一定的脆弱性，并且面临着自然和人为等诸多因素的潜在威胁，为应对各类安全风险，浪潮服务器从硬件、固件、配套软件等层面进行安全架构设计，实现了服务器保密性、完整性、可用性及不可抵赖的安全目标。

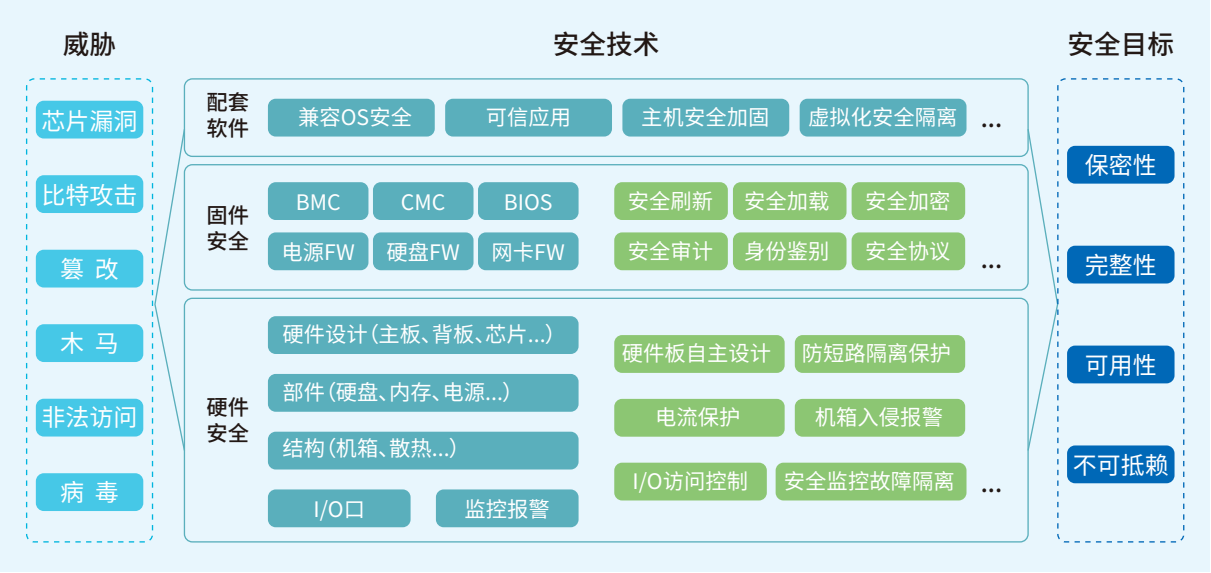

图1-1 服务器安全架构图

1、威胁分析

服务器目前面临的主要威胁分析如下：

目标	脆弱性	威胁	安全技术
机密性保护	弱口令，缺少访问控制机制	非法登录，越权	身份标识与鉴别， 授权与访问控制
	电磁泄露，电磁干扰	利用射频攻击进行窃密	硬件安全设计， 可靠运行支持
	默认开启不安全端口	端口入侵	安全加固
完整性保护	重要信息未加密， 文件缺少保护措施	信息未授权访问， 破坏文件的完整性	数据加密，硬件安全模块
	固件及其存储区域未进行保护	破坏固件的完整性/合法性	BIOS Secure flash

可用性保护	固件设计缺陷，固件配置漏洞	植入固件木马，刷恶意固件镜像，远程非法开机，通过固件攻击硬件等，破坏可用性	固件安全更新，BMC安全启动，BMC备份恢复，BIOS Boot guard，PFR，日志审计
	操作系统和应用软件漏洞	木马入侵，网络窃听，病毒威胁，拒绝服务攻击，后门威胁	BMC Web安全技术，BIOS Secure boot，主机安全加固，可信应用，虚拟化安全
	协议存在安全缺陷	缓冲区溢出攻击，假冒，中间人攻击，网络安全威胁	安全协议，安全加固
	PCI/USB/RJ45/IIC/JTAG接口	进行比特攻击，构建隐蔽通道，使物理隔离措施失效	故障定位，安全监控

2、安全技术架构

为实现服务器产品的安全目标，浪潮服务器安全技术架构涵盖硬件安全、固件安全等层面，并结合配套软件安全方案共同构筑服务器安全，以应对其所面临的攻击和威胁。

硬件安全：硬件板卡安全设计、结构安全、部件安全、I/O安全、安全监控等；

固件安全：安全更新、安全加载、安全加密、备份恢复、认证鉴权、访问控制、安全协议等；

配套软件安全方案：OS安全、可信计算技术应用、虚拟化安全、主机安全加固等。

2 服务器硬件安全技术

2.1 硬件安全模块

(1) TPM/TCM可信模块

支持TPM/TCM可信模块，构建信任链，实现服务器的可信引导。

以可信模块TCM/TPM2.0作为安全的信任根，实现BIOS的主动度量，再到硬件平台、操作系统和应用等，一级度量认证一级，构建起一条完整的信任链。通过对系统平台组件的完整性度量，确保了系统平台完整性，并向外部实体可信地报告平台完整性，从而确保了整个系统平台的安全与可信。

(2) 加密模组

部分机型支持TPCM、密码卡等加密模组，保护数据安全，实现敏感数据的增强保护。服务器中数据安全保护包括平台自身敏感数据的保护和用户敏感数据的保护。利用TPCM、加密模块保护系统平台敏感数据，从根本上解决敏感数据易受攻击的安全问题，实现对敏感数据在存储、传输、处理等全过程的增强保护和管理。

2.2 故障定位技术

为方便用户或运维人员快速发现和解决服务器问题，确保服务器能够持续稳定的工作，内存/CPU和磁盘等服务器关键部件都具备故障定位机制。基于IPMI规范的BMC具有故障定位功能和故障日志记录功能。

(1) 内存/CPU故障定位

利用主板BMC进行内存/CPU故障定位和记录功能，在内存发生可纠正ECC错误或不可纠正ECC错误时，或某个CPU发生故障时，主板BMC可以记录内存/CPU信息，并记录故障发生的内存槽位和CPU编号，从而快速定位有故障的内存/CPU位置。

(2) 磁盘故障定位

通过查看硬盘状态指示灯、阵列状态或收集ADU报告来查看硬盘错误。其中，ADU报告详细记录了当前硬盘的工作状态、报错代码等信息。

2.3 安全监控技术

在安全监控技术方面，机箱面板进行了锁扣设计，机架服务器进行了上盖锁扣设计，当有未经授权的开盖操作时，通过BMC进行入侵检测和报警等。

(1) BMC监控范围

BMC为基板管理控制器，通过系统管理总线与LAN接口模块通信，实现网络连接，用户可通过网络访问实现对远程服

务器的带外管理功能。通过Serial/Modem接口连接Modem，在远程服务器宕机的情况下，用户可以通过拨号访问获取SDR、SEL数据，分析诊断故障原因；通过IPMB接口访问风扇基板、电源基板等上面的管理控制器，实现对基板的温度、电压、风扇转速等关键参数管理。

BMC会收集有关系统健康和系统状态的信息，当有严重事件发生时可以执行控制操作。通常系统健康监视功能是通过数字传感器实现的，它能监视不同的系统电压、温度和风扇速度。BMC采用主动查询的方式发现是否存在超出范围的传感器，为了使监视工作切实有效，BMC可以配置不同的门限值。例如，当BMC监测温度超过某个告警门限时就会提高风扇速度，如果降温措施未能适时奏效，当温度超过另一个紧急门限时，BMC会切断系统电源、记录事件过程并通过LAN或串行调制解调器向远程终端发送告警信息，如图2-1所示。

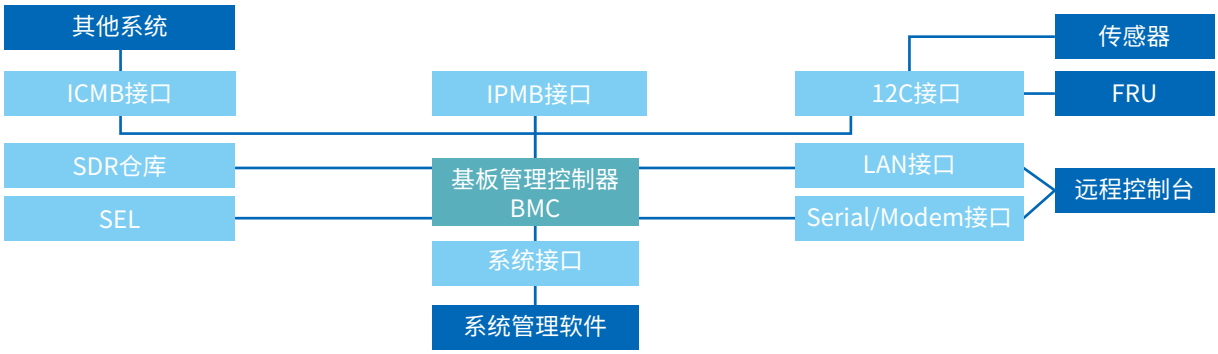

图2-1 BMC监控功能

(2) 机箱入侵检测技术

具有防入侵报警的服务器机箱，通过在机箱盖设置触点开关，与支持报警功能的主板配合，达到较高的安全性。当机箱盖被非法人员打开时，会触发传感器并将信号通过GPIO输入给BMC，BMC通过IPMB接口将事件发送至IPMB事件接收机，再通过平台事件过滤器使BMC根据不同的事件配置不同的行为，由事件匹配来实现。可选择的行为包括：下电、重启、诊断中断和产生告警，实现原理如图2-2所示。

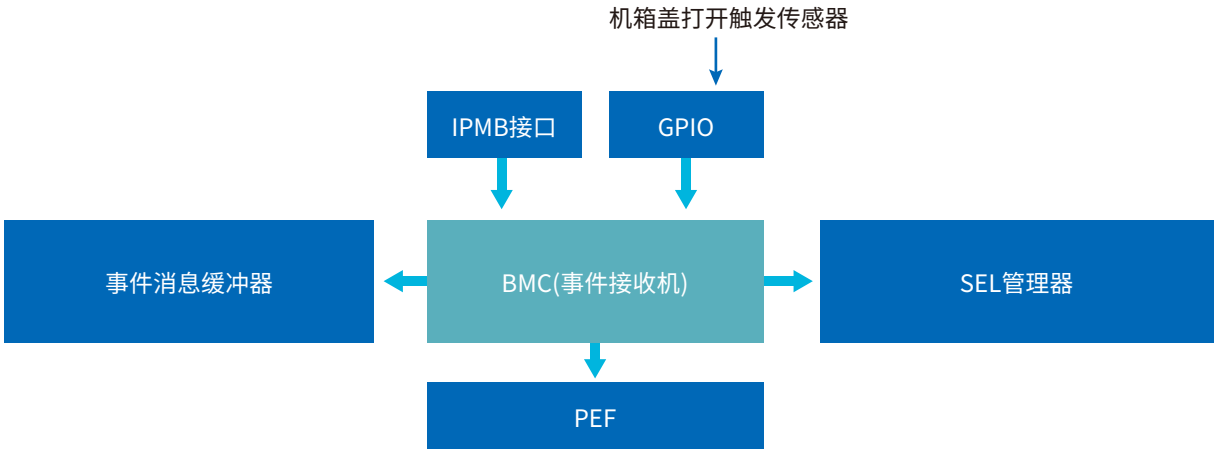

图2-2 机箱开盖报警

(3)内存监控报警

在内存报警监控设计方面，对每个内存都能做到温度监控报警、内存故障的指示报警。在开机后，BIOS通过PCH访问处理器和内存的信息，获取内存中的SPD信息（运行频率、物理安装位置等）、内存自检测试结果等信息，通过LPC或者ESPI总线，以IPMI命令格式发送到BMC。BMC在收到这些内存的报警信息之后，根据这些信息进行分类，判断出内存的故障级别及位置。之后MCU根据已定义的客服维护策略，通过GPIO信号，按照故障位置控制故障灯开关。同时，BMC会将故障信息存储在Log日志中，维护人员可以进行远程访问，快速进行故障点报告。

2.4 硬件板卡安全

在硬件板卡方面：

1）背板：选用专用背板芯片只做转接作用，且将解析信息与其他存储单元隔离，无外部漏洞入侵和信息泄露风险；

2）防短路设计：可热插拔的板卡之间、机构件直接与板卡接触的位置进行了防短路设计，例如设计单元隔离线路、粘贴mylar等，避免信号直接造成短路烧毁或者短路烧毁问题的扩散；

3）防呆设计：板上连接器、线缆均做防呆设计，防止因线缆接反造成的电路安全风险；

4）过压、过流保护：CPU主板设计过压、过流保护功能，背板、风扇板设计过流保护功能。

2.5 可靠运行支持

在部件安全方面，具备的安全技术主要有：

1）通过配置数据中心级持久内存，确保在突然断电等意外情况下内存数据依然保持完整性；另外，利用SMART　PPR内存防护技术可在开机过程中进行检测和内存故障修复。

2）硬盘支持热插拔，配置支持RAID0/1/10/5/6/60等冗余策略（视具体机型而定）；

3）RAID提供RAID Cache，具备超级电容掉电数据保护；

4）电源支持主备供电1+1冗余；

5）风扇支持N+1冗余，支持热插拔（视具体机型而定）；

6）所有插拔部件均进行了防呆设计，从而避免了误/错连接引起的电路安全风险；

7）利用浪潮独特的智能调控技术，设计了先进的风冷/水冷散热系统实现最佳工作环境，保障设备稳定可靠运行。

2.6 Whitley平台安全新特性

(1)Boot Guard 与 TXT 融合

由于 Boot Guard 与 TXT 两者都试图建立静态的测量可信根（STRM），度量值扩展存储于 TPM 中的平台配置寄存器（PCR0），为了消除两种技术之间的冗余、复杂性和低效率，Whitley 对现有 Boot Guard 和 TXT 技术进行了融合，消除了技术之间的重叠 / 冗余，简化实施并提供更强大的保护，改进和简化 BIOS 启动控制策略，消除自动升级并提高安全性，从而解决了早期架构中的问题。

（2）内存数据保护

通过全内存加密对数据进行保护：

1）多密钥全内存加密 MK-TME（Multi-Key Total Memory Encryption）

MK-TME 支持 DRAM 和 NVRAM，不需要重构应用程序，为多用户服务器平台提供基于密码的 VM/container 隔离，并且提供全内存加密，不需要启用必要软件，内联加密实现高性能。

2）单密钥全内存加密 TME（Total Memory Encryption）

通过单个密钥加密全部系统内存，不需要修改 OS/app。

（3）软件保护扩展

1）软件保护扩展 SGX（Software Guard Extensions）

隔离个别应用程序数据空间，需要修改应用程序代码。

2）SGX-TEM（Trusted Environment Mode）

SGX-TEM 在兼容 SGX 的基础上，专门用于扩展 MK-TME 以满足云环境中服务器平台的应用程序隔离要求。通过内置的 CPU 指令、内存访问控制和 BIOS 配置保护提供 BIOS/VMM/OS 的隔离，将信任边界调整到应用程序级别，保护来自 CSP SW 堆栈和客户 OS 层的用户应用程序。

3 服务器固件安全技术

浪潮服务器的固件包括可多级管理的带外管理固件BMC/CMC/RMC、服务器引导固件BIOS以及硬盘、网卡、RAID卡等部件中的固件，还包括CPLD、Expander、硬盘背板等模块中的固件。为应对固件面临的多类安全威胁，浪潮服务器的固件安全设计主要有安全启动、安全更新、备份恢复、访问控制、认证鉴权等，具体如下。

3.1 BMC安全技术

3.1.1 BMC安全启动

BMC安全启动原理如图3-1所示，利用RSA私钥对BMC固件镜像的摘要值进行加密，签名值Signature和镜像Image文件存储于Flash中；RSA公钥存入BMC的一次性可编程存储区OTP中，用于在安全启动过程中的度量和Firmware比对。

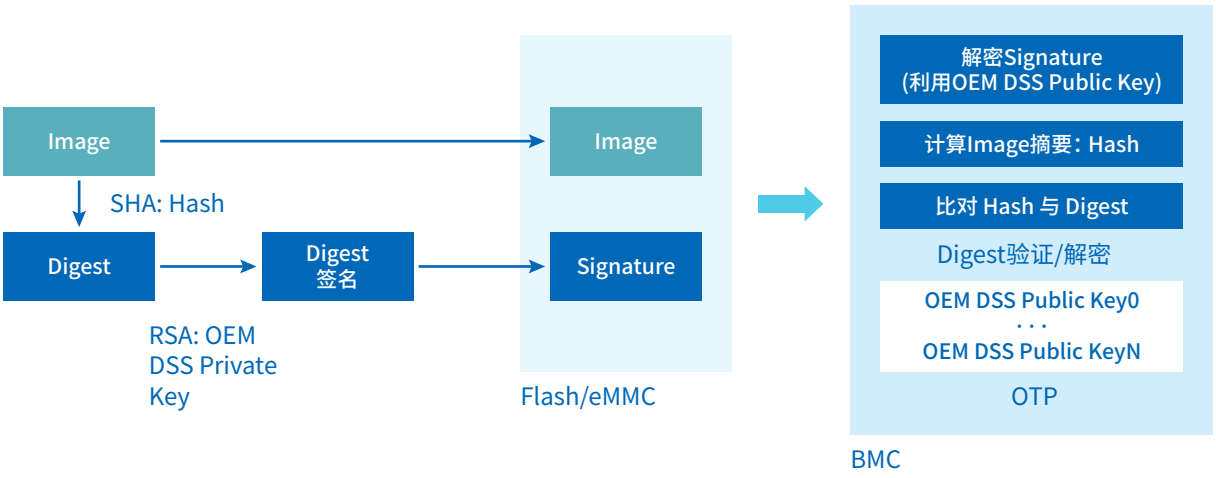

图3-1 BMC安全启动

BMC的安全启动过程如下：

1）在上电启动时，BMC内部的控制模块读取Flash中的签名值Signature，调用RSA公钥对Signature进行解密，恢复出摘要值Digest；

2）控制模块读取Flash中存储的Image镜像文件，调用SHA-256算法模块进行Hash运算，生成Hash值；

3）进行镜像文件的完整性校验，即比对Digest与Hash值，如果二者相等，说明Image镜像文件是完整的，之后启动镜像的加载和引导过程；

4）如果Digest与Hash值不相等，说明Image文件已被篡改，BMC的控制模块禁止镜像的引导，从而保证了BMC在启动阶段的安全性；

5）如果需要更换密钥，用新生成的RSA私钥重新对BMC镜像文件签名，并将对应的RSA公钥存储于BMC的OTP区域中。

3.1.2 BMC备份恢复

BMC通过双镜像方式进行备份恢复，具体原理为：

存放镜像文件的区域分成备份区和临时区两部分，如图3-2所述。备份区用于存放有效的镜像作为备份。当在线升级正在进行时，升级的镜像会被同时拷贝到临时区。一旦升级完成，升级的镜像被确认有效，临时区的镜像会被拷贝到备份区以替换原有的备份镜像文件。

当BMC发生故障出现宕机或回滚操作时，通过双镜像方式切换，备份区的镜像文件会被自动加载，从而确保可用性。

图3-2 BMC备份恢复

3.1.3 身份标识与鉴别

(1) 认证方式

BMC支持本地认证和第三方远程认证两种认证模式。

1) 本地认证：适合小型组网环境，如中小型企业。本地支持用户名密码认证，另外本地自动化 SSH 方式登录 BMC 命令行可以采用公钥认证。

2) 第三方远程认证：支持 LDAP/AD。LDAP 等第三方远程认证方式由于其数量和权限均在服务端设置，不受 16 个本地用户的数量限制，因此适用于具有大量用户的环境。使用域控制器中的用户域、组域、隶属于用户域的 LDAP 用户名及其密码登录 BMC 系统可以提高系统安全性。LDAP 用户可登录 BMC Web 界面，也可通过 SSH 方式登录 BMC 命令行和 Redfish 接口访问 BMC 系统。

(2) 密码及登录策略

包括密码复杂度、密码有效期、历史密码记录和登录失败锁定。为了防止密码猜测和暴力破解，密码复杂度可设置密码长度8位以上，字符类型包含3种以上。本地用户可以开启密码有效期和历史密码记录检查、开启密码登录失败锁定等配置。

3.1.4 授权与访问控制

(1) 基于角色的用户管理

BMC支持多种类型的用户，包括 IPMI、WEB、SSH和SNMP 用户，各类用户按照不同角色分配不同权限，实现用户的权限分立，且仅授予所需的最小访问权限。

BMC采用基于角色的本地用户精细化管理。系统权限类型被化分为用户配置、常规配置、电源控制、远程媒体、远程KVM、安全配置、调试诊断、查询功能、配置自身等九种类型。默认支持“管理员”、“操作员”、“普通用户”角色，不允许配置修改其权限。另外还支持最大4个自定义角色组OEM1、OEM2、OEM3、OEM4，系统管理员可灵活地根据业务维护需求将这九类权限配置给一个自定义角色。

系统管理员可以创建审计角色和维护角色，其中审计角色拥有安全配置和查询功能权限；维护角色拥有调试诊断和查询功能。

（2）访问控制规则

通过 BMC Web 界面可进行系统防火墙设置，包括一般防火墙设置、IP 地址防火墙、端口防火墙、MAC 防火墙等规则设置，从而减少攻击来源。从时间、地点（IP/ 端口 /MAC 地址）等方面对服务器管理接口的访问控制在最小范围内，并且用户可根据需要设置登录规则的白名单。

3.1.5 日志审计

在日志审计方面，BMC记录所有接口的非查询操作，记录内容包括事件发生时间、操作接口、操作源IP、操作源用户、执行动作等。支持自动备份和通过Web导出日志，当审计日志文件超过50K时，日志将会被清除。故障诊断日志IDL是浪潮BMC独有的日志类型，用于记录BMC设备上基于IPMI传感器的事件历史记录，每条日志都有相应的处理建议，能更有效的帮助用户进行日志诊断和分析。

使用 SNMP Trap 功能将 BMC 告警信息发送到远端 Trap 接收端时，为了传输安全，Trap 接收端可使用 SNMP V3 版本协议，配置认证协议选择“SHA”，加密协议使用“AES”，且认证密码、加密密码遵循密码复杂度要求，SNMP Trap BMC 发送端根据接收端各参数进行相应设置。

由于 BMC 本地存储空间有限，为保证日志信息正常记录，可将事件日志设置为循环策略，并使用 Syslog 功能将 BMC 的事件日志及审计日志发送到远端 Syslog 服务器进行保存，且为了传输安全，建议 Syslog 配置使用 TLS 传输协议。

3.1.6 安全加固

（1）命令行安全加固

1）Smash CLI：对OS、Shell命令行进行了封装加固，只能执行白名单定义的命令；

2）SSH Smash：使用Smash命令行，防止登录SSH获取最大权限。

（2）安全协议

1）BMC按照最小化原则对外开放网络服务端口，关闭不使用的服务；

2）默认使用SSH v2、HTTPS、SNMP v3、RMCP+等安全协议保护数据传输安全，默认关闭不安全协议的端口，当启用不安全协议时提示安全风险。

（3）数据加密存储及传输

BMC中的敏感数据在日志、文件或Cookie中使用安全算法进行加密存储，默认使用HTTPS进行通信，支持SMTP电子邮件传输时启用TLS加密功能，保证数据传输的安全性。在使用远程控制台时，BMC支持开启KVM加密、VNC加密功能，实现数据的安全传输。

（4）证书及密钥管理

BMC支持SSL证书生成及证书替换功能，为提高安全性，支持替换成自己的证书和公私钥对，并及时更新证书，保证证书的有效性。BMC还支持LDAP证书的导入功能，为数据传输提供鉴权加密功能，提高系统安全性。

3.2 BIOS安全技术

3.2.1 Intel TXT可信计算技术

Intel TXT 技术以增强型的处理器架构、特殊的硬件芯片和相关固件为基础，主要目标是在系统启动时建立一个可信的运行环境，为系统软件提供一个更加安全的执行环境以保护数据的完整性。同时，Intel TXT 技术为诸如密钥等的敏感数据提供安全的存储，保护其不受恶意攻击、不被窃取。

Intel TXT 度量流程见图 3-3，具体说明如下：

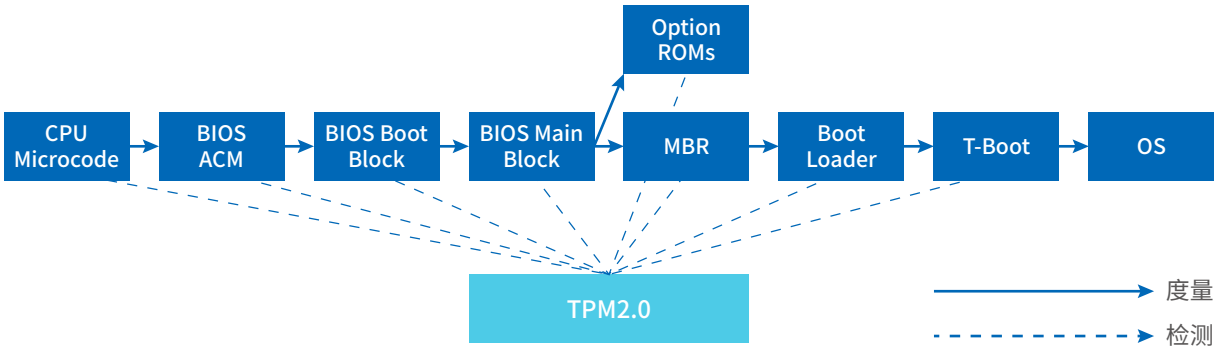

图3-3 Intel TXT度量流程图

1）系统上电后，CPU作为CRTM，首先加载Microcode，然后Microcode加载BIOS ACM；

2）BIOS ACM度量BIOS Boot Block，度量值扩展存储于TPM 2.0芯片中的PCR0；

3）BIOS Boot Block对CRTM版本、BIOS Main Block进行度量，度量值同样扩展存储于PCR0；

4）BIOS Main Block对OP ROM（如：网卡、RAID卡、PCIe卡的OP ROM）进行度量，度量值扩展存储于PCR2；之后度量MBR，度量值扩展存储于PCR5；

5）使用Grub作为Boot Loader，Grub不对之后的软件度量，最后的度量及校验是在TBoot中完成的；

6）TBoot的主要功能是检测Intel TXT、配置处理器、部署策略及策略校验等；其作用是检测平台安全性、度量校验所加载内核、模块的安全性；

7）TBoot之后是操作系统的加载，从而构建起了完整的信任链。

3.2.2 BIOS Secure Boot

Secure Boot是一个安全标准，帮助确保系统引导只使用制造商信任的软件。启用Secure Boot功能后能够使固件强制执行策略，仅启动签名的OS加载程序，OS Loader/EFI Image对Windows组件进行签名验证，从而使恶意软件无法更改引导和操作系统组件。

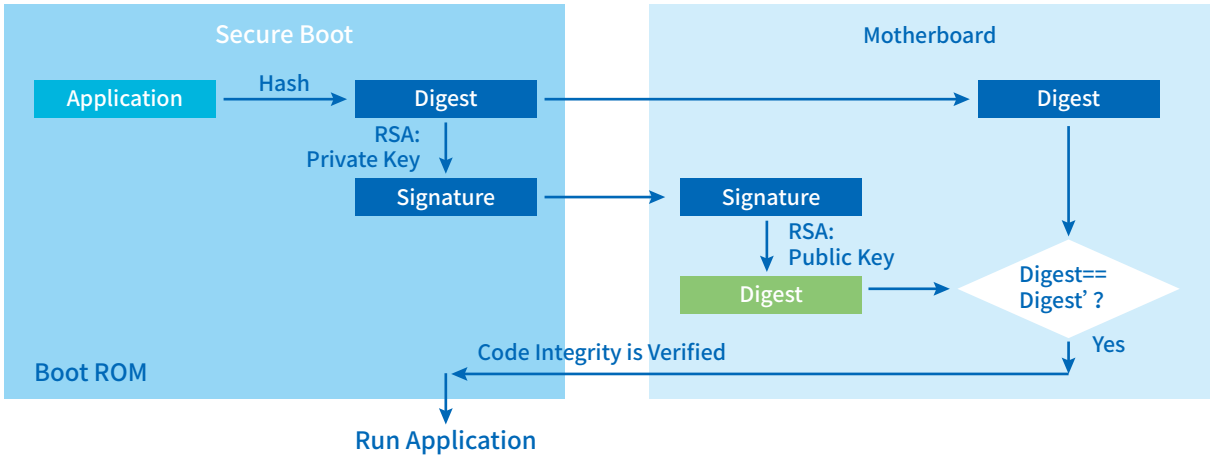

图3-4 BIOS Secure Boot

Secure Boot工作流程如下：

1) 应用程序在加载运行之前，利用Hash算法生成摘要值1；

2) 应用程序经过私钥进行签署，生成签名值；

3) 主板利用公钥验证数字签名，恢复应用程序明文；

4) 主板利用Hash算法生成应用程序摘要值2；

5) 比对摘要值1和2，相同则运行该应用程序，否则拒绝加载该程序。

3.2.3 BIOS Secure Flash

Secure Flash是BIOS的安全更新方案，支持在UEFI Shell/Windows/Linux中通过刷新工具更新BIOS，以及通过BMC Web远程更新BIOS，并且在刷新时会保护MAC地址、系统变量等不被覆盖。

(1) UEFI/OS更新方式

经过签名的新的BIOS镜像文件传递给SMM，由SMM检查该镜像文件的证书（SHA256+RSA2048）。如果验证通过，当前BIOS设置mailbox事件，刷新工具AFU将发出复位指令。重启后，PEI找到对应的新BIOS Image后进行检查，如果检查通过，将新的BIOS写入Flash，然后再重启，使得新BIOS生效。

证书存放于BIOS镜像中的ROM Hole中，ROM Hole为在BIOS代码中设置的一块64K区域，创建完成原有的BIOS镜像（BIOS+ME）后，通过执行脚本对Rom Hole以外的BIOS镜像进行Hash计算和数字签名，并把证书（签名值、签名所用的公钥）放置于Rom Hole中。在刷新BIOS过程中，首先获取当前BIOS及待更新BIOS的Rom Hole数据，检查待更新的BIOS证书并比对产品名称，若验证不通过，说明是非法的BIOS，则禁止执行刷新流程。

(2) BMC更新方式

通过BMC Web对BIOS进行带外升级时，具体过程如下：

1) BIOS镜像文件通过SHA256算法计算出摘要值后，再使用RSA2048算法对摘要值进行数字签名。

2) 通过镜像制作工具制作镜像头和镜像尾（MD5 check sum），把签名值存放在镜像头OEM字段内，镜像头、原始镜像和镜像尾组合成HPM镜像。

3）当BMC进行带外升级时，Web把整个HPM镜像上传给BMC，BMC对镜像头信息进行校验，并分离出原始镜像和数字签名。对BIOS镜像进行签名对比，只有校验通过后才会进行BIOS升级。

3.2.4 BIOS Boot Guard

Boot Guard是浪潮服务器采用的Intel启动完整性的保护技术，目的是阻止未授权的Boot Block。Boot Guard可配置的启动类型包括度量启动、校验启动以及两者的结合。采用Boot Guard可以阻止平台运行未授权的软件，防范Boot Block层恶意软件的执行，提升基于硬件的平台安全，提供硬件信任根用于度量、校验。

平台的启动顺序如图3-5所示，Boot Guard确立了基于硬件的信任根，BIOS继续构建信任链从而完成平台完整性的启动。由于平台软件的第一行没有被校验，黑客可以在杀毒软件启动前植入恶意代码，并且被认为是可信的。Boot Guard能够校验Boot Block包含的第一行代码是由浪潮授权的，在硬件层加强了Secure Boot，减少了恶意软件的攻击。

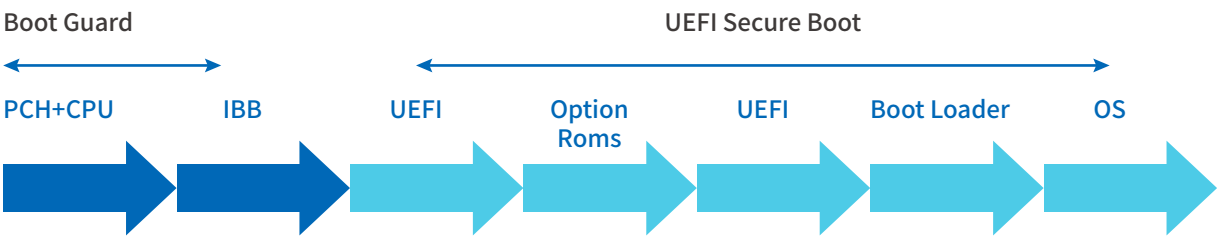

图3-5 平台启动顺序

采用Boot Guard技术的具体步骤是，使用公私钥对中的私钥对发行的BIOS镜像文件进行签名，把公钥烧入CPU，从而使未经过浪潮签名的BIOS固件不会被CPU执行。目的是为了避免黑客通过修改固件的方式绕过UEFI中Secure Boot的安全保护。Boot Guard技术提供了两种模式：Verified Boot模式和Measured Boot模式，Verified Boot模式会验证固件签名，并且完全拒绝未通过验证的固件运行；Measured Boot模式将启动过程的信息记录到TPM2.0模块中，交给操作系统去做后续进一步处理。

采用 Boot Guard 需要 TPM 模块的支持，如果没有 TPM 模块只能做 Boot Guard 的校验，不能进行度量。Boot Guard 技术的思想是用签名代替度量，与 Intel TXT 度量技术互补，用于签名的公私钥对中的公钥经过 Hash 运算后烧写到 PCH chipset 中，而且只能烧写一次。

3.2.5 用户安全

（1）密码安全策略

BIOS用户分为Admin和User，对应的权限不同，对Admin/User Password有复杂度要求，当密码不符合规则时，会进行一般性警告提示。密码复杂度安全策略如下：

1）密码长度为8-20位；

2）密码必须同时包含特殊字符、大写字母、小写字母和数字；

3）不能使用前5次密码；

4）用户登录时对每个登录错误发出相同的报错信息，不会提示具体的错误原因；

5）用户设置或者登录输入口令时，口令不会明文回显；

6）用户重置密码时，必须输入旧密码并校验通过后才能重置密码；

（2）密码存储安全

支持通过BMC修改进入BIOS Setup菜单的密码，新设定密码加入Salt值后再通过SHA256算法加密后保存在SRAM中，并置起一个flag，表明密码已通过BMC修改。

系统启动时，BIOS检查SRAM中的flag，若被置起，则读取SRAM中的密码写入到NVRAM中，同时清除该flag；若没有被置起，则保持原样。

在BIOS Setup中设定密码时，BIOS将新密码写入NVRAM，同时写入SRAM，保证SRAM中的密码为最新。

BMC刷新BIOS后，BIOS检测到是第一次开机，则去SRAM中读取密码写入到NVRAM。

3.3 固件安全更新

对发布的BMC、BIOS、CPLD等固件镜像进行签名，确保其合法性，在更新或升级固件时（例如通过BMC、OS等带外、带内更新方式）提供对固件Image镜像文件的数字签名验证机制，保证固件文件的不可伪造性和完整性，从而防止使用嵌入恶意代码的非官方版本镜像进行滥刷或误刷。

以BMC更新BIOS为例进行说明，如图3-6所示，发行新的BIOS镜像时，利用OpenSSL库的SHA-256算法对BIOS镜像进行Hash运算，得到摘要值，然后利用RSA算法生成的公私钥对中的私钥对摘要值进行签名，之后把BIOS镜像文件和对应的签名值，以及公钥分发给服务器本地端。

本地端BMC利用公钥，调用软件RSA算法和SHA-256算法验证镜像的签名值，当验证通过后BMC才能执行BIOS镜像的更新；当BIOS镜像未通过验证时，说明镜像的来源不明或镜像的完整性受到了破坏，因此BMC不会执行BIOS镜像的刷写。

图3-6 固件安全更新

BIOS更新的流程如下：

1）利用SHA-256算法对BIOS镜像进行Hash运算，生成摘要值；

2）利用RSA算法生成的公钥-私钥对中的私钥对摘要值进行签名；

3）把BIOS镜像、BIOS镜像的签名值、公钥分发给用户端；

4）用户端的BMC调用SHA-256算法对BIOS镜像进行Hash运算，得到摘要值1；

5）调用RSA算法，利用公钥验证签名值，得到摘要值2；

6）比对摘要值1与摘要值2，如果二者相同，BMC对BIOS进行更新；如果二者不相同，BMC不会对BIOS进行更新。

3.4 PFR技术

PFR（Platform Firmware Resilience）是Intel的平台固件恢复技术，增加服务器应对固件层攻击的恢复能力。使系统通过特殊的预引导（pre-boot）检测固件攻击，并且在数分钟内自动恢复到已知的正常状态。在运行过程中进行监控，并且把监控信息存储于非易失存储单元以阻止攻击；在装运过程中通过锁定系统并且对固件签名实现保护的功能。

当前浪潮服务器在硬件线路方面已支持PFR功能，后续在软件方面会持续完善安全启动过程，具体如下：

（1）启动过程的安全

启动过程的安全措施包括检测、保护和恢复，如图3-7所示：

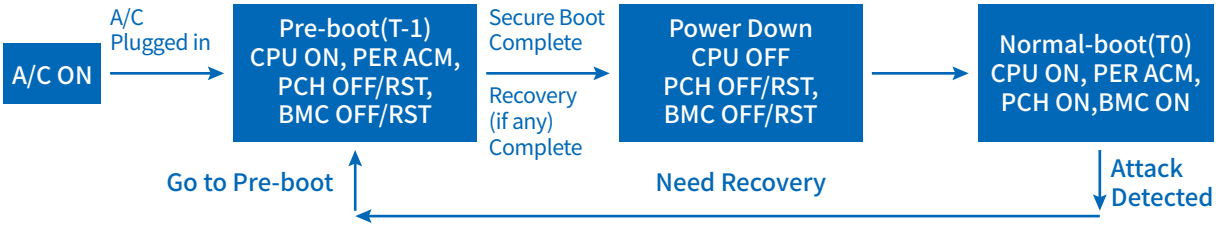

图3-7 PFR功能

1）检测：比较FW的数字签名，用于认证优先启动；

2）保护：如果签名不匹配，非法的FW不允许执行；

3）恢复：PFR功能会自动用可信的镜像替换受破坏的镜像，之后允许系统启动。

（2）供应链安全

1）平台锁定-上电时通过密码保护平台

为PFR CPLD和RF组件提供随机密码（PIT pwd）。如果RF组件中的密码丢失，PFR CPLD在每次AC上电时比较PIT密码并且阻止上电时序。在运输前移除RF中的密码，从而阻止了平台的上电启动。

2）平台固件签名

在运输前 PFR CPLD 计算平台固件（PCH、BMC 以及附加的 SPI 芯片）的摘要值，并存储于安全的 NVRAM 空间。交货时 PFR CPLD 重新计算平台固件的摘要值，并且对任何不匹配的情况进行告警。

4 服务器配套软件安全技术

浪潮为构筑全面的服务器产品安全保障体系，除了产品自身安全技术外，还设计了行之有效的配套软件安全方案，旨在帮助用户规避和减少安全风险，提升浪潮产品和服务的安全性。

4.1 兼容OS安全

浪潮与微软、Redhat、SUSE等OS厂商不定期开展技术研讨及合作，共同推进服务器所兼容的OS安全性，及时关注厂商OS安全技术发展和安全漏洞解决方案，及时提高用户使用服务器过程中遇到的安全问题。

4.2 主机安全加固

浪潮在操作系统网络安全技术领域引入内核加固崭新理念，成功开发了“浪潮主机安全增强系统”系列产品，简称浪潮SSR。浪潮SSR目的就是利用内核加固技术构建一个自身免疫的系统，从根本上实现了一个安全操作系统模型，提升操作系统的安全等级。

浪潮SSR作为服务器安全加固软件，能够有效地预防服务器未知漏洞攻击、病毒等，防止某些类型的恶意缓冲溢流攻击。即使黑客、非法攻击者能够突破防火墙，也不能够对服务器造成任何威胁，保证应用系统的安全运行。

浪潮SSR根据国家三级的安全标识保护级别的标准，为系统中的信息交换的主客体分别加上安全标记，从而达到了强制访问控制（MAC），制约了操作系统原有的自主访问控制策略（DAC），从根本上控制了信息的交换，实现安全的信息交换方法。

浪潮SSR在系统访问界面这一层旁路所有的文件访问操作，从驱动层来达到为主客体进行安全表示判断的目的，实现了一个真正的安全内核。安全功能主要有：

1）强制访问控制：内核级实现文件强制访问控制、注册表强制访问控制、进程强制访问控制，服务强制访问控制；

2）安全审计：文件的完整性检测、服务的完整性检测；

3）自身的保护：保护软件自身进程不被异常终止、伪造、信息注入；

4）安全等级：提供国家第三级安全等级标准的安全功能；

5）可操作性：完全兼容Windows、Linux、Unix系统，专业的技术，人性化的操作界面，运行开销小，不会引起可察觉的系统延时，对用户透明。

4.3 可信应用

作为可信技术的应用，可信增强软件是一款部署在Linux操作系统中的安全软件，且操作系统运行在符合TPM 2.0规范的可信服务器上，与可信服务器配合，实现可信服务器硬件平台的可信校验，操作系统内核及应用软件的可信度量和校验，并为用户提供友好的管理工具，同时为开发者提供API接口，方便开发者更好地使用可信服务器提供的服务。

可信服务器的安全目标是从服务器硬件上电开始，通过可信根逐级度量服务器启动过程的BIOS Boot Block、BIOS Main Block、板载设备、MBR等各个组件，并扩展度量结果到硬件可信根的安全存储空间，同时通过硬件安全芯片提供的密码服务，为上层应用及访问者提供验证平台可信的方法。在操作系统层面，通过可信服务器增强软件进一步将信任链扩展到操作系统，并为操作系统用户提供访问可信服务器硬件可信服务功能的接口与管理工具。

4.4 虚拟化安全隔离

浪潮服务器虚拟化系统 InCloud Sphere 是一种直接安装在物理服务器上的虚拟化产品，它提供了虚拟机运行的环境，每台虚拟机都有一组虚拟的 CPU、内存、存储和网络资源。其组件主要包括管理客户端 iCenter 和计算节点 iNode，iNode 节点运行 Hypervisor 和 Domain 0 服务，Hypervisor 和 Domain 0 作为一个整体共同支持客户虚拟机 Domain U 的运行。

在安全性方面，可实现虚拟机之间计算、存储和网络资源的隔离，保护虚拟机在磁盘和内存中的数据不会被其他虚拟机非法访问。

InCloud Sphere 能够确保管理网络上所有数据的保密性和完整性，其三个组件实现的安全功能如下：

1）Hypervisor：计算隔离；

2）Domain 0：虚拟资源调度、存储隔离、网络隔离、数据传输保护；

3）iCenter：监控告警、安全审计、用户管理与认证、系统管理、虚拟资源管理。

五、结语

浪潮相信，务实造就成功，创新成就未来。浪潮将一如既往地保持着创新的精神，引领IT基础设施发展，专注于客户需求，以匠人精神为客户提供专业、优化、安全、高效的产品体验。最后，感谢我们的众多幕后英雄们，这份白皮书凝聚了多位领导和同事的辛勤工作：刘宝阳、徐鹏翔、孙辉、张松涛、王玲燕、程鹏、吕明旸、张纷纷、孙志超、苏振宇、赵媛、曹柱、刘刚、刘雁鸣、王瑾等，感谢你们为呈现这份白皮书贡献的巧思以及推进浪潮服务器产品安全技术付出的心血。谢谢你们！

尊敬的用户：

商标声明

注意

您购买的产品、服务或特性等应受浪潮电子信息产业股份有限公司商业合同和条款的约束。本文档中描述的全部或部分产品、产品安全服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，浪潮电子信息产业股份有限公司对本文档内容不做任何明示或默示的声明或保证。由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

浪潮电子信息产业股份有限公司

网　址：www.inspur.com

地　址：中国山东省济南市浪潮路1036号

邮　编：250101