申威平台安全启动机制设计与实现

李之健[1] 苏卫强[1] 赵翊含[1]
LI Zhijian SU Weiqiang ZHAO Yihan

摘 要 当前，信息系统广泛依赖国外软硬件产品，存在严重安全隐患，如恶意后门、远程操控等潜在风险。申威处理器虽具备完全自主知识产权，但其安全启动能力仍有待加强。针对现有 UEFI 安全启动方案在申威架构下兼容性差、依赖国际密码算法等局限，文章结合我国在可信计算技术与 SM2/SM3/SM4 等国密算法体系，提出一种基于国产可信密码模块（TCM）为硬件可信根的多级安全启动方案。构建了从固件到操作系统的逐级验证信任链，支持启动过程的主动度量与完整性验证，具备抵御固件篡改、引导器劫持等攻击能力。在申威平台的实验结果表明，该启动机制能有效阻断多种启动阶段攻击，显著提高了申威平台的主动防御能力，为国产化信息系统的安全启动提供了可行的技术路径。

关键词 申威；安全启动；信任链

doi：10.3969/j.issn.1672-9528.2026.05.023

0 引言

随着我国信息化建设的高速发展，信息系统已经在军事、金融、能源、交通等各个行业领域得到了广泛应用，推动社会发展。然而，发展的进程始终与安全挑战相伴而生。计算机病毒、网络攻击与窃密事件频发，信息安全问题愈发严峻[1]。我国各类信息系统对国外产品的依赖也会带来潜在的安全风险。如英伟达对华出售的 H20 芯片被爆出存在“追踪定位”“远程关闭”技术，已被国家互联网信息办公室约谈[2]。由此可见，对国外软硬件的普遍依赖已成为信息系统的潜在风险源，可能导致泄密或影响信息系统正常运行。要从根本上解决此类

1. 无锡先进技术研究院 江苏无锡 214083

够刻画流量复杂性的检测模型，并引入自适应动态更新机制以持续优化检测阈值与参考基线。实验结果表明，在信噪比为 10~15 dB 的高噪声模拟环境下，该方法对 DoS、MITM、Worm 等多类攻击均能实现有效识别与精准标记，异常区间划分清晰，无明显重叠或漏标。漏检次数随系统运行逐步收敛，最终稳定在较低水平。与基于随机森林和深度学习的对照方法相比，本文方法在各攻击场景下的误检率均稳定控制在 4% 以下，展现出更优的鲁棒性与检测一致性。

参考文献：

[1] 田博宇 . 无线通信网络异常流量动态检测方法研究 [J]. 无线互联科技 ,2025,22(10):106-110.
[2] 郝莉萍 , 马迎辉 , 邬迎 . 基于深度学习的无线通信网络异常流量攻击检测方法 [J]. 长江信息通信 ,2025,38(4):172-175.
[3] 杨静 . 基于 GRU 的无线传感器网络汇聚层流量异常检测方法 [J]. 宁夏师范大学学报 ,2025,46(1):81-90.
[4] 张兵 , 卞利 . 基于 FW-PSO 的大区域无线传感网络流量异常检测算法 [J]. 传感技术学报 ,2023,36(7):1116-1121.
[5] 赵伟娜 , 马凯 . 多模态无线传感网络节点流量异常自调节研究 [J]. 传感技术学报 , 2025, 38(4):711-716..
[6] 王洁 , 吕奕飞 . 基于流量异常特征的无线网络攻击行为检测方法 [J]. 电脑知识与技术 ,2024,20(11):78-80.
[7] 吕广旭 , 王小英 , 冯燕茹 , 等 . 基于 VAE-GMM 的高级持续威胁攻击异常流量检测 [J]. 计算机应用与软件 , 2025, 42(11): 325-330.
[8] 安义帅 , 付钰 , 俞艺涵 , 等 . 基于数据增强与特征挖掘的异常流量检测方法 [J]. 通信学报 ,2025,46(8):16-30.
[9] 陈涛 , 薛皓铭 , 马宇翔 , 等 . 基于自适应联邦学习的边端协同网络异常流量检测模型 [J]. 计算机应用研究 , 2025, 42(11): 3461-3467.
[10] 卢庆武 , 赖坤宁 . 网络动态入侵多层特征最优检测方法仿真 [J]. 计算机仿真 , 2025,42(6):379-383.

【作者简介】

古兰君（1996—），女，河南郑州人，硕士，助教，研究方向：数学教学。

樊多妮（1986—），女，河南焦作人，硕士，讲师，研究方向：主题网络爬虫技术。

（收稿日期：2026-01-08 修回日期：2026-05-20）

安全威胁，必须走自主可控道路。

申威处理器基于完全自主设计的SW64指令集与微架构，实现了从核心架构到研发流程的自主可控，广泛应用于高性能计算、服务器、桌面终端及嵌入式设备等领域，为我国软硬件生态的自主化与信息安全提供了重要支撑[3]。然而，其在系统级安全防护能力方面仍显薄弱，尤其缺乏对固件篡改、恶意加载等启动阶段攻击的有效防御机制。

在各类安全威胁中，针对设备启动阶段的攻击是最为难以防御的。由于该阶段处于操作系统及各类防护机制（如防火墙和防病毒软件）加载之前，常规安全措施尚未激活，使得此类攻击具有极强的隐蔽性与防御难度[4]。近年来，随着密码学技术的不断进步，安全启动（Secure Boot）机制被提出并有效应对了这一安全隐患。该机制通过在每个引导环节对后续阶段实施严格的密码学验证，确保仅加载经授权实体签名的固件，从而构建起一条可信的启动链[5]。借助这一过程，安全启动能够有效防范启动文件被篡改或恶意代码注入，保障系统始终能够处于可信状态，进而维护整个系统的完整性与安全性。

目前已有多种成熟的安全启动的方案，UEFI（unified extensible firmware interface）安全启动[6]通过构建信任链来确保引导过程的安全，通过在固件引导与操作系统启动过程中，实现对被加载的UEFI二进制或应用的验证以及对操作系统的验证，从而确保启动过程的安全性。但其无法防御针对UEFI BIOS自身的篡改。为此，其他厂商分别推出了Intel Boot Guard[7]，AMD HVB[8]，Apple Secure Boot[9]等定制化方案。然而，这些方案由于闭源，不符合申威平台的设计等原因均无法直接适用于申威平台。

近年来，我国在信息安全核心技术与标准体系建设上取得了一系列关键突破，显著增强了自主可控能力。包括提出了可信计算密码模块[10]，SM系列国产密码算法以及可信平台控制模块（TPCM）[11]等，这些成果明显提升了我国信息安全体系的自主可控能力，降低了在核心安全技术领域对国外技术的依赖。但要将这些创新成果全面应用于申威平台，仍需推进具体技术方案的落地与相关适配。

综上所述，本文提出了申威平台安全启动方案，使用了先于CPU启动的TCM作为硬件可信根以及SM系列国产密码算法，保证了安全启动流程的自主可控。设计并实现了一套基于验证引导的多级安全启动机制。该机制以硬件可信根为起点，按照第零阶段引导程序（zero stage bootloader, BL0）、第一阶段引导程序（first stage bootloader, BL1）、第二阶段引导程序（second stage bootloader, BL2）至系统内核的顺序，逐一对下一阶段进行验证并传递信任链，实现安全启动。本文在实验中设计了多种针对启动阶段的攻击，对比了使用和未使用申威架构安全启动方案时遭受攻击的情况。实验结果表明在受到攻击后能有效阻止各种攻击，验证了申威架构安全启动方案的有效性，如图1所示。

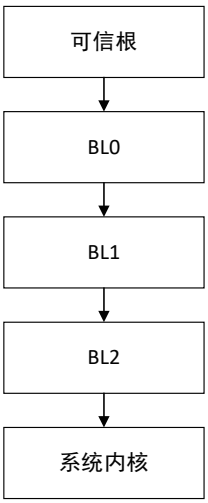

图1 申威平台安全启动信任链

1 相关背景

1.1 密码学

密码学研究通过编码和解码来保护信息安全。本节介绍安全启动相关的密码学算法。

（1）哈希算法

哈希算法是密码学领域的核心基础算法，其核心功能是将任意长度的输入消息通过特定数学变换规则，映射为固定长度的输出，该输出结果即为哈希值。该类算法具备三大核心特性：一是输入长度任意；二是输出长度固定，且相同输入必然生成相同哈希值；三是具备单向不可逆性与抗碰撞性，即无法从哈希值反推原始输入，且难以找到两个不同输入生成相同哈希值。典型的哈希算法包括MD5[12]、SHA-3[13]和国密SM3算法[14]。其中SM3算法在2016年被国家标准化管理委员会定为我国密码行业标准。申威平台安全启动将使用SM3哈希算法。

（2）非对称密码算法

非对称密码算法，也被称为公钥密码，其核心在于使用一对数学关联的密钥：公钥（PK）与私钥（SK）。公钥可公开分发，而私钥则必须严格保密。使用公钥加密的数据仅能由对应私钥解密，从而保证机密性；使用私钥生成的数字签名则可被对应公钥验证，以此确保数据的完整性与身份认证。国际上有RSA[15]与椭圆曲线密码体制[16]等经典方案。我国则推出了自主的国密SM2算法[17]。该算法由国家密码管理局于2012年发布，拥有比RSA更高的安全强度。本文中的申威平台安全启动方案中的非对称加密与数字签名均使用国密SM2算法实现。

（3）数字签名

数字签名使用非对称密码算法确认信息发送者的真实身份，并检测数据在传输过程中是否遭受任何形式的篡改。签名流程中，签名一方使用私钥SK对消息M的哈希值进行加密运算，如图2所示。验签流程中，验签一方可通过公钥PK对该签名进行解密，然后将其与消息M的哈希值比较，以验证消息的完整性和签名者的身份，如图3所示。签名可表示为S(PK, M)，签名验证阶段可表示为V(PK, S)。其中，S为签名生成函数，V为签名验证函数。

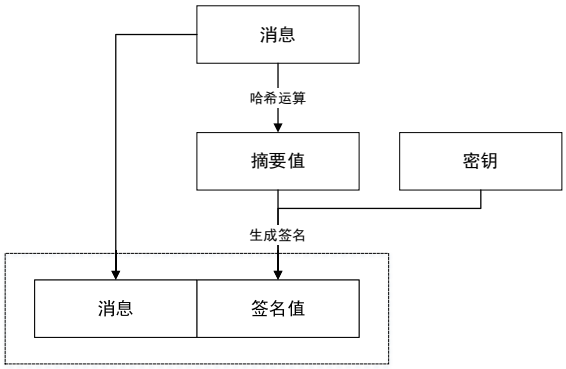

图 2 签名流程

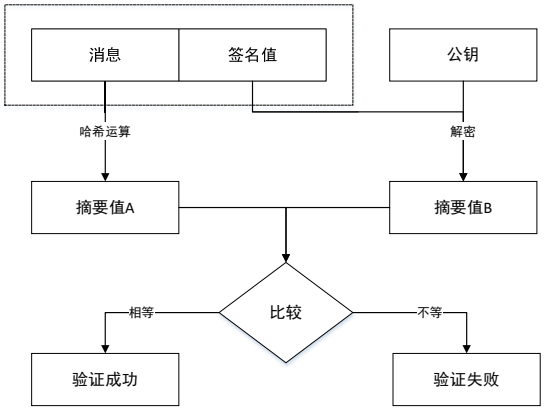

图 3 验签流程

1.2 可信计算

目前可信计算尚未有统一定义，专家学者与相关组织对此有不同解读。国际标准化组织与国际电子技术委员会（ISO/IEC）将可信表述为计算过程中涉及的组件、操作及流程在各类条件下均具有可预测性。可信计算组织（trusted computing group, TCG）则认为当一个实体的行为始终以预期方式朝向预定目标开展时，该实体即属于可信计算范畴。国内学者沈祥昌等 [18] 则提出可信计算系统需要具备可靠性、可用性、信息和行为安全性，且系统的安全性和可靠性是现阶段可信最主要的两个方面。总的来说，这些对可信计算的定义有一些共通点，包括强调实体行为的符合预期以及强调系统的安全与可靠。

1.3 可信根

国际上，TCG 定义了可信平台模块 [19]（trusted platform module, TPM），以安全芯片 TPM 作为可信根。在国内，中国可信计算平台联盟则于 2007 年推出可信密码模块（trusted cryptography module, TCM）规范 [10]。TCM 作为一种独立的安全芯片，通过物理隔离有效防范了恶意软件的直接访问。其内部具备受保护的存储区域，可用于保存密钥等敏感数据。同时其也具有对国密算法的支持，可执行加解密、签名与验签等密码学操作。因此，TCM 能够作为计算机系统的硬件可信根，并以此为基础构建信任链。

针对可信度量根的保护和起始度量点问题，张兴等 [11] 提出了可信平台控制模块（trusted platform control module, TPCM）。该方案不仅将可信度量根固化于芯片内部以强化其安全性，同时还改进了启动序列，使 TPCM 能先于 CPU 运行并主动执行对 BIOS 的度量，从而能够构建以自身为信任起点的完整可信链。

申威平台安全启动使用了支持先于 CPU 启动并进行主动度量的 TCM 安全芯片作为硬件可信根，通过 TCM 对数据，密钥进行储存和加解密。

1.4 安全启动

UEFI 安全启动协议可在操作系统加载并完全运行之前，保护启动过程免受恶意代码的篡改。当计算机系统启动且安全启动功能激活时，固件会检查每个被加载的 UEFI 二进制或应用：首先验证这些二进制文件是否具有有效签名——即通过本地可信证书数据库核对签名真实性，或确认其校验和已被列入“允许”清单；同时还会检测相关证书或校验值是否未出现在“禁止”清单中。若验证通过，固件将执行该二进制文件；若验证失败，则拒绝加载并立即终止启动进程。信任链将从 UEFI 固件开始，经过整个引导过程，最终延伸至系统内核 [20]。

在 UEFI 安全启动中通常还会使用一个名为 shim 的特殊引导程序，其由微软 UEFI 认证机构签发证书，可被 UEFI 信任并执行。shim 可以创建机器所有者密钥（machine owner key, MOK）并存放在一个 MOK 列表中，用于对 GRUB 和系统内核进行签名。shim 将信任 MOK 列表中密钥签名的引导程序和系统内核。

UEFI 安全启动的基本前提是 UEFI BIOS 本身是可信的。然而，该机制无法防御针对 UEFI BIOS 固件本身的篡改行为。正因如此，许多厂商推出了各自的安全启动方案。例如，英特尔（Intel）采用了 Boot Guard 技术，该技术依赖一个由英特尔签名的验证代码模块（authenticated code module, ACM）。在主机 CPU 将控制权转交给 UEFI BIOS 之前，ACM 会对其完整性进行验证。出于启动效率的考虑，ACM 并不验证整个固件映像，而是仅校验初始启动块（initial boot block, IBB），随后由 IBB 负责验证 OEM 启动块（oem boot block, OBB）[7]。

苹果安全启动（Apple Secure Boot）方案则基于其 SoC 中集成的不可修改的 boot ROM，其中的代码在制造阶段被固化，作为硬件的信任根。整个启动流程中涉及的固件、引导加载程序及内核均须由苹果签名方可执行。此外，苹果还引入了 Secure Enclave 安全子系统，该组件集成于 SoC 中，与主处理器隔离运行，提供更高层级的安全保障。其设计目标是即使主应用处理器内核遭受入侵，仍能有效保护用户的敏感数据安全 [9]。

申威平台无法直接采用现有的安全启动方案，主要原因包括：

（1）UEFI 安全启动默认以 UEFI 固件作为系统上电后首先执行的程序，而申威平台将 UEFI 视作 BL1，在此之前还存在 BL0 代码。仅依赖 UEFI 安全启动无法确保 BL0 及后续 UEFI 代码的完整性与可信性。

（2）其他厂商推出的安全启动方案通常未适配申威处理器架构的具体需求，并且多数为闭源方案，缺乏可定制性和移植性。

在使用了支持主动度量的 TCM 安全芯片作为硬件可信根后，申威平台安全启动方案将主要关注开机后将如何将信任链传递到 UEFI。

2 系统实现

2.1 可信根

申威平台的安全启动机制以 TCM 安全芯片作为硬件可信根。该 TCM 需符合国家可信计算相关规范，支持 SM2、SM3 等国密算法，具备受保护的存储区域，并应实现主动度量功能。

2.2 签名流程

申威平台安全启动方案的签名流程如图 4 所示，包括以下步骤：

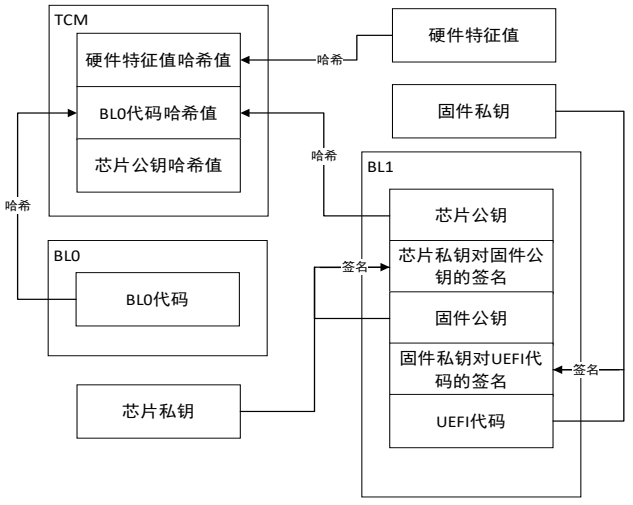

图 4 申威平台安全启动签名生成流程

（1）芯片厂商生成 SM2 芯片密钥对 (PK_a, SK_a)，固件厂商则生成固件密钥对 (PK_b, SK_b)。 芯片公钥 PK_a 的 SM3 哈希值 $H(PK_a)$ 将存入 TCM 中保存。芯片私钥由芯片厂商永久保存，固件私钥 SK_a 由固件厂商永久保存。

（2）芯片厂商对 BL0 代码进行 SM3 哈希运算。该哈希值 H(BL0) 和芯片公钥 PK_a 将保存在 TCM 中。

（3）芯片厂商使用芯片私钥 SK_a 对固件公钥 PK_b 进行签名，该签名 $S(SK_a, PK_b)$ 和芯片公钥 PK_a 将被储存在 BL1 代码（即 UEFI 代码）头中。

（4）固件厂商使用固件私钥 SK_b 对 BL1 代码进行签名，该签名 $S(SK_b, BL1)$ 和固件公钥 PK_b 也将被储存在 BL1 代码头中。

（5）为保障硬件完整性，防止未授权的硬件替换与篡改，采用 SM3 算法对关键硬件（如 CPU、硬盘等）的特征值进行哈希运算，生成的哈希值储存在 TCM 的受保护存储区域中。

2.3 验证流程

申威平台安全启动方案启动验证的流程如图 5 所示，有以下几个步骤：

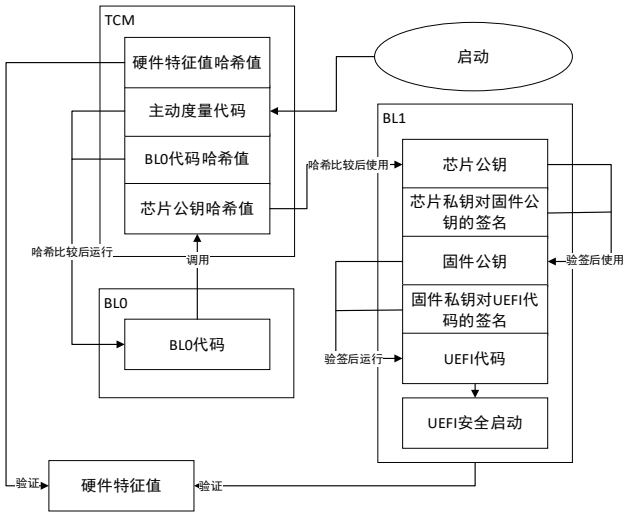

图 5 申威平台安全启动验证流程

（1）TCM 在主板上电的第一时间同时上电，其优先级属于第一优先级。在主板上电，TCM 上电自检之后，TCM 将主动度量 BL0 代码，即对 BL0 代码进行 SM3 哈希运算。该哈希值 H'(BL0) 同 TCM 中保存的 H(BL0) 比较，相等时验证通过，运行 BL0 代码。

（2）BL0 调用 TCM 对 BL1 头中储存的芯片公钥 PK_a 进行哈希运算，将运算的结果 $H'(PK_a)$ 同 TCM 中储存的哈希值 $H(PK_a)$ 进行比较，相等时再使用芯片公钥 PK_a 和固件公钥 PK_b 验签 $S(SK_a, PK_b)$。验签成功时对固件公钥 PK_b 的验证通过。

（3）使用固件公钥 PK_a 和 BL0 验签 $S(SK_b, BL1)$。验签成功时对 BL1 的验证通过，运行 BL1 代码。

（4）BL1 代码对需要验证的硬件的特征值进行 SM3 哈希运算，并同 TCM 中保存的值比对。相同时对硬件的验证通过。后续进行 UEFI 安全启动的流程。

2.4 UEFI 安全启动流程

申威平台安全启动方案将使用 shim 负责验证并加载 GRUB。因此会创建一个 MOK，用于对 GRUB 和系统内核签名。随后将该密钥签名的证书存入 shim 管理的列表中，从而使得 shim 能够验证 GRUB 和系统内核。

表 1 为 UEFI 安全启动所需的变量。

表 1 UEFI 变量

名称	描述
PK	平台密钥，由硬件的原始设备制造商（OEM）发布。可签名 KEK。
KEK	密钥加密密钥，既可用于对数据库进行数字签名，也可直接用于对可执行二进制文件进行签名。
db	签名数据库，被 KEK 签名，包含允许的证书或允许的校验和列表。与存储在 db 中的证书对应的 UEFI 二进制文件，会被固件信任。
dbx	禁止签名数据库，被 KEK 签名，收录了特定 UEFI 二进制文件、证书或被撤销 / 泄露的证书哈希值。当检测到二进制文件哈希值、二进制文件签名或用于签名的密钥被存入 dbx 时，系统将拒绝执行该文件。

UEFI 安全启动的验证流程如图 6 所示。PK 负责验证 KEK 的合法性；KEK 则进一步用于验证数据库 db 和 dbx。

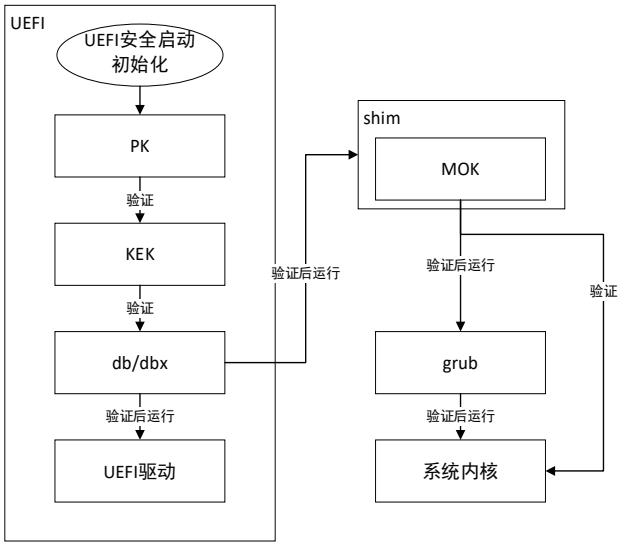

图 6 UEFI 安全启动验证流程

任何 UEFI 二进制文件（如引导加载程序），只要其数字签名能够通过 db 中存储的可信证书成功验证，即被视为可信，从而被加载执行。具体到典型的 Linux 安全启动流程，UEFI 固件首先会验证并执行 shim 引导程序。随后，shim 只要使用用户自主管理的 MOK（机器所有者密钥）列表来验证 GRUB 引导程序及 Linux 内核，验证通过后即将控制权移交，继续启动过程。

3 实验与分析

安全启动的核心目标在于防御针对设备启动阶段的各类攻击。在此类攻击场景中，攻击者可能篡改并植入恶意固件，从而劫持设备启动流程，进一步影响后续启动阶段。具体攻击手段包括植入恶意代码、替换操作系统内核或篡改内核配置等，最终实现本地劫持或远程操控设备。

目前，在主流安全启动机制中，基于可信 UEFI BIOS 对后续固件及操作系统进行完整性验证的技术已较为成熟。因此，本实验主要验证申威平台安全启动方案中从硬件可信根到可信 UEFI BIOS 之间的阶段信任链是否能够可靠传递，抵御各类攻击。文章设计了有效性对比实验：实验组分别对开启安全启动的系统和原申威系统（未开启安全启动） 实施相同类型的固件篡改攻击。由于公钥和固件均会存在闪存中，还设了针对存储于 BL1 头的芯片公钥与固件公钥的篡改攻击以及直接更改硬件的攻击。申威平台安全启动会对硬件进行验证，因此设计了直接更换硬件的攻击。另外，为了验证自主可控的安全机制的重要性，用泄露的芯片私钥对篡改后的固件重新签名，实施攻击。非自主可控的安全机制存在实际实现方式不公开，密钥不能自主控制的问题，密钥存在泄露风险。

实验环境为部署了国民技术 Z32H330TC 安全卡的申威 831 平台。

实验结果如表 2 所示。在有效性验证实验中，开启安全启动时，任何对启动代码的修改均导致了验证失败，启动过程被拦截。对硬件进行更改，则会导致硬件的特征值修改因而导致和 TCM 中储存的哈希值不匹配，验证失败。

表 2 有效性验证实验

攻击方式	是否开启安全启动	攻击结果
修改 BL0 代码	是	失败
修改 BL0 代码	否	成功
修改 UEFI 代码	是	失败
修改 UEFI 代码	否	成功
更改需要被验证的硬件	是	失败
更改需要被验证的硬件	否	成功
修改芯片公钥 PK_a，并相对应修改 SK_a 相关的签名	是	失败
修改固件公钥 PK_b，修改芯片公钥 SK_b，并相对应修改 SK_b 相关的签名	是	失败
在芯片私钥 SK_a 泄露时修改固件公钥 PK_b，并相对应修改 SK_b 相关的签名	是	成功

由于无法篡改安全根中的芯片私钥，对 BL1 头中公钥的修改同样会导致验证错误。原申威系统则会被攻击成功。芯片私钥泄露时攻击成功，攻击者则可以使用该密钥重新签名固件公钥从而篡改固件。这一攻击说明了自主可控，防止密钥泄露的重要性。

申威平台安全启动机制对于未被篡改的方案能够正确完成验证，并将控制权移交至可信 UEFI，确保安全启动进程继

续。这证明了申威平台安全启动机制的有效性。

4 结语

本文设计实现了申威平台安全启动机制，使用了先于CPU启动的TCM作为硬件可信根，采用国密算法逐级完成对下一阶段引导程序的验证，确保安全启动流程的自主可控。方案还采用两对公私钥进行签名。更新UEFI BIOS时，仅需使用受芯片密钥签名的固件密钥对更新后的固件重新签名即可，无需触及固件可信根，在保证安全性的情况下提供了较为灵活的固件更新方法。在实验中验证了本文申威平台安全启动机制的有效性。申威平台安全启动机制显著增强了申威平台的安全性，有效推进了我国信息领域的自主可控建设。

参考文献：

[1] 张晔嘉 . 国内信息系统自主可控生态环境分析 [J]. 电子质量 , 2019(7):58-61.

[2] 国家互联网信息办公室 . 国家互联网信息办公室就 H20 算力芯片漏洞后门安全风险约谈英伟达公司 [EB/OL]. (2025-07-31)[2026-05-08].https://www.cac.gov.cn/2025-07/31/c_1755675743897163.htm.

[3] 郜晨 , 何升 , 杭骁骞 . 基于申威 NMII 的锁死故障监测与诊断 [J]. 计算机应用研究 ,2024,41(4):1015-1021.

[4]Tao Zhenzhong, Rastogi A, Gupta N, et al. DICE*: a formally verified implementation of DICE measured boot[C]//30th USENIX Security Symposium.Berkeley: USENIX Association, 2021:1091-1107.

[5]Tygar J D, Yee B. Dyad: a system for using physically secure coprocessors[M].Pittsburgh: Carnegie Mellon University, 1994.

[6]UEFI Forum. Unified extensible firmware interface specification[EB/OL].(2024-12-21)[2026-05-08].https://uefi.org/specifications.

[7]Intel business client platform security marketing. Intel hardware shield below-the-os security: information technology cybersecurity white paper[EB/OL]. 2024[2026-05-08].https://www.intel.com/content/dam/www/central-libraries/us/en/documents/below-the-os-security-white-paper.pdf

[8]AMD. AMD security and server innovation[EB/OL].2013[2026-05-08].https://uefi.org/sites/default/files/resources/UEFI_PlugFest_AMD_Security_and_Server_innovation_AMD_March_2013.pdf.

[9]Apple Inc.Apple platform security[EB/OL].2013[2026-05-08].https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

[10] 国家密码管理局．可信密码支撑平台技术规范 [EB/OL]. 2007[2025-05-29]http://www.sca.gov.cn/sca/xwdt/2007-12/29/content_1002370.shtml.

[11] 张兴 , 沈昌祥 . 一种新的可信平台控制模块设计方案 [J]. 武汉大学学报 (信息科学版), 2008(10): 1011-1014.

[12]Rivest R L. RFC1321: the MD5 message-digest algorithm[R/OL].1992[2026-05-08].https://www.rfc-editor.org/info/rfc1321.

[13]NIST. SHA-3 standard: permutation-based Hash and extendable-output functions[R/OL]. 2015 [2026-05-08]. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf.

[14]Wang Xiaoyun, Yu Hongbo. SM3 cryptographic hash algorithm[J].Journal of Information Security Research, 2016, 2(11): 983−994.

[15]Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.

[16]Ahlswede R. Elliptic curve cryptosystems[J]. Hiding Data - Selected Topics,2016: 225-336.

[17] 国家市场监督管理总局 , 国家标准化管理委员会 . SM2 椭圆曲线公钥密码算法 [EB/OL]. (2016-08-29) [2026-05-08]. https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=3EE2FD47B962578070541ED468497C5B.

[18] 沈昌祥 , 张焕国 , 王怀民 , 等 . 可信计算的研究与发展 [J]. 中国科学 : 信息科学 ,2010,40(2):139-166.

[19]Trusted Computing Group.Trusted platform module 2.0 library part 0: introduction[EB/OL].(2025-12-11)[2026-05-08]. https://trustedcomputinggroup.org/wp-content/uploads/Trusted-Platform-Module-2.0-Library-Part-0-Introduction_Version-185_pub.pdf.

[20]Hagl J, Mann O, Pirker M. Securing the linux boot process: from start to finish[C]//Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP 2021). Vienna, Austria: SCITEPRESS, 2021:604-610.

【作者简介】

李之健（1998—），男，江苏无锡人，硕士，助理工程师，研究方向：固件工程，email: 893975587@qq.com。

苏卫强（1982—），男，福建龙岩人，硕士，高级工程师，研究方向：软件工程，email: ipaper_purple@163.com。

赵翊含（1999—），女，黑龙江哈尔滨人，本科，助理工程师，研究方向：固件工程，email: 757646459@qq.com。

（收稿日期：2025-10-31 修回日期：2026-05-14）