TECNOLOGIAS AMD PRO

UMA ANÁLISE DA SEGURANÇA AMD PRO E DA ESTRUTURA AMD PARA PCS EMPRESARIAIS SEGUROS, GERENCIÁVEIS E CONFIÁVEIS

O ambiente de trabalho ágil e distribuído continua a evoluir. As operações híbridas estão se tornando a norma, com as empresas equilibrando a colaboração presencial e o trabalho remoto, ao mesmo tempo em que integram a IA aos fluxos de trabalho diários. As empresas enfrentam uma pressão crescente para atualizar seus PCs com sistemas que lidam com os novos desafios apresentados por tais tendências. Elas precisam de soluções que equilibrem desempenho, segurança e capacidade de gerenciamento enquanto se adaptam aos ambientes locais e baseados em nuvem.

Os processadores AMD Ryzen™ PRO capacitam os PCs empresariais modernos com as tecnologias AMD PRO, um conjunto unificado de inovações projetado para atender às demandas em constante mudança das empresas de hoje. Este documento explora o pilar de segurança das Tecnologias AMD PRO, um dos três componentes fundamentais de todos os sistemas equipados com processadores AMD Ryzen PRO. Embora a segurança seja o foco principal deste documento, as Tecnologias AMD PRO também incluem capacidade de gerenciamento avançada e confiabilidade pronta para os negócios, que, juntas, fornecem uma solução abrangente para empresas modernas.

Os três pilares são apresentados aqui para fornecer contexto para as Tecnologias AMD PRO como um todo, mas a discussão neste documento se concentrará especificamente nos recursos de segurança de nível superior dos processadores AMD Ryzen PRO, que são projetados para proteger os PCs empresariais de hoje contra ameaças em evolução.

SEGURANÇA PRO: PROTEGENDO A EMPRESA MODERNA

A base das Tecnologias AMD PRO são recursos de segurança robustos. Recursos avançados de hardware, como o AMD Memory Guard[1] para criptografia total de memória, o AMD Shadow Stack projetado para proteção contra ataques de fluxo de controle e o suporte abrangente para o processador de criptografia segura Pluton da Microsoft, fornecem proteções críticas contra ameaças sofisticadas. Com suporte integrado para inicialização segura[2] e execução confiável, os processadores AMD Ryzen PRO fortalecem os dispositivos em todas as camadas, oferecendo proteção aos dados e aplicativos do usuário, do endpoint até a nuvem.

Embora os recursos de segurança de última geração sejam o foco deste documento, a estrutura mais ampla das Tecnologias AMD PRO, incluindo capacidade de gerenciamento e confiabilidade pronta para os negócios, funciona em conjunto para fornecer às empresas uma solução completa para as demandas emergentes do local de trabalho.

CAPACIDADE DE GERENCIAMENTO PRO: SIMPLIFICANDO AS OPERAÇÕES DE TI

O gerenciamento de diversos PCs é complexo e demorado, especialmente em ambientes de trabalho híbridos. A Capacidade de gerenciamento AMD PRO simplifica as operações com ferramentas baseadas em padrões abertos que possibilitam o gerenciamento remoto baseado em nuvem e o monitoramento de endpoint em tempo real. Essas ferramentas oferecem o mais alto nível de conformidade com padrões abertos para gerenciamento remoto de sistemas.[3] A Capacidade de gerenciamento AMD PRO ajuda a oferecer ao usuário compatibilidade com ferramentas líderes do setor, como o Microsoft Endpoint Manager e o Windows Autopilot, proporcionando um processo de implantação consistente e eficiente.

A Capacidade de gerenciamento AMD PRO suporta as mais recentes especificações DMTF DASH (Desktop and Mobile Architecture for System Hardware, Arquitetura de desktop e dispositivo móvel para hardware do sistema), incorporando protocolos de criptografia e autenticação atualizados, como TLS 1.2 e 1.3. Além disso, os sistemas AMD PRO integram componentes de segurança baseados em hardware, incluindo o TPM 2.0, para possibilitar armazenamento e proteção de chave criptográfica mais seguros. Essa abordagem baseada em padrões oferece proteção mais forte e melhor desempenho em comparação com protocolos proprietários mais antigos.[4] As equipes de TI se beneficiam de recursos como provisionamento remoto, implantação automatizada de correções de erros e diagnóstico em tempo real, que ajudam a reduzir o tempo de inatividade, melhorar a integridade do endpoint e simplificar as operações.

Estudos recentes destacam o impacto da Capacidade de gerenciamento AMD PRO nas operações de TI, mostrando os tempos de implantação reduzidos em até 41%[5] em comparação aos processos tradicionais e uma redução significativa no esforço prático graças às interfaces de gerenciamento unificadas e intuitivas. Esses recursos ajudam a dar às empresas a capacidade de oferecer suporte aos funcionários onde quer que trabalhem, tornando os ecossistemas de PC complexos mais simples, rápidos e confiáveis de gerenciar.

PRO PRONTO PARA EMPRESAS: DESEMPENHO CONFIÁVEL PARA CADA TAREFA

Os processadores AMD PRO com recursos prontos para empresas ajudam a proporcionar aos usuários longevidade do PC, desempenho consistente e confiabilidade para cargas de trabalho empresariais. Processos de validação rigorosos suportam melhor tempo de atividade, o que pode ajudar a reduzir os custos de TI. A disponibilidade mundial estendida em um ano inteiro permite que as empresas implantem sistemas sob demanda, minimizando a necessidade de grandes compras à vista. Seja oferecendo suporte a aplicativos orientados por IA ou a tarefas rotineiras de escritório, os processadores AMD Ryzen™ PRO oferecem a adaptabilidade de que as empresas precisam para prosperar.

Figura 1. Tecnologias AMD PRO. Capacitando todos os PCs empresariais equipados com processador AMD Ryzen™ PRO.

As tecnologias AMD PRO prontas para empresas aumentam essa confiabilidade, fornecendo consistência de longo prazo que simplifica o planejamento de TI e maximiza o retorno do investimento. Todos os processadores AMD Ryzen™ PRO oferecem soluções de nível empresarial com:

- **Estabilidade de imagem:** 18 meses de estabilidade de software planejada para ajudar a fornecer transições suaves e tranquilidade para as equipes de TI.
- **Qualidade:** processos de validação de plataforma avançados que fornecem qualidade de nível empresarial para ambientes de negócios exigentes.
- **Disponibilidade:** 24 meses de disponibilidade planejada para manter a consistência do hardware para operações empresariais estáveis.
- **Confiabilidade:** validação de plataforma contínua para garantir estabilidade de longo prazo e uma experiência de usuário consistente em processadores de várias gerações.

Ao fornecer estabilidade em hardware e software, o AMD PRO pronto para empresas reduz a complexidade para as equipes de TI e oferece uma base confiável para o sucesso empresarial a longo prazo.

À medida que as empresas navegam pelas complexidades de dar suporte ao novo local de trabalho, as Tecnologias AMD PRO oferecem uma vantagem crucial. Ao integrar recursos de segurança com tecnologia de ponta, capacidade de gerenciamento eficiente e recursos prontos para empresas em cada sistema equipado com CPU AMD Ryzen PRO, a AMD equipa as organizações com as ferramentas necessárias para ajudar a proteger suas operações, simplificar o gerenciamento de TI e impulsionar a inovação.

Figura 2. Segurança AMD PRO. Superando os requisitos de segurança mais recentes para dispositivos modernos.

OS PCS DA AMD SÃO PROJETADOS COM SEGURANÇA MULTICAMADA COM TECNOLOGIA DE PONTA EM TODOS OS NÍVEIS

A AMD trabalha de perto com desenvolvedores de Sistemas Operacionais (SO) e fabricantes de equipamento original (OEMs) para fornecer recursos de segurança de hardware que complementem e fortaleçam seus projetos de segurança.

Ao incorporar medidas de segurança com tecnologia de ponta em todos os níveis, desde chip até sistemas operacionais, a AMD capacita as organizações a proteger seus ativos mais importantes, minimizando o tempo de inatividade e reduzindo a complexidade de TI.

SEGURANÇA INTEGRADA EM TODAS AS CAMADAS

As Tecnologias AMD PRO integram a segurança como um pilar fundamental em todos os dispositivos equipados com processadores AMD Ryzen™ PRO. Projetados para os desafios em evolução da empresa moderna, esses processadores oferecem proteção multicamada que começa com uma base de chip robusta e se estende por meio de defesas no nível de firmware e sistema operacional.

RAIZ DE CONFIANÇA DE HARDWARE: INTEGRIDADE DESDE O INÍCIO

A arquitetura do chip da AMD fornece uma raiz de confiança de hardware integrada que auxilia os processos de inicialização segura. O processador AMD Secure 2.0[6] (ASP 2.0) ancora essa confiança, verificando a integridade do firmware e da BIOS do OEM para se defender contra modificações não autorizadas e possíveis ataques de firmware.

PROTEÇÃO DE MEMÓRIA REDEFINIDA: AMD MEMORY GUARD[7]

O AMD Memory Guard criptografa toda a memória do sistema em tempo real, ajudando a proteger dados confidenciais contra ataques físicos e de inicialização a frio. Com mecanismos dedicados de criptografia de hardware, esse recurso ajuda a fornecer uma defesa robusta mesmo em cenários que envolvem roubo de dispositivos.

ARQUITETURA DE ÚLTIMA GERAÇÃO: AMD "ZEN 5" E ALÉM

A mais recente arquitetura de núcleo AMD "Zen 5" apresenta recursos de segurança avançados, incluindo a Segurança da Cadeia de Suprimentos, que aproveita uma ID de processador exclusiva para possibilitar o rastreamento seguro de hardware AMD genuíno durante todo o seu ciclo de vida. Essas inovações fortalecem a resiliência de endpoint contra ameaças cibernéticas cada vez mais sofisticadas.

ALINHADOS COM OS PADRÕES DA INDÚSTRIA

Os processadores AMD PRO foram criados para superar os requisitos de segurança modernos, incluindo a certificação FIPS 140-3 Nível 1 . A integração com o Microsoft Pluton[8] aumenta ainda mais a proteção para sistemas baseados no Windows, adicionando autenticação segura e proteções criptográficas.

A ARQUITETURA DE SEGURANÇA AMD PRO

PROCESSADOR AMD SECURE 2.0:[9] UMA BASE MAIS FORTE

No núcleo da Arquitetura de Segurança AMD PRO está o processador AMD Secure 2.0 (ASP 2.0), um componente de hardware dedicado incorporado em cada sistema em chip (SoC). O ASP 2.0 ancora uma raiz de confiança de hardware e suporta um fluxo de inicialização segura, verificando a integridade do firmware a partir do momento em que um dispositivo é ligado. Seu ambiente de execução confiável isolado ajuda a manter as operações confidenciais protegidas contra possíveis ataques. Os principais componentes incluem:

- **Coprocessador criptográfico (CCP):** um mecanismo criptográfico de alto desempenho que gerencia a geração de chaves e operações criptográficas em hardware, essenciais para tarefas de segurança urgentes.
- **ROM de inicialização:** memória somente leitura segura contendo firmware essencial para inicialização.
- **Memória de Acesso Aleatório Estática (SRAM):** fornece suporte de baixo consumo de energia para processos seguros.
- **Unidade de Gerenciamento de Memória (MMU):** controla o acesso à ROM de inicialização e SRAM para controle rigoroso sobre os recursos de memória.
- **Recuperação bare-metal em nuvem:** facilita a recuperação segura de dispositivos por meio da nuvem, permitindo a continuidade dos negócios mesmo em situações de falhas catastróficas.
- **Segurança da cadeia de suprimentos:** autentica hardware AMD genuíno em cada fase do seu ciclo de vida, protegendo contra adulteração ou falsificação de componentes.
- **Temporizador guardião:** detecta e atenua processos paralisados no nível do hardware, aumentando a resiliência do sistema.

Esses recursos abordam coletivamente o risco elevado de exposição de dados corporativos confidenciais durante viagens, trabalhos remotos ou outros cenários móveis.

INTEGRAÇÃO PERFEITA COM A SEGURANÇA DO WINDOWS

A Arquitetura de Segurança AMD PRO se alinha perfeitamente com os recursos de segurança do Windows 11, como a inicialização segura e a proteção de pilha reforçada por hardware, para criar um sistema de defesa abrangente e multicamadas. Juntos, eles fortalecem os endpoints contra ataques direcionados a firmware, BIOS, drivers e sistema operacional.

BLINDAGEM AMD ROM

A memória flash SPI (Serial Peripheral Interconnect, interconexão periférica serial) em uma placa-mãe contém o UEFI da placa-mãe e informações adicionais de configuração, incluindo o status de inicialização segura.

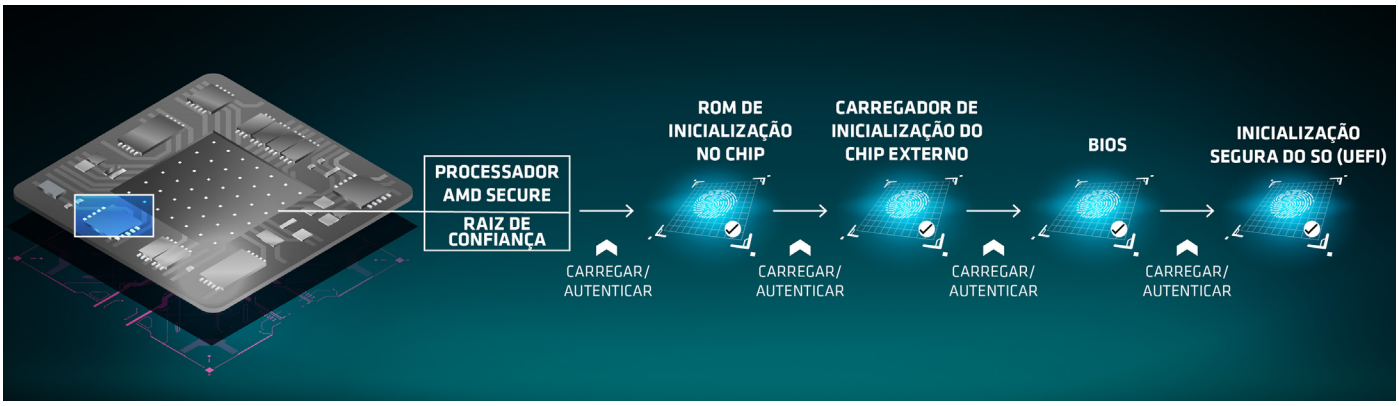
A Blindagem AMD ROM opera antes da inicialização do sistema operacional e fornece proteção contra modificações não autorizadas na flash SPI. Ao fornecer a integridade da flash SPI antes do carregamento do sistema operacional, a Blindagem AMD ROM ajuda a estabelecer uma base reforçada para o sistema. Depois que a Blindagem AMD ROM é configurada e ativada, o dispositivo flash SPI do computador é reforçado contra gravações não autorizadas.

INICIALIZAÇÃO SEGURA DA PLATAFORMA (PSB) AMD

A Inicialização Segura da Plataforma (PSB, Platform Secure Boot) AMD oferece uma raiz de confiança (RoT, root of trust) de hardware para autenticar o firmware inicial, incluindo a BIOS, durante o processo de inicialização do dispositivo. Quando um sistema é ligado, o ASP executa o código da ROM de inicialização do ASP, que autentica vários códigos do carregador de inicialização do ASP antes de iniciar o chip e a memória do sistema. Quando a memória do sistema é inicializada, o código do carregador de inicialização do ASP verifica o código da BIOS do OEM, autenticando outros componentes de firmware antes de o sistema operacional ser inicializado.

A PSB foi projetada para garantir a integridade da plataforma, oferecendo uma proteção mais forte contra firmware malicioso ou nocivo, negando-lhe acesso automaticamente após a detecção. A PSB da AMD ajuda a proteger a transição do firmware de baixo nível para o sistema operacional.

Figura 3. Inicialização Segura da Plataforma AMD.



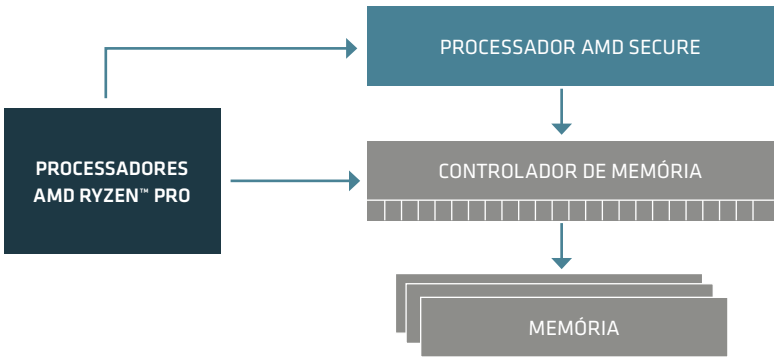
AMD MEMORY GUARD[3]

O AMD Memory Guard é uma tecnologia abrangente de criptografia de memória projetada para proteger os dados do cliente contra ataques físicos. Com o AMD Memory Guard, todo o conteúdo da DRAM é criptografado utilizando uma chave aleatória que ajuda a proteger contra inicialização física a frio, espionagem da interface DRAM e ataques parecidos.

Para sistemas com NVDIMMs, o AMD Memory Guard também ajuda a proteger contra um invasor, removendo um módulo de memória e tentando extrair seu conteúdo, implementado por meio de um hardware dedicado nos controladores de memória embutidos (on-die).

- Cada controlador inclui um mecanismo Advanced Encryption Standard (AES) de alto desempenho que criptografa os dados quando eles são gravados na DRAM e os descriptografa quando lidos.
- Uma chave de 128 bits é gerada por um gerador de números aleatórios de hardware compatível com NIST SP 800-90 on-die, em um modo que utiliza um ajuste adicional baseado em endereço físico para ajudar a proteger contra ataques de movimentação de blocos de texto cifrado.
- A chave de criptografia usada pelo mecanismo AES com o AMD Memory Guard é gerada aleatoriamente em cada redefinição do sistema e não é visível para nenhum software em execução nos núcleos da CPU. Essa chave é gerenciada inteiramente pelo Processador AMD Secure (ASP).

Figura 4. AMD Memory Guard.



AMD SHADOW STACK

A ROP (Return-Oriented Programming, programação orientada para retorno) é um vetor de ataque cada vez mais popular. Os ataques ROP não injetam seu próprio código malicioso. Em vez disso, eles tentam obter o controle de um sistema explorando as fraquezas do código legítimo.

COMO ISSO FUNCIONA?

Na programação computacional, uma "rotina" executa um determinado conjunto de operações. Quando um programa de software é executado, isso se chama rotina. Quando uma rotina termina seu trabalho, ela retorna ao programa principal usando o endereço de retorno. Este processo é chamado de "pular e retornar".

Nos ataques ROP, os agressores alteram o endereço de retorno da rotina de pular. Assim, em vez de voltar para o programa principal, ela pula para diferentes rotinas, reunindo subrotinas para criar um código malicioso que agora pode prejudicar o sistema. E o mais importante é que esse tipo de ataque não é detectado porque parece código legítimo.

A Arquitetura de Segurança AMD PRO ajuda a mitigar ataques ROP, oferecendo acesso ao software para registros especiais na CPU, onde uma cópia do endereço de retorno pode ser armazenada. Os aplicativos podem utilizar uma pilha paralela, chamada de "shadow stack", para ajudar a mitigar ataques de software que tentam modificar o fluxo de controle. O shadow stack usa hardware especializado para armazenar uma cópia dos endereços de retorno, que é comparada à pilha normal do programa em operações de retorno.

Se o conteúdo for diferente, uma exceção será gerada, o que pode ajudar a evitar que códigos maliciosos obtenham controle do sistema. Dessa forma, o hardware com shadow stack pode ajudar a mitigar alguns dos bugs de software mais comuns e exploráveis.

O AMD Shadow Stack acrescenta robustez contra ataques ROP. Como uma cópia do endereço de retorno fica no hardware, é muito difícil para códigos maliciosos interferirem.

O Microsoft Hardware Enforced Stack Protection é compatível com a Arquitetura de Segurança AMD PRO que usa o AMD Shadow Stack.

MICROSOFT SECURED-CORE PC

O Microsoft Secured-Core PC ajuda a proteger seu dispositivo contra vulnerabilidades de firmware, defende o sistema operacional contra ataques, e pode prevenir o acesso não autorizado a dispositivos e dados por meio de controles de acesso avançados e sistemas de autenticação.

O Secured-Core PC é ativado nas plataformas de Arquitetura de Segurança AMD PRO usando várias tecnologias e serviços de segurança:

- AMD-V™ com GMET
- AMD Secure Init and Jump with Attestation (SKINIT)
- AMD Secure Loader (SL)
- AMD Dynamic Root of Trust Measurement (DRTM)
- Supervisor de Modo de Gerenciamento de Sistemas (SMM) AMD
- Proteção de Acesso Direto à Memória (DMA)

TECNOLOGIA DE VIRTUALIZAÇÃO AMD (AMD-V™) COM GMET

O AMD-V é um conjunto de extensões de hardware que possibilitam a virtualização em plataformas AMD. O Guest Mode Execute Trap (GMET) é um aprimoramento de desempenho de chip que possibilita que o hipervisor lide com eficiência com verificações de integridade de código e ajude a proteger contra malware.

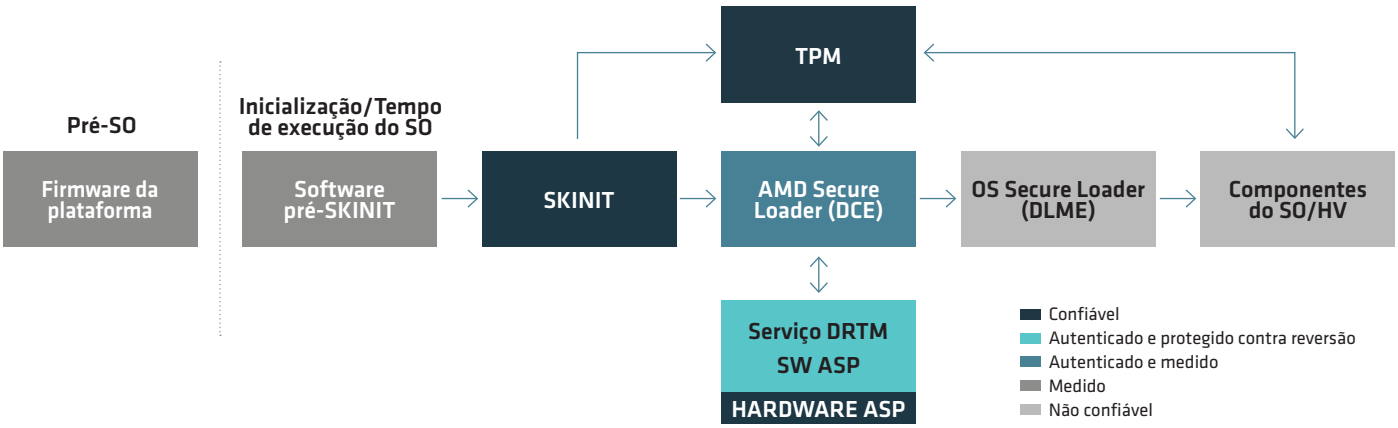
SECURE INIT AND JUMP WITH ATTESTATION (SKINIT)

A instrução SKINIT ajuda a criar uma "raiz de confiança", começando com um modo de operação inicialmente não confiável. A SKINIT reinicializa o processador para estabelecer um ambiente reforçado de execução para um componente de software chamado de Secure Loader (SL), e inicia a execução do SL para ajudar a evitar interferências. A SKINIT estende a raiz de confiança baseada em hardware para o secure loader.

AMD SECURE LOADER (SL)

O AMD Secure Loader é responsável por validar a configuração da plataforma, interrogando o hardware e solicitando informações de configuração do serviço de DRTM oferecido pelo Processador AMD Secure.

Figura 5. Fluxo de DRTM.



A qualquer momento após o sistema inicializar no SO, o sistema operacional pode solicitar que o bloco de serviço AMD reavalie e ateste os valores antes de executar outras operações. Dessa forma, o SO pode ajudar a proteger a integridade do sistema desde a inicialização até o tempo de execução.

AMD DYNAMIC ROOT OF TRUST MEASUREMENT (AMD DRTM)

O bloco AMD DRTM é composto pela instrução de CPU SKINIT, pelo ASP e pelo SL. Este bloco é responsável por criar e manter uma corrente de confiança entre o firmware. O AMD DRTM trabalha com o conceito de que o firmware e o carregador de inicialização podem carregar livremente, partindo do pressuposto de que são códigos desprotegidos e sabendo-se que, logo após a inicialização do sistema, haverá a transição para um estado confiável, com o hardware forçando o firmware de baixo nível por um caminho de códigos conhecido e medido.

O bloco AMD DRTM é composto pela instrução de CPU SKINIT, pelo ASP e pelo SL. Este bloco é responsável por criar e manter uma corrente de confiança entre o firmware.

O AMD DRTM trabalha com o conceito de que o firmware e o carregador de inicialização podem carregar livremente, partindo do pressuposto de que são códigos desprotegidos e sabendo-se que, logo após a inicialização do sistema, haverá a transição para um estado confiável, com o hardware forçando o firmware de baixo nível por um caminho de códigos conhecido e medido.

O bloco DRTM mede e autentica o carregador de inicialização, e coleta e armazena as seguintes informações do sistema de maneira defendida para uso futuro pelo sistema operacional, incluindo verificação e atestamento:

- Mapa de memória física
- Localização espacial da configuração PCI
- Configuração APIC local
- Configuração APIC de E/S
- Configuração da IOMMU/Configuração da TMR
- Configuração de gerenciamento de energia

CONFIANÇA DE HARDWARE COMPARTILHADA

Isso significa que o componente de firmware é autenticado e medido pelo bloco ASP no chip AMD, e a medida é armazenada de maneira protegida para uso futuro pelo sistema operacional, incluindo verificação e atestamento.

AMD SMM SUPERVISOR

O Modo de Gerenciamento de Sistema (SMM, System Management Mode) é um modo de CPU de finalidade especial em microcontroladores x86 que lida com gerenciamento de energia, configuração de hardware, monitoramento térmico e outras operações no nível do dispositivo. Sempre que uma dessas operações de sistema são solicitadas, uma interrupção (SMI) é invocada no tempo de execução, executando o código SMM instalado pela BIOS. O código SMM é executado no maior nível de privilégio e é invisível para o sistema operacional, tornando-o um alvo atraente para atividades maliciosas que podem ser usadas para acessar a memória do hipervisor e comprometê-lo.

O manipulador de SMI geralmente é fornecido por um desenvolvedor diferente do sistema operacional e tem acesso à memória e aos recursos do SO/hipervisor. Isso significa que vulnerabilidades exploráveis no código do SMM podem resultar em comprometimentos do sistema operacional, do Hipervisor (HV) e da segurança baseada em virtualização (VBS) do Windows.

Para ajudar a isolar o SMM, a AMD introduz um módulo de segurança chamado AMD SMM Supervisor, que é executado imediatamente antes do controle ser transferido para o manipulador de SMI após a ocorrência de uma SMI. O AMD SMM Supervisor reside no bloco de serviço AMD DRTM e é usado para:

- Bloquear a habilidade do SMM de modificar o hipervisor ou a memória do SO, exceto por um pequeno espaço de comunicação entre os dois
- Evitar que o SMM introduza novos códigos SMM durante o tempo de execução
- Bloquear o acesso do SMM ao DMA, E\S ou registros que possam comprometer o hipervisor ou o sistema operacional

PROTEÇÃO DE DMA

Com a tecnologia de remapeamento de DMA, as plataformas AMD suportam a proteção de acesso direto à memória (DMA, Direct Memory Access) nos ambientes pré-inicialização e de sistema operacional por meio de tecnologias de segurança da AMD como a Input Output Memory Management Unit (IOMMU).

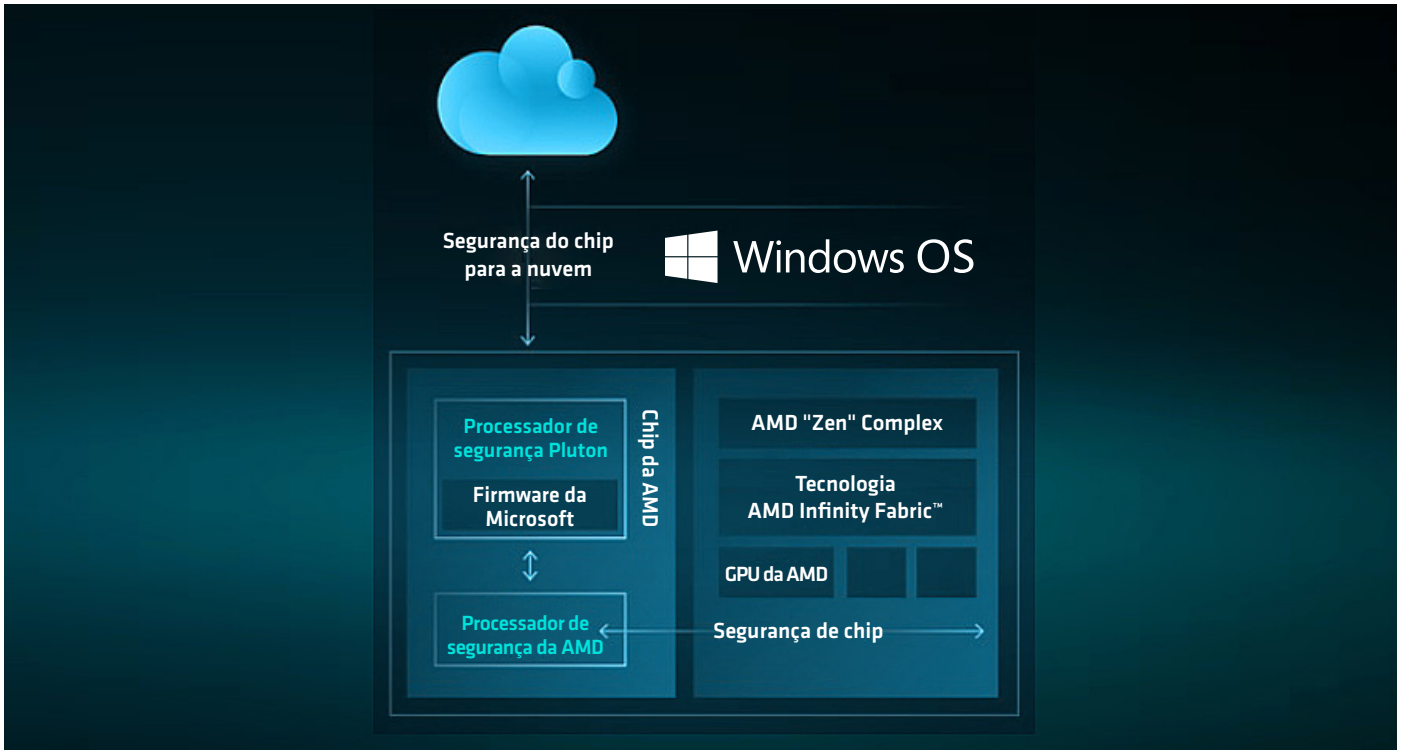
- A proteção de DMA ajuda a proteger contra um possível ataque no firmware da plataforma no qual adversários possam usar dispositivos conectados para realizar ataques de DMA.
- O DMA fornece aos dispositivos acesso direto ao espaço de endereço da memória física para melhor desempenho. Contudo, isso também facilita para que softwares maliciosos injetem malware no sistema, que pode não ser detectado pelo sistema operacional.

Para ajudar a evitar esse tipo de ataque, a AMD projetou uma arquitetura de segurança para gerenciar e controlar o acesso ao DMA do dispositivo por meio da IOMMU no nível de firmware pré-sistema operacional. A arquitetura de segurança do DMA transfere a responsabilidade pelas configurações de proteção da memória do sistema do firmware para o SO depois que o carregador de inicialização do SO é estabelecido na memória. A proteção de DMA usando IOMMU é aplicada em cada inicialização, até que o SO assuma o controle da própria IOMMU.

PROCESSADOR DE SEGURANÇA MICROSOFT PLUTON[8]

Projetado pela Microsoft e criado por parceiros de chip, o Microsoft Pluton é um processador de criptografia segura integrado à CPU para segurança no núcleo para ajudar a confirmar a integridade do código e a proteção mais recente com atualizações fornecidas pela Microsoft por meio do Windows Update.

Figura 6. Visão geral da Arquitetura de Segurança do Microsoft Pluton.



O Pluton protege credenciais, identidades, dados pessoais e chaves de criptografia. As informações são significativamente mais difíceis de remover, mesmo se um invasor tiver instalado malware ou tiver posse física completa do PC.

O Microsoft Pluton foi projetado para fornecer a funcionalidade TPM (Trusted Platform Module, Módulo de Plataforma Confiável) e outras funcionalidades de segurança além do que é possível com a especificação TPM 2.0. Ele permite que o firmware do Pluton e recursos de SO adicionais sejam fornecidos ao longo do tempo por meio do Windows Update.

O processador AMD Secure 2.0 (ASP 2.0) e o processador de segurança Microsoft Pluton coexistem no chip do cliente AMD e se comunicam para ajudar a proteger a integridade do dispositivo. O Microsoft Pluton ajuda a proteger os sistemas de PC Windows, agindo como uma raiz de confiança de hardware integrada para o ecossistema Windows, enquanto o ASP 2.0 atua como a raiz de confiança de hardware de chip, o que ajuda a fornecer integridade autenticando o firmware inicial carregado nas plataformas.

ATUALIZAÇÃO DE PLATAFORMA

Os processadores AMD PRO fornecem defesas de segurança contra invasores que tentam obter acesso ao sistema em tempo real e um mecanismo robusto de atualização. Isso possibilita que as organizações atualizem suas plataformas para corrigir vulnerabilidades criadas por bugs de hardware ou software.

A AMD trabalha em estreita colaboração com OEMs para fornecer uma arquitetura de atualização de plataforma reforçada, que esteja em conformidade com as práticas recomendadas e que possa ser integrada às soluções de atualização de plataforma de OEMs. Além disso, os processadores AMD PRO têm um recurso Firmware Anti-Rollback (FAR) que possibilita que a política baseada em hardware bloqueie o downgrade do firmware do processador AMD Secure 2.0 (ASP 2.0). Por fim, os processadores AMD PRO também oferecem uma estrutura de recuperação segura chamada A/B Recovery, que pode ser integrada a uma solução de OEM para possibilitar a recuperação em caso de falha catastrófica.

ACELERADOR DE CRIPTOGRAFIA

No mundo de hoje, as operações de criptografia são importantes para ajudar a proteger dados e comunicações. Embora sejam essenciais, as operações de criptografia também são intensas em termos computacionais. A AMD fornece novas instruções otimizadas em chip para ajudar a fornecer baixos custos associados à computação de algoritmos criptográficos.

As arquiteturas AMD "Zen 2" e posteriores adicionaram suporte para criptografia AES vetorizada para 256 bits (vAES256) e integraram intrínsecos AES no nível x86, permitindo que os aplicativos do usuário se beneficiem de desempenho criptográfico e eficiência aprimorados.

CERTIFICAÇÃO FIPS 140-3 NÍVEL 1

Dada a natureza confidencial dos dados com os quais as agências governamentais lidam e os serviços essenciais que oferecem, a segurança de endpoints é uma das principais preocupações ao considerar notebooks para compras de TI do governo. Hardware desatualizado, sem recursos de segurança modernos, pode causar altos custos em termos de perda de dados e interrupções de serviço.

Os Padrões Federais de Processamento de Informações (FIPS Federal Information Processing Standards) dos Estados Unidos são um conjunto de padrões anunciados publicamente que o Instituto Nacional de Padrões e Tecnologia (NIST, National Institute of Standards and Technology) desenvolveu para uso em sistemas de computador de agências governamentais americanas não militares e colaboradores.
Os padrões FIPS estabelecem requisitos para segurança e interoperabilidade de computadores.

Os processadores AMD PRO incluem a certificação de segurança da indústria **FIPS 140-3 Nível 1**.

Figura 7. Programa de validação de algoritmo criptográfico para processadores AMD Ryzen™ PRO Série 7000.

Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PROJECTS | CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM

Cryptographic Algorithm Validation Program CAVP

Implementation Name: AMD Ryzen PRO 7000 Series PSP Cryptographic CoProcessor (SHA2_RSAPSS_SIGVER)
Description: The AMD PSP Cryptographic CoProcessor provides cryptographic algorithm support for the Ryzen PRO 7000 Series processor. The following cipher implementation is covered: SHA2-384 and RSA-PSS sigver implementation.
Version: bc0c0140FIPS001
Type: HARDWARE
Vendor: Advanced Micro Devices (AMD)
2485 Augustine Drive
Santa Clara, CA 95054
USA
Contacts: FIPS Contact
FIPS@amd.com
+1 408-749-4000

A3018 First Validated: 11/18/2022

Collapsed | Expanded | Aggregated

Operating Environment	Algorithm Capabilities
AMD Ryzen PRO 7330U (100-000000950)	RSA SigVer (FIPS186-4)
AMD Ryzen PRO 7530U (100-000000949)	RSA SigVer (FIPS186-4)
AMD Ryzen PRO 7730U (100-000000948)	RSA SigVer (FIPS186-4)
AMD Ryzen PRO 7330U (100-000000950)	SHA2-384
AMD Ryzen PRO 7530U (100-000000949)	SHA2-384
AMD Ryzen PRO 7730U (100-000000948)	SHA2-384

O módulo FIPS é uma combinação de hardware e/ou software e/ou firmware que suporta funções de segurança a serem certificadas. Embora o FIPS tenha sido desenvolvido para uso pelo governo federal, muitas empresas do setor privado usam voluntariamente esses padrões, incluindo instituições financeiras e provedores de nuvem. Além disso, o FIPS está expandindo para além da América do Norte, incluindo processadores de computador para parceiros europeus da OTAN.

RECUPERAÇÃO BARE-METAL EM NUVEM

A recuperação bare-metal em nuvem fornece um mecanismo seguro para recuperar sistemas remotamente, minimizando o tempo de inatividade e dando suporte à continuidade dos negócios em caso de falhas catastróficas de hardware ou software. Esse recurso é ativado antes da inicialização do SO para permitir a recuperação do sistema via nuvem sem exigir que o dispositivo seja enviado para manutenção.

Ao integrar-se com a Arquitetura de Segurança AMD PRO, a recuperação bare-metal em nuvem ajuda a fornecer inicialização e recuperação reforçadas no nível do hardware, que é projetado para proteger contra adulteração ou exploração durante o processo de recuperação.

SEGURANÇA DA CADEIA DE SUPRIMENTOS (IDENTIDADE DO DISPOSITIVO)

A Segurança da Cadeia de Suprimentos, habilitada pela Identidade de Dispositivo AMD, autentica o hardware da AMD durante todo o seu ciclo de vida, desde a fabricação até a implantação e além. Esse recurso ajuda a fornecer rastreabilidade e defende contra componentes falsificados ou adulterados, oferecendo garantia às empresas sobre a integridade de seu hardware.

A Identidade de Dispositivo AMD fornece verificação criptográfica do chip AMD genuíno, para que somente o hardware autêntico seja integrado aos sistemas empresariais. Isso ajuda a proteger contra ataques à cadeia de suprimentos que podem comprometer o firmware ou o hardware antes da implantação.

TEMPORIZADOR GUARDIÃO

O Temporizador Guardião aumenta a confiabilidade do sistema, detectando e atenuando processos parados ou não-responsivos no nível do hardware. Essa funcionalidade fornece tolerância a falhas adicional, ajudando os sistemas a permanecer operacionais e a se recuperar harmoniosamente de possíveis problemas.

Integrado à Arquitetura de Segurança AMD PRO, o Temporizador Guardião funciona com inicialização segura e outros recursos básicos para fornecer uma detecção robusta de falhas durante operações de pré-inicialização e tempo de execução. Essa capacidade fortalece a resiliência do sistema em ambientes de missão crucial e reduz o risco de tempo de inatividade causado por falhas de software ou hardware.

DESTAQUES DE SOLUÇÃO

CAMADA DE SEGURANÇA	RECURSOS	BENEFÍCIOS
SISTEMA	RECURSOS DE SEGURANÇA OEM	Colaboração profunda entre desenvolvedor de SO, fornecedor de hardware e parceiros OEM para complementar e ativar recursos de segurança de nível empresarial de OEM.
SEGURANÇA DO SO	SEGURANÇA DO WINDOWS 11	Suporte total para a iniciativa de PC com núcleo seguro, proteção de pilha reforçada por hardware, proteção avançada contra ameaças, login avançado, BitLocker e muitos mais.
HARDWARE E FIRMWARE	PROCESSADOR AMD SECURE 2.0	Processador de segurança dedicado que valida o código antes de ser executado para ajudar a garantir a integridade dos dados e aplicativos.
	INICIALIZAÇÃO SEGURA DA PLATAFORMA AMD	Proteção de inicialização que ajuda a impedir que software e malware não autorizados assumam funções críticas do sistema.
	AMD MEMORY GUARD	Fornece criptografia em tempo real da memória do sistema para ajudar na defesa contra ataques físicos caso você perca seu notebook ou ele seja roubado.
	AMD SHADOW STACK	Abordagem de segurança robusta para ajudar a proteger contra ataques de fluxo de controle, verificando a pilha normal do programa em relação a uma cópia armazenada em hardware e habilitando a segurança do Microsoft Hardware Enforced Stack Protection no Windows 11®.
	PROCESSADOR DE SEGURANÇA MICROSOFT PLUTON	Uma tecnologia de segurança do chip para nuvem projetada e atualizada pela Microsoft, que aumenta a segurança do núcleo do Windows 11 com proteção contínua para credenciais de usuário, identidades, dados pessoais e criptografia.
	TPM DO FIRMWARE DA AMD	Um TPM de versão de firmware que fornece autenticidade à plataforma e ajuda a monitorar sinais de violações de segurança.
	CERTIFICAÇÃO DO MÓDULO FIPS 140-3 DE NÍVEL 1	Padrão de criptografia do governo adotado pelo setor privado como a melhor prática para validar a segurança do hardware criptográfico.
	PROCESSADOR AMD SECURE 2.0	Ancora uma raiz de confiança de hardware, validando o firmware inicial e protegendo a plataforma contra código não autorizado.
	RECUPERAÇÃO BARE-METAL EM NUVEM	Ajuda a permitir a recuperação segura do sistema por meio da nuvem sem exigir o envio de dispositivos, projetado para proporcionar um tempo de inatividade mínimo durante eventos catastróficos.

RESUMO

As Tecnologias AMD PRO oferecem uma base abrangente para atender às demandas em evolução das empresas modernas. Ao integrar segurança avançada, capacidade de gerenciamento perfeita e confiabilidade pronta para os negócios a todos os processadores AMD Ryzen™ PRO, a AMD capacita as organizações a proteger seus dados, simplificar as operações de TI e fornecer produtividade do futuro em diversos ambientes de trabalho.

À medida que os locais de trabalho adotam operações híbridas e integram fluxos de trabalho orientados por IA, a AMD continua comprometida em impulsionar a inovação. A cada geração, as Tecnologias AMD PRO ampliam os limites de segurança, desempenho e capacidade de gerenciamento, para que as empresas estejam equipadas para enfrentar os desafios de hoje e se preparem para as oportunidades do futuro.

ISENÇÃO DE RESPONSABILIDADE

As informações aqui contidas são apenas para fins informativos e estão sujeitas a alterações sem aviso prévio. Embora todas as precauções tenham sido tomadas na preparação deste documento, ele pode conter imprecisões técnicas, omissões e erros tipográficos. A AMD não tem obrigação de atualizar nem de corrigir essas informações. Além disso, os PRODUTOS DA AMD podem incluir erratas que fazem com que o processador se desvie das especificações publicadas e a AMD ocasionalmente identificará essas erratas do produto sem aviso prévio, mas não tem a obrigação de fazê-lo. A Advanced Micro Devices, Inc. não faz representações nem garantias quanto à exatidão ou integridade do conteúdo deste documento e não assume responsabilidade, incluindo quaisquer garantias implícitas de não violação, comercialização ou adequação a uma finalidade específica, para operar ou usar hardware, software ou outros produtos da AMD aqui descritos. Nenhuma licença, implícita ou decorrente de preclusão, de quaisquer direitos de propriedade intelectual, é concedida por este documento. Os termos e limitações aplicáveis à compra ou ao uso dos produtos da AMD são determinados em um contrato assinado entre as partes ou nos Termos e Condições Padrão de Venda da AMD.

NOTAS DE RODAPÉ

1. A criptografia completa da memória do sistema com o AMD Memory Guard está incluída nos processadores AMD Ryzen PRO, AMD Ryzen Threadripper PRO e AMD Athlon PRO. Exige ativação pelo OEM. Confira com o fabricante do sistema antes da compra. GD-206.
2. Um OEM que ativou o recurso Inicialização Segura da Plataforma AMD concede permissão para que seu código BIOS assinado criptograficamente seja executado apenas em suas plataformas usando uma placa-mãe habilitada para Inicialização Segura da Plataforma AMD. Fusíveis programáveis de uma só vez no processador ligam o processador à chave de assinatura de código de firmware do OEM. A partir desse ponto, esse processador só poderá ser usado com placas-mãe que usam a mesma chave de assinatura de código. GD-192.
3. Em comparação com o Intel vPro, a Capacidade de gerenciamento AMD PRO implementa mais perfis da Iniciativa de Gerenciamento DASH para oferecer suporte ao gerenciamento de vários fornecedores para sistemas desktop e móveis. KRKP-7
4. Em comparação com o Intel vPro, a Capacidade de gerenciamento AMD PRO implementa uma versão mais recente do protocolo TLS (Transport Layer Security) que forneceu níveis mais altos de segurança e menor latência (TLS 1.3 vs. 1.2) KRKP-8
5. Relatório da Principled Tech - https://www.amd.com/content/dam/amd/en/documents/products/processors/technologies/ryzen-7-mixed-cpu-deployment.pdf
6. O AMD Secure Processor é um processador de segurança dedicado no chip integrado em cada sistema em um chip (SoC) e Circuito integrado de aplicativo específico (ASIC) projetado pela AMD. Ele permite a inicialização segura com raiz de confiança ancorada no hardware, inicializa o SoC por meio de um fluxo de inicialização seguro e estabelece um Ambiente de execução confiável isolado. GD-72.
7. A criptografia completa da memória do sistema com AMD Memory Guard está incluída nos processadores AMD Ryzen PRO, AMD Ryzen Threadripper PRO e AMD Athlon PRO. Requer ativação de OEM. Confira com o fabricante do sistema antes da compra. GD-206
8. Microsoft Pluton é uma tecnologia de propriedade da Microsoft licenciada para a AMD. Microsoft Pluton é uma marca registrada da Microsoft Corporation nos Estados Unidos e/ou em outros países. Saiba mais em https://www.microsoft.com/security/blog/2020/11/17/meet-the-microsoft-pluton-processor-the-security-chip-designed-for-the-future-of-windows-pcs/. O processador de segurança Microsoft Pluton requer ativação de OEM. Verifique com o OEM antes da compra. A AMD não verificou a reivindicação de terceiros. GD-202.
9. O AMD Secure Processor é um processador de segurança dedicado no chip integrado em cada sistema em um chip (SoC) e Circuito integrado de aplicativo específico (ASIC) projetado pela AMD. Ele permite a inicialização segura com raiz de confiança ancorada no hardware, inicializa o SoC por meio de um fluxo de inicialização seguro e estabelece um Ambiente de execução confiável isolado. GD-72.