Documento técnico

HP Sure Start com detecção de invasão em tempo de execução

Conforme implementado em produtos HP Elite equipados com processadores AMD de 7ª geração
Outubro de 2017

Índice

1 HP Sure Start com detecção de invasão em tempo de execução 2
1.1 Informações gerais 2
1.2 Visão geral do HP Sure Start com detecção de invasão em tempo de execução HP 2
1.3 Detecção de invasão em tempo de execução (RTID, Runtime Intrusion Detection) 2
1.3.1 Contexto 2
1.3.2 Código do BIOS em tempo de execução versus código do BIOS de inicialização 3
1.3.3 Arquitetura da detecção de invasão em tempo de execução 4
1.3.4 Eventos 5
1.3.5 Controles de políticas 5
1.4 Proteção de configuração do BIOS 5
1.4.1 Contexto 5
1.4.2 Visão geral da proteção de configuração do BIOS 5
1.4.3 Eventos 5
1.4.4 Controles de políticas 6
2 Apêndice A 6
2.1 Visão geral do System Management Mode (SMM) 6

1 HP Sure Start com detecção de invasão em tempo de execução

1.1 Informações gerais

A HP possui uma visão holística da segurança do cliente que visa abordar a segurança em todas as camadas da pilha de computação do dispositivo cliente. Nosso foco não está apenas dentro do SO ou em soluções de segurança baseadas em nuvem — acreditamos que a segurança de hardware e firmware do dispositivo "abaixo do SO" também é crucial.

À medida que nosso mundo se torna ainda mais conectado, os ciberataques visam o firmware e o hardware dos dispositivos cliente com cada vez mais frequência e sofisticação. Como o firmware do dispositivo é executado primeiro no hardware e é responsável por inicializar o SO com segurança, você não pode confiar no SO do dispositivo cliente se não puder confiar no firmware.

É extremamente difícil, se não impossível, prever e, dessa forma, prevenir todos os ataques possíveis, e é por isso que a HP também projeta nossos dispositivos clientes com "resiliência cibernética", a capacidade de detectar um ataque bem-sucedido e recuperar-se dele.

O HP Sure Start é a abordagem exclusiva e revolucionária da HP para fornecer proteção "abaixo do SO" avançada para o dispositivo cliente que usa reforço de hardware para garantir que o sistema irá inicializar apenas o HP BIOS original. Além disso, se o HP Sure Start detectar violações com o HP BIOS, ele terá a capacidade de recuperar o HP BIOS original usando uma cópia de backup protegida.

1.2 Visão geral do HP Sure Start com detecção de invasão em tempo de execução

O HP Sure Start com detecção de invasão em tempo de execução inclui os mesmos recursos básicos que as gerações anteriores do HP Sure Start, além de novos recursos que aumentam significativamente o nível para proteção avançada do HP Sure Start, detecção de ataques e recuperação do firmware do sistema HP.[1] Há dois recursos principais que são adicionados ao dispositivo cliente:

- Detecção de invasão em tempo de execução
- Proteção de configuração do BIOS

Além disso, a HP começará a oferecer um kit de integração da capacidade de gerenciamento (MIK, Manageability Integration Kit) que inclui um plug-in Microsoft System Center Configuration Manager (SCCM) que fornecerá aos administradores de TI um mecanismo direto para gerenciar os recursos novos e existentes do HP Sure Start usando sua infraestrutura SCCM existente. O foco deste documento técnico estará nos dois novos recursos do dispositivo cliente em vez dos recursos de gerenciamento remoto prontos para uso habilitados pelo MIK.

1.3 Detecção de invasão em tempo de execução (RTID, Runtime Intrusion Detection)

1.3.1 Contexto

Para fornecer contexto para a forma como o HP Sure Start com o recurso de detecção de invasão em tempo de execução difere dos recursos básicos fornecidos pelo HP Sure Start antes da RTID, é útil analisar essa linha de base ilustrada na **Figura 1.** Essa figura fornece uma visão de alto nível do que é fornecido pelo HP Sure Start básico. Observe que o foco desse recurso básico é garantir que a CPU host (na inicialização) nunca comece a executar o código de firmware que tenha sido substituído ou modificado. Portanto, o HP Sure Start fornece garantias de que o sistema irá inicializar apenas o firmware HP original que irá configurar com segurança o hardware do dispositivo cliente conforme exigido para inicializar o SO com segurança.

Observe que o foco está no monitoramento do código do BIOS no flash do sistema que é executado pela CPU host na inicialização. Essa é uma importante distinção do código do BIOS que permanece residente na memória principal (DRAM) para fornecer gerenciamento de energia e outros serviços essenciais após o sistema ter inicializado para o SO. A seguir, exploramos essa distinção com maiores detalhes.

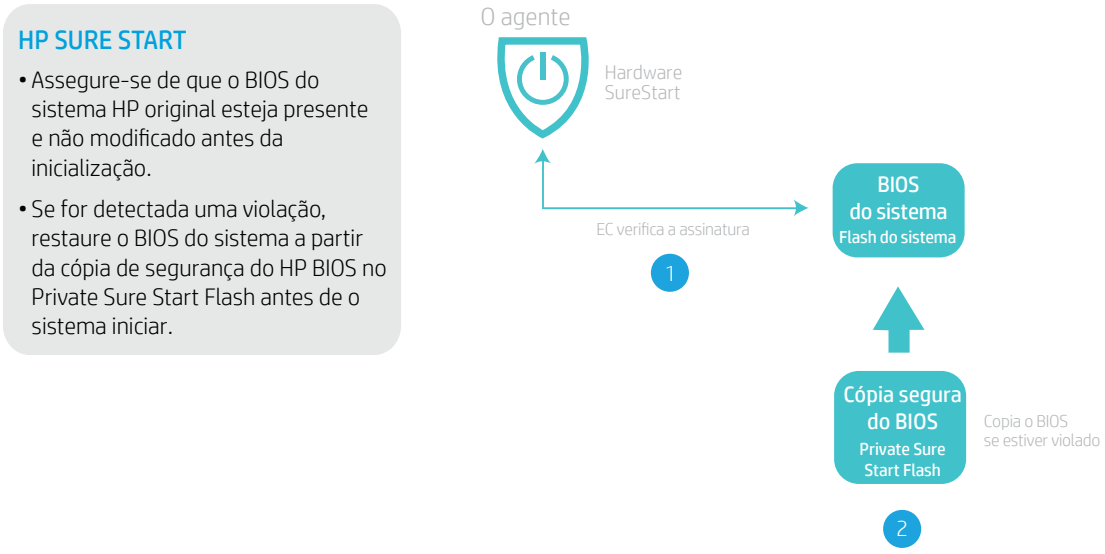

Figura 1. Visão geral do HP Sure Start básico (aplica-se a produtos HP Elite equipados com processadores AMD de 6ª geração e superiores).

1.3.2 Código do BIOS em tempo de execução versus código do BIOS de inicialização

Em cada inicialização, a CPU começa a execução do código do BIOS a partir da memória flash em um endereço fixo. Esse código do BIOS então inicializa o hardware incluindo a memória DRAM e copia todas as rotinas da memória flash para a volátil (DRAM). Uma grande parte desse código do BIOS é usada para fornecer recursos "pré-SO" que são necessários antes que o SO seja iniciado. Exemplos de suporte a BIOS "pré-SO" incluem drivers de vídeo, suporte à inicialização PXE, drivers de teclado e mouse, autenticação pré-inicialização e desbloqueio de criptografia de armazenamento em massa, para citar alguns. A maioria dessas rotinas não é mais necessárias após o SO estar em execução, já que os recursos são relevantes apenas antes da entrega para o SO ou antes que o SO tenha seus próprios drivers.

No entanto, há uma parte do BIOS que permanece na DRAM que é necessária para fornecer recursos avançados de gerenciamento de energia, serviços de SO e outras funções independentes do SO enquanto o SO está em execução. Esse código do BIOS, conhecido como código System Management Mode (SMM), reside em uma área especial dentro da DRAM que está oculta do SO.2 Também o chamamos de código "Runtime" BIOS no contexto da detecção de invasão em tempo de execução do HP Sure Start.

A integridade do código SMM é crítica para a postura quanto à segurança do dispositivo cliente. A implementação do HP Sure Start básico fornece a garantia de que todos os códigos são HP BIOS original sempre que o sistema inicia, incluindo o código SMM que está presente na DRAM quando o SO inicia.

A oportunidade que resta é ir além não apenas para garantir que o local de início do código do BIOS HP SMM seja adequado ao iniciar o SO, mas também para fornecer mecanismos para garantir que permaneça adequado enquanto o SO está sendo executado ao fornecer um meio de detectar qualquer ataque que gerencie para ultrapassar os mecanismos existentes, oferecendo proteção para o código do BIOS HP SMM.

1.3.3 Arquitetura da detecção de invasão em tempo de execução

A **Figura 2** fornece detalhes sobre a implementação do recurso de detecção de invasão em tempo de execução (RTID). O recurso RTID utiliza hardware especializado no chipset da plataforma para detectar modificações no Runtime HP SMM BIOS. A detecção de qualquer uma dessas condições resulta em uma notificação para o hardware HP Sure Start, que pode tomar a ação de política configurada independente da CPU.

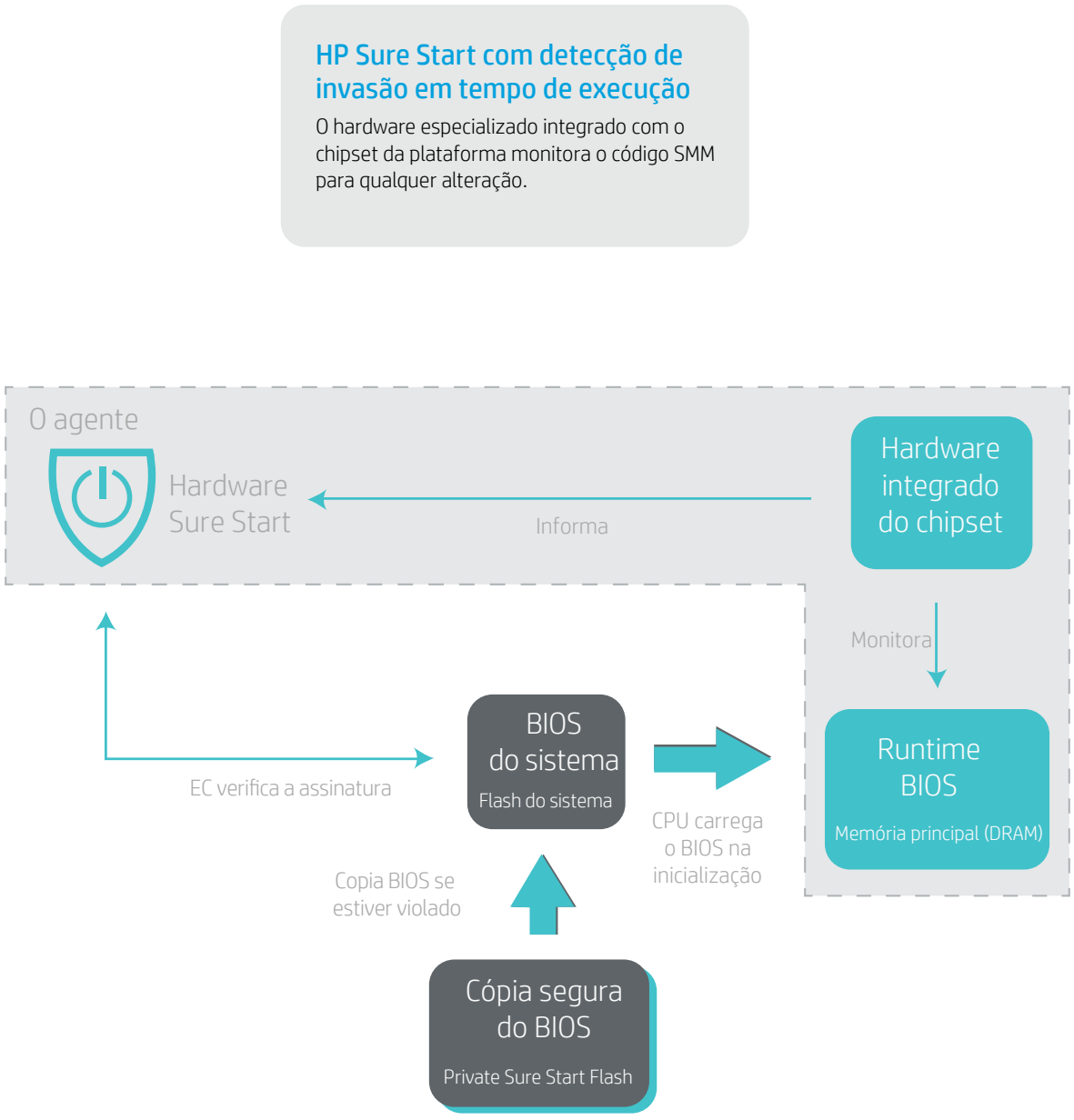

Figura 2. Arquitetura da detecção de invasão em tempo de execução (aplica-se a produtos HP Elite equipados com processadores AMD de 7ª geração).

1.3.4 Eventos

O recurso RTID do HP Sure Start irá gerar eventos para o hardware do HP Sure Start quando qualquer modificação no código do BIOS HP SMM for detectada. O hardware do HP Sure Start irá tomar a ação associada com a política de eventos configurada na configuração do BIOS.

Independentemente da configuração da política de eventos, o evento sempre será registrado no log de auditoria do HP Sure Start e o usuário local irá receber uma notificação do BIOS na próxima inicialização subsequente a um evento de RTID.

1.3.5 Controles de políticas

O recurso RTID é habilitado por padrão para todas as plataformas fornecidas da fábrica da HP. Não há necessidade para o cliente final/administrador habilitar ou de outra forma "implantar" o recurso para aproveitar a RTID do HP Sure Start!

Há duas políticas de BIOS relacionadas ao recurso de RTID que podem ser configuradas opcionalmente pelo proprietário/administrador da plataforma:

- **Detecção de invasão em tempo de execução do firmware HP** (ativar/desativar)
- **Política de eventos de segurança do Sure Start**

1.3.5.1. Detecção de invasão em tempo de execução do firmware HP

Essa configuração de política do BIOS irá ativar ou desativar o recurso RTID. A configuração padrão para essa política é **ativada**.

1.3.5.2. Política de eventos de segurança do Sure Start

Essa configuração de política do BIOS controla qual ação é tomada quando o recurso RTID detecta um ataque ou a tentativa de um ataque. Há três configurações possíveis para essa política:

- Registrar apenas o evento: Quando essa configuração é selecionada, o hardware do HP Sure Start irá registrar eventos de detecção, que podem ser visualizados no caminho "Logs de Aplicativos e Serviços/HP Sure Start" do Visualizador de Eventos do Windows.[3]
- Registrar o evento e notificar o usuário: Essa é a configuração padrão. Quando essa configuração é selecionada, o hardware do HP Sure Start irá registrar eventos de detecção, que podem ser visualizados no caminho "Logs de Aplicativos e Serviços/HP Sure Start" do Visualizador de Eventos do Windows. Além disso, o usuário será alertado no Windows de que o evento ocorreu.[4]
- Registrar o evento e desligar o sistema: Quando essa configuração é selecionada, o hardware do HP Sure Start irá registrar eventos de detecção, que podem ser visualizados no caminho "Logs de Aplicativos e Serviços/HP Sure Start" do Visualizador de Eventos do Windows. Além disso, o usuário será alertado no Windows de que o evento ocorreu e que o desligamento do sistema é iminente.

1.4 Proteção de configuração do BIOS

1.4.1 Contexto

O HP Sure Start básico verifica a integridade e a autenticidade do código do HP BIOS. Como esse código é estático após ser criado pela HP, podem ser usadas assinaturas digitais para confirmar os dois atributos do código. A natureza dinâmica e configurável pelo usuário das configurações do BIOS cria desafios adicionais para proteger essas configurações, já que as assinaturas digitais não podem ser geradas pela HP e usadas pelo hardware do HP Sure Start para verificar essas configurações.

1.4.2 Visão geral da proteção de configuração do BIOS

A proteção de configuração do BIOS do HP Sure Start fornece a capacidade de configurar o sistema de tal maneira que o hardware do HP Sure Start seja usado para fazer backup e fornecer verificação de integridade de todas as configurações do BIOS preferidas pelo usuário.

Quando esse recurso é habilitado na plataforma, todas as configurações de política usadas pelo BIOS subsequentemente passam por backup e uma verificação de integridade é realizada em cada inicialização para garantir que nenhuma das configurações de políticas do BIOS tenha sido modificada. No caso de uma mudança ser detectada, o sistema usa o backup da área posterior protegida do HP Sure Start para reverter automaticamente de volta para a configuração definida pelo usuário.

1.4.3 Eventos

O recurso de proteção de configuração do BIOS do HP Sure Start irá gerar eventos para o hardware do HP Sure Start quando for detectada uma tentativa de modificar as configurações do BIOS. O evento será registrado no log de auditoria do HP Sure Start e o usuário local irá receber uma notificação do BIOS durante a inicialização.

1.4.4 Controles de políticas

A política de proteção de configuração do BIOS é **desativada** por padrão.

Para ativar o recurso, o proprietário/administrador do dispositivo cliente deve primeiro configurar todas as políticas do BIOS para a configuração preferida. O proprietário/administrador também precisa configurar uma senha de administrador da configuração do BIOS para usar a proteção de configuração do BIOS do HP Sure Start.

Uma vez concluída, a política de proteção de configuração do BIOS deve ser alterada para “ativada”. Nesse ponto, uma cópia de backup de todas as configurações do BIOS é criada no armazenamento protegido do HP Sure Start. No futuro, nenhuma das configurações do BIOS poderá ser modificada de forma local ou remota. Em cada inicialização, as configurações da política do BIOS serão verificadas para que estejam no estado desejado e, se houver qualquer discrepância, as configurações do BIOS serão restauradas a partir do armazenamento protegido do HP Sure Start.

Para modificar uma configuração do BIOS, a senha de administrador do BIOS deve ser fornecida e a proteção de configuração do BIOS subsequentemente desativada, e nesse ponto as modificações podem ser feitas nas configurações do BIOS.

2 Apêndice A

2.1 Visão geral do System Management Mode (SMM)

O System Management Mode (SMM) é uma abordagem padrão do setor usada para recursos avançados de gerenciamento de energia de PCs e outras funções independentes do SO enquanto o SO está sendo executado. Embora o termo SMM e a implementação sejam específicos para arquiteturas x86, muitas arquiteturas de computação modernas usam um conceito arquitetônico semelhante.

O SMM é configurado pelo BIOS no momento da inicialização. O código do SMM é populado na memória principal (DRAM) e, em seguida, o BIOS usa registros de configuração especiais (travável) dentro do chipset para bloquear o acesso a essa área quando o microprocessador não está sendo executado em um contexto de SMM. No tempo de execução, a entrada no modo SMM é orientada por evento. O chipset é programado para reconhecer muitos tipos de eventos e tempos limites. Quando ocorre um evento desse tipo, o hardware do chipset declara o PIN de entrada da Interrupção de gerenciamento do sistema (SMI). No limite de instrução seguinte, o microprocessador salva seu estado inteiro e entra no SMM.

À medida que o microprocessador entra no SMM, ele declara um PIN de saída do hardware, o SMI Active (SMIACT). Esse PIN avisa para o hardware do chipset que o microprocessador está entrando no SMM. Uma SMI pode ser declarada a qualquer momento, durante qualquer modo operacional do processo, exceto de dentro do próprio SMM. O hardware do chipset reconhece o sinal SMIACT e redireciona todos os ciclos da memória subsequentes para uma área protegida da memória (às vezes definida como área SMRAM), reservada especificamente para o SMM. Imediatamente após receber a saída de SMI e declarar a saída de SMIACT, o microprocessador começa a salvar todo o seu estado interno na área de memória protegida.

Após o estado do microprocessador ter sido armazenado na memória SMRAM, o código de manipulador especial do SMM que também reside na SMRAM (colocada lá pelo BIOS do sistema no momento da inicialização) começa a ser executado em um modo de operação especial do SMM. Embora operacional nesse modo, a maioria dos mecanismos de isolamento de memória e hardware é suspensa e o microprocessador pode acessar praticamente todos os recursos na plataforma para permitir que execute as tarefas necessárias. O código do SMM conclui a tarefa exigida e, então, é o momento de voltar o microprocessador para o modo operacional anterior. Nesse ponto, o código do SMM executa a instrução Return from System Management Mode (RSM) para sair do SMM. A instrução RSM faz com que o microprocessador restaure seus dados do estado interno anterior a partir da cópia salva em SMRAM após a entrada no SMM. Após a conclusão da RSM, todo o estado do microprocessador está restaurado para o estado pouco antes do evento de SMI, e o programa anterior (SO, aplicativos, hipervisor etc.) reinicia a execução exatamente de onde parou.

[1] O HP Sure Start com detecção de invasão em tempo de execução está disponível em produtos HP Elite equipados com processadores AMD de 7ª geração.
[2] Para obter mais detalhes sobre o SMM e como ele funciona, consulte o Apêndice A.
[3] É necessária a instalação do software HP Notification para ver os eventos do HP Sure Start no Visualizador de Eventos do Windows.
[4] É necessária a instalação do software HP Notification para receber notificações.

4AA6-9340PTL, outubro de 2017