1.Introdução à segurança de host

1.1 Proteção a nível de Firmware

Firmware refere-se a um tipo de software de baixo nível que está embutido em dispositivos eletrônicos e é responsável por controlar o funcionamento e o comportamento desses dispositivos. É um conjunto de instruções programadas permanentemente em chips de memória de leitura/gravação (ROM) ou em memória flash não volátil, o que significa que ele permanece no dispositivo mesmo quando a energia é desligada.

O firmware desempenha um papel crítico em uma ampla gama de dispositivos eletrônicos, desde smartphones e tablets até computadores, eletrodomésticos, consoles de videogame, roteadores de rede, impressoras, câmeras digitais e muito mais. Ele fornece a funcionalidade básica e os recursos essenciais para o funcionamento do dispositivo.

O firmware é responsável por controlar o hardware do dispositivo, permitindo a comunicação e a interação entre os componentes do sistema. Ele contém os drivers e protocolos necessários para garantir a interoperabilidade entre os componentes de hardware e também fornece a interface necessária para que o software de nível superior, como o sistema operacional, possa interagir com o hardware.

O firmware também pode conter configurações e parâmetros específicos que afetam o comportamento do dispositivo, como configurações de energia, configurações de rede, configurações de segurança e muito mais. Essas configurações podem ser alteradas e atualizadas por meio de processos de atualização de firmware, que permitem corrigir bugs, adicionar novos recursos e melhorar a segurança.

2.Hardware Root of Trust

Refere-se a um componente de hardware confiável e imutável que atua como a base segura para a inicialização e operação segura de um sistema. É responsável por estabelecer uma raiz de confiança para o sistema, garantindo que as etapas críticas de inicialização e verificação ocorram em um ambiente confiável e livre de manipulação maliciosa. Ele é projetado para resistir a ataques físicos e lógicos, garantindo a integridade do processo de inicialização.

O Hardware Root of Trust desempenha um papel crítico na segurança de sistemas, incluindo a autenticação do hardware, a verificação da integridade do firmware e do sistema operacional, a proteção de chaves criptográficas e a garantia de um ambiente confiável para a execução segura de aplicativos e processos.

Ao estabelecer uma raiz de confiança confiável no hardware, o HRT ajuda a proteger o sistema contra ameaças como malware, ataques de firmware, ataques de inicialização comprometida e outras formas de manipulação maliciosa.

2.1 Trusted Platform Module (TPM)

É um chip de hardware projetado para fornecer recursos de segurança e criptografia em um sistema computacional. Ele é um componente crítico do Hardware Root of Trust e desempenha um papel fundamental na proteção de dados e na autenticação de dispositivos.

O TPM opera de forma independente da CPU e do sistema operacional, o que significa que ele pode executar suas funções de segurança mesmo quando o sistema está desligado ou em modo de suspensão.

O chip TPM contém uma série de recursos e funcionalidades de segurança, incluindo:

- **Armazenamento seguro de chaves criptográficas:** Possui uma área segura chamada de Armazenamento de Chave Protegida (Protected Storage Key, PSK), onde chaves criptográficas podem ser armazenadas de forma segura. Essas chaves são protegidas contra acesso não autorizado e podem ser usadas para autenticação e criptografia.
- **Geração de chaves criptográficas:** O TPM é capaz de gerar chaves criptográficas seguras, como chaves de criptografia assimétrica (por exemplo, RSA) e chaves de criptografia simétrica (por exemplo, AES). Essas chaves são geradas dentro do TPM e nunca deixam o chip, garantindo sua integridade e confidencialidade.
- **Operações criptográficas seguras:** O TPM fornece um ambiente seguro para executar operações criptográficas, como assinaturas digitais, verificação de integridade, geração de hash e criptografia. Essas operações são realizadas dentro do chip TPM, garantindo a segurança dos dados e a autenticidade das operações.
- **Medição de integridade:** O TPM possui a capacidade de medir a integridade do firmware, do sistema operacional e de outros componentes críticos do sistema. Ele armazena essas medidas em um registro seguro chamado Log de Medição (PCR), permitindo que as medidas de integridade sejam verificadas posteriormente.
- **Autenticação de plataforma:** O TPM pode ser usado para autenticar a plataforma, verificando a integridade do firmware, do sistema operacional e de outros componentes críticos durante a inicialização. Isso ajuda a prevenir ataques de inicialização comprometida e garante a execução apenas de software confiável.

3.Unified Extensible Firmware Interface (UEFI)

O Unified Extensible Firmware Interface (UEFI) é uma especificação de firmware moderna que substituiu o antigo BIOS (Basic Input/Output System) em muitos sistemas computacionais. O UEFI é responsável por inicializar o sistema, configurar o hardware e fornecer uma interface entre o firmware e o sistema operacional.

Ao contrário do BIOS, que é um firmware básico e limitado, o UEFI é projetado para ser mais flexível, extensível e seguro. Ele oferece recursos avançados que permitem inicialização mais rápida, suporte a discos rígidos maiores do que 2,2 terabytes, inicialização em modo protegido, suporte a interfaces gráficas e muito mais.

O funcionamento do UEFI pode ser dividido em várias etapas:

- **Inicialização do UEFI:** Quando o sistema é ligado, o UEFI é o primeiro software a ser executado. Ele é carregado a partir de uma memória não volátil, como ROM ou flash, e começa a inicializar o hardware do sistema.
- **Configuração do hardware:** O UEFI é responsável por detectar e configurar o hardware do sistema, como processadores, memória, dispositivos de armazenamento, interfaces de rede e periféricos conectados. Ele realiza uma série de verificações e inicializações para garantir que o hardware esteja pronto para uso.
- **Inicialização do sistema operacional:** Após a configuração do hardware, o UEFI localiza e carrega o sistema operacional ou um gerenciador de inicialização, como o GRUB. Ele pode verificar a assinatura digital do sistema operacional para garantir sua autenticidade e integridade.
- **Interface do usuário:** O UEFI fornece uma interface de usuário gráfica, conhecida como interface do firmware, que permite que os usuários configurem e personalizem o sistema. Através dessa interface, é possível acessar configurações de inicialização, ajustar configurações de hardware, atualizar o firmware e muito mais.
- **Extensibilidade:** Uma das principais vantagens do UEFI é sua extensibilidade. Ele suporta a execução de aplicativos de terceiros, conhecidos como controladores de inicialização (bootloaders), que podem fornecer recursos adicionais, como criptografia de disco, suporte a sistemas de arquivos avançados e inicialização de múltiplos sistemas operacionais.

4.Secure boot

O Secure Boot é um recurso de segurança implementado em sistemas compatíveis com o UEFI para proteger contra malware e ataques de inicialização comprometida. Ele garante que apenas software confiável e autorizado seja executado durante o processo de inicialização do sistema.

O Secure Boot funciona da seguinte maneira:

- **Verificação da integridade do firmware:** O Secure Boot começa verificando a integridade do firmware do sistema, incluindo o UEFI. Ele verifica se o firmware não foi corrompido ou modificado por algum malware ou ataque.
- **Verificação da integridade do bootloader:** Após a verificação do firmware, o Secure Boot verifica a integridade do carregador de inicialização (bootloader) do sistema. Isso pode ser um carregador de inicialização padrão, como o GRUB, ou um carregador de inicialização específico do fabricante. A assinatura digital do carregador de inicialização é verificada para garantir que ele não tenha sido adulterado.
- **Verificação da assinatura digital do kernel e dos drivers:** Após a verificação do carregador de inicialização, o Secure Boot verifica a assinatura digital do kernel do sistema operacional e dos drivers críticos. Essa verificação garante que apenas software assinado digitalmente por uma chave confiável seja executado.
- **Chave de assinatura confiável:** O Secure Boot depende de uma lista de chaves de assinatura confiáveis, conhecidas como Chave de Assinatura de Conteúdo (Key Exchange Key, KEK), que são usadas para verificar as assinaturas digitais. Essas chaves são pré-instaladas no firmware do sistema e são usadas para garantir que apenas software assinado por chaves confiáveis seja executado.
- **Modo de usuário e configuração:** O Secure Boot permite que os usuários configurem suas próprias políticas de segurança. Isso inclui a capacidade de adicionar chaves de assinatura confiáveis adicionais ou desabilitar o Secure Boot, se necessário. Essas configurações são geralmente protegidas por senhas para evitar alterações não autorizadas.

4.1 Measured boot

É um recurso de segurança que faz parte do processo de inicialização seguro em sistemas compatíveis com o UEFI. Ele é projetado para verificar e medir a integridade de componentes críticos do sistema durante a inicialização, permitindo a detecção de alterações ou comprometimentos no firmware, bootloader, sistema operacional e drivers.

Funciona da seguinte maneira:

- **Coleta de medidas (measurements):** Durante o processo de inicialização, o UEFI coleta medidas (hashes criptográficos) de componentes críticos do sistema, como firmware, bootloader, sistema operacional e drivers. Essas

medidas são armazenadas em uma estrutura de dados conhecida como Log de Medição (PCR - Platform Configuration Register).

- **Criação de cadeias de confiança (certificate chains):** As medidas coletadas pelo UEFI são usadas para criar uma cadeia de confiança de medidas. Cada medida é assinada digitalmente usando uma chave privada confiável. Essas assinaturas garantem a autenticidade e integridade das medidas coletadas.
- **Armazenamento seguro das medidas (secure storage):** As medidas coletadas e suas assinaturas são armazenadas de forma segura no chip de Trusted Platform Module (TPM) do sistema. O TPM protege as medidas contra alterações ou adulterações, fornecendo um ambiente seguro para armazenamento.
- **Verificação da cadeia de confiança (certificate chain verification):** Durante o processo de inicialização, o UEFI verifica a cadeia de confiança de medidas armazenadas no TPM. Ele verifica a assinatura digital das medidas e suas relações de confiança para garantir que as medidas não tenham sido comprometidas.
- **Comparação de medidas (comparison):** O UEFI compara as medidas coletadas durante o processo de inicialização atual com as medidas armazenadas no TPM. Se houver alguma discrepância ou alteração nas medidas, isso indica uma potencial violação ou comprometimento do sistema.
- **Relatórios de integridade (integrity reports):** Com base nas comparações de medidas, o UEFI gera relatórios de integridade que indicam se a inicialização foi bem-sucedida e se o sistema está em um estado confiável. Esses relatórios podem ser usados para fins de auditoria, detecção de ameaças e solução de problemas de segurança.

4.2 Boot attestation

É um mecanismo de segurança que complementa o Measured Boot em sistemas compatíveis com o Unified Extensible Firmware Interface (UEFI). Ele permite que o sistema forneça evidências de integridade durante o processo de inicialização para uma entidade externa confiável, como um servidor de autenticação ou um sistema de monitoramento de segurança.

Funciona da seguinte maneira:

- **Coleta de medidas (measurements):** Mesmo passo apresentado no Secure Boot.
- **Criação de um carimbo digital (digital attestation):** O UEFI cria um carimbo digital (digital attestation) contendo as medidas coletadas durante o

processo de inicialização. O carimbo digital é assinado digitalmente usando a chave privada confiável do TPM, garantindo a autenticidade das medidas.

- **Solicitação de attestation (attestation request):** Uma entidade externa confiável, como um servidor de autenticação, pode solicitar um relatório de attestation (relatório de comprovação) do sistema. Isso pode ser feito através de um protocolo de comunicação seguro.
- **Geração do relatório de attestation (attestation report):** O UEFI gera um relatório de attestation que inclui o carimbo digital assinado, as medidas coletadas e outras informações relevantes sobre o estado do sistema durante a inicialização. O relatório de attestation é enviado de volta à entidade externa.
- **Verificação do relatório de attestation (attestation report verification):** A entidade externa recebe o relatório de attestation e verifica sua autenticidade e integridade. Ela verifica a assinatura digital do carimbo digital usando a chave pública correspondente à chave privada usada na assinatura.
- **Avaliação da integridade do sistema (system integrity assessment):** Com base no relatório de attestation, a entidade externa pode avaliar a integridade do sistema e determinar se ele está em um estado confiável. Isso pode ser usado para fins de auditoria, verificação de conformidade ou para tomar decisões de segurança, como permitir ou negar acesso a recursos.

5.Full Disk Encryption (FDE)

É um método de criptografia que protege todos os dados armazenados em um disco ou unidade de armazenamento, como um disco rígido (HDD) ou uma unidade de estado sólido (SSD).

O FDE criptografa todas as informações no disco, incluindo o sistema operacional, arquivos do usuário e metadados, impedindo o acesso não autorizado aos dados em caso de perda, roubo ou acesso físico ao dispositivo.

O seu funcionamento consiste nas seguintes etapas:

- **Processo de criptografia inicial:** Durante a configuração do FDE, um algoritmo de criptografia forte é usado para criptografar todo o conteúdo do disco. Isso pode ser feito por meio de um software de criptografia, como o BitLocker da Microsoft ou o FileVault da Apple, ou por meio de soluções de hardware.
- **Chave de criptografia:** Durante o processo de criptografia inicial, é gerada uma chave de criptografia que é usada para criptografar e descriptografar os dados no disco. Essa chave é conhecida como chave de criptografia de disco (Disk Encryption Key) ou chave de volume (Volume Key). Geralmente, a chave é protegida por uma senha ou outra forma de autenticação.

- **Desbloqueio do disco:** Quando o sistema é inicializado, o usuário deve fornecer a senha ou outra forma de autenticação para desbloquear o disco. A senha é usada para descriptografar a chave de criptografia do disco e permitir o acesso aos dados.
- **Criptografia em tempo real:** Após o desbloqueio do disco, todos os dados lidos e gravados no disco são automaticamente criptografados e descriptografados em tempo real. Isso garante que todos os dados armazenados no disco permaneçam protegidos, mesmo quando o sistema está em uso.
- **Proteção contra acesso não autorizado:** O FDE protege contra acesso não autorizado aos dados, mesmo em situações em que o disco é removido do sistema ou o dispositivo é roubado. Sem a chave de criptografia correta, os dados permanecem inacessíveis.
- **Gerenciamento de chaves:** O FDE também envolve o gerenciamento seguro das chaves de criptografia. As chaves são armazenadas em locais seguros, como o chip Trusted Platform Module (TPM), um dispositivo USB separado ou outros métodos de armazenamento criptograficamente protegidos.

6.Self-Encrypted Drives (SED)

São unidades de armazenamento, como discos rígidos (HDDs) ou unidades de estado sólido (SSDs), que possuem recursos de criptografia integrados. Ao contrário do Full Disk Encryption (FDE), em que a criptografia é realizada por meio de software, o SED executa a criptografia diretamente no hardware da unidade, proporcionando uma camada adicional de segurança.

Funciona da seguinte maneira:

- **Chave de criptografia:** Cada SED possui uma chave de criptografia interna chamada de Key Encryption Key (KEK). Essa chave é gerada pela unidade no momento da fabricação e é usada para criptografar e descriptografar os dados armazenados na unidade.
- **Autenticação:** Para acessar os dados armazenados em um SED, é necessário autenticar-se usando uma senha, chave de acesso ou outro método de autenticação suportado. Essa autenticação é feita por meio de uma interface de usuário fornecida pelo SED ou por software de gerenciamento de criptografia.
- **Criptografia em tempo real:** Após a autenticação bem-sucedida, o SED executa a criptografia e descriptografia em tempo real conforme os dados são gravados e lidos na unidade. A criptografia ocorre automaticamente no hardware do SED, sem a necessidade de intervenção adicional do sistema operacional ou software.

- **Chave de dados (Data Encryption Key):** Para cada bloco de dados gravado na unidade, o SED gera uma chave de criptografia exclusiva conhecida como Data Encryption Key (DEK). Essa chave de dados é criptografada usando a KEK e armazenada juntamente com os dados na unidade.
- **Rápido apagamento:** Os SEDs geralmente têm a capacidade de realizar um rápido apagamento de dados, tornando-os inacessíveis. Isso pode ser feito redefinindo a KEK ou removendo a chave de criptografia do disco, o que torna impossível descriptografar os dados armazenados.
- **Gerenciamento de chaves:** Os SEDs podem oferecer recursos avançados de gerenciamento de chaves, permitindo que as chaves de criptografia sejam alteradas, adicionadas ou removidas conforme necessário. Além disso, eles podem suportar integração com infraestruturas de gerenciamento de chaves externas, como um servidor de gerenciamento de chaves (KMS).

7.Segurança em USB flash drive

A segurança em USB flash drives (também conhecidos como pen drives ou pendrives) envolve uma série de medidas para proteger os dados armazenados neles contra acesso não autorizado, perda ou roubo.

Veja alguns aspectos-chave da segurança em USB flash drives:

- **Criptografia:** Envolve o uso de algoritmos criptográficos para transformar os dados em uma forma ilegível, a menos que a chave correta seja fornecida para descriptografá-los. O uso de criptografia garante que mesmo se o USB flash drive for perdido ou roubado, os dados permaneçam protegidos.
- **Senhas e autenticação:** Alguns USB flash drives têm recursos de senha embutidos. Eles exigem que o usuário insira uma senha correta antes de permitir o acesso aos dados armazenados. Mesmo que alguém obtenha fisicamente o dispositivo, não poderá acessar os dados sem a senha correta. Algumas unidades também oferecem suporte a autenticação biométrica, como leitores de impressão digital.
- **Armazenamento seguro de dados:** Alguns USB flash drives têm uma área segura separada onde os dados podem ser armazenados. Essa área é protegida por senha ou criptografia adicional, fornecendo uma camada extra de segurança para dados sensíveis.
- **Proteção contra gravação:** Os USB flash drives podem ter um recurso de proteção contra gravação, que impede a gravação de dados no dispositivo. Isso pode ser útil para evitar a alteração acidental ou maliciosa dos dados armazenados no dispositivo.

- **Atualizações de firmware e segurança:** É importante manter o firmware do USB flash drive atualizado, pois as atualizações podem fornecer correções de segurança e melhorias na proteção dos dados. É recomendável verificar periodicamente se há atualizações de firmware disponíveis para o seu dispositivo.
- **Gerenciamento adequado:** A segurança em USB flash drives também envolve o gerenciamento adequado do dispositivo. Isso inclui evitar o compartilhamento indiscriminado do dispositivo com terceiros, proteger o dispositivo físico de danos ou perda e tomar precauções ao conectar o dispositivo a computadores não confiáveis, para evitar a infecção por malware.