

O que é Application Whitelisting (Lista de Permissões de Aplicações)?

- [Introdução](#)
- [Tipos de Application Whitelisting - uma descrição não técnica](#)
 - [A Autorização Óbvia e Incômoda \(algo positivo\)](#)
 - [A Autorização Genérica \(provavelmente não é algo positivo\)](#)
 - [A Autorização Genericamente Específica](#)
 - [A Autorização Específica-Específica](#)
 - [A Aplicação Comprometida](#)
- [Em Resumo - Perguntas a Fazer ao Investigar uma Capacidade de Application Whitelist](#)
- [Leitura Aprofundada do National Institute of Standards & Technology \(NIST\)](#)

Introdução

Application whitelisting, no contexto da Cyber Crucible, consiste em conceder a uma aplicação permissão para executar uma determinada ação que, de outra forma, poderia ser considerada suspeita ou maliciosa.

A tecnologia de application whitelisting é tipicamente encontrada em técnicas defensivas de análise comportamental, embora alguns atacantes também a utilizem (não abordado aqui) nas suas operações.

Pense nisto como na escola, onde os alunos normalmente não tinham permissão para circular pelos corredores durante as aulas. No entanto, se lhes fosse dada uma “autorização de saída” de alguma forma por uma figura de autoridade, os alunos não eram levados de volta à sala de aula nem enviados ao gabinete do diretor.

Tipos de Application Whitelisting - uma descrição não técnica

Se continuarmos com a analogia da “autorização de saída”, existem diferentes técnicas que os responsáveis escolares aprenderam, que ajudaram a formalizar os comportamentos que alguns alunos (definitivamente não o nosso CEO Dennis) poderiam ter tentado utilizar em seu proveito. Todas estas têm uma correlação direta com as operações de segurança.

A Autorização Óbvia e Incômoda (algo positivo)

21987331.jpg?width=278

Lembra-se de alguma vez ter recebido uma autorização de saída, ou uma chave para alguma sala, que era incrivelmente grande e óbvia?

Havia algumas boas razões para isso:

1. Para não se perder.
2. Para reduzir o tempo e o esforço investidos por uma figura de autoridade, na verificação rápida das atividades aprovadas do aluno.

Um bom software não vai “perder” uma lista de permissões, mas o software de application whitelist deve permitir uma validação rápida e eficiente em termos de recursos de que a aplicação foi inspecionada.

A Autorização Genérica (provavelmente não é algo positivo)

Esta é provavelmente a menos útil tanto para a monitorização de aplicações como para as escolas, mas é a que requer menos gestão ou especialização.

Neste caso, o aluno tem permissão para realizar o seu recado no corredor. O professor pode saber, por exemplo, mas não há validação por parte dos monitores do corredor quanto ao que o aluno está a fazer. Além disso, se houver uma tentativa de validação, existem dois níveis de investimento considerável de recursos:

1. o nível de esforço para abordar o aluno e questioná-lo sobre os seus comportamentos e intenções
2. o nível de esforço para garantir que o aluno está a ser honesto, de forma a validar a explicação do aluno

Com as aplicações, isto é mais frequentemente observado quando um programa é adicionado a uma lista de permissões, sem que exista qualquer validação adicional dos comportamentos ou atividades permitidas. Infelizmente, a capacidade de obter contexto sobre os comportamentos de uma aplicação normalmente não está disponível para aquisição, a menos que seja acompanhada externamente por alguma outra estrutura.

A Autorização Genericamente Específica

Não confundir com “avança, Aplicação, faz o que quiseres!”

Voltemos à autorização de ida à casa de banho, porque é muito apropriada aqui. Dada a visibilidade da autorização, é relativamente fácil avaliar o que o aluno deveria estar a fazer. Comportamentos flagrantemente fora do esperado para “ir à casa de banho” podem ser identificados sem grande dificuldade.

O application whitelisting com limites genéricos de atividades é o mais comum, embora, em muitos casos, esses limites equivalham a permitir que um aluno com uma autorização para a casa de banho brinque no recreio.

A Autorização Específica-Específica

Não confundir com a autorização “genericamente específica”!

22642689.jpg?width=340

Embora, com a autorização genericamente específica, saibamos que o aluno está a usar a casa de banho - numa escola grande, não sabemos

1. Quem deu permissão ao aluno
2. De onde é que ele veio.
3. Qual casa de banho a figura de autoridade tinha em mente quando deu a aprovação.
4. Há quanto tempo o aluno está “fora e por aí”.

Isto exigiu mais trabalho por parte da estrutura de autoridade da escola.

Voltando ao application whitelisting, a análise comportamental é mais precisa quanto mais variáveis forem adicionadas a qualquer capacidade de tomada de decisão.

Além disso, ao investigar uma autorização de saída que foi emitida, normalmente não é necessário rastrear uma cadeia de 5 professores até chegar à origem. Também se pode quase sempre confiar que o professor não era algum tipo de “mau professor” a incitar os alunos a comportarem-se de forma imprópria. O application whitelisting, num exemplo de lista de permissões específica-específica, requer trabalhar ao contrário, examinando todas as aplicações “pai” ou “ancestrais” que abriram a aplicação seguinte. Por exemplo, um malware pode ter aberto um utilitário legítimo do Windows.

As seguintes perguntas são aproximadamente equivalentes à “autorização de saída do aluno” acima mencionada:

1. Para que foi iniciada a aplicação, ou o que lhe foi ordenado fazer? Precisamos de conhecer o comportamento pretendido.
2. Quem iniciou a aplicação? Normalmente, é outro programa.
3. Que programas “pai” ou “ancestrais” resultaram na abertura deste programa? O que é que cada um deles estava a fazer, ou pretendia fazer?

A Aplicação Comprometida

Lembra-se, em várias obras de ficção científica, ou de literatura e filmes de terror, quando um impostor de alguma forma toma

22413315.jpg?width=226

o controlo do comportamento de uma personagem? Nas escolas, não há muita probabilidade de um professor ser dominado por alienígenas.

A tomada de controlo de aplicações é uma técnica favorita dos atacantes porque, tal como nos filmes, a maioria dos observadores não repara em nada de errado até ser tarde demais.

Neste caso, um atacante toma um programa em execução, que está atualmente carregado na memória. Assim, o programa totalmente intacto no sistema de ficheiros é ignorado. O programa na memória é editado para incluir o código do atacante. Tal como um alienígena dentro do corpo de um humano. O atacante realiza os seus comportamentos criminosos e, quando o programa termina a execução, a maior parte das provas desaparece. Quando o programa legítimo é executado novamente, se o atacante não editar novamente o código, tudo funciona exatamente como os programadores legítimos originais previram. Talvez uma analogia melhor, neste caso, fosse a de um lobisomem?

Uma lista de permissões de aplicações, então, precisa de trabalho adicional para garantir que o programa, e quaisquer programas ancestrais ou pai, permanecem intactos, sem que um hacker edite os programas enquanto estão em execução.

Em Resumo - Perguntas a Fazer ao Investigar uma Capacidade de Application Whitelist

Certifique-se de compreender os limites que uma lista de permissões permite, ao discutir application whitelisting com a sua equipa de tecnologia ou fornecedor.

1. Esta capacidade examina e monitoriza o que um programa deveria fazer, e compara o comportamento esperado com o observado?
2. Quanto detalhe é que a capacidade de whitelist capta na sua tomada de decisão? Mais, ou menos, do que uma autorização de saída de aluno detalhada?
3. A capacidade de whitelist monitoriza e investiga programas pai e ancestrais quanto a maliciosidade? (Programa A abre B, abre C, abre D – muito comum)
4. A capacidade de whitelist valida que o programa em execução não foi adulterado?

Leitura Aprofundada do National Institute of Standards & Technology (NIST)

Uma publicação de referência que não é para leitura casual, mas é muito descritiva.

Embora não cubra todos os cenários, e os detalhes não sejam atualizados com frequência suficiente para acompanhar todos os cenários, as descrições são suficientemente estratégicas para serem valiosas na maioria das circunstâncias.

A equipa da Cyber Crucible valoriza sempre os conhecimentos das publicações do NIST, e reserva tempo em conformidade.

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-167.pdf>

Revision #1

Created 2026-07-24 05:38:49 UTC by Dennis Underwood

Updated 2026-07-24 05:38:49 UTC by Dennis Underwood