Fiche pratique sur l'analyse de la surface d'attaque

Qu'est-ce que l'analyse de la surface d'attaque et pourquoi est-elle importante ?

Cet article décrit une méthode simple et pragmatique pour effectuer une analyse de la surface d'attaque et gérer la surface d'attaque d'une application. Il est destiné aux développeurs qui souhaitent comprendre et gérer les risques liés à la sécurité des applications lorsqu'ils conçoivent et modifient une application, ainsi qu'aux spécialistes de la sécurité des applications qui effectuent une évaluation des risques liés à la sécurité. L'accent est mis ici sur la protection d'une application contre les attaques externes. Les attaques visant les utilisateurs ou les opérateurs du système (par exemple, l'injection de logiciels malveillants, les attaques d'ingénierie sociale) ne sont pas prises en compte, et les menaces internes sont moins mises en avant, bien que les principes restent les mêmes. La surface d'attaque interne est susceptible d'être différente de la surface d'attaque externe, et certains utilisateurs peuvent disposer d'un accès étendu.

L'analyse de la surface d'attaque consiste à cartographier les parties d'un système qui doivent être examinées et testées afin de détecter les vulnérabilités de sécurité. L'objectif de l'analyse de la surface d'attaque est de comprendre les zones à risque d'une application, de sensibiliser les développeurs et les spécialistes de la sécurité aux parties de l'application qui sont exposées aux attaques, de trouver des moyens de minimiser ce risque et de remarquer quand et comment la surface d'attaque change et ce que cela signifie du point de vue du risque.

Bien que l'analyse de la surface d'attaque soit généralement effectuée par des architectes de sécurité et des testeurs d'intrusion, les développeurs doivent comprendre et surveiller la surface d'attaque lorsqu'ils conçoivent, construisent et modifient un système.

L'analyse de la surface d'attaque vous aide à :

1. identifier les fonctions et les parties du système que vous devez examiner/tester pour détecter les vulnérabilités de sécurité
2. identifier les zones à haut risque du code qui nécessitent une protection approfondie - les parties du système que vous devez défendre
3. identifier les moments où vous avez modifié la surface d'attaque et où vous devez procéder à une évaluation des menaces

Définition de la surface d'attaque d'une application

La surface d'attaque décrit tous les différents points par lesquels un attaquant pourrait pénétrer dans un système et extraire des données.

La surface d'attaque d'une application est :

1. la somme de tous les chemins d'accès aux données/commandes entrant et sortant de l'application, et
2. le code qui protège ces chemins (y compris la connexion aux ressources et l'authentification, l'autorisation, la journalisation des activités, la validation et le codage des données)
3. toutes les données précieuses utilisées dans l'application, y compris les secrets et les clés, la propriété intellectuelle, les données commerciales critiques, les données personnelles et les informations d'identification personnelle, et
4. le code qui protège ces données (y compris le chiffrement et les sommes de contrôle, l'audit des accès, l'intégrité des données et les contrôles de sécurité opérationnelle).

Vous superposez à ce modèle les différents types d'utilisateurs (rôles, niveaux de privilèges) qui peuvent accéder au système (qu'ils soient autorisés ou non). La complexité augmente avec le nombre de types d'utilisateurs différents. Il est important de se concentrer sur les deux extrêmes : les utilisateurs non authentifiés et anonymes et les utilisateurs administrateurs hautement privilégiés (par exemple, les administrateurs de bases de données, les administrateurs système).

Regroupez chaque type de point d'attaque en catégories en fonction du risque (externe ou interne), de l'objectif, de la mise en œuvre, de la conception et de la technologie. Comptez ensuite le nombre de points d'attaque de chaque type. Choisissez ensuite quelques cas pour chaque type. Enfin, concentrez votre examen/évaluation sur ces cas.

Grâce à cette approche, vous n'avez pas besoin de comprendre chaque point d'extrémité pour comprendre la surface d'attaque et le profil de risque potentiel d'un système. Vous pouvez plutôt compter les différents types généraux de points d'extrémité et le nombre de points de chaque type. Cela vous permet d'estimer le budget nécessaire pour évaluer les risques à grande échelle et de déterminer quand le profil de risque d'une application a considérablement changé.

Applications microservices et cloud natives

Les applications microservices et cloud natives sont composées de plusieurs petits composants, faiblement couplés à l'aide d'API et évolutifs de manière indépendante. Lorsque vous évaluez la surface d'attaque des applications de ce type d'architecture, vous devez donner la priorité aux composants accessibles depuis une source d'attaque (par exemple, le trafic externe provenant d'Internet). Ces composants peuvent se trouver derrière des niveaux de proxys, d'équilibreurs de charge et de contrôleurs d'entrée, et peuvent s'adapter automatiquement sans avertissement.

Des outils open source tels que Scope ou ThreatMapper aident à visualiser la surface d'attaque.

Identification et cartographie de la surface d'attaque

Vous pouvez commencer à établir une description de base de la surface d'attaque à l'aide d'une image et de notes. Passez quelques heures à examiner les documents de conception et d'architecture du point de vue d'un attaquant. Lisez le code source et identifiez les différents points d'entrée/de sortie :

- Formulaires et champs de l'interface utilisateur (UI)

- En-têtes HTTP et cookies
- API
- Fichiers
- Bases de données
- Autres stockages locaux
- E-mails ou autres types de messages
- Arguments d'exécution
- ...Vos points d'entrée/sortie

Le nombre total de points d'attaque différents peut facilement atteindre plusieurs milliers, voire plus. Pour faciliter la gestion, divisez le modèle en différents types en fonction de la fonction, de la conception et de la technologie :

- Points d'entrée de connexion/authentification
- Interfaces d'administration
- Fonctions de recherche et de consultation
- Formulaires de saisie de données (CRUD)
- Workflows métier
- Interfaces transactionnelles/API
- Interfaces/API de commande opérationnelle et de surveillance
- Interfaces avec d'autres applications/systèmes
- ...Vos types

Vous devez également identifier les données précieuses (par exemple, confidentielles, sensibles, réglementées) dans l'application, en interrogeant les développeurs et les utilisateurs du système, et en examinant à nouveau le code source.

Vous pouvez également vous faire une idée de la surface d'attaque en analysant l'application. Pour les applications web, vous pouvez utiliser un outil tel que ZAP, Arachni, Skipfish, w3af, ou l'un des nombreux outils ou services commerciaux de test dynamique et d'analyse des vulnérabilités pour explorer votre application et cartographier les parties de l'application accessibles via le web. Certains pare-feu d'applications web (WAF) peuvent également être capables d'exporter un modèle des points d'entrée de l'application.

Validez et complétez votre compréhension de la surface d'attaque en parcourant certains des principaux cas d'utilisation du système : inscription et création d'un profil utilisateur, connexion, recherche d'un article, passation d'une commande, modification d'une commande, etc. Suivez le flux de contrôle et de données à travers le système, voyez comment les informations sont validées et où elles sont stockées, quelles ressources sont touchées et quels autres systèmes sont impliqués. Il existe une relation récursive entre l'analyse de la surface d'attaque et la modélisation des menaces applicatives : les modifications apportées à la surface d'attaque doivent

déclencher la modélisation des menaces, et la modélisation des menaces vous aide à comprendre la surface d'attaque de l'application.

Le modèle de surface d'attaque peut être approximatif et incomplet au départ, surtout si vous n'avez jamais effectué de travail de sécurité sur l'application auparavant. Comblez les lacunes au fur et à mesure que vous approfondissez votre analyse de sécurité ou que vous travaillez davantage avec l'application et que vous vous rendez compte que votre compréhension de la surface d'attaque s'est améliorée.

Mesurer et évaluer la surface d'attaque

Une fois que vous disposez d'une carte de la surface d'attaque, identifiez les zones à haut risque. Concentrez-vous sur les points d'entrée distants (interfaces avec des systèmes externes et Internet), en particulier lorsque le système autorise un accès public anonyme.

- Code exposé au réseau, en particulier au réseau Internet
- Formulaires Web
- Fichiers provenant de l'extérieur du réseau
- Interfaces rétrocompatibles avec d'autres systèmes – anciens protocoles, parfois anciens codes et bibliothèques, difficiles à maintenir et à tester dans plusieurs versions
- API personnalisées (protocoles, etc.) susceptibles de comporter des erreurs de conception et de mise en œuvre
- Code de sécurité : tout ce qui a trait à la cryptographie, à l'authentification, à l'autorisation (contrôle d'accès) et à la gestion des sessions

C'est souvent là que vous êtes le plus exposé aux attaques. Ensuite, identifiez les contrôles compensatoires dont vous disposez, les contrôles opérationnels tels que les pare-feu réseau et les pare-feu applicatifs, ainsi que les systèmes de détection ou de prévention des intrusions qui contribuent à protéger votre application.

Michael Howard, de Microsoft, et d'autres chercheurs ont mis au point une méthode permettant de mesurer la surface d'attaque d'une application et de suivre son évolution dans le temps, appelée « quotient relatif de surface d'attaque » (RSQ). Cette méthode permet de calculer un score global de surface d'attaque pour le système et de mesurer ce score à mesure que des modifications sont apportées au système et à son déploiement. Les chercheurs de Carnegie Mellon se sont appuyés sur ces travaux pour développer une méthode formelle de calcul d'une métrique de surface d'attaque pour les grands systèmes tels que SAP. Ils calculent la surface d'attaque comme la somme de tous les points d'entrée et de sortie, des canaux (les différentes façons dont les clients ou les systèmes externes se connectent au système, y compris les ports TCP/UDP, les points de terminaison RPC, les canaux nommés...) et des éléments de données non fiables. Ils appliquent ensuite un ratio potentiel de dommages/effort à ces éléments de la surface d'attaque afin d'identifier les zones à haut risque.

Notez que le déploiement de plusieurs versions d'une application, le fait de conserver des fonctionnalités qui ne sont plus utilisées au cas où elles seraient nécessaires à l'avenir, ou le fait de conserver d'anciennes copies de sauvegarde et du code inutilisé augmentent la surface d'attaque. Le contrôle du code source et des pratiques de gestion/configuration robustes

devraient être utilisées pour garantir que la surface d'attaque réellement déployée corresponde autant que possible à la surface d'attaque théorique.

Les sauvegardes de code et de données, en ligne et sur des supports hors ligne, constituent une partie importante mais souvent négligée de la surface d'attaque d'un système. Protéger vos données et votre propriété intellectuelle en écrivant des logiciels sécurisés et en renforçant l'infrastructure ne servira à rien si vous laissez tout entre les mains de personnes mal intentionnées en ne protégeant pas vos sauvegardes.

Gestion de la surface d'attaque

Une fois que vous avez acquis une compréhension de base de la surface d'attaque, vous pouvez l'utiliser pour identifier et gérer progressivement les risques à mesure que vous apportez des modifications à l'application. Posez-vous les questions suivantes :

- Qu'est-ce qui a changé ?
- Qu'est-ce que tu fais différemment ? (technologie, nouvelle approche, ….)
- Quelles failles avez-vous pu créer ?

La première page web que vous créez élargit considérablement la surface d'attaque du système et introduit toutes sortes de nouveaux risques. Si vous ajoutez un autre champ à cette page, ou une autre page web similaire, vous avez certes élargi la surface d'attaque sur le plan technique, mais vous n'avez pas augmenté le profil de risque de l'application de manière significative. Chacun de ces changements incrémentiels est similaire, à moins que vous ne suiviez une nouvelle conception ou n'utilisiez un nouveau cadre.

Si vous ajoutez une autre page Web qui suit la même conception et utilise la même technologie que les pages Web existantes, il est facile de comprendre l'ampleur des tests et des contrôles de sécurité nécessaires. Si vous ajoutez une nouvelle API de services Web ou un nouveau fichier pouvant être téléchargé depuis Internet, chacun de ces changements présente à nouveau un profil de risque différent : vérifiez si le changement correspond à une catégorie existante, vérifiez si les contrôles et protections existants s'appliquent. Si vous ajoutez un élément qui n'entre pas dans une catégorie existante, cela signifie que vous devez procéder à une évaluation des risques plus approfondie afin de comprendre quels types de failles de sécurité vous risquez d'ouvrir et quelles protections vous devez mettre en place.

Les modifications apportées à la gestion des sessions, à l'authentification et à la gestion des mots de passe ont une incidence directe sur la surface d'attaque et doivent être examinées. Il en va de même pour les modifications apportées à la logique d'autorisation et de contrôle d'accès, en particulier l'ajout ou la modification de définitions de rôles, l'ajout d'utilisateurs administrateurs ou de fonctions administratives dotées de privilèges élevés. Il en va de même pour les modifications apportées au code qui gère le chiffrement et les secrets. Les modifications fondamentales apportées à la manière dont la validation des données est effectuée. Et les modifications architecturales majeures apportées à la stratification et aux relations de confiance, ou les modifications fondamentales de l'architecture technique - remplacement de votre serveur web ou de votre plateforme de base de données, ou modification du système d'exploitation d'exécution.

Lorsque vous ajoutez de nouveaux types d'utilisateurs, rôles ou niveaux de privilèges, vous effectuez le même type d'analyse et d'évaluation des risques. Superposez le type d'accès aux données et aux fonctions et recherchez les problèmes et les incohérences. Il est important de comprendre le modèle d'accès de l'application, qu'il soit positif (l'accès est refusé par défaut) ou négatif (l'accès est autorisé par défaut). Dans un modèle positif

Dans un modèle d'accès positif, toute erreur dans la définition des données ou des fonctions autorisées à un nouveau type d'utilisateur ou à un nouveau rôle est facilement identifiable. Dans un modèle d'accès négatif, vous devez être beaucoup plus vigilant pour vous assurer qu'un utilisateur n'ait pas accès à des données/fonctions qui ne lui sont pas autorisées.

Ce type d'évaluation des menaces ou des risques peut être effectué périodiquement, dans le cadre du travail de conception dans le cadre de projets de développement en série, par étapes, en spirale ou en cascade, ou de manière continue et progressive dans le cadre d'un développement agile ou itératif.

Normalement, la surface d'attaque d'une application augmente au fil du temps à mesure que vous ajoutez des interfaces et des types d'utilisateurs et que vous intégrez d'autres systèmes. Vous devez également chercher des moyens de réduire la taille de la surface d'attaque lorsque cela est possible, en simplifiant le modèle (par exemple, en réduisant le nombre de niveaux d'utilisateurs ou en ne stockant pas les données confidentielles qui ne sont pas absolument nécessaires), en désactivant les fonctionnalités et les interfaces qui ne sont pas utilisées, en introduisant des contrôles opérationnels tels qu'un pare-feu d'application web (WAF) et une détection en temps réel des attaques spécifiques aux applications.