



Formation

Architecture Microservices

La sécurité



Fabien BRISSONNEAU

Une formation
Alphorm.com

Cursus





Plan

Le propriétaire de la ressource

La ressource

Le principal : identité et rôle

Authentification

Autorisation

Chiffrement

Une formation
Alphorm.com



Public concerné

Développeurs

Pratiquants devops

Chefs de projet

Une formation
Alphorm.com



Connaissances requises

Langage de programmation

Une formation
Alphorm.com





Présentation du projet



Fabien BRISSONNEAU

Une formation
Alphorm.com



Plan

Les généralités sur la sécurité
Projet Visual Studio pour C#
Architecture microservice
Créer une API Gateway
Projet PHPStorm
Projet IntelliJ pour Java

Une formation
Alphorm.com



Les outils

Visual Studio pour C#

IntelliJ pour Java

PHPStorm pour PHP

Une formation
Alphorm.com



Comprendre les notions de la sécurité



Fabien BRISSONNEAU

Une formation
Alphorm.com



Plan

Le propriétaire de la ressource

La ressource

Le principal : identité et rôle

Authentification

Autorisation

Chiffrement

Une formation
Alphorm.com



Le propriétaire

Détient les preuves

Devrait avoir accès aux ressources

Une formation
Alphorm.com



La ressource

Ce qui est protégé
Fichiers, données, informations...

Une formation
Alphorm.com



Le principal

Informations sur l'utilisateur
Rôles qu'il assume

Une formation
Alphorm.com



Authentification

Etablir et vérifier l'identité d'un principal



Autorisation

Déterminer si un principal est autorisé

Accès à une ressource



Chiffrement

Symétrique ou asymétrique

Être le seul à chiffrer

Être le seul à déchiffrer

Une formation
Alphorm.com



Cryptographie

Intégrité des données

Authentification de l'origine

Non-répudiation de l'origine

Une formation
Alphorm.com



Une formation
Alphorm.com

Utiliser le Framework OAuth2



Fabien BRISSONNEAU



Une formation
Alphorm.com

Plan

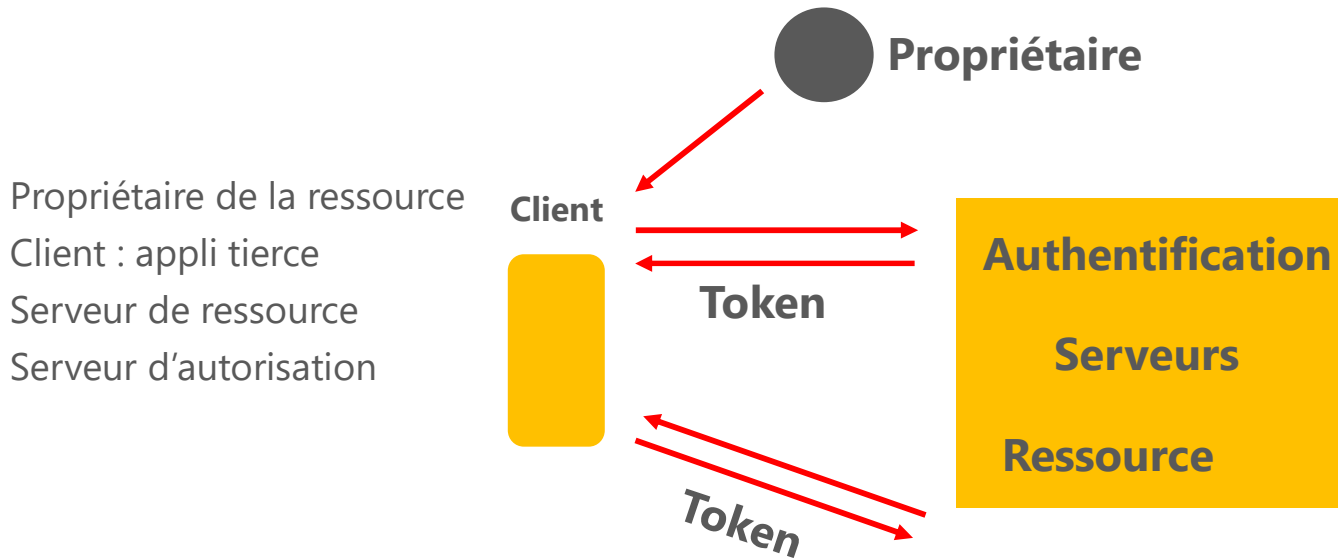
Les composants principaux

Les tokens

Les scénarios d'authentification

Exemple Google APIs

Les composants principaux



Les tokens

Token d'accès : accéder à la ressource

Token de refresh : pour obtenir un nouveau token



Les scénarios d'utilisation

Avec un code

Autorisation implicite

Avec identifiants du propriétaire

Avec identifiants du client



Exemple Google APIs

Récupérer des infos de client

Obtenir un token de Google
Authorization Server

Examiner les scopes d'accès

Envoyer le token à une API

Rafraîchir le token d'accès



Une formation
Alphorm.com

Valider les entrées



Fabien BRISSONNEAU



Une formation
Alphorm.com

Plan

Les problèmes

La validation au plus tôt



Les problèmes

Aspect général du logiciel
Cas particuliers des applis Web
Formulaires, paramètres, uploads...
Injections SQL
XSS (cross-site scripting)

Une formation
Alphorm.com



Les solutions

Vérifier les entrées le plus tôt
Filtrer les caractères spéciaux
Les champs sont typés
Réduire la surface d'attaque
Syntaxique et sémantique

Une formation
Alphorm.com



Les solutions

Les validations HTML5
Whitelist plutôt que blacklist
Validateurs des frameworks
Schémas JSON et XML
Conversion de types
Minimum et maximum
Expressions régulières

Une formation
Alphorm.com



Définir la sécurité .Net



Fabien BRISSONNEAU

Une formation
Alphorm.com



Plan

Sécurité basée sur les rôles

La stratégie

Sécurité de type

Chiffrement

Une formation
Alphorm.com



Sécurité basée sur les rôles

Le principal est basé sur une identité

Les informations sur le principal sont
disponibles pour le thread courant

Un principal encapsule identité et rôles

Les autorisations sont accordées en
fonction de l'identité ou du rôle

Une formation
Alphorm.com



La stratégie

La sécurité .Net est pilotée par stratégie
Associer autorisations et preuves
Le stockage isolé



Les secrets

Un secret est une information qui ne
doit pas être publique
Le secret a une durée de vie limitée
Les secrets sont protégés par crypto



Chiffrement

Le système de chiffrement est organisé par héritage

Type d'algorithme : SymmetricAlgorithm, HashAlgorithm, ..

Classe d'algorithme : Aes, RSA, ECDiffielHellamn, ...

Implémentations : AesManaged, ...

Les implémentations

*CryptoServiceProvider, des wrappers autour de CAPI

*Cng, des wrappers autour de CNG

*Managed des classes entièrement en code managé

Une formation
Alphorm.com



Utiliser les outils de sécurité



Fabien BRISSONNEAU

Une formation
Alphorm.com



Plan

Les noms forts des assemblies
ILDASM
Rechercher dans le code

Une formation
Alphorm.com



Les noms forts

Créer un nom fort
Utiliser Visual Studio
La livraison dans le GAC

Une formation
Alphorm.com



ILDASM

Désassembler IL

Les attributs de l'assembly

Retrouver la signature

Une formation
Alphorm.com



Rechercher dans le code

A partir d'un autre assembly

Récupérer les informations

Une formation
Alphorm.com



Une formation
Alphorm.com

Mettre en œuvre la sécurité



Fabien BRISSONNEAU



Une formation
Alphorm.com

Plan

- Le contrôle basé sur les rôles
- Les attributs
- Authentification externe
- Lire le principal



Le contrôle basé sur les rôles

Les utilisateurs portent des rôles

Les rôles sont contrôlés



Les attributs

Authorize

```
[Authorize(Users = @"DESKTOP-P15HT02\Eixa6")]
```

0 références

```
public ActionResult Contact()  
{
```

Applicable aussi sur une classe

AllowAnonymous est l'inverse



Authentification externe

Consiste à utiliser un service externe
Echange de preuves et de token
Plusieurs scénarios possibles
Plusieurs services possibles



Lire le principal

La propriété User.Identity
Vérifications d'authentification
Récupération du nom



Une formation
Alphorm.com

Protéger le contenu des assemblies



Fabien BRISSONNEAU



Une formation
Alphorm.com

La décompilation

Un outil : ILDASM
Lire Intermediate Language



L'obsfucation

Mettre en œuvre
Le résultat

Une formation
Alphorm.com



Conclusion

Pour éviter la décompilation
Utiliser l'obsfucation

Une formation
Alphorm.com



Protéger l'exécution des programmes



Fabien BRISSONNEAU

Une formation
Alphorm.com



Plan

Chargement des assemblies
Compilation JIT
Code Access Security

Une formation
Alphorm.com



Chargement des assemblies

Une application interagit avec le CLR

Un jeu d'autorisations par appli



Compilation JIT

Quand IL est exécuté

Compilation JIT

Vérification type-safe

Vérifier avec peverify



Code Access Security

Restrictions selon le niveau de confiance
Exécution selon les permissions données
Exécution ou levée d'exception



Conclusion

Donner des autorisations aux applis
Identifier les preuves des assemblies
Lier les assemblies aux groupes de code
En déduire un ensemble d'autorisations



Déployer une stratégie de sécurité dans le CLR



Fabien BRISSONNEAU

Une formation
Alphorm.com



La stratégie de sécurité

Associer les autorisations aux preuves

Limiter l'accès autorisé

Preuves : namespaces, zones, ...

Autorisations : fichiers, exécutions, ...

Une formation
Alphorm.com



Les niveaux de stratégies

Stratégie de l'ordinateur

Stratégie de l'utilisateur

Stratégie de l'hôte



Les impacts sur l'exécution

Limitation à des droits

Limitation à des exécutables



Conclusion

La stratégie de sécurité est définie
Impacts sur l'exécution

Une formation
Alphorm.com



Choisir confiance totale ou partielle



Fabien BRISSONNEAU

Une formation
Alphorm.com



Le code de type sécurisé

Un code qui accède aux types autorisés

Accès sécurisé

Lié au compilateur



Syntaxe

Impérative / déclarative

Le code demande des autorisations

Soit avec du code impératif

Soit avec des déclarations



Bibliothèques de classes

Utilise des demandes de sécurité
Oblige le client à avoir les droits
Net framework en propose certaines



Code transparent

A partir de Framework 4
Ne peut pas appeler du code critique
Pour applications confiance totale
Et applications confiance partielle



Conclusion

Le niveau de confiance du code
Le lien avec le langage de
programmation

Une formation
Alphorm.com



Les différences avec une architecture monolithique



Fabien BRISSONNEAU

Une formation
Alphorm.com



Plan

La surface d'attaque

La sécurité et les performances

Le démarrage des micro-services

Les requêtes sur plusieurs

Une formation
Alphorm.com



La surface d'attaque

Les points d'entrée

Un seul pour le monolithe

Nombreux en micro-services

Une formation
Alphorm.com



La sécurité et les performances

Tester la sécurité
Au point d'entrée
Sur chaque micro-service

Une formation
Alphorm.com



Le démarrage

Les micro-services sont liés
Automatisation nécessaire
Validation d'un service par ses pairs

Une formation
Alphorm.com



Les requêtes sur plusieurs

Doit être observable

Créer des logs

Créer des métriques

Générer des traces



Conclusion

Autres défis

Les conteneurs sont immuables

Le contexte utilisateur

Architecture multi-techniques



Mettre en œuvre un serveur OpenId Connect



Fabien BRISSONNEAU

Une formation
Alphorm.com



Standard ouvert

L'implémentation est libre

Un client, serveur quelconque

Utilise JSON Signing and Encryption

Une formation
Alphorm.com



Basé sur OAuth2

ID Token utilise un JWT
Pour le propriétaire de la ressource
Doit être parsé



Dédié à l'authentification

ID Token contient un accès aux data
Utilise un UserInfo endpoint
Récupère les preuves de l'utilisateur



Une formation
Alphorm.com

Utiliser un serveur OpenId Connect



Fabien BRISSONNEAU



Une formation
Alphorm.com

Générer un ID Token

Le token possède des champs
URL du demandeur
L'id de l'utilisateur, du client
Une durée de vie, une date
Tout est signé



Créer un URL endpoint

Méthodes GET et POST

Fournit les preuves de l'utilisateur



Parser l'ID Token

Utilisant la clé du serveur

Déchiffrer, vérifier

Récupérer les informations



Justifier une API Gateway



Fabien BRISSONNEAU

Une formation
Alphorm.com



Exposition des microservices

Eviter d'exposer les microservices
URL complexes
Hétérogénéité

Une formation
Alphorm.com



Découpler la sécurité

Gérer la sécurité en transparence

Aspects non fonctionnels

Code polluant

Code changeant

Une formation
Alphorm.com



Améliorer la cohérence

Les granularités des services

Difficultés à consommer

Les interfaces ne sont pas cohérentes

Une formation
Alphorm.com



Gérer la granularité

Les services sont hétérogènes
Granularité très différentes
Orchestration des appels

Une formation
Alphorm.com



Mettre en place une API Gateway



Fabien BRISSONNEAU

Une formation
Alphorm.com



Rôle de l'API Gateway

Gérer la sécurité : accès, quotas, ...

Tracer les actions : logs, métriques, ...

Régler le routage, ...

Equilibrer les charges



Exemples d'implémentations

Kong

Ambassador

Gloo

Istio



Sécuriser entre services avec TLS



Fabien BRISSONNEAU

Une formation
Alphorm.com



L'exposition avec TLS

Savoir avec qui on parle
Sécuriser les transferts d'information
Https est http sur TLS
Handshake client-serveur

Une formation
Alphorm.com



Autorité de certification

Capacité de vérification du certificat
OpenSSL est une implémentation
Une autorité connue des services



Utiliser mutual TLS

TLS seul identifie le serveur
mTLS permet la réciproque



Une formation
Alphorm.com

Communiquer entre services avec JWT



Fabien BRISSONNEAU



Une formation
Alphorm.com

Plan

Intérêt de JWT

Nécessité d'un SecurityTokenService

Usages du JWT



Intérêt de JWT

Communiquer entre services
Standard (Header)
Sécurisé (Signature)
Partager un contexte (Payload)



Définition de JWT

Infos en JSON contenant une preuve
Auto descriptif

```
{  
  "name": "John Doe",  
  "email": "john@johndoe.com",  
  "admin": true  
}
```



Nécessité d'un STS

Service de production du token
Accessible des services du cluster
Seul AS produit la signature



Usages du JWT

Contient de l'information
Authentification de l'utilisateur
Gestion de session
Encodé Base64 / Base64Url



Informations

Iss pour l'entité génératrice (serveur)
iat pour le timestamps de création
Sub pour l'id technique de l'utilisateur
Exp pour le timestamps expiration



Conclusion

Sécuriser avec JWT
Capable de déchiffrer
Contexte utilisateur avec JWT
Identification et expiration



Les bons réglages en PHP



Fabien BRISSONNEAU

Une formation
Alphorm.com



Plan

- Les bonnes pratiques
- La configuration php.ini
- Les fonctions non sécurées
- Les fonctions à restreindre
- Activer les protections

Une formation
Alphorm.com



Les bonnes pratiques

Être à jour des versions

Utiliser du SQL précompilé

Valider les entrées utilisateurs

Protocole SSL

Eviter l'inclusion de fichiers

Une formation
Alphorm.com



La configuration php.ini

display_errors Désactiver l'affichage des erreurs

group_id à un niveau bas

allow_url_include OFF

memory_limit : attaque DoS

max_execution_time

max_input_time

Une formation
Alphorm.com



Les fonctions non sécurées

Utiliser `disable_functions` pour
phpinfo, system, mail, exec
Dimensionner les ressources



Les fonctions à restreindre

Si non nécessaires
File_uploads, display_errors,
allow_url_fopen, expose_php, ...



Activer les protections

Plus d'information

`cgi.force.redirect`, `log_errors`

Safe modes

`safe_mode`, `sql.safe_mode`



Conclusion

Modifier les paramètres pour sécuriser

Eviter de fournir des informations

Eviter les accès non souhaités



PHP, la sécurité des bases de données



Fabien BRISSONNEAU

Une formation
Alphorm.com



Plan

- Chaque base propose ses primitives
- Les PHP data objects
- Les crédits de connexion
- Le SQL précompilé

Une formation
Alphorm.com



Les primitives

Chaque base propose ses fonctions
Autant d'extensions à installer
Interfaces différentes
Accroît les difficultés

Une formation
Alphorm.com



Les PHP Data Objects

Une interface unique
Plusieurs bases de données
Nécessite d'utiliser un SQL commun

Une formation
Alphorm.com



Les crédits de connexion

Déplacer les infos de connexion
Ne pas les placer dans le code
Par environnement
Ne pas les versionner



Le SQL pré compilé

Ne pas exécuter SQL + variables
Filtrer les entrées utilisateur
Utiliser Prepared Statements
Et Bound Parameters



Conclusion

Utiliser les PDO

Pré compiler le SQL

Lié des paramètres vérifiés

Une formation
Alphorm.com



Les vulnérabilités des applications Web



Fabien BRISSONNEAU

Une formation
Alphorm.com



Plan

- Injection
- Authentification
- Exposition de données sensibles
- Données externes XML
- Contrôle d'accès brisé
- Mauvaise configuration de sécurité
- Cross-site scripting

Une formation
Alphorm.com



Injection

- Injection de données non vérifiées
- Dans une commande ou un requête
- L'interpréteur va exécuter la commande

Une formation
Alphorm.com



Authentification

Compromission de mots de passe

Ou de clés, de tokens ...

Par exemple en PHP, les données de session stockées en clair sur le filesystem



Exposition de données

Données sensibles non protégées

Le vol ou la modification de ces infos

Les données doivent être protégées, au repos comme en transit

Attention particulière lorsqu'elles sont échangées avec un navigateur



Données externes XML

Données XML parsées

Une référence vers une donnée externe

Mène au vol de données, DoS, scan de ports ...



Contrôle d'accès brisé

Les restrictions d'accès aux utilisateurs

L'attaque consiste à utiliser ces accès

Vol de données, modifications...



Mauvaise configuration

La configuration de sécurité

Définie et déployée

Pour l'application, les serveurs, les
frameworks, ...

Par défaut, souvent non sûrs



Cross site scripting

Exécution de script sur le navigateur

Pour récupérer des infos, rediriger ailleurs

Une application prend des données et les
envoie sans validation au navigateur



Conclusion

OWASP a décrit les cas fréquents
Ces erreurs se répètent
Pas toujours corrigées

Une formation
Alphorm.com



Java, charger les classes et utiliser SandBox



Fabien BRISSONNEAU

Une formation
Alphorm.com



Plan

Les class loader de Java
La vérification du bytecode
Le SecurityManager

Une formation
Alphorm.com



Les class loader de Java

Class loader primordial
Class loader d'extensions
Class loader d'application
Vérifient que le code nouveau ne
remplace pas des éléments systèmes

Une formation
Alphorm.com



La vérification du bytecode

Lorsque le loader présente la classe
Le « verifier » contrôle les instructions
Variables initialisées, méthodes sur les
types, règles de visibilité, variables locales
dans la pile, pas de débordement ...



Le SecurityManager

Vérifie à l'exécution
Méthodes dangereuses :
entrées/sorties, accès réseau,
définition de class loader ...



Conclusion

Le modèle SandBox

Empêche le code malveillant de nuire
Plusieurs composants coopèrent

Une formation
Alphorm.com



Java, Utiliser SecurityManager



Fabien BRISSONNEAU

Une formation
Alphorm.com



Plan

La classe SecurityManager
Interagir avec le SecurityManager
Les fichiers de configuration



La classe SecurityManager

Définit la politique de sécurité
Quelles actions sont safe
Fournit des informations aux
applications



Avec SecurityManager

Récupérer le SecurityManager
Tester la possibilité d'une permission

Une formation
Alphorm.com

Les fichiers de configuration

La liste des fichiers
Modifier les permissions

```
Main.java x policy x
grant {
    permission java.security.AllPermission "", "";
};|
```



Conclusion

SecurityManager vérifie les permissions
La configuration peut être modifiée

Une formation
Alphorm.com



Java, Mettre en œuvre la protection du bytecode



Fabien BRISSONNEAU

Une formation
Alphorm.com



Plan

Le bytecode décompilé
L'obfuscation du code



Le bytecode décompilé

Il existe plusieurs décompilateurs
Code résultant proche du source
Avec infos de debug éventuellement



L'obfuscation du code

Définition de l'obfuscation

Des outils pour obfusquer

Les limites de l'obfuscation

Une formation
Alphorm.com



Conclusion

Le bytecode est facilement décompilé

L'obfuscation masque le source

Une formation
Alphorm.com



Une formation
Alphorm.com

Découvrir l'architecture de JAAS



Fabien BRISSONNEAU



Une formation
Alphorm.com

Définition de JAAS

Java Authentication and Autorisation
Gérer identifications et droits



Principales classes

Principal

Une identité du demandeur

Subject

Le demandeur

LoginModule

Interface du AP

LoginContext

Méthode de login

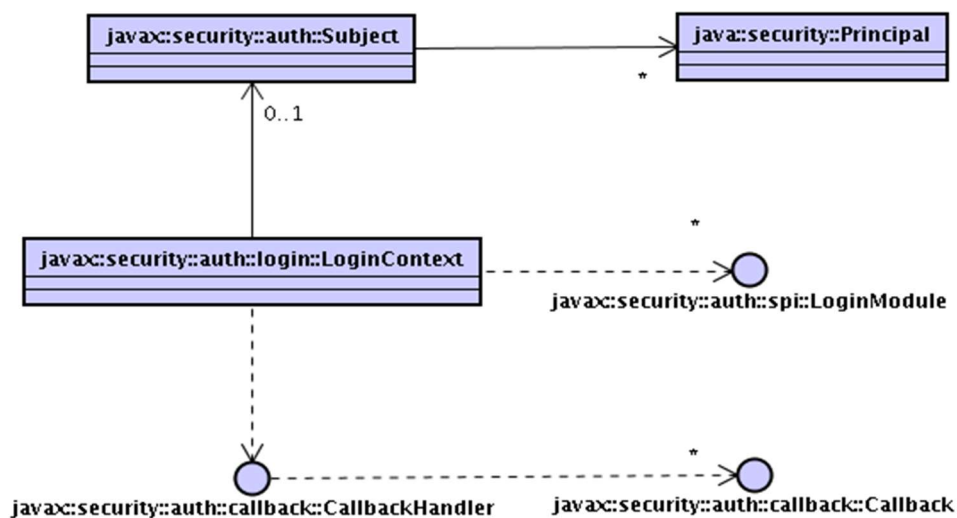
Callback

Interface de la demande

Une formation
Alphorm.com

Schéma

Mis en œuvre dans Jboss, BEA, ...





Conclusion

JAAS est une solution pour sécuriser
Partie de J2SE
Utilisé par les composants JEE

Une formation
Alphorm.com



S'authentifier avec le PAM



Fabien BRISSONNEAU

Une formation
Alphorm.com



Définition de PAM

Pluggable Authentication Modules

Intégrer des stratégies diverses

Une API pour étoffer une phase

Une librairie pour intégration



Fonctionnement

Définit des services (applications)

Un service contient des règles

Une règle lance un module



Cas concret

Choisir une application /etc/pam.d/x
Pile plus ou moins complète



Conclusion

Composant de l'ensemble gnu/linux
Nombreux usages
Cohérence de la sécurité



Gérer les permissions



Fabien BRISSONNEAU

Une formation
Alphorm.com



Exemple avec check_user

Récupérer les sources
Construire le binaire

Une formation
Alphorm.com



Exemple sans permission

Le fichier / application n'existe pas
Traitement par défaut



Mise en oeuvre

Création d'un fichier / application
Définir
auth required pam_unix.so
account required pam_unix.so



Une formation
Alphorm.com

Conclusion



Fabien BRISSONNEAU



Une formation
Alphorm.com

Bilan

Les généralités sur la sécurité
La sécurité en code .Net
La sécurité avec les microservices
La sécurité avec API Gateway
La sécurité avec PHP
La sécurité avec Java

