



MACARONS DES COOKIES EN MIEUX !

Julien Tanguy

WHOAMI



AUTORISATION

AUTHENTIFICATION VS AUTORISATION

Qui suis-je ?

Qu'ai-je le droit de faire ?

BEARER TOKENS

A security token with the property that any party in possession of the token (a "bearer") can use the token in any way that any other party in possession of it can.

— RFC6750

EXAMPLE: GOOGLE DRIVE

[https://drive.google.com/open?
id=197u0vRt8_VvTa0GaNknMRVQkm-Q](https://drive.google.com/open?id=197u0vRt8_VvTa0GaNknMRVQkm-Q)

CAS D'USAGE: PARTAGE DE FICHIERS

- Système de fichiers dans le cloud
- Je veux partager un dossier à *Alice*
- *Alice* veut repartager une partie de ce dossier à *Bob*

MACAROONS

- Papier de recherche Google publié en 2014 [[pub41892](#)]
- Restriction des accès avec des *caveats*

ANATOMIE D'UN *MACAROON*

- Secret
- Identifiant
- Url
- Signature
- *Caveats*

CRÉATION

1. Macaroon m = `Macaroon.create(secret, identifier, location)`
2. Done.

CAVEATS

Liste **ordonnée** de prédicats qui limitent l'autorité
d'un macaroon

Deux types de caveat * primaires (*first party*) * tiers (*third party*)

CAVEATS PRIMAIRES

- `account = 123456`
- `file in ["accounts.pdf", "bills.pdf"]`
- `time < 2017-05-18T14:45+02:00`

AJOUT

0. Macaroon m , assertion $\mathcal{A} = \text{account} = 123456$
1. $m.\text{addFirstPartyCaveat}(\mathcal{A})$
2. Done.

VÉRIFICATION

- `account = 123456`
- `file in ["accounts.pdf", "bills.pdf"]`
- `time < 2017-05-18T14:45+02:00`

CAVEATS TIERS

Prédicats externes non listés dans le *macaroon*.

- L'utilisateur doit être authentifié chez `auth.com` comme *Alice*
- L'utilisateur doit être authentifié comme *Bob*

AJOUT

- 3. Assertion $\mathcal{A}$ = 'user = Alice', secret $\mathcal{S}$
- 2. Envoi de $\mathcal{A} + \mathcal{S}$ à **auth.com**
- 1. On récupère l'identifiant id_{auth}
- 0. Macaroon m
 - 1. $m.addThirdPartyCaveat(\mathcal{S}, id_{auth}, \text{auth.com})$
 - 2. Done.

*Le secret partagé n'est **pas** dans le macaron final*

VÉRIFICATION

Un *caveat* tiers doit être *déchargé* par un autre macaron.

SIGNATURE

La signature est recalculée à chaque fois que l'on rajoute un *caveat*.

1. $sig_0 = HMAC(secret, identifier);$
2. $sig_1 = HMAC(sig_0, caveat_0);$
3. $sig_2 = HMAC(sig_1, caveat_1);$
4. etc...

MACAROONS VS JWT

SIMILITUDES

- Token
- Signature

DIFFÉRENCES

	<i>Macaroon</i>	JWT
Algo de hash	HMAC-SHA256	Dans le JWT
Donnée additionnelle	Caveats (soustractif)	Claims (additif)
Délégation	Possible (client-side)	Impossible (nouveau JWT)

EXEMPLE: PARTAGE DE FICHIERS

- Accès aux fichiers grâce à des macarons
- On peut modifier et restreindre le partage

EXAMPLE

1. *Macaroon* m_{julien}
2. `prefix = subfolder` $\rightarrow m_{alice}$
3. `mode = readonly` $\rightarrow m_{bob}$

AUTORISATION DANS UN CONTEXTE MICROSERVICES



clever cloud

- Infrastructure immutable
- Microservices

GESTION DES CACHES DE BUILD

- Caches sauvegardés sur un S3-like
- Service qui gère le déploiement de l'application
- Service qui gère le cache de build
- Proxy S3: API gateway

UTILISATION DES MACARONS

1. L'*application manager* crée un bucket pour stocker les caches de build
2. Les clés sont stockées *chiffrées* dans la DB de l'*API gateway*
3. l'*API gateway* donne un macaron qui permet de demander des urls présignées
4. Le macaron est passé au *build cache manager*, qui peut discuter directement avec la *gateway S3*

IMPLÉMENTATIONS

<http://macaroons.io>

C, C#, Go, Java, Javascript, Python, Ruby, Rust, PHP (Haskell)

LIENS

- [libmacaroons] *Implémentation de référence.*
<https://github.com/rescrv/libmacaroons>
- [pub41892] Arnar Birgisson et al. *Macaroons: Cookies with Contextual Caveats for Decentralized Authorization in the Cloud.* Network and Distributed System Security Symposium, Internet Society. 2014. <https://research.google.com/pubs/pub41892.html>
- [cordellBlog] Evan Cordell. *Macaroons 101: Contextual Confinement.* Elegant authorization, for a more civilized age. 2015.
<http://evancordell.com/2015/09/27/macaroons-101-contextual-confinement.html>

MERCI

- <https://twitter.com/jutanguy>
- <https://github.com/jtanguy>
- <https://jtanguy.cleverapps.io>