

A first glance at the Universal Second Factor (U2F) protocol

Florian Maury
ANSSI

Mickaël Bergem
ParisTech

2 juin 2016
SSTIC



Pourquoi faire un nouveau protocole d'authentification à deux facteurs ?



Des problèmes avec les codes SMS et TOTP

Retransmission des codes :

- ▶ SMS et TOTP vulnérables au hameçonnage

Secrets symétriques :

- ▶ stockage en clair d'information par le serveur



FIGURE : <https://xkcd.com/525/>

SS7 est peu sûr (SS7 Security Report – Positive Technologies)



Universal Second Factor (U2F)



U2F : qui ? quand ? quoi ? comment ?

Qui ?

- ▶ normalisation : consortium FIDO Alliance
- ▶ services actuellement protégeables par U2F : Google, Github, Dropbox

Quand ?

- ▶ spécifications 1.0 : mai 2015

Quoi ?

- ▶ tokens cryptographiques logiciels, USB, BT ou NFC

Comment ?

- ▶ tokens disponibles en ligne



U2F : qui ? quand ? quoi ? comment ?

Qui ?

- ▶ normalisation
- ▶ services en ligne : Github, D

Quand ?

- ▶ spécifications

Quoi ?

- ▶ tokens connectés

Comment ?

- ▶ tokens disponibles en ligne



ce
U2F : Google,

u NFC



U2F : qui ? quand ? quoi ? comment ?

Qui ?

- ▶ normalisation : consortium FIDO Alliance
- ▶ services actuellement protégeables par U2F : Google, Github, Dropbox

Quand ?

- ▶ spécifications 1.0 : mai 2015

Quoi ?

- ▶ tokens cryptographiques logiciels, USB, BT ou NFC

Comment ?

- ▶ tokens disponibles en ligne



Procédure d'authentification U2F typique

Authentification en deux étapes :

- ▶ saisie d'un mot de passe
- ▶ puis, activation du token U2F

The image displays two sequential screenshots of the Google authentication interface, connected by a red arrow pointing from left to right.

Left Screenshot: "Tout Google avec un seul compte"
Title: Google
Text: Connectez-vous à votre compte Google.
Form: A text input field labeled "Saisissez votre adresse e-mail" with a blue "Suivant" button below it.
Text: Besoin d'aide ?
Text: Créer un compte
Text: Tout Google avec un seul compte
Icons: G, M, Y, R, B, P, L, T, C

Right Screenshot: "Validation en deux étapes"
Title: Google
Text: Pour contribuer à préserver la sécurité de vos e-mails, de vos photos et d'autres contenus, veuillez procéder comme suit.
Image: A security key icon.
Text: Insérez votre clé de sécurité.
Text: Si votre clé de sécurité comporte un bouton, appuyez sur celui-ci. Si ce n'est pas le cas, retirez-la, puis insérez-la à nouveau.
Text: Ne plus me demander sur cet ordinateur
Text: Essayez de vous connecter d'une autre manière



Cryptographie asymétrique :

- ▶ une bi-clé par *origin*
- ▶ ECDSA sur P-256
- ▶ validation manuelle unitaire



Cryptographie asymétrique :

- ▶ Une *origin* = (scheme, host, port)
 - ▶ exemple : (http, www.ssi.gouv.fr, 80)
- ▶ validation manuelle unitaire



Cryptographie asymétrique :

- ▶ une bi-clé par *origin* \Leftarrow **prévient le hameçonnage**
- ▶ ECDSA sur P-256
- ▶ validation manuelle unitaire



Cryptographie asymétrique :

- ▶ une bi-clé par *origin* \Leftarrow **prévient le hameçonnage**
- ▶ ECDSA sur P-256
- ▶ validation manuelle unitaire \Leftarrow **limite les oracles**



Du stockage des clés cryptographiques

Utilisation d'un identifiant de clé, associé à une *origin*

- ▶ *key handle*

Deux types de stockage de clés :

- ▶ dans le token ; mémoire interne finie
- ▶ hors du token : *key handle* = clé privée *wrappée*

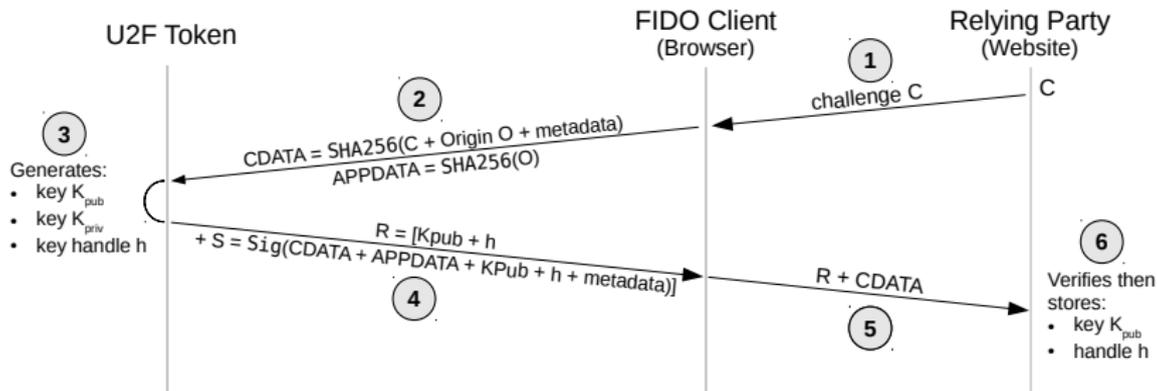
Objectif de la première phase d'authentification :

- ▶ identifier le *key handle* à utiliser par U2F

Détails des échanges protocolaires

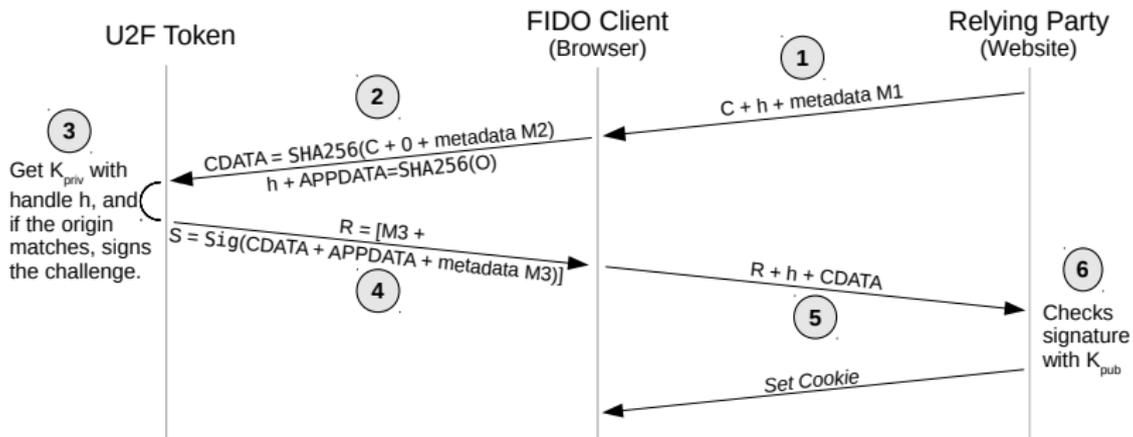


Détails des échanges protocolaires : Enregistrement





Détails des échanges protocolaires : Authentification



Analyse de sécurité



Propriétés étudiées :

- ▶ anti-rejeu
- ▶ résistance au hameçonnage

Prérequis :

- ▶ TLS pour assurer la confidentialité du matériel authentifiant
- ▶ Chrom{e,ium} 41+



Propriétés étudiées :

- ▶ anti-rejeu \Leftarrow **nonces, compteur**
- ▶ résistance au hameçonnage

Prérequis :

- ▶ TLS pour assurer la confidentialité du matériel authentifiant
- ▶ Chrom{e,ium} 41+



Propriétés de sécurité « étudiées »

Propriétés étudiées :

- ▶ anti-rejeu \Leftarrow **nonces, compteur**
- ▶ résistance au hameçonnage \Leftarrow **clé unique par origin**

Prérequis :

- ▶ TLS pour assurer la confidentialité du matériel authentifiant
- ▶ Chrom{e,ium} 41+



Propriétés étudiées :

- ▶ anti-rejeu \Leftarrow **nonces, compteur**

- ▶ **Avertissement :**

- ▶ pas de vérification formelle

Pré

- ▶ TLS pour assurer la confidentialité du matériel authentifiant
- ▶ Chrom{e,ium} 41+

Contre-mesure aux MITM TLS



Définition du MITM TLS

Dans le cadre d'U2F, MITM TLS signifie :

- ▶ attaquant sur le chemin réseau
- ▶ même *origin* que le site légitime
- ▶ certificat « validé » (par le navigateur ou l'utilisateur)



TLS Channel ID :

- ▶ extension TLS
- ▶ défini dans un Internet-Draft expiré
- ▶ redéfinition en cours par le GT tokbind
- ▶ prise en charge optionnelle dans U2F
- ▶ une bi-clé générée une fois par serveur



Objectif de TLS Channel ID

Être un identifiant liant les deux terminateurs de connexion et le transcript TLS



Objectif de TLS Channel ID

Être un identifiant liant les deux terminateurs de connexion et le transcript TLS

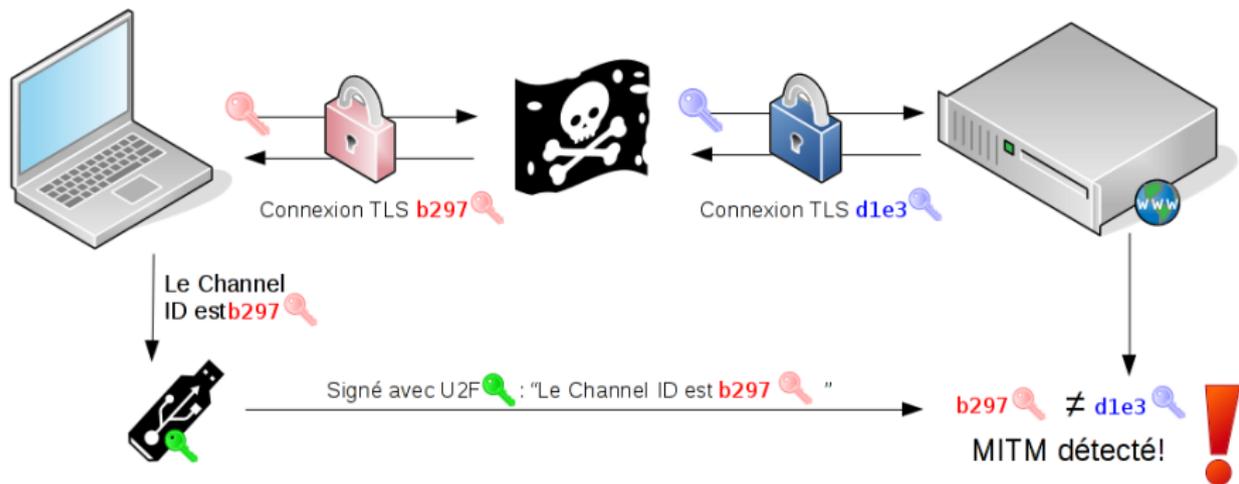


FIGURE : U2F signe le TLS Channel ID pour prévenir le MITM TLS



Objectif de TLS Channel ID

Être un identifiant liant les deux terminateurs de connexion et le transcript TLS

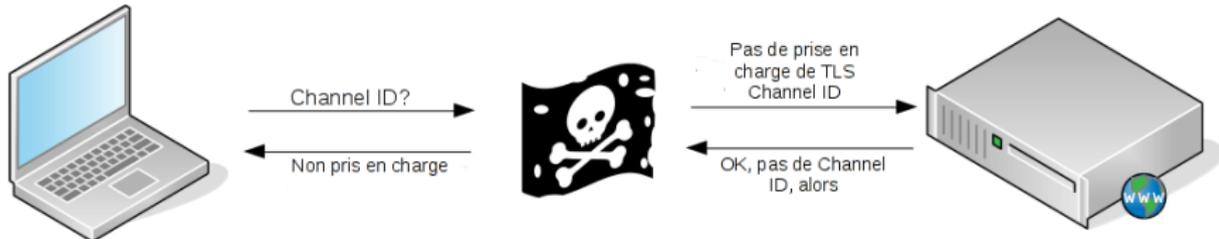


FIGURE : TLS Channel ID est vulnérable aux attaques par dégradation du niveau de sécurité s'il est optionnel et utilisé seul



Objectif de TLS Channel ID

Être un identifiant liant les deux terminateurs de connexion et le transcript TLS

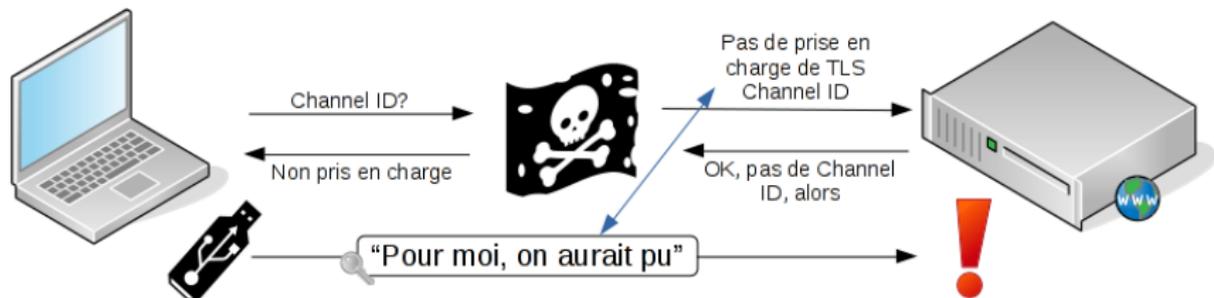


FIGURE : U2F renforce TLS Channel ID en prévenant ce type d'attaque

« Et ça marche, ce truc ? »



Qui essaie de négocier TLS Channel ID ?

Service Web	Prise en charge de TLS Channel ID
Google	✓
Github	✗
Dropbox	✗



Connexion avec mot de passe à Google

Burp Suite: TLS Proxy

The screenshot displays the Burp Suite interface. The top menu bar includes Applications, Places, and StartBurp. The main toolbar contains Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Sequencer, Options, and Alerts. Below the toolbar, there are tabs for Intercept, HTTP history, WebSockets history, and Options. A filter is set to 'HTTP history: CSS, image and general binary content'. The main workspace is divided into two panes. The left pane shows a browser window with the URL 'https://accounts.google.com/ServiceLoginAuth#identifier'. The page content includes the Google logo, the text 'Veillez saisir à nouveau votre mot de passe', a profile picture of Alfred de GéoPons, his name, email 'alfred@geoponts.erpc.org', a password field, a 'Connexion' button, and a 'Besoin d'aide ?' link. The right pane shows a table of intercepted requests:

Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
1	GET	http://www.google.com			302	456	HTML		
					302	230			302 Moved
					301	434			
					302	434			
					200	26305	HTML		Welcome Comput
					302	488	HTML		302 Moved
					302	230			302 Moved
					302	434			
					302	434			
					200	26305	HTML		Welcome Comput
					302	488	HTML		302 Moved
					302	488	HTML		302 Moved
					302	574	HTML		302 Moved
					302	126	HTML		302 Moved



Authentification avec le token U2F

The screenshot shows the Burp Suite Free Edition v1.6.01 interface. The top menu bar includes Applications, Places, and Start Burp. The main toolbar contains Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Options, and Alerts. Below the toolbar is the Intercept tab, with sub-tabs for HTTP history, WebSockets history, and Options. A filter is set to 'HTTP history, image and general binary content'. The main window displays a list of intercepted requests. The first request is a GET request to 'http://www.google.com'. The response is a 302 Moved status. The log table is as follows:

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
1	http://www.google.com	GET	/			302	488	HTML		302 Moved
						302	290			
						301	474			
						301	474			
						200	26305	HTML		Welcome Comput
						302	488	HTML		302 Moved
						302	230			
						301	474			
						301	474			
						200	26306	HTML		Welcome Comput
						302	480	HTML		302 Moved
						302	480	HTML		302 Moved
						302	576	HTML		302 Moved
						301	100			

The browser window shows the Google sign-in page with the heading 'Validation en deux étapes' and the instruction 'Utiliser votre appareil pour vous connecter à votre compte Google'. Below this is a U2F security key icon and the text 'Insérez votre clé de sécurité.' followed by instructions on how to use the security key. A checkbox at the bottom is checked and labeled 'Ne plus me demander sur cet ordinateur'.



Authentification acceptée !? == MITM réussi !

The screenshot shows the Burp Suite interface at the top, with a table of intercepted requests. The table has columns for Name, Value, URL, Params, Status, Size, Length, Method, and Source. The first row shows a request to 'https://myaccount.google.com/?pli=1' with a status of 200 and size of 15425 bytes. Below the browser window, the text reads: 'Bienvenue, Alfred de GéoPonts' and 'Contrôlez, protégez et sécurisez votre compte, depuis un même endroit'. At the bottom, it says: 'Sur la page "Mon compte", accédez rapidement aux paramètres et aux outils dont vous avez besoin pour protéger



Accès aux messages U2F transmis dans TLS

Applications ▾ Places ▾ burp-StartBurp ▾ Wed 15:25 1

Burp Suite Free Edition v1.6.01

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
57	https://safebrowsing-cache.google...	GET	/safebrowsing/rd/chFnB29nLXBo...			200	1881			
58	https://safebrowsing-cache.google...	GET	/safebrowsing/rd/ChFnB29nLXBo...			200	485			
59	https://safebrowsing-cache.google...	GET	/safebrowsing/rd/ChFnB29nLXVu...			200	268			
60	https://clients4.google.com	GET	/chrome-variations/seed?osnam...			200	34962	HTML		Comptes Google
61	https://accounts.google.com	GET	/signin/challenge/sk/1045?check...			304	225			
62	https://ssl.gstatic.com	GET	/accounts/static/_fjs/k=gaia.gai...			304	225			
63	https://ssl.gstatic.com	GET	/accounts/static/_fjs/k=gaia.gai...			304	225			
67	https://fonts.gstatic.com	GET	/s/opensans/v13/DX1LORHCpsQ...			304	226			
68	https://fonts.gstatic.com	GET	/s/opensans/v13/cjZKeOuBrn4kE...			304	226			
69	https://ssl.gstatic.com	GET	/accounts/static/_fjs/k=gaia.gai...			304	225			
70	https://accounts.google.com	POST	/signin/challenge/sk/1045			302	1209	HTML		Moved Temporarily
71	https://accounts.google.com	GET	/FinishSignIn?checkedDomains=...			302	3927	HTML		Moved Temporarily
72	https://accounts.google.com	GET	/CheckCookie?checkedDomains=...			200	8041	HTML		Comptes Google
73	https://accounts.youtube.com	GET	/accounts/SetSID?ssid=1&sidt=...			200	4047	HTML		

Request Response

Raw Params Headers Hex

POST request to /signin/challenge/sk/1045

Type	Name	Value
Cookie	GALX	AL8_gfrfC4o
Cookie	GAPS	1:D5y_X_LGgjl/Qgea8l1NDB4vPuqRA:BTddv35tj2z409li
Cookie	TC	AHnYQLz_dOIRve9wgDMFZL4vszvkvic-vjDm2sAxbqEcKLxAmhg5PxSPatRwBxYU7A8Usrp3g-yU_G9g_ITG2Eji-YMOjp33kffPBYIs1gLO5LwjcZTIZ...
Body	challengeId	1045
Body	challengeType	2
Body	checkedDomains	youtube
Body	checkConnection	youtube: 253:1
Body	pstMsg	1
Body	gxf	AFoagUV09f65ErsBYvcuuYjB-EU6iqZAg:145511773060
Body	id-challenge	{ "appId": "https://www.gstatic.com/securitykey/origins.json", "challenges": [{ "challenge": "hNhX2oI9ccxHetpkzKQx7TbOWGndEcbzUESvOvsC9...
Body	id-assertion	{ "appId": "https://www.gstatic.com/securitykey/origins.json", "browserData": "eyJ0eXh0eXZpZ2F0b3l1aWwQuZ2V0QXNzXj0aW91ulwiy2hhb...
Body	TrustDevice	on



Contact avec Google :

- ▶ la vérification de TLS Channel ID est désactivée
 - ▶ « support expérimental par Chrome »
 - ▶ « usage incompatible avec les proxy-cache interceptants »
- ▶ vérification de l'efficacité effectuée avec un compte de test

Résultat net :

- ▶ TLS Channel ID n'est pas implémenté ou vérifié

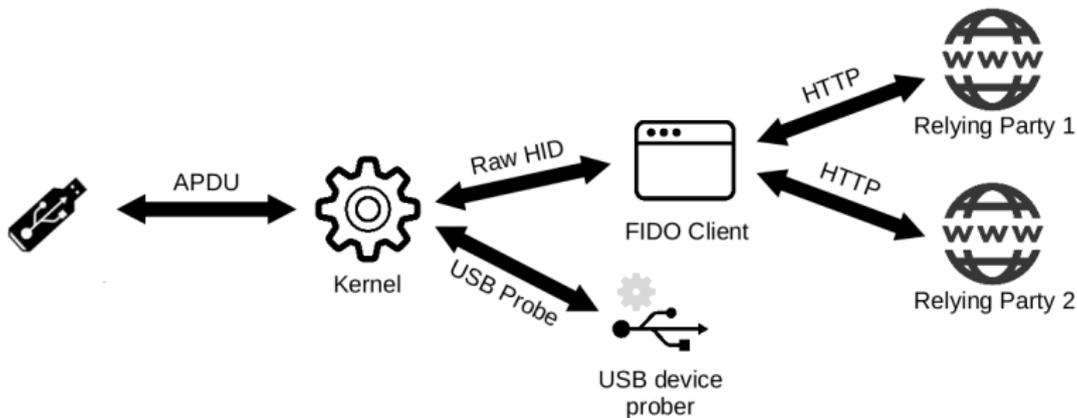
Autre limitation d'U2F :
le cas de la confirmation
de transaction



Limite d'U2F assumée par les spécifications

Pas de confirmation de transaction

- ▶ pas de propriété WYSIWYS*



* : WYSIWYS : *What You See Is What You Sign*



Limite d'U2F assumée par les spécifications

Pas de confirmation de transaction

- ▶ pas de propriété WYSIWYS*

Contrairement à SMS et TOTP, pas de saisie utilisateur dans un champ affiché à l'écran :

- ▶ incertitude de ce que l'on confirmerait

Usage impossible, par exemple, pour valider une transaction bancaire (3DSecure)

* : WYSIWYS : *What You See Is What You Sign*

Comparatif avec l'authentification TLS du client par certificat



Parmi les objectifs premiers d'U2F :

- ▶ être *plug 'n play*, sans pilote (RawHID)

Authentification par certificat :

- ▶ navigateurs coupables d'interfaces utilisateur kafkaesques
- ▶ utilisation simplifiable avec la complicité d'un service informatique



U2F :

- ▶ en théorie, résistant grâce à TLS Channel ID*
- ▶ en pratique, pas de déploiement

Authentification par certificat :

- ▶ résistant*

* : L'attaque [SLOTH](#) (et autres attaques par collision de transcript) peut affecter U2F et l'authentification par certificat client



U2F :

- ▶ utilisation de formulaires web
- ▶ interaction avec l'application sans authentification
- ▶ vol de session potentiel par XSS

Authentification par certificat :

- ▶ sans certificat valide, impossible de voir/communiquer avec l'application



U2F :

- ▶ jeune (peu d'implémentations, peu de déploiements)
- ▶ cette étude est la première qui soit indépendante

Authentification par certificat :

- ▶ spécifié en 1995
- ▶ [3SHAKE](#), [SLOTH](#), [MS09-007](#)...

Conclusions sur le protocole U2F



Conclusion

U2F :

- ▶ second facteur semblant satisfaisant pour le grand public
- ▶ facilité d'utilisation
- ▶ pas de confirmation de transaction : n'est pas un remplacement universel du SMS/TOTP
- ▶ nécessite des études supplémentaires :
 - ▶ pas d'étude des implémentations
 - ▶ pas d'étude de la fonctionnalité *facets*

Authentification par certificat :

- ▶ pas encore remplacé pour les applications sensibles

Q & A

Merci pour votre attention

Florian Maury

ANSSI

Mickaël Bergem

ParisTech