Please Remember Me: Security Analysis of U2F Remember Me Implementations in The Wild

Gwendal Patat
Mohamed Sabt

5 juin 2020

Contexte

Mot de passe comme système d'authentification

Mot de passe:

- De loin la méthode d'authentification la plus répandue
- La majorité des utilisateurs utilise un seul même mot de passe[1]
- Peut être aisément volé/craqué (ex. hameçonnage, force brute, rainbow table, etc...)

[1] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. "i added '!' at the end to make it secure": Observing password creation in the lab. In SOUPS, pages 123–140. USENIX Association, 2015.

2FA: Two-Factor Authentication

(a) SMS OTP

(b) Application OTP

(c) Jeton OTP

Figure: Quelques de solutions 2FA

FIDO Alliance

FIDO Alliance:

Crée par Google et Yubico, FIDO Alliance a pour but de standardiser un protocole 2FA plus résistant: **Universal 2nd Factor** (U2F).

Definitions

Jargon FIDO

- **Authenticateur FIDO:** L'authenticateur, dispositif utilisateur, pouvant être logiciel ou matériel.
- **Client FIDO:** L'entité logiciel traitant les messages du protocole FIDO sur l'appareil (ex. navigateur internet).
- **Relying Party (RP):** Un site internet ou autre entité utilisant le protocole FIDO pour authentifier les utilisateurs.

Protocole Universal 2nd Factor

Protocole U2F: Consentement Utilisateur

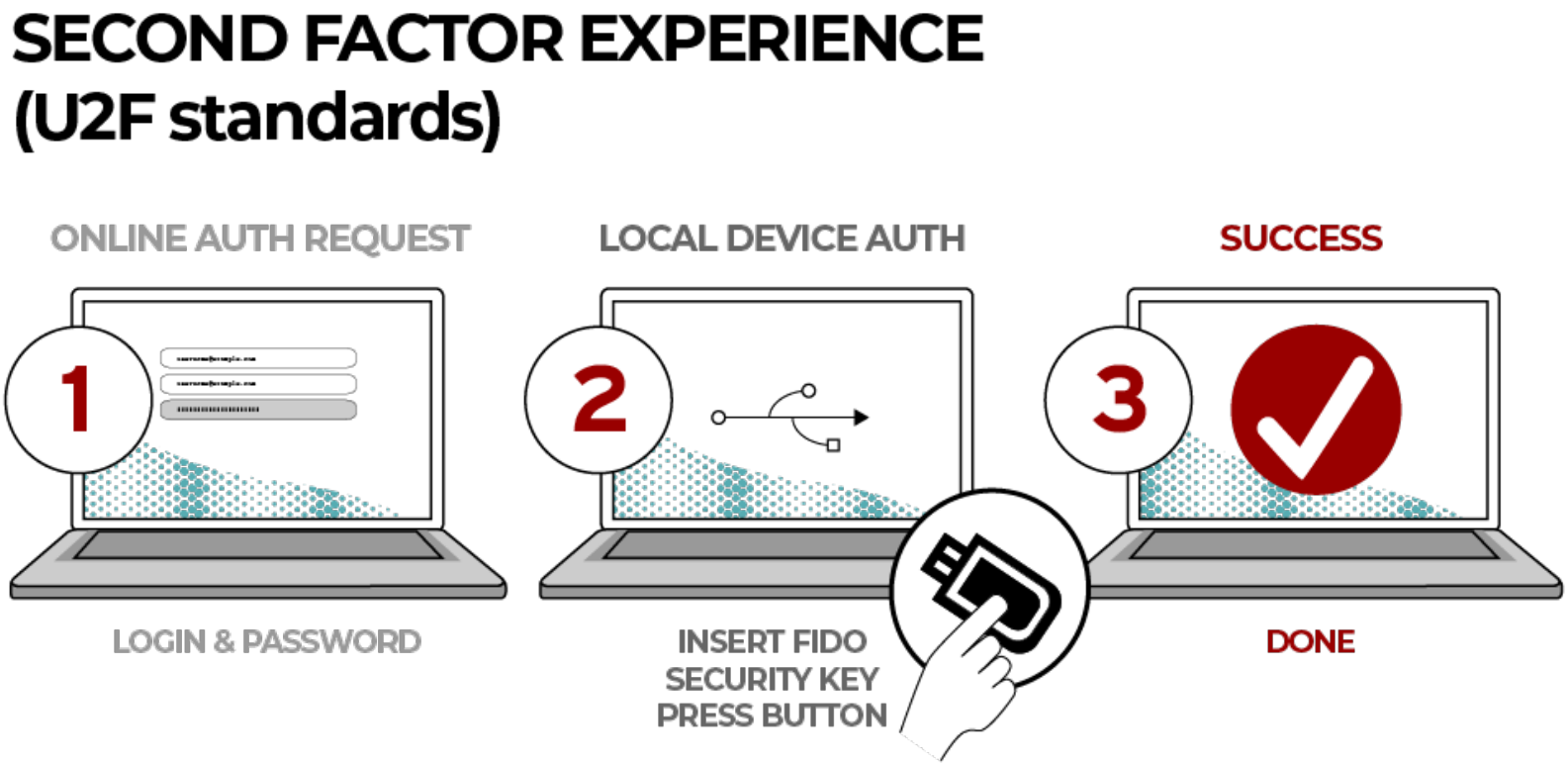


Figure: U2F utilisant un authenticateur FIDO physique[2]

[2] src: https://fidoalliance.org/specifications/

Authenticateur FIDO

Authenticateur FIDO

Figure: Exemples d'authenticateur FIDO

U2F: Enregistrement

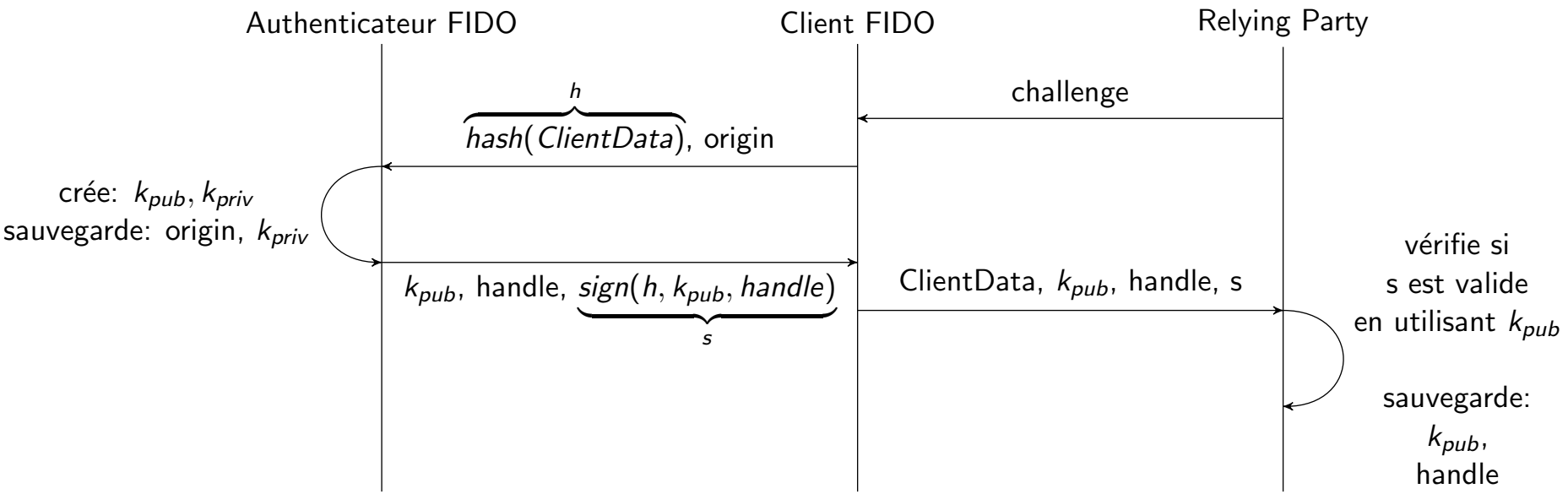


Figure: FIDO U2F Enregistrement

U2F: Authentification

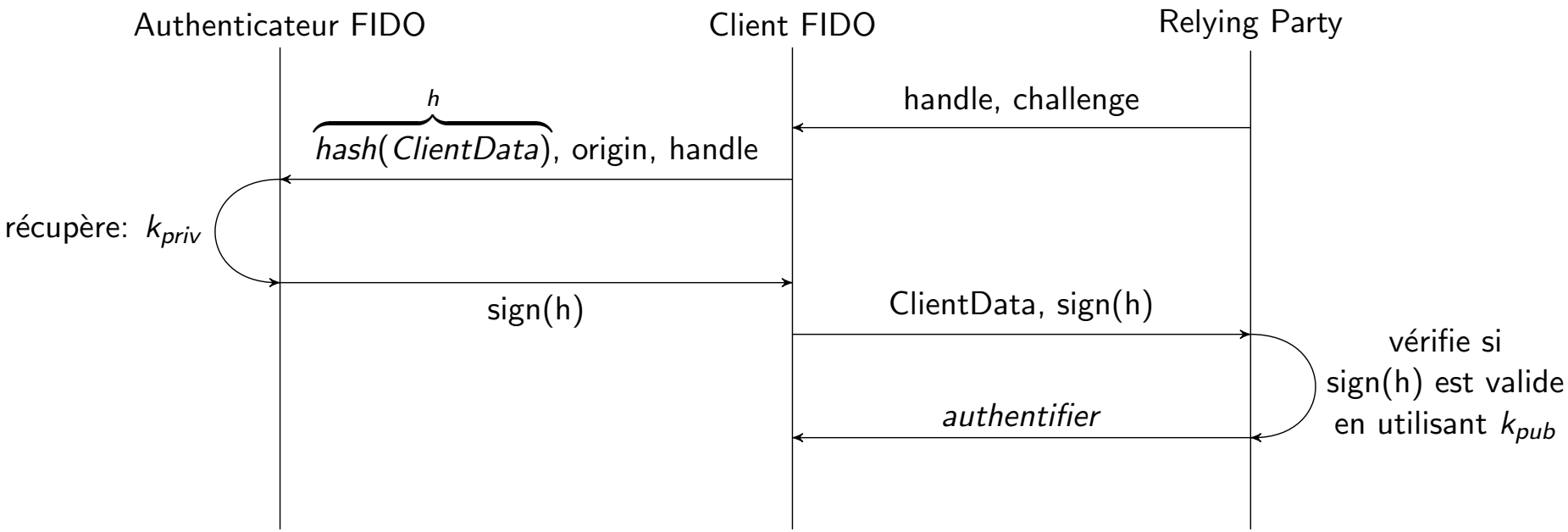


Figure: FIDO U2F Authentication

U2F: Analyses de Sécurité (1)

Analyse de Sécurité Initiale:

Pereira et al.[3] ont utilisé pi-calcul et ProVerif afin de vérifier le protocole.

Analyse Complémentaire:

Jacomme et Kremer[4] ont continué l'analyse précédente en prenant en compte les communication via TLS et les logiciels malveillants.

[3] Olivier Pereira, Florentin Rochet, and Cyrille Wiedling. Formal analysis of the FIDO 1.x protocol. In FPS, volume 10723 of Lecture Notes in Computer Science, pages 68–82. Springer, 2017.

[4] Charlie Jacomme and Steve Kremer. An extensive formal analysis of multi-factor authentication protocols. In CSF, pages 1–15. IEEE Computer Society, 2018.

U2F: Analyses de Sécurité (1)

Analyse de Sécurité Initiale:

Pereira et al.[3] ont utilisé pi-calcul et ProVerif afin de vérifier le protocole.

Analyse Complémentaire:

Jacomme et Kremer[4] ont continué l'analyse précédente en prenant en compte les communication via TLS et les logiciels malveillants.

Le protocole U2F est prouvé *sécurisé de manière formelle*.

[3] Olivier Pereira, Florentin Rochet, and Cyrille Wiedling. Formal analysis of the FIDO 1.x protocol. In FPS, volume 10723 of Lecture Notes in Computer Science, pages 68–82. Springer, 2017.

[4] Charlie Jacomme and Steve Kremer. An extensive formal analysis of multi-factor authentication protocols. In CSF, pages 1–15. IEEE Computer Society, 2018.

Security Benefits (Propriétés)(1)

Originalement définie par Bonneau et al.[5] pour classer la sécurité des solutions 2FA, nous avons adapté leurs "*Security Benefits*" à U2F:

[5] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In IEEE Symposium on Security and Privacy, pages 553–567. IEEE Computer Society, 2012.

Security Benefits (Propriétés)(1)

Originalement définie par Bonneau et al.[5] pour classer la sécurité des solutions 2FA, nous avons adapté leurs "*Security Benefits*" à U2F:

- **Resilient-to-Physical-Observation:** Résistant aux shoulder surfing, accès physiques au dispositif utilisateur etc...

[5] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In IEEE Symposium on Security and Privacy, pages 553–567. IEEE Computer Society, 2012.

Security Benefits (Propriétés)(1)

Originalement définie par Bonneau et al.[5] pour classer la sécurité des solutions 2FA, nous avons adapté leurs "*Security Benefits*" à U2F:

- **Resilient-to-Physical-Observation:** Résistant aux shoulder surfing, accès physiques au dispositif utilisateur etc...
- **Resilient-to-Input-Observation:** Résistant aux keyloggers, accès au système de fichier du navigateur etc...

[5] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In IEEE Symposium on Security and Privacy, pages 553–567. IEEE Computer Society, 2012.

Security Benefits (Propriétés)(1)

Originalement définie par Bonneau et al.[5] pour classer la sécurité des solutions 2FA, nous avons adapté leurs "*Security Benefits*" à U2F:

- **Resilient-to-Physical-Observation:** Résistant aux shoulder surfing, accès physiques au dispositif utilisateur etc...
- **Resilient-to-Input-Observation:** Résistant aux keyloggers, accès au système de fichier du navigateur etc...
- **Resilient-to-Communication-Observation:** L'écoute des communications n'offre pas d'avantage à l'attaquant.

[5] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In IEEE Symposium on Security and Privacy, pages 553–567. IEEE Computer Society, 2012.

Security Benefits (Propriétés)(2)

- **Resilient-to-Leaks:** Compromettre une RP ne facilite pas l'usurpation d'identité sur cette même RP.

Security Benefits (Propriétés)(2)

- **Resilient-to-Leaks:** Compromettre une RP ne facilite pas l'usurpation d'identité sur cette même RP.
- **Resillient-to-Phishing:** Usurper l'identité d'une RP ne permet pas de s'identifier sur la vraie RP.

Security Benefits (Propriétés)(2)

- **Resilient-to-Leaks:** Compromettre une RP ne facilite pas l'usurpation d'identité sur cette même RP.
- **Resillient-to-Phishing:** Usurper l'identité d'une RP ne permet pas de s'identifier sur la vraie RP.
- **Resillient-to-Theft:** Voler l'authenticateur FIDO n'est pas suffisant pour l'utiliser.

Security Benefits (Propriétés)(2)

- **Resilient-to-Leaks:** Compromettre une RP ne facilite pas l'usurpation d'identité sur cette même RP.
- **Resillient-to-Phishing:** Usurper l'identité d'une RP ne permet pas de s'identifier sur la vraie RP.
- **Resillient-to-Theft:** Voler l'authenticateur FIDO n'est pas suffisant pour l'utiliser.
- **Long-Term-Resillient-to-Theft:** Un authenticateur peut être révoqué.

Modèle de Menace

Modèles d'Attaquants:

Modèle de Menace

Modèles d'Attaquants:

Physical Proximity Attacker [PP]: peut avoir un accès physique aux possessions de l'utilisateur, y compris son authentificateur FIDO.

Modèle de Menace

Modèles d'Attaquants:

Physical Proximity Attacker [PP]: peut avoir un accès physique aux possessions de l'utilisateur, y compris son authentificateur FIDO.

Man-in-the-Browser [MitB]: peut compromettre le client FIDO.

Modèle de Menace

Modèles d'Attaquants:

Physical Proximity Attacker [PP]: peut avoir un accès physique aux possessions de l'utilisateur, y compris son authentificateur FIDO.

Man-in-the-Browser [MitB]: peut compromettre le client FIDO.

Man-In-The-Middle [MitM]: peut s'immiscer dans la communication sécurisée entre le client FIDO et la RP.

Modèle de Menace

Modèles d'Attaquants:

Physical Proximity Attacker [PP]: peut avoir un accès physique aux possessions de l'utilisateur, y compris son authentificateur FIDO.

Man-in-the-Browser [MitB]: peut compromettre le client FIDO.

Man-In-The-Middle [MitM]: peut s'immiscer dans la communication sécurisée entre le client FIDO et la RP.

Intruder: peut compromettre la RP, lui permettant de lire, écrire et executer du code arbitraire dans le contexte d'authentification de la RP.

U2F: Analyses de Sécurité (2)

	Security Benefits								
	Resilient-to-Physical-Observation	Resilient-to-Input-Observation	Resilient-to-Communication-Observation	Resilient-to-Leaks	Resilient-to-Leaks-from-Other-Verifiers	Resilient-to-Phishing	Resilient-to-Theft	Long-Term-Resilient-to-Theft	Unlinkable
YubiKey	✓	✓	✓	✓	✓	✓	✗	✓	✓

✗ does not satisfy our definition of "Security Benefit";
✓ implements the "Security Benefit".

L'option U2F Remember Me

Option Remember Me

U2F Remember Me:

- Evite le besoin d'utiliser l'authenticateur FIDO sur les appareils mémorisées.
- Améliore l'utilisabilité[6]
- Originalement crée pour le protocole 2FA

Développé par les Relying Parties elles-mêmes, mais une fonctionnalité **non documenté ni standardisé**.

[6] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Faith Cranor, and Nicolas Christin. "it's not actually that horrible": Exploring adoption of two-factor authentication at a university. In CHI, page 456. ACM, 2018.

Nos Contributions

Nos Contributions:

- Introduction d'un modèle général de menace pour les implémentations U2F.
- Analyse de *toutes* les implementations "remember me"[7].
- Pour chaque implementation, nous avons identifié des attaques et faiblesses ne respectant pas notre modèle de sécurité.
- Définition de scenarii dans lesquels un attaquant peut *contourner avec succès* le protocole U2F sur des appareils jamais mémorisées.

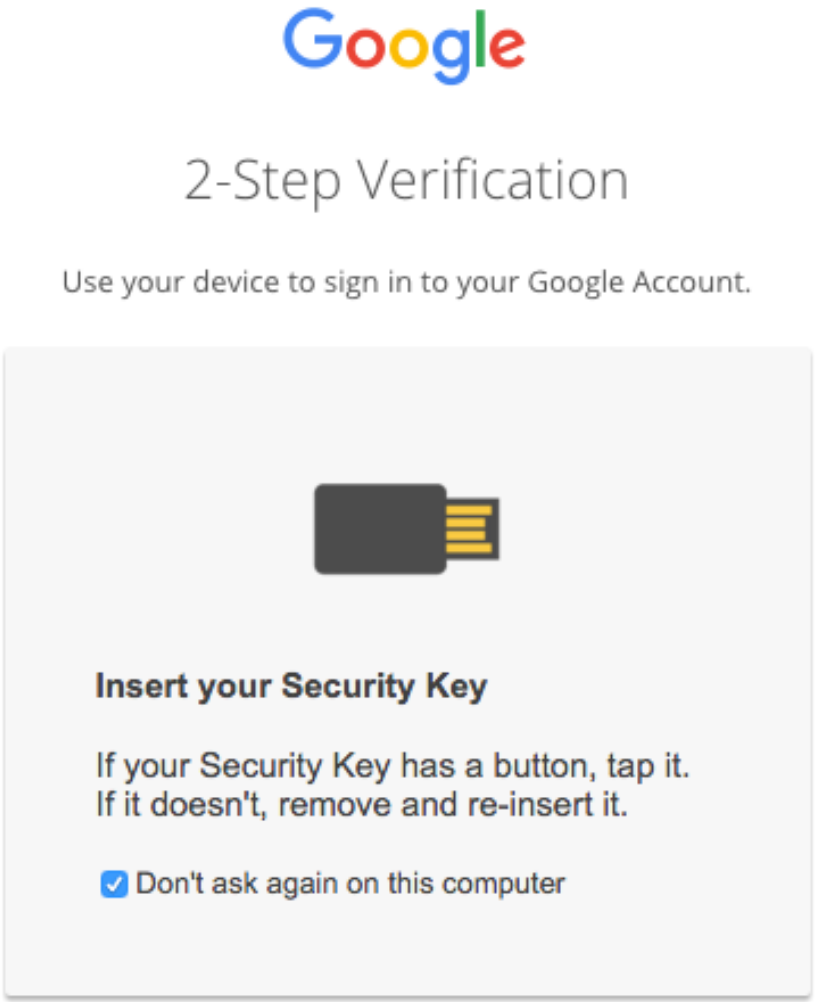
[7] sur un total de 67 fournisseurs de service proposant U2F `https://www.yubico.com/works-with-yubikey/catalog`

Relying Parties

Le choix des Relying Parties: Cookies

Toutes les RPs utilisent des **cookies** comme méchanisme pour l'option U2F remember me!

Google Implementation (1)



Google Implementation (2)

Google Remember Me Cookie:

Name	**Value**[8]
SMSV	*ADHTe*-AhcjLI49...
Domain	**Flags**
.account.google.com	secure, httpOnly
SameSite	
Lax	

Avec une durée de vie de deux ans à partir de la création.

[8] Ici, les valeurs proviennent de véritables cookies récupérés lors de nos recherches.

Google Implementation (3)

Méthodes de Révocation:

Google Implementation (3)

Méthodes de Révocation:

- ✓ Changer l'authenticateur FIDO

Google Implementation (3)

Méthodes de Révocation:

- ✓ Changer l'authenticateur FIDO
- ✗ Changer le mot de passe

Google Implementation (3)

Méthodes de Révocation:

- ✓ Changer l'authenticateur FIDO
- ✗ Changer le mot de passe
- ✗ Utiliser le Google Dashboard

Facebook Implementation (1)

Facebook Remember Me Cookies:

Deux cookies **indépendant**.

Name	**Value**[9]
datr	d5iiXlrd2v4vJ2wKYPwOdZWi
sb	iZiiXqdqYfgcxzLlwkP-_XJI

Attributs en communs:

Domain	**Flags**
.facebook.com	secure, httpOnly

SameSite

None

Durée de vie de deux ans après la création.

[9] Ici, les valeurs proviennent de véritables cookies récupérés lors de nos recherches.

Facebook Implementation (2)

Méthodes de Révocation:

Facebook Implementation (2)

Méthodes de Révocation:

Aucune

RPs Remember Me Recap

Relying Parties	Evaluation Criteria			
	Ephemerality	Effectiv-of-Revocation(1)	Effectiv-of-Revocation(2)	SameSite
Google	✗	✓	✗	None
Dropbox	✗	✗	✓	None
Facebook	✗	✗	✗	None
FastMail	✗	✗	✗	None
login.gov	✓	✓	✗	Lax

✗ does not satisfy the associated definition;
✓ satisfy the associated definition;

Depuis nos premières analyses, l'attribut *SameSite* de Google est devenu `Lax` au lieu de `None`

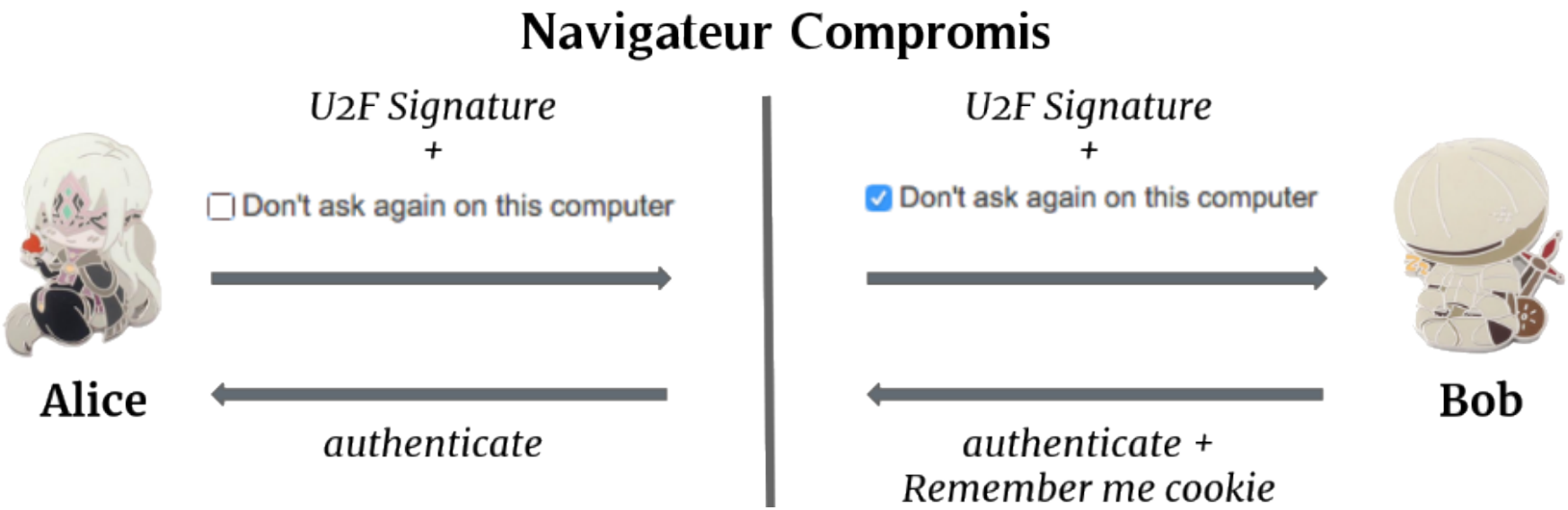
Analyse de Sécurité Revisitée

U2F: Analyse de Sécurité avec Remember Me activée

	Security Benefits								
	Resilient-to-Physical-Observation	Resilient-to-Input-Observation	Resilient-to-Communication-Observation	Resilient-to-Leaks	Resilient-to-Leaks-from-Other-Verifiers	Resilient-to-Phishing	Resilient-to-Theft	Long-Term-Resilient-to-Theft	Unlinkable
YubiKey	✓	✓	✓	✓	✓	✓	✗	✓	✓
Cookie	✗	✗	✗	✗	✓	✗	✗	✗	✓

✗ does not satisfy our definition of "Security Benefit";
✓ implements the "Security Benefit".

Exemple de scénario d'attaque: Plugin Malicieux



Contre-mesures Possibles

La sécurité initialement proposée par FIDO permet de résister à de puissants attaquants (ex. MitM, Intruder...) grâce à l'aspect **challenge-réponse** du protocole.

Contre-mesures Possibles

La sécurité initialement proposée par FIDO permet de résister à de puissants attaquants (ex. MitM, Intruder...) grâce à l'aspect **challenge-réponse** du protocole.

Néanmoins, les solutions remember me basées sur des cookies l'**affaiblissent**.

Contre-mesures Possibles

La sécurité initialement proposée par FIDO permet de résister à de puissants attaquants (ex. MitM, Intruder...) grâce à l'aspect **challenge-réponse** du protocole.

Néanmoins, les solutions remember me basées sur des cookies l'**affaiblissent**.

Contre-mesures:

- Remplacer les cookies par un authenticateur FIDO logiciel.
- Utiliser l'attribut `isFreshUserVerificationRequired` de l'authenticateur logiciel afin de **désactiver le besoin du consentement utilisateur**.

Conclusion

Recap

- Nous avons analysé toutes les implementations de l'option remember me du protocole U2F.
- Nous avons adapté et appliqué le modèle de Bonneau et al. ainsi que le modèle de menace de FIDO à cette fonctionnalité afin de juger sa sécurité.
- Nous avons montré que l'actuel implémentations de cette option affaiblisait grandement la sécurité initialement proposée par le protocole U2F en montrant la faisabilité de scénarii d'attaque classique.
- Nous avons proposé des contre-mesures afin de réduire les vecteurs d'attaques.

Merci pour votre attention