Ma femme, ma Google Home et moi

Piotr Chmielnicki
Twitter / Medium / LinkedIn : @piotrcki

L’assistant Google

Mode non authentifié

- recherches
- météo
- ect.

Voice Match

- “authentification” vocale
- interaction avec les appareils du propriétaire
- interactions avec le compte Google
- **accès à des données protégées**

Exemple de commande authentifiée

“Ok Google, qu’est ce qu’il y a dans mon agenda le 3 mai ?”

À venir :

- ❏ accès à GMail (disponible en anglais !) ;
- ❏ appels audio ou vidéos ;
- ❏ et bien plus encore.

Attaque par rejeu

- Une requête enregistrée peut-être rejouée.
- C’est facile à faire dans un cadre familial.
- Contre mesures possibles ?

(C’est pas le sujet de la Rump.)

Retour sur l’exemple

“*Ok Google, qu’est ce qu’il y a dans mon agenda le 3 mai ?*”

Retour sur l’exemple

“Ok Google, qu’est ce qu’il y a dans mon agenda le 3 mai ?”

“authentifié”

pas “authentifié”

~~Démo~~

- Fallait venir à BeeRumP.

Conséquences

- N’importe quelle requête peut être forgée à partir de n’importe quelle autre requête.
- C’est (encore plus) facile à faire dans un cadre familial.
- “Ok Google” : **un mot de passe qu’on doit prononcer à voix haute et qu’on ne peut pas changer**.

Google a été prévenu

- “*We think the issue might not be severe enough for us to track it as a security bug.*”
- Numéro du ticket : 126093867.

Questions

Piotr Chmielnicki
Twitter / Medium / LinkedIn : @piotrcki