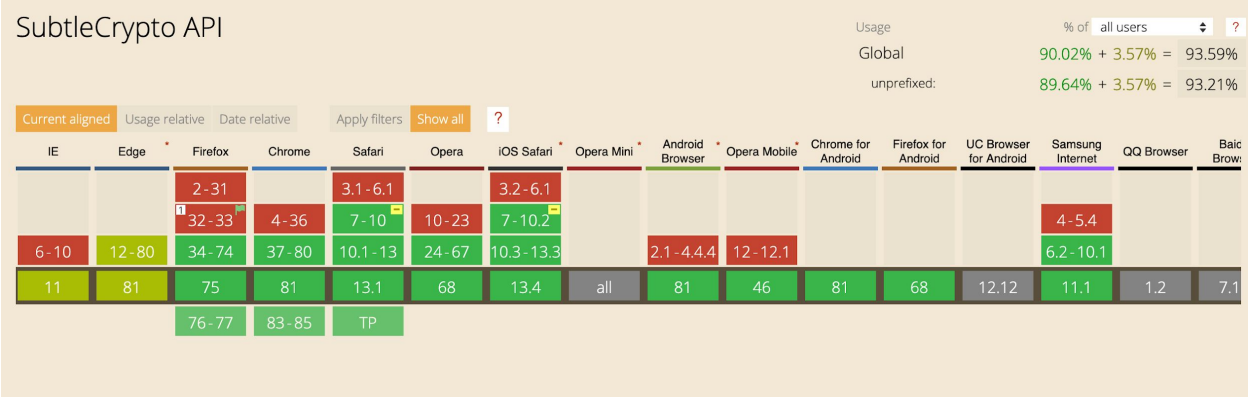
La Crypto API des navigateurs
simple, efficace

Meetup OWASP Paris

Fabien Leite, mai 2020

La crypto API ?

- L'API crypto (normée) des navigateurs
- Disponible (basique) pour tous les navigateurs modernes (2015 +)



https://caniuse.com/#search=SubtleCrypto

Pourquoi de la crypto côté client ?

1. Pour faire du zero knowledge
2. Parce que les hashs sont des outils utiles en dehors d'un contexte sécurité
3. Parce que la crypto API n'est pas codée en JavaScript 😜

En pratique

- Une API composée de primitives bas niveau (comme en Java, Python)
- Une API qui va donc retourner la réelle nature des éléments manipulés
- Une API à ne pas mettre entre toutes les mains donc

- Peu d'algorithmes (c'est une bonne nouvelle)
- Utilisable uniquement dans un contexte HTTPS *

* Mais ne pas être en HTTPS en 2020 n'est plus acceptable

Analyse d'une fonction de hash

```
export async function hasherSha512(texte) {
  const encoder = new TextEncoder();
  const texteAsUnicode = encoder.encode(texte);
  const hashBinaire = await crypto.subtle.digest("SHA-512", texteAsUnicode);
  return transformerEnBase64(hashBinaire);
}
```

Analyse d'une fonction de hash

```
export async function hasherSha512(texte) {
  const encoder = new TextEncoder();
  const texteAsUnicode = encoder.encode(texte);
  const hashBinaire = await crypto.subtle.digest("SHA-512", texteAsUnicode);
  return transformerEnBase64(hashBinaire);
}
```

Analyse d'une fonction de hash

```
export async function hasherSha512(texte) {
  const encoder = new TextEncoder();
  const texteAsUnicode = encoder.encode(texte);
  const hashBinaire = await crypto.subtle.digest("SHA-512", texteAsUnicode);
  return transformerEnBase64(hashBinaire);
}
```

Analyse d'une fonction de hash

```
export async function hasherSha512(texte) {
  const encoder = new TextEncoder();
  const texteAsUnicode = encoder.encode(texte);
  const hashBinaire = await crypto.subtle.digest("SHA-512", texteAsUnicode);
  return transformerEnBase64(hashBinaire);
}
```

Analyse d'une fonction de hash

```
export async function hasherSha512(texte) {
  const encoder = new TextEncoder();
  const texteAsUnicode = encoder.encode(texte);
  const hashBinaire = await crypto.subtle.digest("SHA-512", texteAsUnicode);
  return transformerEnBase64(hashBinaire);
}
```

Conclusion

- Une API crypto simple et bien faite
- Des primitives bas niveau → un besoin de comprendre la crypto pour l'utiliser

- Pas en JS, dormez sur vos deux oreilles

- Mauvaise compatibilité avec IE et les vieux Safari …
- … Mais la meilleure solution si vous n'en avez pas besoin