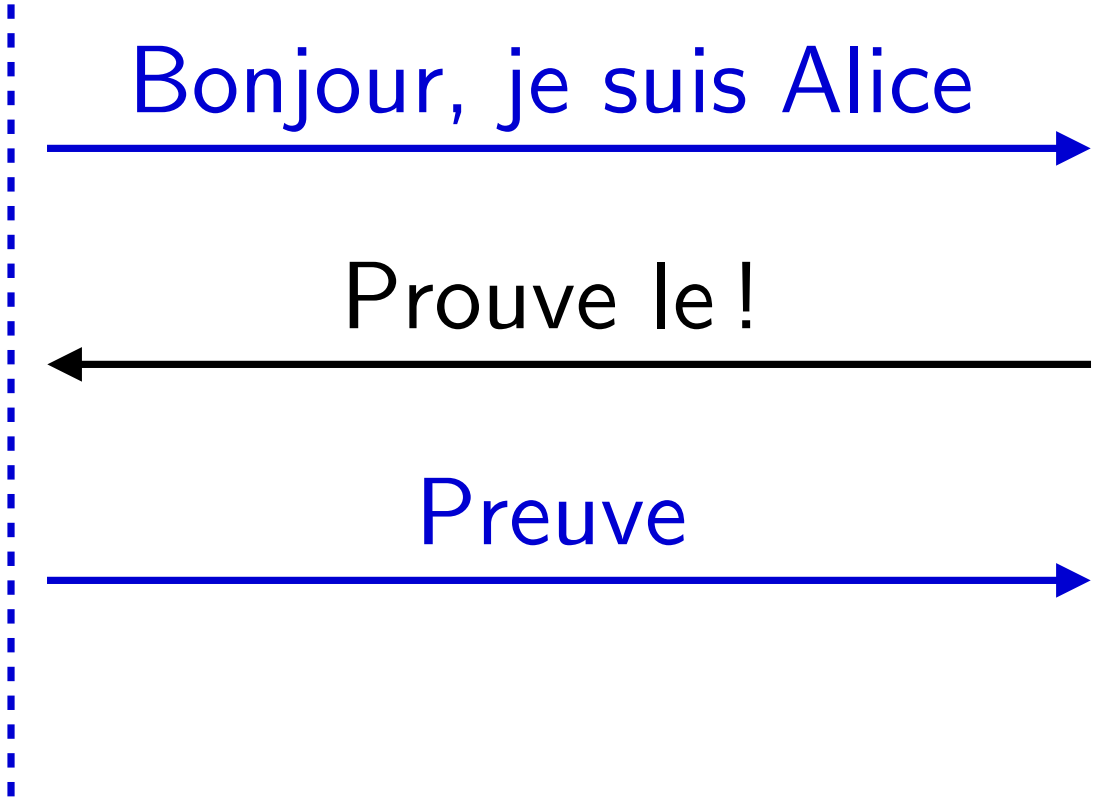
Les mots de passe

Cédric Lauradoux

Authentification



Authentification contre identification

- *Durant une identification, Charlie obtient le nom d'Alice.*
- *Durant une authentification, Charlie obtient une* ***preuve*** *sur l'identité d'Alice.*
- Nous allons voir comment les utilisateurs s'authentifie sur à des services sur Internet.

Attaques

- **Usurpation d'identité :** *Eve arrive à s'authentifier auprès de Charlie comme étant Alice.*
- **Vie privée :** *Eve arrive à suivre les faits et gestes d'Alice.*
- **Déni de service :** *Eve empêche Alice de s'authentifier auprès de Charlie.*

Mot de passe

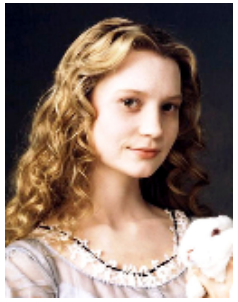
- **Vérification (à distance) :** *Alice ne veut pas divulguer son mot de passe et Charlie veut établir de façon certaine l'identité de son interlocuteur.*

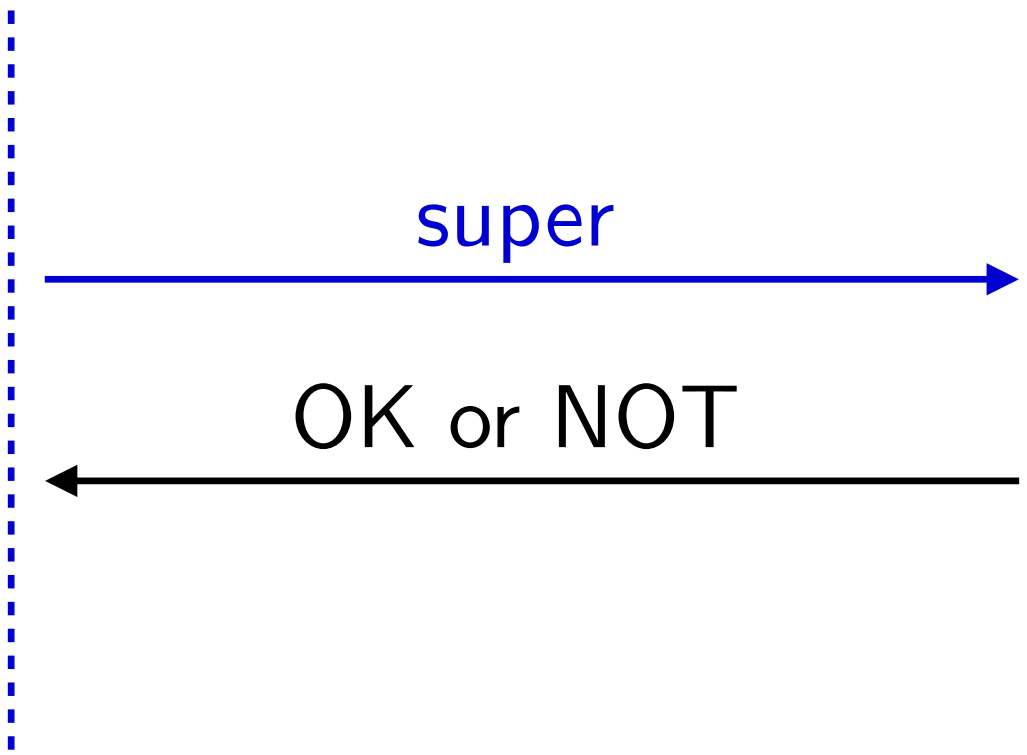
- **Stockage :** *Charlie stocke de façon sûre le mot de passe d'Alice.*

- **Mise à jour :** *Quand Alice oublie son mot de passe, elle veut pouvoir le réinitialiser.*

Protocole PAP

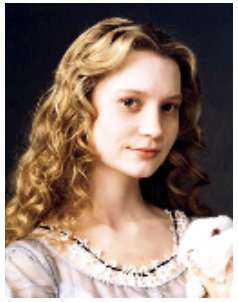
Password Authentication Protocol

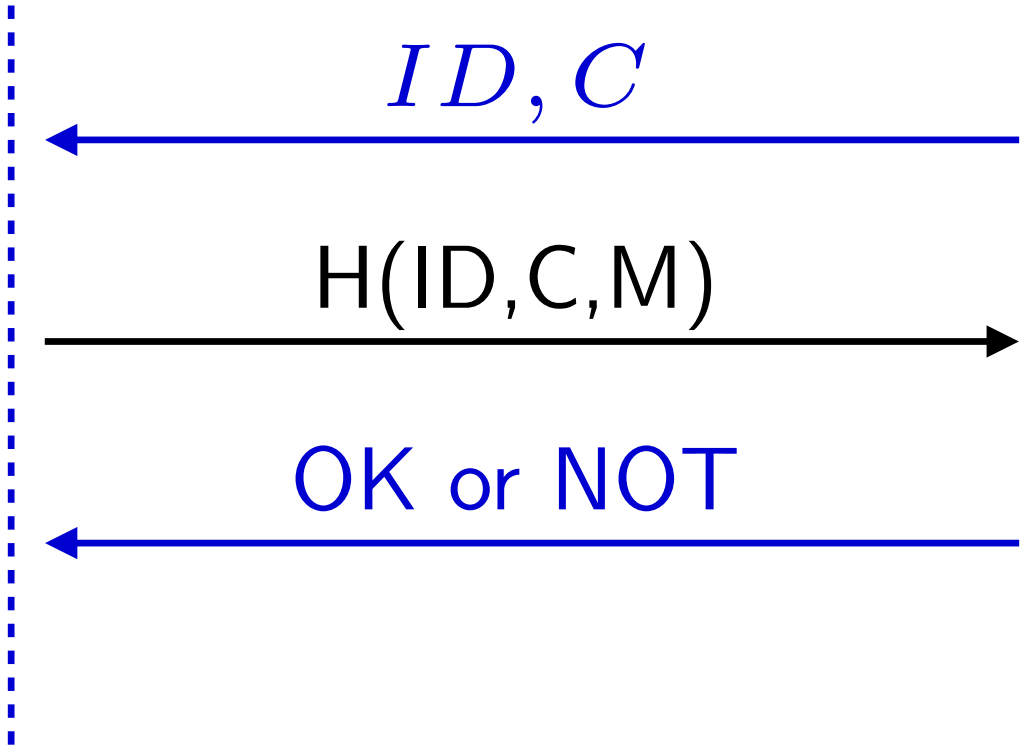




Protocole CHAP

Challenge-Handshake Authentication Protocol





Améliorer CHAP

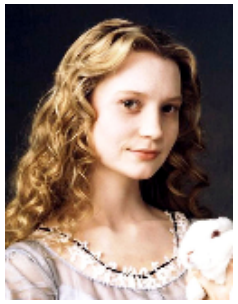
- Faut il qu'Alice et Bob partage le mot de passe ?
- CHAP est il respectueux de la vie privée ?
- Attention MS-CHAP une extension de Microsoft est totalement cassée.
- PAP est amélioré par CHAP.
  CHAP est amélioré par EAP.

Authentification HTTP

- S'authentifier auprès d'un serveur HTTP grâce à un nom d'utilisateur et un mot de passe valide.

- Il existe deux modes d'authentification :
  — Basic
  — Digest

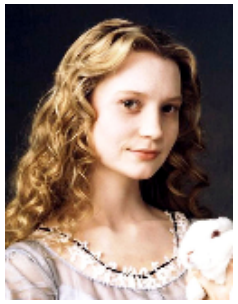
Basic

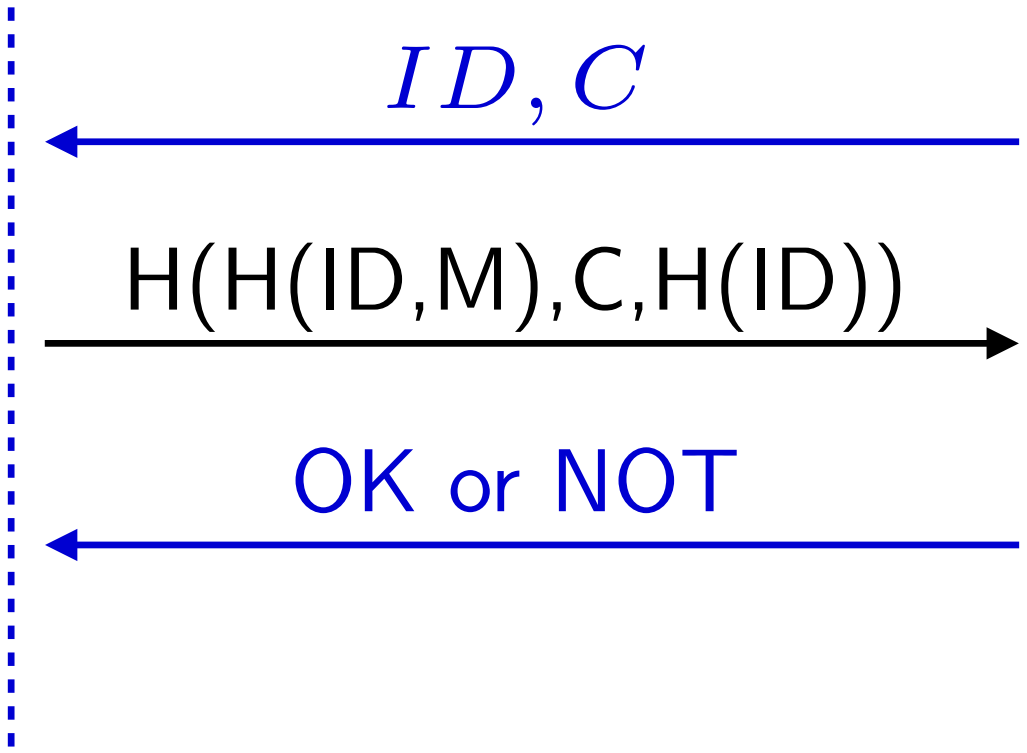


alice :super

OK or NOT

Digest





Comment attaquer ces protocoles ?

- A partir de l'interception d'une session, on essaye de faire une recherche exhaustive sur le mot de passe.

- Est difficile de faire une recherche exhaustive sur des mots de passe ?

Combinatoire

#	min.	min.+maj.	alphanum.	imprimable
3	10^4	10^5	10^5	10^6
4	10^5	10^6	10^7	10^7
5	10^7	10^8	10^9	10^{10}
6	10^8	10^{10}	10^{10}	10^{11}
7	10^9	10^{12}	10^{12}	10^{13}
8	10^{11}	10^{13}	10^{14}	10^{15}
14	10^{14}	10^{24}	10^{25}	10^{27}