Passwords

Thierry Sans

Two operations

- **Sign-up** : store user id and password
- **Sign-in** : verify user id and password

How to store and verify password?

- ~~Clear~~

Data can be hack/lost

- ~~Encrypted~~

A key is needed to store and verify passwords

- ~~Hash~~

Weak passwords have known hash

- Slated Hash

Salt and hash must be stored

Do/Don't with passwords

- On the client side, do <u>send passwords</u> in:
  - ✓ headers (automatic with basic authentication)
  - ✓ body (POST request with session authentication)
  - ◉ never in the URL
- On the server, do <u>store passwords</u> as
  - ✓ salted hash passwords only
  - ◉ never in clear