Users should be aware on how to construct **STRONGER PASSWORDS** which are more resistant to many attacks.

### Current Solutions

- Generating random passwords.
- Enforcing strong password policies.
- Using proactive password checker (meters).

### Our Contributions

- 1-D password meter to 2-D space.
- Supports multiple threats at the same time.
- Provides detailed information about all threats.
- Reconfigurable and extensible.
- Pure HTML5/CSS/JavaScript based solution.
- Fairly fast; work even on mobile devices.
- Uses NIST password guessing entropy estimator [1].
- Supports naive and rule-based dictionary attacks.
- Supports personalized dictionary attacks (e.g., Facebook).

### Design

**Targeted users:** normal end users.

We used the radar concept for reducing users' learning curve and showing different threats in a more structural & user-friendly way.

### 3. Implementation

- **Programming Languages:** HTML5, CSS and JavaScript.
- Because of the screen limitation, the prototype shows up to 3 edit distance.

### References