Phorce Field

Cookie: 12 images
Password: Sequence of those 12 images

- So you perform some condition safe ceremonies (like secure machine registration)
And the cookie that will be se through this process will be this set of 12 images.

- User must see images to login.
- User Must click on certain images in a certain order.
- So if you go to a phishing webpage it is most likely that the attacker won’t be able to get the 12 images to show to the user.

Phisher/Attacker’s options (not including malware being on victim’s machine):

- Search Interface (We’ve lost your password (blah blah blah) we need you to search through our \ database for your images) (if there’s enough images in the DB this most likely won’t work)

- Guess Images X (Way to many possibilities for this to be likely to work)

Passpoints - New and more secure graphical password system, based on clicking on spots in an image in a particular order rather than entering an alphanumeric password.

Attack Scenario should look as different as possible from non-attack scenario.

- Breaks click-whirr behavior (Click-Whirr = Reflexive clicking response)

OR make click-whirr behavior safe.

One of the reasons why Phorce Field was so successful was because you couldn’t ignore it. This is known as a “force function”.

- Use Forcing Functions

Secure Device Pairing Problem:

Device A
(Laptop)  Protocol  Device B
(Bluetooth Phone)

- If there is a Man in the Middle, everyone can participate in the key generation. So if there is a Man in the middle actively participating then the key on the Laptop won’t be the same one on the Phone. So this way the user can check if the codes are the same and if they’re not he can give input saying such to regenerate the code.
**Solutions and their Problems:**

- Show to user (scenario above)
  
  Problem: User Will Ignore

- Force user to make a choice (Display 3 keys and make sure the user picks the one from the other device)
  
  Problem: Probability of Success is limited to the number of keys (user could still accidently guess the key on other device)

- Sound
  
  - IR (infrared) requires line of sight
  
  - Vibration (put one phone up against the other, use pulse coded vibrations to represent one’s and zeros, sensors in the other phone pick up the key.)

- Bump (No good)