Deterring Shoulder Surfing with Inverting Images

March 21, 2007

CSE 227 – Winter 2007

Varun Almaula and Taurin Tan-atichat

Motivations

- Inspired by what Passfaces left out in paper:
  - Tari, Ozok and Holden, A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords", SOUPS 2006.
  - Passfaces successful against humans, but what about electronic equipment?
    - Cameras
    - Video recording
  - Proliferation of camera/video enabled cell phones makes Passfaces vulnerable
- Decouple the input method and the visual output for true effectiveness (hide one or both)

Idea

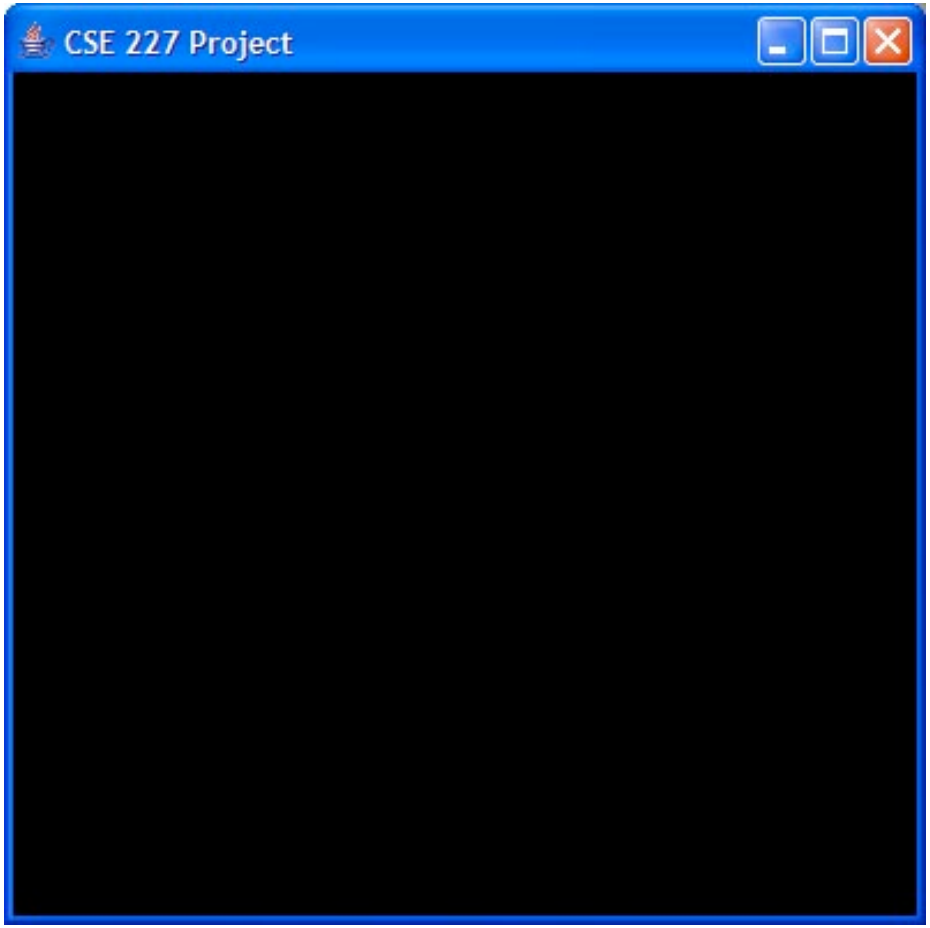
- How can we defeat these devices? Do we need special hardware?
- Cameras (especially cell phones) are slow to react to lighting changes
  - Change from a dark scene to a bright one requires changing of aperture, shutter speed, white balance, ISO, focus…
  - Human visual system can do this faster than cameras…let's exploit this!

System Description

- Create a fast lighting change when displaying the characters of a graphical password

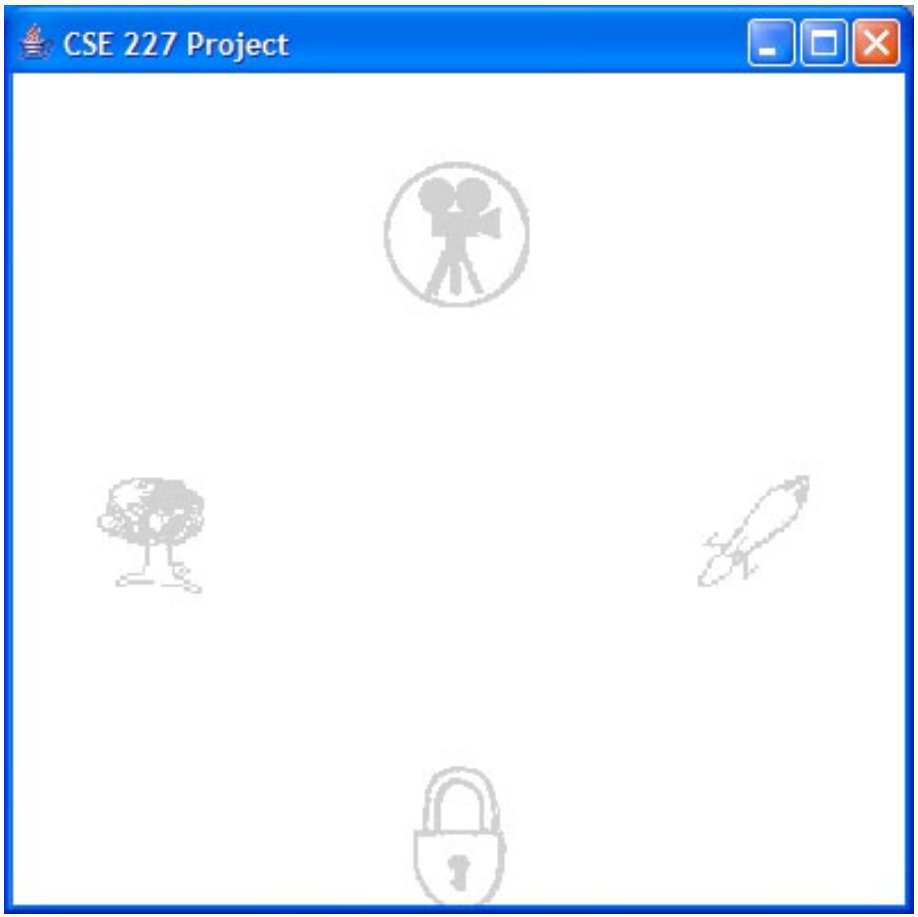
System Description

- Dark screen displayed for relatively long time (~ seconds)



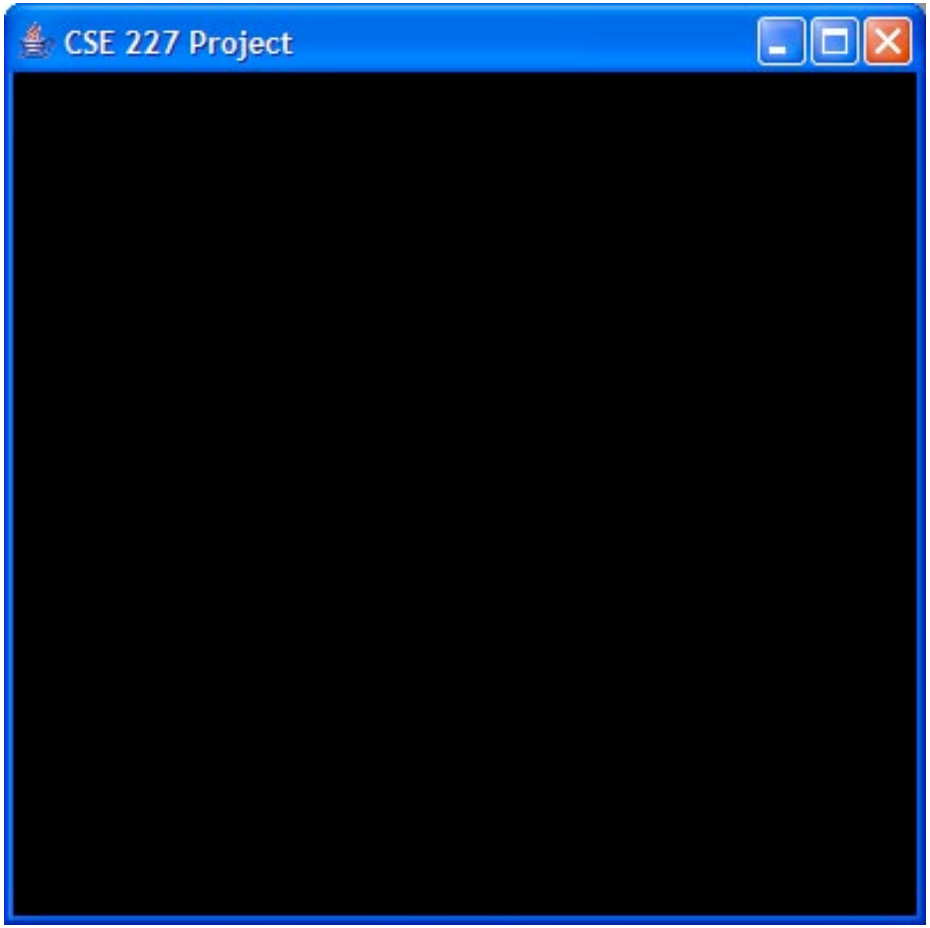
System Description

- After random interval, screen goes white and display low contrast icons for short time (~300ms)



System Description

- Screen goes back to black



System Description

- Repeat for length of graphical password
  - Used 3 character long password, with 2x2 icon display

Results

- Three 23 year old subjects (Computer Science, Mechanical Engineer, Management Science) as shoulder surfers and users
  - (640x480, 30fps) video camera
  - Used VirtualDub for frame by frame analysis of video
- Random icon display makes camera (picture taking) difficult
- When icons are statically displayed like Passfaces, 100% defeat rate for shoulder surfing with video camera
- 100% input accuracy (authenticated every time) using switching screen method
- On ‘easy’ UI setting 1/3 icon screens visible with frame analysis (but had to fill entire view with screen – need two cameras)
- On ‘hard’ UI setting, 0% defeat rate

Conclusions

- It is possible to deter video shoulder surfing with just software
  - Works well for video digital cameras, works very well for cell phone video cameras
- Usable for test group, but what about those with vision problems?
- Usability vs. deterrence capability tradeoff
- Technology will get better, but will it ever get as good as human visual system?
- Augment/improve system?
- Much more investigation needs to be done (usability, hardware, software)