Deterring Shoulder-Surfing At The Logon Terminal

UCSD Jacobs | Computer Science and Engineering

Varun Kartik Almaula Taurin Tan-atichat
Stefan Savage

Problem Statement

Identity Theft claimed $50 billion from 8.4 million Americans in 2006

- **Attacks to obtain passwords include: information harvesting, social engineering, direct observation (including shoulder-surfing), automated cracking software**
- **We focus on shoulder-surfing: looking/recording over a victim's 'shoulder' while inputting password**

Most widely used authentication mechanism is the traditional text/PIN password, which suffers from multiple vulnerabilities

- **Hard to remember complex random passwords, yet trivial to compromise simple passwords**
- **Passwords are inputted 'in the clear' with a keyboard and are easy to share (write down, observe, tell others)**
- **Increasing number of passwords to manage encourages users to 'cope' by using insecure methods to compensate for usability issues**

Graphical password mechanisms can improve upon these vulnerabilities

- **"Picture Superiority Effect" – humans can remember many images with better Long Term Memory (LTM) performance**
- **Easier to remember by relying on imprecise recognition (interpret meaning of picture) rather than precise recall (reproduce picture)**
- **Hard to write down or share a graphical password with others**
- **Potential for larger usable password space**

Potential for increased resiliency to above attack methods, except direct observation can still defeat many graphical password systems

Related Work

PassFaces

- **Use human faces as graphical password (humans are inherently adept at recognizing faces)**
- **Map 3 X 3 grid of images to the numeric keypad**
- **Decouple presentation of secret authentication information (faces) from pure input into system (using number pad instead of mouse clicks to make image selections obfuscates user input)**
- **Deters human shoulder-surfing, but still vulnerable to camera attack (video camera phones are now ubiquitous!)**

Camera Zapping

- **Detect cameras in vicinity and direct laser at camera's CCD**
- **Overwhelm CCD (exploit 'blooming' and 'lens flare' optics errors) to disrupt unwanted recording activities, but requires hardware**

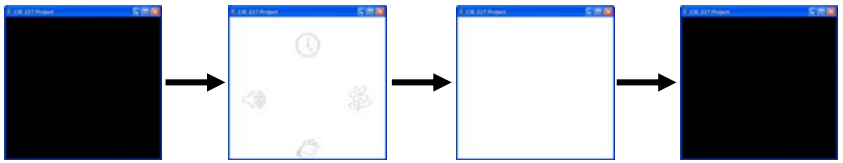

Figure 2. System logon process

Step (1): Present black screen for ~2 seconds

Step (2): Immediately present graphical password options for 200 ms

Step (3): Display white screen for 500 ms. Repeat steps (1) – (3) for each round

Goals

- **Determine threat level of camera based shoulder-surfing attacks on PassFaces style graphical password systems**
- **Create a logon interface that is not vulnerable to human shoulder-surfing and far less vulnerable to video recording with commodity cameras**
- **Increase resource requirement (time and equipment) required for attacker to launch successful attack**
- **Pure software implementation to avoid complex hardware and cost**
- **Take advantage of slow automatic exposure on consumer-grade cameras to 'trick' optics, while allowing users to login with high success rate (human visual system can react to contrast inversion faster than camera optics)**
- **Threat model: attacker with commodity camera has clear view of number pad and logon screen, can record entire logon session, and can analyze the recording frame by frame offline to extract information**

System Design

The system is designed with both human and electronic shoulder-surfing attacks in mind

- **A black screen is initially displayed**
- **The graphical password input screen is displayed in light gray on a white background for a few hundred milliseconds (contrast inversion)**
- **The graphical password fades and a white screen remains, repeat for each icon in user's graphical password**

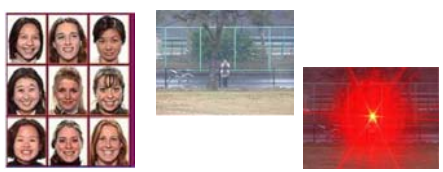

Figure 1. (left) PassFaces example (image grid maps to number pad), (right) Camera Zapping example – defeating the CCD of a camera with a laser from 100 meters

Results

PassFaces style system:

- **Attackers defeated PassFaces style system 100% of the time with a recording device**

Our contrast inversion system:

- **Users were able to login 100% of the time**
- **Attackers were unable to record usable footage with neither cell phone cameras or standard video cameras (0% success rate on compromising passwords)**

Figure 3. Shoulder-surfing attack test

Future Work

- **Reduce the cognitive load on the user during the contrast inversion process**
  - **Don't use contrast inversion to obfuscate presentation of password, only use it to obfuscate input of user's selection (input selection with cognitive trapdoor game)**
- **Increase password and system strength**
  - **Obfuscate image presentation separately using associative image passwords or optical illusions**
- **Study usability for users with sight disabilities**
- **Use of SLR and HD video cameras**
- **Ambient light conditions**

Conclusion

- **We have shown a PassFaces style system can easily be defeated with electronic shoulder-surfing**
- **We have demonstrated a novel, cost effective, software tactic that can be utilized in more complex systems to successfully deter against both human and electronic methods of shoulder-surfing**
- **Such a system would have the potential to greatly reduce the costs associated with identity theft, while improving usability**