2014

My Smartwatch Sees Your Password!

My Google Glass Sees Your Password!

My iPhone Sees Your Password!

Qinggang Yue
University of Massachusetts Lowell

In Collaboration with
Zhen Ling, Southeast University, China
Xinwen Fu, Benyuan Liu, University of Massachusetts Lowell
Wei Yu, Towson University
Wei Zhao, University of Macau

UMASS LOWELL

Outline

- Introduction
- Blind recognition of touched keys
- Evaluation
- Countermeasures
- Conclusion

Motivation

- Smart devices are ubiquitously used.
- Most smart devices are equipped with a camera.
- The camera can spy on people tapping and inputting credentials such as passcodes or passwords.

Existing Work on Recognizing Touch Inputs

1. Directly identify text on screen or its reflections on objects.
2. Detect visible features of the keys such as light diffusion surrounding pressed keys and popups of pressed keys.
3. Blindly recognize the text input on mobile devices while text or popups are not visible to the attacker.

Most Related Work

- Use computer vision techniques to recognize possible touched keys and use a language model to correct the prediction.
- Poor success rate for passwords.

We are able to recognize passcodes with a success rate of as high as 90%!

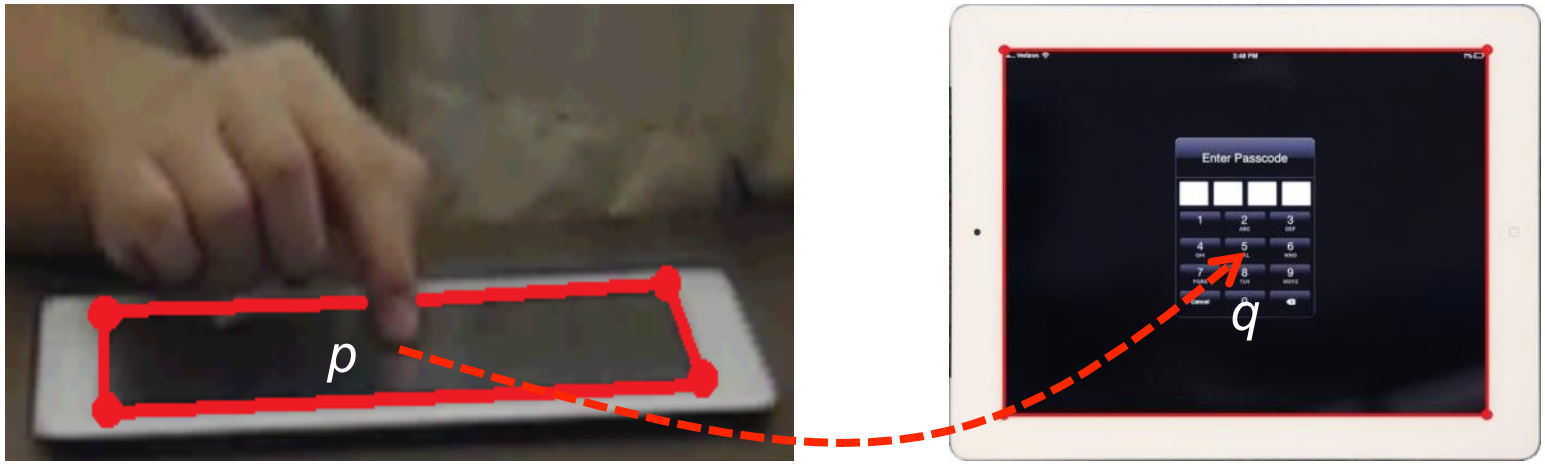
Outline

- Introduction
- Blind recognition of touched keys
- Evaluation
- Countermeasures
- Conclusion

Basic Idea

- **Assumption**: naked eyes cannot see anything on screen in the video.
- **Basic idea**: track fingertip movement, identify a touched point and map its location to a reference image of the soft keyboard. Use homography between two images:

$$q = \mathbf{H}p.$$



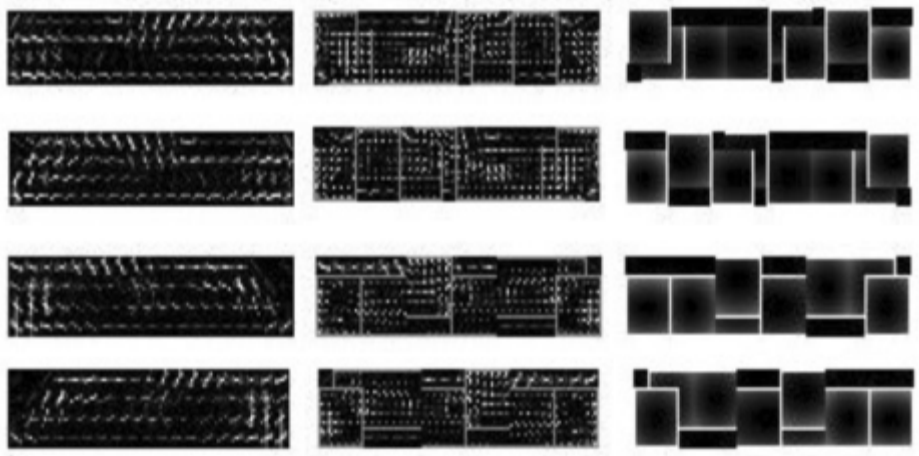
Step 1. Taking Videos

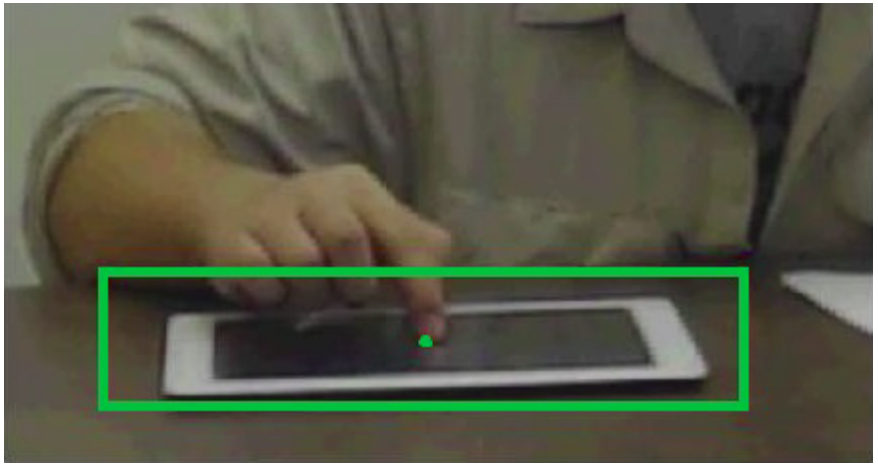
- Use sneaky cameras including Google Glass, web cameras, smartphone cameras, even smartwatch!
  - Factors: camera angle, distance, lighting
- Adjust the camera angle at a distance to record the device and touching fingertip movement.

Example Video by Google Glass

Step 2. Preprocessing

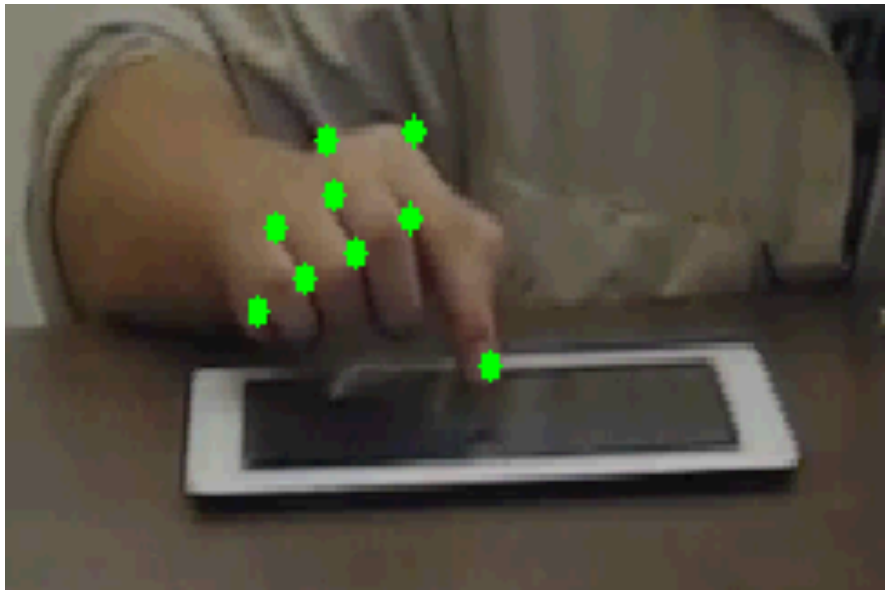
- Keep the area of moving hand on screen.
  - Use Deformable Part-based Model (DPM) - an object tracker - to track the area of interest for a moving target.





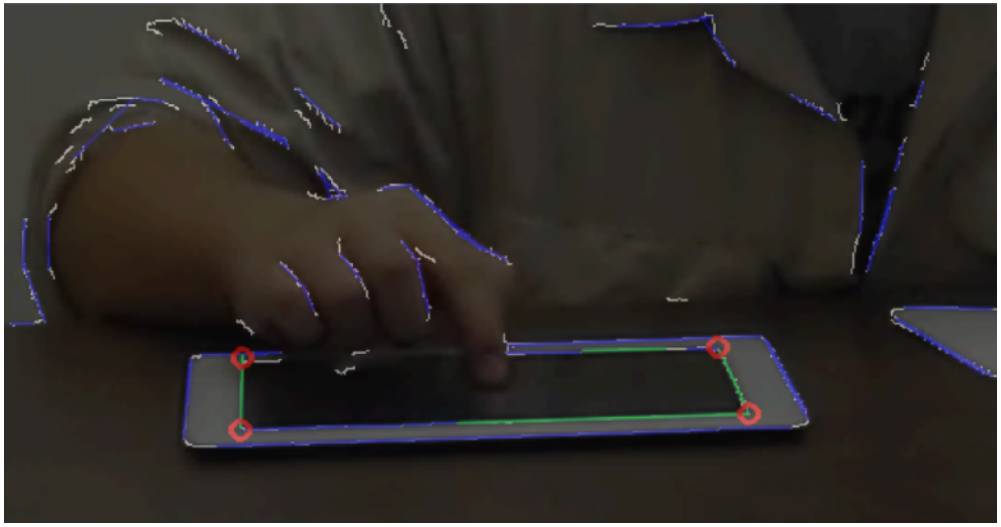
Step 3. Detecting Touching Frames

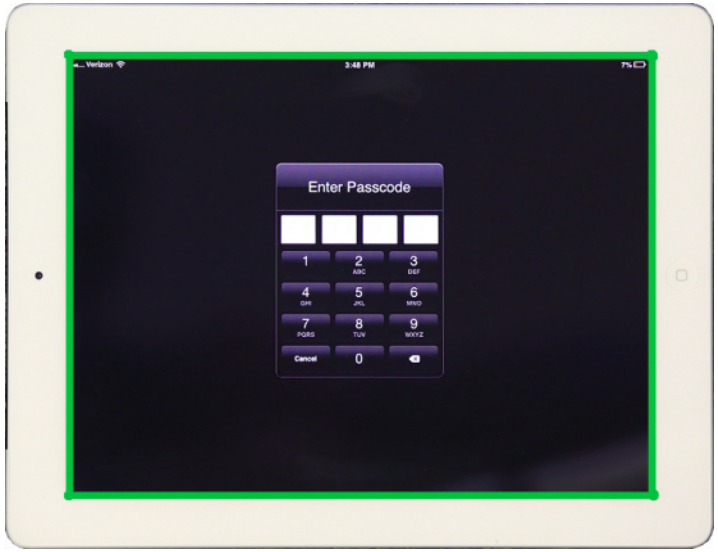
- Derive a pattern of the touching finger movement
  - Finger moves downward, stops and then upward.
- Track feature points on the hand by optical flow.
  - All fingers keep the same gesture during touching.
- Use the frame in which velocity of most tracked points changes the direction as touching frame.



Step 4. Deriving Homography Matrix

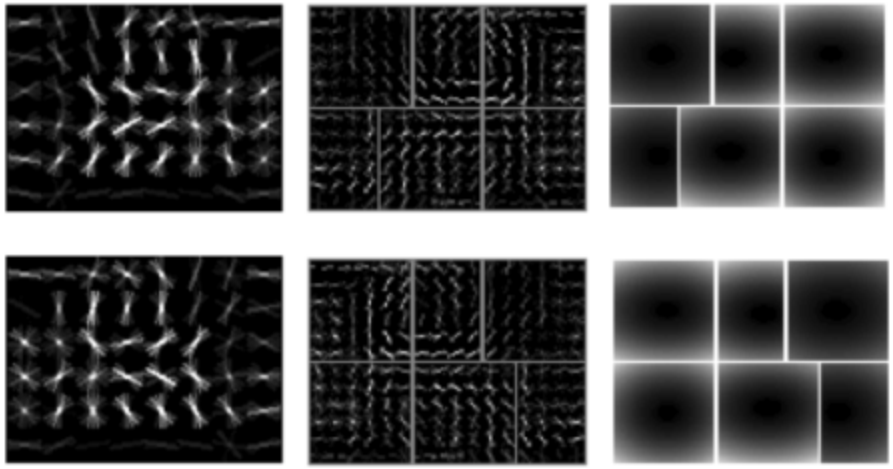
- Derive touch screen corners, intersection of the four edges of the touch screen.
  - Canny edge detector to detect edges
  - Hough line transform to get the lines.
- Use these four pairs of corner points to derive the homography matrix.





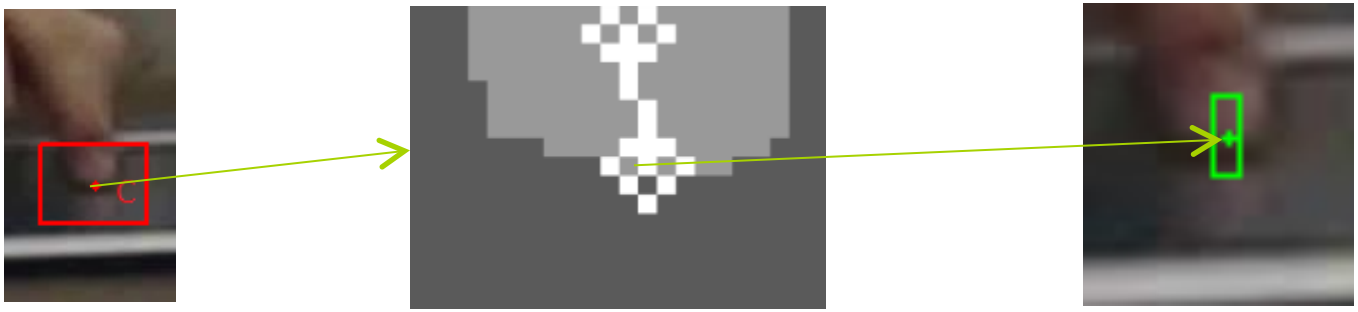
Step 5 - Locating Touching Fingertip

- Use the DPM object detector to locate the touching fingertip in touching frames.
- Derive a large box bounding the touching fingertip.



Step 6. Estimating Touched Area

- Deriving the fingertip contour
  - Use k-means clustering to cluster pixels in a small bounding box to get the fingertip contour.
  - Two groups bright fingertip and dark screen.
- Deriving the accurate touched area
  - Fit a line over central points of the contour and get fingertip direction and top.
  - Train the touched area around the fingertip top.

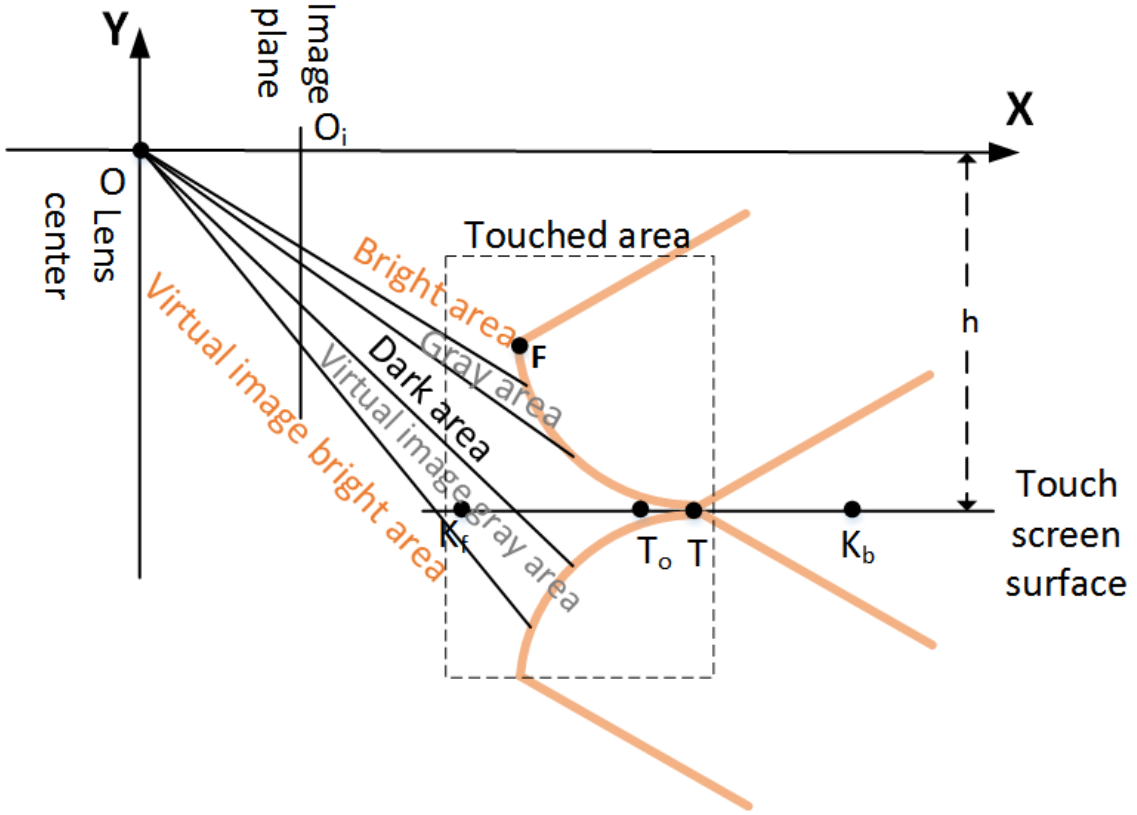


Step 7. Recognizing Touched Keys

- Which pixels are the touched points in this estimated tiny touched area?
- If the touched point is found, map the estimated touched point to the reference image of the software keyboard.

Step 7. Recognizing Touched Keys (Cont'd)

- Apply k-means clustering to estimated touched area.
  - k=5, because of illumination and shadowing.
- Use a point in the upper part of the darkest cluster as the touched point.



Outline

- Introduction
- Blind recognition of touched keys
- Evaluation
- Countermeasures
- Conclusion

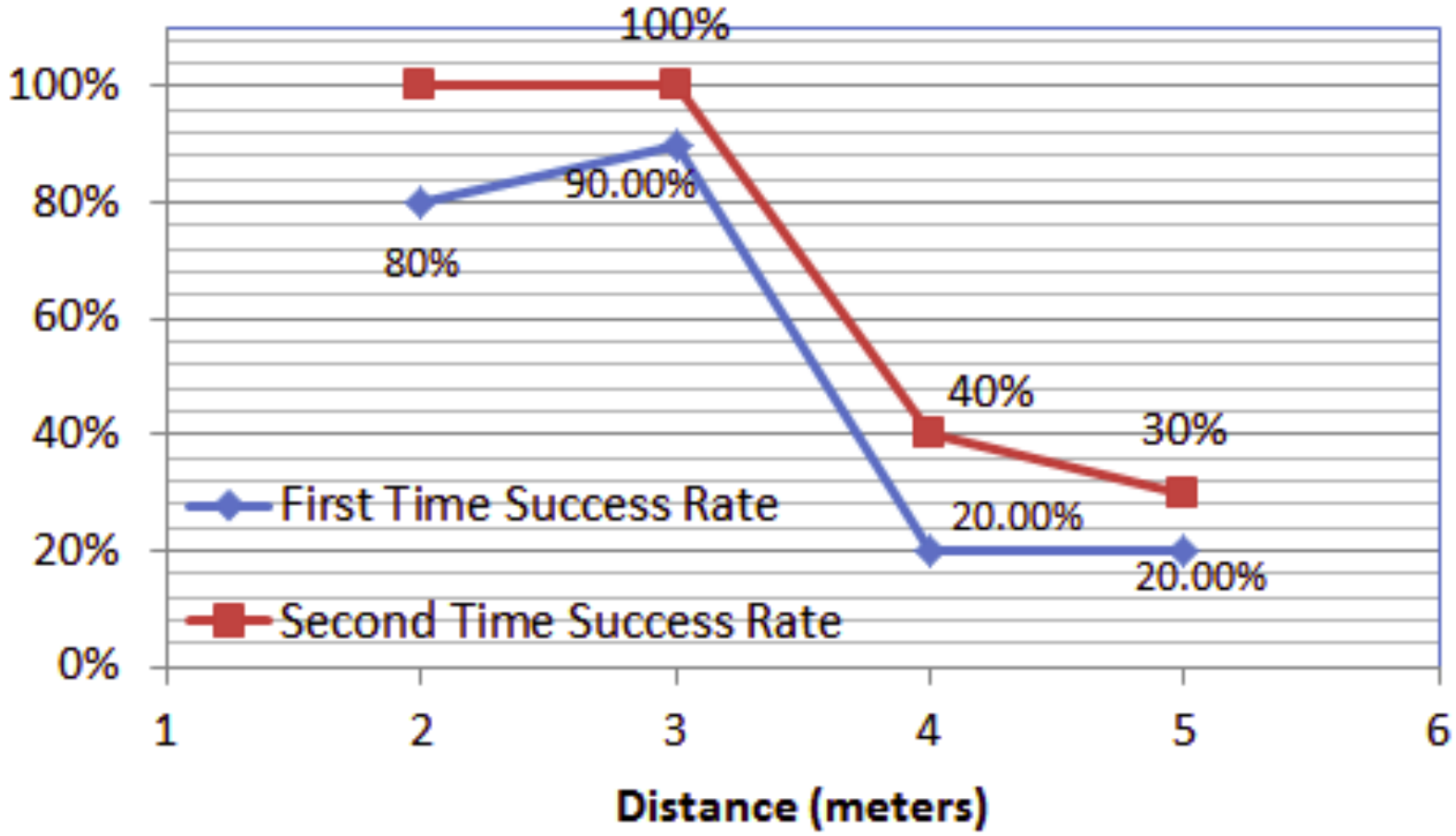
Recognizing Touched Keys on iPad via Webcam

- Around 8 feet

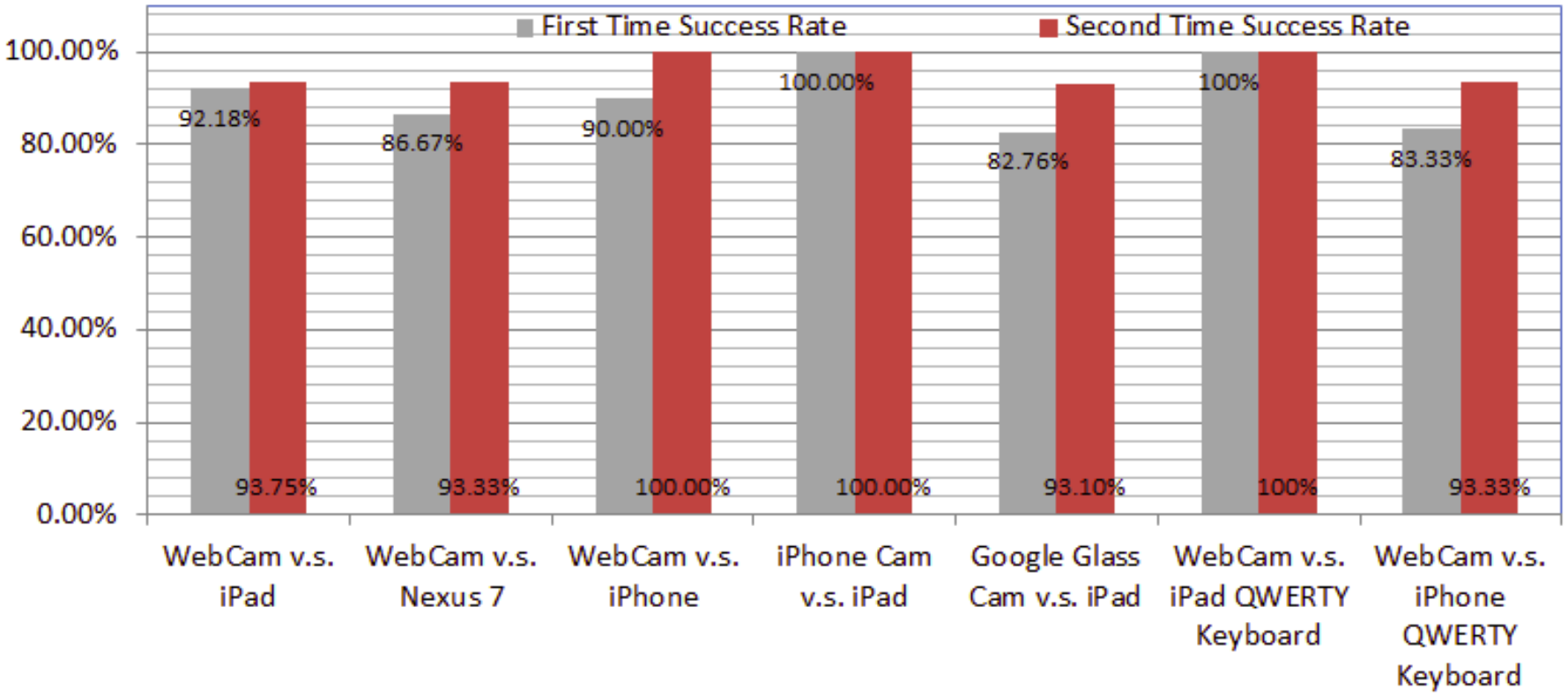
	Front	Left	Right	Total
First Time	92.18%	75.75%	79.03 %	82.29%
Second Time	93.75%	89.39%	90.32%	91.14%
Per Digit	98.04%	96.59%	97.58%	97.39%

Success Rate v.s. Distance

- WebCam



Comparing Different Targets and Cameras



Remote Attack

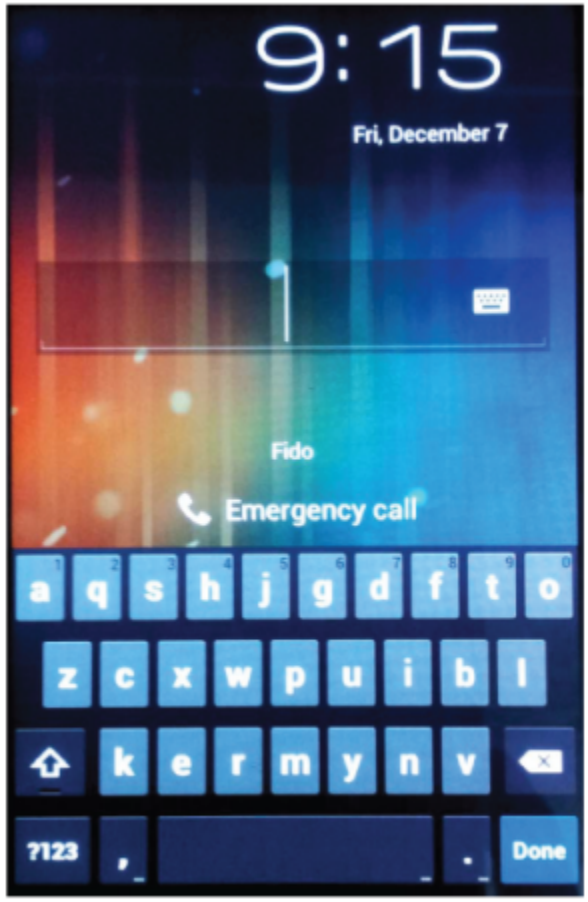
- Success rate 100% in the following case.

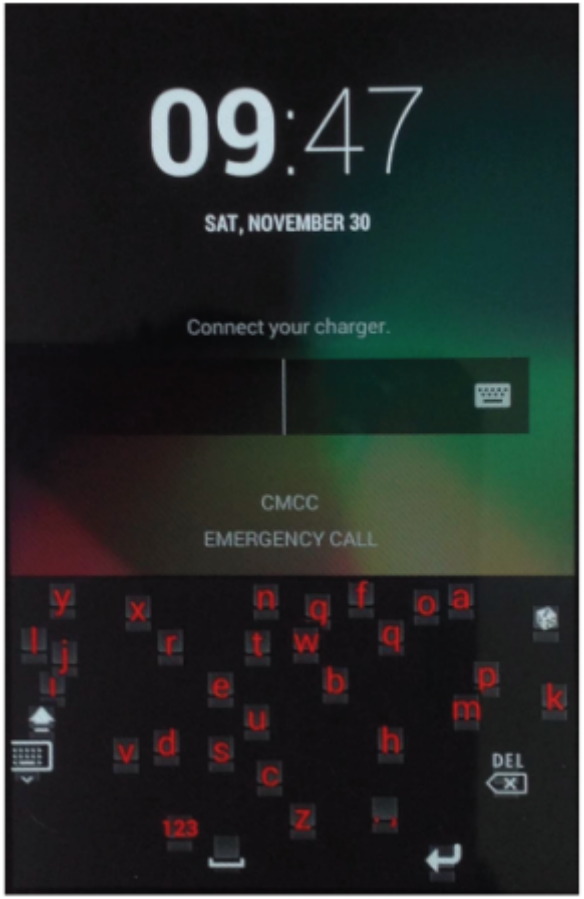
Outline

- Introduction
- Blind recognition of touched keys
- Evaluation
- Countermeasures
- Conclusion

Countermeasures

- Privacy Enhancing Keyboard (PEK): context aware randomized software keyboard





Outline

- Introduction
- Blind recognition of touched keys
- Evaluation
- Countermeasures
- Conclusion

Conclusion

- Sneaky cameras may take away credentials.
- Our attack tracks the finger movement and recognizes touched keys
  - High success rate. It is not a fluke.
- The attack can be made automatic.
- Our context aware Privacy Enhancing Keyboard (PEK) helps resist the attack and other attacks.
- Please watch demo at CNN Money - Google Glass wearers can steal your password

Thank you!