无数双“眼睛”都看到你的密码啦！

付新文, 副教授, 马萨诸塞大学罗威尔分校, 美国

凌振, 博士, 东南大学, 中国

2014年9月

ISC 2014 中国互联网安全大会

360互联网安全中心

China Internet Security Conference 2014

2014中国互联网安全大会

提纲

- 背景介绍
- 盲识别密码
- 攻击评估
- 防护措施
- 总结
- 演示

研究动机

- 智能设备在我们的生活中无所不在
- 很大一部分智能设备都配有相机
- 这些相机可能会被恶意使用，窥觑您的隐私

其它可能场景

相关工作

1. 直接识别屏幕上或反射在物体上的文字
2. 识别输入键的其它可见特征，例如按键的光晕和跳起的提示键
3. 盲识别触摸输入
   - 看不到触摸屏上的光晕或提示键

盲识别最相关工作

- 用计算机视觉识别可能输入的键，然后用语言模型排除掉不可能的键
- 无法很好的识别密码

我们的技术识别密码成功率大于90%！

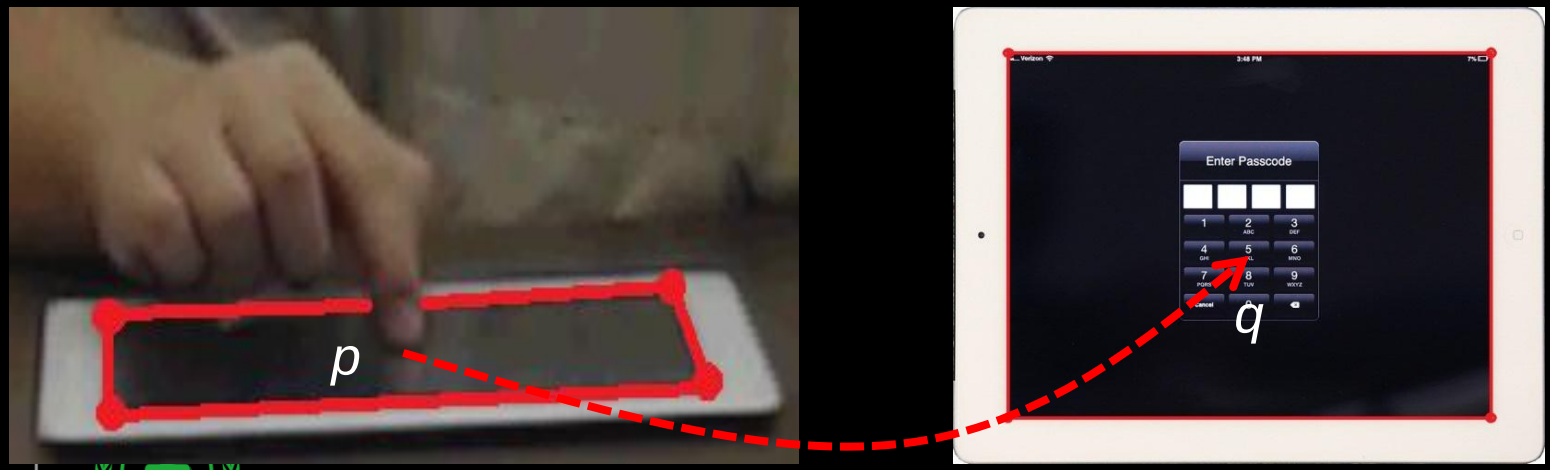
提纲

- 背景介绍
- 盲识别密码
- 攻击评估
- 防护措施
- 总结
- 演示

方法概述

- 假设：肉眼在所录视频中看不到任何东西
- 基本方法：跟踪指尖移动，识别触摸点，把触摸点映射到一个参考键盘上从而识别相应键
  - 利用平面在两张图像中homography关系

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



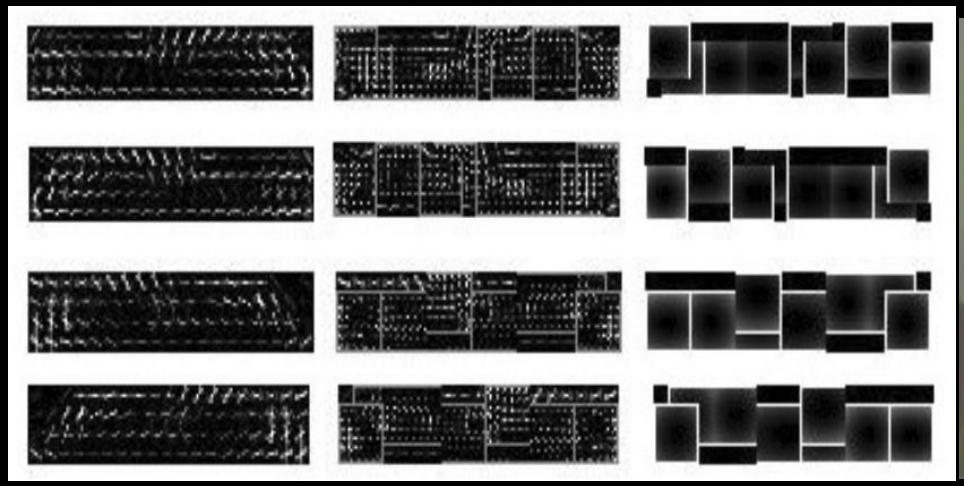
步骤1：录像

- 用谷歌眼镜、网络摄像头、智能手机、智能手表偷拍
  - 视频质量影响因素：角度，距离，照明等
- 黑客需要调整角度以拍到手指在屏幕上的移动

谷歌眼镜例频

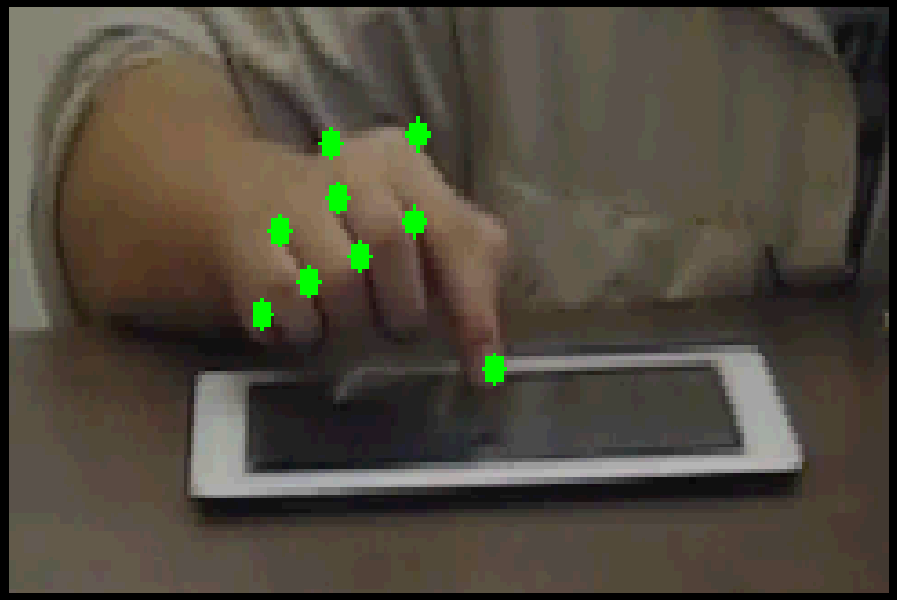
步骤2：预处理

- 只保留手和触摸屏区域
  - 使用物体跟踪技术Deformable Part-based Model (DPM) 识别跟踪感兴趣区域



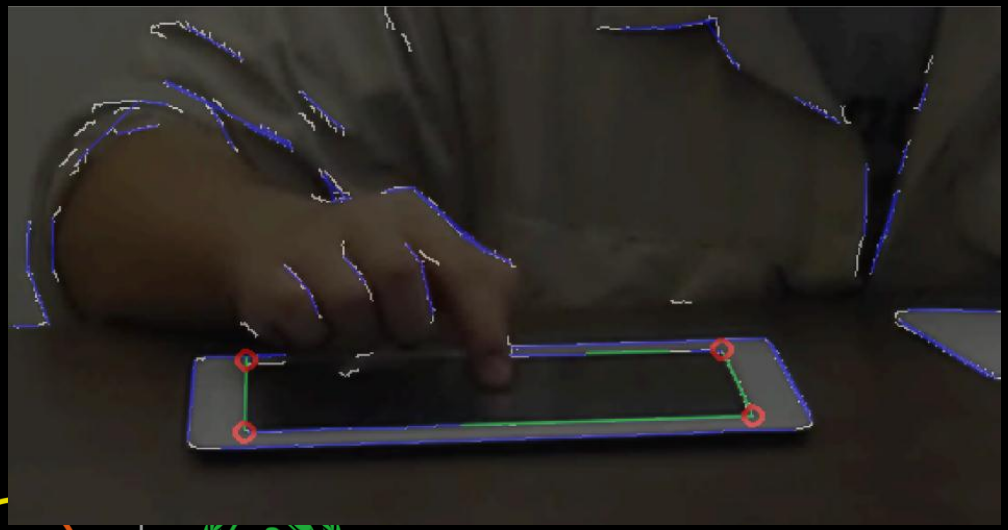
步骤3：识别触摸帧

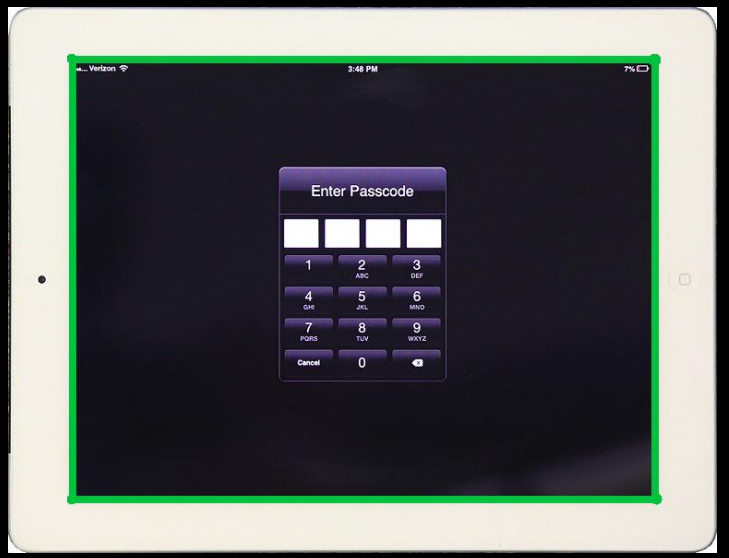
- 对手指触摸输入建模
  - 手指先向下移动，停住，然后向上移动
- 用光流（ optical flow ）跟踪手的特征点
  - 观察：在触摸输入过程中所有手指基本保持同样手势
- 触摸帧是大部分特征点改变移动方向的那一帧



步骤4：获取Homography矩阵

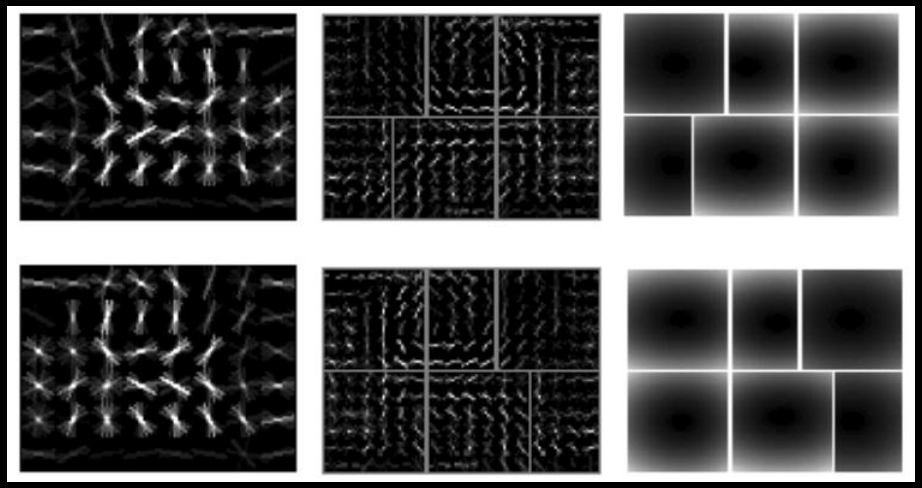
- 获取触摸屏四角，即触摸屏四边的交叉点
  - 用Canny边测试技术获取图像中的边界
  - 用Hough线变换从边界中选出触摸屏边界
- 用两个图像中对应四角求homography矩阵

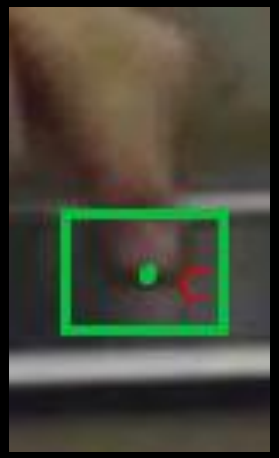




步骤5：定位触摸指尖

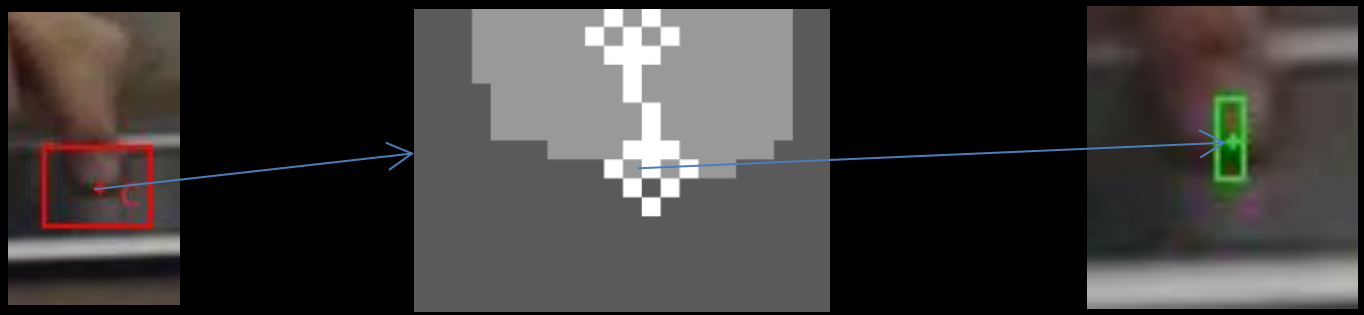
- 使用DPM物体探测技术在触摸帧中识别触摸手指尖
  - 手指尖在DPM用于检测的大框中





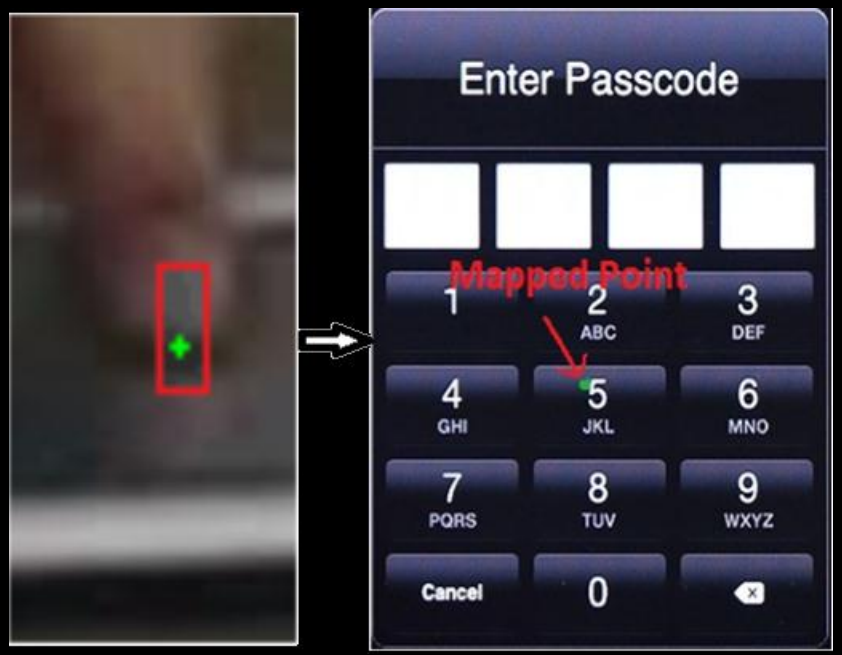
步骤6：估计触摸区域

- 获取指尖轮廓
  - 用k-means聚类法将DPM找到的区域像素聚成两类
  - 亮的区域便是指尖轮廓
- 获取精确的触摸区域
  - 拟合找到指尖轮廓的中间线从而获得指尖方向和最高点
  - 选取围绕指尖最高点的狭小区域作为精确触摸区域



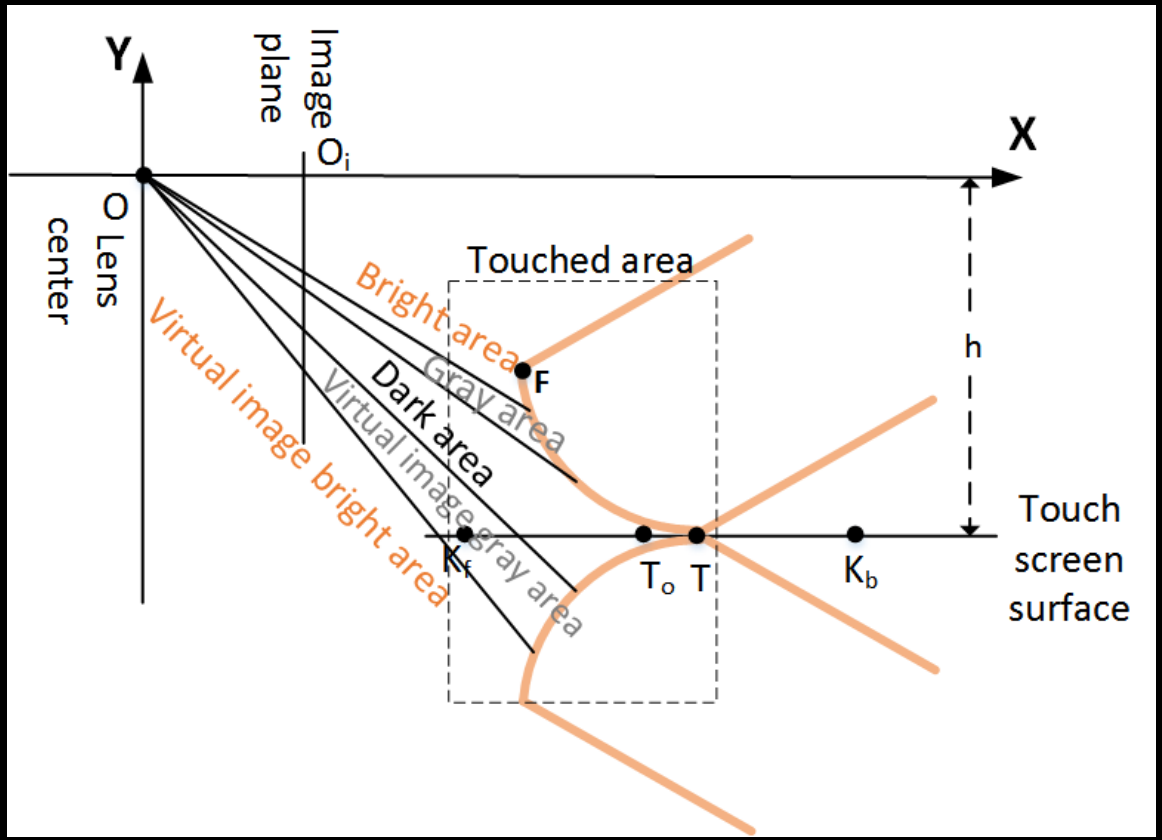
步骤7：识别触摸键

- 在获取的触摸区域中，哪些像素是触摸点呢？
- 如果触摸点找着了，把这个触摸点映射到参考键盘就可以找着触摸键了。



步骤7：识别触摸键（续）

- 用k-means聚类已获得的狭小触摸区域
  - k=5, 由于照明、阴影和指尖在触摸屏上的成像
- 用最黑类上部的中点作为触摸点



提纲

- 背景介绍
- 盲识别密码
- 攻击评估
- 防护措施
- 总结
- 演示

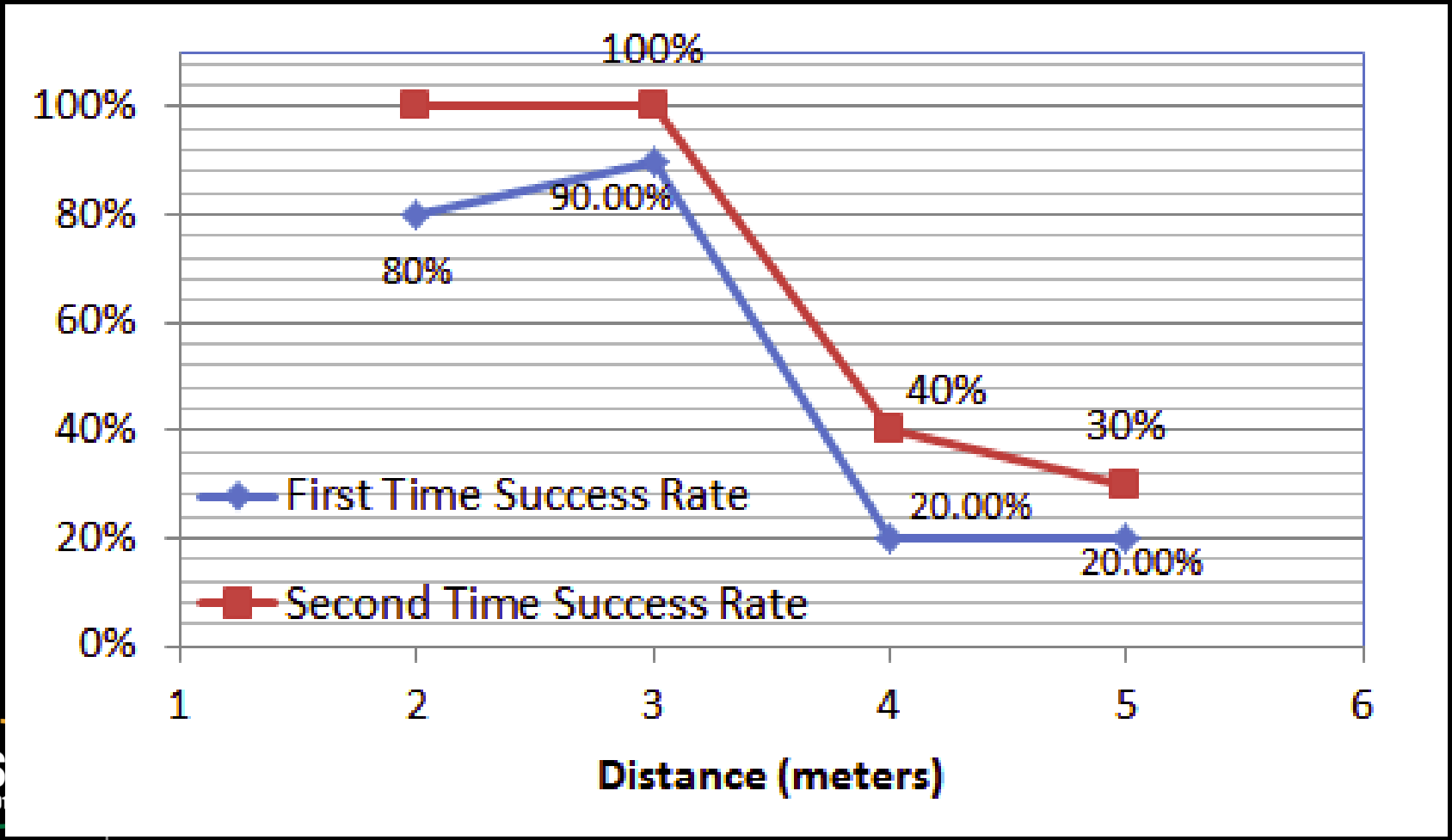
识别iPad上的触摸输入-网络摄像头

- 2.5米远，攻击锁屏密码(4键)

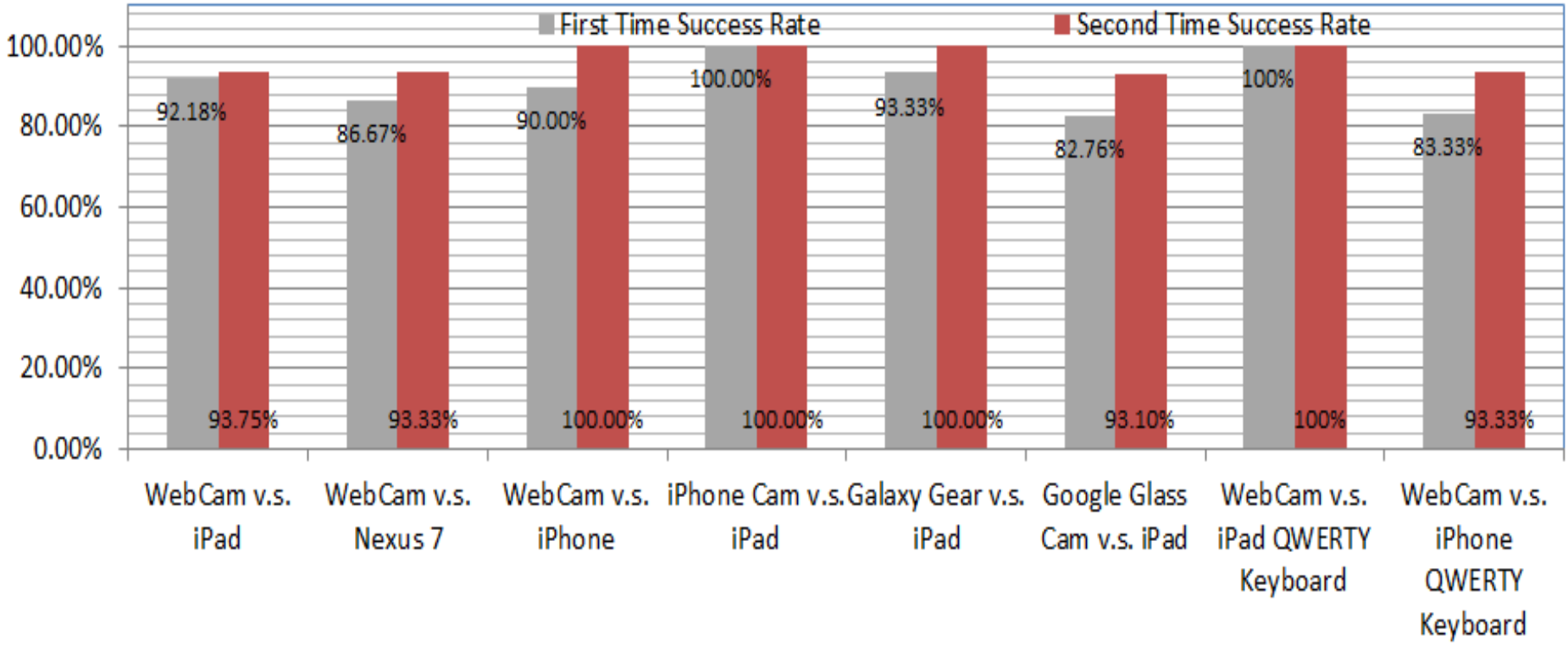
	Front	Left	Right	Total
First Time	92.18%	75.75%	79.03 %	82.29%
Second Time	93.75%	89.39%	90.32%	91.14%
Per Digit	98.04%	96.59%	97.58%	97.39%

成功率和距离关系

- 网络摄像头



比较不同的目标和相机效果

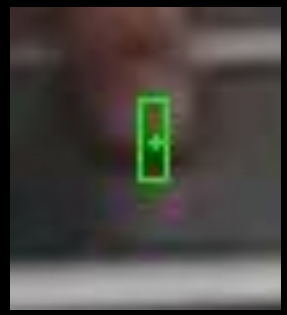


远程攻击

- 在如下场景中100%成功率

攻击适用范围

- 结论：只要能拍到手指和触摸屏，攻击就有效
- 由于视频质量的不确定，不是每次都能*自动识别*视屏中的触摸输入
  - 各种手工协助识别法：例如，手工选取精确触摸区域

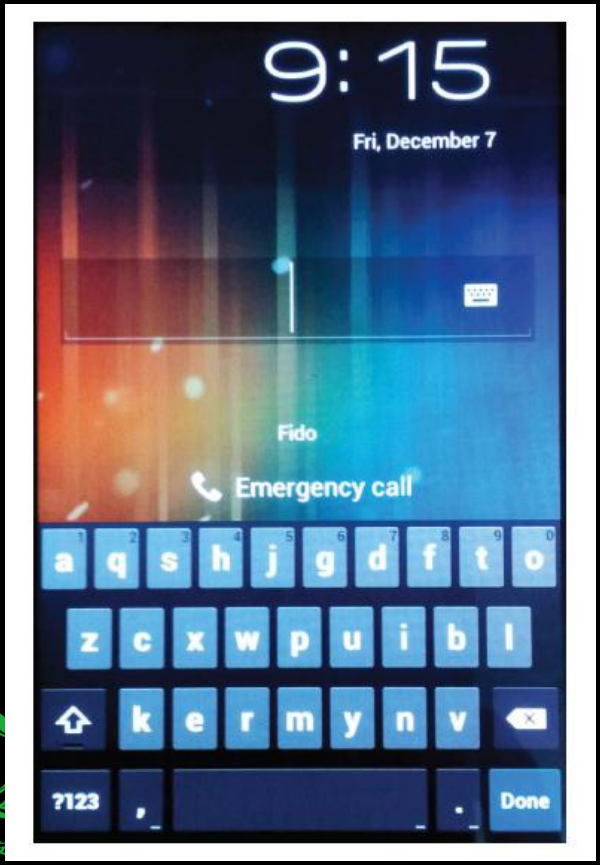


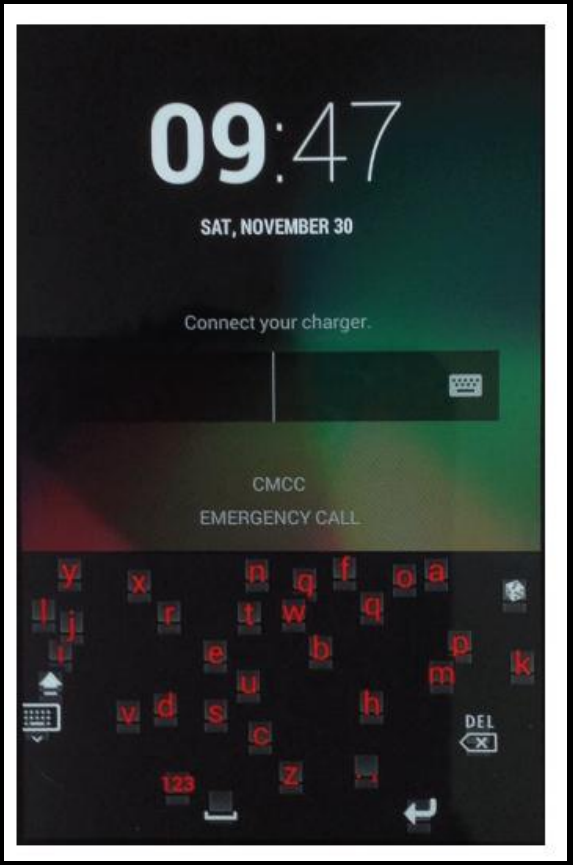
提纲

- 背景介绍
- 盲识别密码
- 攻击评估
- 防护措施
- 总结
- 演示

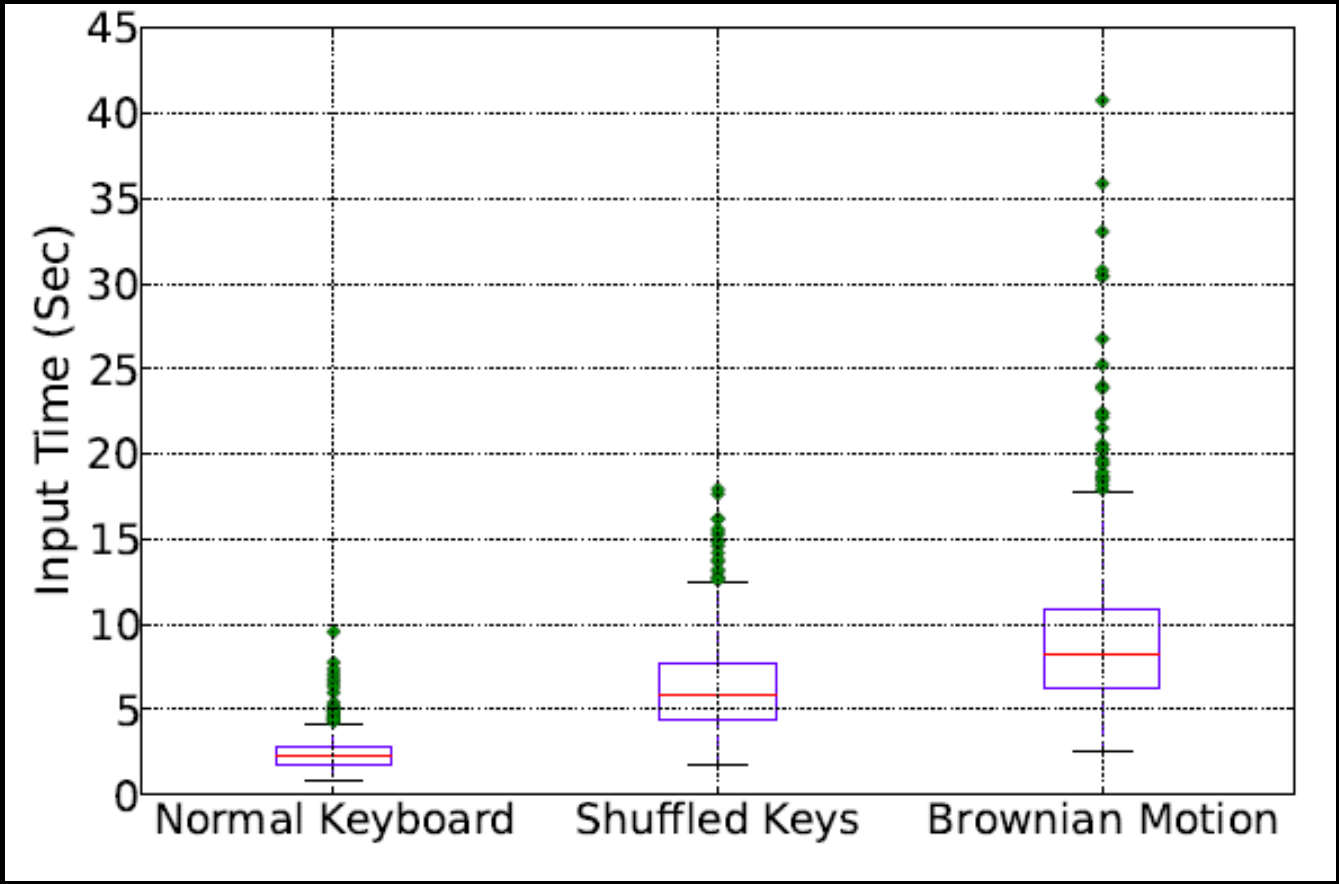
智能隐私增强键盘（PEK）

- Android系统级第三方键盘app
- 输密码时弹出随机键盘，否则显示正常键盘





PEK性能评估


Input Time (Sec)
0
5
10
15
20
25
30
35
40
45
Normal Keyboard
Shuffled Keys
Brownian Motion

提纲

- 背景介绍
- 盲识别密码
- 攻击评估
- 防护措施
- 总结
- 演示

总结

- 各种移动设备的相机会偷走您的秘密！
- 我们的攻击能够自动跟踪手指移动从而获取触摸输入
  - 高成功率。不开玩笑！
- 我们的智能隐私提升键盘（PEK）可以防御此攻击。

谷歌市场（Google Play）

提纲

- 背景介绍
- 盲识别密码
- 攻击评估
- 防护措施
- 总结
- 演示

演示

- 自动分析视频获取密码
- 智能隐私提升键盘（PEK）

谢谢！

小问题：“请问我们的攻击攻击哪一人种较困难？”为什么？