WHEN CSI MEETS PUBLIC WI-FI: INFERRING YOUR MOBILE PASSWORD VIA WI-FI SIGNALS

ZIFAN QU

Introduction

- Smartphones and tablets are commonly used for performing privacy sensitive transactions of banking, payment, and social applications.
- Two types of eavesdropping attacks:
  - Directly observing input from screen and keyboard
  - Side channel attacks to infer input – Using video from a camera, acoustic signal at microphone, motion sensors, electromagnetic signal at radio antenna, etc.
- previous works on the latter make one of two assumptions:
  - There is one (or more) external device(s) to collect the required signals
  - The target device's sensors are compromised to provide side channel information

PREVIOUS APPROACH – OUT-OF-BAND KEYSTROKE INFERENCE (OKI) MODEL

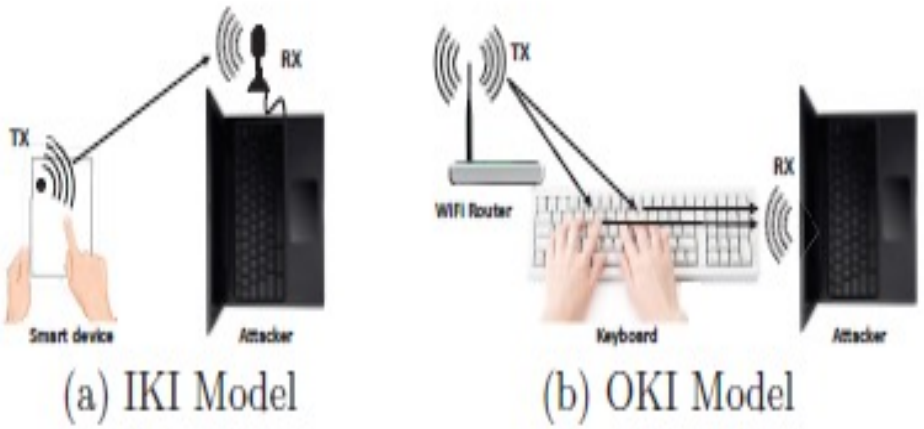


Figure 1: WiFi-based Keystroke Inference Models

- Adversary deploys two Wi-Fi devices close to the target device and makes sure the target device is placed right between the two.
- One is the sender device and the other one is the receiver device.
- The keystrokes are inferred from the multi-path distortions in signals.

WINDTALKER!!

- A novel and practical keystroke inference framework that allows an attacker to infer the sensitive keystrokes on a mobile device through Wi-Fi signals.
- Deploys rogue hotspot, unlike previous works which deploy external devices close to the target device or compromise the sensors.
- Challenges in design:
  1. Signal analysis to analyse keystrokes from the limited Channel State Information
  2. Prior CSI collection method required two Wi-Fi devices which are deployed close to the victim. More practical method needed
  3. The key inference must be done at some selective moments for obtaining a sensitive keystroke, such as payment PIN

IN-BAND KEYSTROKE INFERENCE (IKI) MODEL

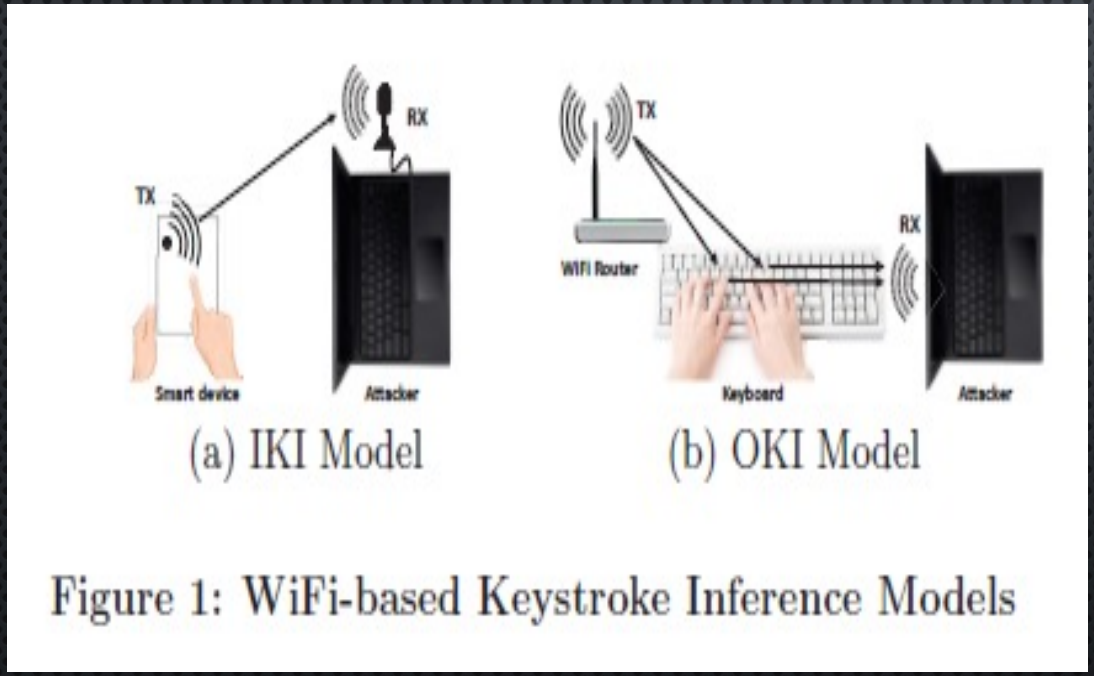


Figure 1: WiFi-based Keystroke Inference Models

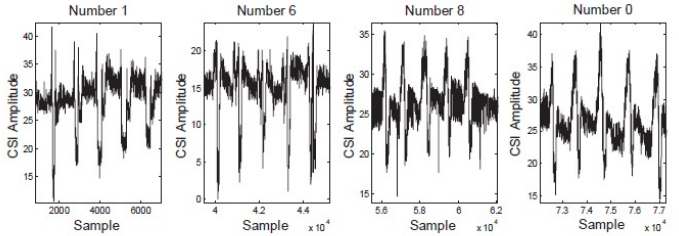
- THE WI-FI HOTSPOT PROVIDES FREE WI-FI NETWORKS FOR NEARBY USERS.
- WHEN A USER CONNECTS THEIR DEVICE TO THE HOTSPOT, THE WI-FI HOTSPOT IS ABLE TO MONITOR THE APPLICATION CONTEXT.
- IN ADDITION, THE WI-FI HOTSPOT PERIODICALLY SENDS ICMP PACKETS TO OBTAIN THE CSI INFORMATION FROM THE TARGET DEVICE.
- WHEN A SENSITIVE OPERATION IS DETECTED, THE HOTSPOT ADAPTIVELY LAUNCHES ITS KEYSTROKE INFERENCE METHOD.

Channel State Information (CSI)

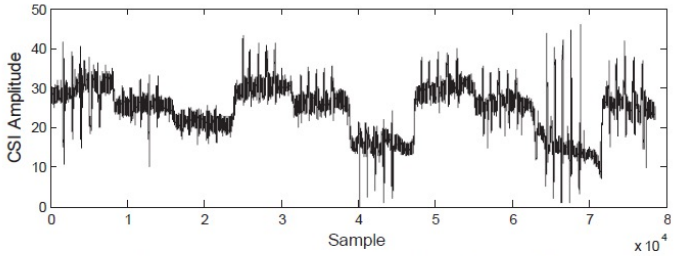
- Wi-Fi standards support Orthogonal Frequency Division Multiplexing (OFDM)
- In a system with N_{T_X} transmitter antennae, N_{R_X} receiver antennae, and N_S OFDM subcarriers, the overall system will use $N_{T_X} \times N_{R_X} \times N_S$ subcarriers
- CSI is information which represents the state of a communication link
- CFR $H(f,t)$ represents the state of wireless channel f in a signal transmission process
- Let $X(f,t)$ and $Y(f,t)$ represent the transmitted and received signal respectively
- CFR is given by the formula $H(f,t) = \frac{Y(f,t)}{X(f,t)}$
- Received signal represents interference from several signals scattered from various physical objects, the movement of the hand and fingers can generate a unique pattern in the time-series of the CSI values
- Using a directional antenna helps

FACTORS CONTRIBUTING TO CSI CHANGES

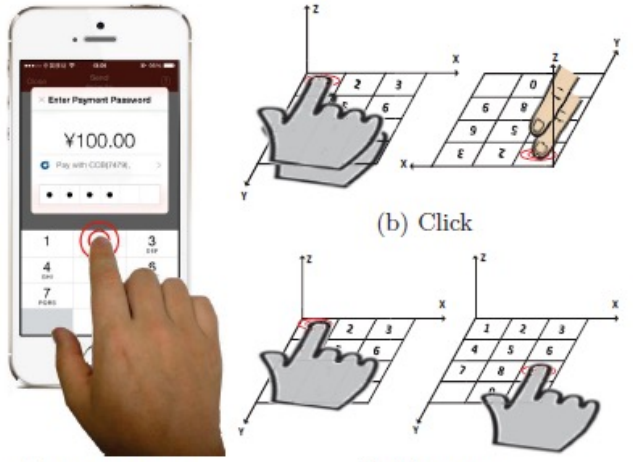
- TWO MAJOR FACTORS THAT AFFECT THE CSI:
  - HAND COVERAGE AND FINGER POSITION
  - FINGER CLICK



(a) Continuously Click in Different Keys



(b) Continuously Click in the Same Key



(a) Finger typing

(b) Click

(c) Coverage

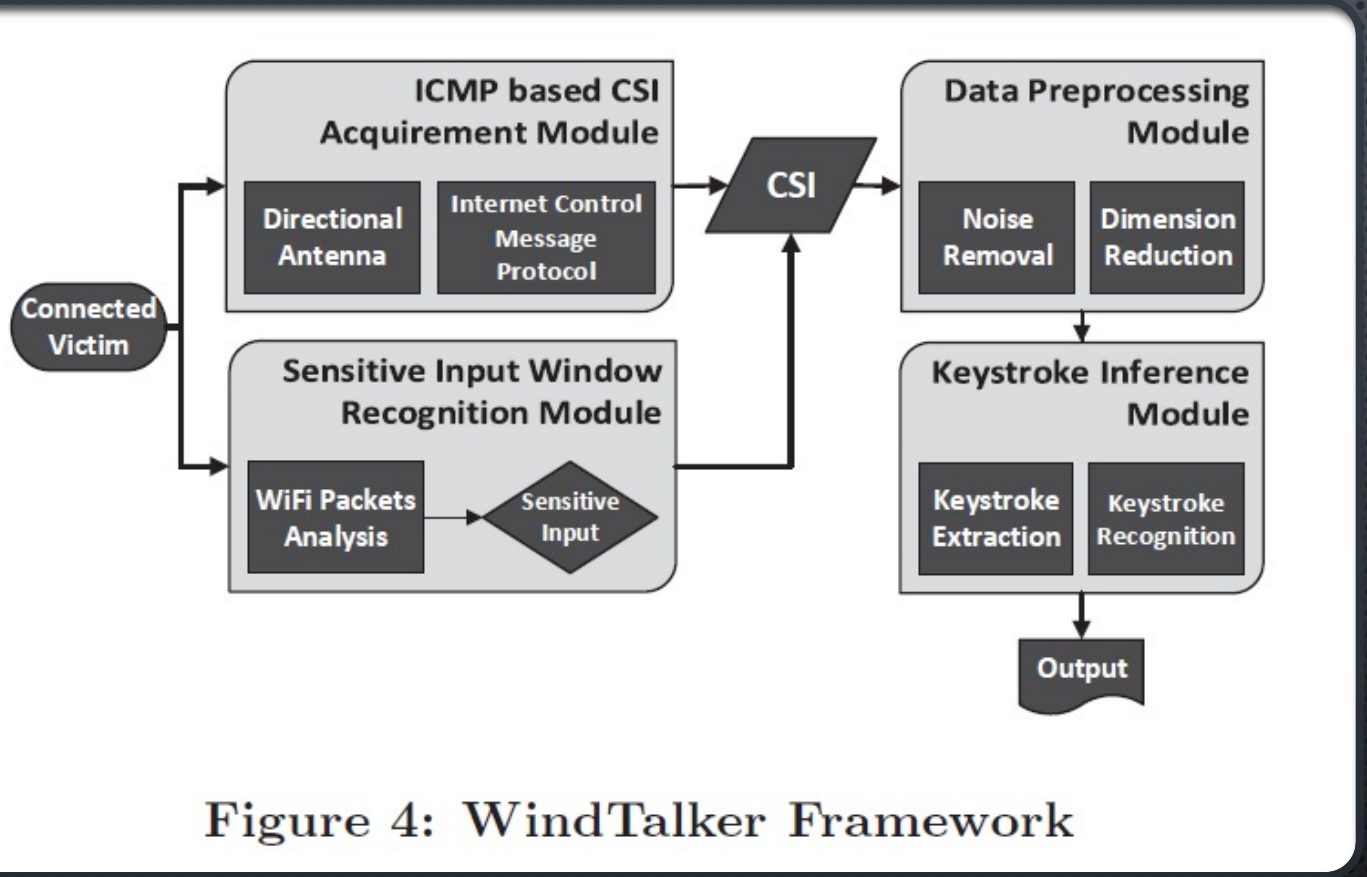


Figure 4: WindTalker Framework

DESIGN OF WINDTALKER

SENSITIVE INPUT WINDOW RECOGNITION MODULE

- To distinguish the time window of the sensitive input from that of insensitive input, WindTalker captures all the packets of the victim with Wireshark and records timestamp of each CSI data
- HTTPS does not protect the metadata of the traffic
- WindTalker builds a 'sensitive IP pool' and launches its keystroke inference module during access to these IPs

ICMP BASED CSI ACQUIREMENT MODULE

- Leverages Internet Control Message Protocol (ICMP) in hotspot to collect CSI data
- WindTalker periodically sends a ICMP Echo Request to the victim smartphone, which will reply an Echo Reply for each request
- To acquire enough CSI information of the victim, WindTalker needs to send ICMP Echo Request at a high frequency

ICMP BASED CSI ACQUIREMENT MODULE

- HOW TO MINIMIZE THE INTERFERENCE CAUSED BY NEARBY HUMAN BEINGS AND OTHER OBJECTS
- ANSWER = NOISE REDUCTION BY USING A DIRECTIONAL ANTENNA

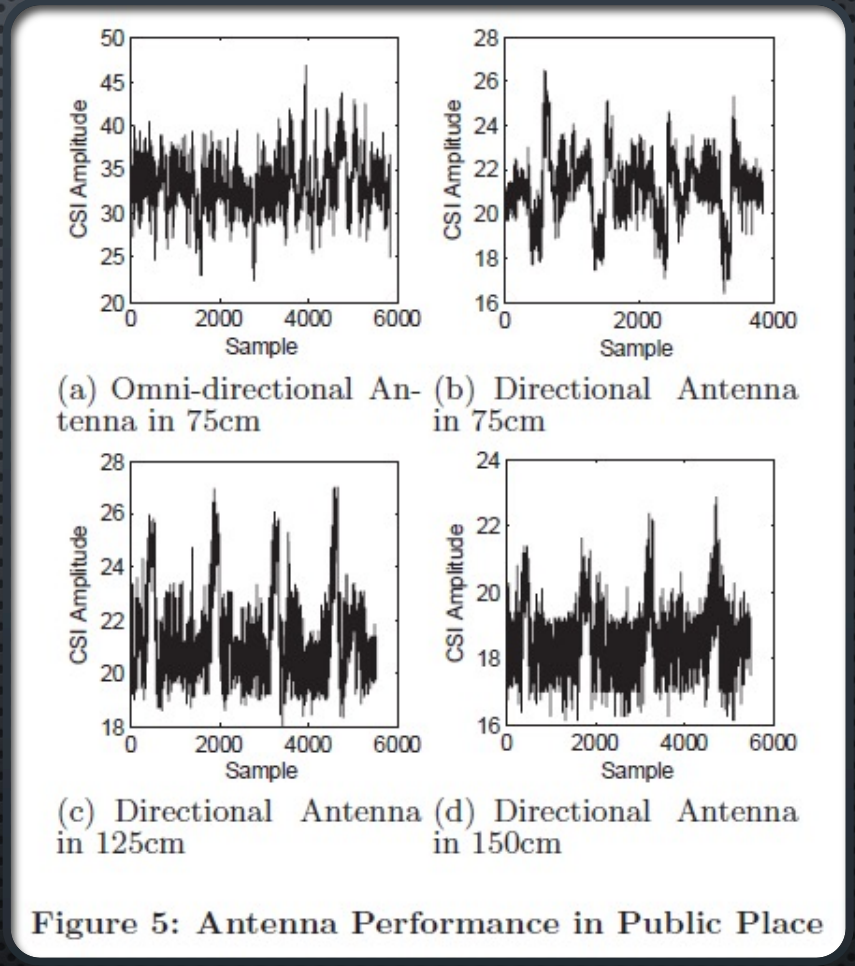


Figure 5: Antenna Performance in Public Place

DATA PREPROCESSING MODULE

- CSI FIRST PASSED THROUGH A LOW PASS FILTER
- DIMENSION REDUCTION IS THEN PERFORMED
- USES PRINCIPAL COMPONENT ANALYSIS FOR THE SAME

KEYSTROKE INFERENCE MODULE

IDENTIFYING KEYSTROKES IS DIVIDED INTO THREE MODULES:

1. KEYSTROKE EXTRACTION – TO DETECT START AND STOP OF KEYSTROKE. HAS THREE FURTHER STEPS:
   i. WAVEFORM PROFILE BUILDING
   ii. CSI TIME SERIES SEGMENTATION AND FEATURE SEGMENT SELECTION
   iii. KEYSTROKE WAVEFORMS EXTRACTION

2. KEYSTROKE RECOGNITION – CHOOSING FEATURES TO UNIQUELY REPRESENT KEYSTROKES.

3. CLASSIFIER TRAINING – TO RECOGNISE THE KEYSTROKES BASED ON THEIR WAVEFORM SHAPES

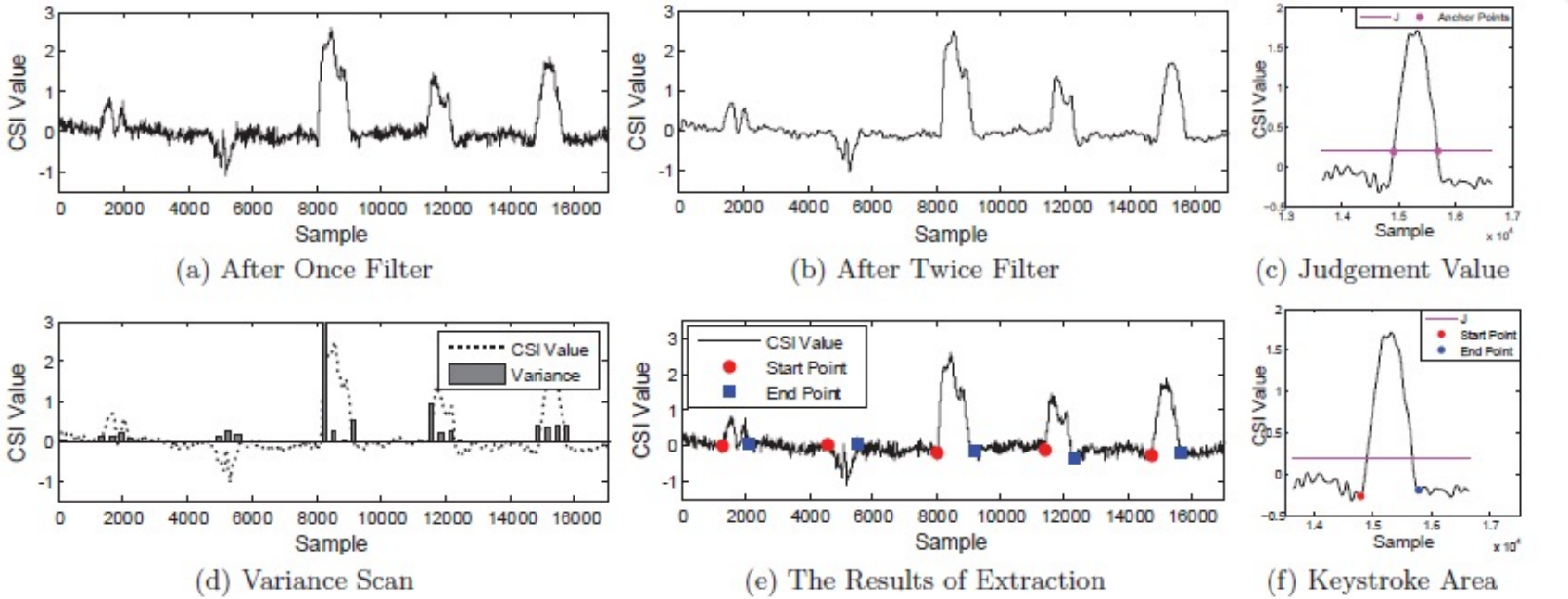


Figure 6: Keystroke Extraction

KEYSTROKE EXTRACTION

KEYSTROKE RECOGNITION

1. KEYSTROKE RECOGNITION – CHOOSING FEATURES TO UNIQUELY REPRESENT KEYSTROKES. USES DISCRETE WAVELET TRANSFORM TO COMPRESS THE WAVEFORM AND DYNAMIC TIME WARPING TO DETERMINE THE SIMILARITY BETWEEN WAVEFORMS

2. CLASSIFIER TRAINING – TO RECOGNISE THE KEYSTROKES BASED ON THEIR WAVEFORM SHAPES

EVALUATION

- Recruited 10 volunteers and asked them to input number passwords
- In the data training phase, WindTalker records each input and its corresponding CSI data
- In the test phase, WindTalker infers the input data based on the observed CSI time series

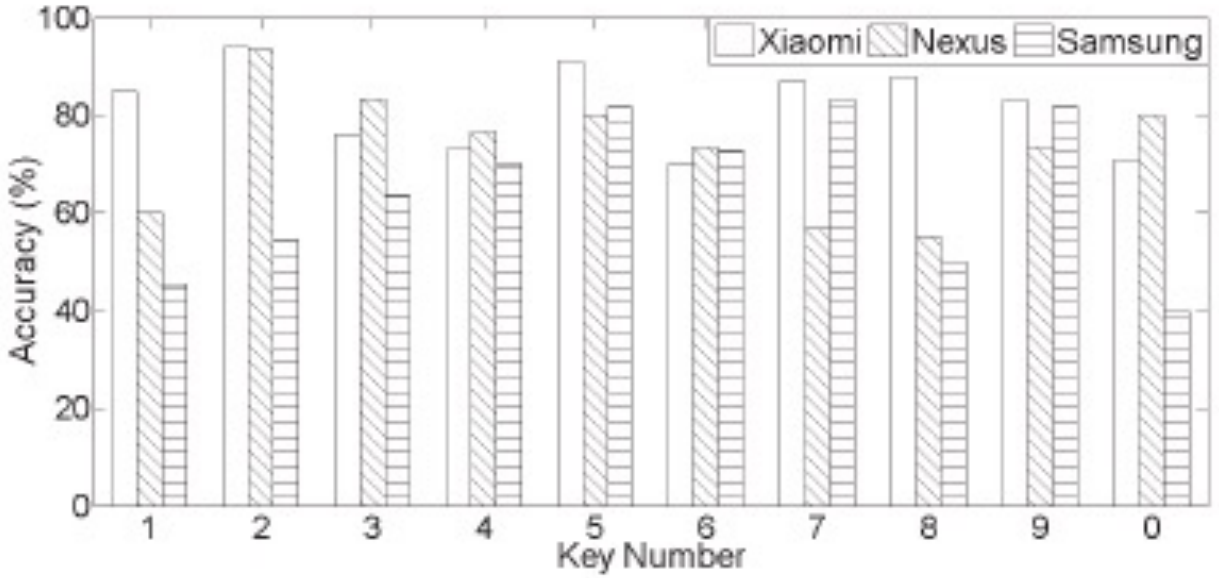


Figure 8: Classification Accuracy per key

Real world example: Alipay

- Deployed at a cafeteria like environment
- Simulated real world attack by:
  1. Online training phase – Volunteers enter randomly generated numbers
  2. Normal use phase – Volunteers browse the internet as a normal user
  3. Mobile payment phase – Using Alipay to enter a password and complete a payment
- With the traffic meta data, WindTalker obtains the rough start time and end point of Sensitive Input Window via searching packets whose destination is "110.75.xx.xx"
- The top three password candidates in this case were 773919, 773619, 773916 while the actual password was 773919
- Experiment results show that the attacker can successfully recover 2, 4, 7 and 9 passwords if allowed to try the password input for 5, 10, 50 and 100 times respectively

LIMITATIONS

- Hardware limitations - In WindTalker, the authors used Intel 5300 NIC and Linux 802.11n CSI Tool. In their experiments, it was observed that the system would crash when they performed ICMP based CSI data collection for iPhone or some versions of Android smart phones
- Fixed typing gesture – WindTalker only works in scenarios where the user touches the screen with relatively fixed gesture and if the phone is in a stable environment like a table
- User specific training - Hard to adopt the classifiers trained by other people to infer the victim's input