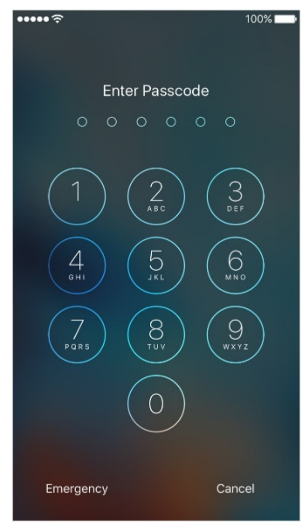
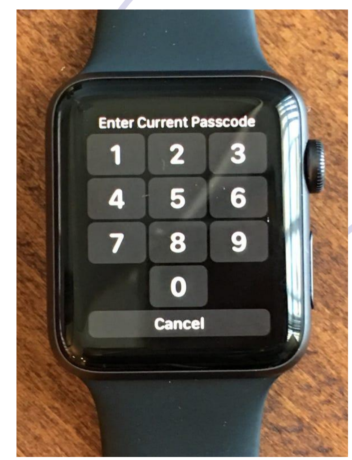
LightDefender: Protecting PIN Input using Ambient Light Sensor

Jiacheng Shang and Jie Wu
Center for Networked Computing
Dept. of Computer and Info. Sciences
Temple University

Personal Identification Number (PIN)

- A numeric or alpha-numeric password used in the process of authenticating a user accessing a system
- Applications

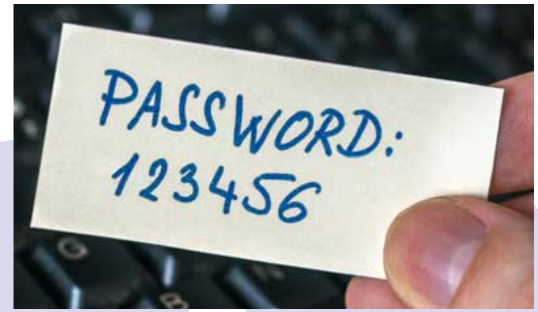


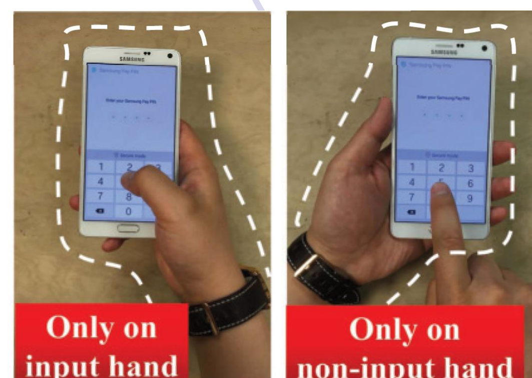


PIN Security

- Context related PINs
  - E.g. birthday data
  - Largely decreasing the randomness
- Shoulder-surfing attack
  - Using eyes or cameras
- Side-channel attacks
  - Acoustic signal [1]
  - Motion sensor [2]

[1] KeyListener: Inferring Keystrokes on QWERTY Keyboard of Touch Screen through Acoustic Signals, INFOCOM 2019
[2] WristSpy: Snooping Passcodes in Mobile Payment Using Wrist-worn Wearables, INFOCOM 2019



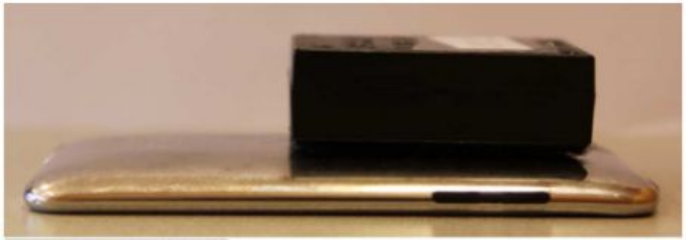


Existing solutions

- Challenge-response-based
  - User is given a random challenge
  - Input the correct response that is calculated using the PIN
  - Attackers can observe the challenge
  - The attacker can gather useful information by repeating the challenge procedure

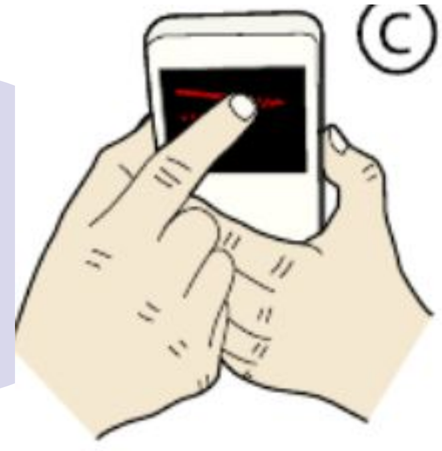
Existing solutions

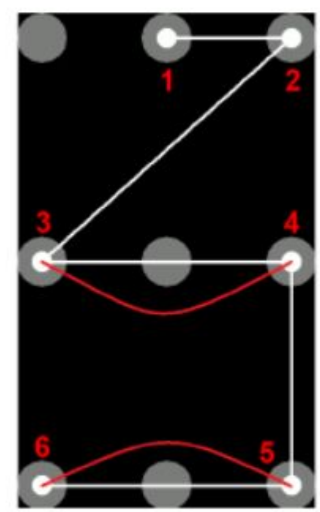
- Enhanced Challenge-response-based
  - Preventing attackers from observing challenges
  - Using secure secondary channel
  - Low usability
  - High learning cost



Existing solutions

- Indirect-input-based
  - Inputting PIN on a secondary interface
  - Altering original interaction methods of PIN input
- Input-behavior-based
  - Leveraging biometrics in input behavior
  - Only considering limited features in the time domain



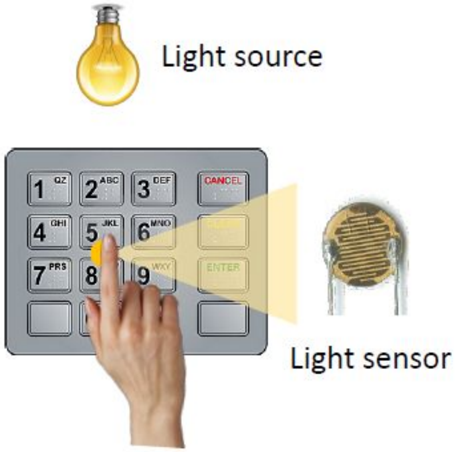


Attack Model

- Attackers aim to break PIN-based systems
- The capabilities of the attackers are
  - Simple PIN replay attack
    - Attackers only know the victim's PIN
  - Strong PIN replay attack
    - Attackers only know the victim's PIN
    - Attackers can also observe and imitate victim's PIN input behavior

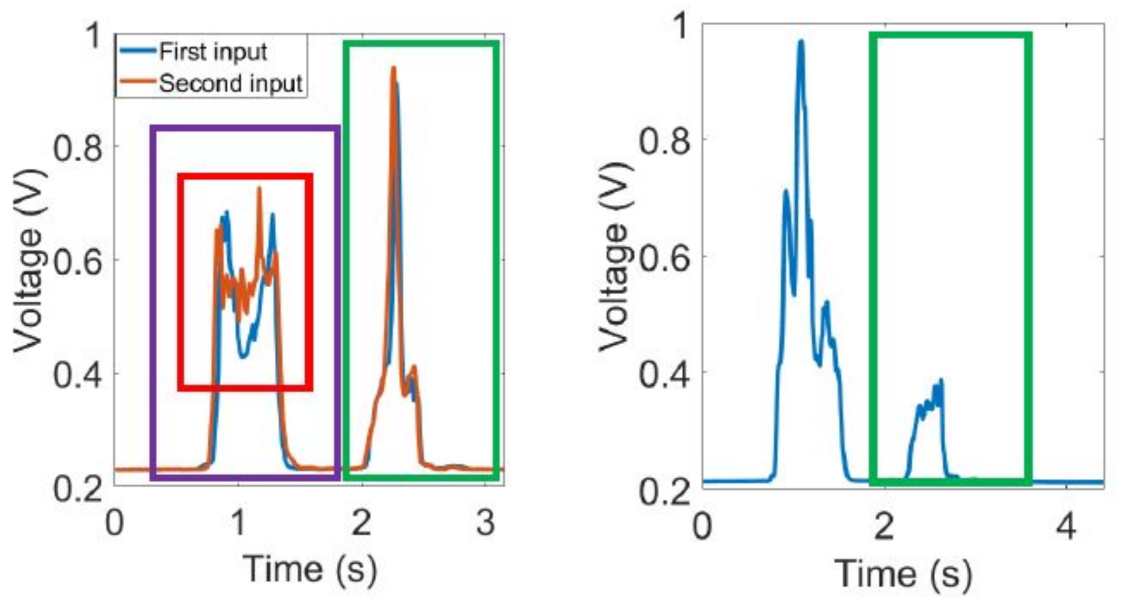
Research Goal and Insights

- Objective
  - Do not alter original interaction method of PIN input
  - Can effectively defend against shoulder-surfing attacks
- Basic idea
  - Embedding a light sensor on the PIN pad
  - PIN input will impact the amount of received light
  - Checking whether the newly detected light signal match well with those of the normal user



Research Goal and Insights

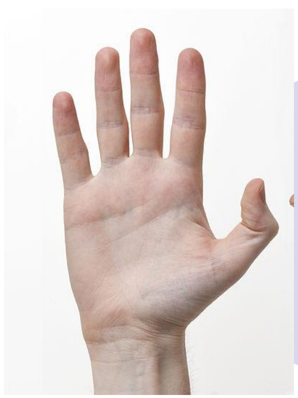
- Insights against simple PIN replay attacks
  - Different users have different input behaviors for the same PIN

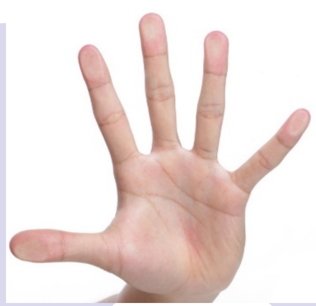


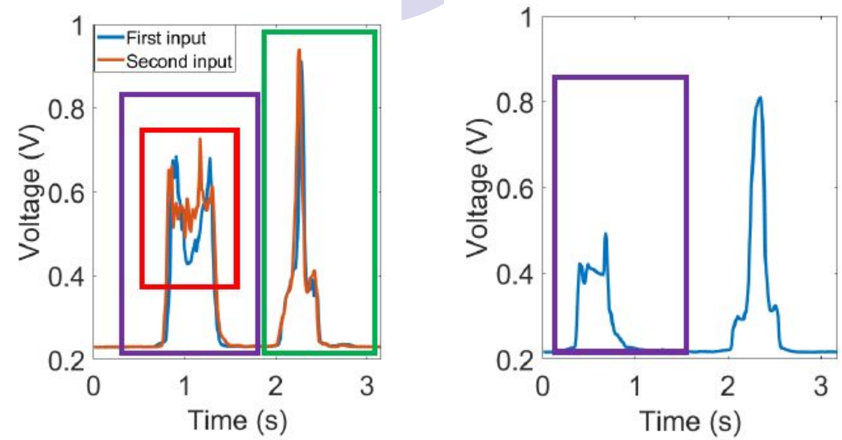
(a) Normal user. (b) Simple replay attack

Research Goal and Insights

- Insights against strong PIN replay attacks
  - Biological differences exist among hands of different people







(a) Normal user.

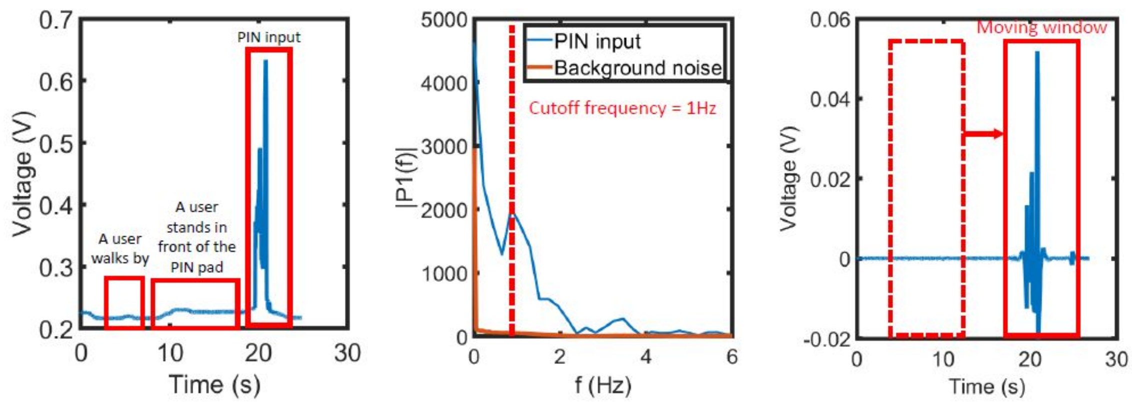
(c) Strong replay attack

Challenges

- Detecting PIN input from raw light intensity signal
- Extracting useful features from detect PIN input
- Selecting proper classification model to determine whether PIN input is from the normal user

Solutions

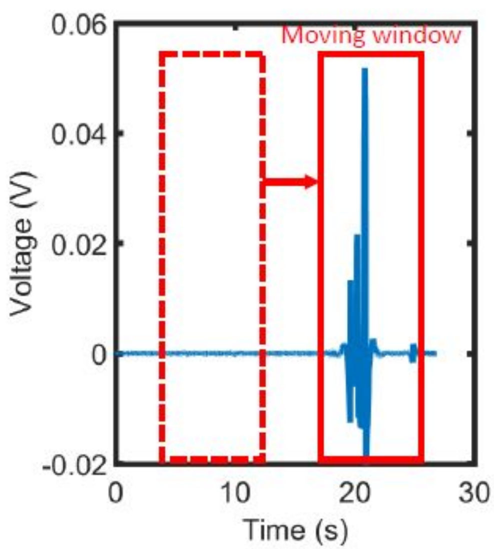
- Detecting PIN input
  - PIN input generates much larger variance to raw light signal compared with environmental noise
  - The influence of PIN input lies at low frequency

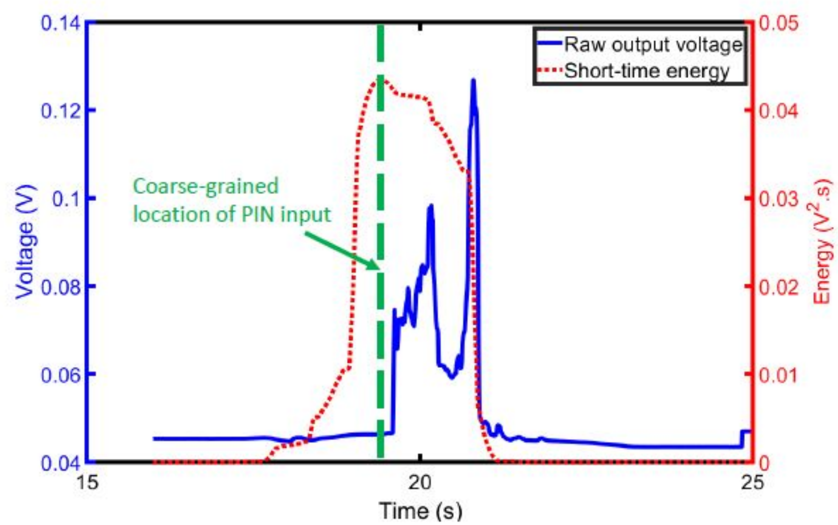


(a) The raw output voltage signal. (b) Fast Fourier transform of the raw signal. (c) The output signal of high-pass filter.

Solutions

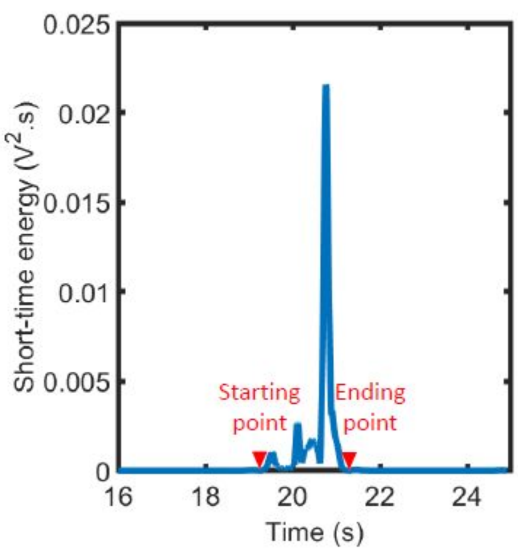
- Detecting PIN input
  - Detecting the starting point by studying the short-time energy of light signal





Solutions

- Detecting PIN input
  - The ending point can be detected using a threshold
  - Threshold: average light intensity value in the environment



Solutions

- Feature extraction
  - 34 different features in time, frequency, and time-frequency domains

Domain	**Features**
Time	Maximum, average amplitude, peak-to-peak distance, variance, root-mean-square (RMS) level, average dynamic time wrapping (DTW) distances
Frequency (fast Fourier transform)	Skewness, kurtosis, mean value, median value, variance, and peak-to-peak distance

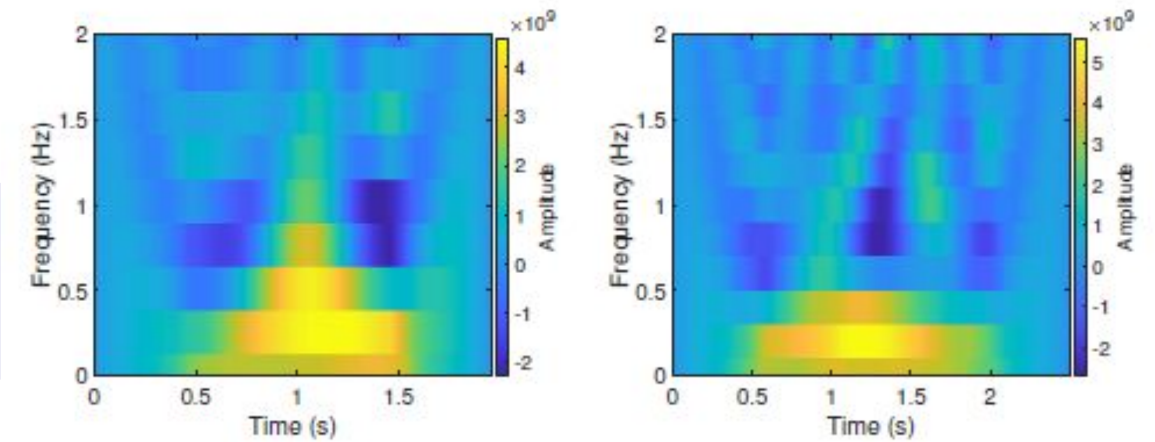
Solutions

- Feature extraction
  - 34 different features in time, frequency, and time-frequency domains

Domain	Features
Time-frequency	**Maximal overlap discrete wavelet transform:** mean value, peak-to-peak distances, RMS, and variance
	Wigner-Ville distribution location of the minimal amplitude and its amplitude value, and standard deviation of the energy distribution for each frequency frame under 2 Hz

Solutions

- Feature extraction
  - Example: Wigner-Ville distribution



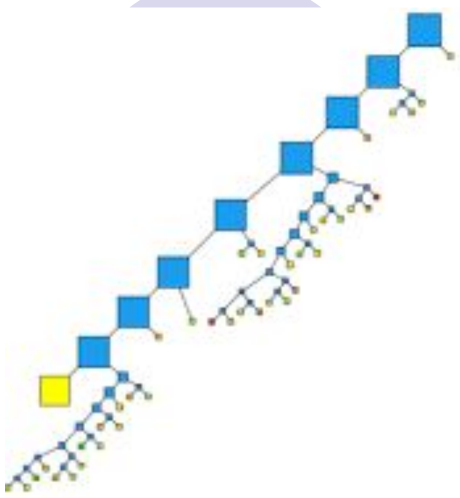
(b) The low-frequency Wigner-Ville distribution of the victim.

(c) The low-frequency Wigner-Ville distribution of the strong attacker.

$$WVD_G(t,f) = \sum_{k=-n}^{n} G(t+\frac{k}{2})G^*(t-\frac{k}{2})e^{\frac{-j2\pi fk}{n}}, \qquad (3)$$

Solutions

- Classification
  - Binary classifier based on Multiple Additive Regression Tree
    - Robust to various types of features with different scales and units
    - Features extracted from different domains may not be totally independent of each other



$$F_m(\mathbf{x}) = F_{m-1}(\mathbf{x}) + b_m h(\mathbf{x}; \mathbf{a})$$

Evaluation

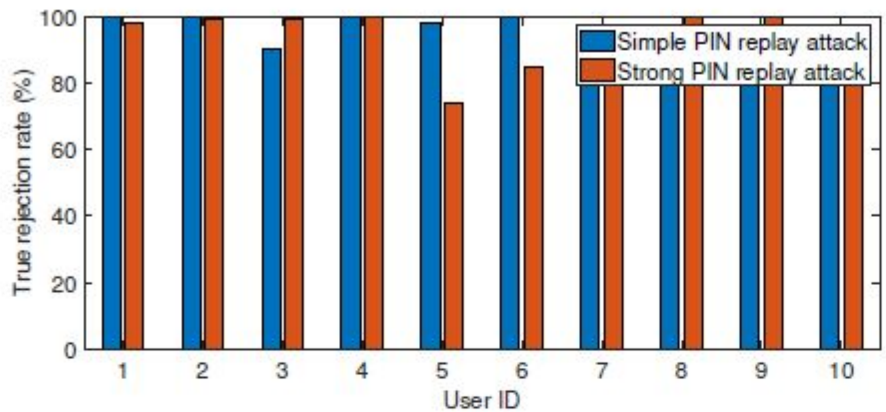
- Prototype
  - Five components
    - A prototype PIN pad (made by cardboard)
    - An LDR-based ambient light sensor
    - An analog-to-digital converter
    - A light source (WORKRITE ERGONOMIC VERANO LED array)
    - A data sink and processing center (Raspberry Pi 3 b+)

Evaluation

- Overall performance (with attackers' data)
  - Average true acceptance rate of 95% for legitimate users
  - Average true rejection rate of 98% for simple attackers
  - Average true rejection rate of 96% for strong attackers

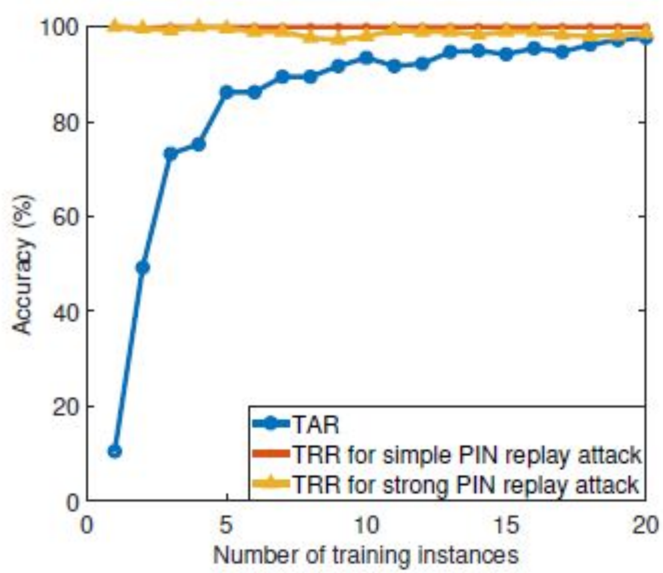
Evaluation

- Overall performance (without attackers' data)
  - Average true rejection rate of 96.8% for simple attackers
  - Average true rejection rate of 93.6% for strong attackers



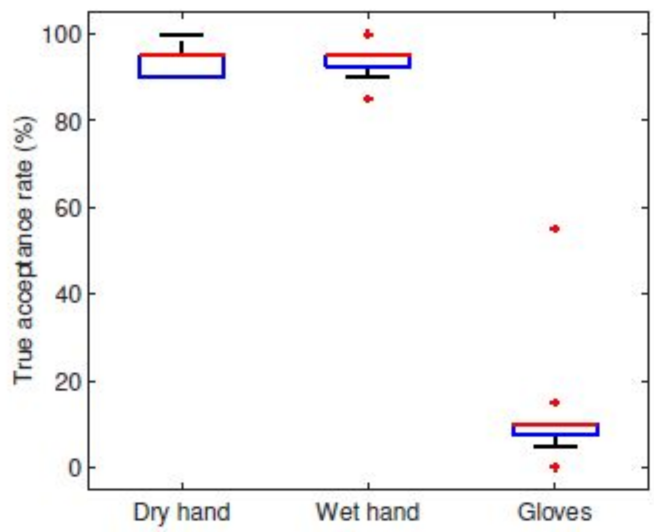
Evaluation

- Impact of training dataset size
  - High performance when only 10 instances are available



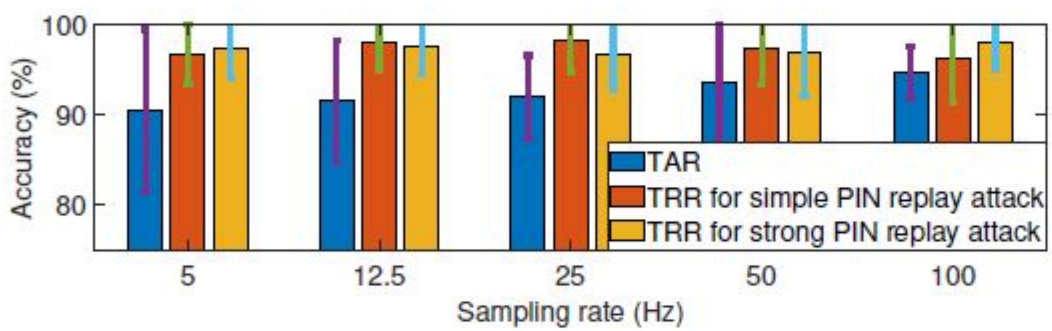
Evaluation

- Impact of hand conditions
  - Work well without gloves



Evaluation

- Impact of sampling rates
  - High performance when sampling rate is only 12.5Hz



Conclusion

- Propose a new system to defend against PIN replay attacks by leveraging the biometrics in the received light intensity that is influenced by PIN input

- Experimental results show that LightDefender can achieve an average true acceptance rate of 95% for normal users and correctly reject two types of PIN replay attacker with average true rejection rates of at least 93.6%

Thanks you

Q&A