Implicit Sensor-based Authentication of Smartphone Users with Smartwatch

Wei-Han Lee

Ruby Lee

June 18, 2016

PRINCETON
UNIVERSITY

Motivation

- Personal and sensitive information
  - SMS
  - Email
  - Geo-information
  - Social relationships
  - Bank accounts

Can password protect us?

- What if the attacker takes over the phone after we login?

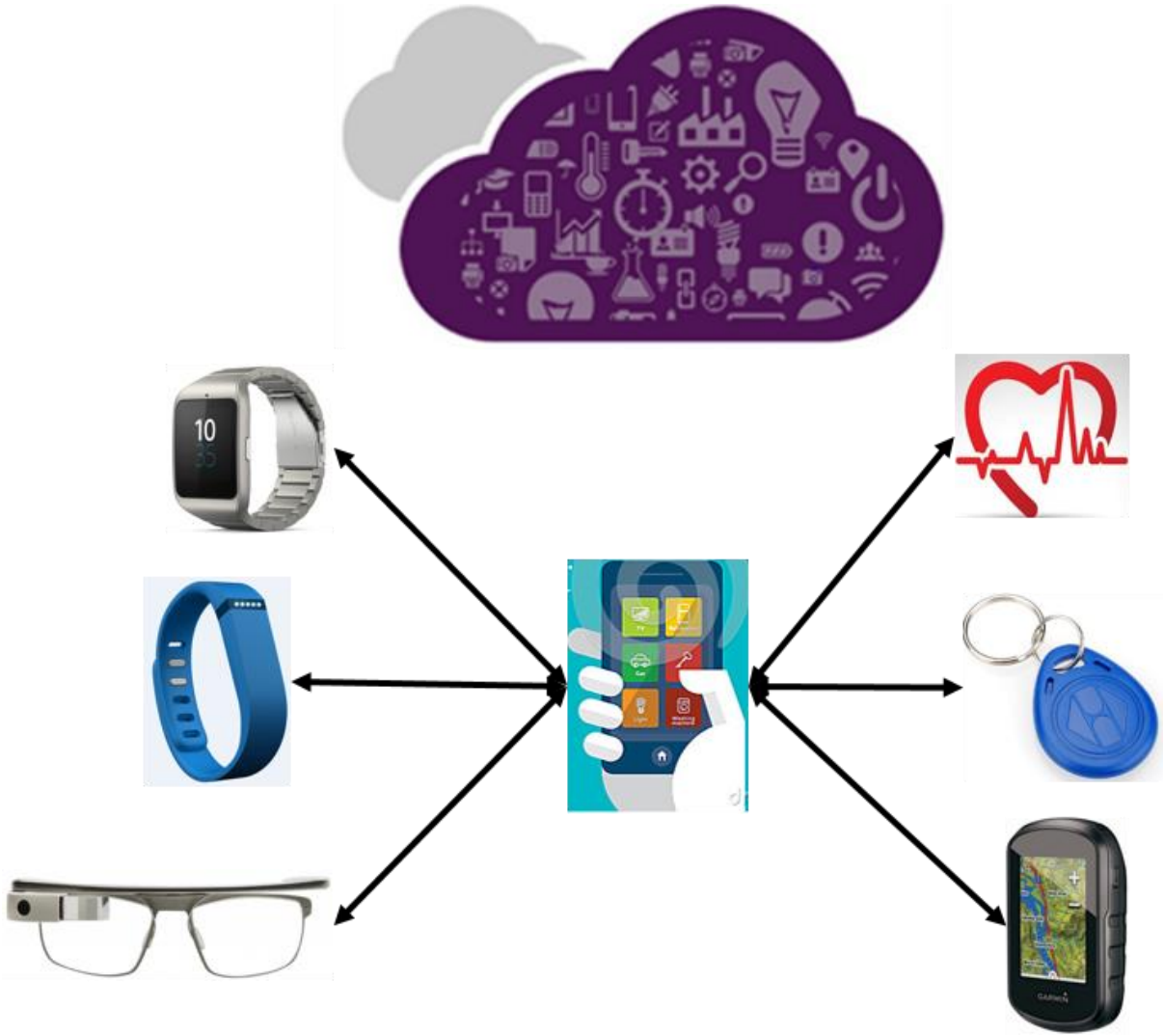
Motivation

- Implicit and continuous re-authentication is required!!!

Motivation

Features of smartphones

Auxiliary Information (Smartwatch)



Outline

- Usage scenario and threat model
- Architecture
- Algorithm
- Experimental results
- Conclusions

Usage Scenario and Threat model

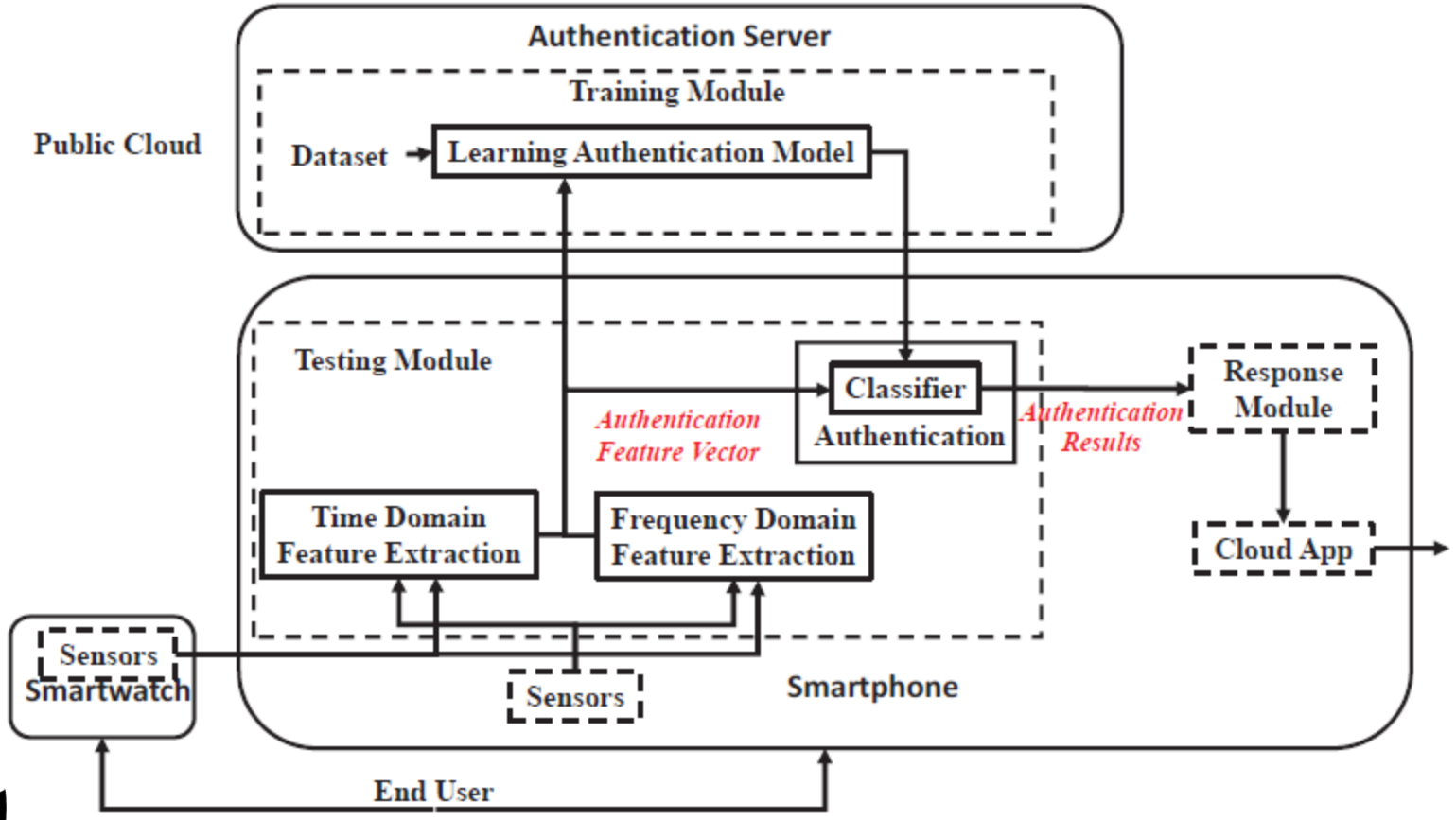
- Threat model

  The attacker steals smartphone, or takes over the user's smartphone after the legitimate user has logged in.

- Usage Scenario

  After the user enrolls into the authentication system, the system continuously and implicitly monitors and alerts when the system detects abnormal usage.

Architecture



Sensors

- Accelerometer, Gyroscope
  - No permission
  - Common
  - Not privacy sensitive
  - Different representation of user's behavior

Features

- Time domain

$$SP_i^t(k) = [mean(S_i(k)),\ var(S_i(k)),\ max(S_i(k)),\ min(S_i(k))]$$

- Frequency domain

$$SP_i^f(k) = [energy(S_i(k)), freq(S_i(k)), energy_{fre}(S_i(k))]$$

Kernel Ridge Regression

Objective function

$$\boldsymbol{w}^* = \text{argmin}_{\boldsymbol{w}\in\mathbb{R}^d} \rho\|\boldsymbol{w}\|^2 + \sum_{k=1}^{N}(\boldsymbol{w}^T\boldsymbol{x}_k - y_k)^2$$

Solution

$$\boldsymbol{w}^* = \boldsymbol{\Phi}[\boldsymbol{K} + \rho\boldsymbol{I}_N]^{-1}\boldsymbol{y}$$

Where

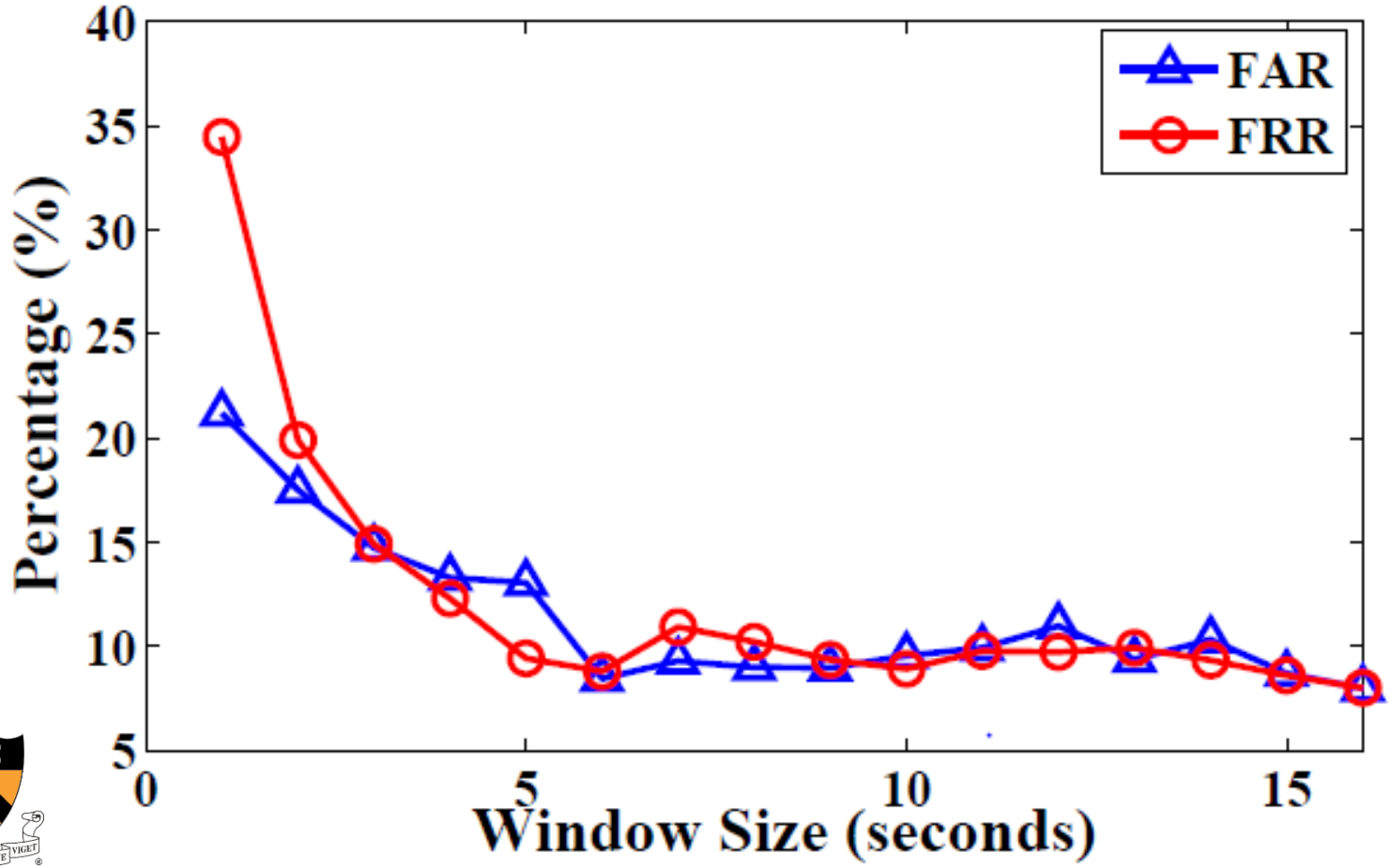
$$\boldsymbol{\Phi} = [\vec{\boldsymbol{\phi}}(\boldsymbol{x}_1)\vec{\boldsymbol{\phi}}(\boldsymbol{x}_2)\cdots\vec{\boldsymbol{\phi}}(\boldsymbol{x}_N)]$$

$$\boldsymbol{K} = \boldsymbol{\Phi}^T\boldsymbol{\Phi}$$

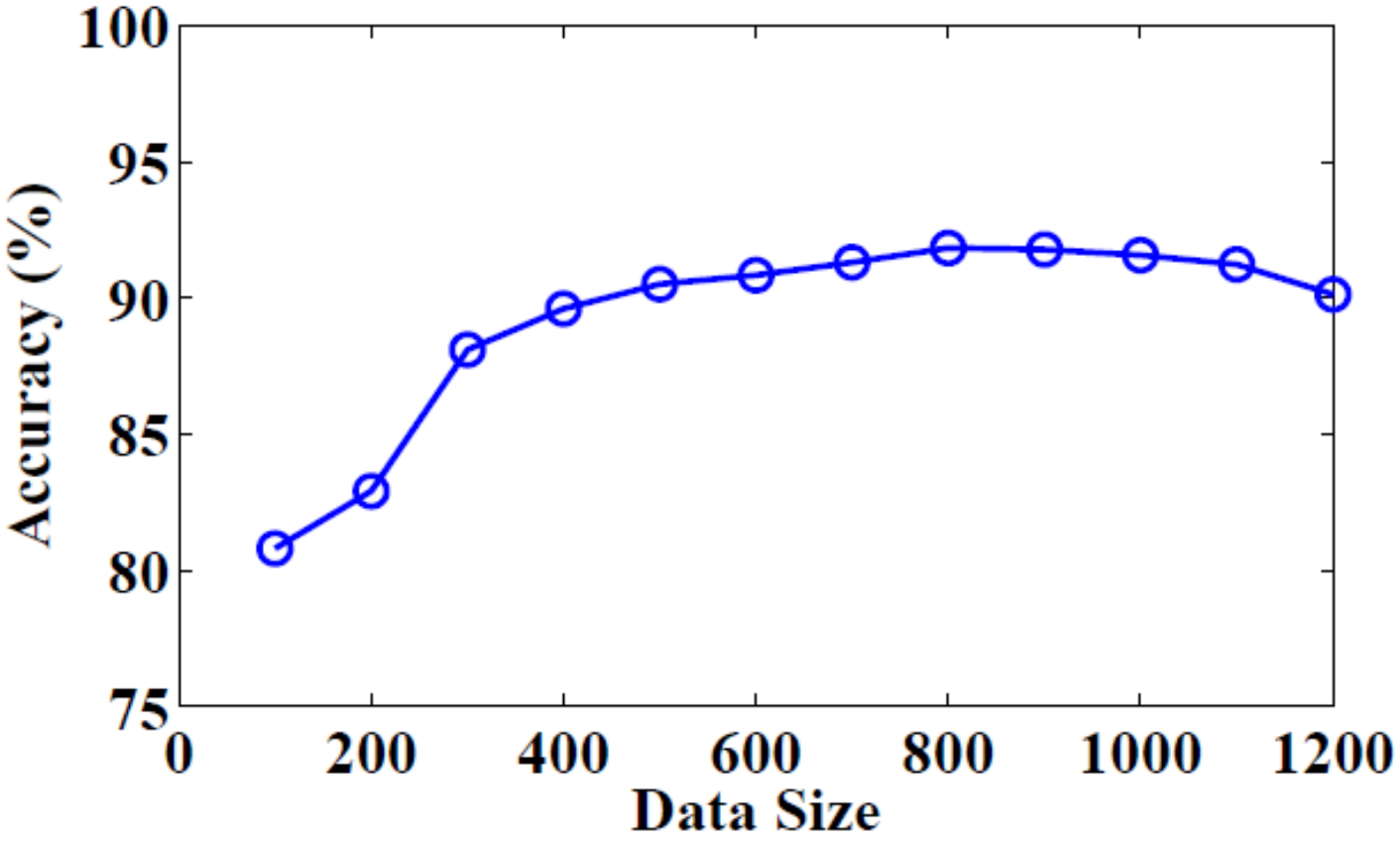
Data Collection

- Nexus 5, Moto 360
- 20 users
- 50 Hz

Parameters – Window Size



Parameters – Data Size



Authentication Performance

Device	FRR	FAR	Accuracy
Smartphone	22.3%	13.4%	83.2%
Smartphone& Smartwatch	8.3%	7.5%	92.1%

Security Analysis

- Mimicry attack
  - 90% attackers can be detected in 18s
  - All attackers can be detected in 24s

Performance evaluation

CPU is 4% on average

Power consumption is 2% per hour

Conclusions

- Implicit and continuous re-authentication
- Time and frequency domain features
- Multiple devices as auxiliary information

Thanks!