

Learning Sensitive Indoor Location From Unprotected Sensors On Mobile Devices

Huadi Zheng(Hardy), Haibo Hu

Department of Electronic and Information Engineering

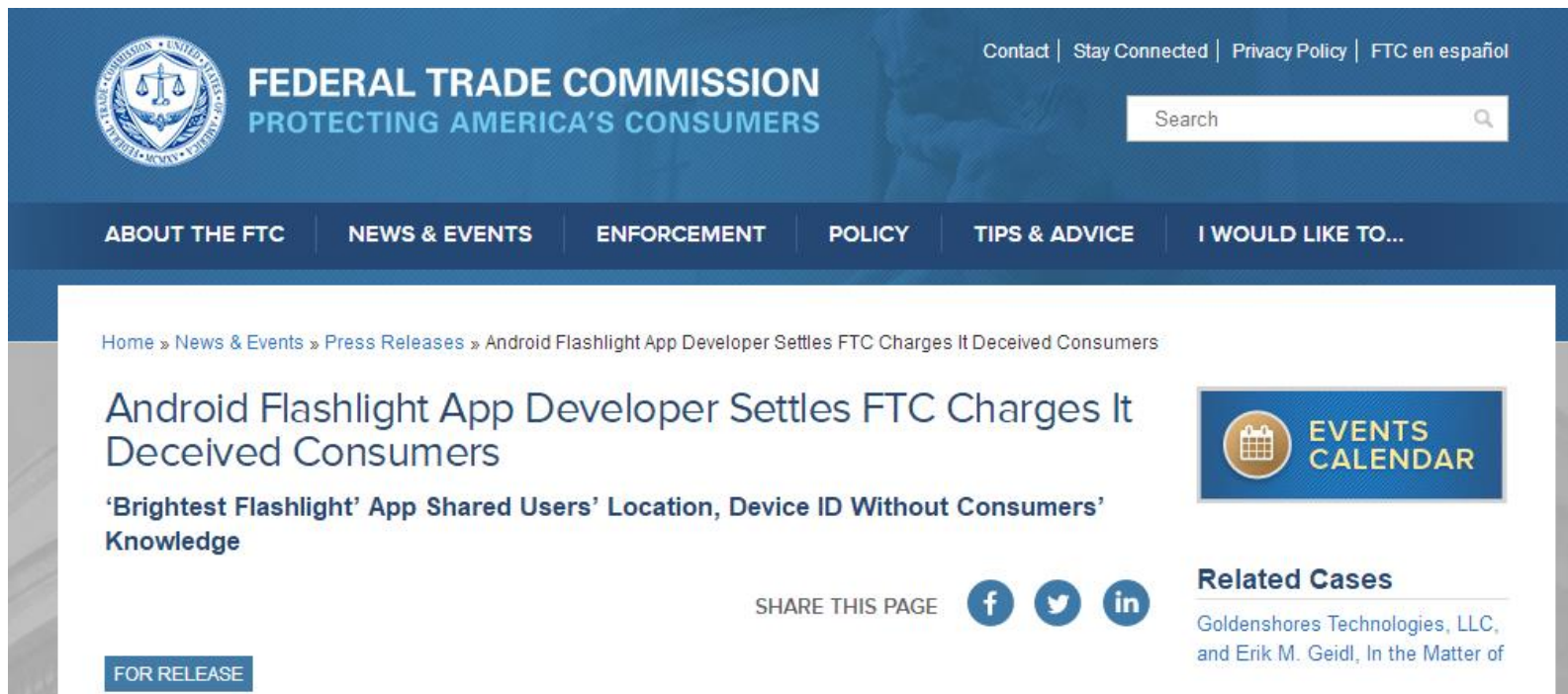
The Hong Kong Polytechnic University

Privacy Concerns

- Data collection scandal and protection



Particularly, Mobile Data



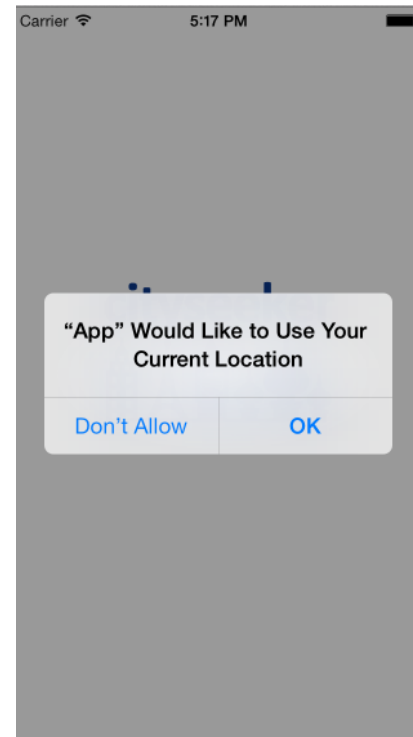
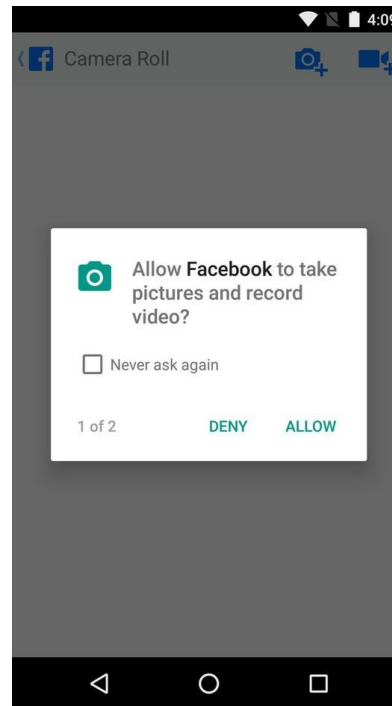
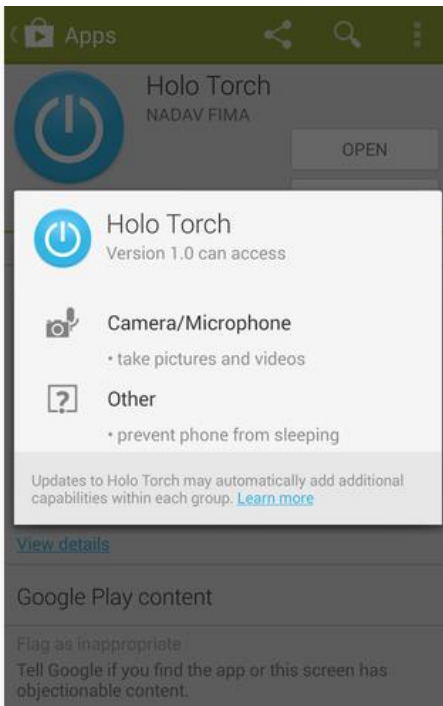
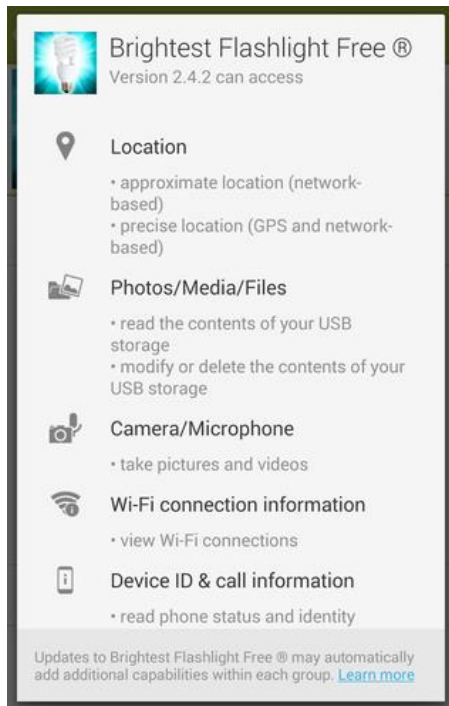
The screenshot shows the FTC website with the following elements:

- Header:**
 - FTC Seal and Logo: **FEDERAL TRADE COMMISSION**, **PROTECTING AMERICA'S CONSUMERS**
 - Navigation links: [Contact](#) | [Stay Connected](#) | [Privacy Policy](#) | [FTC en español](#)
 - Search bar with the text "Search" and a magnifying glass icon.
- Menu:**
 - [ABOUT THE FTC](#)
 - [NEWS & EVENTS](#)
 - [ENFORCEMENT](#)
 - [POLICY](#)
 - [TIPS & ADVICE](#)
 - [I WOULD LIKE TO...](#)
- Breadcrumbs:** [Home](#) » [News & Events](#) » [Press Releases](#) » [Android Flashlight App Developer Settles FTC Charges It Deceived Consumers](#)
- Main Content:**
 - ## Android Flashlight App Developer Settles FTC Charges It Deceived Consumers
 - ### 'Brightest Flashlight' App Shared Users' Location, Device ID Without Consumers' Knowledge
- Events Calendar:** A blue button with a calendar icon and the text **EVENTS CALENDAR**.
- Related Cases:**
 - Related Cases**
 - Goldenshores Technologies, LLC, and Erik M. Geidl, In the Matter of
- Share This Page:**
 - Text: **SHARE THIS PAGE**
 - Icons for Facebook (f), Twitter (t), and LinkedIn (in).
- FOR RELEASE:** A blue button with the text **FOR RELEASE**.

Various Sensors

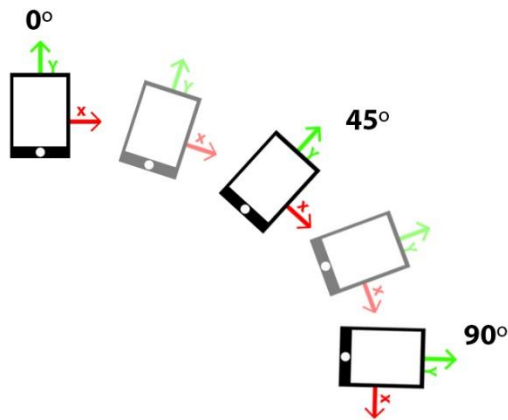
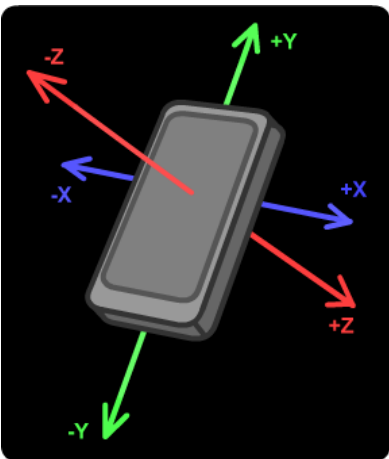


Permission Mechanism



Unprotected

Motion Sensors: Accelerometer, Gyroscope...

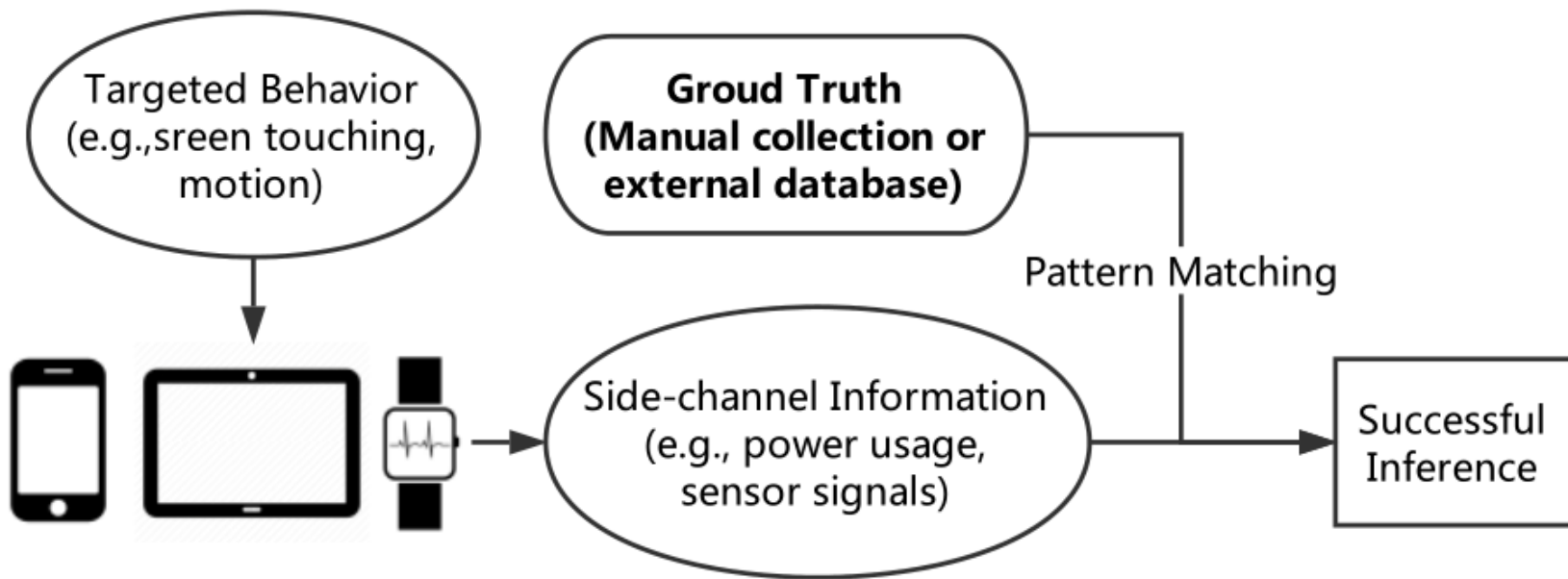


Unprotected

Ambient Sensors: Magnetometer, Barometer, Light Sensor, Thermal Sensor ...



Side-channel Attack

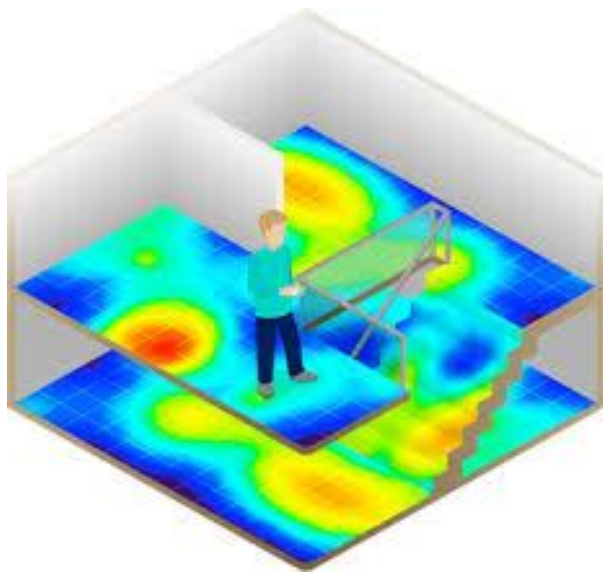


[1] S. Narain, T. D. Vo-Huu, K. Block and G. Noubir, "Inferring User Routes and Locations Using Zero-Permission Mobile Sensors," *2016 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, 2016, pp. 397-413.

[2] Y. Michalevsky, A. Schulman, G. A. Veerapandian, D. Boneh, G. Nakibly, "Powerspy: Location tracking using mobile device power analysis", *Proceedings of the 24th USENIX Conference on Security Symposium*, pp. 785-800, Aug. 2015

Key Observations

- Indoor? Complicated Design---> Pattern
- Sensitive? Victims Frequently Visit



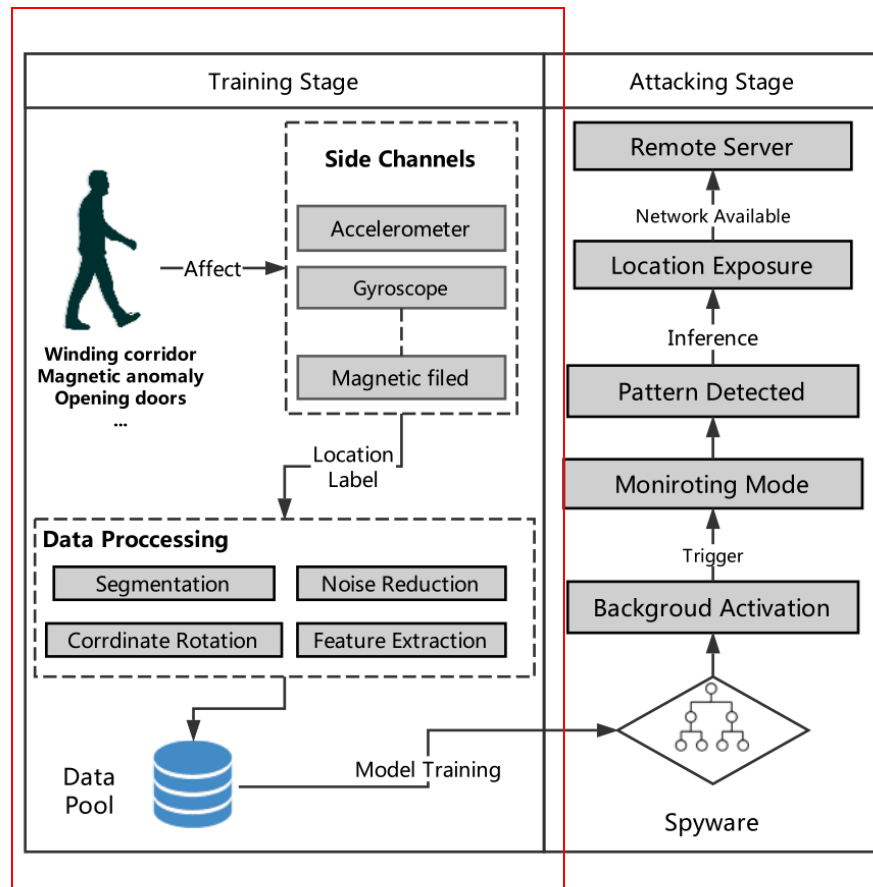
Question

- Unprotected sensors as side channels
- Feasibility of detecting sensitive indoor locations when users pass by?
- ONE location is enough

System Design

Training phase:

- Target identification
- Data collection
- Data processing
- Model construction



Sensitive Locations

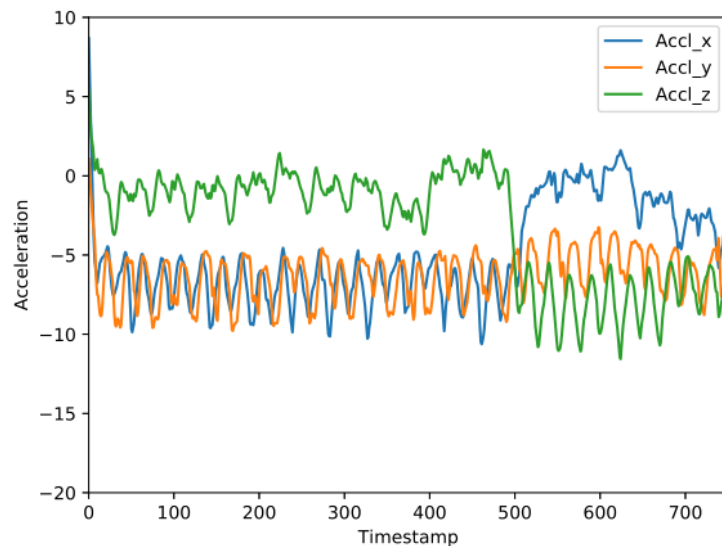
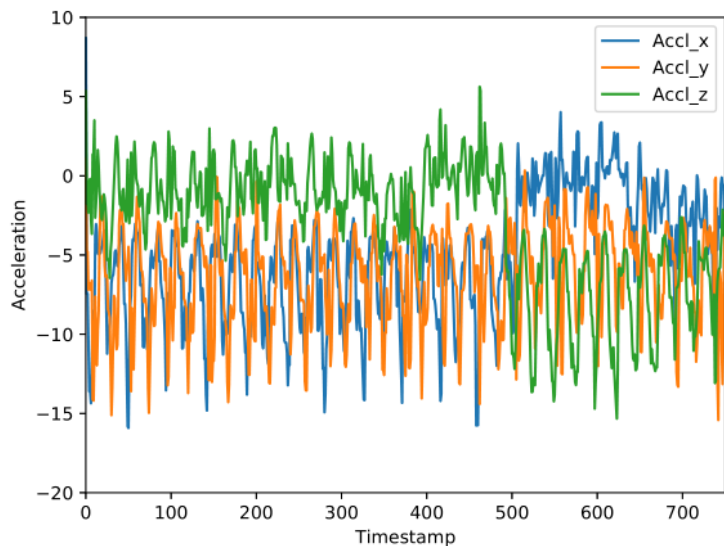


Just Need a Label

- Quick Self-developed Dataset
- Beacons, Wi-Fi, By Hand



Pre-processing



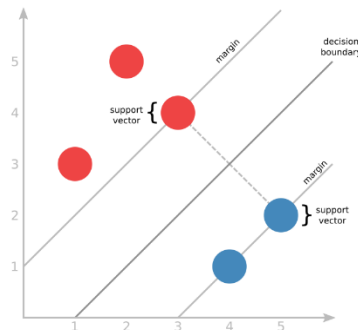
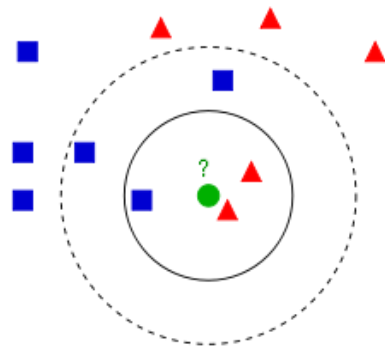
Build A Classifier

- Naive Bayesian
- K Nearest Neighbors
- Decision Tree
- Random Forest
- Support Vector Machine
- Neural Network

$$P(c|x) = \frac{P(x|c)P(c)}{P(x)}$$

Labels in the diagram:
- $P(c|x)$ is labeled as Posterior Probability.
- $P(x|c)$ is labeled as Likelihood.
- $P(c)$ is labeled as Class Prior Probability.
- $P(x)$ is labeled as Predictor Prior Probability.

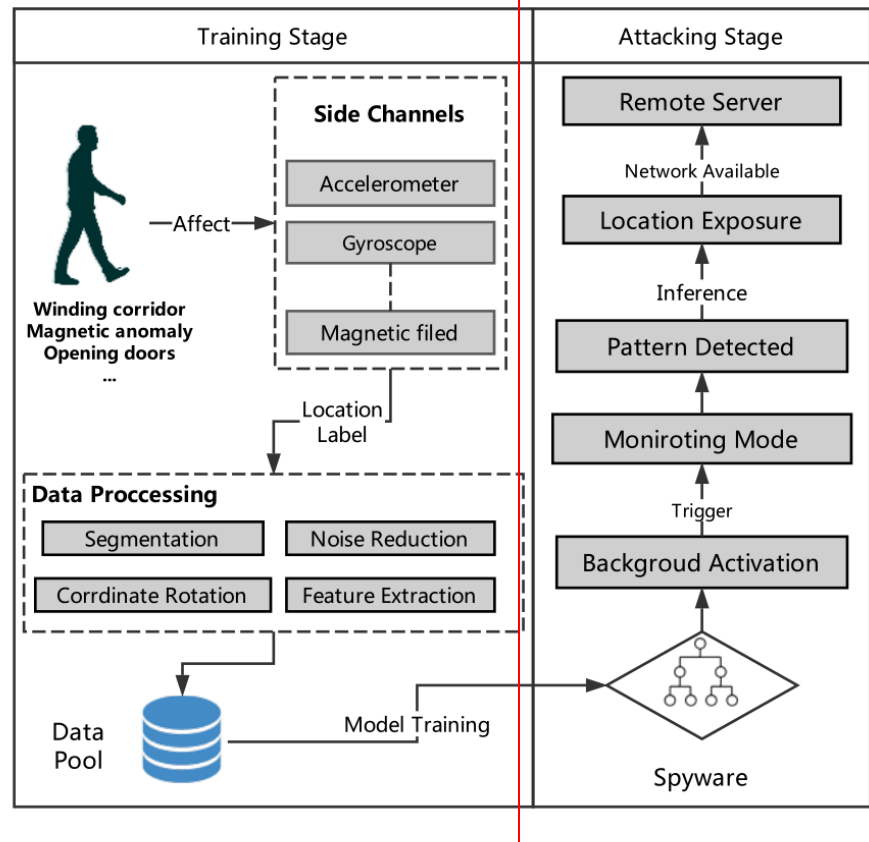
$$P(c|X) = P(x_1|c) \times P(x_2|c) \times \cdots \times P(x_n|c) \times P(c)$$



System Design

Attack phase:

- Spyware installed
- Monitoring
- Pattern occurs
- Deliver to attacker



Risk of Leakage

- 15 Locations, 5 devices, 4 sensors, 5 victims

Devices	LG G3, Google Pixel, HTC U Ultra, Redmi Note4X, Samsung Galaxy S8
Selected Sensors	Accelerometer, Gyroscope, Magnetic Field Sensor, Linear Acceleration Sensor

Recognizer	Weighted Average F1-score
Decision Tree + Euclidean Norm(DTEN)	41.15%
Decision Tree + Rotation Matrix(DTRM)	52.09%
Random Forest + Euclidean Norm(RFEN)	62.86%
Random Forest + Rotation Matrix(RFRM)	73.26%

Threatening?

- Immune to Antivirus
- Massive Users, Cross Reference
- Plus Social Engineering

Upcoming Focus

Potential Defense

- Permission List
- Background Limit
- Frequency Limit
- Functional API

Attack Improve

- Stateful Inference
- Sensor Fusion
- Webpage Implant
- More Sensors

Thank You