ipShield: A Framework For Enforcing Context-Aware Privacy

Supriyo Chakraborty, Chenguang Shen, Kasturi Rangan Raghavan, Yasser Shoukry, Matt Millar, Mani Srivastava
From sensor data to inferences
From sensor data to inferences
From sensor data to inferences

Sensor Data

Apps

Inferences
Utility Providing
Fitness
mHealth
Lifelogging
Phone operation
From sensor data to inferences

Sensor Data

Apps

Inferences

Utility Providing
- Fitness
- mHealth
- Lifelogging
- Phone operation

Sensitive
- Location
- Password
- Media habits
- Physiological habits
From sensor data to inferences

Sensor Data → Apps → Inferences

Sensor Data:
- Location
- Password
- Media habits
- Physiological habits

Apps:
- Fitness
- mHealth
- Lifelogging
- Phone operation

Inferences:
- Utility Providing
- Sensitive
From sensor data to inferences

Sensor Data → Apps → Inferences

**Apps**
- Social media
- Fitness
- mHealth
- Lifelogging
- Phone operation

**Inferences**
- Utility Providing
- Fitness
- mHealth
- Lifelogging
- Phone operation

**Sensitive**
- Location
- Password
- Media habits
- Physiological habits
From sensor data to inferences

Sensor Data -> Apps -> Inferences

Apps:
- Social Media (e.g., Facebook, Twitter)
- Fitness Apps
- Lifelogging

Inferences:
- Utility Providing:
  - Fitness
  - mHealth
  - Lifelogging
  - Phone operation

Sensitive:
- Location
- Password
- Media habits
- Physiological habits
From sensor data to inferences

Apps

Sensor Data

Inferences
Utility Providing
Fitness
mHealth
Lifelogging
Phone operation

Sensitive
Location
Password
Media habits
Physiological habits
Protecting inference privacy while providing utility

**Apps**
- [Icon 1]
- [Icon 2]
- [Icon 3]
- [Icon 4]
- [Icon 5]

**Sensor Data**
- [Icon 6]
- [Icon 7]
- [Icon 8]
- [Icon 9]
- [Icon 10]

**Inferences**
- Utility Providing:
  - Fitness
  - mHealth
  - Lifelogging
  - Phone operation

**Sensitive**
- Location
- Password
- Media habits
- Physiological habits

**Whitelist**

**Blacklist**
Protecting inference privacy while providing utility

Apps

Inference firewall

Inferences
- Utility Providing
  - Fitness
  - mHealth
  - Lifelogging
  - Phone operation
- Sensitive
  - Location
  - Password
  - Media habits
  - Physiological habits

Sensor Data

Whitelist

Blacklist
Protecting inference privacy while providing utility

- **Inferences**
  - Utility Providing
    - Fitness
    - mHealth
    - Lifelogging
    - Phone operation

- **Sensitive**
  - Location
  - Password
  - Media habits
  - Physiological habits

- **Inference firewall**

- **Sensor Data**

- **Apps**
  - Fitness
  - mHealth
  - Lifelogging
  - Phone operation
Prior notions of privacy in databases

\[ D := \{ \]
\[ P = \text{personal identifiers}, \ (\text{name, ID}) \]
\[ Q = \text{quasi identifiers}, \ (\text{age, zip code}) \]
\[ V = \text{measurement values} \ (\text{sensor data}) \]
Prior notions of privacy in databases

Population Scale Database

1. K-anonymity
2. L-Diversity
3. t-closeness

Privacy $M=\langle P',Q',V \rangle$

inference = identity

D := {
P = personal identifiers, (name, ID)
Q = quasi identifiers, (age, zip code)
V = measurement values (sensor data)}
Prior notions of privacy in databases

1. K-anonymity
2. L-Diversity
3. t-closeness

D := {
P = personal identifiers, (name, ID)
Q = quasi identifiers, (age, zip code)
V = measurement values (sensor data)

M = R(<P, Q, V>) + noise

inference = identity

Population Scale Database

Sensor Data Capture

Data Processing

Privacy M = <P', Q', V>

Data Processing

Differential Privacy

inference = membership
Prior notions of privacy in databases

Sensor Data Capture → Data Processing

Aggregate Queries

M:=(P, Q, V')

Sharing an Individual’s data
Prior notions of privacy in databases

- Sensor Data Capture
- Data Processing
- Aggregate Queries
- Sharing an Individual’s data

Privacy of Data (secrecy)
Privacy of Identity (anonymity)
Privacy of Behavior
Controls provided by current systems are insufficient

Android Manifest

Do you want to install this application?

Allow this application to:

- Network communication
  - full Internet access

- Your personal information
  - read contact data

- Your accounts
  - Act as account authenticator, manage the accounts list

- Storage
  - modify/delete USB storage contents

- System tools

Binary Policies

Install  Cancel
Controls provided by current systems are insufficient

pDroid

Static Policies
Controls provided by current systems are insufficient

ProtectMyPrivacy

Invite to Facebook
121 contacts found

Hoaatnnj Eoprph
Hht@pneraoenh.pjuon.tatdcoel

Hoaatnnj Ongy
Tcowa@mrd.tngohyo.nolnnjal

Hoaatnnj Witrehs
Toljrmelaiocs@ihnyogemgon.w

Iaastnab Oeogrtd
14193728116+

Iarntm
79757701 300

Ickr Dinso
Ociem@tcsikm.r

Ieema Ngfndiaerh
Di@ooyaheemmcrer.o

Share Random Data
Design requirements of ipShield
Design requirements of ipShield

Combination of benign sensors can be used for privacy attack.
Design requirements of ipShield

- GPS
- Network
- Accelerometer
- Microphone
- Light

Sensor Monitoring
Design requirements of ipShield

- GPS
- Network
- Accelerometer
- Microphone
- Light
- Location
  - Transportation Mode
  - Password/PIN
  - Stress
  - Media Watching
- Sensor Monitoring
- Privacy Abstraction
Design requirements of ipShield

- User Privacy Preferences
  - Whitelist/Blacklist
    - Translation Algorithms
      - Privacy Rules on Sensors
        - Rule Enforcement
  - Sensor Monitoring
  - Privacy Abstraction
Design requirements of ipShield

- User Privacy Preferences
- Whitelist/Blacklist
  - Translation Algorithms
  - Privacy Rules on Sensors
  - Rule Enforcement
- Sensor Monitoring
- Privacy Abstraction
- Rule Recommender
Design requirements of ipShield

- User Privacy Preferences
- Whitelist/Blacklist
- Translation Algorithms
- Privacy Rules on Sensors
- Rule Enforcement

- Sensor Monitoring
- Privacy Abstraction
- Rule Recommender
- Manual Override (Rules)
Design requirements of ipShield

User Privacy Preferences

Whitelist/Blacklist

Translation Algorithms

Privacy Rules on Sensors

Rule Enforcement

Sensor Monitoring

Privacy Abstraction

Rule Recommender

Manual Override (Rules)

Rule Enforcement
Rule Recommender

Whitelist/Blacklist

Privacy rules on sensors
Recommender objective

Generate a plan for **context-aware obfuscation of sensor data** depending on the **prioritized whitelist and blacklist** such that

- **accuracy of whitelist is maximized** and
- **accuracy of blacklist is minimized**.
Divide-and-conquer strategy

Recommend a plan containing 

**allow/deny rules for sensors**

depending on the

**prioritized whitelist and blacklist**

such that

**accuracy of whitelist is maximized and accuracy of blacklist is minimized.**
Divide-and-conquer strategy

Recommend a plan containing

allow/deny rules for sensors
depending on the

prioritized whitelist and blacklist
such that

accuracy of whitelist is maximized and
accuracy of blacklist is minimized.

+ 

Support manual override/configuration of
fine-grained context-aware rules
Elements of the problem: accuracy
Elements of the problem: accuracy

<table>
<thead>
<tr>
<th>Inference Database (A)</th>
<th>Activity</th>
<th>Location</th>
<th>OnScreen Taps</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPS+Acc+Gyro</td>
<td>95%</td>
<td>97%</td>
<td>80%</td>
</tr>
<tr>
<td>GPS+WiFi</td>
<td>83.1%</td>
<td>97%</td>
<td>0%</td>
</tr>
<tr>
<td>GPS+GSM</td>
<td>81.7%</td>
<td>98.2%</td>
<td>0%</td>
</tr>
<tr>
<td>GSM+WiFi</td>
<td>72.9%</td>
<td>94.03%</td>
<td>0%</td>
</tr>
</tbody>
</table>
## Elements of the problem: accuracy

<table>
<thead>
<tr>
<th>Inference Database (A)</th>
<th>Activity</th>
<th>Location</th>
<th>OnScreen Taps</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPS+Acc+Gyro</td>
<td>95%</td>
<td>97%</td>
<td>80%</td>
</tr>
<tr>
<td><strong>Sensor Combination</strong></td>
<td>97%</td>
<td>97%</td>
<td>0%</td>
</tr>
<tr>
<td>GPS+GSM</td>
<td>81.7%</td>
<td>98.2%</td>
<td>0%</td>
</tr>
<tr>
<td>GSM+WiFi</td>
<td>72.9%</td>
<td>94.03%</td>
<td>0%</td>
</tr>
</tbody>
</table>
Elements of the problem: accuracy

<table>
<thead>
<tr>
<th>Inference Database (A)</th>
<th>Activity</th>
<th>Inference Type</th>
<th>OnScreen Taps</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPS+Acc+Gyro</td>
<td>95%</td>
<td></td>
<td>80%</td>
</tr>
<tr>
<td>Sensor Combination</td>
<td></td>
<td>97%</td>
<td>0%</td>
</tr>
<tr>
<td>GPS+GSM</td>
<td>81.7%</td>
<td>98.2%</td>
<td>0%</td>
</tr>
<tr>
<td>GSM+WiFi</td>
<td>72.9%</td>
<td>94.03%</td>
<td>0%</td>
</tr>
</tbody>
</table>
Elements of the problem: accuracy

<table>
<thead>
<tr>
<th>Inference Database (A)</th>
<th>Activity</th>
<th>Inference Type</th>
<th>OnScreen Taps</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPS+Acc+Gyro</td>
<td>95%</td>
<td></td>
<td>80%</td>
</tr>
<tr>
<td>Sensor Combination</td>
<td></td>
<td>Accuracy of Prediction</td>
<td>0%</td>
</tr>
<tr>
<td>GPS+GSM</td>
<td>81.7%</td>
<td>98.2%</td>
<td>0%</td>
</tr>
<tr>
<td>GSM+WiFi</td>
<td>72.9%</td>
<td>94.03%</td>
<td>0%</td>
</tr>
</tbody>
</table>
Elements of the problem: priority

\[ \text{Priority} = (p_{\text{activity}}, p_{\text{location}}, p_{\text{tap}}) \]

\[ \downarrow \quad \downarrow \quad \downarrow \]

priority = \{10, 4, 10\}
Elements of the problem: priority

\[ \text{Priority} = (p_{activity}, p_{location}, p_{tap}) \]

\[ \downarrow \quad \downarrow \quad \downarrow \]

priority = \{10, 4, 10\}

**Whitelisted inferences**

priority ↑ ⇒ allow whitelisted inferences

**Blacklisted inferences**

priority ↑ ⇒ block blacklisted inferences
Rule recommender in ipShield

\[
\max_{\Phi \in 2^N} \sum_{l \in \mathcal{W}} A(\Phi, l)2^{p_l} - \sum_{l \in \mathcal{B}} A(\Phi, l)2^{p_l}
\]

\[
\text{s.t. } \sum_{l \in \mathcal{B}, p_l = p_{max}} A(\Psi, l) = 0
\]

\(\mathcal{W} = \text{whitelist}, \mathcal{B} = \text{blacklist}, p_l = \text{priority}, \text{ and } \Phi = \text{Sensor combination}\)
Rule recommender in ipShield

\[
\max_{\Phi \in 2^N} \sum_{l \in \mathcal{W}} A(\Phi, l)2^{p_l} - \sum_{l \in \mathcal{B}} A(\Phi, l)2^{p_l}
\]

s.t. \[ \sum_{l \in \mathcal{B}, p_l = p_{max}} A(\Psi, l) = 0 \]

\( \mathcal{W} = \) whitelist, \( \mathcal{B} = \) blacklist, \( p_l = \) priority, and \( \Phi = \) Sensor combination

\[ \downarrow \]

Over all sensor combinations
Rule recommender in ipShield

\[
\max_{\Phi \in 2^N} \sum_{l \in \mathcal{W}} A(\Phi, l) 2^{pl} - \sum_{l \in \mathcal{B}} A(\Phi, l) 2^{pl}
\]

s.t. \[ \sum_{l \in \mathcal{B}, pl=p_{\text{max}}} A(\Psi, l) = 0 \]

\[ \mathcal{W} = \text{whitelist}, \mathcal{B} = \text{blacklist}, pl = \text{priority}, \text{and} \]
\[ \Phi = \text{Sensor combination} \]

\[ \Downarrow \]

Over all sensor combinations

maximize accuracy of prioritized whitelist and
Rule recommender in ipShield

\[
\max_{\Phi \in 2^N} \sum_{l \in \mathcal{W}} A(\Phi, l) 2^{p_l} - \sum_{l \in \mathcal{B}} A(\Phi, l) 2^{p_l}
\]

s.t. \[\sum_{l \in \mathcal{B}, p_l = p_{\text{max}}} A(\Psi, l) = 0\]

\[\mathcal{W} = \text{whitelist}, \mathcal{B} = \text{blacklist}, p_l = \text{priority}, \text{and} \quad \Phi = \text{Sensor combination}\]

\[\downarrow\]

Over all sensor combinations

maximize accuracy of prioritized whitelist and minimize accuracy of prioritized blacklist
Rule recommender in ipShield

\[
\max_{\Phi \in 2^N} \sum_{l \in \mathcal{W}} A(\Phi, l)2^{p_l} - \sum_{l \in \mathcal{B}} A(\Phi, l)2^{p_l} \\
\text{s.t.} \sum_{l \in \mathcal{B}, p_l = p_{\text{max}}} A(\Psi, l) = 0
\]

\(\mathcal{W}\) = whitelist, \(\mathcal{B}\) = blacklist, \(p_l\) = priority, and \(\Phi\) = Sensor combination

\[\implies\]

Over all sensor combinations

maximize accuracy of prioritized whitelist and
minimize accuracy of prioritized blacklist
such that highest priority blacklists are always blocked.
Rule recommender at work

<table>
<thead>
<tr>
<th>Activity</th>
<th>Location</th>
<th>OnScreen Taps</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPS+Acc+Gyro</td>
<td>95%</td>
<td>97%</td>
</tr>
<tr>
<td>GPS+WiFi</td>
<td>83.1%</td>
<td>97%</td>
</tr>
<tr>
<td>GPS+GSM</td>
<td>81.7%</td>
<td>98.2%</td>
</tr>
<tr>
<td>GSM+WiFi</td>
<td>72.9%</td>
<td>94.03%</td>
</tr>
</tbody>
</table>
Rule recommender at work

<table>
<thead>
<tr>
<th>Activity</th>
<th>Location</th>
<th>OnScreen Taps</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPS+Acc+Gyro</td>
<td>95%</td>
<td>97%</td>
</tr>
<tr>
<td>GPS+WiFi</td>
<td>83.1%</td>
<td>97%</td>
</tr>
<tr>
<td>GPS+GSM</td>
<td>81.7%</td>
<td>98.2%</td>
</tr>
<tr>
<td>GSM+WiFi</td>
<td>72.9%</td>
<td>94.03%</td>
</tr>
</tbody>
</table>
Rule recommender at work

<table>
<thead>
<tr>
<th>Activity</th>
<th>Location</th>
<th>OnScreen Taps</th>
<th>Priority1 {10, 4, 10}</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPS+Acc+Gyro</td>
<td>95%</td>
<td>97%</td>
<td>80%</td>
</tr>
<tr>
<td>GPS+WiFi</td>
<td>83.1%</td>
<td>97%</td>
<td>0%</td>
</tr>
<tr>
<td>GPS+GSM</td>
<td>81.7%</td>
<td>98.2%</td>
<td>0%</td>
</tr>
<tr>
<td>GSM+WiFi</td>
<td>72.9%</td>
<td>94.03%</td>
<td>0%</td>
</tr>
</tbody>
</table>
## Rule recommender at work

<table>
<thead>
<tr>
<th></th>
<th>Activity</th>
<th>Location</th>
<th>OnScreen Taps</th>
<th>Priority1 {10, 4, 10}</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPS+Acc+Gyro</td>
<td>95%</td>
<td>97%</td>
<td>80%</td>
<td>0</td>
</tr>
<tr>
<td>GPS+WiFi</td>
<td>83.1%</td>
<td>97%</td>
<td>0%</td>
<td>835.4</td>
</tr>
<tr>
<td>GPS+GSM</td>
<td>81.7%</td>
<td>98.2%</td>
<td>0%</td>
<td>820.0</td>
</tr>
<tr>
<td>GSM+WiFi</td>
<td>72.9%</td>
<td>94.03%</td>
<td>0%</td>
<td>731.45</td>
</tr>
</tbody>
</table>

**Allow**
ipShield

Monitoring
Privacy Abstraction
Rule Recommender
Fine-grained Rules
Enforcement

Prototype implementation on Android
Sensor subsystem in android and data interception

Third Party Apps

Sensor Manager
Android Framework
Location Manager
Sensor Data
Sensor Data
Sensor Service
LocationManager Service
System Server
Android Native/Linux Kernel
Hardware

System Processes
User Processes
Sensor subsystem in Android and data interception

Third Party Apps

- Sensor Manager
- Android Framework
- Location Manager
- Sensor Data
- Sensor Service
- LocationManager Service
- System Server
- Android Native/Linux Kernel
- Hardware

System Processes
User Processes
Sensor subsystem in android and data interception

Third Party Apps

Sensor Manager  Android Framework  Location Manager

Sensor Data  Sensor Data

Sensor Service  LocationManager Service

System Server

Android Native/Linux Kernel

Hardware

System Processes  User Processes
Sensor subsystem in android and data interception

Third Party Apps

Sensor Manager | Android Framework | Location Manager

Sensor Service | Location Manager Service

System Server

Android Native/Linux Kernel

Hardware

System Processes | User Processes
Sensor subsystem in android and data interception

App and Managers run as part of the same process

- Third Party Apps
- Sensor Manager
- Android Framework
- Location Manager
- LocationManager Service
- System Server
- Android Native/Linux Kernel
- Hardware

- System Processes
- User Processes
Sensor subsystem in android and data interception

- **Third Party Apps**
  - **Sensor Manager**
  - **Location Manager**

- **Android Framework**
  - **Sensor Data**
  - **Location Data**

- **System Server**
- **Android Native/Linux Kernel**
- **Hardware**

- **System Processes**
- **User Processes**

**Legend**
- App and Managers run as part of the same process
- Services run in separate system owned processes
Implementing ipShield

**Trusted App part of ipShield**

- **Sensor Manager**
- **Location Manager**

**Whitelist and Blacklist of inference**

**ipShield**

- Monitoring
- Privacy Abstraction
- Rule Recommender
- Fine-grained Rules
- Enforcement

**System Server**

- SensorService
- LocationManagerService

**Native Runtime**

**Hardware**

- System Processes
- User Processes
- Trusted App (User Process)
Implementing ipShield

- Trusted App part of ipShield
  - Whitelist and Blacklist of inference
  - Semantic Firewall Configurator
  - SensorManager
  - FirewallConfigManager
  - LocationManager
  - SensorService
  - FirewallConfigService
  - LocationManagerService
  - System Server
  - Native Runtime
  - Hardware

- System Processes
- User Processes
- Trusted App (User Process)

- ipShield
  - Monitoring
  - Privacy Abstraction
  - Rule Recommender
  - Fine-grained Rules
  - Enforcement
Implementing ipShield

Trusted App part of ipShield

Semantic Firewall Configurator

Inference Database

Sensor Manager

FirewallConfig Manager

Location Manager

SensorService

FirewallConfig Service

LocationManager Service

System Server

Native Runtime

Hardware

System Processes

User Processes

Trusted App (User Process)

ipShield

Monitoring

Privacy Abstraction

Rule Recommender

Fine-grained Rules

Enforcement

Whitelist and Blacklist of inference
Implementing ipShield

Trusted App part of ipShield

Semantic Firewall Configurator

Rule Recommender

Inference Database

Sensor Manager

FirewallConfig Manager

Location Manager

SensorService

FirewallConfig Service

LocationManager Service

System Server

Native Runtime

Hardware

System Processes  User Processes  Trusted App (User Process)
Implementing ipShield

Whitelist and Blacklist of inference

Context Engine

Direct Configurator

Semantic Firewall Configurator

Rule Recommender

Inference Database

Sensor Manager

FirewallConfig Manager

Location Manager

SensorService

FirewallConfig Service

LocationManager Service

System Server

Native Runtime

Hardware

System Processes

User Processes

Trusted App (User Process)

Monitoring

Privacy Abstraction

Rule Recommender

Fine-grained Rules

Enforcement
Implementing ipShield

**Trusted App part of ipShield**

- Context Engine
- Direct Configurator
- Semantic Firewall Configurator
- Rule Recommender
- Inference Database

**Sensor Manager**

- SensorService
- Obfuscator

**FirewallConfig Manager**

- FirewallConfig Service

**Location Manager**

- LocationManager Service
- Obfuscator

**System Server**

**Native Runtime**

**Hardware**

- **System Processes**
- **User Processes**
- **Trusted App (User Process)**

**ipShield**

- Monitoring
- Privacy Abstraction
- Rule Recommender
- Fine-grained Rules
- Enforcement

Whitelist and Blacklist of inference
User interaction with ipShield
User interaction with ipShield

### Rule Config

**Transportation mode (Outdoor)**
- Still, walking, running, biking, driving
- 93.6% accuracy using: GPS; Accelerometer;
- Priority: 30%

**Movement**
- Stationary, moving
- 97.4% accuracy using: Accelerometer; Gyroscope;
- Priority: 40%

**Touch-screen usage**
- Tapped location on the screen
- 90.0% accuracy using: Accelerometer; Gyroscope;
- Priority: 10%

### ipShield Features

- **Monitoring**
- **Privacy Abstraction**
- **Rule Recommender**
- **Fine-grained Rules**
User interaction with ipShield
User interaction with ipShield
Feasibility of running ipShield on mobile platforms

- **Time (in secs)**
  - 0.015
  - 0.03
  - 0.045
  - 0.06

- **# rules**
  - 1
  - 50
  - 100
  - 150
  - 200

- **Legend**
  - Blue: time to load rules into memory
  - Grey: time for the rules to take effect

The graph illustrates the time taken to load rules into memory and the time for the rules to take effect as the number of rules increases from 1 to 200.
Feasibility of running ipShield on mobile platforms

SENSEOR_DELAY_NORMAL, SENSOR_DELAY_UI

<table>
<thead>
<tr>
<th># rules</th>
<th>Time (in secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.015</td>
</tr>
<tr>
<td>50</td>
<td>0.045</td>
</tr>
<tr>
<td>100</td>
<td>0.03</td>
</tr>
<tr>
<td>150</td>
<td>0.015</td>
</tr>
<tr>
<td>200</td>
<td>0.06</td>
</tr>
</tbody>
</table>

- Green bars: time to load rules into memory
- Orange bars: time for the rules to take effect

0.1
Feasibility of running ipShield on mobile platforms

- SENSOR_DELAY_NORMAL, SENSOR_DELAY_UI
  - Time to load rules into memory: 0.1
  - Time for the rules to take effect:

- SENSOR_DELAY_GAME
  - Time to load rules into memory: 0.02
  - Time for the rules to take effect:

- Time (in secs):
  - 0.015
  - 0.03
  - 0.045
  - 0.06

- # rules:
  - 1
  - 50
  - 100
  - 150
  - 200
Feasibility of running ipShield on mobile platforms

- **SENSOR_DELAY_NORMAL, SENSOR_DELAY_UI**: 0.1
- **time to load rules into memory**
- **time for the rules to take effect**

![Bar chart showing time (in secs) vs. # rules for different sensor delays.](chart)

- **SENSOR_DELAY_GAME**: 0.02
- **SENSOR_DELAY_FASTEST**: 0.006
Feasibility of running ipShield on mobile platforms

<table>
<thead>
<tr>
<th>Platform</th>
<th>Memory (in MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOSP</td>
<td>26.45</td>
</tr>
<tr>
<td>Passthrough</td>
<td>26.575</td>
</tr>
<tr>
<td>Constant</td>
<td>26.7</td>
</tr>
<tr>
<td>Perturb</td>
<td>26.7</td>
</tr>
<tr>
<td>Suppress</td>
<td>26.325</td>
</tr>
</tbody>
</table>
Feasibility of running ipShield on mobile platforms

<table>
<thead>
<tr>
<th>Setting</th>
<th>Memory (in MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOSP</td>
<td>26.45</td>
</tr>
<tr>
<td>Passthrough</td>
<td>26.575</td>
</tr>
<tr>
<td>Constant</td>
<td>26.7</td>
</tr>
<tr>
<td>Perturb</td>
<td>26.575</td>
</tr>
<tr>
<td>Suppress</td>
<td>26.2</td>
</tr>
</tbody>
</table>
Concluding Remarks

• We designed and implemented ipShield which
  - proposes the use of inferences as the currency for privacy and utility specification.
  - advocates that the burden of configuring fine-grained privacy rules should be shifted from the user to the system.
  - provides insight into how and what data is being used by apps and better visibility into potential risks and consequences of sharing data.

• Going forward we want to...
  - develop the rule recommender to generate rules for obfuscating data.
  - augment ipShield with ability to perform static analysis of app code to better understand the risks presented by the apps.
  - allow crowd-sourcing for bootstrapping of rules.

ipShield can be downloaded at http://tinyurl.com/ipshieldgit
Thank You
Rules supported

- **Contexts**
  - **Built-In**
    - Time
    - Place
    - App
    - Day
    - NameOfWeek
  - **External**
    - Normal
    - Constant
    - Suppress
    - Perturb
    - Play-back
      - Scalar
      - Vector
      - Distribution
        - Name
        - Param

- **SensorType**
  - **Sensor**
    - Type
    - Source
  - **App**
  - **Name**
  - **Day**
  - **OfWeek**
  - **Walking**
  - **Running**
  - ...
Rules supported

- **Contexts**
  - Built-In
    - Time
    - Place
  - External
    - App
    - Day
    - NameOfWeek

- **Sensor Type**
  - Normal
  - Constant
  - Suppress
  - Perturb
  - Play-back
    - Scalar
    - Vector
    - Distribution
      - Name
      - Param

- **Action**
  - Rule

- **Suppression**
  - Walking
  - Running
  - ...
Rules supported

- **Built-In**
  - Time
  - Place
  - App
  - Day
  - NameOfWeek
  - Walking
  - Running

- **External**
  - Normal
    - Scalar
    - Vector
  - Constant
  - Suppress
  - Perturb
  - Play-back
  - Distribution
    - Name
    - Param
  - Sensor
    - Type
    - Source

- **Contexts**
  - Rule
  - SensorType
  - Action

- **Action**
  - Suppress
  - Perturb
  - Play-back

- **Sensor Type**
  - Normal
  - Constant
  - Scalar
  - Vector

- **Time**
  - OfDay

- **Place**

- **App**

- **Day**

- **NameOfWeek**

- **Walking**

- **Running**

- **Sensor Source**

- **ipShield**
  - Monitoring
  - Privacy Abstraction
  - Rule Recommender
  - Fine-grained Rules
  - Enforcement
Rules supported

- **Contexts**
  - Built-In
  - External
    - **Time OfDay**
    - **Place**
    - **App**
    - **Day OfWeek**

- **Rule**
  - **Sensor Type**
    - Normal
    - **Constant**
    - Suppress
    - Perturb
    - Play-back
      - **Scalar**
      - **Vector**
        - **Distribution Name**
        - **Distribution Param**

- **Action**
  - **Suppress**
  - **Perturb**
  - **Play-back**

- **Sensor Source**

**ipShield**

- Monitoring
- Privacy Abstraction
- Rule Recommender
- Fine-grained Rules
- Enforcement
Rule: If ((TimeOfDay in [12am-11:59pm]) and (Place=Bar) and (AppName=Saga))
then apply action = Constant and Value = Restaurant on SensorType = GPS;
Sensor usage for apps

% of apps vs # sensors
Distribution of sensors by type

- Accelerometer
- GPS
- Microphone
- WiFi
- Soft Sensors
- Bluetooth
- Gyroscope
- Cellular
- Camera
- Others

% of apps