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

Apps

Sensor Data

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

- Sensor Data
  - Apps
    - mHealth
    - Phone operation
  - 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
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
Utility Providing
- Fitness
- mHealth
- Lifelogging
- Phone operation

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

Sensor Data

Apps

- Fitness
- mHealth
- Lifelogging
- Phone operation

Inferences

Sensitive
- Location
- Password
- Media habits
- Physiological habits

Utility Providing

- From sensor data to inferences

- Sensor Data

- Apps

- Inferences

- Sensitive
Protecting inference privacy while providing utility

Apps

Sensor Data

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

Sensor Data

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

Sensor Data

Inferences

Utility Providing
- Fitness
- mHealth
- Lifelogging
- Phone operation

Sensitive
- Location
- Password
- Media habits
- Physiological habits

Whitelist

Blacklist
Prior notions of privacy in databases

Population Scale Database

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

Population Scale Database

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

inference = identity

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

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

Population Scale Database

Sensor Data Capture → Data Processing → Privacy 

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

Differential Privacy

\[ M = R(<P, Q, V>) + \text{noise} \]

\[ M = <P', Q', V> \]

\[ \text{inference} = \text{identity} \]

\[ \text{inference} = \text{membership} \]

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

Sensor Data Capture → Data Processing → Aggregate Queries

M := \langle P, Q, V' \rangle

Sharing an Individual’s data

Information Recipient
Prior notions of privacy in databases

- Sensor Data Capture
- Data Processing
- Aggregate Queries

Privacy of Data (secrecy)
Privacy of Identity (anonymity)

Traditional

M:=<P, Q, V'>

Sharing an Individual’s data

Privacy of Behavior
Controls provided by current systems are insufficient

Android Manifest

Binary Policies
Controls provided by current systems are insufficient

pDroid

Static Policies
Controls provided by current systems are insufficient

ProtectMyPrivacy

Share Random Data
Design requirements of ipShield

[Diagram showing a smartphone with options for unrestricted access and protected APIs]
Design requirements of ipShield

- **Sensor Monitoring**
- **Unrestricted Access**
- **Protected APIs**

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
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></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>Sensor Combination</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>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><strong>Sensor Combination</strong></td>
<td><strong>95%</strong></td>
<td><strong>Accuracy of</strong></td>
<td><strong>0%</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Prediction</strong></td>
<td></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

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

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

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

\[
\downarrow \quad \downarrow \quad \downarrow \\
\text{priority} = \{10, 4, 10\}
\]

**Whitelisted inferences**

priority ↑ \rightarrow \text{allow whitelisted inferences}

**Blacklisted inferences**

priority ↑ \rightarrow \text{block blacklisted inferences}
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. \( \sum_{l \in \mathcal{B}, p_l = p_{\text{max}}} A(\Psi, l) = 0 \)

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

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

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

\[\downarrow\]

Over all sensor combinations
Rule recommender in ipShield

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

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

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

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

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

\[\downarrow\]

Over all sensor combinations

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

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

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

\[\downarrow\]

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, Location, OnScreen Taps</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPS+Acc+Gyro, 95%, 97%, 80%</td>
</tr>
<tr>
<td>GPS+WiFi, 83.1%, 97%, 0%</td>
</tr>
<tr>
<td>GPS+GSM, 81.7%, 98.2%, 0%</td>
</tr>
<tr>
<td>GSM+WiFi, 72.9%, 94.03%, 0%</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
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 Service**
  - **Location Manager 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
Sensor subsystem in android and data interception

Third Party Apps

Sensor Manager

Android Framework

Sensor Service

System Server

Android Native/Linux Kernel

Hardware

Location Manager

LocationManager Service

Sensor Data

Sensor Data

App and Managers run as part of the same process

System Processes

User Processes
Sensor subsystem in android and data interception

Sensor Manager

Android Framework

Sensor Data

Location Manager

Sensor Data

Sensor Service

LocationManager Service

System Server

Android Native/Linux Kernel

Hardware

Third Party Apps

App and Managers run as part of the same process

Services run in separate system owned processes

System Processes

User Processes
Implementing ipShield

**Trusted App part of ipShield**

**Whitelist and Blacklist of inference**

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

- **SensorService**
- **LocationManager Service**

**System Server**

**Native Runtime**

**Hardware**

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

Whitelist and Blacklist of inference

System Processes User Processes Trusted App (User Process)
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

Whitelist and Blacklist of inference

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

Trusted App part of ipShield

- Sensor Manager
- FirewallConfig Manager
- Location Manager

System Server

- SensorService
- FirewallConfig Service
- LocationManager Service

Native Runtime

Hardware

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

**Trusted App part of ipShield**

- 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**

**Whitelist and Blacklist of inference**

**ipShield**

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

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

**Trusted App part of ipShield**

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

**System Server**

- SensorManager
- FirewallConfig Manager
- Location Manager

- SensorService
- FirewallConfig Service
- LocationManager Service
- Obfuscator

**Native Runtime**

**Hardware**

- System Processes
- User Processes
- Trusted App (User Process)
User interaction with ipShield

- Firewall Manager
  - Saga: 8 inferences via 4 sensors
  - GPS Status: 2 inferences via 1 sensor
  - Facebook: 2 inferences via 1 sensor
  - Maps: 5 inferences via 3 sensors
  - Playback Manager: 2 inferences via 1 sensor
  - SensorRecorder: 2 inferences via 1 sensor
  - AmbulationLite: 5 inferences via 2 sensors

- ipShield
  - Monitoring
  - Privacy Abstraction
  - Rule Recommender
  - Fine-grained Rules
User interaction with ipShield

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

**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%
User interaction with ipShield

ipShield
Monitoring
Privacy Abstraction
Rule Recommender
Fine-grained Rules

Accelerometer
Use count: 66
Suppress

Time Context
Apply during following times (24hr format):

From 00:23 to 00:59

Location Context
Apply when I am within 1000ft
of location Work

Gyroscope
Use count: 64
Normal
User interaction with ipShield

<table>
<thead>
<tr>
<th>Sensor</th>
<th>Use count</th>
<th>Rule Options</th>
<th>Current Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accelerometer</td>
<td>66</td>
<td>Normal, Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>Gyroscope</td>
<td>64</td>
<td>Supress, Playback</td>
<td></td>
</tr>
<tr>
<td>Pressure</td>
<td>10</td>
<td>Constant, Perturb</td>
<td></td>
</tr>
<tr>
<td>GPS</td>
<td>6</td>
<td>Normal</td>
<td></td>
</tr>
</tbody>
</table>
Feasibility of running ipShield on mobile platforms

- Time to load rules into memory
- Time for the rules to take effect

Time (in secs)

<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>0.03</td>
</tr>
<tr>
<td>100</td>
<td>0.045</td>
</tr>
<tr>
<td>150</td>
<td>0.06</td>
</tr>
<tr>
<td>200</td>
<td></td>
</tr>
</tbody>
</table>
Feasibility of running ipShield on mobile platforms

- Time to load rules into memory
- Time for the rules to take effect

For SENSOR_DELAY_NORMAL, SENSOR_DELAY_UI:

- Time (in secs)
- # rules
- 0.1
- 0.045
- 0.03
- 0.015
- 0

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

**Chart Description:**
- **X-axis:** Number of rules (# rules)
- **Y-axis:** Time (in secs)
- **Legend:**
  - Time to load rules into memory
  - Time for the rules to take effect
- **Data Points:**
  - SENSOR_DELAY_NORMAL, SENSOR_DELAY_UI
  - SENSOR_DELAY_GAME

**Graph Analysis:**
- As the number of rules increases, the time to load rules into memory and the time for the rules to take effect also increase.
- For SENSOR_DELAY_NORMAL and SENSOR_DELAY_UI, the time is relatively constant across different numbers of rules, with a slight increase.
- For SENSOR_DELAY_GAME, the time increases significantly as the number of rules increases, indicating a potential limitation in mobile platforms for this specific setting.
Feasibility of running ipShield on mobile platforms

- Time to load rules into memory
- Time for the rules to take effect

- SENSOR_DELAY_NORMAL, SENSOR_DELAY_UI
  - 0.1

- SENSOR_DELAY_GAME
  - 0.03
  - SENSOR_DELAY_FASTEST
  - 0.06

<table>
<thead>
<tr>
<th># rules</th>
<th>Time in secs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.006</td>
</tr>
<tr>
<td>50</td>
<td>0.015</td>
</tr>
<tr>
<td>100</td>
<td>0.02</td>
</tr>
<tr>
<td>150</td>
<td>0.045</td>
</tr>
<tr>
<td>200</td>
<td>0.06</td>
</tr>
</tbody>
</table>
Feasibility of running ipShield on mobile platforms

<table>
<thead>
<tr>
<th>Method</th>
<th>Memory (in MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOSP</td>
<td>26.325</td>
</tr>
<tr>
<td>Passthrough</td>
<td>26.45</td>
</tr>
<tr>
<td>Constant</td>
<td>26.575</td>
</tr>
<tr>
<td>Perturb</td>
<td>26.7</td>
</tr>
<tr>
<td>Suppress</td>
<td>26.2</td>
</tr>
</tbody>
</table>
Feasibility of running ipShield on mobile platforms

![Bar chart showing memory usage (in MB) for different scenarios: AOSP, Passthrough, Constant, Perturb, Suppress. The memory usage ranges from 26.2 to 26.7 MB.]

- AOSP: Memory usage around 26.4 MB
- Passthrough: Memory usage around 26.5 MB
- Constant: Memory usage around 26.7 MB
- Perturb: Memory usage significantly higher, close to 26.7 MB
- Suppress: Memory usage significantly lower, close to 26.2 MB

The bar chart illustrates the memory footprint for each scenario, with Perturb showing the highest usage and Suppress showing the lowest.
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
- Sensor Type
- Action

- Built-In
- External

- Time of Day
- Place
- App
- Day of Week
- Walking
- Running

- Normal
- Constant
- Suppress
- Perturb
- Play-back

- Scalar
- Vector

- Distribution Name
- Param

- Rule Recommender
- Fine-grained Rules
- Enforcement
Rules supported
Rules supported

- Built-In
  - Time
  - Place
  - App
  - Day
  - OfWeek

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

- Contexts
- SensorType
- Action

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

- Rule
  - Contexts
    - Built-In
      - Time
      - Place
      - App
      - Day
      - Name
    - External
      - Walking
      - Running
  - Sensor Type
    - Normal
    - Constant
    - Suppress
    - Perturb
    - Play-back
  - Action
    - Scalar
    - Vector
    - Distribution
    - Name
    - Param
    - 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

# sensors

0 1 2 3 4 5 6

1 2 3 4 5 6

50 37.5 25 12.5 0

27
Distribution of sensors by type

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

% of apps