ipShield: A Framework For Enforcing Context-Aware Privacy

Supriyo Chakraborty, Chenguang Shen, Kasturi Raghavan, Yasser Shoukry, Matt Millar, Moustafa Alzantot, Mani Srivastava

University of California Los Angeles, IBM Research

Privacy Problem

- Mobile phones provide a sensing platform where sensors data are shared with third party applications to draw inferences from in order to provide adaptive and personalized useful services.
- Not all applications are trustworthy, some application may abuse the sensors data and infer sensitive information.
- Not all sensors are treated equally by mobile OSes; Access to some sensors does not require user permission: accelerometer, gyroscope, and magnetometer. However, those sensors combined have been exploited to mount serious attacks:
  - Using accelerometer, and gyroscope from smartwatch to identify smoking events.
  - Reconstruction of travel trajectories.
  - Using microphone to detect stress/ mood.

ipShield: Sensors Firewall

- ipShield performs monitoring for each sensor access by an app and uses this information to perform privacy risk assessment.
- ipShield presents to the user a list of possible inferences that can be drawn from the shared sensors data.
- A recommender system recommends a privacy rule based on the users configuration. Also users can override the recommended action.
- ipShield enforces the privacy rules for applications accessing sensor data.

ipShield Implementation

- Rule Example: If ((TimeOfDay in [12am-11:59pm]) and (Place=Bar) and (AppName=Saga)) then apply action = Constant and Value = Restaurant on SensorType = GPS;

Rules Supported

- Rule Example: If ((TimeOfDay in [12am-11:59pm]) and (Place=Bar) and (AppName=Saga)) then apply action = Constant and Value = Restaurant on SensorType = GPS;

Evaluation

- Time for loading rules into memory, and time overhead to fetch one new sensor data sampled at SENSOR_DELAY_FASTEST

ipShield: Sensors Firewall

- ipShield is implemented as a modified version of the Android Open-Source Project.

User Interaction with ipShield

- Monitoring applications sensor data usage and abstracting privacy risks.
- Fine-grained privacy-rules overriding option.

Future Work

- Augment ipShield with ability to perform static analysis of app code to better understand the risks presented by the apps.
- Integrate more actions based on cryptographic solutions.
- Use crowdsourcing to bootstrap the privacy rules.

References

- ipShield is an open-source project, Find us at http://nesl.github.io/ipShield/

MD2K is supported by the National Institutes of Health Big Data to Knowledge Initiative Grant #1U54EB020404