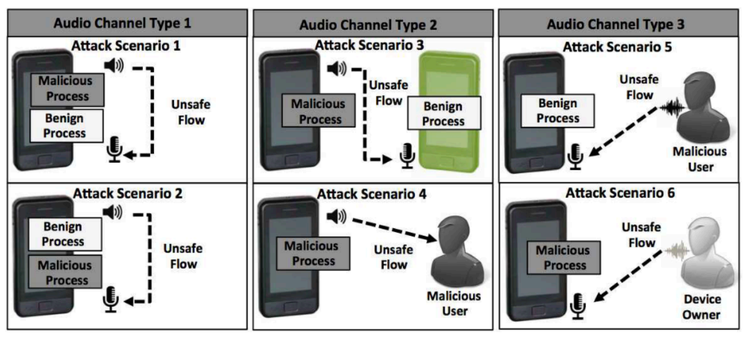
On Limitations of Access Control Models for Privacy-Sensitive Sensors

Giuseppe Petracca, Yuqiong Sun, and Trent Jaeger

As IoT and mobile devices rise into dominance, sensors are playing a pivotal role for measuring the physical world. However, such sensors constitute a new attack vector:

- **Audio Channels** may allow cybercriminals to trick devices able to process voice commands into leak secrets or modify critical information.
- **Continuous-Sensing Sensors**, such as GPS, Accelerometer, and Gyroscope, may allow cybercriminals to perform inference attacks and derive sensitive information.
- **Audio-Visual Sensors**, such as Camera and Microphone may allow cybercriminals to stalk device owners and obtain sensitive information via GUI attacks.

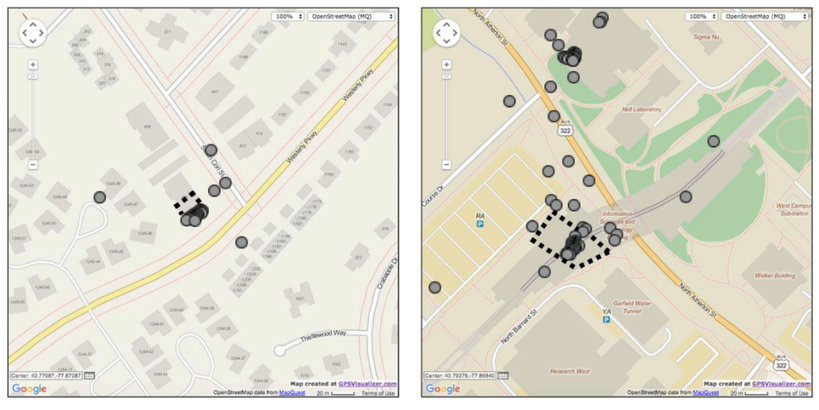
Audio Channels



Proposed Approach (**AuDroid**):

- Extension of existing reference monitors to enforce lattice security policies over dynamically-created communication channels
- Placement of mediation hooks to arbitrate access to security-sensitive sensors exploitable by cybercriminals.
- Resolution of unsafe information flows to preserve functional requirements.

Continuous-Sensing Sensors

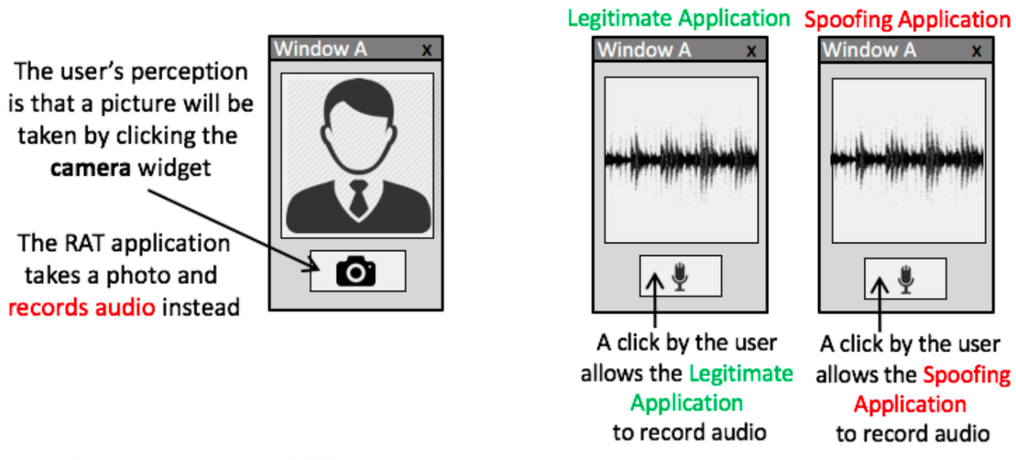


Sensitive Locations (Dashed Areas) Home (Left) and Work (Right) of a victim being tracked via GPS

Proposed Approach (**Sense**):

- Opportunely distribute synthetic data among real sensed data to achieve an incremental uniform distribution of data points in the space of readings to deceive cybercriminals performing inference attacks on such data.
- Measure the effect of targeted agile maneuvers designed to reduce the probability of success of inference attacks on sensed data.

Audio-Visual Sensors



Proposed Approach (**AWare**):

- Bind each operation request to the state of the user interface when the user initially approves an operation, and presents the operation request to user for explicit authorization.
- Reuse such explicit authorization as long as the application always uses the same user interface configuration to request the same operation.

Experimental Results

AuDroid prevents 6 types of attack scenarios on audio channels while permitting 17 widely used mobile apps to run effectively (1-5 µs overhead per sensor access).

Sense shows that agility maneuvers are more robust against inference attacks resulting in a probability of success for the attacker of only 2.68% on average, compared to an average of 56.92% when using state-of-the-art Location-Privacy Preserving Mechanisms.

AWare offers users an effective additional layer of defense against Graphic User Interface attacks as demonstrated via a laboratory-based user study involving 90 human subjects. Furthermore, **AWare** maintains the number of decisions imposed to the users very modest, as demonstrated via a field-based study involving 24 human subjects. Lastly, 1,000 of the most-downloaded can operate effectively under **AWare** while incurring less than 4% performance overhead on microbenchmarks.

Related Publications

- AuDroid: Preventing attacks on audio channels in mobile devices. G. Petracca, Y. Sun, A. Atamli, and T. Jaeger (ACSAC'15)
- Agility maneuvers to mitigate inference attacks on sensed location data. G. Petracca, L. M. Marvel, A. Swami, and T. Jaeger (MILCOM'16)
- AWare: Preventing Abuse of Privacy-Sensitive Sensors via Operation Bindings. G. Petracca, A. Atamli, J. Grossklags, and T. Jaeger (Under Submission)

Sponsor: Army Research Laboratory ARL