

Discovering and Restricting Undesirable Information Flows Between Multiple Spheres of Activities



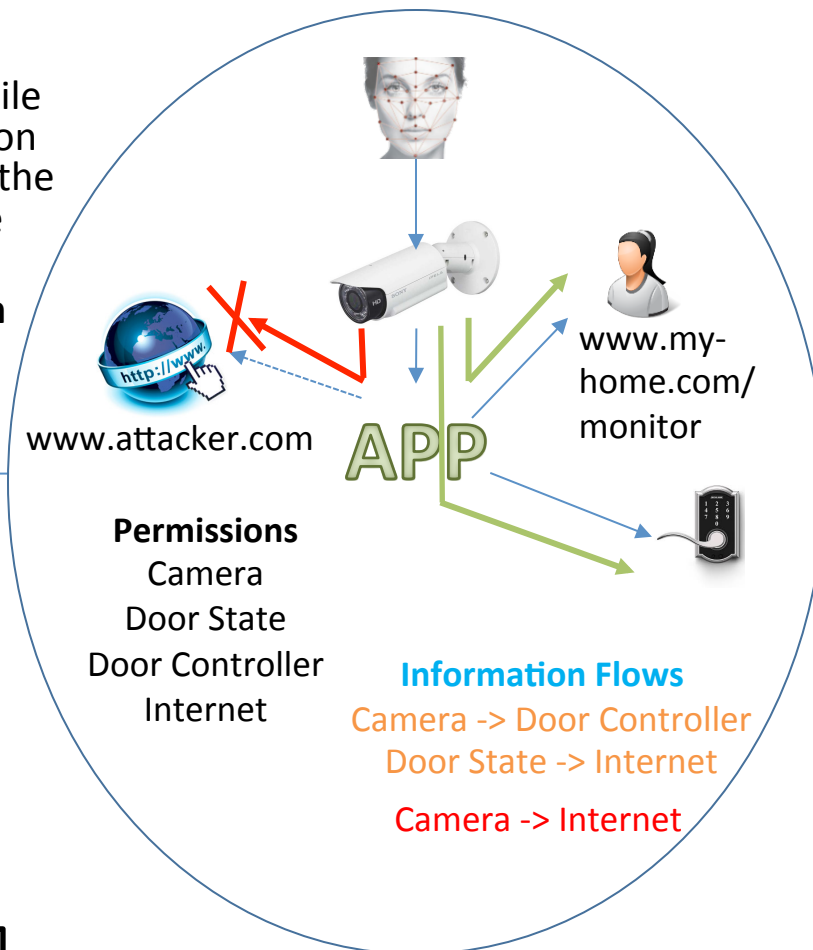
<https://iotsecurity.eecs.umich.edu/#flowfence>

Challenge:

- How do we enable Mobile & IoT apps to compute on the sensitive data from the built environment while mitigating leakage?
- Can we use **Information Flow Control as a first class primitive**?

Solution:

- Programmer-defined information flows
- Move from permission model to information flow control model



Scientific Impact:

- Focus on Information Flow Control as a first class security primitive instead of permissions
- Information Flow Control model where consumers can request policies while framework enforces policies

Broader Impact:

- Move towards IoT => Pressing need to ensure proper use of sensitive data. FlowFence: significant step in this direction
- Programming Model approach encourages security best practices in developers

FlowFence project
(Usenix Security Symposium'16)

Award: 1318722
PI: Atul Prakash, University of Michigan