Privaros: A Framework for Privacy-Compliant Delivery Drones

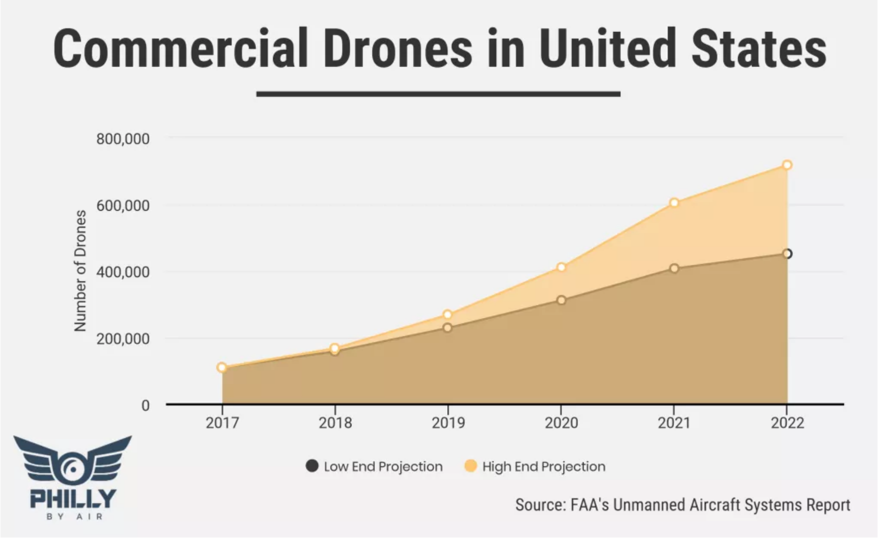
Rakesh Rajan Beck, Abhishek Vijeev, Vinod Ganapathy

Computer Systems Security Laboratory

IISc Bangalore

ACM CCS 2020

Privacy in the age of drones



Source: FAA's Unmanned Aircraft Systems Report

Predicted 2.4 million hobbyist UAVs by 2022
Predicted 450,000 commercial UAVs by 2022
[FAA Aerospace Forecast FY 2018-2038]

- End-user drones are now commonly available.
- Equipped with sensors such as cameras and GPS.
- Threat to individual privacy.
- Regulations are loose and mechanisms to enforce privacy are lacking!

Our focus: Delivery drones

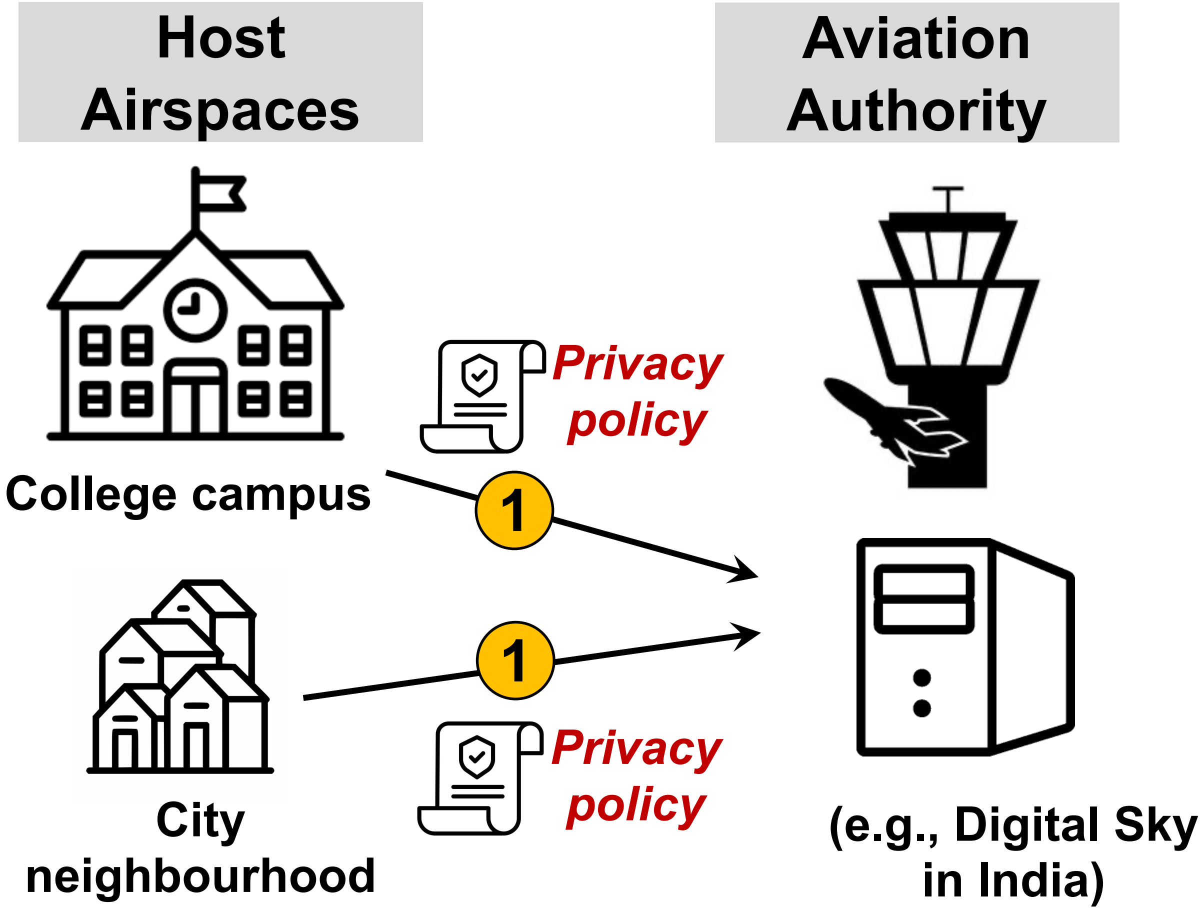
- Incentive to comply with privacy regulations?
  - E-commerce companies with reputations to protect → no overt malicious intentions → our threat model can exclude rogue drones.
  - Strong interest to comply with local regulations.
- Yet, we need to mechanisms to enforce privacy:
  - Different **host airspaces** may have different privacy needs
  - E-commerce companies may contract out drone operations to third-party fleet operators (*a.k.a.* “delivery-service partners”).
  - Host airspaces may wish to determine that these **guest drones** comply with their privacy requirements.

Main contribution: Privaros

Drone software stack with mechanisms to enforce privacy policies specified by host airspaces

- Adds **mandatory access control (MAC)** based policy enforcement to the **Robot Operating System** (ROS v2).
- **Runs on the guest delivery drone** and enforces MAC policies in the OS and ROS layer.
- Uses **hardware-based attestations** from a trusted execution environment (TEE) on guest drone convince host airspace that guest drone runs Privaros.

1 Host airspaces specify their privacy policies and send it to the aviation authority



Host Airspaces

Aviation Authority

College campus

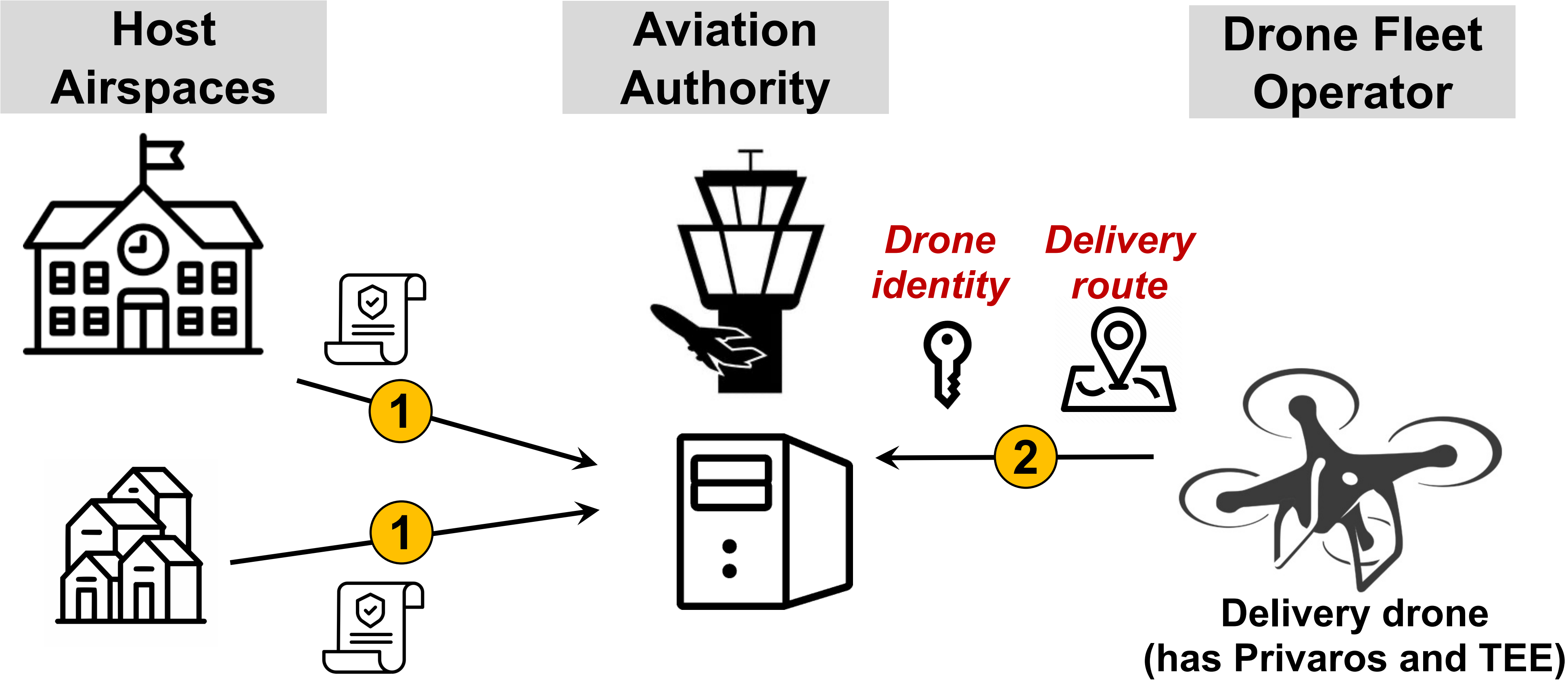
City neighbourhood

1 *Privacy policy*

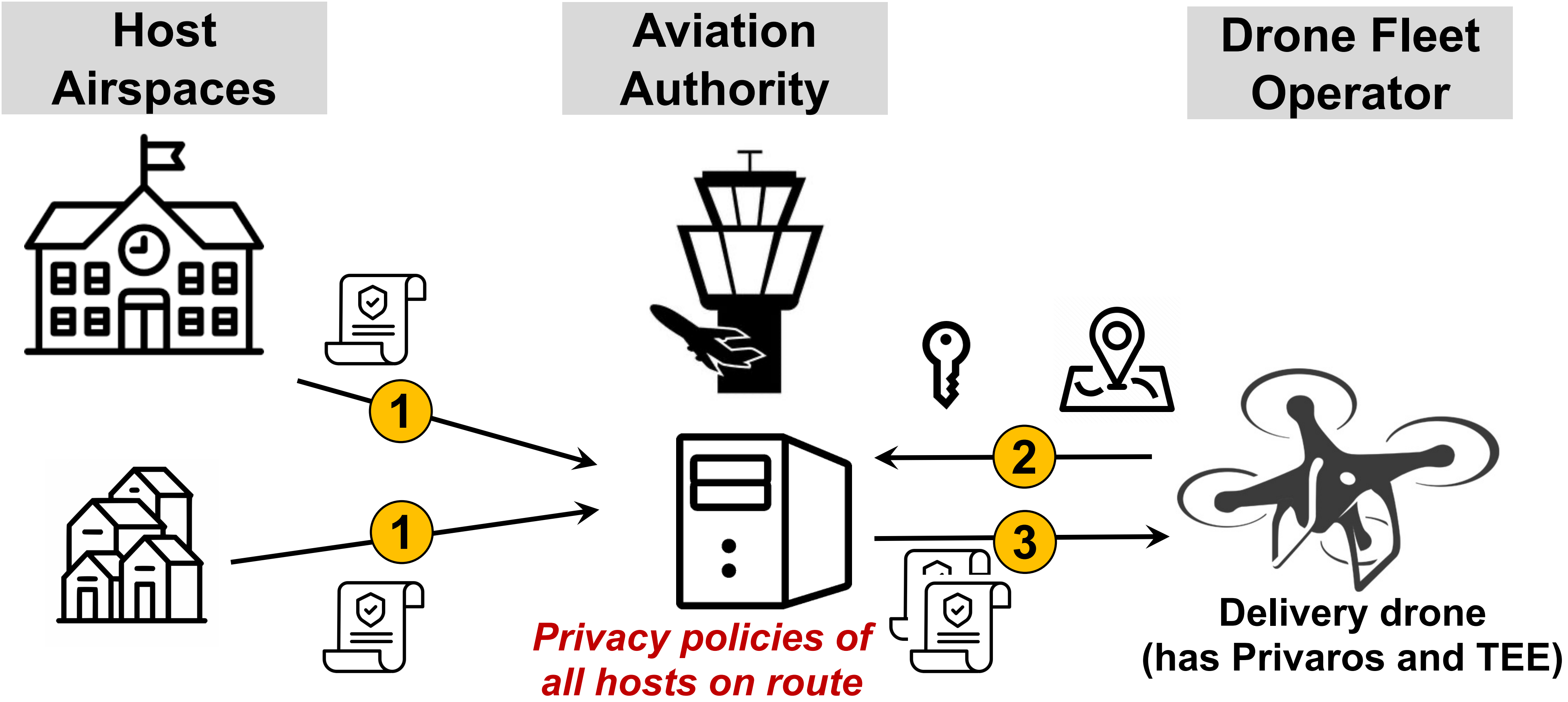
1 *Privacy policy*

(e.g., Digital Sky in India)

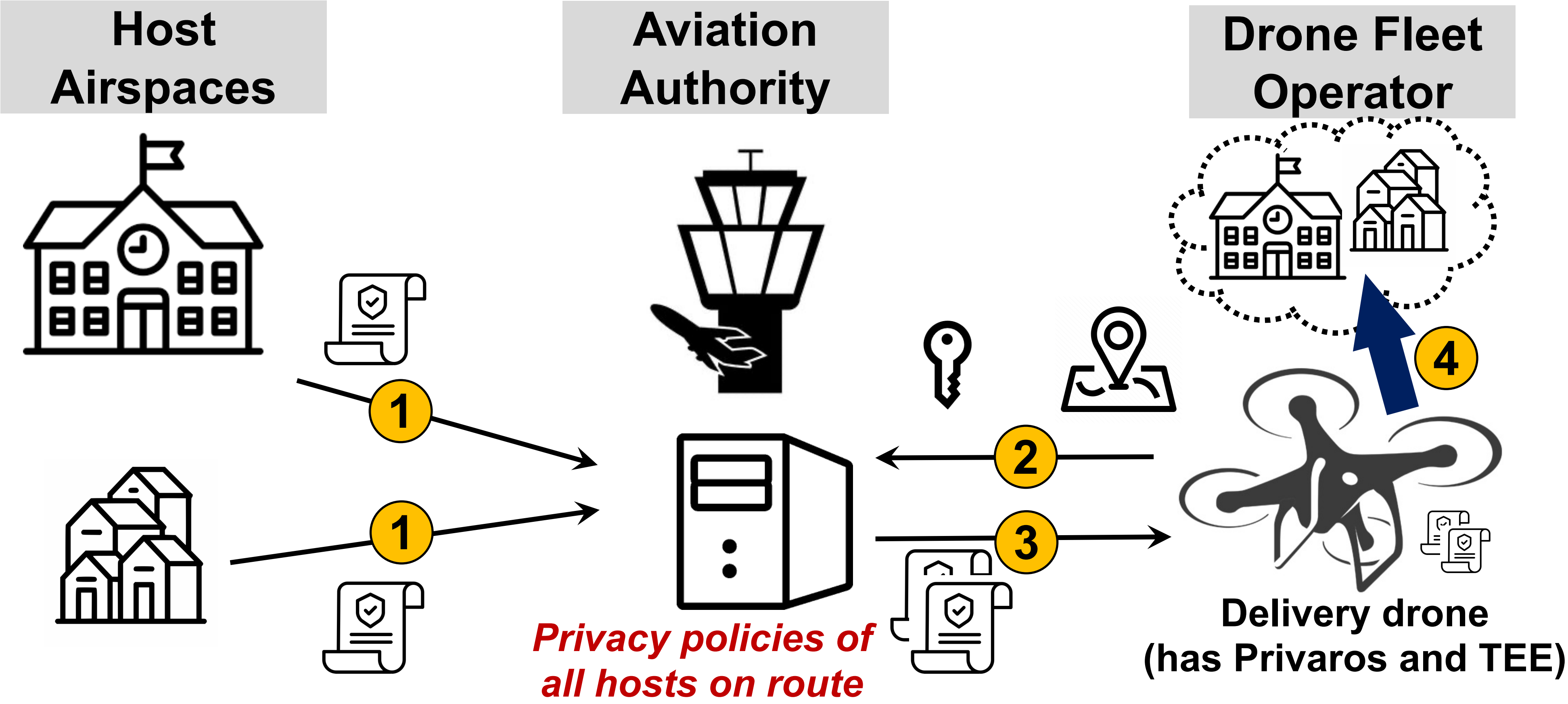
2 Drone sends its identity, attestation, and delivery route to aviation authority prior to delivery run



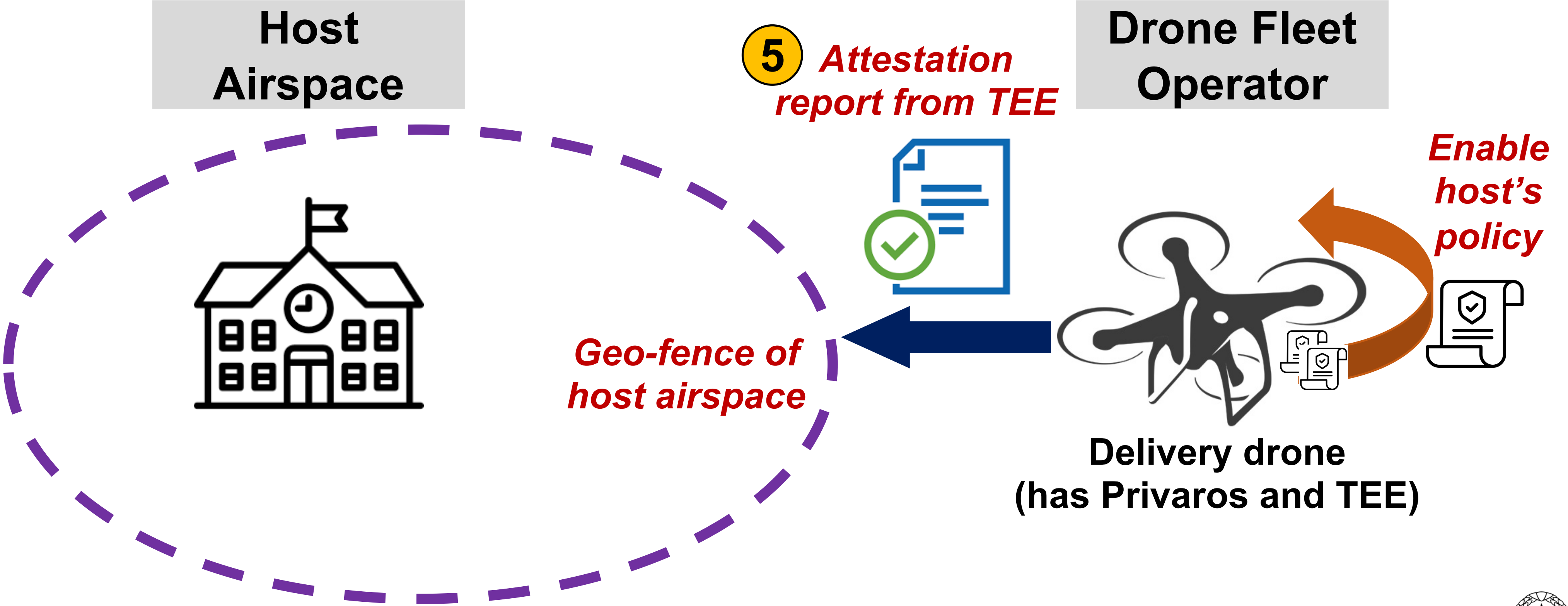
3 Aviation authority sends the drone the privacy policies of all host airspaces in its delivery run


Host Airspaces
Aviation Authority
Drone Fleet Operator
1
1
2
3
Privacy policies of all hosts on route
Delivery drone (has Privaros and TEE)

4 Drone loads privacy policies and starts route


Host Airspaces
Aviation Authority
Drone Fleet Operator
1
1
2
3
4
Privacy policies of all hosts on route
Delivery drone (has Privaros and TEE)

5 Drone applies host’s privacy policy before entering airspace. Drone proves to host that it is equipped with Privaros and that the host’s policy is applied



Host Airspace

Drone Fleet Operator

5 *Attestation report from TEE*

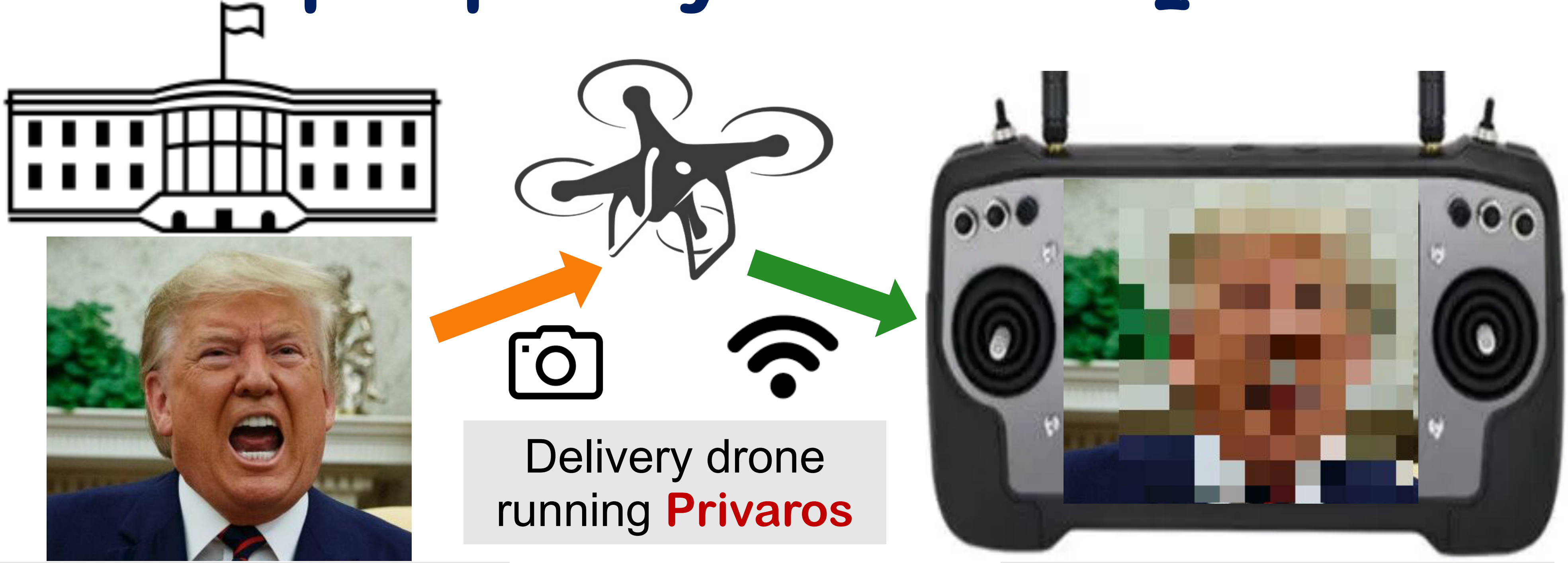
Enable host’s policy

Geo-fence of host airspace

Delivery drone (has Privaros and TEE)

6 Customer enjoys delivered product!

Example policy: **Blur-Exported**



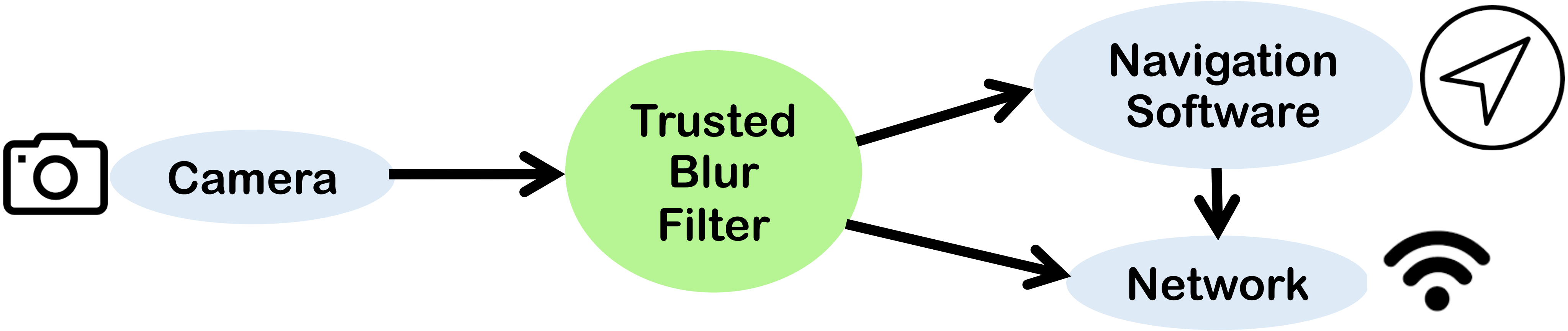
Delivery drone running **Privaros**

Host airspace → sensitive objects captured in video feed of drone

First-person view on untrusted remote control → sensitive parts hidden

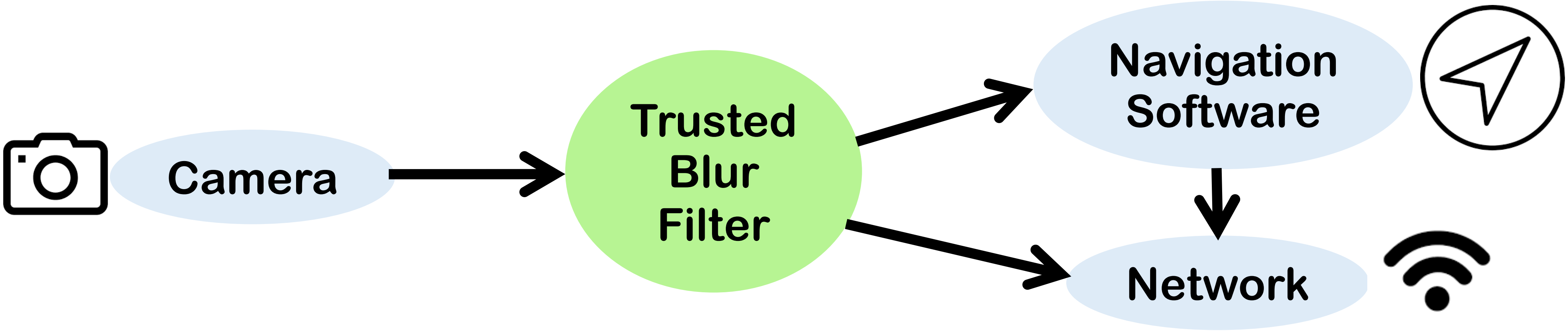
Policies as communication graphs

- Hosts use a **communication graph** to specify their policy, which restricts how applications on the drone can communicate with each other.



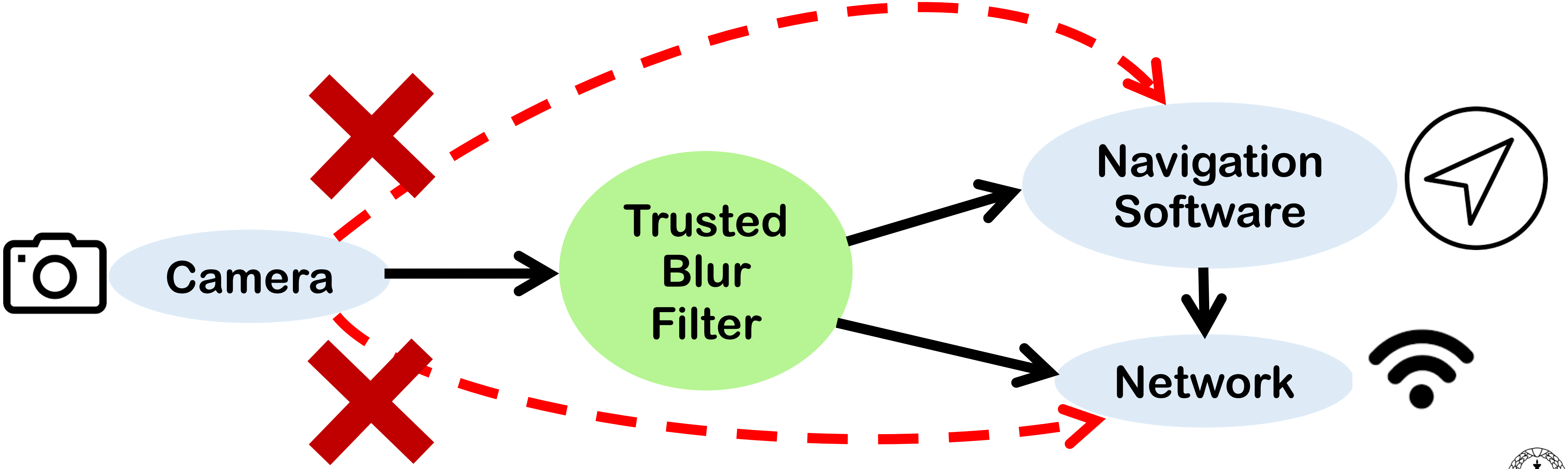
Trusted applications

- **Trusted applications** running on the drone process sensitive data before the data leaves the drone.
- Hosts identify these trusted applications that they entrust with data declassification.

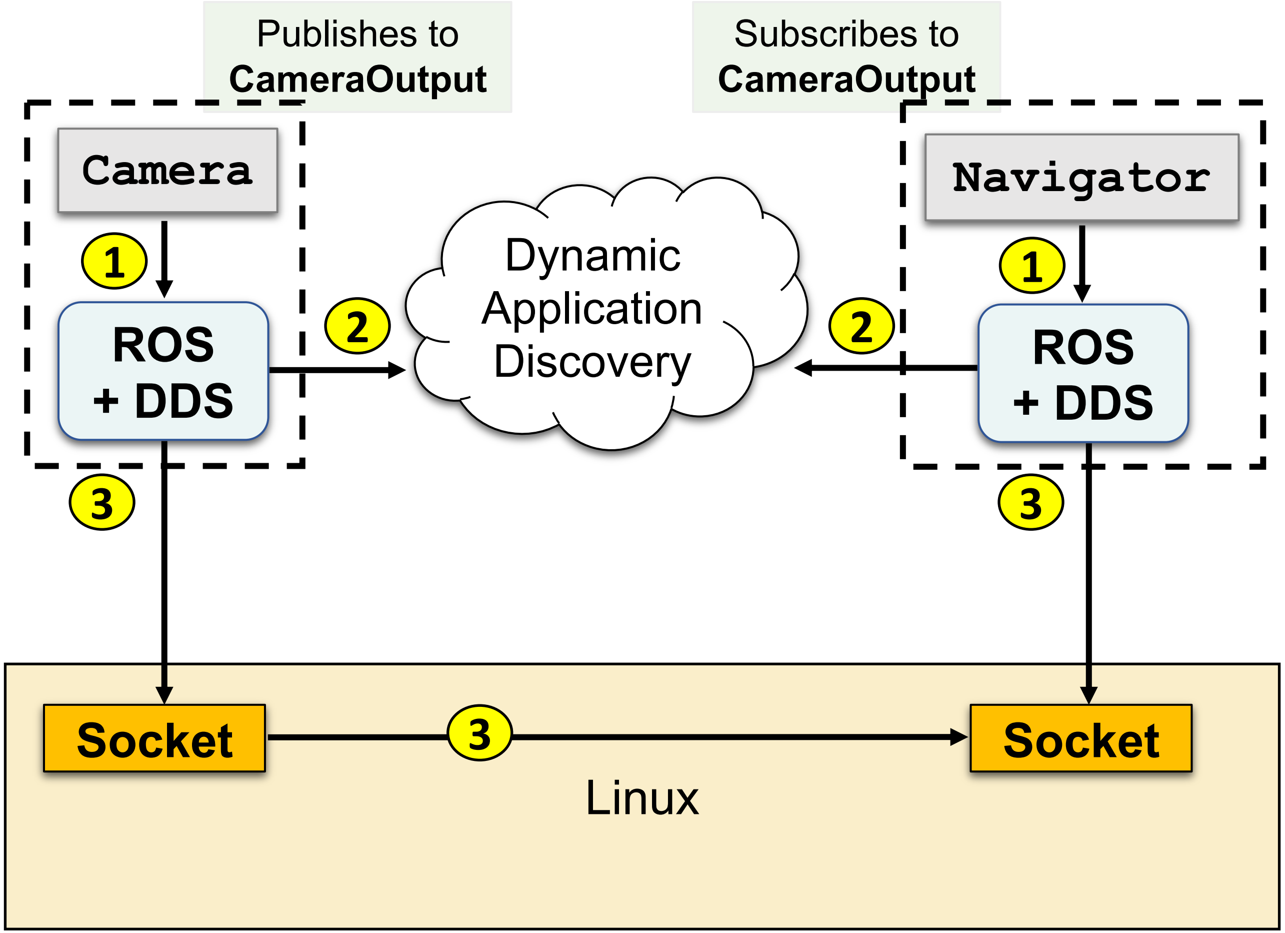


Mandatory access control

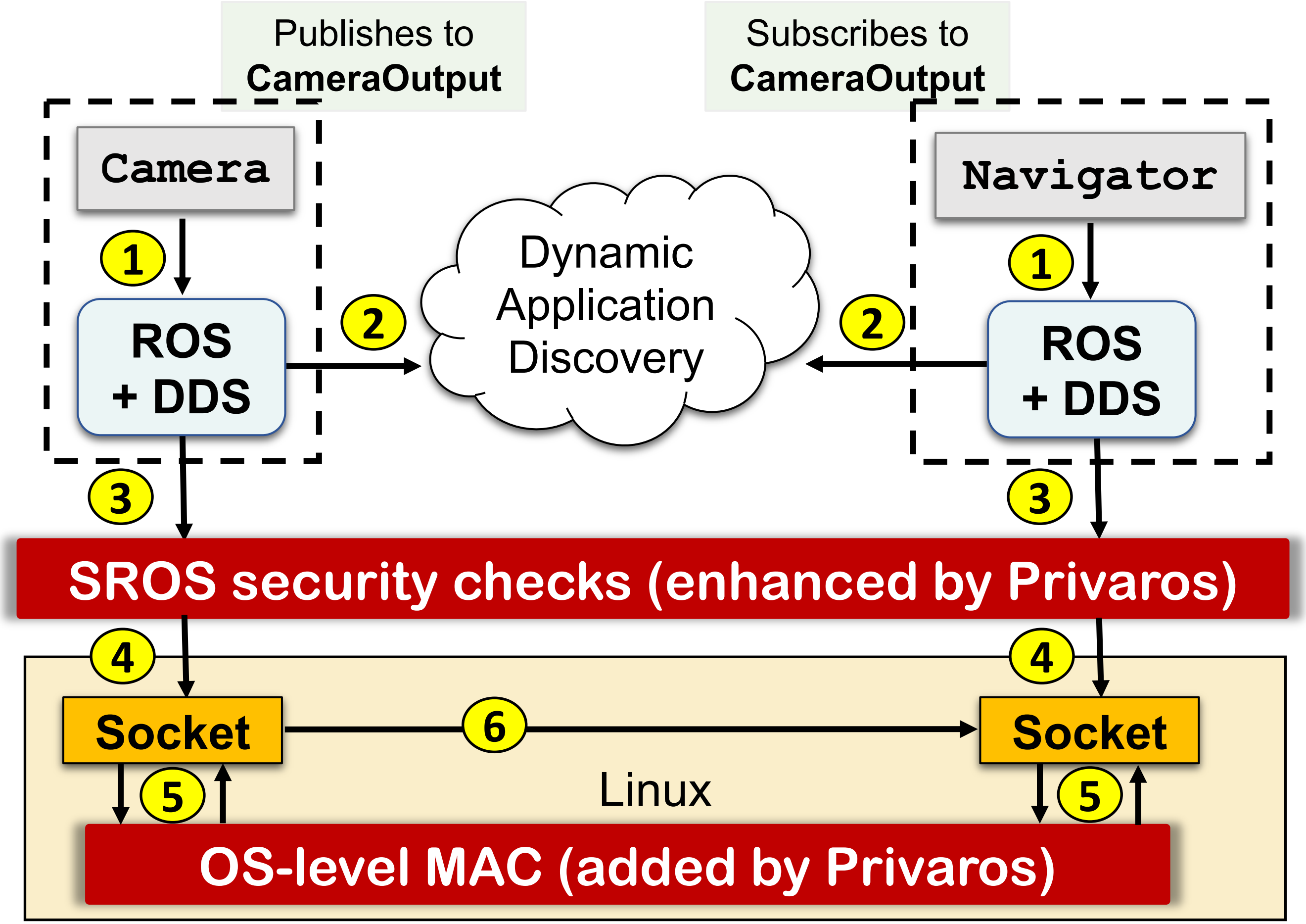
- Privaros uses mandatory access control to ensure that applications communicate as specified by the communication graph.



Mechanisms in Privaros

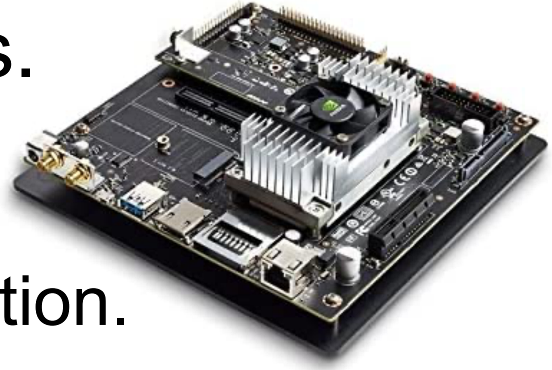


Mechanisms in Privaros

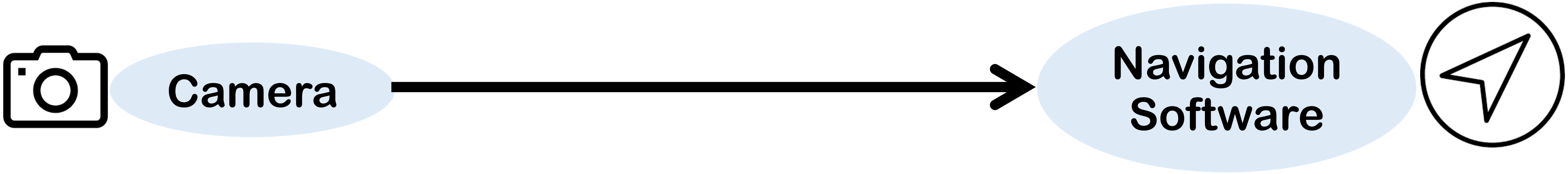


Snippet from our evaluation

- What is the **performance impact of redirecting flows** through trusted applications?
- **Experimental Platform**: **Nvidia Jetson TX2** evaluation board running Privaros.



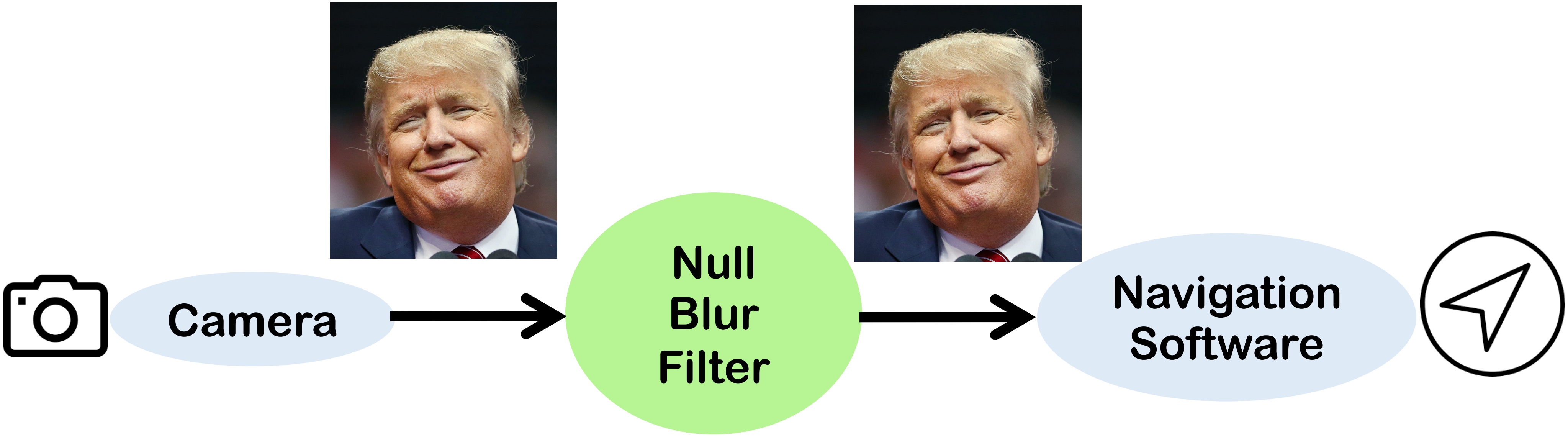
- **In the paper**:
  - **Security and robustness** evaluation.
  - Performance evaluation with **microbenchmarks**.



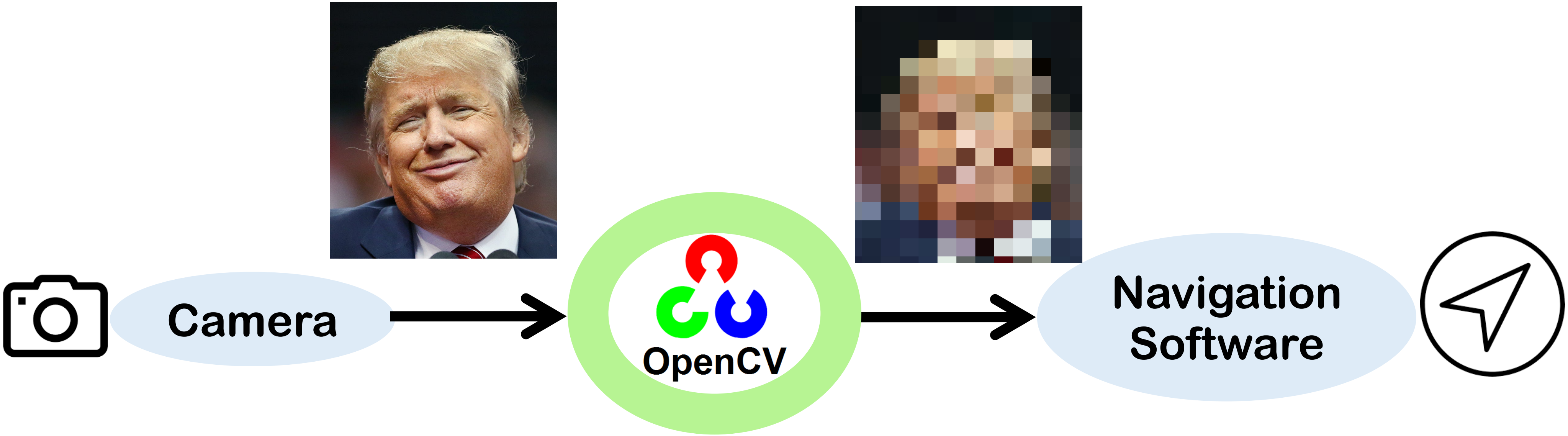
Camera

Navigation Software

Scenario	Latency (ms)	Power (mW)
No redirection	8.1	4749.4



Scenario	Latency (ms)	Power (mW)
No redirection	8.1	4749.4
Null blur filter	17.5 (+115.5%)	4836.2 (+1.8%)



Scenario	Latency (ms)	Power (mW)
No redirection	8.1	4749.4
Null blur filter	17.5 (+115.5%)	4836.2 (+1.8%)
OpenCV blur filter	21.5 (+164.8%)	5132.4 (+8.1%)

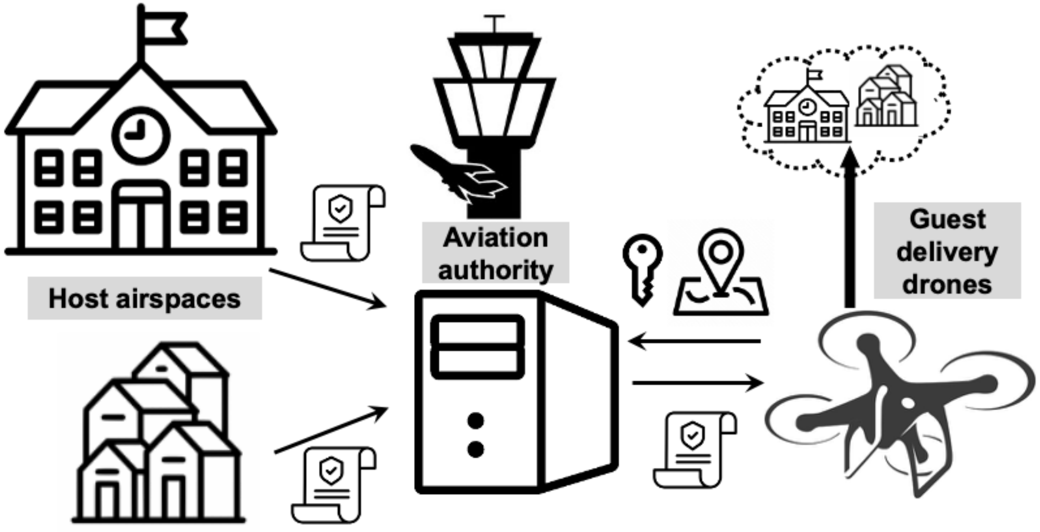
If I had more time, I’d show you …

- More examples of **host privacy policies**.
- Why **secure ROS (SROS) is inadequate**, and why new mechanisms are needed.
- How Privaros **tightly integrates** policy enforcement in the operating system and the ROS middleware.
- How Privaros can readily be deployed within existing regulatory frameworks like **India’s Digital Sky portal**.
- More **results** from our experimental evaluation.

For more details …

Questions?

Privaros: A Framework for Privacy-Compliant Delivery Drones



Computer Systems Security Laboratory