Towards a Threat Model
for Actors in the Swarm

Michael Rushanan, *Johns Hopkins University*; **Denis Foo Kune, Kevin Fu,** *University of Michigan*

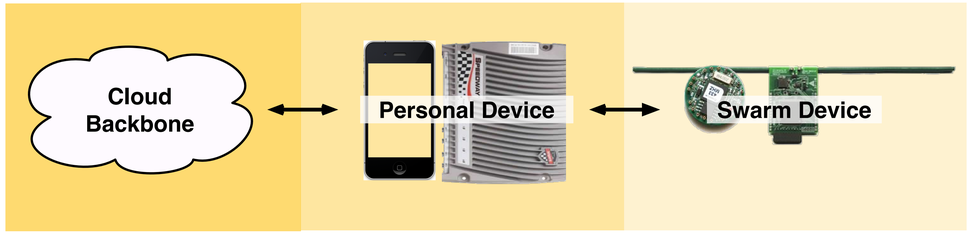
Problem

TerraSwarm, a sense and actuate network, introduces the seamless integration of cyber and physical worlds. Though the potential of such integration is limitless, there are also many new challenges and implications that transcend traditional security and privacy. These challenges elicit the need for a TerraSwarm-specific threat model.

Known Models Fall Short

The TerraSwarm network relies on three distinct actors: 1) cloud backbone for data storage and computation; 2) personal devices for adhoc communication between cloud and swarm, and; 3) swarm devices for physical sensing. Each actor is critical for actuation and thus is susceptible to targeted passive and active attacks.

Sense Physical World



With respect to similar domains such as RFID and WSN, TerraSwarm is unique in that it couples both resource-constrained devices and large-scale computing. For example, injecting malicious signals to sensors or compromising cloud admin credentials both thwart actuation.

Objective Comparison

	Goals	Example Capabilities	Scale	Difficulty
RFID/WSN	> Thwart data collection.	Physically access sink node or tag.	Small	Easy
	> Intercept sensitive data.	Introduce RFID reader to sniff data.	Small	Average
		Deploy a malicious node.	Small	Average
	> Falsify collected data.	Introduce a cloned RFID tag.	Small	Hard
	> Cause aggregate data stagnation.	DoS a sink node.	Small	Easy
Swarm	> Thwart valid actuation.	Physically access swarm sensors.	Large	Easy
	> Intercept sensitive sensor data.	Modify a personal device to store transmitted data.	Large	Easy
		Introduce a device (e.g. RFID reader) to sniff data.	Large	Average
	> Falsify collected sensor data.	Acquire and maliciously repurpose swarm devices.	Large	Average
		Inject signals to swarm sensors or personal devices.	Large	Average
	> Cause aggregate data stagnation.	DDos the cloud backbone.	Large	Easy

Attacker

An *active* attacker attempts to destroy, disable, alter, or gain unauthorized access to sensor data or an actor in the network.

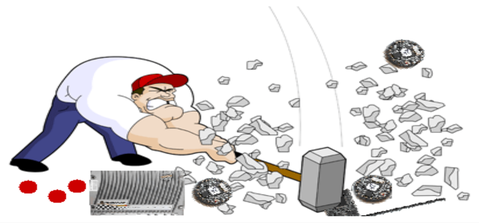
> Implant a malicious device
> Compromise cloud admin credentials
> Physically destroy a publicly accessible swarm device
> Inject signals to analog swarm sensors.

A *passive* attacker attempts to unobtrusively obtain sensitive sensor data.

> Modify phone software
> Deploy personal RFID reader

Example real-world attackers include:

> State actors
> Political dissidents
> Organized criminals



This work was supported in part by the TerraSwarm Research Center, one of six centers supported by the STARnet phase of the Focus Center Research Program (FCRP) a Semiconductor Research Corporation program sponsored by MARCO and DARPA.