An Attacker-Centric Threat Model for Actors in the Swarm

Michael Rushanan[1], Miran Alhaideri[2], Denis Foo Kune[2], and Kevin Fu[2]

[1]Johns Hopkins University, micharu1@cs.jhu.edu
[2]University of Michigan, malhaide@umich.edu, dfkune@umich.edu, kevinfu@umich.edu

1 Context

The seamless integration of cyber and physical worlds requires the proactive consideration of security and privacy risks. TerraSwarm, a sense and actuate network, introduces a triple of well-defined peers to sense the physical world, aggregate and store collected data long-term, and actuate in real-time [3]. The definitions and labels of these peers are defined as follows: a) Cloud Backbone: A scalable distributed presence that provides compute and storage for data mining and archiving; b) Personal Device: A commodity mobile device, or RFID reader, that brokers the communication link between cloud and swarm, and; c) Swarm Device: An embedded and low-power device that employs sense and actuate capabilities to the physical world.

While mandatory for the success of the TerraSwarm network, these peers are inevitably choke points to a critical system that can realize physical actuation. Moreover, if any trust assumption, biased or naive, between peers is formed, the *entire* sense and actuate pipeline may be compromised. Due to the critical nature of TerraSwarm (e.g., malformed aggregated sensor injection that actuates a life-threatening response), we propose an insightful attacker-centric threat model construction that diverges from similar work done for wireless sensor networks [4]. We begin our construction with the definition of an attacker, transition to discuss her goals and intent for malicious behavior, and finally dissect her capabilities.

2 Attacker

An *active* attacker, with respect to TerraSwarm, is an individual whom attempts to destroy, disable, alter, or gain unauthorized access to sensor data or a peer in the network. This attacker may: employ the use of a personal RFID reader to capture sensitive sensor data, implant a malicious device that injects false data, attempt to bruteforce administrative cloud backbone credentials, or simply introduce a hammer to a publicly accessible device.

A *passive* attacker, with respect to TerraSwarm, is an individual whom attempts to unobtrusively obtain sensitive sensor data. This attacker may modify her phone's firmware/software stack to recover data flow between the swarm device and the cloud, or she may also employ the use of a personal RFID reader.

We believe that the following list of actors is more likely to share the goals and capabilities of the attackers in our model: government actors, organized criminal actors, and political dissidents, as suggested in white papers such as [1].

3 Building a New Model

3.1 Goals

We define the core goals of an attacker in the TerraSwarm network as follows: a) to thwart valid actuation, and; b) to collect sensitive data. There also exists subgoals for thwarting actuation. These subgoals include the falsification of sensor data and denial-of-service (DoS) of some set of N peers — causing the stagnation of aggregate data. As TerraSwarm will support safety-critical health and societal applications, we are certain that sensitive data will be sensed and thus targeted by an attacker.

3.2 Capabilities

Unlike traditional networks, all actors can physically access a swarm device that is not encased in some rigid confine (e.g., concrete). Due to the scale of swarm sensor deployments, in the order of thousands of devices per mile, it is unreasonable to expect some semblance of physical security. Additionally, a DoS is plausible by physically destroying swarm and personal devices.

The low expense of swarm devices also enables a set of unique attacks. Firstly, an attacker can acquire and maliciously repurpose a swarm device to report false data. Secondly, an attacker may acquire the software or hardware (e.g., RFID reader) to perform a passive sniff on transmitted data. Worst yet, if there is no mutual authentication or end-to-end encryption, the attacker will not need to rely on advanced approaches such as a correlation attack or power analysis [2].

Finally, an attacker is capable of attacking the cloud backbone. From the network perspective, it is possible to DDoS the cloud backbone. This act results in the inaccessibility of the data store — halting actuation for any significant outage time. If the cloud backbone is outsourced to a Thirdparty (e.g., Amazon), then it may be possible for an attacker to perform a VM side-channel attack by mapping the internal cloud infrastructure and landing her VM on the same physical server as the backbone [5].

3.3 Putting it Together

We have defined the goals and capabilities of an attacker with respect to the TerraSwarm network. This model is allowably more permissible than traditional models due to the energy budget constraints of low power swarm devices, lack of reasonable physical security for deployment areas, relative cost, and undefined trust assumptions between peers. Thus, we propose a new attacker-centric threat model that is unique to TerraSwarm.

References

[1] Max Goncharov. Russian Underground 101. Technical report, Trend Micro, 2012.

[2] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. 1999.

[3] Edward A. Lee et al. The TerraSwarm Research Center. Technical Report UCB/EECS-2012-207, EECS Department, University of California, Berkeley, Nov 2012.

[4] Alessio Di Mauro, Davide Papini, Roberto Vigo, and Nicola Dragoni. Toward a threat model for energy-harvesting wireless sensor networks. volume 294 of *Communications in Computer and Information Science*, 2012.

[5] Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In *Proceedings of the 16th ACM conference on Computer and communications security*, CCS '09, 2009.