Confronting a Mobile Adversary in Unattended Sensor Networks

Gene Tsudik
Computer Science Department
Mr. Burns School of Information and Computer Science University of California, Irvine
gts@ics.uci.edu

ABSTRACT

Unattended sensor networks operating in hostile environments might collect data that represents a high-value target for the adversary. The unattended sensor's inability to off-load – in real time – sensitive data to a safe external entity makes it easy for the adversary to mount a focused attack aimed at eliminating or modifying certain offending data. In order to facilitate data survival, sensors must collectively attempt to confuse the adversary by changing the location and the representation of the data. Unfortunately, since the network is unattended most of the time, the adversary (even if it is limited in scale/scope of simultaneous compromise) has free reign and can move freely among sensors, compromising them at will.

A very similar "mobile adversary" model is quite well-known in cryptography, having spawned an entire line of research, called "proactive cryptography". However, the mobile adversary model has not been embraced by the security research community. This talk will address several flavors of the mobile adversary in the context of unattended sensor networks, discuss some viable and simple counter-measures (with varying degrees of effectiveness) and outline open problems and challenges.

ASIACCS '08, March 18-20, Tokyo, Japan