Reader-Powered RFID Denial of Service Attacks
Christos H. Xenophonostos, University of Illinois
ADVISOR: Yih-Chun Hu

Background
• Traditional DoS attacks on RFID jam the frequencies used by flooding them with signals.
• Such attacks are less power efficient than attacks that take advantage of the protocol.
• Our attack aims to be maximally power efficient, capable of using only power absorbed from the Reader signal perform a DoS attack by attacking RFID anti-collision protocols.

Goals
• To research the feasibility of attacking anti-collision protocols as a means of disrupting normal operation with minimal power use.

Research Plan
• Use a USRP radio along with GNUradio software radio to simulate a “rogue” tag and test possible attacks against anti-collision protocols.

Research Results
• Using a laptop running GNUradio Companion connected to the USRP we were able to receive and transmit signals to an RFID Reader (PCMCIA card with external antenna). Thus we can simulate a “rogue” tag.

Fundamental Questions/Challenges
• If the anti-collision protocols can be attacked with a “rogue” RFID tag, can we defend against these attacks?