CS 525W Mobil & Ubiquitous Computing

Project Update

Andrew Zafft
Computer Science Dept.
Spring 2011
The Problem

• The “Problem” is two part:
  – How tolerant is a wireless network to malware?
  
  – What is the effect (in terms of throughput) felt by other users in a wireless network infected by malware?
Big Picture

• Perform Research
  – Malware in general
  – Wireless network (WiFi) topology & structure

• Acquire/Build Applications
  – Custom Droid application
  – Wireshark & netcap

• Experiment
  – Infect a Droid phone with the “virus”
  – Capture network traffic both with a wireless listener and at the target machine
  – Analyze results
Where am I?

Big Picture
- Perform Research
  - Malware in general
  - Wireless network (WiFi) topology & structure
- Acquire Applications
  - Custom Droid application
  - Wireshark & netcat
- Experiment
  - Infect a Droid phone with the virus
  - Capture network traffic with a listener
  - Analyze results

Right Here

What I’ve done: Performed general malware research
Loosely studied wireless topology

Near Term: Decide method of malware (I’m looking at abusing RTS/CTS signals if possible)
Build malware application

Long Term: Run experiment
Analyze results