Final Project Proposal

Garret Naegle

Baseband Attacks on Mobile Devices

- Attacks mobile devices through use of cellular base stations
- Most baseband processors have few attack countermeasures (no ASLR, no DEP, etc)
- Is now dramatically cheaper to implement than before

Motivation to Research Baseband Attacks

- New/nontraditional attack vector
- Has potential to affect many people, so everyone should care about this
- Difficult to detect without expensive hardware

Past Research

- “Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks” by Ralf-Philipp Weinmann
  - Uses open source BTS to launch attack on iPhone 4 and HTC Dream to illustrate baseband vulnerabilities

Plans for Project

- Survey past attacks and how they were executed (1 week)
- Try to check if vulnerabilities exploited in past attacks have been fixed (2.5 weeks)
- Look into commands that can be issued to the baseband and what implications those commands have (0.5 weeks)

Plans for Project

- Find out if baseband companies are implementing countermeasures to prevent attacks (1 week)
- Research what more can be done to prevent and/or detect these attacks (1 week)

Questions?