Summary Slides

Things we agree on:

- Security is hard
  - Adversaries ⇒ Assumptions = vulnerabilities
- There is currently some science in security, but we would benefit from more
  - Process: hypothesis driven experiments
  - Results: abstractions and models, theorems (not just artifacts)
- We have made a lot of progress on point solutions and particular vulnerabilities, but need to find ways to *systematize* and *generalize* that knowledge

Charge for Breakouts

Identify some specific, well-defined, useful next steps

Charge Topics

1. What are the most important ideas from other fields that we should be trying to integrate into computer security?
2. Metrics: what are the steps toward more useful metrics?
3. Formal methods – reducing complexity
   1. Close to the intersection point for hypervisors, should we do this for other things?
   2. What can we do at the limits of formal methods?
   3. What can we conclude from it?
4. How should we build better adversary models?
   1. Using what we already know
   2. Learning things we need
5. Principles: do we have them all, or are there more fundamental principles to discover?
   1. How can we abstract from point solutions into general principles?
   2. How can we conduct experiments to validate principles?
6. How should we constraint the space to make problems solvable?
   1. Useful abstract models
   2. Assumptions