Academic Differences

- Limits to experience
- Limits to scope
- Different environments
- Different equipment
- Different policies
- Limited continuity & event horizon

- Sometimes larger view
- Fewer constraints
- Requirement to be “clever”
- Access to different sources of data and information

Next Steps

- Understand policy in clear manner
- Understand expected environment
- Vision of goals

- More clearly identify opportunities & strengths.

Some Thoughts

What Do We *Really* Want?

- Intrusion Detection
- Misuse Detection
- Anomaly Detection
- Performance Analysis
- Forensic Examination
- Easy to Use
- Infinitely Scalable
- Finds Unknown Conditions
- Easy to Maintain
- Updates Itself
- Standardized Testing
- Completely Portable
- Free of Charge

Redefine the Problem

We want understanding

- Of program interaction
- Of system interaction
- Of user behavior
- Of fault and exception consequences

Note: is there any way to distinguish a bug from a fault from a mistake from a violation of security, in general?

Maybe we’ve been asking too narrow a set of questions?