Agile Applied Research for Cybersecurity

Rick Linger, ORNL
Luanne Goldrich, JHU/APL
Matt Bishop, UC Davis
Melissa Dark, Purdue

Acknowledgements: DoE contract DE-AC05-00OR22725 to UT-Battelle, LLC;
NSF grant DGE-1303211 to UC Davis, DGE-1303048 to Purdue Universiy

Research Gap

- Traditional research aimed at developing, understanding, applying foundational work
- But sometimes problems require
  - Short term research leading into …
  - Better understanding of the problem
  - Results that can be applied quickly
  - What long-term research would be most useful and interesting to deal with the problem over the long term

Agile Research

- Exploratory research where speed is overarching requirement
- Contribution: merge
  - Exploratory methods that focus on applied research
  - Academic, broader methods that focus on foundational research

Innovation

- Institutions produce technical change via research and development
- Institutions are places *and social roles*
- Innovations change both social roles of these places and social rules by which they interact
  - Example: Bayh-Dole Act (1980)

Agile Research Basis

- Sponsors pose research questions
- Researchers carry out the research and produce results
- Done iteratively, and with sponsors able to reframe the direction of the research if needed

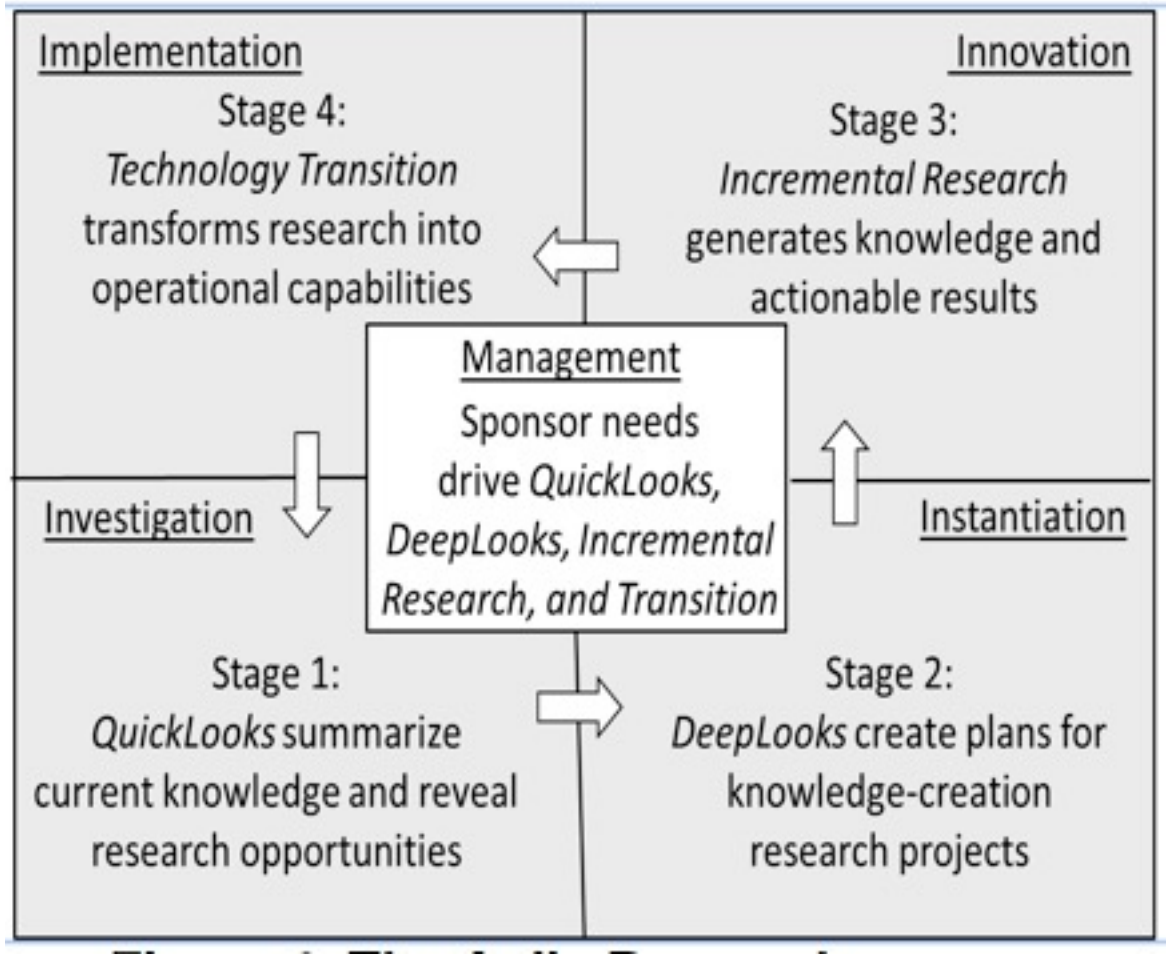
Agile Research Principles

- **Predefined Infrastructure**: resources, logistics defined and allocated *before* research needs emerge
- **Incremental Research**: structured into iterative, short-term, accumulating increments each producing something of value to sponsor

Agile Research Principles

- **Incremental management**: process provides built-in, short-term checkpoints for sponsors to understand research, redirect if needed based on incremental results
- **Transferability**: one group may carry out research, but must do so in a way that allows the current state to be transferred to another group if necessary

Agile Research Process



Agile Research Properties

- Flexible
- Anticipatory
- Staged
- Speedy
- Visible
- Effective
- Impactful
- Incremental

Example: Data Tagging

- Problem: use data tagging to support access and retention policies
- Research questions from QuickLook Study:
  - Examine current use of data tagging for ABAC, with policy-based attributes and tags used for a large enterprise
  - Identify technologies that can be adapted to data tagging needs
  - Research how to use data tagging to support access, retention policies
  - Identify other relevant research objectives

Data Tagging Way Forward: Recommendations

- Define a path forward in light of the complexity of the problem
  - Organize complexity of problem using structured, divide and conquer refinement of goals and requirements
  - Explore existing data tagging solution space for cost-effective application to the problem set to address sponsor needs
- Conduct incremental research and development.
  - Research tag representation and management as foundation for information sharing
  - Develop proof of concept system to explore and evaluate potential solutions

Data Tagging Solution Space: Recommendations

- There are promising existing commercial solutions.
  - Run public challenge for data tagging to elicit potential solutions
  - Conduct data tagging product evaluations
- Sponsor organization is beginning to pilot solutions for enterprise data tagging in several areas
  - Study data tagging design patterns of sponsor organization
- Other organizations beginning to tackle enterprise data tagging
  - Evaluate design patterns used in sponsor organization
  - Investigate an earlier sponsor organization information discovery and assured access study

Data Tagging Requirements Analysis: Recommendations

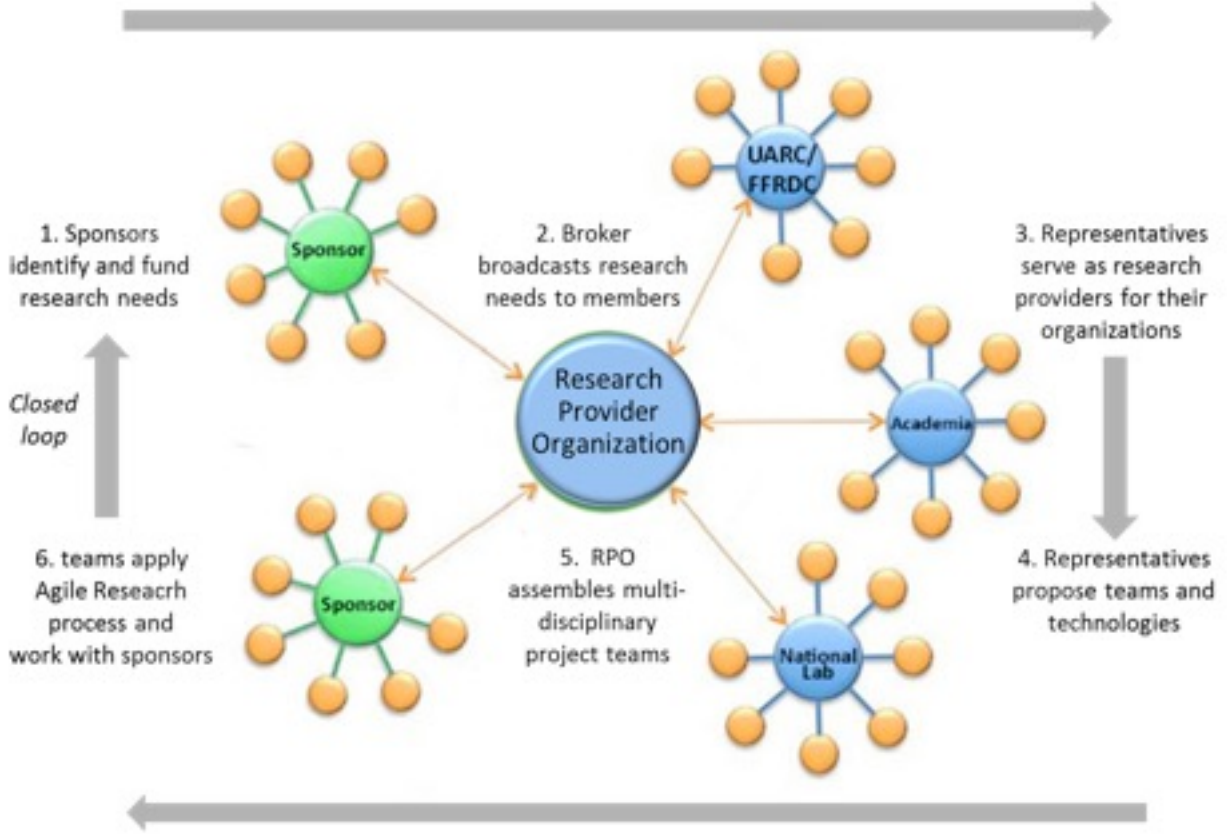
- Problem domain too complex to tackle with traditional requirements specification
  - Conduct structured engineering assessment to define incremental development, deployment stages
- Information architecture needed for data tags
  - Develop a data tagging Concept of Operations
  - Conduct an organizational inventory of attribute data
  - Assess taxonomies, ontologies for representing tags.
  - Conduct study of trade-offs between tagging data at rest and on the fly

Data Tagging Requirements Analysis: Recommendations

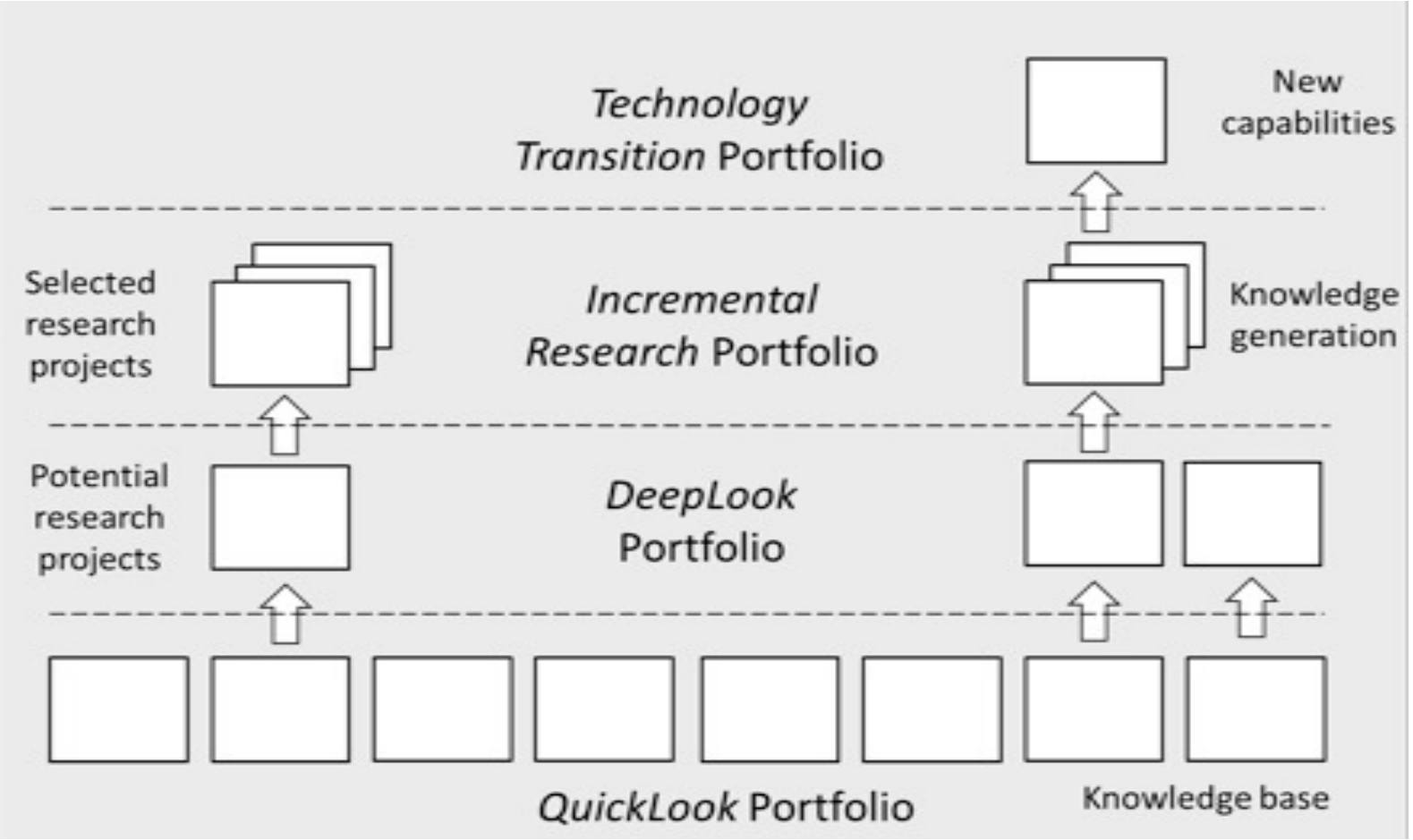
- Tagging technologies, mechanisms must be secured.
  - Identify potential threats and vulnerabilities.
  - Develop security reference architectures for data tagging
  - Assess efficacy of Identity-Based Internet Protocol (IBIP) to secure data tagging network

Lots of grist for DeepLook Step! Also suggests several foundational research questions

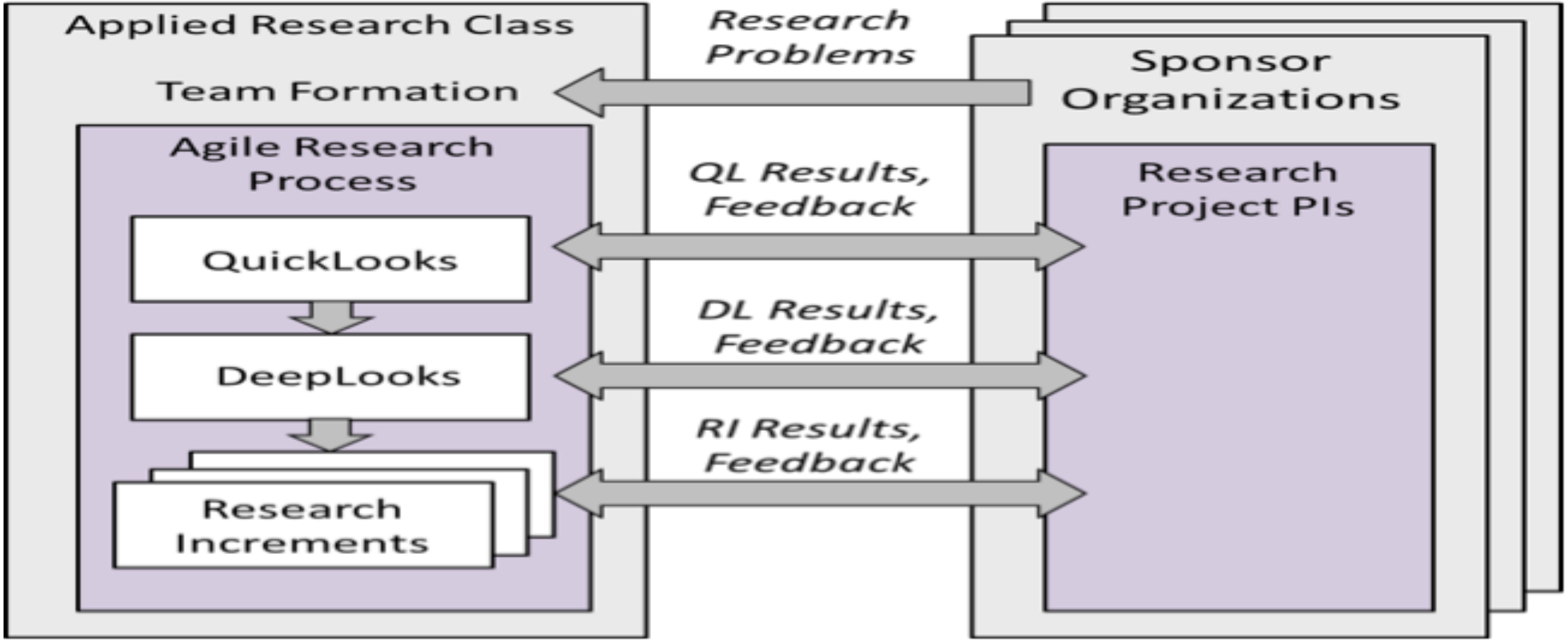
Agile Research Structure



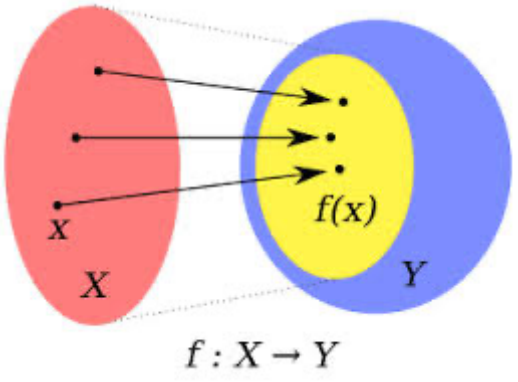
Agile Research Portfolio



Putting It Together



Mapping of INSuRE to Agile Research



- Bid, proposal ➔ QuickLook
  - Difference: students don't identify subject matter experts; instead, explain why they should be considered (or will become) experts
- Proposal preparation ➔ DeepLook
  - Presents goals, what the research plan can be expected to accomplish
- Research ➔ Incremental Research Stage
  - Weekly meetings allow sponsor to adjust goals of research to meet needs, and based on weekly outcomes