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
Definition of Research

Research is what I’m doing when I don’t know what I’m doing.

— Wernher von Braun
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

- **Stage 1:** QuickLooks summarize current knowledge and reveal research opportunities
  - DeepLooks create plans for knowledge-creation research projects

- **Stage 2:**
  - Incremental Research generates knowledge and actionable results

- **Stage 3:**
  - Technology Transition transforms research into operational capabilities

- **Stage 4:**
  - Management Sponsor needs drive QuickLooks, DeepLooks, Incremental Research, and Transition
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
INSuRE Project

• Focal activity: cybersecurity research class
  – INSuRE stands for INformation Security Research and Education

• Sponsors propose problems
  – If selected, sponsor expected to provide guidance, feedback students in conjunction with faculty
  – Sponsor must agree that, if results merit publication, the research can be published
    • So far, no problems with doing this
Overview of Structure

1. Project bid
2. Project proposal
3. Literature review
4. Progress report and presentation
5. Final report, presentation for schools on semester system
   –Penultimate report, presentation for quarter system
6. Final report, presentation for schools on quarter system
Set-Up

• Faculty solicit research proposals from (potential) sponsors
  – Typically, a paragraph describing problem in general terms
  – Examples
    • Identifying ICS components in a network
    • Code variation as a defense against attacks
    • Analysis of proposed TCPcrypt protocol

• Sponsors then “pitch” the projects to the students in first 1 or 2 class meetings
Research

• Students meet weekly with sponsor, faculty to report progress, challenges encountered and overcome, next week’s goals

• Goals may change based on challenges found
  – Allow sponsors to modify incremental research goals
  – Sponsors can apply intermediate results as work progresses
  – Students see their work being used
Reports

• Weekly progress reports
• Midterm progress report
  – Delivered as formal paper, presentation to all participating teams
• Final report
  – Also delivered to all teams
• Critical idea: document results, tools, datasets so that another team can pick up where this team left off
  – Teaches data curation
Putting It Together
Mapping

• 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
Questions

• How to determine when to use Agile Research rather than (or in addition to) long-term research
• How to develop intermediate goals so that:
  – Incremental results are useful
  – Incremental results will enable the sponsor to provide further guidance to the research group
  – Incremental goals will provide insight into the foundational research necessary to provide deeper understanding of the problem and, possibly, long-term solutions (this, especially in an academic setting)
Conclusion

• Long-term research questions arise from Agile Research projects
  – Agile Research is applied research towards a particular, pressing end
  – Thus, ideal for identifying interesting long-term research projects

• Agile Research exhibits properties that are critical to research involvement in the fast paced and unpredictable world of cybersecurity
Closing Thought

• To those accustomed to the precise, structured methods of conventional system development, exploratory development techniques may seem messy, inelegant, and unsatisfying. But it’s a question of congruence: precision and flexibility may be just as dysfunctional in novel, uncertain situations as sloppiness and vacillation are in familiar, well-defined ones. Those who admire the massive, rigid bone structures of dinosaurs should remember that jellyfish still enjoy their very secure ecological niche.

— Beau Sheil, “Power Tools for Programmers”