Software & Supply Chain Assurance Summer Forum
July 14, 2016

Reducing Software Vulnerabilities: Overview

Barbara Guttman
Leader, Software Quality Group

Session Goal

- We have a draft list of ideas for reducing software vulnerabilities
- We want your ideas & insights
  - Improve our current ideas
  - Add new ones
- How?
  - Comment during the session
  - Send us email
  - Volunteer
    - Help brainstorm ideas
    - Help write sections
    - Critique sections

- Email: bguttman@nist.gov; paul.black@nist.gov; lee.badger@nist.gov

What Will be the Result?

- End Product: a report entitled “Dramatically Reducing Software Vulnerabilities”
- Draft anticipated by the end of September 2016 for public comment
- Final report to White House by November 2016

- Timeline is very short

What Will the Report Look Like?

I. Introduction/background/motivation

II. Overall Approach

II. Major Ideas (6 so far)

A. Idea 1 (each 3-5 pages)

1. Define idea,
2. How mature is it?
3. References

….

IV. Metrics (5-10 pages)

V. Summary and Moving Forward

Who Will Care?

- Future administrations
- Future program managers
- The software assurance and security communities

  - This problem isn’t going away

Why these ideas?

- Have potential for dramatic improvement
- Have the potential for impact in 5 years
- There are lots of great ideas that aren't in scope
  - X Anything about funding e.g., stable funding for key community resources
  - X Grand challenges and other ways to get new ideas or get them built
  - X Research topics such as increased research on bugs, software composition
- Metrics is in but not being discussed today
  - Workshop was held July 12

Draft List of Ideas

- System Level Security (Lee)
- Resilience (Lee)
- Software Development Frameworks (Paul)
- Additive Software Analysis (Paul)
- Formal Methods & Richer Programming Environments (Rich)
- Program Diversity & Moving Target Defenses (Konrad)

(There is some overlap and some of the topics have subtopics. All of them have ambiguous names. We have 4 presenters to walk you through them.)