

Software Assurance (SwA) for Cloud and Handheld Applications

Jeff Voas

March 12, 2010

Cloud

- *Trust* is a central theme of the cloud continuously in the literature
 - DARPA, ISAT Meeting, “Black Cloud” March 25-26, 2010
 - B. Michael and G. Dinolt, “Establishing Trust in Cloud Computing”, *IAnewsletter*, Vol 13 No. 2, Spring 2010.
- SLAs appear to be the only contractual verbiage related to trust but SLAs remain suspicious in *intent* and *enforcement*.
- Why? What is the evidence needed to form a *well-defined* SLA and where is it collected from?
- Several SwA Working Groups seem closely aligned to ideas that address this issue:
 - Processes & Practices
 - Technology, Tools & Product Eval.
 - Acquisition & Outsourcing
 - Measurement
 - Malware

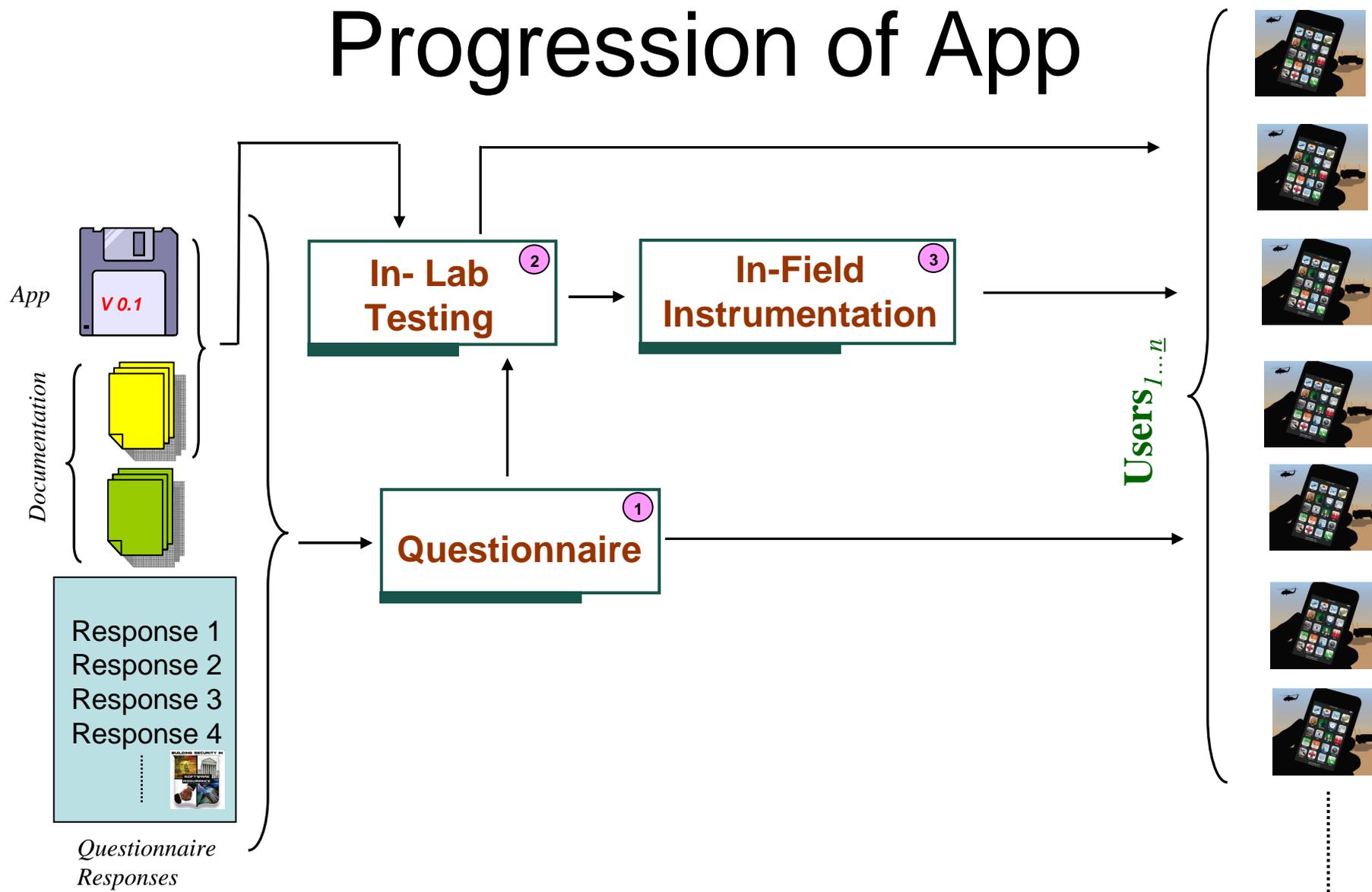
Cloud (cont'd.)

- Potential idea is to hold a 1-day workshop for the how the work from the SwA community applies to “trust” in the cloud during the June 2010 series of meetings.
- Next step: further discussions with Joe Jarzombek

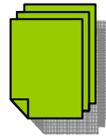
Handheld Applications

- NIST is looking to stand up an evaluation process using the work from this SwA community as one piece of a 3-piece puzzle (discussed in next slides).
- The result would be an evaluation lab, somewhat similar to NIST SAMATE, however focused on military applications of handheld devices with both application security evals and “system of system” evals at a higher level. Assurance cases for this higher level are appropriate.
- Time is of the essence for this effort for Iraq and Afghanistan.

Progression of App



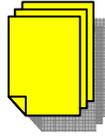
Questionnaire Approach ①



*Documentation:
(Organization, Processes Followed, Tools)*



*Software Documentation
Including Requirements*



*Initial App
Version*



**Third-Party Validation
of Selected Developer
Answers**

Developer

Response 1
Response 2
Response 3
Response 4
⋮

*Self
Assessment:
Questionnaire
Responses*



DHS Software Assurance

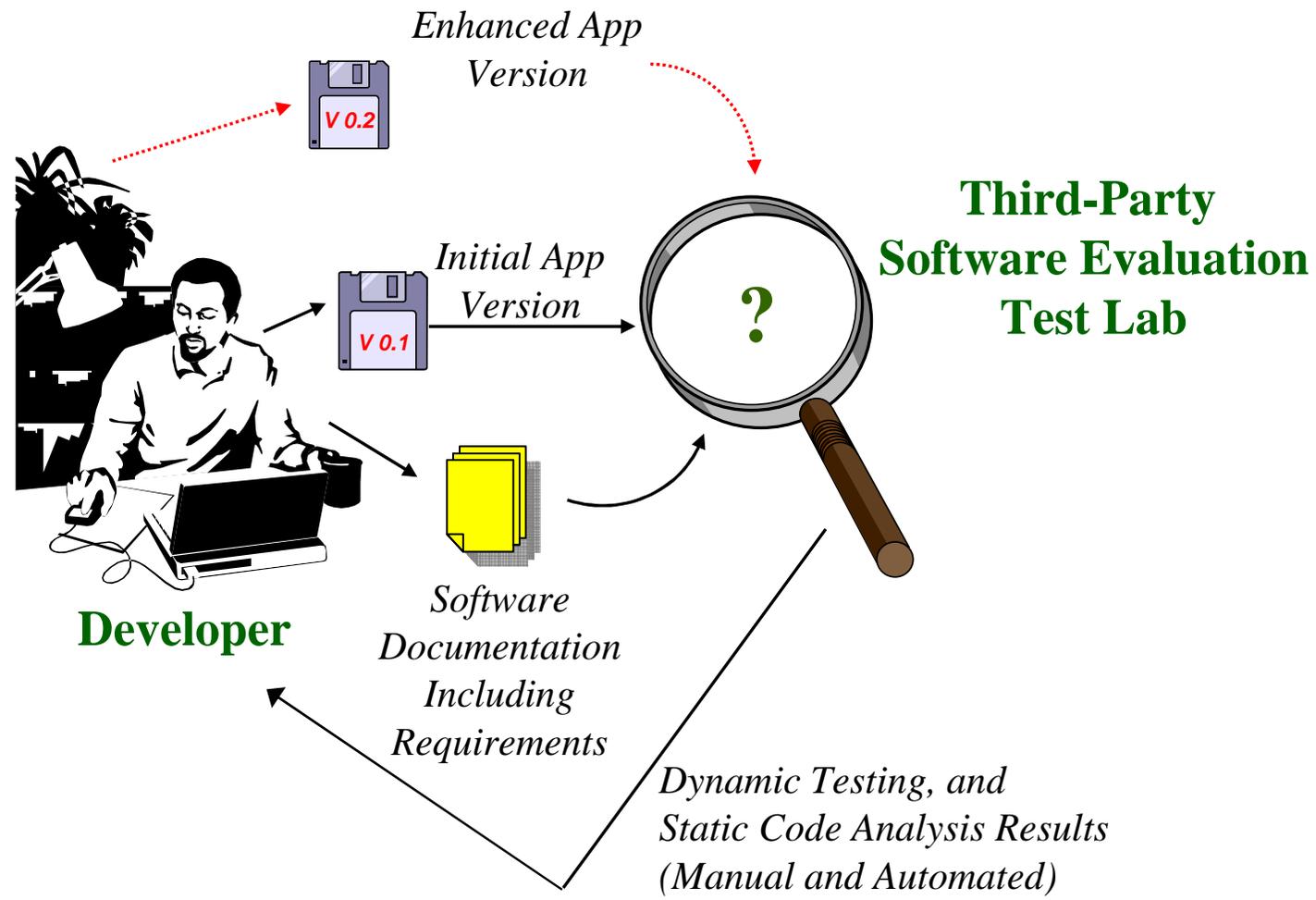
Questionnaire for Acquired Software

[Ref: Software Supply Chain Risk Management & Due-Diligence, Vol. II
Version 1.2, May 24, 2009 (Draft), DHS]

Results

- An examiner will review the responses from the developer
- A human evaluation of trust in the responses is made
- If questionable, developer may be asked for clarifications or app recommended for re-work
- If believed, app is ready for handheld deployment or for next two assurance approaches

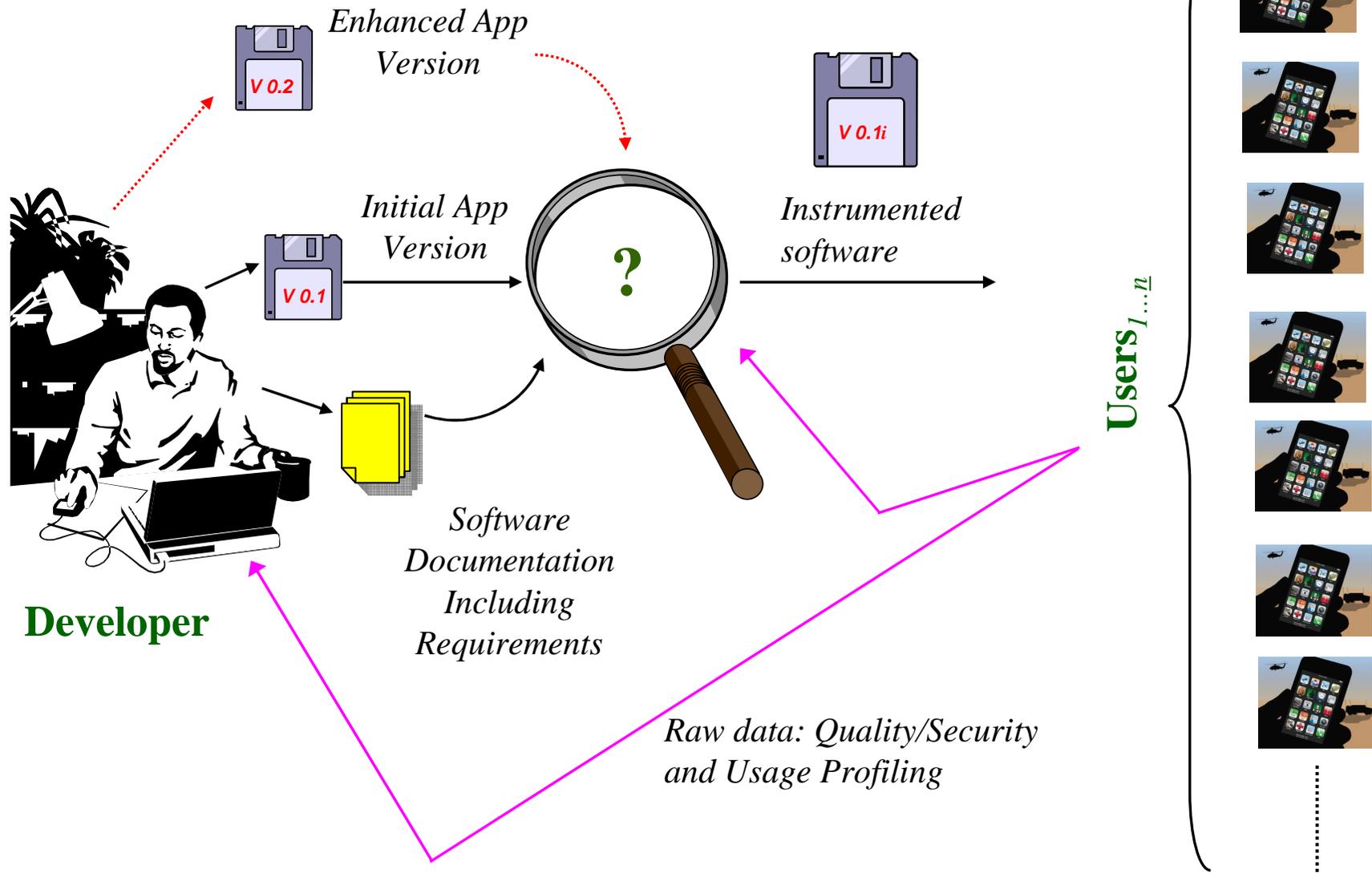
In-Lab Testing Approach ²



Results

- Dynamic reliability and *performance* measurement of the product in the lab under assumed operational profiles.
- Static analysis of the source code using COTS and open source tools that search for programming errors such as buffer overflows.
- Use Automated and Manual analysis of the top 25 Common Programming Weaknesses
[<http://cwe.mitre.org/top25/#ProfileAutomatedManual>]

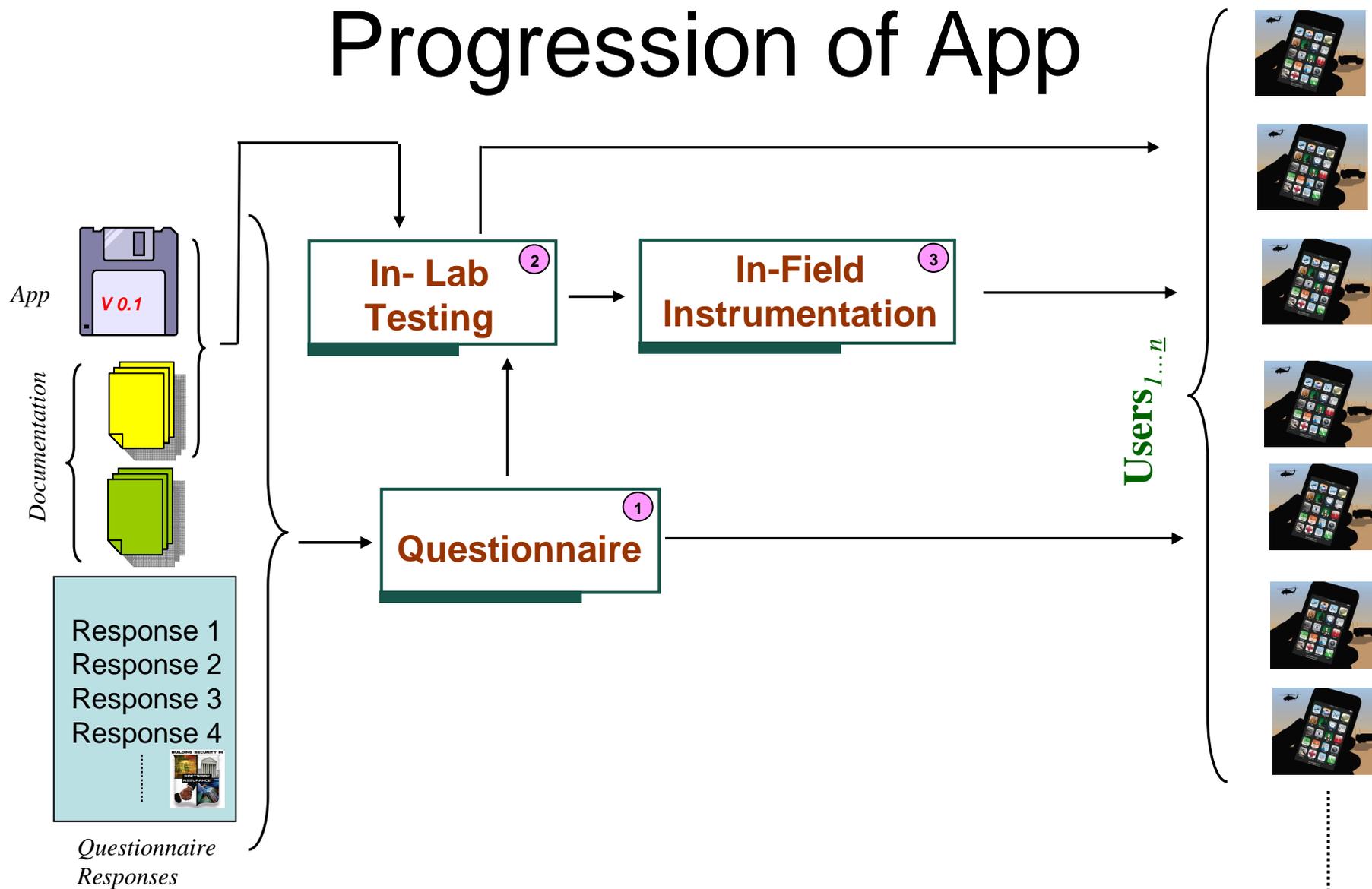
In-Field Instrumentation Approach 3



Results

- Typical types of data collected might include:
 - Amount of time an app is executed
 - Type and amount of data transmitted
 - Feature usage within an app
 - Number of exception calls
- Benefits include: (1) usage data that can be used for billing, (2) reducing bloatware, and (3) additional app testing
- Note: Instrumentation can be turned on and off easily, and done selectively as well. Also, instrumentation does incur performance and footprint hits.

Progression of App



Proposed Two-Phase App Evaluation Roll-Out Strategy

Phase I

Questionnaire ¹

Phase II

In-Lab Testing ²

In-Field Instrumentation ³

