Software Assurance CBK and University Curricula

Matt Bishop
Sophie Engle

UC Davis
Computer Security Laboratory

Contact Us

- Matt Bishop Sophie Engle
- mabishop@ucdavis.edu sjengle@ucdavis.edu
- Department of Computer Science
- University of California at Davis
- One Shields Ave.
- Davis, CA 95616-8562

SwACBK

- No standard or agreed-upon body of knowledge for software assurance education
- DHS, DoD began effort to define CBK in 2004
  - "to provide an inclusive list of the knowledge needed to acquire, develop, and sustain secure software"
  - Also "to help … academia target [its] education and training curricula"

Goal of Talk

- Suggest changes in this SwACBK that will make it more useful as a basis for curriculum development
  - Restructure to emphasize principles
  - More comprehensive framework to base levels of abstraction on
  - Include more seminal references

Background

- Academic curriculum emphasizes principles, concepts
  - UC Davis: "courses should present an integrated body of knowledge, with primary emphasis upon elucidation of principles and theories rather than upon the development of skills and techniques"
- Why: students must be prepared for wide variety of environments (gov't, industry, personal, etc.); technologies will differ, but foundations, concepts, principles the same

Secure Software

- §5.2.5: interdependence of components
- "[s]ecurity inspired requirements on nature and attributes of computing hardware, infrastructure, or other externally available services must be explicitly recorded as requirements or assumptions and assured"
- §8 (Secure Software Verifcation, Validation, and Evaluation):
  - No discussion of requirements, assumptions; implication is once validated, software can be moved anywhere and still be safe

Orientation

- Parts of SwACBK overlook non-governmental requirements
  - §2.2: background on risks, threats
    - Examples focus on government agencies, national security; industry mentioned in an aside; academia ignored
  - §7.2.1: list of sources of vulnerabilities, patches
    - Omits SecurityFocus, OSVDB, X-Force

Classifications

- Taxonomies non-rigorous, confusing
  - §6.7 (Architectures for Security):
    - "Reference monitors", "layered", "system high", "filters, guardians, firewalls"
  - §2.4 (Methods for attacks):
    - Against operating system; against software; against physical system

Basis and Depth

- Too little on concepts, principles
  - Saltzer & Schroeder, plus "Defense in depth", "Analyzability"
  - Models: no integrity models; only confidentiality Bell-LaPadula model
  - Malicious logic: Trojan horse = backdoor
  - Reference monitor: mentioned 4 times, not explained in detail
  - Trade-off between dynamic, static analysis

Motivation

- Motivates importance of software security
- Often omits motivation for individual facets of software assurance
- §9.5 (Static Analysis)
  - Says techniques conservative, "making worst case assumptions to ensure the soundness of the analysis"
  - May or may not be true (which is worse, false positives or false negatives?)

References

- 6 references to before 1985
  - One mention of collection of historical, seminal papers
- Should add references to seminal works
  - Reference monitors in Anderson (1974), but only 2003 book cited
  - Trojan horse in same report, but cites book from 2005
- Miss much of reason for, richness of, term

Use in Higher Education

- Undergraduate education
  - Should emphasize reinforcement in *all* courses, not just software engineering courses
- Graduate education
  - Suggests using training guidance for incoming grad students
  - No mention of teaching principles
  - Focuses on acquiring skills to develop secure software

Improving SwACBK

- Separate *functionality* from *assurance*
- Organize chapters around principles
  - Leads to good classifications
- Examples from industry, academia
  - Including personal security
- Choose original reference sources
  - Say why each reference is there
- Expand discussion of principles, concepts
  - Much more on reference monitors, etc.

Conclusion

- Long way to go before SwACBK useful as basis for academic curriculum
- *Excellent* that this discussion has started
- Now need to do it right!