DHS-DoD Software Assurance Forum Workforce Education and Training Status Briefing

Samuel T. Redwine, Jr., Chair

James Madison University

October 3, 2007

Homeland Security

Agenda

- Working Group Context and Goals
- Current Emphases
- July 11 Meeting
- Principles and Guidelines document
- Planned revision of Software Assurance Common Body of Knowledge
  - Current Situation
  - Plans
- Short-term Outcomes

Homeland Security

Workforce Education & Training Working Group Purpose Context

- Producers supply (more) secure software
  - **Workforce has ability to produce (more) secure software**
  - And organizations provide context (e.g. processes, tools, environment) and successfully use this workforce ability
- This software widely deployed and successfully used
  - Acquired and sustained
- Software-intensive systems in use are (more) secure
- Damage and danger reduced

Homeland Security

Workforce Education & Training Working Group Goals

- Have software security and assurance successfully included in
  - Higher education
  - Workforce training
  - Elsewhere, e.g. standards and guides
- Objectives
  - Provide underlying basis – e.g. Software Assurance of Common Body of Knowledge
  - Promote and motivate – e.g. publicity, encourage faculty or institution, personnel certification, higher education accreditation
  - Facilitate – e.g. educational and training materials, book publications
  - Build community and provide a means for communication and cooperation among interested parties

Homeland Security

Workforce Education & Training Working Group Current Emphases

- Propagate Software Assurance Common Body of Knowledge contents usage in
  - Higher Education
  - Training
  - Personnel Certification
  - Standards, guidelines, and improvement efforts
  - Individuals and organizations
  - Other Software Assurance Working Groups (multi-way interaction)
- Systematize software system security principles and guidelines
- Revise Software Assurance Common Body of Knowledge (CBK) for by October 2007

Please let us know of relevant contacts in these areas

Homeland Security

July 11 Meeting

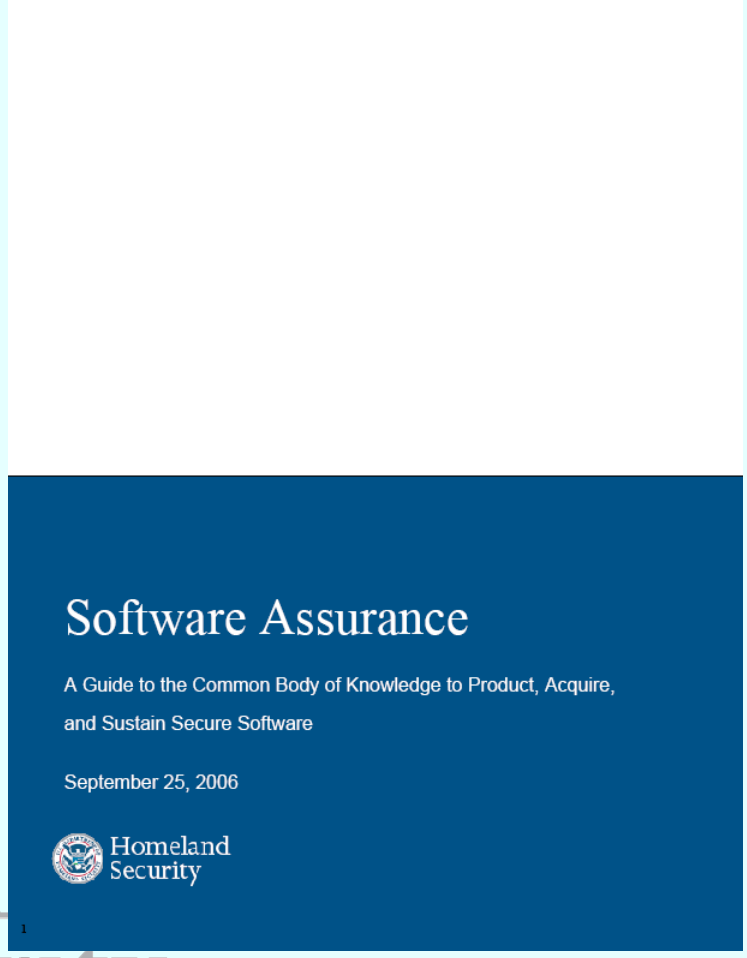
- Brenda Oldfield, DHS, *Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework*
- Status and Planning for revised version of SwA CBK
- Discussion of CBK changes
- Discussion of usage situation and technology transfer

Homeland Security

Software Assurance Common Body of Knowledge (SwA CBK)

Version 1.1

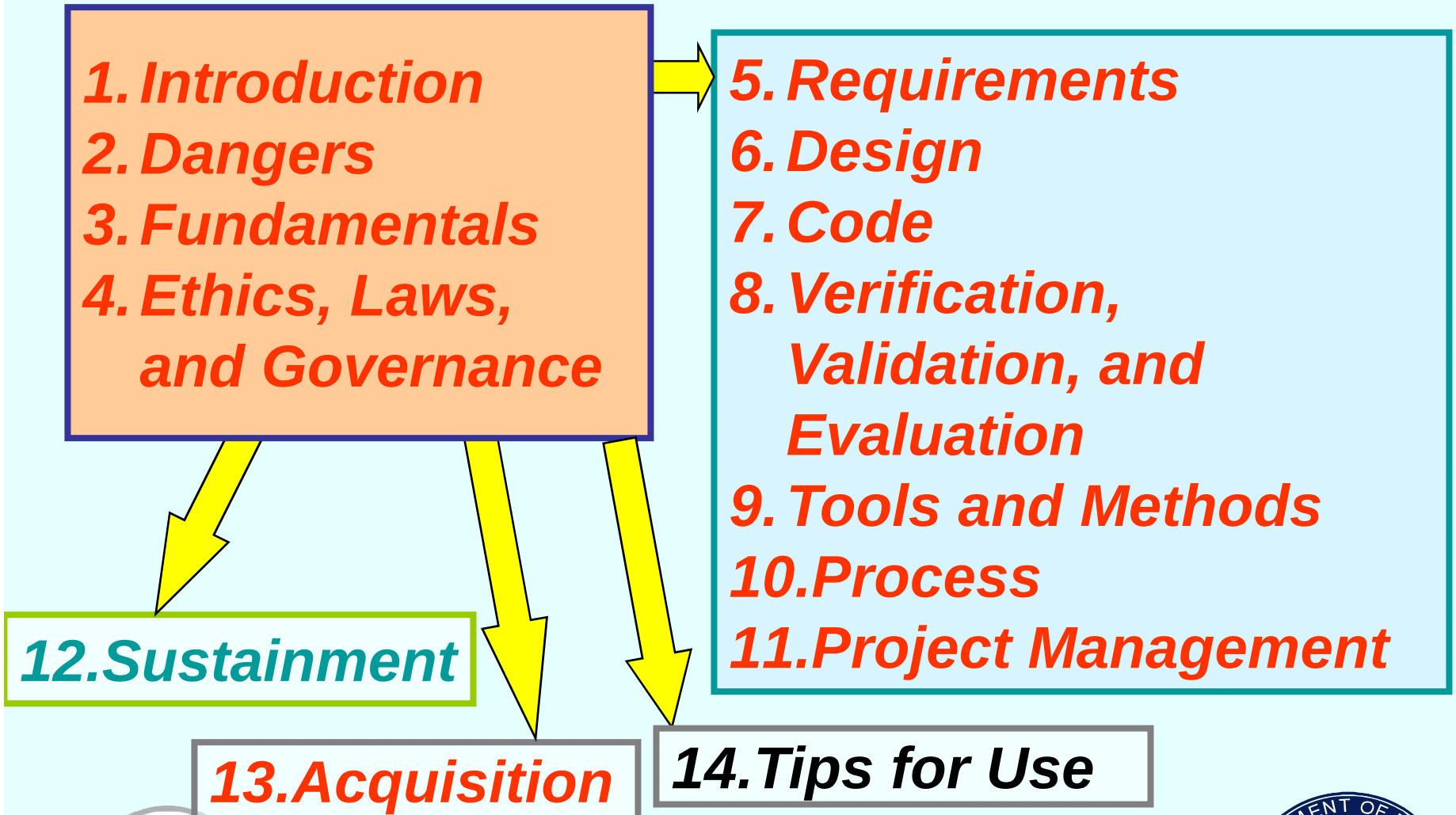
Ready for Use



Example Users

- Detroit Mercy
- JMU
- Mississippi State
- UNCC

Overview of SwA CBK version 1.1



Homeland Security

Document History

- Spring 2005
  - Collected lists of added or changed activities
  - Formed subgroups & assigned authors
- Summer2005
  - Started writing in June
  - Many iterations within Working Group
  - Draft distributed at October 2-3 Software Assurance Forum
- 2006 versions
  - January 23
  - March 14
  - April 17
  - May
  - July
  - September 25 version 1.1
    - Mature and ready for wide use

Homeland Security

Revised Version of SwA CBK

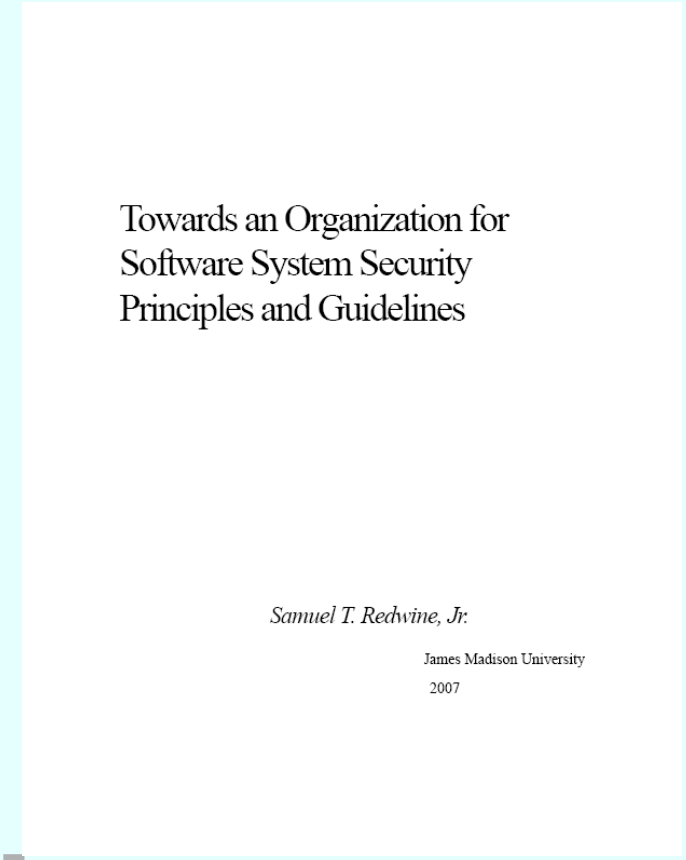
- Current version 1.1 is mature and has received wide praise
- The three main purposes of the revision are
  - Update the document to reflect developments and references of the last 15 months in
    - software security and assurance
    - experience with use of the CBK
  - Systematically include the work on organizing software security principles and guidelines
  - Expand a few weaker sub-areas
- In addition, two lesser purposes exist
  - Placing reference entries not only in bibliography but at the end of each major sections
  - Make minor editorial improvements
- The overall purpose and audiences remain unchanged
- Progress has been slow since start of revision in May
- Input from other WGs could help
- Still need volunteers to help

Homeland Security

Organized Principles and Guidelines

Fifteen Months in Development

Small Group plus wider review


Towards an Organization for Software System Security Principles and Guidelines

Samuel T. Redwine, Jr.

James Madison University

2007

Homeland Security

Organize Principles and Guidelines

- Top Level Breakdown (Timelines of)
  - The Adverse (bad guys + mistakes by good guys)
  - The System (good guys, and good and bad things)
  - The Environment
- Second Level
  - Nature/Size, Benefits, Losses, Uncertainties
- Third and lower levels are principles and guidelines layered by inclusion, or cause and effect

Homeland Security

Conceptual Example

- Limit, Reduce, or Manage Uncertainty
  - Predictability
    - Verifiability
      - Analyzability
        - » Analyzable Compositions (Compositionality, Composibility, Additivity)

Homeland Security

Example Substructure (Partial)

- *Purpose: limit opportunities for violations*
- Accurate Identification
  - Positive Identification
  - Adequate authentication
    - Valid, tamper-proof identification-related data
- Separate Identity from Privilege
- Positive Authorization (part of Fail-Safe Defaults)
- Least Exposure
  - Isolation from Source of Danger
    - Isolation of user groups
      - Isolate publicly accessible systems from mission-critical resources
    - Domain isolation
  - Continuous Protection of Assets
  - Complete Mediation of Accesses
    - Tamper Proof or Resistant
  - Least Privilege

Homeland Security

Workforce Education & Training WG Short-Term Outcomes

- Revise and Publish
  - Software Assurance CBK (including review)
  - Principles and Guidelines Report
- Efforts within
  - Object Management Group
  - DoD and National Defense Industry Association
  - DHS
  - Drafting of proposed IEEE/ISO 15026 System
  - Other Software Assurance Working Groups
- Wider availability and use of SwA CBK and Principles and Guidelines documents

Homeland Security