Practical Software and Systems Measurement

A foundation for objective project management

Security Measurement TWG

PSM Security TWG Meeting
26, 27 July 2006

John Murdoch, Cheryl Jones

General Objectives of PSM TWG

- To support the application of measurement principles and practices to the development, acquisition, assurance, operation and maintenance of dependable software-intensive systems
- General Strategy:
  - apply PSM and ISO/IEC 15939:2002
  - develop guidance materials in the PSM framework
  - collaborate with other groups: UK MoD, DHS NCSD SW Assurance working groups, NIST, ISSEA MWG (ISO/IEC 27004)

Progress

- Existing TWG outputs
  - Safety Measurement White Paper v3
  - Security Measurement White Paper v3
    issued in January 06
  - Draft security measurement ICM Table
- Recent Meetings
  - 16 March 06, SW Assurance Forum DHS
  - 29-30 March 06, TWG, SSCI, Herndon, VA
  - 9 May 06, TWG, SW Assurance Forum, BAH Arlington
  - 20 July 06, SW Assurance Forum, BAH Arlington
- Recent Events
  - 14,15 March 06 ISSSE Conference, Arlington
  - 17-19 May 06 ISSEA Annual Conference, Ottawa

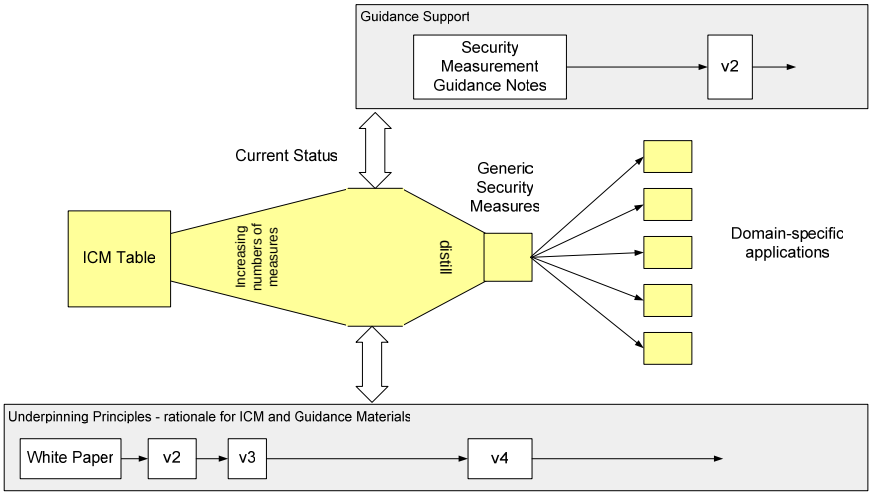
Recent Materials from Collaborating Groups

- Outputs from DHS SW Assurance Forum meeting 20th July 2006
  - Metrics WG outbrief: Nadya Bartol
  - SW Assurance CBK Definitions matrix
  - Acquisition Guide
  - Assurance cases and stds harmonization (SC 7)
- ISSEA MWG
  - measurement table
  - Draft 27004 – security msmt (SC27)

Current Issues for the PSM TWG

- *Large numbers of prospective measures are being identified, covering different aspects of security; meeting different needs*
  - *How to structure/ organize guidance material? How to keep the ICM Table to a usable size?*
- *Demand for practical guidance: how best to mature the work into guidance materials of use to practitioners?*
- *Methodology: to develop measures further, we need to engage with domain specialists in a systematic way: how best to do this?*

Current Status of PSM TWG



Current TWG To Do List

- Review work of and support collaborating groups
- Review White Paper (underpinning) work
- Review Security ICM Table and distil into a generic form
- Develop Security Measurement Guidance Documentation: plan and draft
  - Include how to apply the generic measures to a domain specialty: 'security-specific version of the PSM 15939 msmt development process'
  - Generic Measurement Specification examples
- Draw up a plan to develop measurement instances in different domains - with outline proposals

Later on

- Security Measurement Training Package
- Security Measurement Trials Reports

Objectives of this Workshop

- Discuss ICM Table distillation down to a 'generic essence' for security
- Discuss process/tasks to apply generic measures to a particular domain ('instantiate' the generic table) – take sw devlpt process as example domain (or other if preferred)
- Planning for development with specialists:
  - Map of relevant domains
  - How to engage efficiently and effectively
  - Relationships between domains

Workshop Agenda

Wed 26th July 2:15 – 5:30 (break 3:45 – 4:00)

2:15 Overview of progress

2:30 – 3:15 De-Brief of DHS NSCD workshop 20th July 2006

3:15 – 3:45 Review of Security Measurement fundamentals

4:00 Break-Out 1: Review ICM Table and distil to a minimum generic set of measures, applicable to 'any' specialist domain

5:15 Report back

Workshop Agenda

Thu 27th July 8:30 – 12:00 (break 10:00 - 10:30)

8:30 Review of measurement development process

9:00 – 10:45 Break Out 2: Application of generic measures to a specialist domain

10:45 Report Back

11:15 – 11:45 Planning for Development

- **Map the application domains of concern**
- **Methodology for engaging with specialist groups**
- **Integration**

11:45 Define actions and plans for next workshop

12:00 Close