Security Workshop March 2005 Outbrief

Attendees

Joe Jarzombek
Greg Larsen
James Moore
Phil Flora
Iona Rus
Cheryl Jones
John Murdoch

Input Materials

PSM TWG Security Measurement White Paper v1.0

Joe Jarzombek's commentary on White Paper, with questions: *Initial Review Of The Draft Technical Paper On Security Measurement*

Greg Larsen's presentation: *Strategic Observations and Thoughts on a System Model for Security Metrics/ Measurements: why can't we get traction?*

Vivian presentation DoD Information Assurance (IA) Metrics Program", Kristy Branstetter, International Business Machines

Outputs

Discussion Notes (below)

Potential Work Plan to develop Security Measures (PSM and other initiatives)

Summary

Going into the workshop, we had a first draft White Paper on security measurement plus expressions of need for security metrics (CRS report etc). We lacked awareness of some related efforts. We were looking to test reaction to the White Paper and to plan further work. Implication: we need to connect the PSM effort with other related work and develop additional effort to support 'systemic' security issues (including methods etc to support the adjudicator role, identified in Greg Larsen's work).

One reaction to the PSM White Paper: "good start, but it assumes the business case is adequately and properly articulated with its own set of metrics and measures." Implication: need to reference other PSM measures from the White Paper.

Related work includes (from Greg's presentation):

- Threat-based Risk Management Methodology - JHU/DoD study of foreign influence on Telecommunications Industry –Great start on security demand metrics, but… only a smart part of one-half of the business equation

- IA Metrics - DoD; NR-KPP; NCOW-RM –Great start, but… it assumes same issue as PSM-TWG and has no data models

- WP - Office of the Chief Engineer; SPAWAR, Charleston –Great warfighter scenario driven and technology agnostic approach to a net-centric security characterization, but… again it assumes same issue as others and has no analytics to align and compare the conceptual and logical technical data models to the metrics and measures of a business-case

- Uncertainty Analysis and Parameter Tolerancing - Castrup; 1992-2001+ –Great analytics, but… nowhere to apply it

"Each (inc the PSM White Paper) is individually a heroic effort for which there is no connective tissue that makes it relevant and significant to the people and organizations that make the adjudication decisions about efficacious demands for security and commitments to supply security affordably."
Vivian Cocca's IA Metrics DoD presentation reported on practical work to collect existing security measures (700 metrics etc) – second item above.

Joe Jarzombek (US DHS) and Paul Caseley (UK MoD) are wishing to encourage this work.

Action: PSM TWG is to respond with a suggested Work Plan, elements of which suggested for the PSM project. In particular, identify near term tasks that can be addressed before July, for review at the PSM Users Group meeting.

Action: PSM to explore collaboration with the DoD metrics work.

Action: Greg Larsen to provide above referenced documents, where possible.

Discussion Notes

Based on the questions from Joe Jarzombek's *Initial Review*.

1. What is the capability/competence of the resources deployed on security? (this should address operations, acquisition/procurement, and development -- how would this be objectively evaluated/appraised, and how can it be linked, as appropriate, to safety?)

What is the capability of this supplier? What are their process capabilities? What are the attributes of a secure product? What are the artifacts of the processes that provide evidence of a secure product? (c.f. QA methods)

What is the capability of the demand side? Capability of specifying needs? What are my needs, constraints, trades?

What is the capability of the adjudicator role? Prioritization of security threats. Tell me the product limitations and the product devlpt process limitations.

COTS product suppliers: threat modeling? Crashing/ suitability for use?

Differences between certification lab processes: how to develop commonality? 'Gold standard' tool sets for standard contexts? Require products to be tested against a reference checker/ suite of tools. (safe & secure subset of languages …) Added to that, will be the reqmts of the demand-side specific context.

Resources deployed on security: HW, SW, people?

Configuration of resources to deliver security? Risk reduction/ ROSI?

Supplier delivering a capability .. mix of these three.

TASK: Guidance about how to prioritize security needs, using the R7 radar diagram. 'Stack' of different diagrams for different requirements; average mission. Bridging demand-side need with supply-side specs. What decision did the adjudicator make? Develop rigor / methods for this role.

Trade between development time investment and operational costs? Models that help with devlpt time investment choices, trades? Hence acq by specs rather than performance in DoD.

TASK: Supplier-side: system model to guide me about process / product improvement priorities that will enable me to meet security performance targets.

Identification of lower-level measures for security – i.e. of lower level components/ process elements… and how the roll up into higher level indicators. Ref: JHU study. DoD IA Metrics study (700 metrics etc) Map DoD study to higher level indicators. Will support development of draft PSM guidance materials.

Cost of non-conformance ..

TASK: Set of reasonable measures, indicative of security .. (to whom?) Qualitative arguments, conventional wisdom etc. Purpose: supports trade with downstream operational costs. For decision-makers, in the absence of eng-type measures, a qualitative indicator helps with choice. Some scoring 1 – 5, indicative of 'security rating' of the product/ services. Built from checklists, existence of security actions.
Fitness criteria at milestones. Born secure. Scoring a system at the point of transition to operations.
Ref: Net-centric Operations & Warfare Reference Model. (where are the security functions placed? Must be specified.)
Performance reference models associated with this…
Model is comprehensive, but complex and hard to comprehend….

User changes to a system from the originally delivered system. Execute-only components.

2. Are security actions based on known best practice and in compliance with applicable standards and legal requirements? (from a US industry perspective, this should also address security requirements derived from compliance with Sarbanes-Oxley.)

Among the drivers of the checklists in above indicator concept.
Banking Industry technology security BITS, checklists.
World Bank Technology Risk Check List.
HIPAA Health Insurance Portability Act, further checklist inputs.

3.How is the security risk being managed?
How is safety risk being managed? (and specifically, how does measurably improved security contribute to managing safety risk and privacy risks?)
Venn diagram to differentiate between different risks, and overlaps. Also other risks. In, out, criteria.
Different variants of security risk (privacy, integrity etc). Task for adjudicator.

4. What is the assurance evidence that defines our degree of confidence in likely future security performance? (what of this could be used as indicators for future security performance? How should the PSM "Security Measurement" White Paper v1.0 30-Nov-04 be revised to target specific user needs?)

Where is the reference point? Where's the ground reference point? Standards, criteria.

5. What is the achieved performance of our systems in terms of managing threats, vulnerabilities, responding to events and recovering from & controlling damage? (what level of decomposition is needed to address software assurance, information assurance, cybersecurity, etc.?) R7 model.

Again, ground?

Devolution of a service: emergent

Evolution: emergent of properties/ performances.

Mixed analog/digital.

Consistent with the recommendations for future work (listed in the paper), I will explore the possibility of co-sponsoring with UK MOD (if necessary via task order funded by DoD and/or DHS via PSM):

1. Development of example measurement specifications based on particular security/safety practices/standards, and particular technologies (e.g. software development, CC security functional components, etc.);

Ref: the 16 practices identified in the Safe Sec AAs. Open to development.
Based on standards. But when connected to a user; context-specific issues arise. Voluntary or regulated adaptation?

Need experimentation: enables demonstration of value to users.

Common Criteria: practical use is the difficulty. E.g. protection profiles could be specified to be difficult to meet. But an expressive way to characterize security needs. Who should be responsible for writing this?

2. Development of practical guidance on how to develop security/safety measures in support of management decision-making;

Template example:
PSM – generic situation: decisions to be made, indicators reqd, example data, analytics. Plus guidance for tailoring to the context-specific.

But in security: there is a minimum, common set of decisions, and sets of indicators, data that support this.
Figure of merit for security.

Raise the floor – do not need sophisticated measures ….

Example: how is confidentiality achieved: what mechanisms achieve this?

Sample responses to the relevant questions, with scenarios for how the answers could provide the indicators management needs in making decisions regarding security/safety. Ref: Jack Lenihan report.

3. Pilot/test proposals in conjunction with security/safety specialists and standards organizations (test measurement proposals and improve by means of project trials);

Eventually … standards, curriculum..