PSM Security Measurement Workshop
26, 27 July 2006
Vail CO

Attendees:
Don Reifer
Tom Conrad
Gary Hafen, LM
Scott Rigby, Raytheon
Nadya Bartol
Michele Moss
Cheryl Jones
John Murdoch

Workshop Notes

Additional Security Contacts

NDIA (National Defense Industrial Association) Kristen Baldwin
Publishing DoD-wide SW Assurance policy and guidelines
For OSD

Anti-Tamper Conference
Annual in May Classified
Air Force, Wright Patterson
For OSD (Office of the Secretary of Defense)

NCOIC (Network Centric Operations Industry Consortium)
Command and Control, network security, operations security
Sponsored, led by DISA (Defense Information Systems Agency (US DoD))
Consortium Lead Chris Gunterson

Our objective: to develop security measurement guidance. Many groups are publishing security, assurance guidance, but none focusing on measurement – so gap to be filled.

Michele: Objective: Eliminate the assurance peoples' jobs.

General feeling in security field: too much assurance, not enough accountability.

Don: Must drive abstract to the realistic. Pilot case studies needed.

TC: Behavioral problem in security: don't actually want visibility; wish to pass muster at minimum cost.

When to apply msmt to a pilot project? In DoD – as project enters DITSCAP phase.
DIACAP - DOD Information Assurance Certification and Accreditation Program (supercedes DITSCAP)

Merit in considering programs at different stages. Overall aim – build security in.

Nadya's Presentation

Next Sw Assurance Group meeting 2, 3 Oct

Definition of risk: add ISO/IEC16085

Ref: cross-std definitions matrix, maintained by NSA, Larry Wagner

DR: DoD Stds missing from list:

Policy, instructions 5000 series (weapons side of DoD)
8500 series NII – side

But DHS responsibility:
Public/private partnership
Govt/industry
Critical infrastructure protection
Use of ISO stds where available etc

Also UK NATO stds.

In particular
JC3IEDM (Joint C^3 Information Exchange Data Model)
Relevant for security because
Information assurance issues associated with coalition ops
RT access mngt
Etc

Other communities moving in same direction – exchange data models

IE model implemented in sw. Does it accommodate security msmt data needs? Is it itself secure?
Related implementation issue: re-partitioning of data bases

Security is a quality attribute. Metrics to serve quality checkpoints/ decisions.

False positives issue.

Summary of Meeting of 20th July

DR: Works with three aspects of security:
Software, build security in
Network security
Anti-tamper

NB, MM: add enterprise

A network metric: no. sensors per node
Cost to achieve acceptable false alarm rates

SW Assurance ideas:
Msmt toolbox
Cross-walk specs - terminology across different specs
White space between current stds

Break out on the 20th:
Acquirer Goals, then mapped to PSM ICM Table for comparison

DR: suggestion for structuring work:
Take ISO/IEC 15288 as a ref phased life cycle model.
Cross with each of the areas
SW, network, AT, enterprise
And consider msmt in each cell.

Fundamentals

DR DoD experience; cost and delay associated with certification and re-cert. Onerous process.

Must trade-off security with performance. Sometimes security must take second place to performance.
Value of information inversely related to trusted-ness.

RT performance is a major issue. Performance-sensitive technologies.
Wish to build security in from beginning of dvlpt., not to bolt on at end. Architecture has security msmt implications.

Must be aware of trade space with performance. Security specialty contributes to SE decision making. Also involves other –iliites.

Different applications of security msmt may be distinguished on basis of trade space involved.

CVE (Common Vulnerability Exposures (MITRE))
Vulnerability database Mitre. Many vulns identified, but can be generalized.

BREAK

Discussion

ICM Table reviewed

Look at scope/size

Discussion of product/service distinction

DR: network security issues not covered by table (which started from sw devlpt and proj mngt)
Networks part of development systems and part of delivered product systems
e.g. system devlpt environment/ bench.

Network sizing parameters:
No. nodes
No. proxy servers
IPS devices
No. firewalls
Router type

Size of assets

Network devices
No. nets (one proxy server per net)
No. interfaces with other nets
No. nets in network (sat net, LAN, WAN)

SC: what are units, in table? Generic, HW SW. Purchased items.

DR: for sizing a network, uses
Security Requirements
No. system interfaces with external systems/ networks
Operational scenarios
Nodes
No. unique algorithms

These map to COSYSMO parameters. Overlap between measurement and estimation fields.
DR: consider rolling these together in a proposal ….

No. interfaces, protocols
Security classification for network (TRL)
Acceptable practices to meet the demands of the security level?

How well am I protected?
How well will the system/network perform?
Does it do what I want it to do? Does it not do what I don't want it to do?

What are the false alarm rates?

Definition of 'node' = gateway between networks. Where IDS\ IPS, perimeter defenses, DMZ are placed.
But also, defense in depth, layered defense.

Also concerned with protection against insider threats.

Goodness of protection

Defn of ‘node’ will vary with architecture. Security attributes of a node.

Security architecture/ in depth
Apply to org/ enterprise

Scope of enterprise – depends on application. Equivalent to defining the ‘system of interest’ in SE.

BSI: performance also needs to be considered. Needs to be viewed as a trade space.

Scope of prohibited activities.
Protection Profile (CC) – solution concept. How secure is this item? CC –set of criteria applied to a product. Assurance attributes. (DIACAP)

Discussion about AT, physical security.

AT: no. critical program information items (CPIs)
PPP – Program Protection Plan
= what items you are protecting
What technology used
Design, board, GNC, algorithm, data item etc

Further size/scope issues
No. foreign collaborators
COTS product sources
Global economy problems
Sources, deliverables
Measure people? Country of origin
Product pedigree
Analysis of COTS – security research issue

TC: No. components derived from an offshore source
Degree of trust

Also issues around use/operation of end products/systems by other parties.

Thursday 27th July

Continue review of ICM Table, looking at threat environment.

What is our current security status?
What are our current threats?
Mix of high and low level.

DR: Network view of threats:
Distinguish between Project network and Corporate network

Privacy

Gateways
Communication enterprise-wide and interfaces with external networks.

DoD systems have physical concerns also eg TEMPEST, depending on level of security.

Mix of things in the ICM Table under 'threats'.
Application program calls another program, middle layer .. how do know whether to trust these programs etc.

NB: 27001 contains a reference-able list of threats.

No anti-tamper interpretation under threats.
The negative aspect of AT is that it makes the product more difficult to understand.
Positive aspect – more secure. Mainly for military applications, but also applicable to digital rights management in the commercial sector, for example.

On consideration, AT is perhaps out of balance with the other views – enterprise, network and build security in. Agree to drop AT for current cycle of work; can be treated as specialty field later.

NB: NIST and DoD standards have lists of controls.
Risk-orientated controls
Physical controls
The ICM table can contain pointers to these standards –why repeat?
For example: 27001 – Are you protected from …?
Do you understand the network connection?
CEO question: the reputation, or 'Washington Post' question …

Product Quality
Common Criteria covers this area in the defense sector.
Ref CC from the ICM Table.

Trade space issues must be included, however.
Security is a quality attribute, and should be traded with other –ilities and functional performance.
Risk trade-off issues.

This usually is done in SE by means of key performance parameters e.g. growth, response time etc

Why is security not treated as a key performance parameter, or constraint? Security is a NFR.
Security by component. Global / system security.

Security should be requirements-driven, then developed using best practice or CMMI-like practices.
Is not the trade space contextual to security msmt itself?

TC: Example issue: If a network or system is made secure by doing the same thing at every node, for example, this may itself be vulnerability. Trade within the security domain.

Security people do not understand measurement and are often risk averse/ compliance-orientated. 'Don't rock the boat'.

TC: Is not (product) standardisation itself a security risk?

What body of knowledge addresses the issue of std components representing a vulnerability? Std components simplify the problem for the attacker. How do I measure that I am at risk from a bad security policy?

Example of a trade-off between mngt and security.

Treating security as a product quality, could reference work from the 70's by Walter, McCall, Boehm (NBS report 75 05).

Quality treated as a contribution from many factors. Empirical numbers can be ascribed. Test/verify to provide assurance.

Specify quality that is required. Then design in.
*What do we need to know to determine if we have achieved the quality objectives?

Example of difference between testability (a quality) and security. Leave hooks in a program for testing purposes. But these are then vulnerabilities.

Damage costs
Operations trade space.
Example: NDA '3 min war'. Cannot permit security to tie down the system.

TC: Issues around human in the loop and autonomous systems. Sometimes autonomy is required b a mission.
How secure should the system be? If humans are involved -there is a security risk.
Autonomous systems have implications for testing.

Perhaps the ICM Table need a 'people' category.
Ref: ISSEA set: has measures associated with training needs etc

Msmt problem: goodness of autonomy v people in a system.
Maybe comes down to training. Measures of training.

DR: Everything is net-centric today.
Proposes concept of 'net-ready'
No msmt yet exists for net-readiness.
Metrics proposal for GIG.

SoS functional capability
Net readiness dimensions

SCOPE model
DoDAF model
Example measure.

N&M: Difficulty: whose language to use? DHS different from DoD.

DHS: approach must be generally useful over a broad variety of stds.
Proposal:
Approach 1
Take stds; map DoD lists. Look for overlaps. Foster convergence.

Or Approach 2
Take a 'fundamental questions' approach – simplified ICM, selected measures etc.

Not necessarily either-or.

TC: Vast body of knowledge 'out there'.
PSM approach must be practical. Not universal solution to anything. Practical set of things to address. Intersect with Body of Knowledge.
Practical, doable, affordable approach to msmt.

Standards seek full coverage to perfection.

NB: Problem with keeping things simple by just using current metrics. How does security affect our mission?

Tendency to have checklists – compliance based. Due diligence – protection from legal challenge.

To develop cross mappings between standards is a large task. Would need to be funded.

For PSM, we shouldn't pursue something we couldn't get funding for.

Need a msmt approach that means we don't miss the big issues. We cannot use a process with 1,000 measures.

Always the pressure – have it done by yesterday.

What is the key, top-level list of security questions?
NB: need to go to standards
GH: Current table has too many questions, at different levels.

DR: proposes third approach. Translate ICM directly to a specific application. Develop generic measures etc from that.

Consider the three views:
Enterprise,
Network
Sw/ BSI

Product quality: design security in
Network – one server, good architecture, good sources of components.

MM; Can we 'sort' the ICM Table. Put into Excel. Have an application column. Can then sort on that.

Good high level question – if I new the answer, could I do something?

Quality question appears in all three views.

* Is the product of acceptable quality? How can I tell?

Recommended approach: reference out to standards where applicable, but retain thinking for the white space etc. PSM is about supporting that core 'independent' thinking, with a commitment to strive for objectivity.

What application domain should we consider? DHS would welcome BSI application.

*How do we integrate security into our development processes?

Current problem – security not integrated in to SE – separate communities.

(In ICM Table, re-categorise Training).

SDLC implemented. Tech environment.
MM; Just having someone with appropriate certification does not mean he/she is the right person for the job.

Key process questions (GH)

- What is the process?
- Does it comply?
- What is the performance of the process as implemented?
- What are the outcomes?

*Have security/performance/trade-offs been defined and accepted?
*Have all compliance reqmts been addressed?
*Have all required computer security functions been incorporated and tested in the product?

*Have security reqmts been documented?
*Have the security policies, functions, capabilities been documented?

*If encryption is reqd, is it provided?
*If AT is reqd, is it provided?

Current ICM Table is too much. TC; PSM-P stands for practical.

Some of these questions are binary check box things.

Review questions in PSM book.

*What is the security performance of our system, today? Devlpt security profile, today?

Questions that bridge across the three views.

There will be cost and schedule questions.

*How vulnerable is this system to security lapses?

*What is my security capability?
*How confident am I in the assessed security?
*What are my security needs?

Apply questions to each of the three areas.

*What is the average complexity of HW and SW components in my system, whether FPGAs, SW etc?
*How many HW, SW modules exceed some level X?
Define ‘complexity’ Logical, security etc.

*How well understood, documented and addressed are the risks in the operational environment?
*How many attacks have been attempted, been successful?
*What is the cost / damage resulting from security attacks?

These are perhaps measures. Top level question might be:
*How successful has my security program been, as evidenced in operation?

*How much devlpt re-work and at what cost, is caused by the security process?

*Am I addressing security at an appropriate level?
*Will my system maintain the required trust level?

*Is my system net-ready?
*Are my support networks secure?
*Will security impede my system performance?

*How secure are my sw products?

*Have security access controls been implemented in he system or service architecture?
*What level of security wrt the CC is required and what has been achieved?

*How secure is the development environment?
*To what extent is security adaptable to surge requirements?

*How effective is the enterprise at protecting sensitive data?

*Is customer and employee data protected in compliance with applicable legislation?

*What is the level of awareness of security of executives, PMs, developers, network, system administrators about security-related issues related to their work?

*How effective is security training wrt security requirements?

TC: e-mail experience. People sometimes forward an attachment without looking at it. May contain one classified page in an otherwise unclassified document.

*Is my network agile enough to ensure confidence, integrity, availability to users?

*How certain are we that we will not have successful attacks?
*How confident am I that my security posture is compliant with my risk tolerance?

Planning Discussion, led by Cheryl.

Clean up top level questions	Jm, cj	End sept
Consider Delphi exercise to refine questions		Oct meet?
Develop first draft basic guidance to accompany questions	Jm cj	End sept
Clean up and structure ICM table, simplify	Jm cj	End sept
Map Guidance, measures to various standards.	NB, MM	
Map terminology across standards	NB, MM	
Tailor or provide tailoring g guidance for selected applications. Add column to table.		
Pilot studies		Late 06, early 07 meet
Develop some sample msmt specifications, including description of core data, base measures		
Define core stakeholder communities (cf Build in, networks and enterprise are 'views')		

Consider different lifecycle phases; phases will differ according to questions and stakeholders.
Issue for networks – they are put in place (in the devlpt envt) before work starts.
15288 terms – phase names etc.

GH; LM, Raytheon, Boeing should be ready to offer pilots at the next workshop, or the one after …

CJ: 15288 top level processes;
Project enabling processes
Agreement processes
Project processes
Tech processes

Stakeholder reqmts define the processes.
Perhaps just taking concept, devlpt and operation is sufficient for this work.