Practical Software and Systems Measurement

PSM Users' Group Conference, 14-18 July 2008 Mystic, Connecticut

Security Measurement: Applying PSM Principles

Cheryl Jones, CIV USA AMC

John Murdoch, UK SSEI, University of York
john.murdoch@ssei.org.uk
john.murdoch@cs.york.ac.uk

Motivation

- **Security measurement / metrics is now quite a crowded field**
- **What distinctive and complementary contribution should PSM be making to security measurement? What kind of measurement guidance?**
- **In developing PSM security measurement guidance, how can we apply the fundamental principles of PSM?**

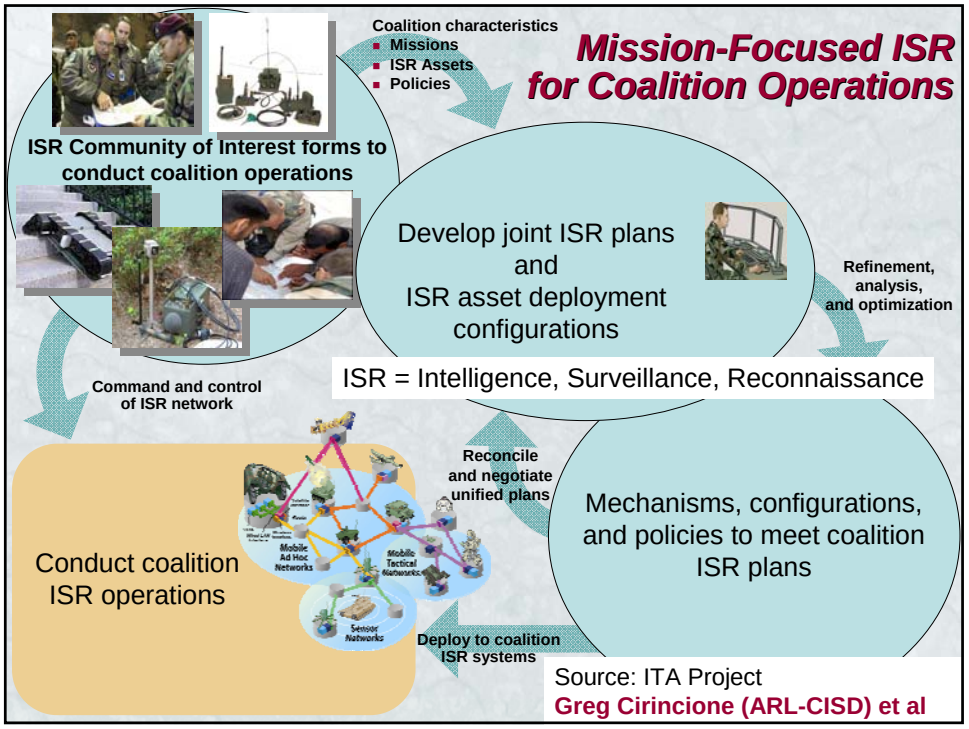
Security Measurement – very brief review

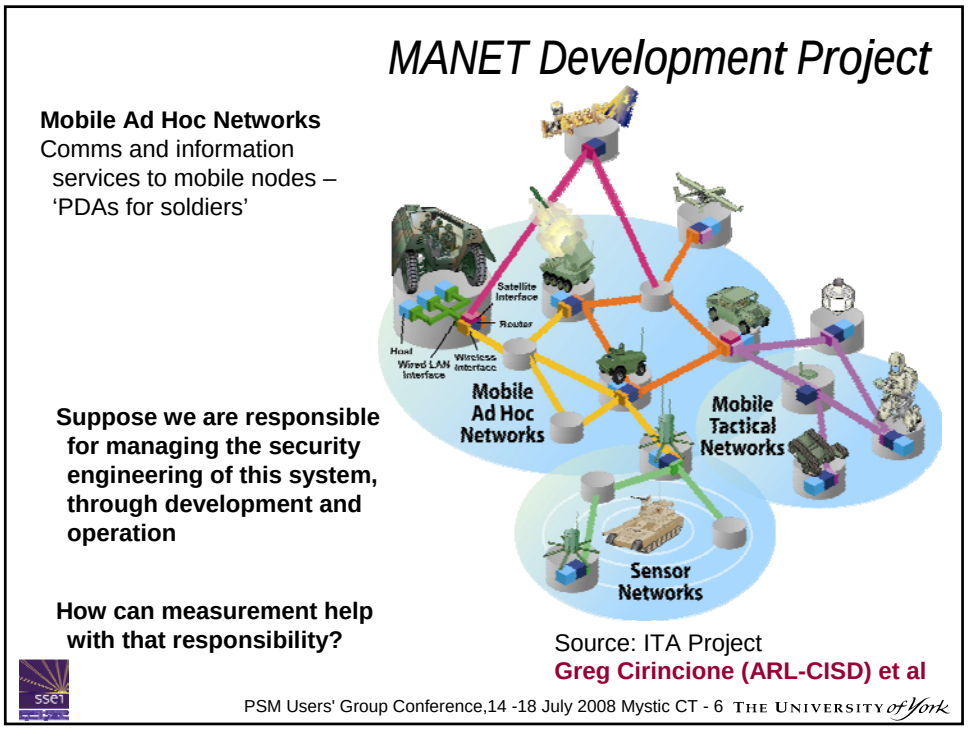
- PSM Workshops
- DHS SW Assurance Forum Workshops
- ISO/IEC 27004
- ISSEA
- Herrmann, Jaquith
- Software security metrics conference series
- Cyber security, CERT
- Build Security In

- Very large number of potential measures
  - Serving different information needs
  - Applying to different threats
  - Applying to different technologies

Agenda

1. Example Application: Security in MANETs
2. Observations about Security Measurement
3. PSM ISO/IEC 15939 Measurement Fundamentals
4. A Strategy for PSM Security Measurement Guidance: Generic Security Measurement
5. Tailoring to Specific Applications and Technologies
6. Conclusion


Mission-Focused ISR for Coalition Operations
Coalition characteristics
Missions
ISR Assets
Policies
ISR Community of Interest forms to conduct coalition operations
Develop joint ISR plans and ISR asset deployment configurations
Refinement, analysis, and optimization
ISR = Intelligence, Surveillance, Reconnaissance
Command and control of ISR network
Reconcile and negotiate unified plans
Conduct coalition ISR operations
Mechanisms, configurations, and policies to meet coalition ISR plans
Deploy to coalition ISR systems
Source: ITA Project
Greg Cirincione (ARL-CISD) et al


MANET Development Project
Mobile Ad Hoc Networks
Comms and information services to mobile nodes – 'PDAs for soldiers'
Suppose we are responsible for managing the security engineering of this system, through development and operation
How can measurement help with that responsibility?
Satellite Interface
Router
Wireless Interface
Wired LAN Interface
Mobile Ad Hoc Networks
Mobile Tactical Networks
Sensor Networks
Source: ITA Project
Greg Cirincione (ARL-CISD) et al
PSM Users' Group Conference,14 -18 July 2008 Mystic CT - 6 THE UNIVERSITY of York

MANET Security Challenges 1

- Wireless system: need to protect against eavesdropping, implying encryption and key management services are needed
- Authentication of users: *ad hoc* network, so we need protocols to enable flexible acceptance of new nodes
- No pre-existing comms or infrastructure: all security and other functions are carried by the user nodes: resource constraints
- Many different types of threat – combining information and physical aspects e.g. node eqpt acquired by adversary
- Many different types of countermeasure

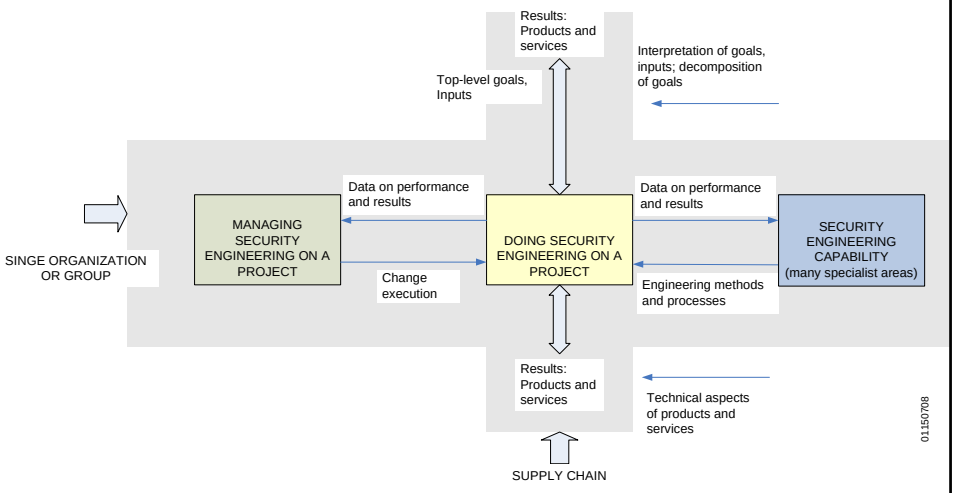
MANET Security Challenges 2

- Coalition operations: different security domains involved
- Info - security risk exists in a context of tactical and strategic risk
- Variable threat environment: adversaries are flexible and innovative; variable damage environment; time value of information
- Defense info system – so likely to be a MLS: have to control access to different levels of classified information under different conditions, for different users
- Nodes are resource-constrained; users are attention-constrained

Observations about Security

- ‘Security’ has many meanings, defined by the operational context and system: different operations, missions, threats: different technologies and countermeasures
- There is change and uncertainty - threat environment
- There are trade-offs:
  - Op risks, infosec risks: different risks to different parties
  - Resource limitations – opportunity costs of countermeasures
  - Between different mitigation types and distributions
  - Damages sustained
- There is a need for adaptive protection but under policy constraints
- Automation envisaged to simplify security operations, but how to decide on the built-in risk management function?

Security Engineering Management



Potential Uses of Measurement

- **ACTIVITY - Compliance with policy (or other commitment) and testing of policy assumptions (or other commitments)**
- **PRODUCT - Assessing achieved properties, of committed-to solutions and validity of those commitments**
- **RISK MANAGEMENT– prioritization of threats and damages to enable risk acceptance decision making, prioritization**
- **COORDINATION between countermeasures: therefore between parties: monitoring threat mitigation assumptions being made by different suppliers in the supply chain**
- **ENVIRONMENT Assessing adversaries, monitoring threat environment**
- **OUTCOMES - damages – also dynamic (e.g. information aggregation)**
- **COSTS of security, opportunity costs, trades with performance; when do we have enough security, enough assurance?**
- **AUTOMATION - built-in trust or risk management functions**

PSM Fundamentals

- **Focussed on acquisition and ENGINEERING MANAGEMENT, especially during system development on a PROJECT**
- **Measurement is driven by INFORMATION NEEDS of identified decision makers: establishes value of information and measures**
- **Measurement PROCESS**
- **Links indicators with base measures via explicit MEASUREMENT INFORMATION MODELS**
- **Identifies GENERIC PROPERTIES (size, quality, costs etc) to support specialization and tailoring**
- **ANALYTIC MODELS for modelling causality, prediction and decision support**

Strategy for Security Measurement Guidance

Develop a simple-as-possible generic approach to serve decision makers in security engineering management roles

- **Basic information needs**
- **Simple model of security**
- **ICM table – type list of a few measurement types**
- **Method of application and tailoring**

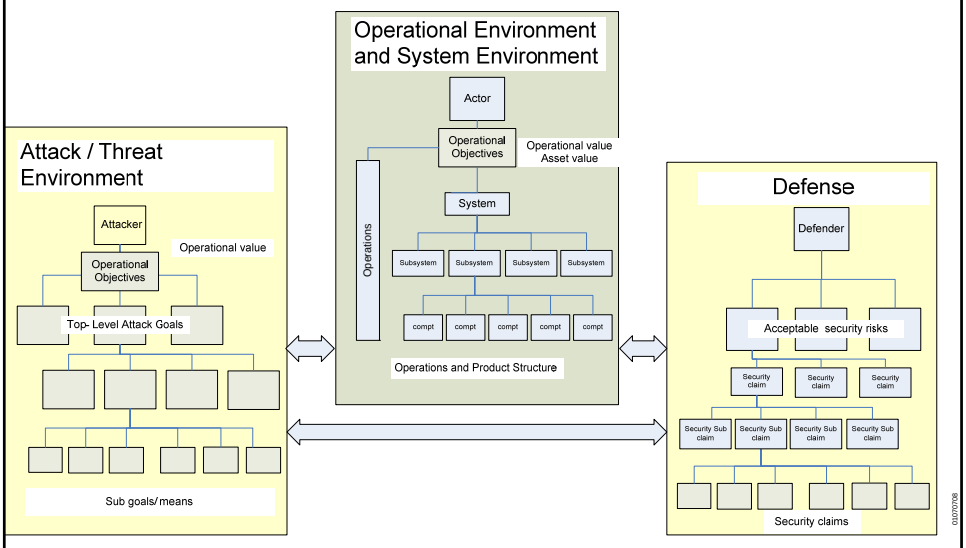
Generic Security Measurement

- **What is common across security engineering management?**
- **A shared meaning for the security of a product system:**
  - **'security of a system or service is the degree of resistance to attack' Therefore, security is a property of a system in relation to a threat environment.**
- **Security measures will be of:**
  1. **Security properties of the end-product or service delivered to the acquirer**
  2. **Activities involved in the performance of security engineering on the project**
  3. **Properties of intermediate work products associated with (2) that support prediction and control of (1).**

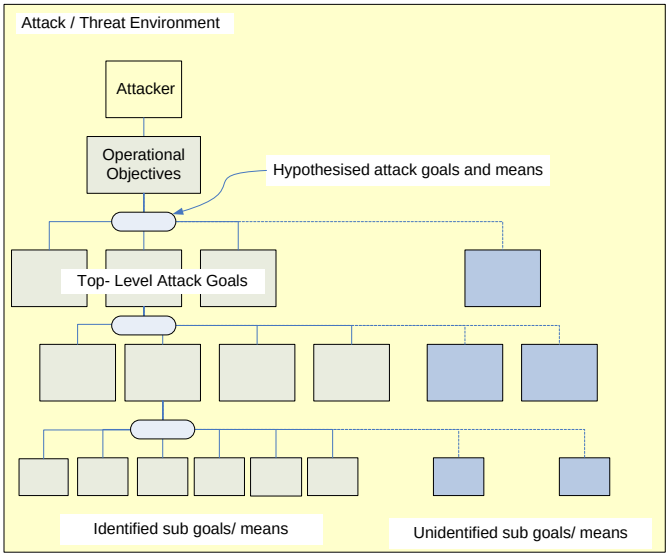
Questions about a Particular Countermeasure

- **How effective is *this* countermeasure expected to be?**
- **Have we tested / demonstrated / obtained evidence that it performs as specified?**
- **Have we monitored / explored the assumptions about the threats that are being countered?**
- **Are secondary generated risks monitored?**
- **What are the costs of this countermeasure? Direct and opportunity costs?**
- **What is the cost/benefit trade-off of this countermeasure? How confident are we of the assumptions and assessments that underlie the answer to this question?**
- **What is the progress in implementation of the countermeasure?**
- **What is the operational performance of the countermeasure? What attacks have been countered? What are the potential damage events?**

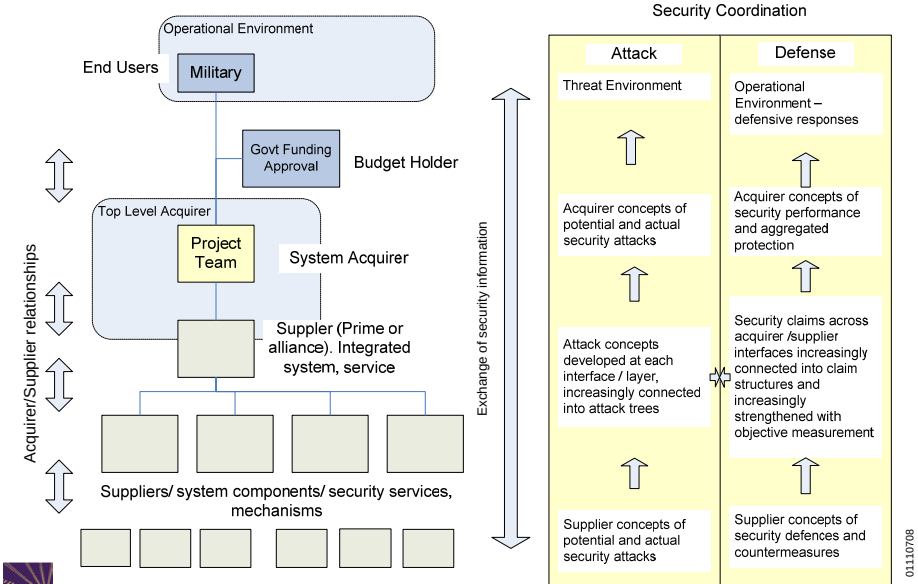
Attack, Defense and Operations



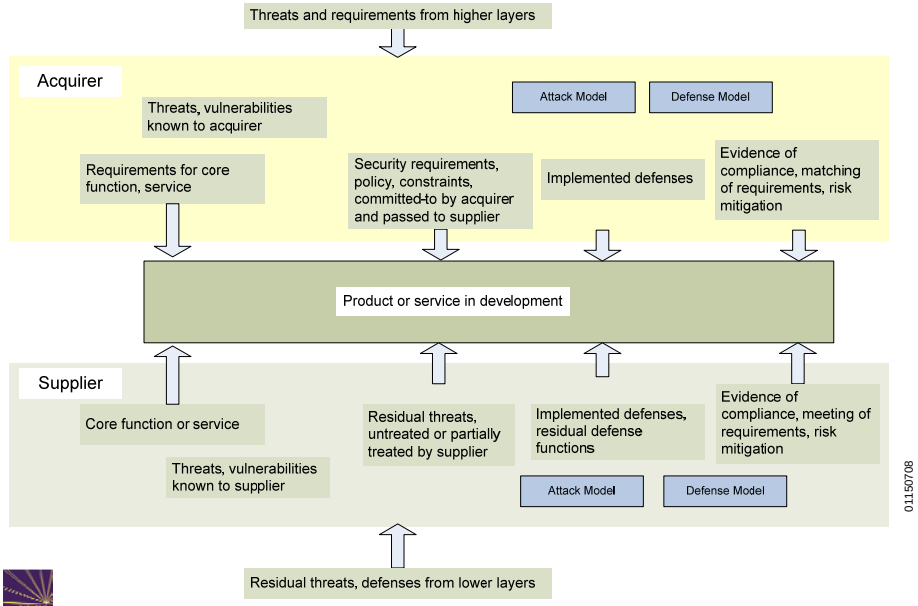
Identified and Unidentified Attacks



Integrated Security



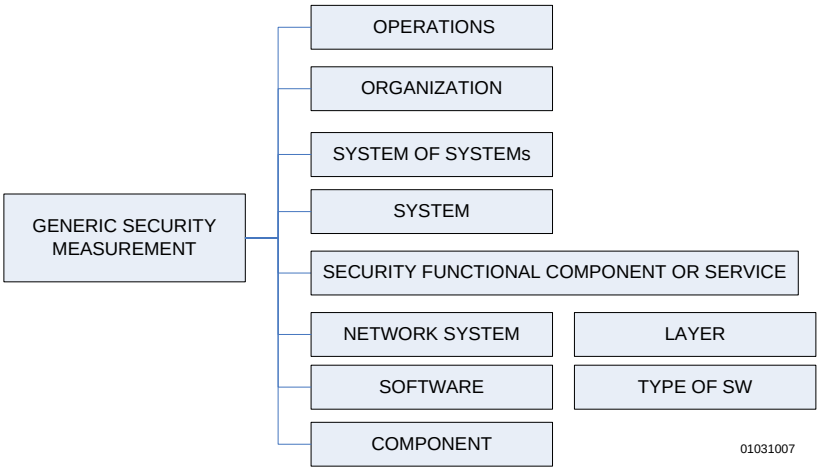
Security Across an Acquirer - Supplier Interface



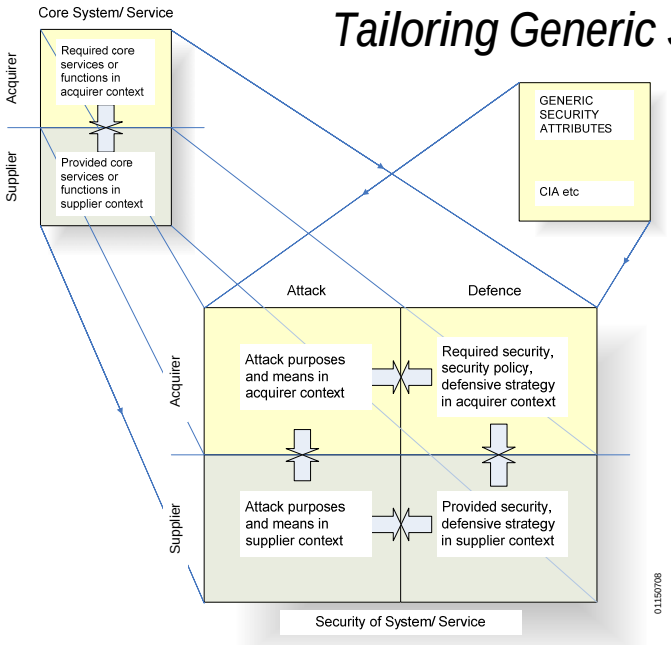
Tailoring to Specific Situations

- **Generic security – not tailored to any domain or technology**
- **Tailored to types of system or technology, or types of operational concept**
- **Tailored to particular projects, ops, systems**

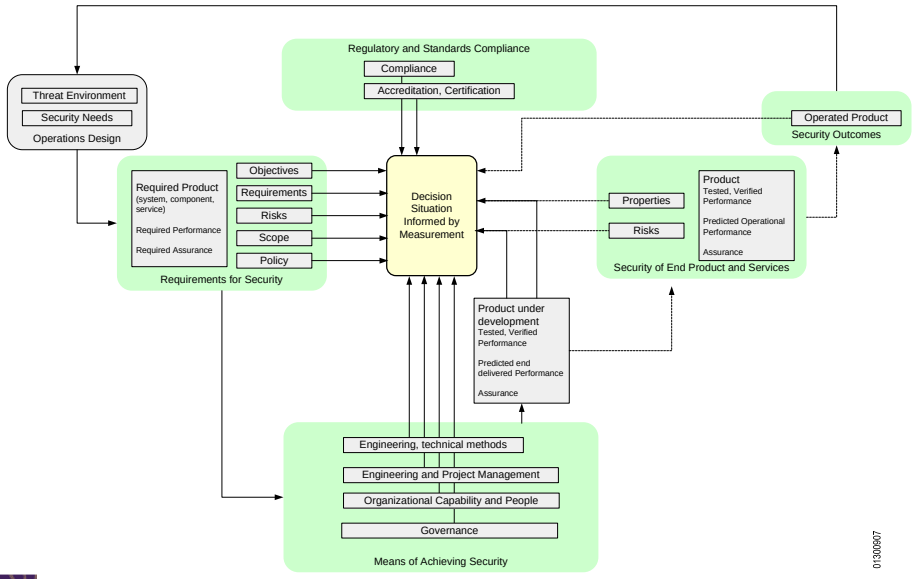
Application Areas



Tailoring Generic Security



Summary: Decision Situation



Decomposition dependent on system and technologies involved
Ref: V-Process Model

Application to MANETs

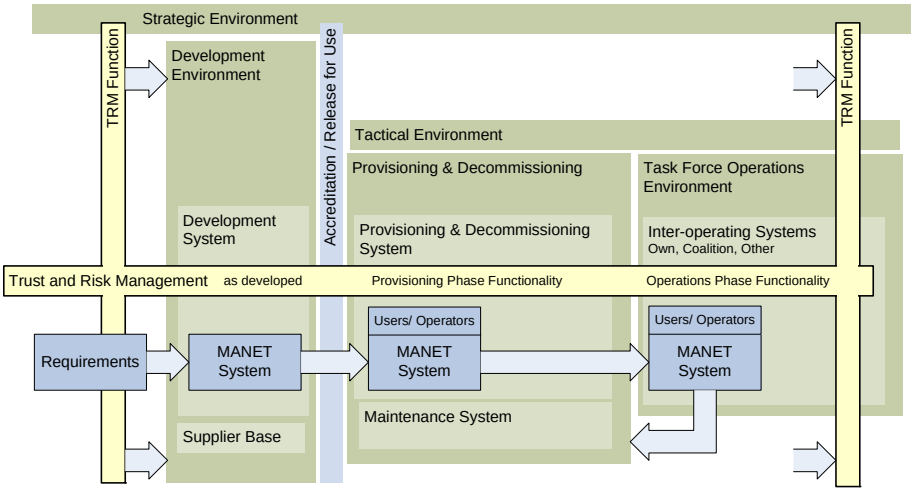
- Operational setting is very important to establish security requirements
- Monitor validity of assumptions - measure outside the system
- Technical development at each layer has to be coordinated: models and assumptions
- Integrate and mature threat and defense models synched with system development
- Balanced design – risk mitigation allocated across the system
- Info security and user/ operational trade-offs
- Measurement in different lifecycle phases

- Commitment management: when to commit, V&V monitoring; what to leave to operations and embedded functions

Conclusion

- Topic: development of security measurement guidance based on PSM principles, generic and tailorable to different decision situations / operational settings / systems
- Support security engineering management of new systems, threats
- Issues mentioned:
  - Proof of presence of properties
  - Demonstration of falsity – failure to refute
  - Coordination through supply chains
  - Integrated security - attack trees and claim structures
  - Careful about compliance and commitment to 'received' models
  - Maintain awareness to avoid blindness introduced by models – Msmt Info Models help with this.
- PSM principles continue to give value in this challenging area

MANET Life Cycle Phases



02140207