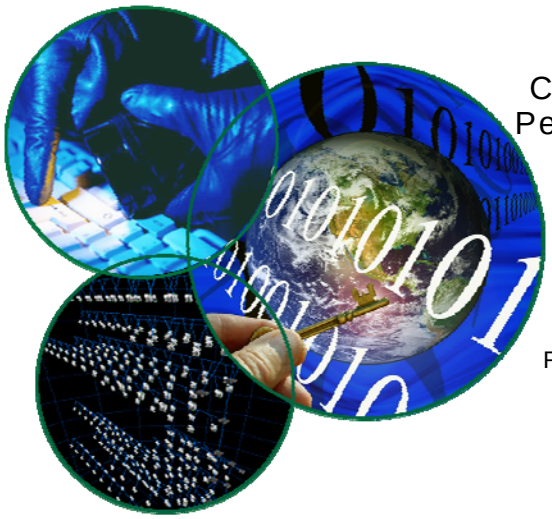
Oak Ridge National Laboratory:
Delivering 21st Century Science and Technology



Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission

Frederick T. Sheldon, Ph.D.

Robert K. Abercrombie, Ph.D.

Ali Mili, Ph.D.

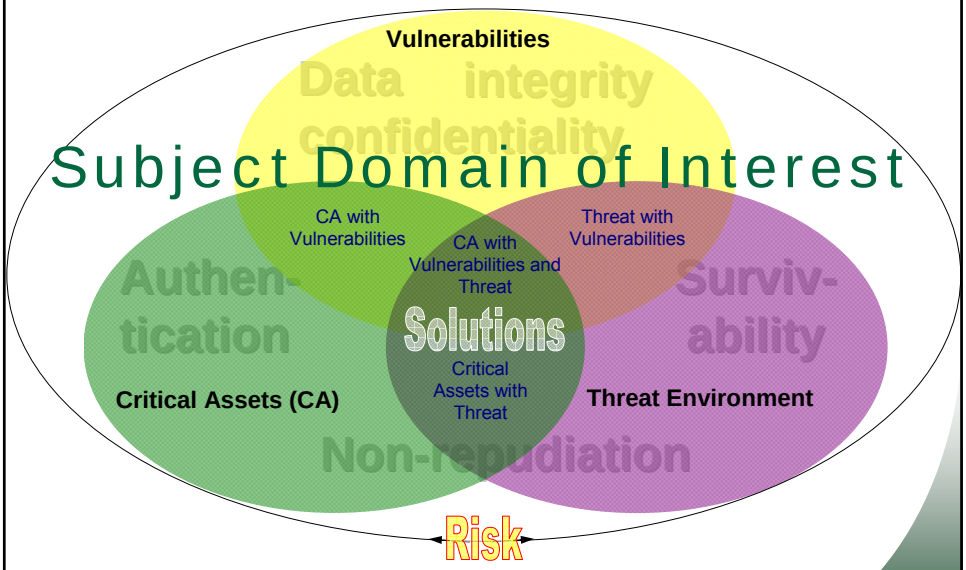
May 14, 2008

Managed by UT-Battelle
for the Department of Energy

The submitted manuscript has been authored by a contractor of the U.S. Government under contract DE-AC05-00OR22725. Accordingly, the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes.

Today's Agenda

- **SDI: Cyberspace Dominant Infrastructures**
- **The Security Gap: A Looming Crisis**
- **Current Security Management Methods**
- **Cyber Security Econometrics**



The Security Gap: A Looming Crisis

- **Increased threat**
  - as a consequence of:
    - emerging global tensions and
    - increased sophistication of the perpetrators
- **Increased criticality**
  - because the emergence of the Internet has shifted more economic and social activity online, making security virtually synonymous with cyber security
- **Increased vulnerability**
  - because emerging computing paradigms such as
    - networking,
    - distributed computing, and
    - mobile/pervasive computing

    open wide security gaps that are hard to control

Current Security Management Methods

- **Defensive:**
  - Traditional security measures are primarily defensive geared to:
    - predefined, pre-categorized,
    - vulnerabilities and threats, and

    are unable to deal effectively with unknown threats.
- **Qualitative:**
  - Security measures are taken because they are perceived to help with predefined threats;
    - there is no quantification of
      - how well they deal with the specific threat they are intended to mitigate,
      - nor with any other variations on this threat.
- **Ad-Hoc:**
  - When security requirements are perceived to be high due to:
    - high criticality, vulnerability, or threat level
    - **several measures are taken in concert; there is usually** no acknowledgement of whether these measures are**:**
      - are redundant, complementary, overlap or
      - together they ensure that some security goal is met, etc.

What is needed for *disciplined security management*

- **A logic**
  - for specifying security requirements and verifying secure systems against such requirements.
- **A model**
  - for managing system security by quantifying
    - costs,
    - risks,
    - measures/ countermeasures,
    - and for estimating ROI.
- **Automated tools**
  - that support security management according to the proposed models.

Vulnerabilities have widely varying impact

- **High impact vulnerabilities are more attractive targets**
  - Security should not be:
    - defined as the absence of vulnerabilities, no more than reliability is defined by the absence of faults (i.e., low impact vulnerabilities do not affect security in a meaningful way).
    - measured or quantified by the number of vulnerabilities, just as it is widely agreed (as highlighted by Adams' and Mills' work) that faults per KLOC is an inappropriate measure of reliability.
  - Security cannot be improved by simply focusing on vulnerabilities,
    - no easy way to tell whether a given vulnerability has low (1) or high (50) impact on security.

Rather, security should be managed by pursuing a policy that leads us to the highest impact vulnerabilities first (a similar approach to usage pattern testing).

Toward Mobile Security Certification

- **Confidentiality** protects against unauthorized disclosure of information.
  - One of the most serious threats to confidentiality is ***infiltration***.
    - e.g., an insider could compromise an end node and plant hostile code.
- **Integrity** protects against unauthorized modification or destruction of information. The integrity of data relies in large part on the quality of the routing network.
  - Mobile code routing networks are not guaranteed to function. The network
    - can be in constant flux,
    - could easily be faulty,
    - garble or drop messages.
- **Availability** protects against disruption of access to or use of an information system.
  - But mobile nodes cannot guarantee availability.
  - Mobile node communications are limited
    - by the physical capabilities of their communications devices and therefore can be dropped from the network occasionally.

Toward Mobile Security Certification
Continued

- **Authentication** is the process of establishing confidence (trust) in electronically presented identities.
  - If an adversary can *hijack mobile nodes*, confidence in identity becomes meaningless.
  - A formerly trustworthy node does not lose any information, knowledge, or capability after falling into adversarial hands yet a hijacked node can also provide any representation or reassurance that the trustworthy node could have provided (spoofing).
- **Reliability** measures a systems ability to maintain stated performance objectives under stated environmental conditions for a stated period of time.
  - Mobile code runs on small platforms with inferior batteries, small memories, limited computing power, and faulty software, which presents the essential dilemma for deploying reliable mobile code/platforms.

Validating Cyber Security Requirements

- **Develop a security target**
- **Develop specific approaches to help achieve the security targets**
- **Validation testing**

Develop a security target

- **A set of security requirements and specifications used as the basis for evaluation of an information system and associated resources**.
  - Typical security analyses postulate codes that run on untrusted platforms, platforms that run untrusted code, or both. These assumptions, however, do not completely describe many mobile code implementations. In many real-world applications, a limited number of mobile platforms are deployed pre-loaded with a small number of known software packages.
  - Additional software packages could potentially be loaded if needed, but many mobile platforms will never load any additional software.
- **Platforms are of known provenance, and are in the physical custody and control of their owners until they are deployed.**
  - Fielded sensors, mobile units given to first responders and mobile battlefield units all fit this description. Accordingly, the security requirements and analysis are substantively different from the analysis in most of the literature.

Develop specific approaches to help achieve the security targets

- **Trust gradients**
- **Clone detection**
- **Route tracing**

Validation Testing

- Understand how new countermeasure technologies strengthen the overall integrity of critical assets
  - Process of refining facility requirements/policies into sub-blocks and assigning each one/more verification mechanisms
  - Compose queries about expected system performance, best investments, performance (or lack of) guarantees
- Assess complimentarity and exposure of counter measures and critical assets
- Determine what
  - Security requirements are reinforced
  - Defensive measures are most effective

Determination of Three Matrices

- **Stakes Matrix**
- **Dependency Matrix**
- **Impact (Threat) Matrix**

Stakes Matrix: Stakeholder vs. Requirements

		Security Requirements				
		R1	R2	R3	…	Rn
Stakeholders	S1					
	S2					
	S3					
	…				FC_i^j	
	Sm					

The Stakes Matrix showing how Failure Cost (FC) is derived.

The estimation of mean failure cost depends on the following premises:

- The same stakeholder may have different stakes in different security requirements.
- The same security requirement may carry different stakes for different stakeholders.

The best way to represent this situation is through a 2 dimensional matrix, where the rows represent stakeholders, the columns represent security requirements, and the entries represent stakes, as shown below in the Table.

The FC entry at row i, column j, represents the cost that stakeholder Si would lose if the system failed to meet the security requirement Rj (i.e., also represented as FC(Si,Rj)).

•Stakeholder	•Requirements	
	•Requirement 1: Safety record	•Requirement 2: Timeliness
•Passengers	•Arrive safely	•Inconvenience, missed opportunities
•Airline company	•Reputation with passengers Value 1	•Reputation with passengers Value 2
•Aircraft Manufacturer	•Reputation with passengers Value 3	•Reputation with passengers Value 4
•Insurance related to Aircraft	•Premium owed for loss of aircraft	•Zero
•Insurance related to Passenger	•Value of life insurance	•Zero

Dependency Matrix: Requirements and Components

		Components				
		C1	C2	C3	…	Ck
Requirements	R1					
	R2					
	R3					
	…				$\pi(R_i \mid E_j)$	
	Rn					

- An analysis of the system architecture, by architecture subject matter experts, can lead to the derivation of conditional probabilities that link the probability of component failures with the probabilities of failing to meet specific requirements.
- This information can be represented in a 2 dimensional matrix, which we call the **Dependency matrix**.
- The term π(Ej) represents the probability of event Ej
- The term π(R|Ej) represents the probability of failing to satisfy requirement Ri, given hypothesis Ej (i.e., that event j has occurred).
- In the table there exists an component event Ej for a requirement Ri where the probability of failure to satisfy requirement R exists (π (Ri|Ej)):

Requirements	Components					
Safety (with respect to Passenger)	Stalling speed	Ensuring never to reverse thrust in mid-air	Ensuring landing gears are out before landing			
Timeliness (with respect to Passenger)				Departure on Schedule	Arrival on Schedule	Ability to Make Connections

The *Dependency* Matrix showing the relationship between Requirements and their respective components and failure results with Respect to Passenger.

Impact Matrix (Component Failure vs Threat Relationship)

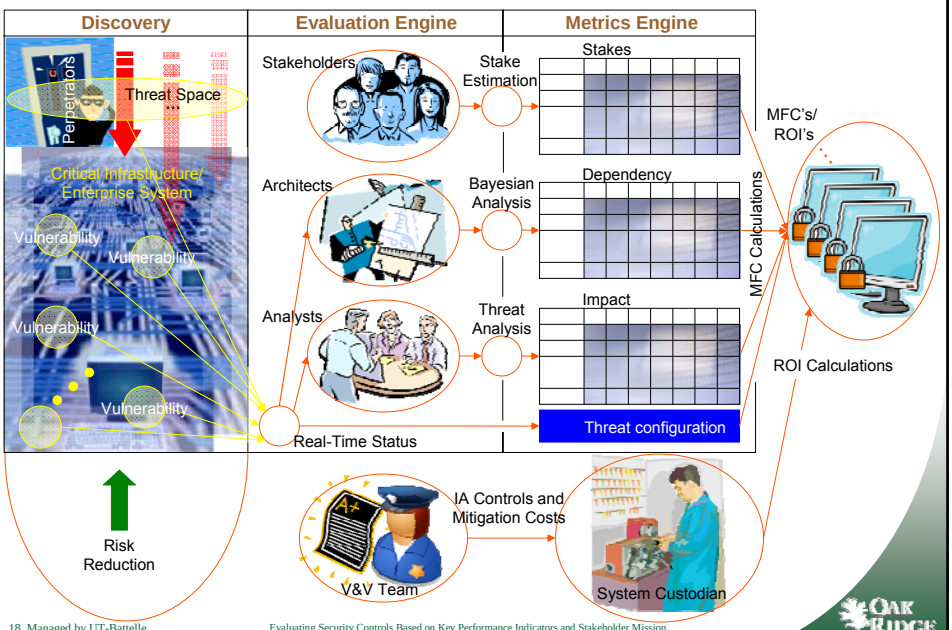
		Threats				
		T1	T2	T3	…	Th
Components	C1					
	C2					
	C3					
	…				$\pi(E_i \mid V_j)$	
	Ck					

The *Impact* Matrix showing Component Failure versus Threats Relationship Grouping

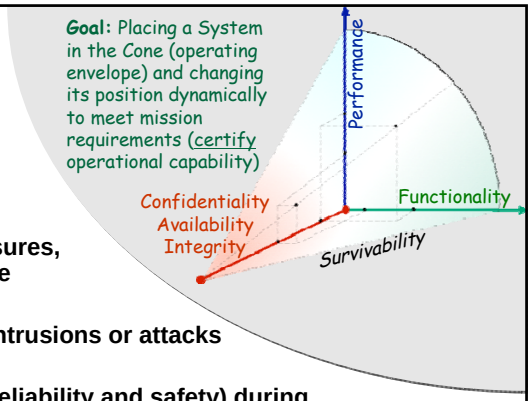
- To assess the likelihood that a particular threat leads to the failure of a component, we consider a set of cataloged threats (or families of threats with common attributes), say T1, T2, T3, … Th, and we consider the events V1, V2, V3, … Vh, Vh+1, where Vi, for $1 \le i \le h$, stands for: Threat i has materialized, and Vh+1 stands for: No threat i has materialized.
- The probability of threat Tj (which is π(Vj)) to the probability of component failure for component Ci (which is π(Ei)). To apply this formula, we need to derive the conditional probabilities, which we propose to represent in a 2 dimensional matrix, that we call the ***Impact* matrix**.

Components	Threats – Elemental Categories				
	Technical Controls	**Pattern Catalog**	**V&V**		
Stalling speed	Mechanical Failure – Maintenance Schedule	Security protection against tampering	Testing	Inspection	Static Analysis
Ensuring never to reverse thrust in mid-air	Mechanical Failure – Maintenance Schedule	Security protection against tampering	Testing	Inspection	Static Analysis
Ensuring landing gears are out before landing	Mechanical Failure – Maintenance Schedule	Security protection against tampering	Testing	Inspection	Static Analysis
Departure on Schedule	Ensure Scheduling Slack		Public awareness	FFA Oversight	
Arrival on Schedule	Ensure Scheduling Slack		Public awareness	FFA Oversight	
Ability to Make Connection	Ensure Scheduling Slack		Public awareness	FFA Oversight	

Cyber Security Econometrics (CSE)



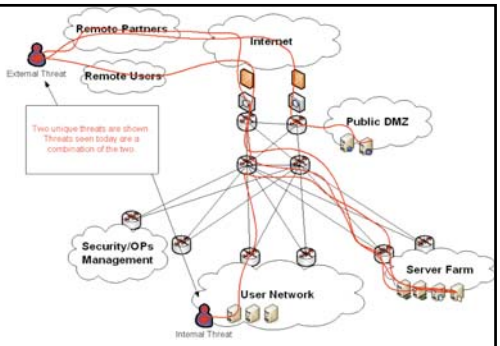
CSE Application



- **Provide a framework for measuring the appropriate attributes that support the decisions necessary to**
  - **Design security countermeasures, to choose between alternative security architectures,**
  - **Respond to events such as intrusions or attacks and,**
  - **Improve security (including reliability and safety) during both design and operational phases.**

- **Provides a comprehensive basis for choosing courses of action that have the highest risk reduction return on investment, i.e., reduce the most risks for the lowest cost.**

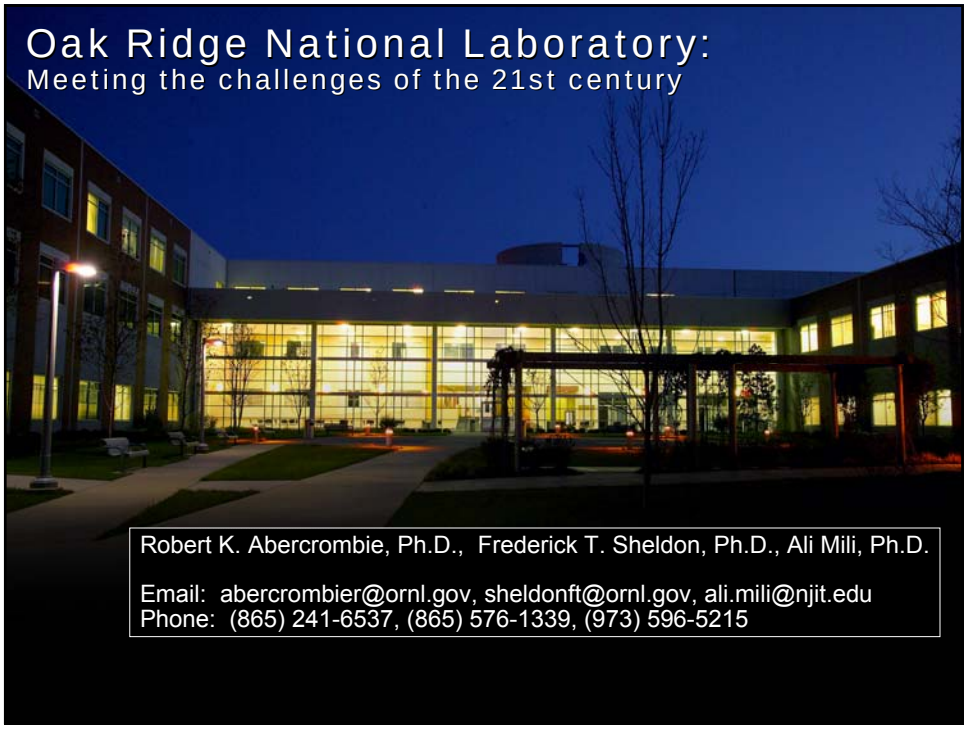
CSE Rationale



- **Consistent with the spirit of *Value Based Software Engineering* and comprehends the different organizational mission needs for all stakeholders.**
  - **For example, CSE identifies information assurance controls and mitigation costs as an investment toward assuring mission success, including**
    - **Essential activities such as real-time threat analysis and**
    - ***Fed by knowledge discovery tools and capabilities within the threat and vulnerability space.***

- **Framework enables us to rapidly develop new metrics that offer a bottom line understanding of the costs and benefits of alternative approaches to securing cyberspace assets.**

Oak Ridge National Laboratory:
Meeting the challenges of the 21st century



Robert K. Abercrombie, Ph.D., Frederick T. Sheldon, Ph.D., Ali Mili, Ph.D.

Email: abercrombier@ornl.gov, sheldonft@ornl.gov, ali.mili@njit.edu
Phone: (865) 241-6537, (865) 576-1339, (973) 596-5215