



**Presentation and Demonstration
to participants of the
Cyber Security and Information Infrastructure Research Workshop
14-15 May 07**

- * Dr. Martin Carmichael
Chief Information Officer, The Rader Network

- * Mike Rader
President / CEO, The Rader Network

- * Katie Carmichael
Principal Engineer, Technology Risk Manager



Philosophy



- * Quantitative metrics are desirable, and should be attempted in all verification, validation, and accreditation activities
- * Quantitative metrics in information assurance eliminate ambiguity in computational-experimental comparisons
- * Prior to TRM, obtaining quantitative metrics in information assurance and defining their associated success criteria was not possible



The Challenge (Narrative View)



Non-Parametric

Parametric

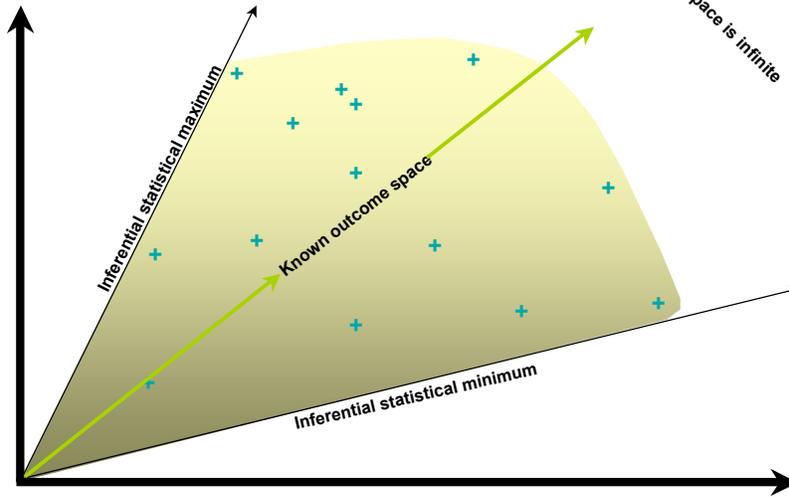
- * National Infrastructure Protection Plan (NIPP)
- * National Institute of Standards & Technology (NIST)
- * National Security Agency (NSA)
- * Security Technical Implementation Guides (STIGs)
- * Department of Defense (DoD):
 - ** DOD Information Assurance Certification and Accreditation Program (DIACAP)
 - ** DoD Information Technology Security Certification and Accreditation Process (DITSCAP)
- * Defense Information Systems Agency (DISA)
- * Defense Information Technology Contracting Office (DITCO)
- * Defense Modeling and Simulation Office (DMSO)
- * U.S. Air Force (USAF)
- * Health Insurance Portability and Accountability Act of 1996
- * Public Key Infrastructure

**Prior to TRM,
not possible in
information assurance**



The Challenge (Scientific View)

Possible outcome space is infinite

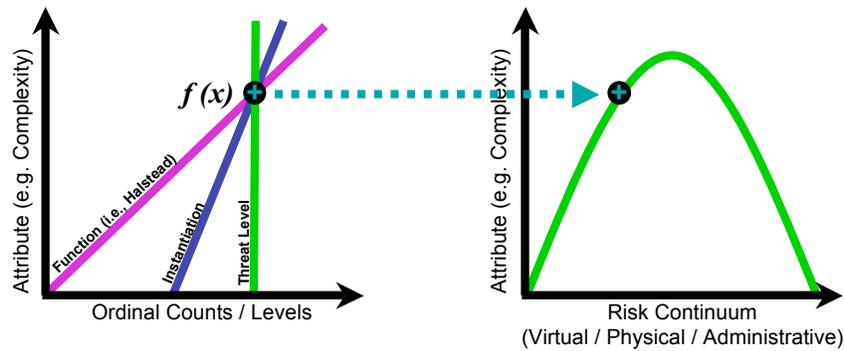


The Rader Network®

RaderM, 14-15 May 2007, Slide 5



The Challenge (Mathematical View)

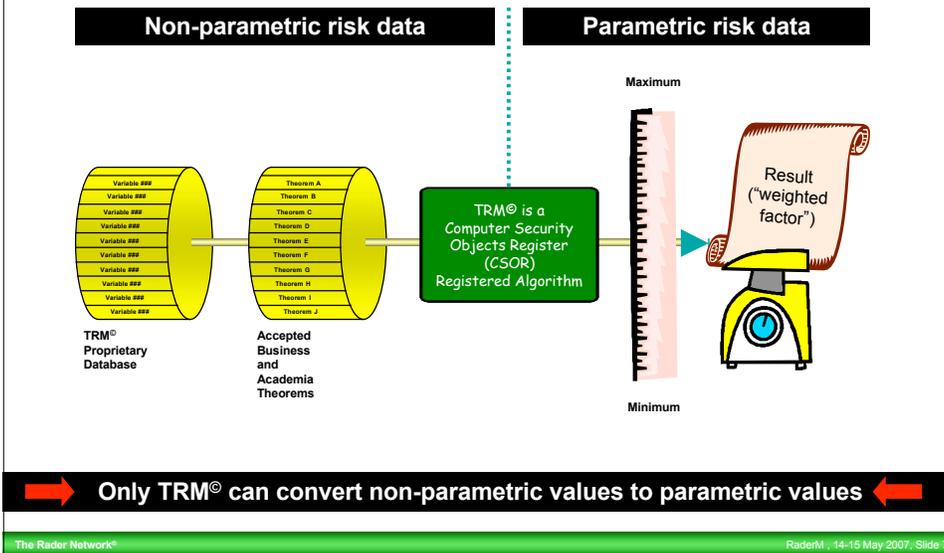


Example of only 1 of 22 interactive formula

The Rader Network®

RaderM, 14-15 May 2007, Slide 6

The Challenge (TRM View)



TRM – Calculating Metrics



- * Each process on the network is evaluated for its security characteristics
- * Adjacencies are measured and the results are aggregated to determine each host's security characteristics
- * Adjacencies are measured a second time and the host calculations are aggregated to calculate the Risk Indices



Definitions



* Not all numbers qualify as metrics. True metrics are numerical facts based on statistical analyses:

- ** **Objective:** the number is based strictly on mathematical risk characteristics
- ** **Quantitative:** the number represents the only true statistical knowledge
- ** **Repeatable:** mathematical or scientific facts must always be repeatable
- ** **Defensible:** statistical analysis is a long-established and highly respected science



Definitions (continued)



* **TRM Metrics** are predictive:

- ** TRM metrics predict the likelihood of a **future** security failure along each of the Four Dimensions of Risk
- ** Other “metrics” consist of counts -- patches to upload, vulnerabilities noted, past security compromises, etc



Definitions (continued)



* The Four Dimensions of Risk

- ** **Confidentiality**: measures how well an organization can authenticate and authorize its users
- ** **Integrity**: shows how reliable the systems of an organization are in keeping information accurate
- ** **Availability**: measures how likely an authorized individual is to be able to access appropriate information
- ** **Audit**: shows how effectively an organization can determine which individuals accessed what data while on their systems



Definitions (continued)



- * **TRM Risk Indices** describe the likelihood of failure (as a percentage) along the specified dimension given three months and a hacker of average abilities

High Numbers are Bad

Risk Profile	
	Risk Index
Confidentiality	94.393
Integrity	60.980
Availability	64.681
Audit	96.381

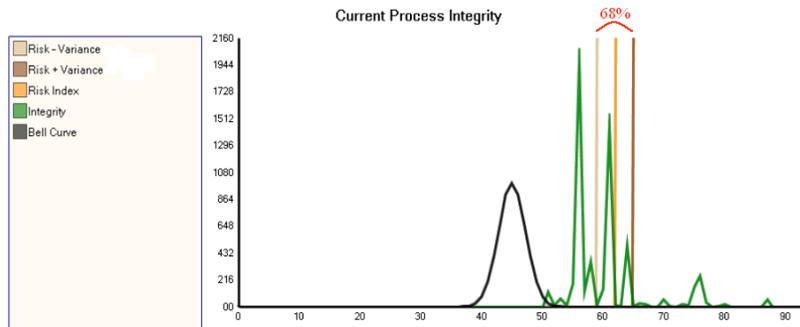


* **TRM Return on Investment** – TRM’s metrics enable straightforward ROI calculations

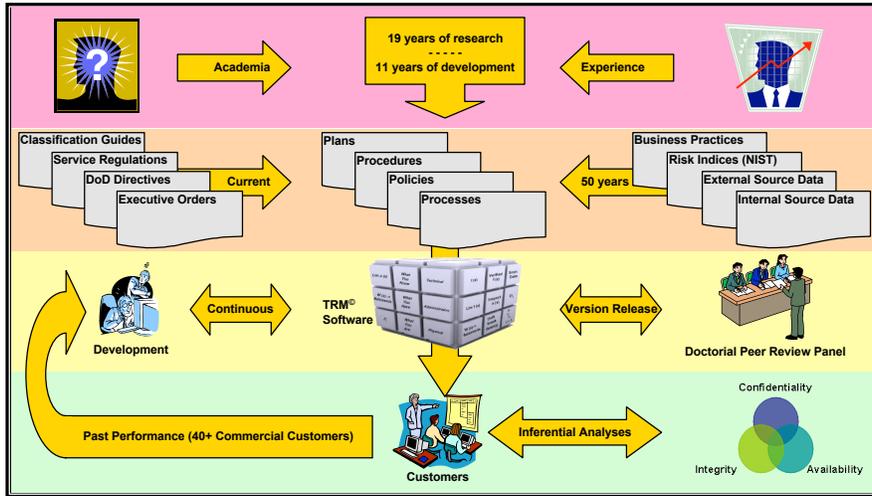
Risk Profile	
	Risk Index
Current Confidentiality	94.393
Simulated Confidentiality	66.251
Current Integrity	60.980
Simulated Integrity	45.307
Current Availability	64.681
Simulated Availability	68.255
Current Audit	96.381
Simulated Audit	58.328



* **TRM’s Consistency and Variance** -- reducing the Risk Index is not the whole story. There needs to be consistency across the network.



TRM – Maturity



The Radar Network®

RaderM : 14-15 May 2007, Slide 15

TRM – Product Comparisons



Parameters	Harris (STAT)	eEye (Retina)	IBM (ISS)	TRM
Metrics and Risk Analysis	X	X	X	▲
C I A A	X	X	X	▲
Quantitative, Objective, & Repeatable	X	X	X	▲
Engineering Principles Based	X	X	X	▲
Adjacencies	X	X	X	▲
Baselines	X	X	X	▲
Modeling and Simulations	X	X	X	▲
Trend Analysis	X	X	X	▲
Administrative Rights Required	Yes	Yes	Yes	No

The Radar Network®

RaderM : 14-15 May 2007, Slide 16



TRM – The Next Level of Security



* ***“If you can’t measure it, you can’t manage it”***

Peter Drucker

* TRM enables you to both measure and manage information assurance with unprecedented accuracy



Principal Contacts



Mike Rader	MichaelRader@ RaderNetwork.com	(719) 930-1183
Katie Carmichael	KatieCarmichael@ RaderNetwork.com	(214) 794-9615
Martin Carmichael	MartinCarmichael@ RaderNetwork.com	(214) 794-9510



Questions and Answers (Product Demonstration)



 Technology
Risk
Manager

Thank you