



## Mission-Oriented Risk and Design Analysis (MORDA)

Don Buckshaw  
Sr. Decision Analyst, Innovative Decisions, Inc.  
dbuckshaw@innovativedecisions.com  
443.472.3061

7 March 2007 (MORS IA Special Session, Laurel, MD)

## What is MORDA?

---

- A “risk” and “design” method developed by NSA & IDI for designing functional and secure networks
- Based on Multiple Objective Decision Analysis (MODA)
- Supports systems engineering, cost, performance and security analysis
- Integrates the work of cross-discipline teams
- Accounts for multiple stakeholder perspectives
  - Users
  - Security
  - Designers
  - Decision-makers

## Scenario

- DoD needs to build a new secure telephone that uses a smart card
- User's cryptologic key and pin are stored on the card
- DoD needs to ensure the smart card is
  - Secure
  - Easy to use
  - Inexpensive



## Confusion Follows



Chief Security Officer



You can't use this design. There is a vulnerability that will allow an unauthorized person to get the key off the card.

Then encrypt the key using 256 bit encryption

Really? Then do something else...add a biometric to the phone or something. I won't approve this!

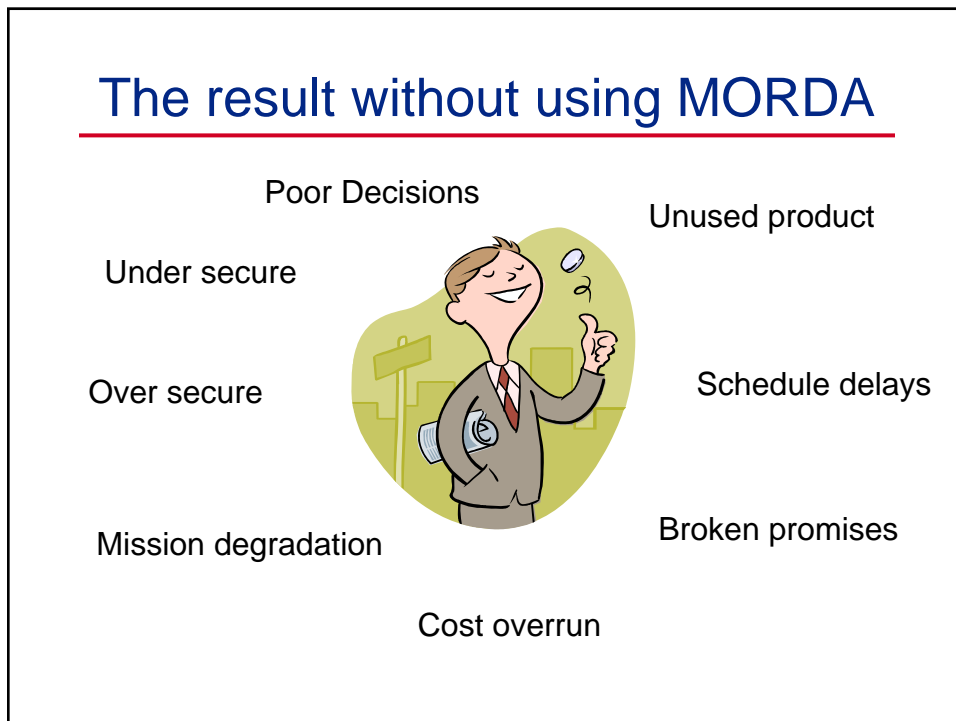
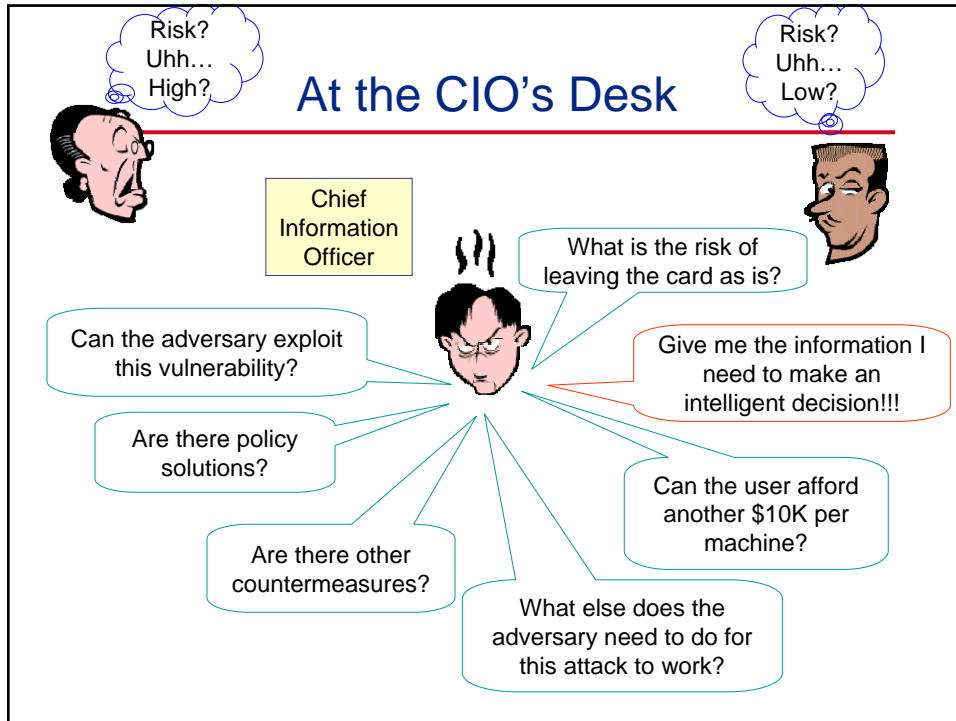
Chief Technology Officer



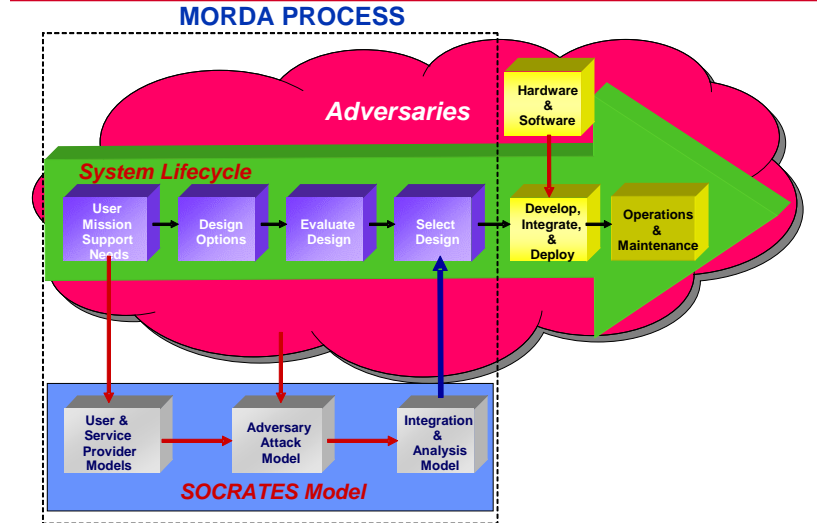
We have to use the card

Then the pin would have to be 90 characters long!!!

We can do that. But it will slip the project by 1 year and cost an extra \$10,000 per phone.

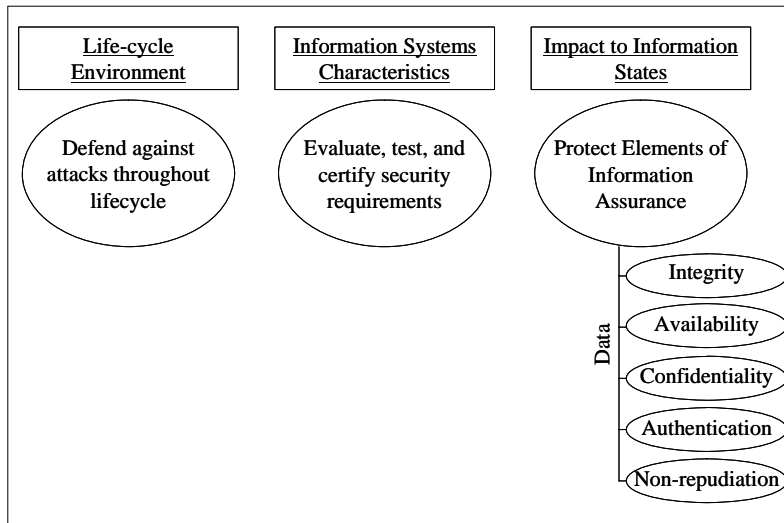


# MORDA supports the design process with MODA models



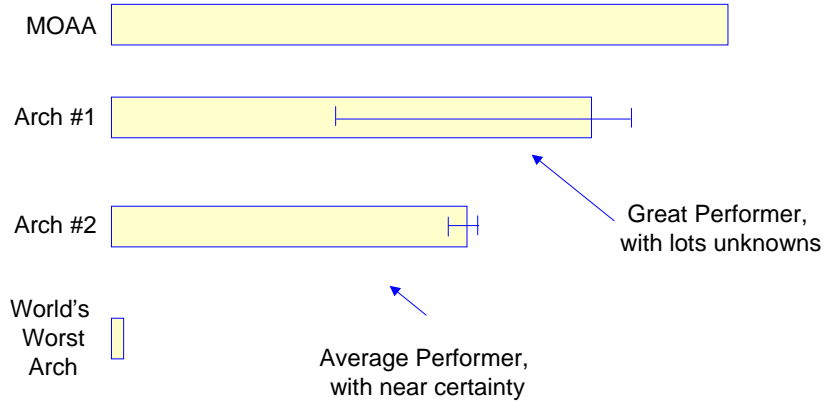
Buckshaw, D. L., Parnell, G. S., Unkenholz, W. L., Parks, D. L., Wallner, J. M. and Saydjari, O. S., "Mission Oriented Risk and Design Analysis of Critical Information Systems," *Military Operations Research*, 2005, Vol 10, No 2, pp. 19-38.

# But what is Information Assurance?



## Which Architecture is better?

---



## And what is the lifecycle?

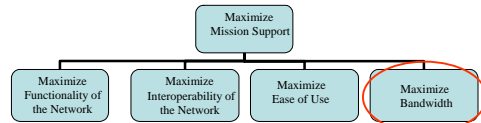
---

- DCID uses:
  - Design and Development,
  - First Test and Evaluation,
  - Second Test and Evaluation,
  - Operations and Maintenance, and
  - Disposal.
- DITSCAP uses:
  - Design,
  - Development,
  - Deployment,
  - Operation,
  - Support, and
  - Termination/Disposal.
- NIST uses:
  - Initiation,
  - Development/Acquisition,
  - Implementation,
  - Operation/Maintenance, and
  - Disposal.

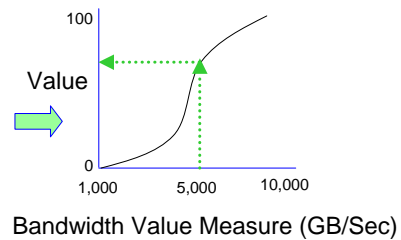
User & Service Provider Models

## Multiple Stakeholders have their own models

- Users are often concerned with performance, cost and mission support
- Service Providers worry about lifecycle costs, maintenance, and day-to-day operations
- All stakeholder preferences captured in value hierarchies with scales and value measures
- Architecture options are scored against the model



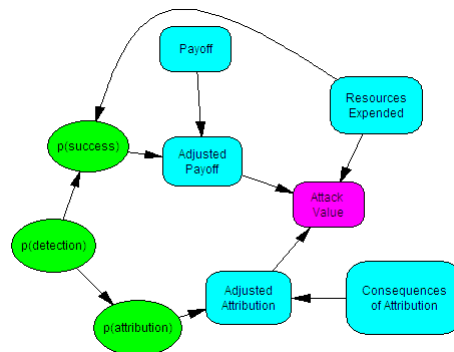
$$v(x_{Arch}) = \sum_{i=1}^n w_i v_i(x_{Arch})$$



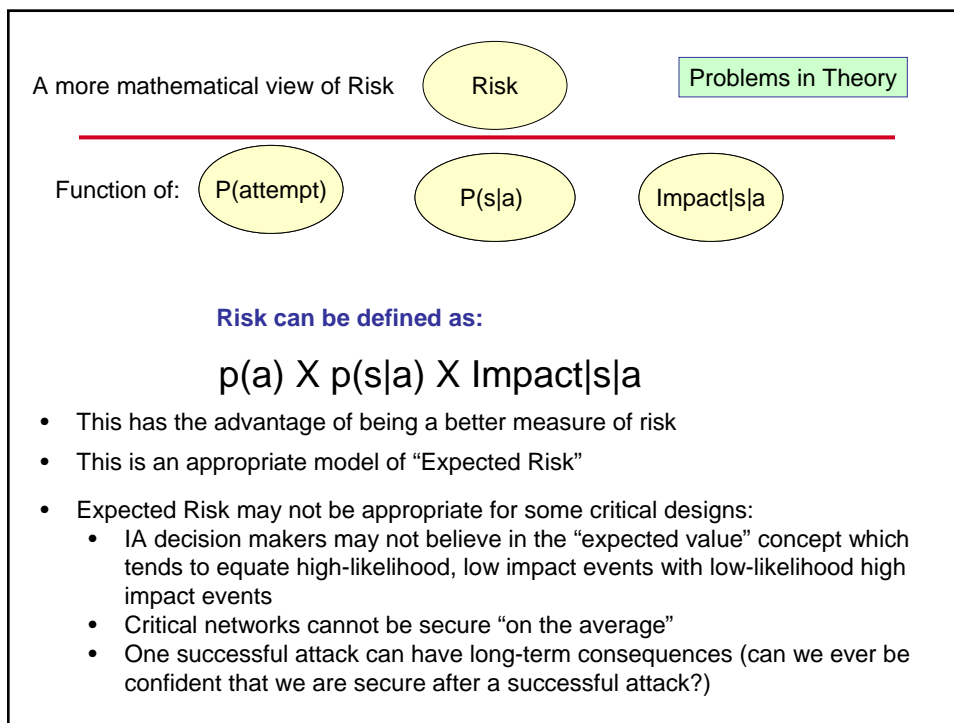
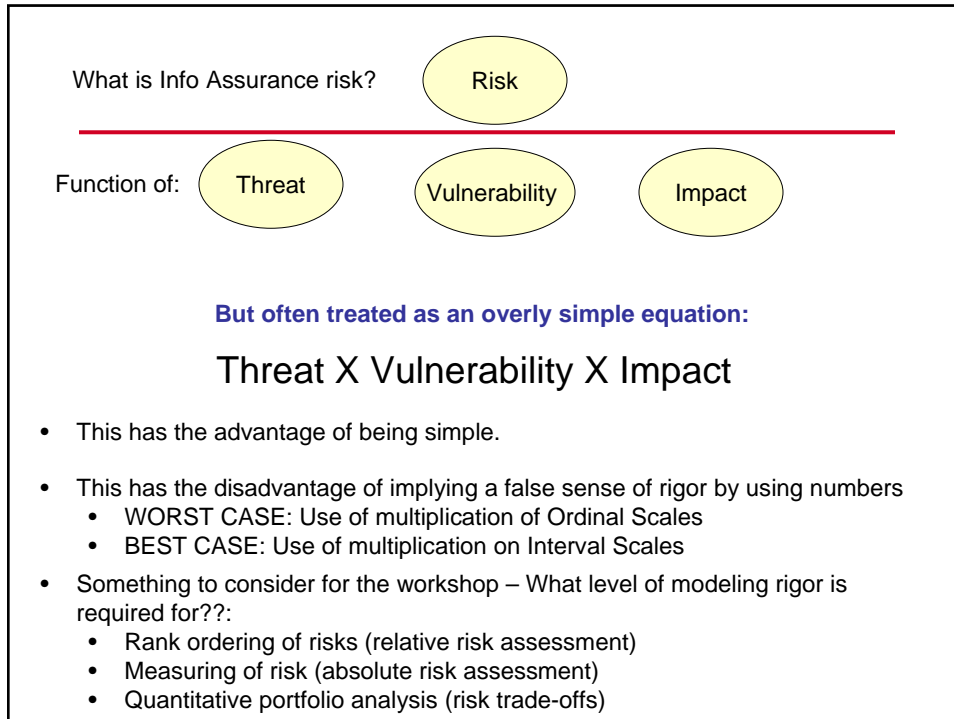
Adversary Attack Model

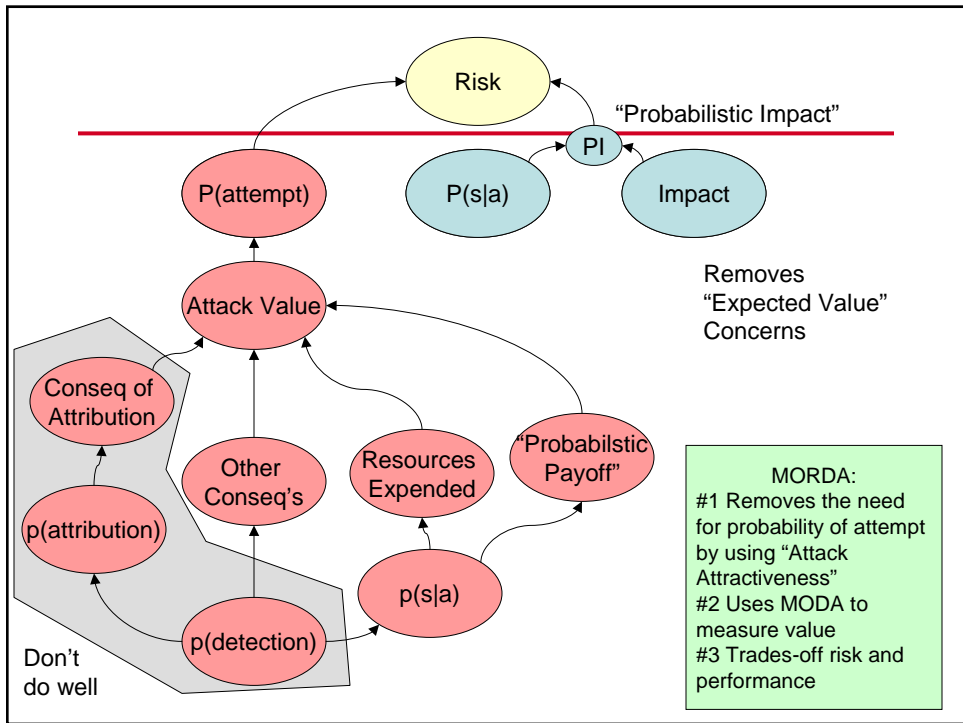
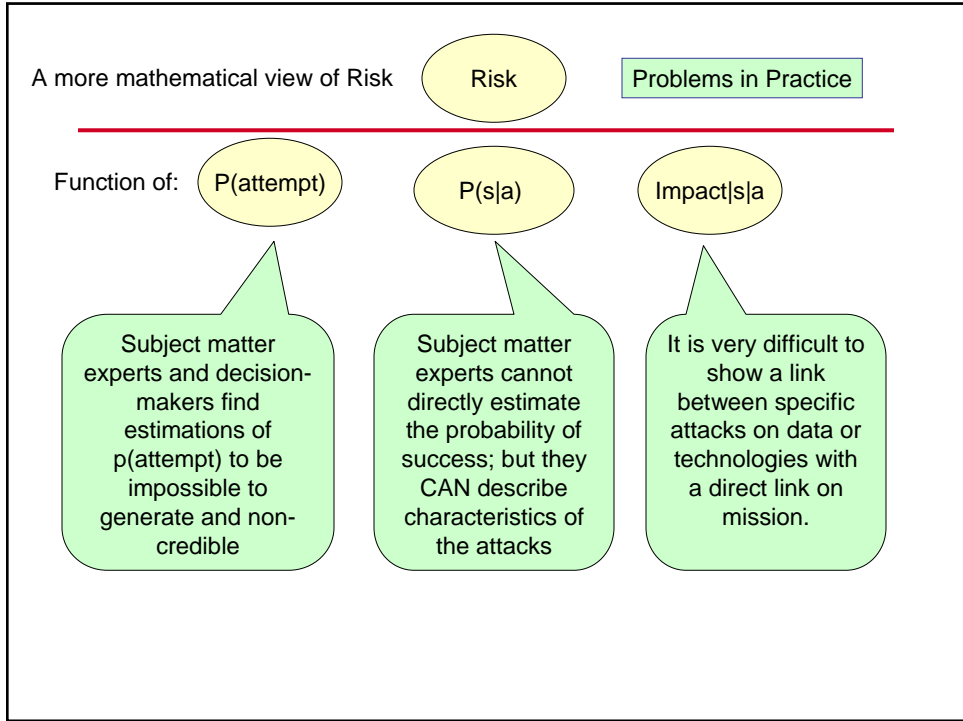
## Threat experts develop adversary models

- Adversaries have their own value model
- Adversary preferences often have multiple dependencies
- Attacks are scored with the adversary's value model



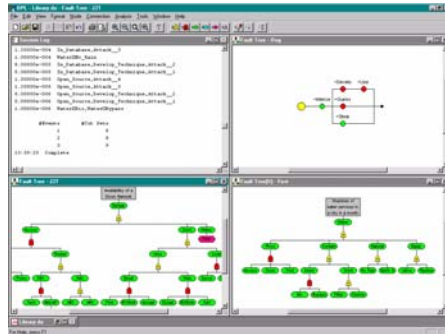
$$v(x_{Attack}) = \sum_{i=1}^n w_i v_i(x_{Attack})$$





## Security experts identify attacks against the system

- Attacks are defined as the minimum set of steps required to fulfill an adversary's objectives
- Attacks are comprised of attack steps
- Each attack step exploits a vulnerability
- Security Experts characterize attack steps using the adversary model
- Countermeasures alter the attractiveness of attack steps
  - Less likely to succeed
  - Less damaging
  - More detectable
  - More costly to attempt



## The attacks become the adversary's attack portfolio

<u>Attack Number</u>	<u>Attack Value</u>
Attack #1	1
Attack #2	.95
Attack #3	.7
o	o
o	o
o	o
Attack n	<u>.04</u>
$\Sigma$	25.65

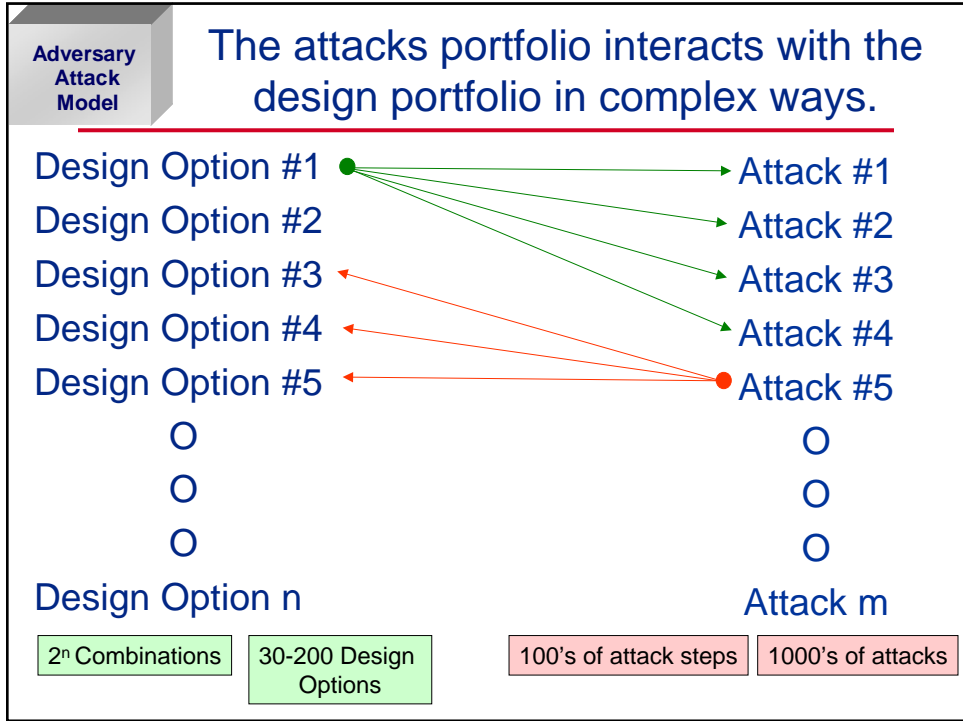
An attack with a value of "1" is:

- Very Likely to Succeed
- Unlikely to be detected
- Inexpensive to conduct

An attack with a value of ".04" is:

- Very Unlikely to Succeed
- Likely to be detected
- Expensive to conduct

We aggregate the individual attack scores into a portfolio score. We measure how this score changes with different design options.



**Adversary Attack Model**

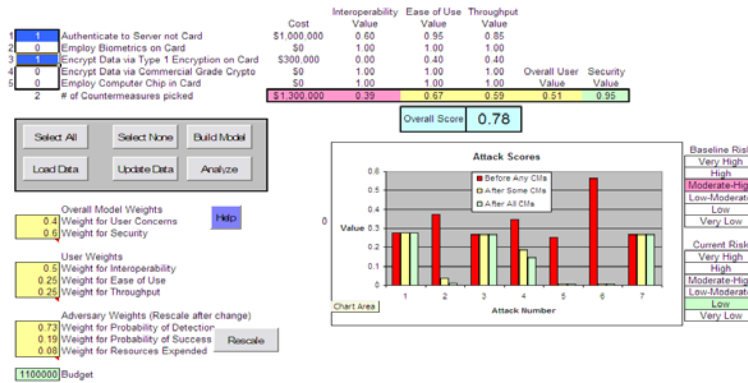
### Countermeasures and Design Options (CDOs) are very dependent on each other

Attack/CDO Effect Matrix	Adversary Value Model Measures			Cost to US to Implement CDO
	Likelihood of Detection	Likelihood of Success	Adversary Resources Required	
Password Attack Baseline - Outsider	Low-Medium	Medium - High	Very Low	N/A
CDO #1 Auditing	High			\$10,000
CDO #2 Good PW Policies	Medium	Medium		\$5,000
CDO #7 Install Firewall	Medium	Low	Low	\$35,000
CDO #8 Install VPN	Medium	Low	Low	\$35,000
CDO #9 Install IDS	Very High			\$35,000
Combined Effect of all CDOs	Very High	Very Low	Low	\$120,000

- CDOs interact in a complex manner
- The first CDO selected in a CDO portfolio will have its full security-mitigating value
- Subsequent CDOs added to the portfolio will have less value than if they were considered independent
- Heuristics are used to minimize data collection
  - 4 value measures, 10 attack steps, 15 CDOs = 1.3 Mil assessments
  - 610 assessments using the heuristic

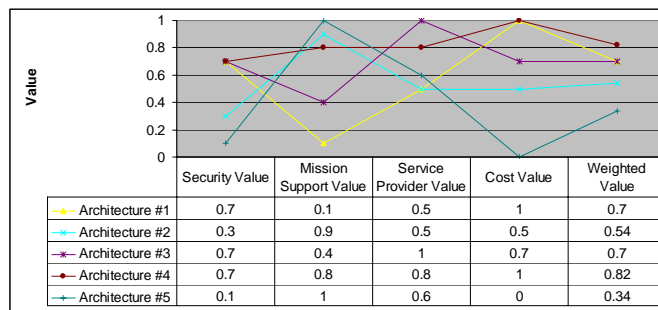
## The integration and analysis model trades off security and performance

- Excel-based Value Model
- Small numbers of architectures can be directly evaluated
- Moderate number of CDOs can be evaluated using optimization
- Large numbers of CDOs can be evaluated using benefit-cost analysis



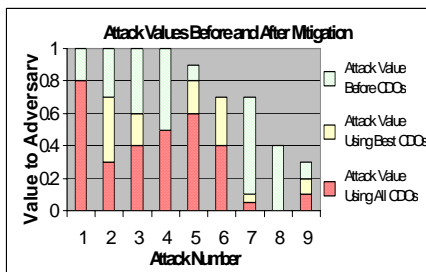
## The Aggregated Value Model can be used to pick the best architecture from a few options

- Directly score small number of good alternatives using Value Focused Thinking
- Swing weights can be applied across models
- Designers can then improve their architectures



## Optimization can be used to determine the best trade-off of performance versus cost

- Countermeasures can be combined to form hundreds of possible architectures
- The optimization is complex, but spreadsheet-based
- The optimization maximizes the net benefit of security versus performance for multiple stakeholders

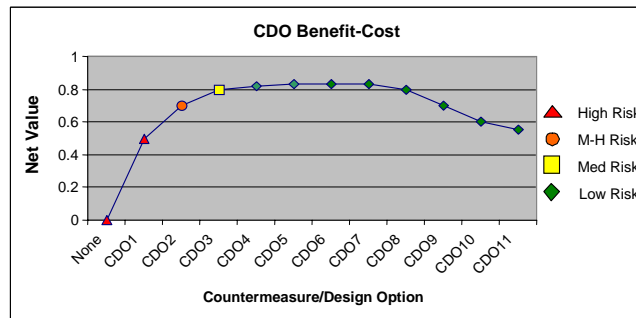


Baseline Design	Arch #1	Arch #2	Arch #3	Hypothetical best	Attack Value Range
11	1	1			>.9 Very High
4	2				.7-.9 High
1	1	1	5	1	.5-.7 Moderate-High
	2	4	6	7	.3-.5 Low-Moderate
	6	9	5		.1-.3 Low
	4	1		8	<.1 Very Low

Table 5. Risk Profile for Three Architectures

## The Net-Value Added model provides a stable ordering of CDOs

- Different than traditional, independent benefit-cost analysis
- The best CDO is the first added to the portfolio
- Subsequent CDO value is determined given that the first CDO is in place
- This provides a good, stable solution



## MORDA has been successfully used on ten projects.

Applications	Adversaries' Attack Value Model				User Model	Service Provider Model	Integration and Analysis Model	
	Scenarios	Attacks/Total Attack Steps	Adversary Classes	Attributes	# of Attributes	# of Attributes	# of CDOs	Architectures
Multilevel Network	1	10,000/10,000	1	1	0	0	10	10
DoD C2 Network	2	29/29	1	3	4	0	25	2^25
Agency Software	2	128/83	2	3	5	0	93	2^93
Joint C2	2	400/400	2	4	6	0	200	2^200
Agency Hardware	2	400/400	2	4	6	0	40	2^40
Key Management	1	482/27	2	5	11	11	68	44
Architecture Down-Select	3	75/38	1	3	0	0	0	3
Parallel Operations	1	2549/134	3	5	7	0	0	5
Web Vulnerabilities	1	51/25	2	6	0	0	2	2
GIG IA	2	100,000's	4	4	?	?	?	?

## MORDA has been gaining acceptance with all stakeholders

- Managers at all levels love the process...
  - Feel like they understand the problem space for the first time
  - Feel comfortable making resource commitments

But expanding assessments to new teams are causing managers to feel that the process is too hard, takes too long

- Customers still worried
  - Are they trying to use numbers against us?
  - If I tell them my preferences, I won't get everything I want!!
- System Certifiers and Developers have mixed feelings
  - Lots of work, but good, traceable output
  - I can make a better product with this!
- Threat evaluators are starting to participate
  - Initial reluctance to provide estimates of adversary behavior
  - Leadership pressure for predictive analysis and threat-based decisions prompted participation in the process

## Challenges for Implementing MORDA

---

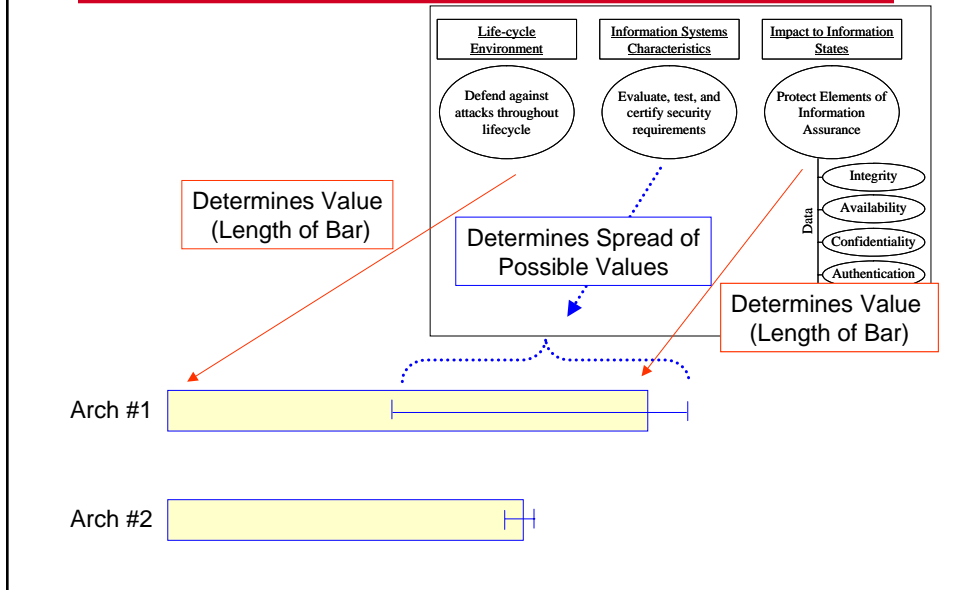
- Data, Data, and..... Data
  - Good data doesn't exist
  - Reluctance to make assumptions
  - Conflicting definitions among groups
  - Sensitivity issues
  - Problems with existing data
  - SOLUTION: Standardized attack lists and characteristics
- Experienced modelers needed
  - Axioms behind MODA
  - Independence assumptions
  - Measurable Value for Portfolio Analysis
  - Appropriate and consistent level of detail
  - SOLUTION: Experienced modelers on team; standardized attack data
- Conflicting interests from different stakeholders
  - Certifiers may be more interested in security
  - Developers may be more interested in an operational network
  - Users want something cheap and easy to use...and secure too
  - SOLUTION: Traceable and transparent methods using best practices (MODA); Sensitivity analysis

## Challenges for Implementing MORDA

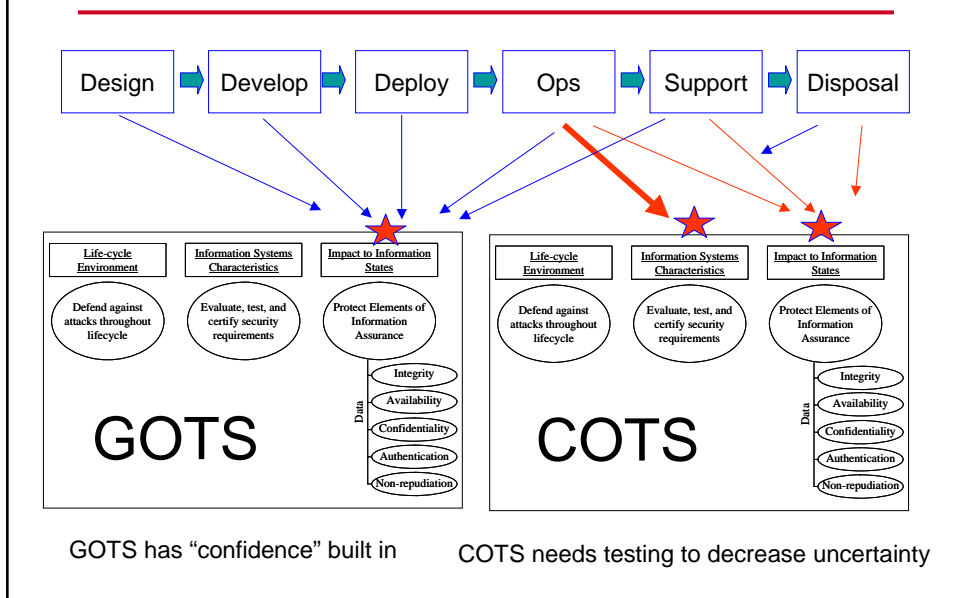
---

- Difficult to get network owners and security analysts to understand each other and the architectures
  - SOLUTION: Using questionnaires, formatted interviews and defining IA architectures through standard IA Functions
- Nonlinear nature of countermeasure and attack interaction
  - SOLUTION: Data elicitation framework and techniques that simplify and clarify the data collection process
- Hard to link attacks to technologies to effects on mission
  - SOLUTION:?
- Aggregating and translating numbers and analysis into meaningful, easy to understand results
  - SOLUTION:?

## Different Aspects of Assurance Have Different IA Benefits



## Assurance Countermeasures Might Appear Throughout the Lifecycle; COTS & GOTS may differ





# Questions??

Don Buckshaw  
Sr. Decision Analyst, Innovative Decisions, Inc.  
[dbuckshaw@innovatedecisions.com](mailto:dbuckshaw@innovatedecisions.com)  
540.226.5113