PURDUE UNIVERSITY CERIAS SEMINARS
Spring'09

M. Sahinoglu, Ph.D.
Director, Informatics Institute
Auburn University Montgomery, AL

SECURITY& PRIVACY METER-QUANTITATIVE RISK ASSESSMENT and MANAGEMENT WITH GAME THEORY

Key Words: Quantitative, Security, Privacy,Vulnerability, Threat, Countermeasure, Management, Game Theory, Cost

Motivation behind the Proposed Security Model

- The quantitative risk measurements are needed to objectively compare alternatives and calculate monetary figures to budget for reducing or minimizing the existing risk.

- There are virtually no such quantitative and probabilistic measures in the academia or corporate circles other than high, medium or low denominations which are descriptive, subjective and free to any interpretations as one pleases. They do not carry analytical monetary evaluations for comparisons when mitigation is done.

Motivation

- Among those existing analyses that favor a quantitative study, either
- i) there is no probabilistic frame about whether to add or multiply risks in a correct probabilistic frame of mind, or
- ii) the risk calculations are handled on singular basis without system picture.

The Proposed Math-Stat Model

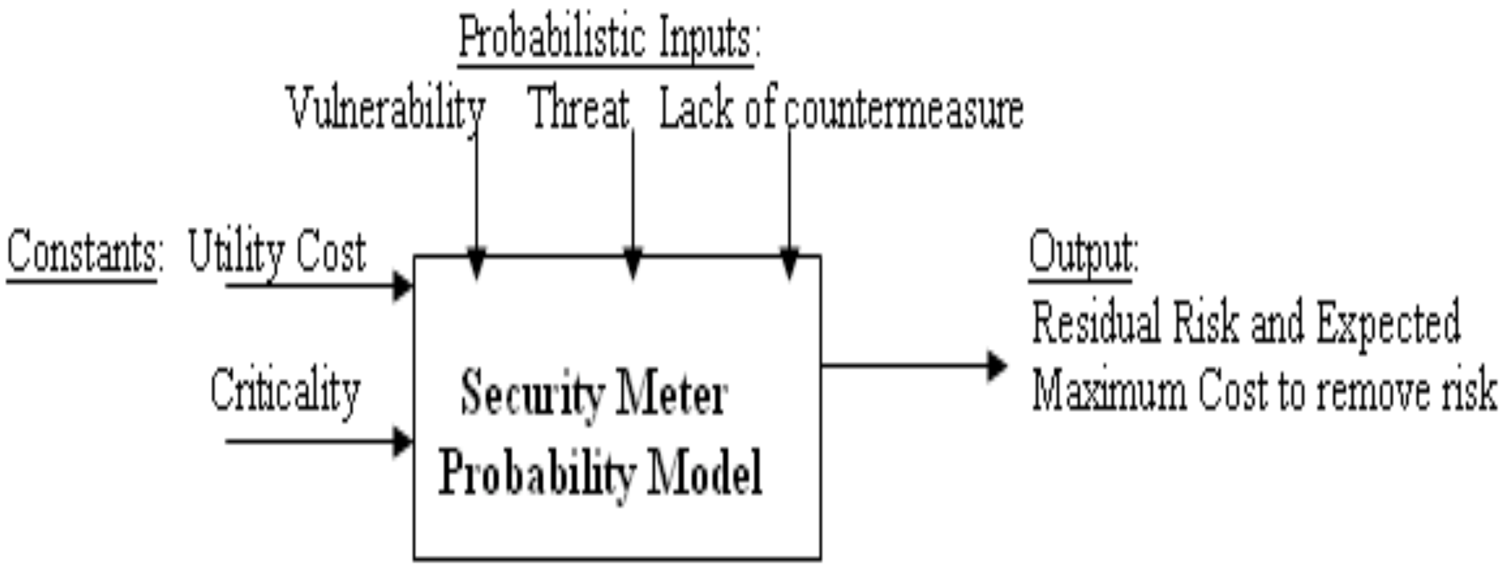
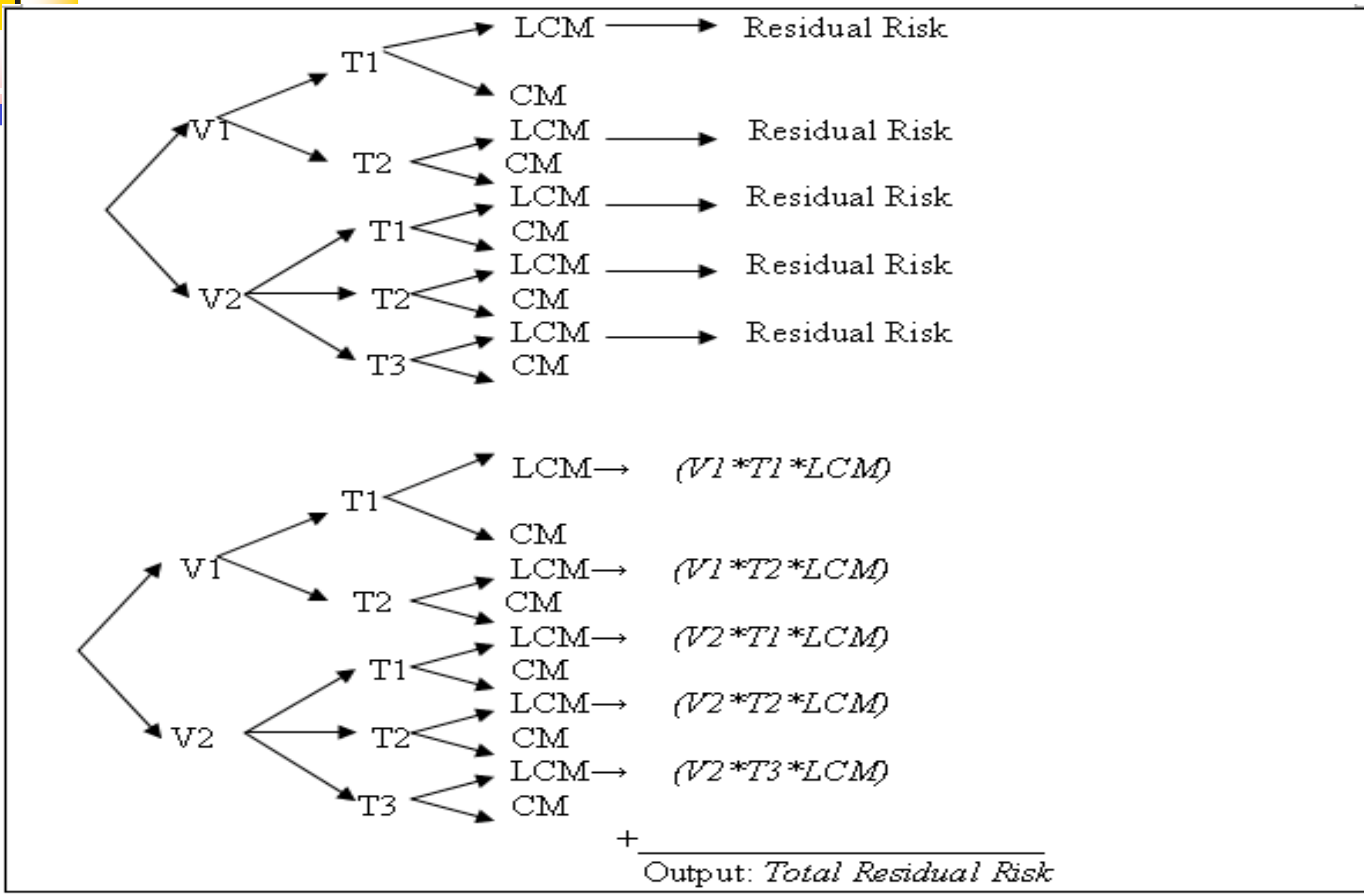


Figure 1. Quantitative Security Meter Probability Model

General Purpose Tree Diagram Example- Figure 2



Addition and Multiplication Laws of Probability

- Tree Diagram: Given that in a simple sample scenario, there are two or three or more of each choice, the following probabilistic frame holds.
- Note: Sum of V_i=1 and sum of T_{ij}=1 for each i, and Sum of LCM+CM=1 for each j, within a tree diagram structure.

A Real World Example to Implement the Security-Meter Design using Survey Results

- In a recent field study, CSI/FBI, Deloitte and Pricewaterhouse survey results were evaluated regarding the security concerns at the University of Virgina School of Continuing and Professional Studies Northern Virginia Regional Center. The Center's Senior Network Administrator estimated the servers to be worth $8,000.00. With a general risk assessment in mind and the quantitative security- meter method was selected as the primary method. (ref. 2008 IEEE I&M, June)

CSI / FBI Survey Countermeasure	% Of Respondents Reporting Them
Firewalls	97 (= CM_{13})
Anti-Virus Software	96 (= CM_{23})
Security Audits	80 (= CM_{14})
Intrusion Detection Systems (IDS)	72 (= CM_{31})
Security Awareness Policy Training	70 (= CM_{11})
Server-Based Access Control Lists (ACL)	70 (= CM_{32})
Encryption For Data In Transit	68 N/A, redundant, not used in the final table
Reusable Account/Login Passwords	52 N/A, redundant, not used in the final table
Encrypted Files	46 (= CM_{33})
Smart Cards/ One-Time Password Tokens	42 (= CM_{12})
Public Key Infrastructure	35 (= CM_{21})
Intrusion Prevention Systems	35 (= CM_{22})
Biometrics	15 N/A, redundant, not used in the final table

Figure 3: Security Meter Probability Source Data for Countermeasure actions utilized in Table 19

CSI / FBI Survey Threats and CIO / Pricewaterhouse Survey Threats	% Of Respondents Reporting Them
Virus	**66 (=T_{23})**
Malicious Code	**59 (=T_{32})**
Insider Abuse of Net Access	**48 (=T_{11})**
Laptop/Mobile Theft	**48 N/A, redundant, not used in the final table**
Unauthorized Access to Information	**32 (=T_{31})**
Denial of Service (DOS)	**32 (=T_{13})**
Abuse of Wireless Network and Web Site Defacement	**22 (=T_{21})**
System Penetration	**16 (=T_{12})**
Theft of Proprietary Information	**9 (=T_{33})**
Misuse of Public Web Application	**5 N/A, redundant, not used in the final table**
Financial or Telecom Fraud	**4 (=T_{14})**
Sabotage	**2 (=T_{22})**

Figure 4: Security Meter Probability Source Data for Threats utilized in Figure 6

Deloitte Survey Vulnerabilities	% Of Respondents Reporting Them
Internal Security Breach only	35 (= V_1)
External Security Breach only	26 (= V_2)
Both Internal and External Security Breach	39 (= V_1 and V_2)

Figure 5: Security Meter Probability Source Data for Vulnerabilities utilized in Figure 6 and 7.

Criticality Definition	Value Rating Factor
Asset's Loss has negligible impact on Center's mission	0.0
Asset's Loss has minor impact on Center's mission	0.2
Asset's Loss has moderate impact on Center's mission	**0.4 (selected in this example)**
Asset's Loss has significant impact on Center's mission	0.6
Asset is mission-critical to the Center. Loss would have serious impact on Center's Mission.	0.8
Asset is mission-essential to the Center. Center could not absolutely carry out mission without it.	1.0

Figure 5: Asset Criticality Rating for the Security Meter Design for an Asset of $8,000.00.

Vulnerability	Threat	Countermeasure
$V_1 = 0.35$ (Internal Security Breach Only)	$T_{11} = 0.48$ (Internal Abuse of Network Access)	$CM_{11} = 0.70$ (Security Awareness Policy Training) $LCM_{11}=0.30$ by Subtraction
	$T_{12} = 0.16$ (System Penetration)	$CM_{12} = 0.42$ (Smart Cards/Other One-Time Password Tokens) $LCM_{12} = 0.58$ by Subtraction
	$T_{13} = 0.32$ (Denial of Service	$CM_{13} = 0.97$ (Firewalls) $LCM_{13} = 0.03$ by Subtraction
	$T_{14} = 0.04$ (Financial / Telecom Fraud)	$CM_{14} = 0.80$ (Security Audits) $LCM_{14} = 0.20$ by Subtraction
$V_2 = 0.26$ (External Security Breach Only)	$T_{21} = 0.32$ (Denial of Service)	$CM_{21} = 0.35$ (Public Key Infrastructure) $LCM_{21} = 0.65$ by Subtraction
	$T_{22} = 0.02$ (Sabotage)	$CM_{22} = 0.35$ (Intrusion Prevention Systems) $LCM_{21} = 0.65$ by Subtraction
	$T_{23} = 0.66$ (Virus)	$CM_{23} = 0.96$ (Anti -Virus Software) $LCM_{23} = 0.04$ by Subtraction

Figure 6: Security Meter Probability Table for a Production server at The Center using Tables 15-18

$V_3 = 0.39$ (Both Internal and External Security Breaches Only)	$T_{31} = 0.32$ (Unauthorized Access to Information)	$CM_{31} = 0.72$ (Intrusion Detection Systems) $LCM_{31} = 0.28$ by Subtraction
	$T_{32} = 0.59$ (Malicious Code)	$CM_{32} = 0.70$ (Server Based Access Control) $LCM_{32} = 0.30$ by Subtraction
	$T_{33} = 0.09$ (Theft of Proprietary Information)	$CM_{33} = 0.46$ (Encrypted Files) $LCM_{33} = 0.54$ by Subtraction

Figure 6 continued: Security Meter Probability Table for a Production server at The Center using Tables 15-18.

Let's take a time-out, we will now play a Game like the whale plays everyday to outsmart rivals!

Game-Theoretic Approach for Firm A vs B in a two-player zero-sum game.

Note: 2% .NE.4%, a pure strategy solution does not exist. IT IS NOT OPTIMAL FOR EACH FIRM TO PREDICT AND SELECT a pure strategy regardless of what the other does. The optimal solution is a mixed STRATEGY (Maximin=Minimax).

Fig.7 Modified Payoff Table showing the % gain(loss) in Market Share for Firm A (B)

A / B	Increase Advertising b_1	Quantity Discounts b_2	Extended Warranty b_3	ROW MINIMUM		
Increase Advertising a_1	4	3	2	**2 Maximin**		
Quantity Discounts a_2	-1	4	1	-1		
Extended Warranty a_3	5	-2	5 (0)	-2		
COLUMN MAXIMUM	5	**4 Minimax**	5 (2) **Minimax**	~The solution to the game is for Firm A to raise advertising (a_1) by 2% and for Firm B to extend warranty (b_3) by 2%		
				CON: Firm A's market share will increase by 2%. Firm B's shall decrease by 2%.		

What to do next: Optimize by Linear Programming

Firm B's optimal mixed strategy is to provide quantity discounts (b_2) with probability 0.375, extend warranty (b_3) with prob. 0.625 and should not increase advertising b_1 with prob. 0. Expected loss of market share for Firm B of this mixed strategy is 2.375%, or gain of 2.375% for Firm A. This is in equilibrium. Firm B (or A) cannot improve the game by changing the B's (A's) probabilities. The expected B-loss (or A-gain) of this mixed strategy is 2.375%, which is better than Firm B's best pure strategy (b_2) with Minimax : 4% of share in the payoff table (or A's maxi in=2%).

- Min LOSSB, st.
- $4PB_1+3PB_2+2PB_3-LOSSB <=0$ (Strategy a_1)
- $-1PB_1+4PB_2+1PB_3-LOSSB<=0$ (Strategy a_2)
- $5PB_1- 2PB_2+ 5PB_3 - LOSSB<=0$(Strategy a_3)
- $PB_1 + PB_2 + PB_3 = 1$; LP results:
- $PB_1=0$, $PB_2=0.375$, $PB_3=0.625$, LOSSB=2.375

The Payoff Matrix in the Small Pox Example

In game-theoretic terms, the payoff matrix for this problem is:

	No Attack	Minor Attack	Major Attack
Stockpile	C_{11}	C_{12}	C_{13}
Biosurveillance	C_{21}	C_{22}	C_{23}
First Responders	C_{31}	C_{32}	C_{33}
Mass Inoculation	C_{41}	C_{42}	C_{43}

Note: Ideally, the option of not even stockpiling vaccine could have been part of this table. However, FDA management ruled against that exploration.

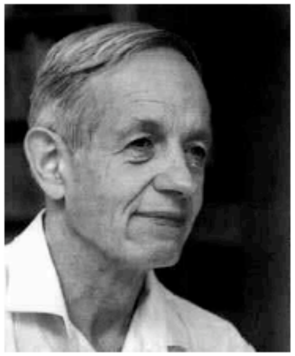
A classical game theory person would use the minimax theorem to find the optimal play for U.S. policy-makers. But this overlooks many problems.

History of Game Theory & Today

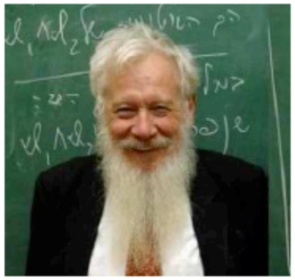
If we believed the assumptions, the von Neumann (1928) showed that the minimax solution is optimal. The U.S. picks the defense with the smallest row-wise maximum cost, and the terrorist picks the attack with the largest column-wise minimum cost.

If the common cell is not the one that attains the U.S. minimum and the terrorist maximum, then randomization is used. This gives a stable solution.

von Neumann



Nash



Aumann

Vulnerab.	Threat	CM & LCM	Res. Risk		CM & LCM	Res. Risk	Change	Cost	C= COST	per 1%
0.35	0.48	0.7			1		0.3	$170.10		$5.6
		0.3	0.0504		0	0				
	0.16	0.42			0.42		0	$0.00		
		0.58	0.03248		0.58	0.03248				
	0.32	0.97			0.97		0	$0.00		
		0.03	0.00336		0.03	0.00336				
	0.04	0.8			0.8		0	$0.00		
		0.2	0.0028		0.2	0.0028				
0.26	0.22	0.35			0.35		0	$0.00		
		0.65	0.03718		0.65	0.03718				
	0.02	0.35			0.35		0	$0.00		
		0.65	0.00338		0.65	0.00338				
	0.76	0.96			1		0.04	$22.63		
		0.04	0.007904		0	0				
0.39	0.32	0.72			0.9852		0.2652	$150.37		
		0.28	0.034944		0.0148	0.00184704				
	0.59	0.7			1		0.3	$170.10		
		0.3	0.06903		0	0				
	0.09	0.46			0.46		0	$0.00		
		0.54	0.018954		0.54	0.018954				
		Total Risk	0.260432		Total Risk	0.10000104	0.9052	$513.25		
		Percentage	26.04%		Percentage	10.00%				
BASE	SERVER	Final Risk	0.1041728		Final Risk	0.040000416		IMPROVED	SERVER	
Asset=	$8000	ECL	$833.38		ECL	$320.00				
Criticality=	0.40				Delta ECL	-$513.38				

Figure 8. Risk Management Spreadsheet prepared from Tables 14 and 18 to break even at $513 (difference due to round-off errors) for 90.52% countermeasure (CM) improvement with final RR = 10%.

Cm_{11} **NOTE: Rows □denote bad offenses, and columns good defenses in an information war**	cm_{12}	cm_{13}	Cm_{14}	cm_{21}	cm_{22}	cm_{23}	cm_{31}	cm_{32}	cm_{33}	loss B	<= >	RHS
V_1t_1 .35*.48=**.168**										-1	<	0
V_1t_2 .35*.16	**.056**									-1	<	0
V_1t_3 .35*.32		**.112**								-1	<	0
V_1t_4 .35*.04			**.114**							-1	<	0
V_2t_1.26*.22				**.0572**						-1	<	0
V_2t_2.26*.02					.0052 **Mini-max**					-1	<	0
V_2t_3.26*.76						**.1976**				-1	<	0
V_3t_1.39*.32							**.1248**			-1	<	0
V_3t_2.39*.59								**.2301 Maxi-min**		-1	<	0
V_3t_3.39*.09									**.0351**	-1	<	0

Mathematical Observations

- Interesting (unusual) tableau, because all elements are diagonals, and both max and min due to being singletons. Simply choose a minimum column-wise and maximum row-wise, which are not equal.

- CONCLUSION: The game-theory application software stabilized this lack of equilibrium into a desired two-player zero-sum game. This provides a list of countermeasure probabilities, CM11 with prob. 1.0, CM12 with 0.42…CM33 with 0.46. This is the optimal mixed strategy for Company B (defense) to minimize its expected loss while Company A (offense) maximizes its gain. Now the game plan is at equilibrium. Defense and Offense teams cannot change the game by altering CMij.

Vulnerab.	Threat	CM & LCM	Res. Risk		CM & LCM	Res. Risk	Change	Cost	C= COST per 1%	
0.35	0.48	0.7			1		0.3	$170.10		$5.6
		0.3	0.0504		0	0				
	0.16	0.42			0.42		0	$0.00		
		0.58	0.03248		0.58	0.03248				
	0.32	0.97			0.97		0	$0.00		
		0.03	0.00336		0.03	0.00336				
	0.04	0.8			0.8		0	$0.00		
		0.2	0.0028		0.2	0.0028				
0.26	0.22	0.35			0.35		0	$0.00		
		0.65	0.03718		0.65	0.03718				
	0.02	0.35			0.35		0	$0.00		
		0.65	0.00338		0.65	0.00338				
	0.76	0.96			1		0.04	$22.68		
		0.04	0.007904		0	0				
0.39	0.32	0.72			0.9852		0.2652	$150.37		
		0.28	0.034944		0.0148	0.00184704				
	0.59	0.7			1		0.3	$170.10		
		0.3	0.06903		0	0				
	0.09	0.46			0.46		0	$0.00		
		0.54	0.018954		0.54	0.018954				
		Total Risk	0.260432		Total Risk	0.10000104	0.9052	$513.25		
		Percentage	26.04%		Percentage	10.00%				
BASE	SERVER	Final Risk	0.1041728		Final Risk	0.04000042		IMPROVED	SERVER	
Asset=	$8000	ECL	$833.38		ECL	$320.00				
Criticality	0.40				Delta ECL	-$513.38				

Nonlinear Minimization of the Portfolio Variance (= Average of the sum of squares of the deviations from the mean value under each scenario) s.t. a constraint on the expected return of the portfolio.

- MIN = 1/10*(R1-Rb)^2 + 1/10*(R2 -Rb)^2 + 1/10*(R3 -Rb)^2 + 1/10*(R4 - Rb)^2 + 1/10*(R5-Rb)^2 + (R6 -Rb)^2 + 1/10*(R7 -Rb)^2 + 1/10*(R8 - Rb)^2 + 1/10*(R9-Rb)^2 + 1/10*(R10 - Rb)^2;

- **1*X1 < 1; 1*X2 < 1; 1*X3 < 1; 1*X4 < 1; 1*X5 < 1; 1*X6 < 1; 1*X7 < 1; 1*X8 < 1; 1*X9 < 1; 1*X10 < 1;**
- **1*X1 >0.7;**
- **1*X2 > 0.42;**
- **1*X3 > 0.97;**
- **1*X4 > 0.8;**
- **1*X5 > 0.35;**
- **1*X6 > 0.35;**
- **1*X7 > 0.96;**
- **1*X8 > 0.72;**
- **1*X9 > 0.7;**
- **1*X10 > 0.46;**
- **0.168*X1 = R1;**
- **0.056*X2 = R2;**
- **0.112*X3 = R3;**
- **0.014*X4 = R4;**
- **0.057*X5 = R5;**
- **0.0052*X6 = R6;**
- **0.1976*X7 = R7;**
- **0.1248*X8 = R8;**
- **0.2301*X9 = R9;**
- **0.0351*X10 = R10;**
- **1/10*(R1 + R2 + R3 + R4 +R5 + R6 + R7 + R8 + R9 + R10) = Rb;**
- **Rb > 0.09;**

Porfolio Approach (Markowitz Nonlinear Optimization Solution by LINGO Software):

- Porfolio Approach (MArkowitz Nonlinear Optimization Solution):
- Rows= 33 Vars= 21 No. integer vars= 0 Nonlinear rows= 1 Nonlinear vars= 11
- Objective value: 0.1026704E-01

Variable	Value
R1	0.1451340
RB	0.9000000E-01
R2	0.5600000E-01
R3	0.1120000
R4	0.1400000E-01
R5	0.5700000E-01
R6	0.5200000E-02
R7	0.1896960
R8	0.1248000
R9	0.1610700
R10	0.3510000E-01
X1	0.8638929
X2	1.000000
X3	1.000000
X4	1.000000
X5	1.000000
X6	1.000000
X7	0.9600000
X8	1.000000
X9	0.7000000
X10	1.000000

Nonlinear Portfolio Risk Table

Vulnerab.	Threat	CM & LCM	Res. Risk		CM & LCM	Res. Risk	Change	Cost	C= COST per 1%
0.35	0.48	0.7			0.8638929		0.1638929	$27.23	$1.6
		0.3	0.0504		0.136107	0.02286599			
	0.16	0.42			1		0.58	$96.36	
		0.58	0.03248		0	0			
	0.32	0.97			1		0.03	$4.98	
		0.03	0.00336		0	0			
	0.04	0.8			1		0.2	$33.23	
		0.2	0.0028		0	0			
0.26	0.22	0.35			1		0.65	$107.99	
		0.65	0.03718		0	0			
	0.02	0.35			1		0.65	$107.99	
		0.65	0.00338		0	0			
	0.76	0.96			0.96		0	$0.00	
		0.04	0.007904		0.04	0.007904			
0.39	0.32	0.72			1		0.28	$46.52	
		0.28	0.034944		0	0			
	0.59	0.7			0.7		0	$0.00	
		0.3	0.06903		0.3	0.06903			
	0.09	0.46			1		0.54	$89.72	
		0.54	0.018954		0	0			
		Total Risk	0.260432		Total Risk	0.0997999	0.0938929	$514.02	
		Percentage	26.04%		Percentage	9.98%			
BASE	SERVER	Final Risk	0.1041728		Final Risk	0.03992		IMPROVED	SERVER
Asset=	$8000	ECL	$833.38		ECL	$319.36			
Criticality	0.40				Delta ECL	$514.02			

Conclusion: COCA (Cost Optimal Countermeasure Action)

- Game Theory Linear Programming approach yields better economical results than the Portfolio Nonlinear (Markowitz) for the same SEC-METER scenario: 90.52% vs. 309%, and if the same cost factor is used as in the earlier COCA approach, then 309-90.5= 218.5% times $5.67 would save $1239.

A QUICK JAVA APPLICATION

- THIS DEMO WILL SHOW HOW ACTUALLY THE GAME THEORY IS APPLIED TO COST/EFFORT OPTIMIZE THE COUNTERMEASURE ACTION AGAINST THE COMMON ENEMY SUCH AS HACKERS, CRACKERS, VIRUSES, HORSES, WORMS, COBRAS (THIS IS NEW - this strangler virus may poison- Need 'antivenom' software). Also beware Stingray virus whose cousin killed the Crocodile Hunter, Steve Irwin in Australia.

BABY COBRA SHOT BY THE AUTHOR AT THE CHILDREN'S ZOO IN MONTGOMERY AL in June 2005. SHE EXPECTS TO SOCIALIZE… Hint: There's no cobra virus, it was a joke only to jolt the sleepy!

A Humanoid StingRay shot by the Author in Sydney Aquazoo (April'05). Her name is Smiley Ray, she's all smiles. NO this was a joke too, no such StingRay virus exists. This picture won the "Featured Photographer" award in 2008 Exclusive and Private Laureates Society of Photography yearbook.

Featured Photographer

MEHMET SAHINOGLU

SMILEY RAY(A HUMAN-LIKE SIMILING STINGRAY)

Prof. M. Sahinoglu holds an Eminent Scholar position of Computer Science at Troy U. in Montgomery AL. A 2006 Microsoft Research Scholar, he is a published author in Turkey. His hobbies are amateur photography, writing, globe traveling. His new book is "Trustworthy Computing" by Wiley. MeSa@troy.edu

Security Meter Screenshot to Show Cost Optimization with Game Theory

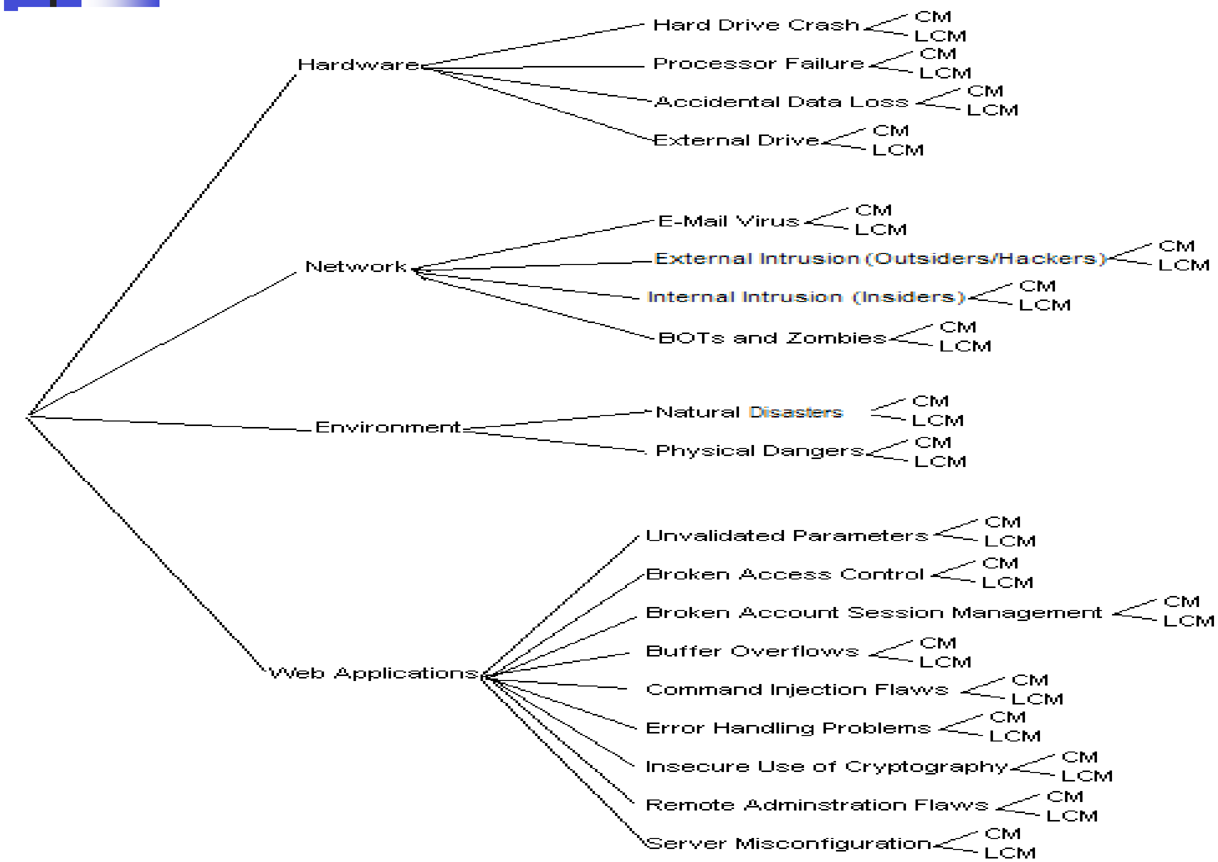
Vulnerab.	Threat	CM & LCM	Res. Risk	CM & LCM	Res Risk	Change	Cost	Advice
0.350000	0.480000	0.700000		1.000000		0.300000	$170.13	Increase the countermeasure capacity against the threat of "0.36" for the vulnerability of
		0.300000	0.050400	0.000000	0.000000			"v1" from the current 70.00% to suggested 100.00% for an improvement of 30.00%.
	0.160000	0.420000		0.420000				
		0.580000	0.032480	0.580000	0.032480			
	0.320000	0.970000		0.970000				
		0.030000	0.003360	0.030000	0.003360			
	0.040000	0.800000		0.800000				
		0.200000	0.002800	0.200000	0.002800			
0.260000	0.220000	0.350000		0.350000				
		0.650000	0.037180	0.650000	0.037180			
	0.020000	0.350000		0.350000				
		0.650000	0.003380	0.650000	0.003380			
	0.760000	0.960000		1.000000		0.040000	$22.68	Increase the countermeasure capacity against the threat of "" for the vulnerability of
		0.040000	0.007904	0.000000	0.000000			"v2" from the current 96.00% to suggested 100.00% for an improvement of 4.00%.
0.390000	0.320000	0.720000		0.985410		0.265410	$150.51	Increase the countermeasure capacity against the threat of "0.78" for the vulnerability of
		0.280000	0.034944	0.014590	0.001821			"v3" from the current 72.00% to suggested 98.54% for an improvement of 26.54%.
	0.590000	0.700000		0.999890		0.299890	$170.06	Increase the countermeasure capacity against the threat of "" for the vulnerability of
		0.300000	0.069030	0.000110	0.000025			"v3" from the current 70.00% to suggested 99.99% for an improvement of 29.99%.
	0.090000	0.460000		0.460000				
		0.540000	0.018954	0.540000	0.018954			
						Total Change	Total Cost	Cost per 1%
						90.53%	$513.38	$5.67

Criticality	**0.40**	**Total Risk**	**0.260432**	**Total Risk**	**0.100000**
Capital Cost	**$8000.00**	**Percentage**	**26.043200**	**Percentage**	**10.000004**
		Final Risk	**0.104173**	**Final Risk**	**0.040000**
		ECL	**$833.38**	**ECL**	**$320.00**
		Optimize	Change Cost	**ECL Delta**	**$513.38**

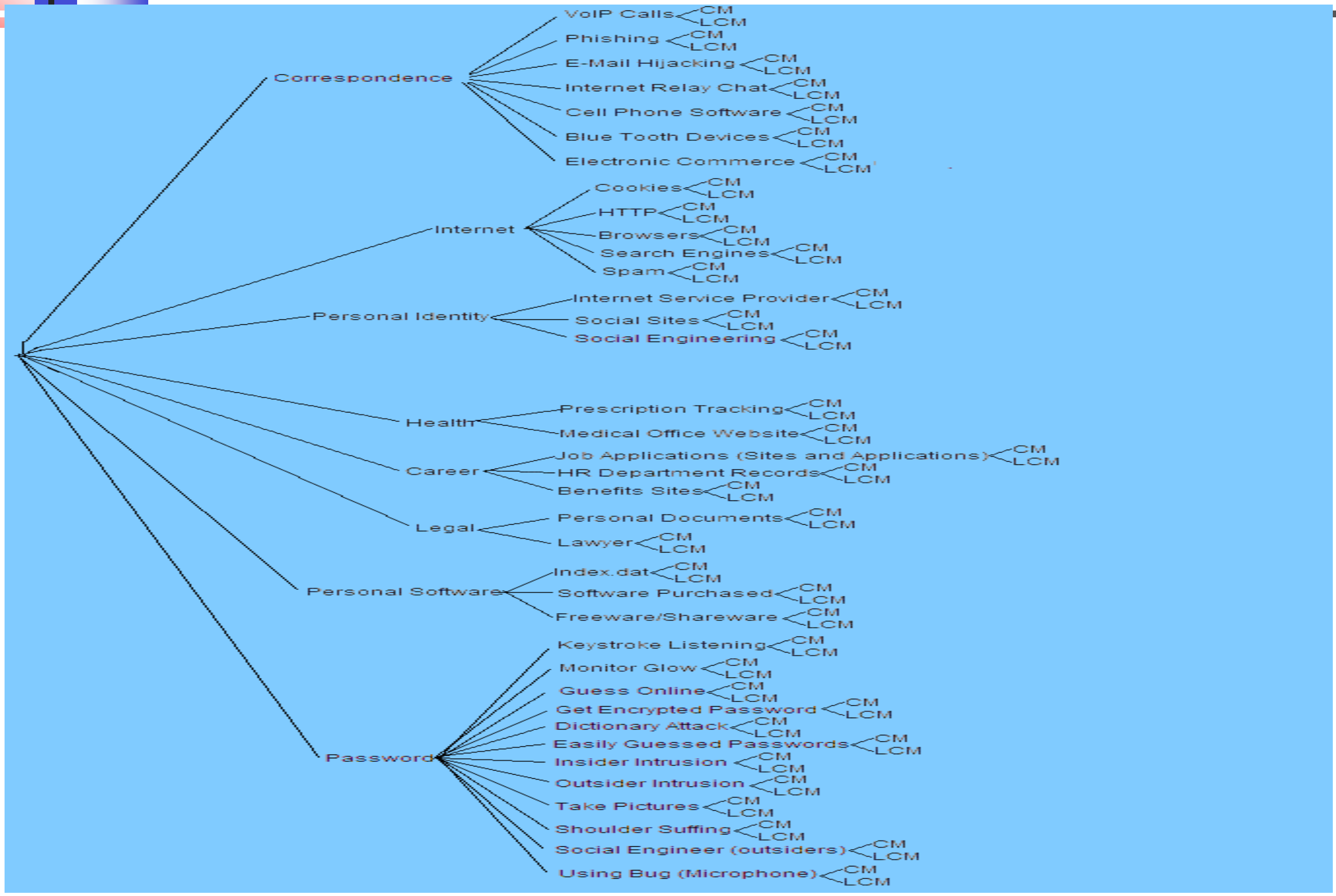
Further Research- Questionnaire Version

- We will not dwell on the earlier slides due to lack of time. Hope, you will see them before the seminar. During the majority of the seminar, I would rather demonstrate a challenging non-numerical data entry version (when numerical input data for vulnerabilities-threats-countermeasures are unavailable) which transforms the verbal-input domain to a numerical-output. Then, the Security-Meter machine will assess the Risk and apply Game-Theory to produce Cost Optimal Countermeasure Allocation (COCA). One can allocate market-realistic costs. We'll demo how to do mobile (external) text editing with XML files.
- Next observe tree diagrams of vulnerabilites, threats and countermeasures of 1)security, 2)privacy, 3)e-voting and 4)ecological risks, 5)wireless (pending) to name a few popular problem domains, which will be dealt with during the demo.

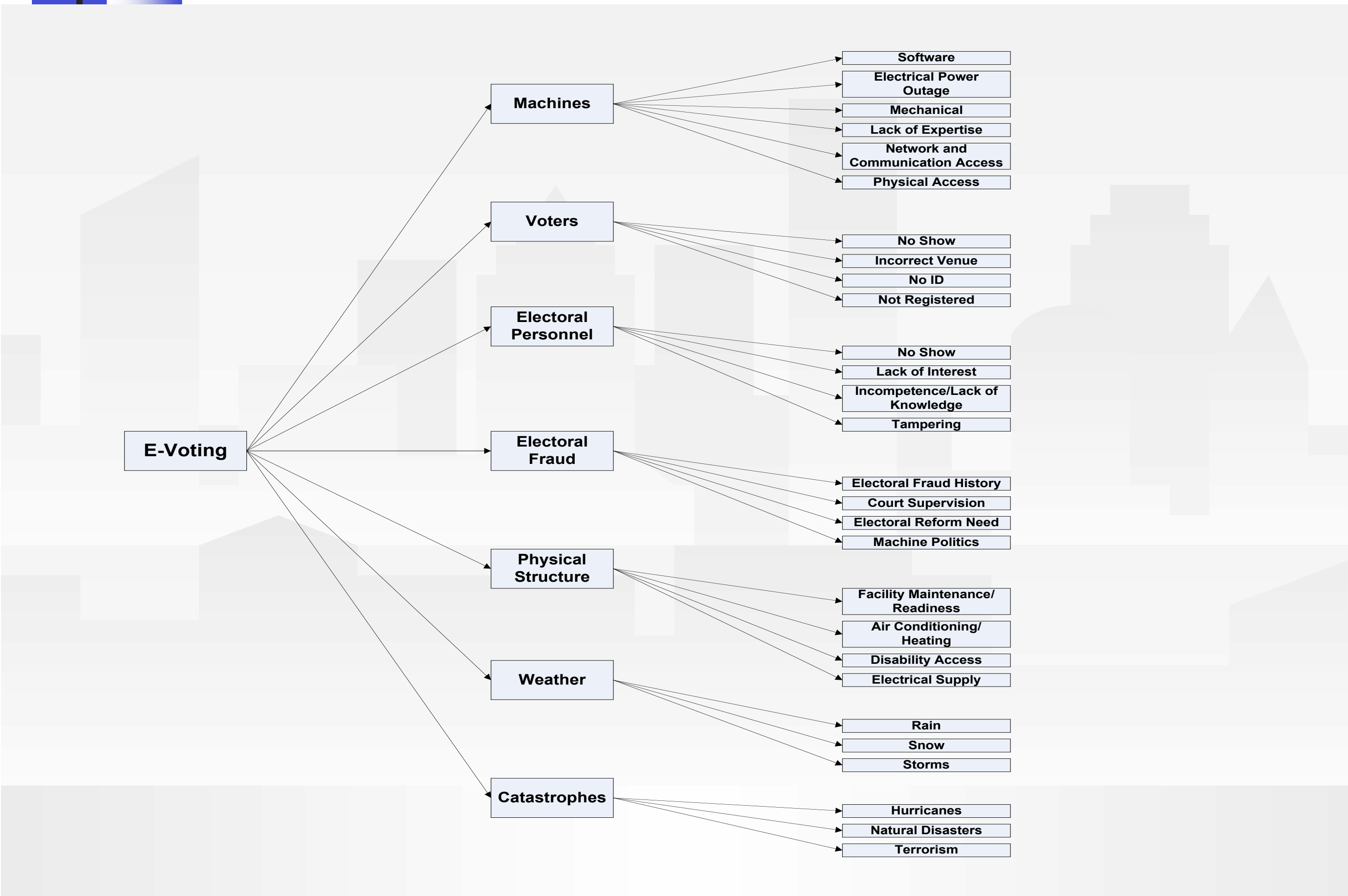
Security Risk Tree Diagram



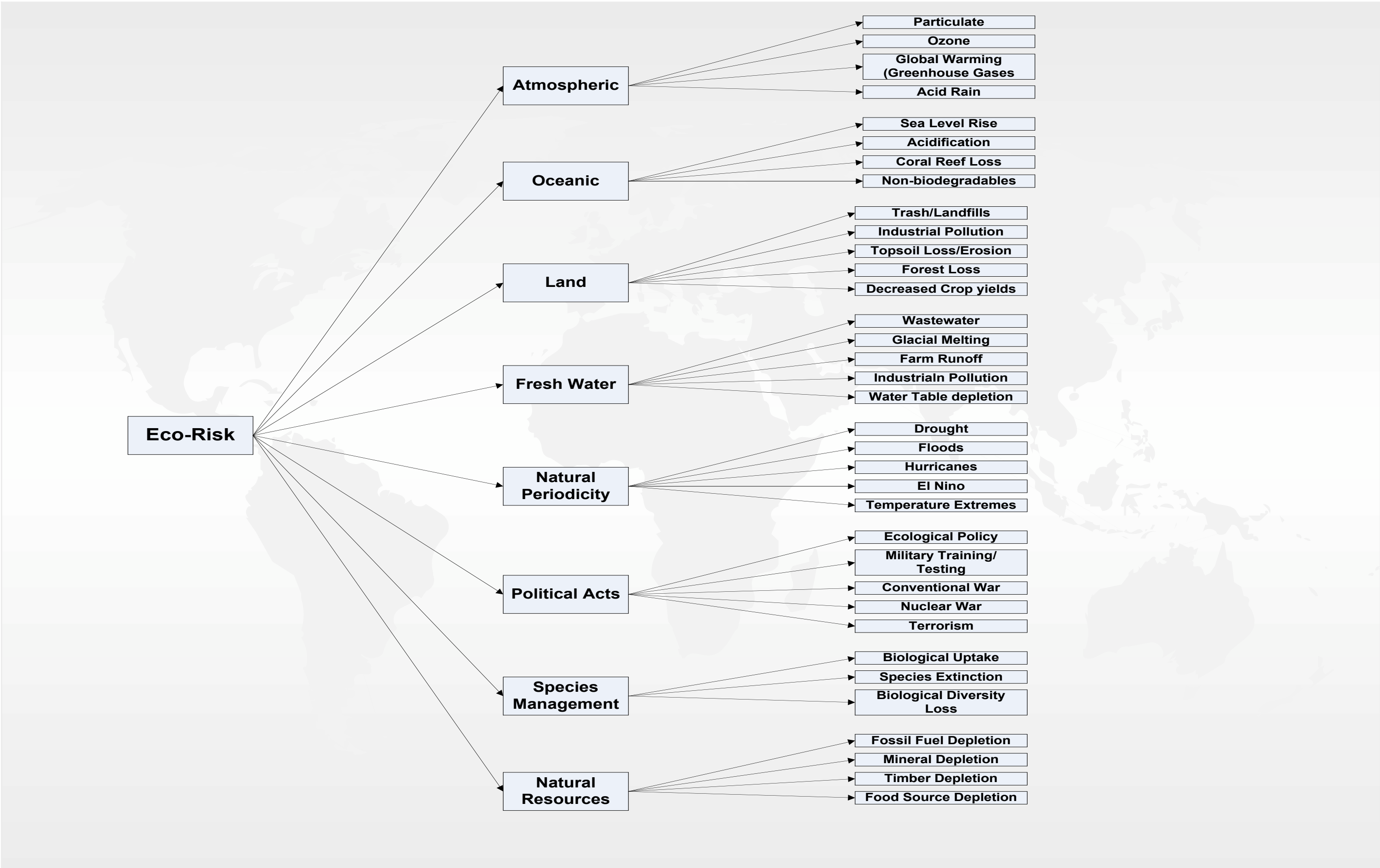
Privacy Risk Tree Diagram



E-Voting Risk Tree Diagram



Ecological Risk Tree Diagram



Thank You