Using Red Teams to Evaluate Adversary Impact on Survivable Systems

Bradley Wood
(bwood@bbn.com)
Senior Network Security Engineer
BBN Technologies

Outline

- Motivation
- Experiences
- Alternatives

Motivation

- Why measure "adversary impact"?
  - Adversaries have a negative impact on systems.
  - We want to limit the adversary's impact…
    - without complicating the operator's life.
- Approach
  - Measure the effort required by an adversary to impart a negative impact…
    - Let's call this value Adversary Work Factor.
    - We want to maximize this value.

Complications

- Direct observation of an adversary is problematic.
- Alternative
  - Use a Red Team to model the adversary
  - Main advantage is that observation is easier
  - Risks:
    - Does a Red Team provide a good model of an adversary?
    - Processes resembles experimentation with humans.
    - Processes have many variables.

Experiences

- This approach used by DARPA since 1998 in the (former) Information Assurance program and elsewhere *[Levin2003]*
- Successes
  - Information sharing, document generation, data collection, common understandings
- Challenges
  - Cost
  - Fragility of research mechanisms

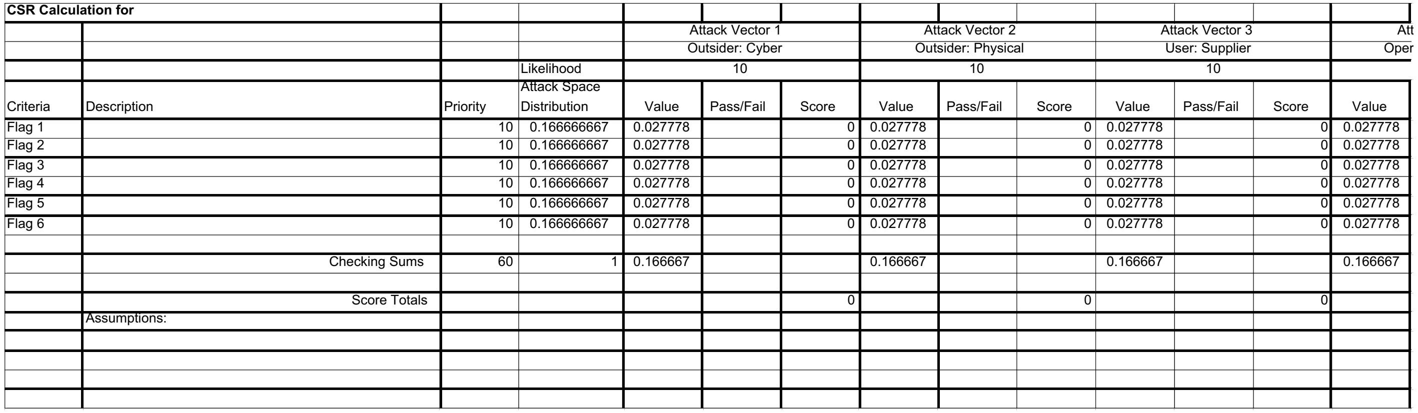
Alternative

- Requirements:
  - Absolute measure of security
  - Relevant for a given application and environment
  - Promotes desired behaviors:
    - Fix the biggest problems first.
    - The higher the measure, the better the security.
  - Simple enough to be calculated by operators
  - Cheap enough for commercial use

Critical Security Rating (CSR)

← Risks →

Consequences



CSR Calculation for													
				Attack Vector 1			Attack Vector 2			Attack Vector 3			Att
				Outsider: Cyber			Outsider: Physical			User: Supplier			Oper
			Likelihood	10			10			10			
Criteria	Description	Priority	Attack Space Distribution	Value	Pass/Fail	Score	Value	Pass/Fail	Score	Value	Pass/Fail	Score	Value
Flag 1		10	0.166666667	0.027778		0	0.027778		0	0.027778		0	0.027778
Flag 2		10	0.166666667	0.027778		0	0.027778		0	0.027778		0	0.027778
Flag 3		10	0.166666667	0.027778		0	0.027778		0	0.027778		0	0.027778
Flag 4		10	0.166666667	0.027778		0	0.027778		0	0.027778		0	0.027778
Flag 5		10	0.166666667	0.027778		0	0.027778		0	0.027778		0	0.027778
Flag 6		10	0.166666667	0.027778		0	0.027778		0	0.027778		0	0.027778
	Checking Sums	60	1	0.166667			0.166667			0.166667			0.166667
	Score Totals					0			0			0	
	Assumptions:												

↑ Mitigation Matrix ↑

CSR Values

- Consequence Values
  - What are the “bad things” to avoid?
  - How much do these impact our enterprise (percentages)
- Risk Values
  - Who or what might cause the “bad things”
  - How much do we worry about them (percentages)
- Mitigation Values
  - Is Consequence X mitigated against Risk Y?
  - Yes => Px*Py; No => 0
- CSR = Sum(Px*Py) for all X and Y values

Example

	Adversary			A		B		C		D		E		F	
	Description			Outsider: Cyber		Outsider: Physical		User: Supplier		Operational Insider		Knowledgable Outsider		Lifecycle Developer	
	Rank			10		9		8		7		6		5	
	Probability of Attack			0.2222		0.2000		0.1778		0.1556		0.1333		0.1111	
Risk	Description	Rank	Priority	Value	Pass/ Fail	Value	Pass/ Fail	Value	Pass/ Fail	Value	Pass/ Fail	Value	Pass/ Fail	Value	Pass/ Fail
A	DOS of customer web interface	10	0.2041	0.0454		0.0408		0.0363		0.0317		0.0272		0.0227	
B	DOS of company trading capability	9	0.1837	0.0408		0.0367		0.0327		0.0286		0.0245		0.0204	
C	Steal $$$	8	0.1633	0.0363		0.0327		0.0290		0.0254		0.0218		0.0181	
D	Cause 60% Slowdown, (>30 min)	7	0.1429	0.0317		0.0286		0.0254		0.0222		0.0190		0.0159	
E	Publicly Report Compromise	6	0.1224	0.0272		0.0245		0.0218		0.0190		0.0163		0.0136	
F	Make Fraudulent trades	5	0.1020	0.0227		0.0204		0.0181		0.0159		0.0136		0.0113	
G	Steal Customer Data	4	0.0816	0.0181		0.0163		0.0145		0.0127		0.0109		0.0091	
	Score Totals														

Observations

- Process was tested at a West Coast R&D laboratory with favorable results
- Process is still highly subjective
  - Burden is on the *operator; s*imilar to *reality* in many groups
- Process is much cheaper than a Red Team assessment
- Process can be completed by the operator
- Mitigation matrix needs some work.
- Effects can be extended to survivability factors

Summary

- In the beginning, we tried measuring Team Work Factor
  - Very informative process
  - Very expensive process
- New measure is the Critical Security Rating (CSR)
  - Potential to have a large positive impact
  - It is a new process that needs some work

To probe further…

Schudel and Wood, Adversary Work Factor as a Metric for Information Assurance, proceedings from the *New Paradigms in Security Workshop,* September 18-22, 2000, Ballycotton, County Cork, Ireland, published by the Association of Computer Machinery

Schudel and Wood, DARPA IA Red Team Experiments, *MILCOM 2000*, October 2000, proceedings published by the IEEE Press

Wood, Bouchard, and Farrell, Evaluating the Effects of Adversary Behavior on Dependable Systems, proceedings from the *2001 Dependable Systems and Networks Conference*, June 30 to July 4, 2001, Goteborg, Sweden, available from IEEE press

Kewley, D. and Bouchard, J., DARPA Information Assurance Program Dynamic Defense Experiment Summary, proceedings from the *IEEE SMC IAS Conference*, West Point, New York, June 2000

Levin, David, *Lessons Learned in Using Live Red Teams in IA Experiments*, Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX III), 22-24 April 2003, published by the IEEE press

Cyber-Security and the Insider Threat to Classified Information, published by the National Research Council, Computer Science and Telecommunications Board, 1-2 November 2000

Wood, Bradley, *An Insider Threat Model for Adversary Simulation*, proceedings from Workshop #2, Research on Mitigating the Insider Threat to Information Systems, August 2000, published by the RAND Corporation

Wood, Bradley, and Duggan, Ruth, *Red Teaming of Advanced Information Assurance Concepts,* proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX I), Volume II of II, January 2000, published by the IEEE