Quantifying Security Threats and Their Impact

A. Ben Aissa, Tunis

R.K. Abercrombie, F.T. Sheldon, ORNL

A. Mili, NJIT

Plan

- Shifting/Expanding the Focus of Cybersecurity
- Challenging traditional metrics
- The Mean Failure Cost
- Illustration: an E-Commerce Application
- Applications for Decision Support
- Summary and Assessment

Shifting/Expanding the Focus of Cybersecurity

- Cybersecurity: An arms race
  - Perpetrators vs System Custodians.
  - Perpetrators are winning, One trick ahead.
  - Custodians: defensive posture, plugging vulnerabilities.
- Cybersecurity defenses
  - Defends against known/ pre-modeled threats.
  - Unable to deal with unknown threats.
  - Unable to predict/ plan for future threats.

Shifting/Expanding the Focus of Cybersecurity

- First Step: A viable metric of Cybersecurity.
  - *Une Science a l'age de ses instruments de mesure*.
  - A science is as advanced as its instruments of measurement.
- Required Background for:
  - Measuring security requirements, security attributes.
  - Planning cybersecurity defenses.
  - Assessing, comparing solutions, alternatives.

A Shift of Focus is Needed

- From hypothesized causes (vulnerabilities, threats, intrusions),
- To actual, observable, quantifiable, measurable effects: the loss caused by (lack of) security.
- Insights/Experience from Reliability: a shift from faults and errors (hypothesized causes) to failure (observable effects).
- Insights/Experience from Reliability Measurement: a shift from fault density to MTBF and MTTF.
- Empirical Rationale: great variance in impact of faults on failure. Same for security?

A Shift of Focus is Needed

- Adapted to Systems of the Future.
  - Ultra Large Scale Systems (www.sei.cmu.edu/uls/).
  - SEI Panel (11+11), 2005-2006.
  - Projected Size: 1 B lines of code.
    - ***Size Changes Everything***.

A Shift of Focus is Needed

- Characteristics of ULS Systems.
  - Decentralized control,
  - Conflicting, unknowable, diverse requirements,
  - Continuous evolution and deployment (erosion of the development/ maintenance boundary),
  - Heterogeneous, inconsistent, and changing elements,
  - Erosion of the people/ system boundary,
  - Normal Failures.

Plan

- Shifting/Expanding the Focus of Cybersecurity
- Challenging traditional metrics
- The Mean Failure Cost
- Illustration: an E-Commerce Application
- Applications for Decision Support
- Summary and Assessment

Taking Cues from Reliability

- Reliability: MTBF, MTTF.
- Security: MTTD, MTTE.
- MTBF, MTTF: Major flaws
  - Independence vis a vis stakeholders. The same MTTF may mean different things to different stakeholders.
  - Independence vis a vis requirements clauses. The same MTTF may mean different things depending on what clause has been violated.
  - Independence with respect to V&V impacts.

Independence vis a vis stakeholders

Stakeholders are not created equal.

- The MTTF is a characteristic of the system.
- The same MTTF value may mean different things to different stakeholders depending on their stakes in the system's operation.
- Need for a metric that is stakeholder dependent. Characteristic of the system and the stakeholder.

Independence vis a vis requirements clauses

Requirements are not created equal.

- The MTTF is blind vis a vis the structure of the requirements specification.
- It considers that any failure with respect to any requirement is a failure with respect to the whole specification.
- But stakeholders may have different stakes in different clauses. This is not reflected in the MTTF.

Independence vis a vis V&V measures

V&V Impacts are not created equal.

- When we take a V&V measure to improve the reliability of the system, we may improve the likelihood of satisfying one requirement more than another.
- The MTTF is blind to this structure, and captures only the likelihood of satisfying the overall requirements specification.

Plan

- Shifting/Expanding the Focus of Cybersecurity
- Challenging traditional metrics
- The Mean Failure Cost
- Illustration: an E-Commerce Application
- Applications for Decision Support
- Summary and Assessment

The Mean Failure Cost

- We consider a system S and stakeholders H1, H2, H3, … Hk.
- Random variable FCi: loss incurred by stakeholder Hi as a result of possible lack of security.
- Mean Failure Cost for stakeholder Hi: MFC(Hi), the mean of random variable FCi.

Stakes and Stakeholders

- We consider a system S and stakeholders H1, H2, H3, … Hk.
- Random variable FCi: loss incurred by stakeholder Hi as a result of possible lack of security.
- Mean Failure Cost for stakeholder Hi: MFC(Hi), the mean of random variable FCi.

Sample Stakes and Stakeholders

- Flight Control System, MTTF = 20 000 hours.
  - Wrt what requirement?
- Safety requirement
  - Airline company: civil liability + airline reputation.
  - Aircraft manufacturer: aircraft's track record.
  - Insurance company: price tag.
  - Passenger: his/her neck.
  - Passenger's life insurance company: payout.
  - Passenger's spouse: spouse – life insurance.
- Most of these costs can be quantified with great precision.

ST: *The Stakes Matrix*

- Requirement clauses R1, R2, R3… Rn.
  - STi,j: stakes that stakeholder Hi has in meeting requirement Rj (loss that Hi incurs if Rj is not satisfied),
  - PRj: probability that Rj is not satisfied.
- MFC(Hi): $$MFC_i = \sum_{1 \le j \le n} ST_{i,j} \times PR_j.$$
- Algebraically: $$MFC = ST \circ PR.$$

ST: *The Stakes Matrix*

ST	**R1**	**R2**	**R3**	**R4**	**…**	**…**	**…**	**…**	**Rn**
H1									
H2									
H3									
H4									
…					**Stakes that stakeholder Hi puts on meeting requirements Rj**				
…									
…									
…									
Hm									

ST: *The Stakes Matrix*

<table>
<tr><th>ST</th><th>R1</th><th>R2</th><th>R3</th><th>R4</th><th>…</th><th>…</th><th>…</th><th>…</th><th>Rn</th></tr>
<tr><td>H1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>H2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>H3</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>H4</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>…</td><td></td><td></td><td></td><td></td><td colspan="4" rowspan="4">Loss that stakeholder Hi incurs on failing to meet requirement Rj</td><td></td></tr>
<tr><td>…</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>…</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>…</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Hm</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

ST: *The Stakes Matrix*

Qualification:

$$MFC_i = \sum_{1 \le j \le n} ST_{i,j} \times PR_j.$$

This formula is approximative, usually an over-estimation.

- Requirements overlap,
- Some stakes/costs are counted multiple times.
- Failing to satisfy Ri and failing to satisfy Rj are not statistically independent.

To improve precision:

- Analyze how complex specifications are structured.
- Lattice Structure of Specifications (Refinement).

DP: *The Dependency Matrix*

- How do we compute PR? Probability of failing to meet requirement Ri.
- We consider the architecture of the system,
  - Components C1, C2, C3, … Ch
- Events Ei, $1 \leq i \leq h+1$:
  - Ei, $1 \leq i \leq h$: Ci has failed (single fault hypothesis)
  - E_{i+1}: No component has failed.
- Events Fj: System S has failed with respect to requirement Rj,

DP: *The Dependency Matrix*

- Bayesian Formula,
- PRj: probability of event Fj,
- Events Ek disjoint
- Hence:

$$PRj = \sum_{k=1}^{h+1} P(F_j \mid E_k) \times P(E_k).$$

- Algebraically,

$$PR = DP \circ PE.$$

DP: *The Dependability Matrix*

<table>
<tr><th>DP</th><th>E1</th><th>E2</th><th>E3</th><th>E4</th><th>…</th><th>…</th><th>…</th><th>E_h</th><th>E_{h+1}</th></tr>
<tr><td>R1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>R2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>R3</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>R4</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>…</td><td></td><td></td><td></td><td></td><td rowspan="4" colspan="4">Probability that Requirement Ri is violated if component Cj is compromised</td><td></td></tr>
<tr><td>…</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>…</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>…</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Rn</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

IM: The *Impact Matrix*

- How do we compute PE? The probabilities that various components are compromised?
- We consider the threat configuration of the system,
  - Threats T1, T2, T3, … Tp.
- Events Ti, 1≤i≤p+1:
  - Ti: Threat Ti has materialized during a unitary operation time.
  - T_{p+1}: No threat has materialized.
  - Hypothesis: No more than one threat per unit of time.
- Events Ek: Component Ck has been compromised as a result of a security failure,

IM: The *Impact Matrix*

- Bayesian Formula,
- PE_k: probability of event E_k,
- Events T_q disjoint
- Hence:

$$PE_k = \sum_{q=1}^{p+1} P(E_k \mid T_q) \times PT_q.$$

- Algebraically,

$$PE = IM \circ PT.$$

IM: The *Impact Matrix*

<table>
<tr><th>IM</th><th>T1</th><th>T2</th><th>T3</th><th>T4</th><th>…</th><th>…</th><th>…</th><th>T_p</th><th>T_{p+1}</th></tr>
<tr><td>E1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>E2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>E3</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>E4</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>…</td><td></td><td></td><td></td><td></td><td colspan="4" rowspan="4">Probability that component Ci is compromised if threat Tj has materialized</td><td></td></tr>
<tr><td>…</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>…</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>E_h</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>E_{h+1}</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

PT: The *Threat* Vector

- Now we must compute PT, the Threat vector.
  - Catalog of threats under consideration,
  - Probability of occurrence of each threat.
- Provided by the security team, on the basis of:
  - Analyzing perpetrator behavior,
  - Reviewing System vulnerabilities,
  - Collecting empirical data, etc.
- Similar to fault models in reliability analysis.

PT: The *Threat* Vector

IM	**Probability**
T1	
T2	
T3	
T4	
…	**Probability that threat T_q materializes during a unit of operational time (e.g. 1 hour)**
…	
…	
T_h	
T_{h+1}	**Prob that no threat materializes**

PT: The *Threat* Vector

- Summary Formula:

$$MFC = ST \circ DP \circ IM \circ PT.$$

- Stakes matrix, ST: Stakeholders.
- Dependability matrix, DP: architects.
- Impact matrix, IM: V&V group.
- Threat vector, PT: Security team.

Plan

- Shifting/Expanding the Focus of Cybersecurity
- Challenging traditional metrics
- The Mean Failure Cost
- Illustration: an E-Commerce Application
- Applications for Decision Support
- Summary and Assessment

Illustration: an E-Commerce Application

- Stakeholders,
- Requirements,
- Components,
- Threats.

E-Commerce: Stakeholders

- The Customer,
- The Merchant,
- The technical intermediary,
- The financial intermediary.

E-Commerce: Requirements

- Confidentiality,
- Integrity,
- Availability,
- Non repudiation,
- Authenticity,
- Privacy.

E-Commerce: Components

- Browser,
- Proxy Server,
- Router/ Firewall,
- Load Balancer,
- Web Server,
- Application Server,
- Database Server.

E-Commerce: Threats

- Threats on Communication protocols,
- Threats on systems,
- Threats on the information,
- Passive listening,
- Viruses,
- Trojan horses,
- DoS threats,
- Threats on the database.

Stakes Matrix

ST		Security Requirements					
		Confidentiality	Integrity	Availability	Non-repudiation	Authenticity	Privacy
Stake-holders	Customer	10	5	3	4	6	12
	Merchant	120	70	140	110	105	6
	Tech Int	20	20	40	20	30	20
	Fin Int	20	60	50	40	40	60

- Each row filled by relevant stakeholder, or on his behalf.
- Expressed in monetary terms: dollars, yens.
- Represents loss incurred and/or premium placed on requirement.

Dependability Matrix

DP		Components							
		Browser	Proxy Server	Router/ Firewall	Load Balancer	Web Server	Appl. Server	Database Server	No Failure
Security Requirements	Conf	0.2	0.2	1.0	1.0	0.333	0.333	0.5	0.0
	Int	0.2	0.2	1.0	1.0	0.333	0.333	0.0	0.0
	Avail	1.0	1.0	1.0	1.0	0.333	0.333	0.0	0.0
	NR	0.2	0.2	1.0	1.0	0.333	0.333	0.0	0.0
	Auth	0.2	0.2	1.0	1.0	0.333	0.333	0.5	0.0
	Priv	0.2	0.2	1.0	1.0	0.333	0.333	0.5	0.0

- Filled by System Architects,
- Probability of failure with respect to a requirement given that a component has failed.
- Dependent on topology, and operational attributes.

Impact Matrix

IM		Threats								
		Comm	Sys	Info	List	Virus	Troj	DoS	DB	NoT
Components	Brws	0.0	0.1	0.1	0.1	0.3	0.4	0.2	0.0	0.0
	Prox	0.5	0.1	0.1	0.3	0.3	0.4	0.2	0.0	0.0
	R/FW	0.5	0.1	0.1	0.3	0.3	0.4	0.6	0.0	0.0
	LB	0.0	0.1	0.1	0.1	0.3	0.4	0.6	0.0	0.0
	WS	0.0	0.6	0.6	0.2	0.3	0.4	0.2	0.0	0.0
	AS	0.0	0.1	0.1	0.1	0.3	0.4	0.2	0.0	0.0
	DBS	0.0	0.1	0.1	0.0	0.5	0.6	0.3	0.8	0.0
	NoF	0.4	0.3	0.1	0.1	0.05	0.05	0.1	0.2	1.0

- Filled by V&V Team,
- Probability of compromising a component given that a threat has materialized.
- Dependent on the target of each threat, likelihood of success of the threat.

Threat Vector

PT		Probability
Threats□	Comm	0.01
	Sys	0.02
	Info	0.01
	List	0.01
	Virus	0.03
	Troj	0.06
	DoS	0.03
	DB	0.02
	NoT	0.81

- Filled by Security Team,
- Probability of realization of each threat.
- Dependent on perpetrator models, empirical data, known vulnerabilities, known counter-measures, etc.

MFC Vector

Stakeholders	MFC $/hour
Customer	8.11
Merchant	112.97
Technical intermediary	31.17
Financial intermediary	54.24

- To be subtracted from each stakeholder's bottom line.
- Customer: passed on through higher prices + risks resulting from using e-commerce site (ID theft, etc).

Plan

- Shifting/Expanding the Focus of Cybersecurity
- Challenging traditional metrics
- The Mean Failure Cost
- Illustration: an E-Commerce Application
- Applications for Decision Support
- Summary and Assessment

Applications for Decision Support

- Trivial Application: lower bound on bottom line.
- Trivial Application: upper bound on insurance premium.
- Other Application: Cost Benefit Analysis.

Security Measures

Tentative classification into four categories:

- Preventive Measures: Controlling the Threat Vector.
- Evasive Measures: controlling the impact matrix.
- Hardening Measures: controlling the dependability matrix. Redundancy.
- Mitigation measures: controlling the stakes matrix. Contingency.

Assessing Security Measures

We want to improve the security of the system by taking some measure. Question: how do we know if the measure is worthwhile? How do we dispatch the cost of the measure on different stakeholders?

- We propose: Computing its ROI.
  - Investment cycle length,
  - Discount rate,
  - Investment cost,
  - Episodic (e.g. yearly) costs/ benefits

Assessing Security Measures

Estimating the yearly benefits of the security measure:

- Computing the current MFC, hypothetical MFC if the measure is implemented.
- Computing the MFC difference, in $/Hr.
- Converting it to $/yr using hours of usage per year for each stakeholder.

Assessing Security Measures

How do we dispatch investment costs on stakeholders?

- In proportion to MFC gains,
- In such a way as to make ROI's equal across stakeholders.

Is the investment worthwhile?

- For each stakeholder: if ROI>0, or some threshold.
- For the community: according to community-wide formula of benefit; for example, the cumulative NPV (NPV's are additive, ROI's are not).

Illustration: Deploying an Anti-virus

Stakeholers	Inv. Cost	ROI
Customer	0.98	0.073
Merchant	1426.35	0.073
Tech. Int.	391.98	0.073
Financ. Int.	680.68	0.073
	2500.00	

Illustration: Deploying Redundancy

Stakeholers	Inv. Cost	ROI
Customer	39.21	4.216
Merchant	45377.49	4.216
Tech. Int.	12351.18	4.216
Financ. Int.	22232.12	4.216
	$ 80 000.00	

Illustration: Effectiveness of DoS Defenses

Assessing the effectiveness of DoS defenses.

- For each stakeholder, estimate MFC gain achieved by defense,
- Match against cost to stakeholder.

Stakeholders:

- System administrator,
- Network administrator,
- End User.

Illustration: Effectiveness of DoS Defenses

Factor	System Administrator	End User
IC	Acquisition, installation cost	Stakeholder contribution
Y	Discretionary	Discretionary
d	Discretionary	Discretionary
C(y)	Operating cost, CPU overhead	Reduced service, operating risks
B(y)	MFC reduction	MFC reduction
R	Discretionary	Discretionary
ROI	Computed from above data	Computed from above data

Plan

- Shifting/Expanding the Focus of Cybersecurity
- Challenging traditional metrics
- The Mean Failure Cost
- Illustration: an E-Commerce Application
- Applications for Decision Support
- Summary and Assessment

Summary and Assessment

- Sound approach to cybersecurity: Focus on observable/ quantifiable effects.
- Proposed: Metric of cybersecurity that quantifies stakeholder value in \$/hr of operation.
- Can be used to make effective economics-based decision making.

Summary and Assessment

Extended to other dimensions of variability.

- Reliability:
  - Stakes matrix, dependability matrix, failure vector.
- Safety:
  - No difference between low stakes failures and high stakes failures: continuum of requirements, continuum of failure costs.
- Availability:
  - reduction in gain/ unit of time due to downtime.

Summary and Assessment

- MFC: Subject of joint research with ORNL.
  - ORNL stake: infrastructure protection.
- Subject of US Patent application, submitted by ORNL.
- Subject of joint research, NJIT/ORNL/Purdue/Sypris, for DOE.
- Industrial Interest from Europe.

Plan

- Shifting/Expanding the Focus of Cybersecurity
- Challenging traditional metrics
- The Mean Failure Cost
- Illustration: an E-Commerce Application
- Applications for Decision Support
- Summary and Assessment

Thank you for your attention