Systematic Information Assurance Assessment

Victoria Stavridou, Bob Riemenchneider and Steve Dawson

SRI International

System Design Laboratory

The nature of the problem

- IA is only an issue in (very) complex systems
- IA is intricately related to humans as well as systems (attackers, defenders)
- IA is an evolving aspect of a system – a moving target
- No unified theory exists
- Evidence is disparate
- Beliefs are central to assessment

Our approach

- We have to live with measures as well as less definitive judgments
  - Measures
  - Information Assurance Cases
- Objective of the program that sponsors this work: develop improved measures of more aspects of IA
  - IA Cases
  - Global IA measures
  - Critical Security Rating

IAC experience so far

- OASIS reviews
  - With thanks to
    - Bob Balzer
    - Bill Sanders
    - Crispin Cowan
    - Robbert van Rennesse
    - Feiyi Wang
    - And all our reviewees
  - Participated in setting up the process and 5 project reviews
- Ultralog survivability case
- GENOA IA
- Other projects

We asked projects to:

- Define their claims
  - Category A – complete evidence + argument in report
  - Category B – some evidence + argument in report
  - Category C – no evidence or argument yet
- State their assumptions
- Describe their evidence
- Propose an argument linking the evidence and/or assumptions to the claims
- Put everything together in a self contained IA case
- The objective was self assessment
- Reviewers acted as auditors and mentors

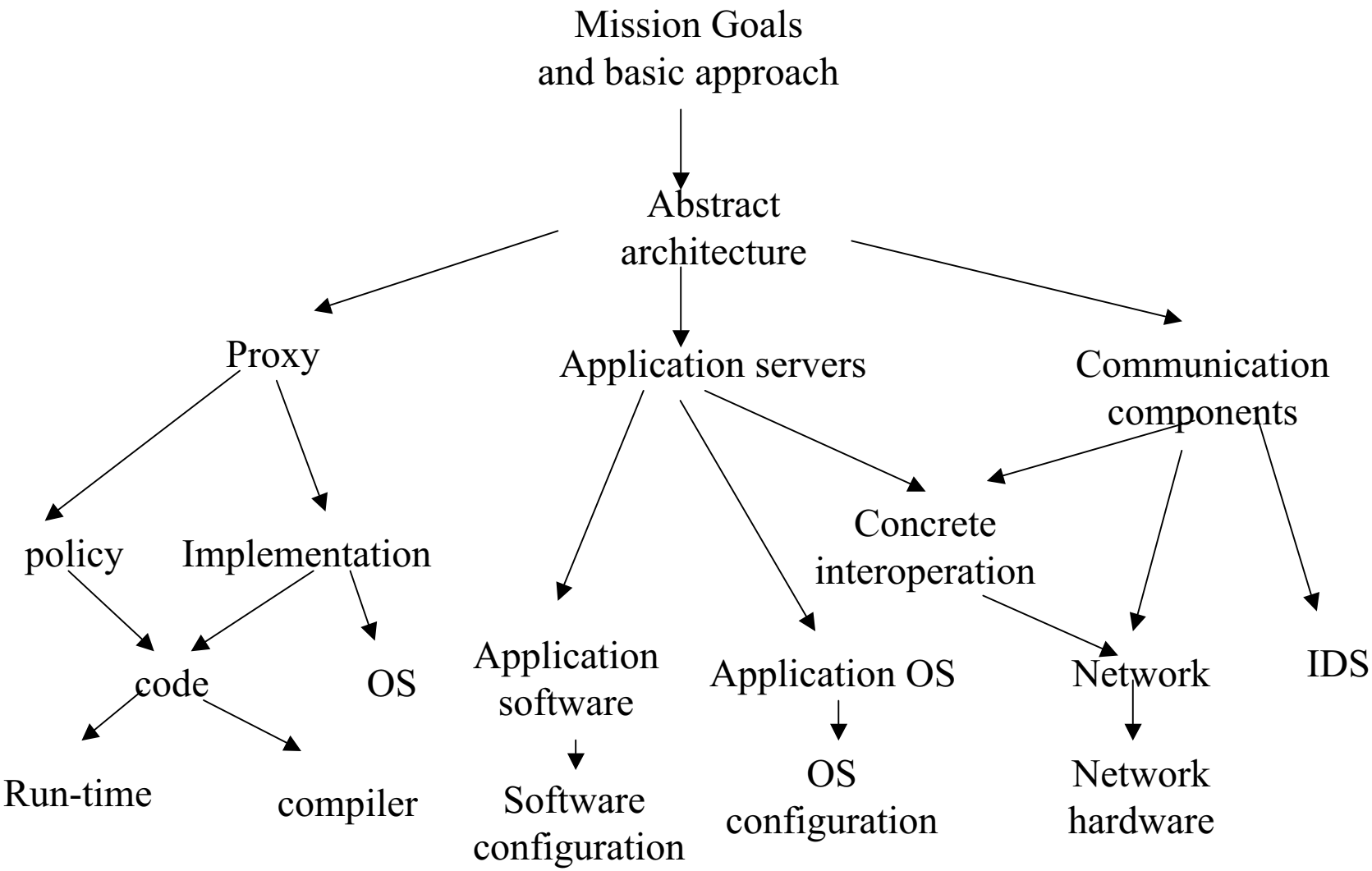
IAC guidance

- **Claims**
  - Requirements documentation
- **Sources of evidence and assumptions**
  - **Product**
    - Design documentation
    - Formal evaluation of architecture, policies, and algorithms, etc
    - Run-time monitoring
    - Checking robustness against known attack scenarios
    - Red team penetration testing
  - **Process**
    - Use of secure programming techniques and tools
    - Use of secure languages and OS
    - Use of assessment tools and methodologies
    - Use of skilled, security-aware engineers
  - **Codesign process**
    - Different sources from different parts, aspects, and/or layers of abstraction in the design and implementation
- **Arguments**
  - Structured, sound and broad to cover various levels of abstraction
  - Deterministic > probabilistic > qualitative

Observations on the OASIS review process

- Claims difficult to formulate adequately – often missing, vague or imprecise
- Claim hierarchies difficult to discern
- Unclear how the claim hierarchy supports the overall claim
- The nature of assumptions (scope vs technology) not explicitly understood and stated
- Mechanism descriptions often masquerading as claims and vice versa
- The nature of evidence unclear to PIs
- Assessing design with implementation evidence and implementations with design arguments
- Report often not self contained
- PIs do not know how to put IA cases together. OASIS has pioneered a new art

An example of claim hierarchy



Building IA Cases with SEAS

- SEAS: Structured Evidential Argumentation System
  - Web-based, collaborative system for argument construction
  - Originally developed for intelligence assessment and crisis prediction
  - Structured arguments
  - Main benefits for IA case construction:
    - Argument structuring and organization
    - Evidence recording and maintenance
    - Capability for automated combination and propagation of evidential support for argument claims

SEAS Approach

- Facilitate, not automate IA assessment
- Systematic, thorough and repeatable assessment by reminding the assessor of the full spectrum of factors to be considered
- Eases argument comprehension and communication by allowing multiple representations of evidential data
- Invites and facilitates argument comparison by framing arguments within a common structure

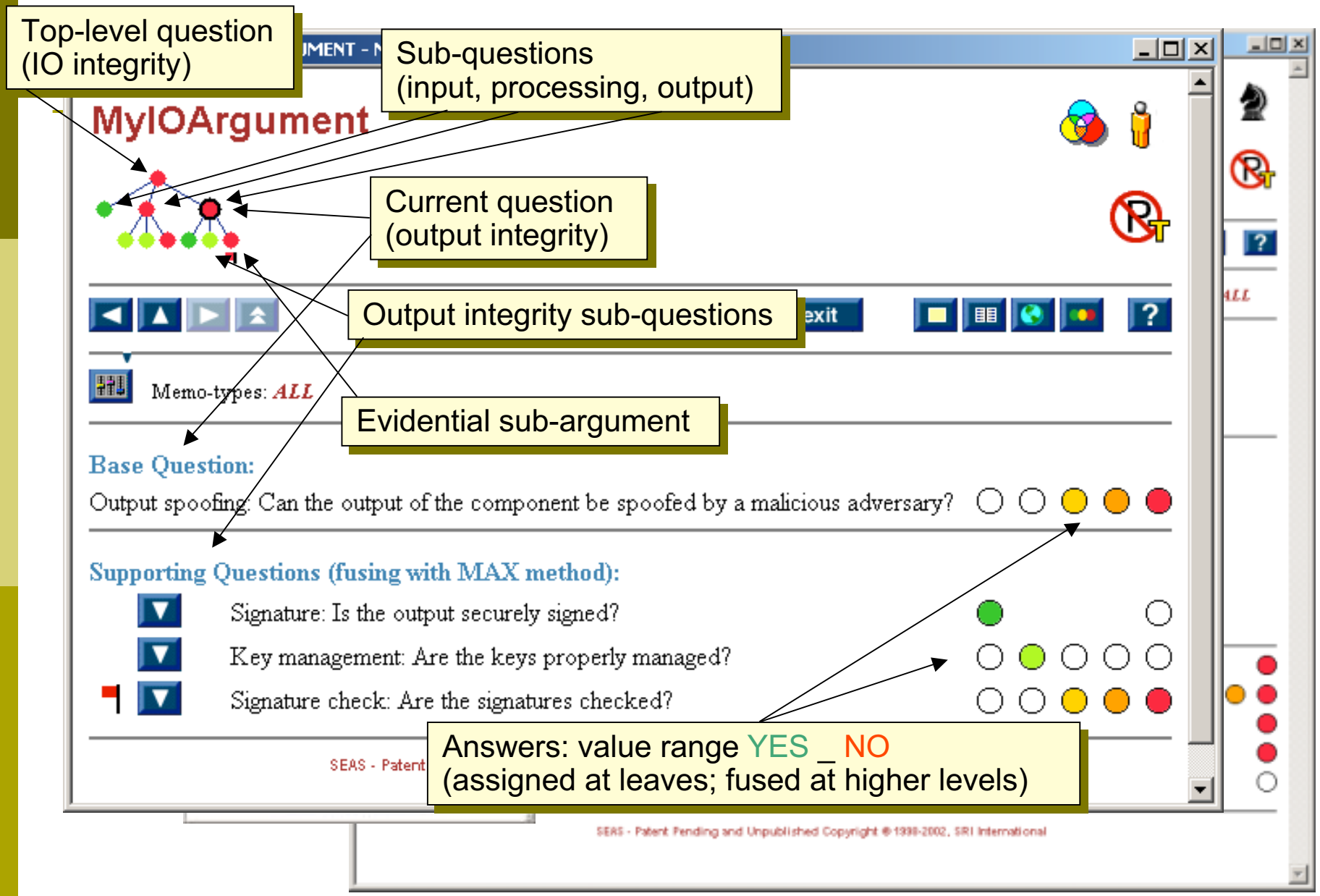
Developing an IAC

- *Templates* capture generic argument structures (claims, evidence types, and propagation rules) applicable to classes of system elements
  - Example: A template for integrity of client Information Object (IO) generation might be broken down into three subclaims addressing input, processing, and output integrity
- *Arguments* are instantiations of templates for specific components
- *Memos* allow access to corporate memory
- *Discovery tools* are recommended methods for acquiring information relevant to answering questions in a template.

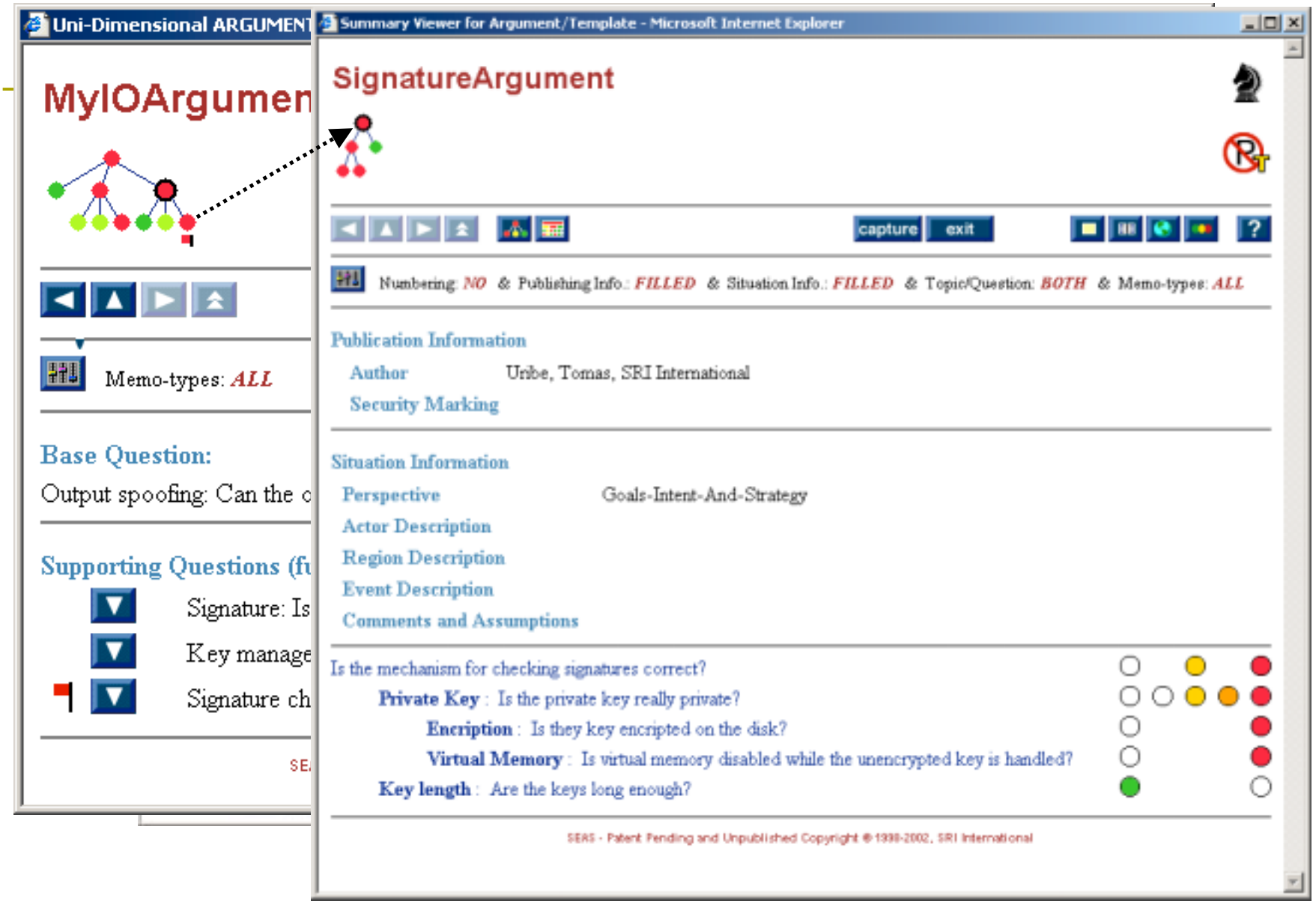
An example argument template

- Political: Is this country headed for a political crisis?
  - **Political instability:** Is political instability increasing?
    - Increasingly unstable/weak government?
    - Increasing conflict over policy/issue area?
    - Decreasing public confidence?
  - **Power struggle**
    - Factionalism?
    - Opposition challenge?
    - Subnational group influence?
  - **Government response to socio-political discord**
    - Repression of political opposition
    - Repression of social/religious groups
    - Internal security measures
  - **Structural/Institutional problems**
    - Constitutional conflict/crisis
    - Eroding legal authority/administrative functions?

Example SEAS Argument (Instantiated Template)



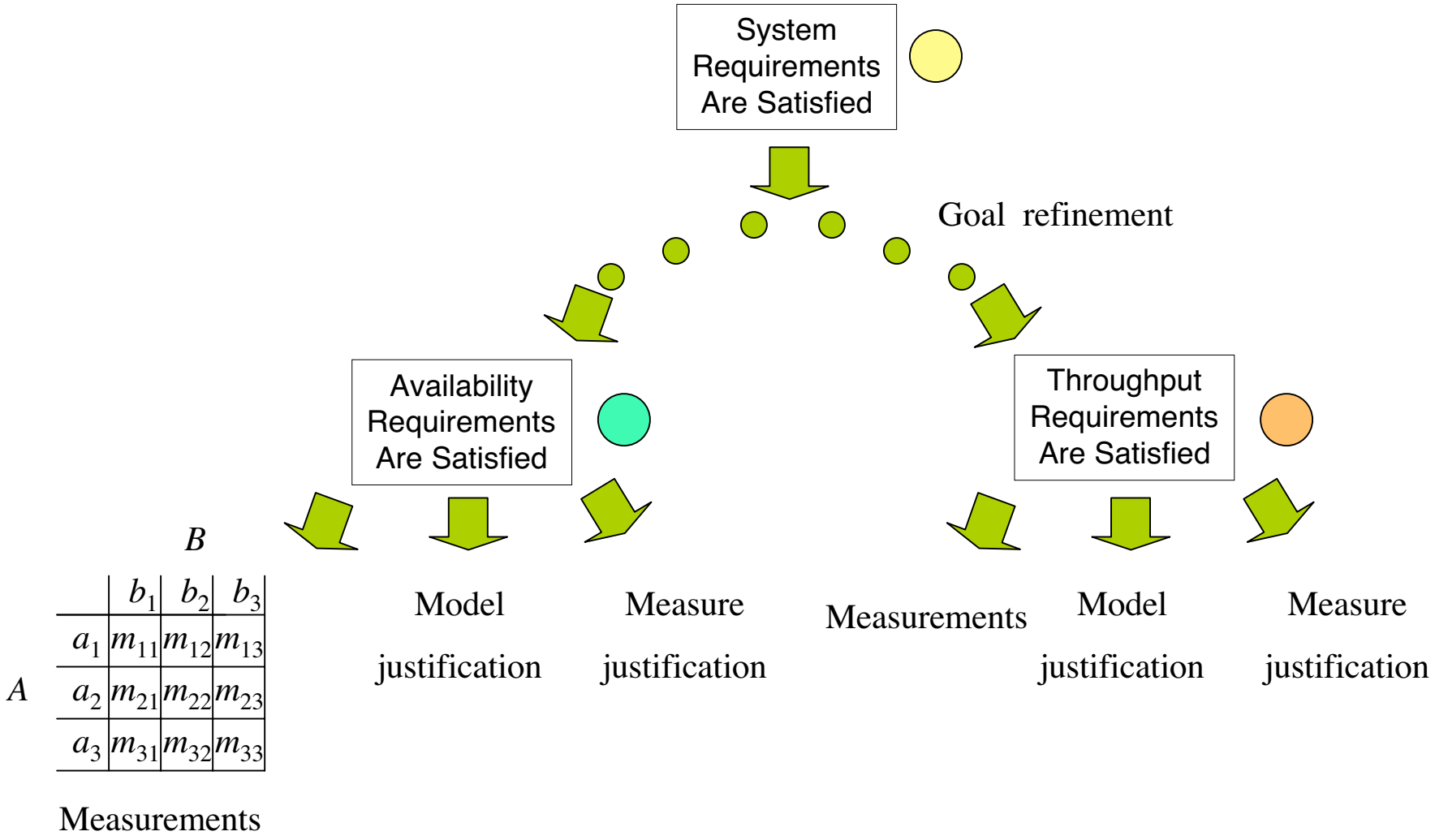
SEAS Sub-argument



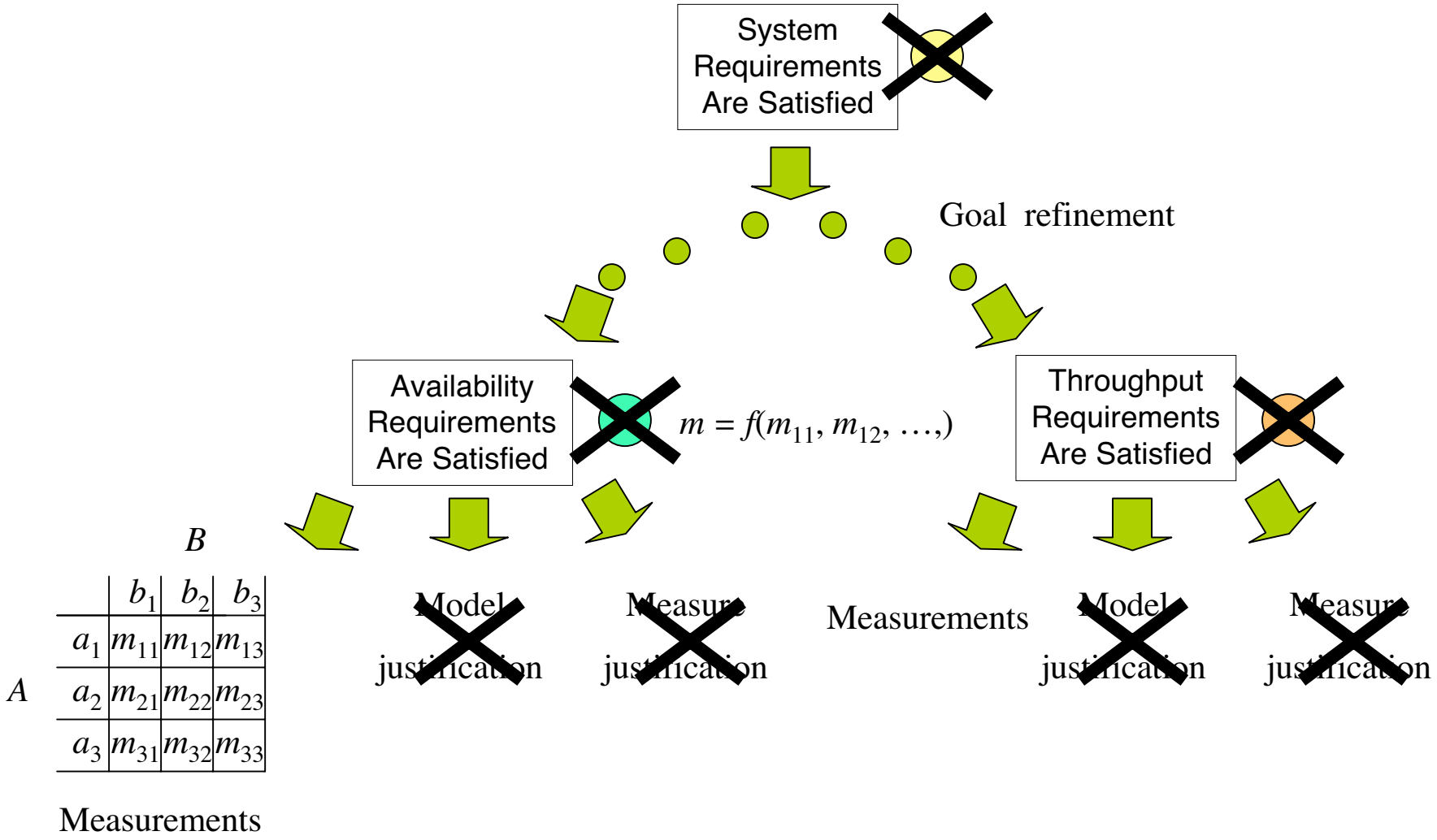
Global measure approach

- Have "local" IA measures
  - "Local" means a measure of some particular, specific aspect of IA
  - And maybe that only a subsystem of the entire system is measured
- Need to combine these many local measures into an global measure of IA
- Support tradeoffs among properties with local measures
- Extract measure(s) from the IA case

IA Cases in SEAS



Measure Propagation in SEAS



	b_1	b_2	b_3
a_1	m_{11}	m_{12}	m_{13}
a_2	m_{21}	m_{22}	m_{23}
a_3	m_{31}	m_{32}	m_{33}

Measure Combination

- Original hypothesis: linear combination of measures + a conditional operator is sufficiently flexible
  - e.g., max(m_1, m_2) = if $m_1 < m_2$ then m_2 else m_1
- Current hypothesis: Slightly more discipline is needed
  - Estimation of lower probabilities ("degrees of belief")
  - Propagation a la Dempster-Shafer (using GISTER)

Seedling experiment

- Extend SEAS to support use of Dempster-Shafer
- Pare down existing IA case to (mostly) probabilistic local measures
- Define candidate propagation functions (= global measures) as proof-of-concept
- Evaluate results

Status

- SEAS inference engine extensions complete
- Working on extensions to SEAS interface
- IA case for experiment selected
- Work on paring and other adjustments (e.g., estimates of lower probabilities from probabilities and resiliency) is underway

CSR motivation

- Develop an assurance measure that is:
  - easy to calculate;
  - obviously relevant to a given system; and,
  - understandable to a broad audience
- Measure should promote desirable behaviors.
  - Measure improves as real security improves.
  - Measure improves most when the greatest risk is mitigated.
- The result is the Critical Security Rating (CSR).

Technical Approach

- Process:
  1. Identify the *system of interest*
  2. Identify the critical security *risks*
     - *Assign priorities to those risks, P_r*
  3. Identify the potential adversaries
     - *Assign priorities to those adversaries, P_a*
  4. Determine if a given risk is currently mitigated for a particular adversary.
  5. Determine the sum of products, R = _(P_r*P_a) for all risk/adversary pairs that are mitigated in a system.

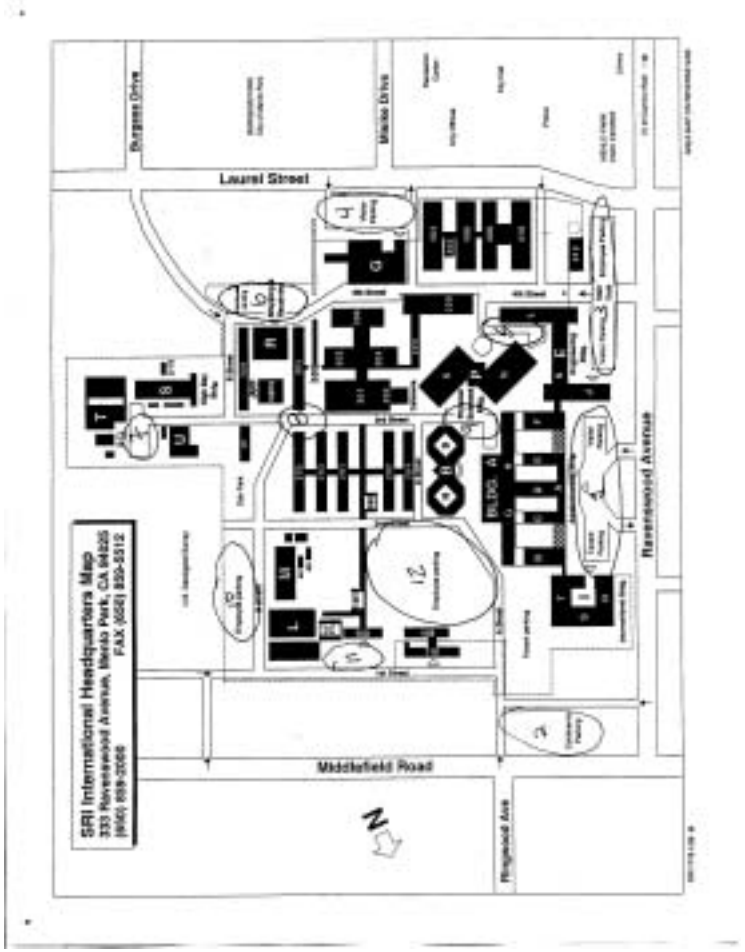
Expected results

- R is a number between 0 and 1 that indicates the degree to which the most important risks are mitigated.
- Obtained from a matrix of risk/adversary pairs that structure the value of mitigating a given risk.

	Adversary A	Adversary B	Adversary C	Adversary D	Adversary E
Risk 1	✓				✓
Risk 2		✓	✓	✓	✓
Risk 3					✓

Field Trial

- Customer
  - SRI Corporate Information Security Manager
- System of Interest
  - Wireless LANs on SRI's Menlo Park campus



Driving Forces

- Risks:
  - Sniffing network traffic
  - Taking control of access points
  - Unauthorized association with an access point
  - Discovery of WEP keys
  - Non-attribution of a discovered attacker
- Adversaries:
  - Wardrivers
  - Internal Staff
  - SRI visitors and onsite conference attendees
  - Nearby residents
  - Ex-employees
  - Foreign intelligence agencies
  - Competitor

Critical Success Factors

- The system must protect broadcast data from eavesdroppers
- The system must prevent an unauthorized host from communicating with authorized wireless hosts or the access points
- The system must ensure that only authorized hosts may become nodes on the wireless network
- The system must prevent an unauthorized principal from modifying the network configuration in order to gain access

Threats to success factors

- [0.3] Sniffing network traffic
- [0.2] Taking control of access points
- [0.2] Unauthorized association with an access point
- [0.15] Discovery of WEP keys
- [0.10] Non-attribution of a discovered attacker
- [0.05] DOS on wireless infrastructure

Basic Calculation

		Wardrivers			Internal Staff			SRI Visitors			Nearby Residents			Ex-employees			Foreign Intelligence			Competitor		
		0.24			0.19			0.17			0.15			0.1			0.1			0.05		
Criteria		Value	P/F	Score	Value	P/F	Score	Value	P/F	Score	Value	P/F	Score	Value	P/F	Score	Value	P/F	Score	Value	P/F	Score
Flag 1	0.3	0.07	0	0	0.057	0	0	0.051	0	0	0.045	1	0.045	0.03	0	0	0.03	0	0	0.015	0	0
Flag 2	0.2	0.05	1	0.05	0.038	1	0.04	0.034	1	0.034	0.03	1	0.03	0.02	1	0.02	0.02	0	0	0.01	1	0.01
Flag 3	0.2	0.05	0	0	0.038	0	0	0.034	0	0	0.03	0	0	0.02	0	0	0.02	0	0	0.01	0	0
Flag 4	0.15	0.04	1	0.04	0.029	0	0	0.026	1	0.026	0.023	0	0	0.02	0	0	0.02	0	0	0.0075	1	0.0075
Flag 5	0.1	0.02	0	0	0.019	0	0	0.017	1	0.017	0.015	0	0	0.01	0	0	0.01	0	0	0.005	0	0
Flag 6	0.05	0.01	1	0.01	0.01	0	0	0.009	1	0.009	0.008	1	0.008	0.01	0	0	0.01	0	0	0.0025	0	0
Score Totals				0.1			0.04			0.085			0.083			0.02			0			0.0175
																				Total CSR:		**0.339**