Probabilistic Modeling of Insider Threat Detection Systems

21 August 2017

Dr. Brian Ruttenberg, David Blumstein, Michael Howard, Fred Reed, Dr. Jeff Druce, *Charles River Analytics*

Leslie Wilfong, Crystal Lister, *Cognitio Corp*

Dan Scofield, *Assured Information Security*

Steve Gaskin, Meaghan Foley, *Applied Marketing Science*

Outline

- Introduction to the Problem
- Quick Overview of Insider Threat Detection Systems (ITDS)
- Graphical Modeling of ITDSs
- Example Uses and Experiments

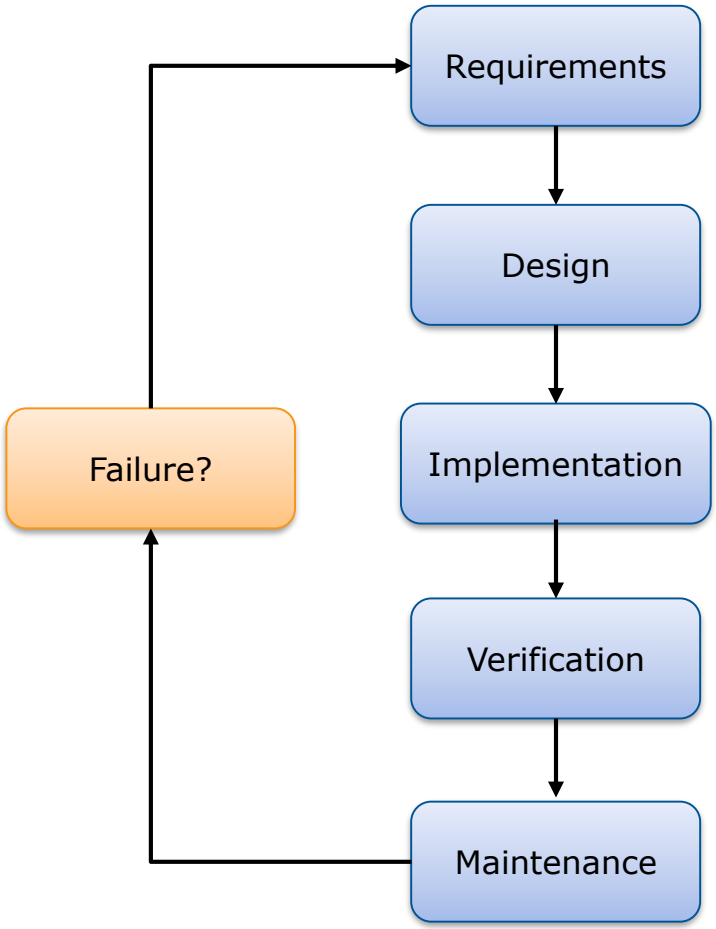
Problem Setting

- Insider threats are a major source of concern to many large organizations
  - E.g., intelligence community, Department of Defense, corporations
- Automated inference methods are the only feasible means to locate threats in these large organizations

- But these methods have many interacting parts:
  - The organization and its processes
  - People in the organization
  - Data used to support inference
  - Indicators of possible threats
  - Automated detectors of those indicators
  - Down-select algorithms to identify possible inside threats

Developing Inference Enterprises

- Implementing an Insider Threat Detection System (ITDS) is an expensive and complex procedure
  - Large number of interacting human and automated components
  - Requires lots of engineering and expensive development of IE software and the supporting infrastructure
- Highly desirable to accurately forecast IE performance *before* it is placed into operation
  - More effective threat detection
  - Understanding of weak/vulnerable points
  - Enormous time and cost savings

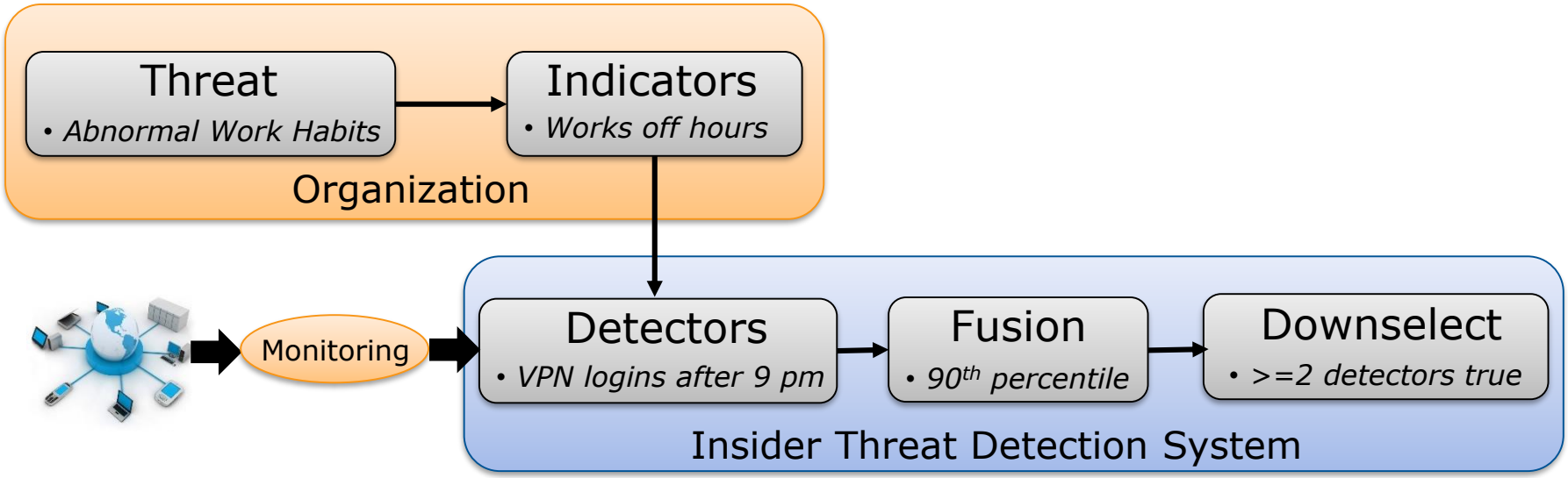


ITDS Modeling

- Modeling the performance of an ITDS *before* deployment is not small task itself!

- Many challenges include:
  - Dynamics – models must capture how organizations change over time
  - Uncertainty – raw data used for modeling might be noisy or redacted, and some parameters may be unknown
  - Complexity of ITDS components – models must capture the complex operation of detection algorithms
  - Scalability – ITDS can be large and involve many interacting components

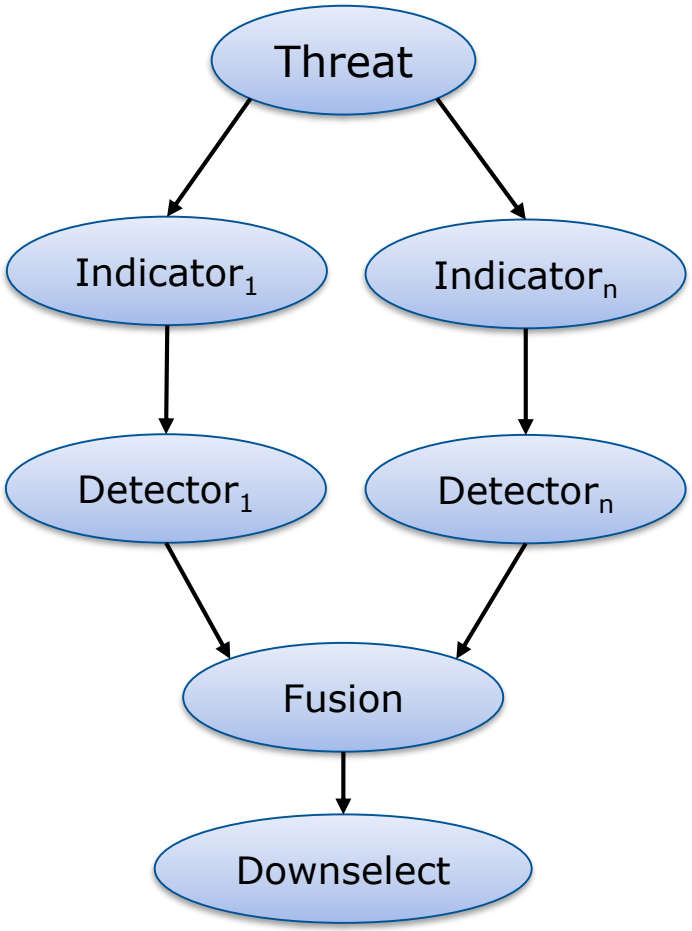
Formulation of an ITDS



- An organization contains threats and indicators of those threats
- An ITDS monitors the network infrastructure to detect for realizations of the indicators
- Data from several detectors is fused together and suspicious users are downselected for review

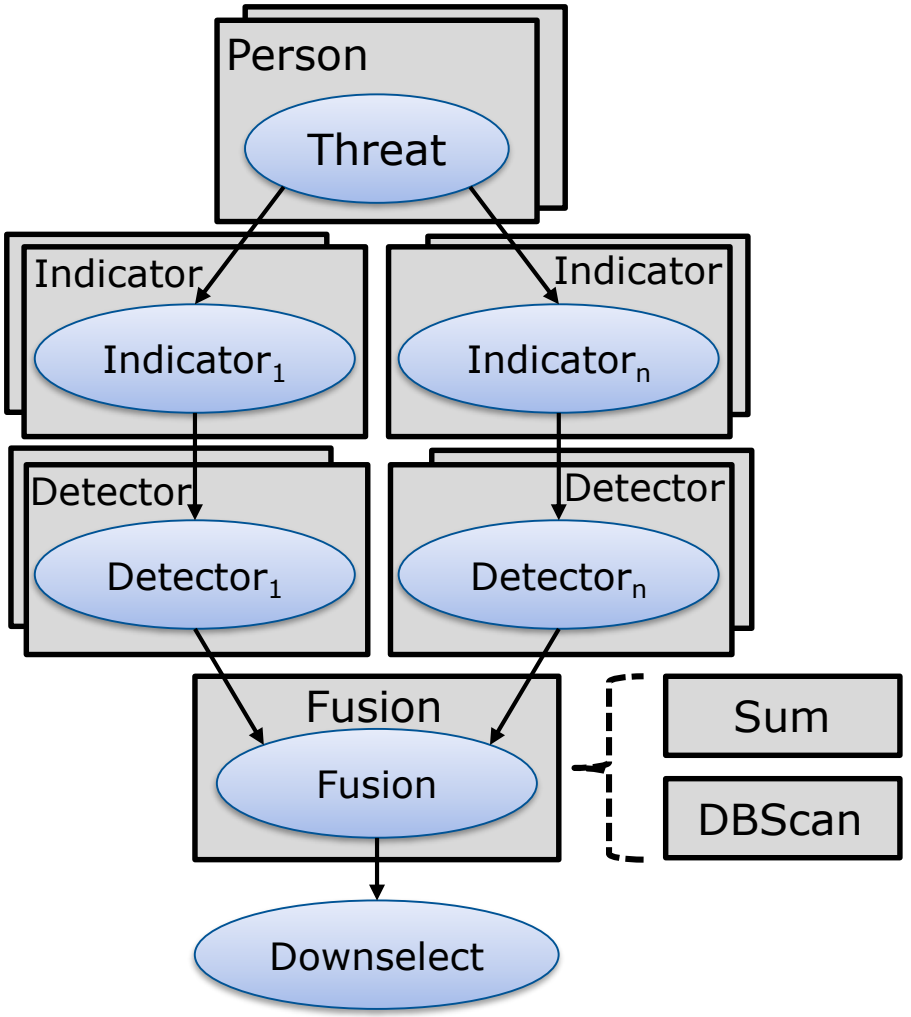
A Bayesian Network (BN) Representation of ITDS

- Convert each component of ITDS into node in BN that represents uncertainty of operation given parents
  - *Threat*: Probability of a person being a threat in the organization
  - *Indicator*: Probability of person having behavior given threat
  - *Detector*: Probability of observing the behavior in the organization
- Can augment this BN with organizational hyperpriors
  - Hyperprior over threat given different types of organizations



Implementation of ITDS Model

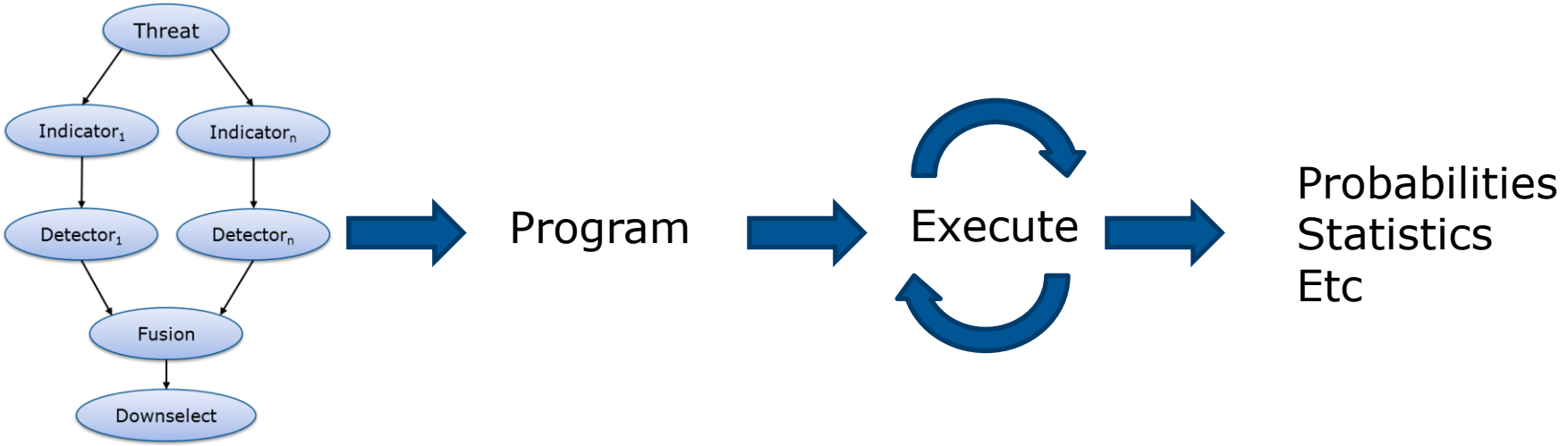
- For implementation purposes, more convenient to express model as a *probabilistic relational model* (PRM)
  - Essentially an object-oriented BN
- Easily represent uncertainty over different types of people, detectors, etc
- Can easily model groups of people at same time
- Can represent structural uncertainty



Building an ITDS Model

- Build ITDS models using *probabilistic programming* (PP)
  - Well suited to building PRMs and generalized inference on ITDS models

- PP uses programming language concepts to encode the definition of a model as a program
  - Use power of programming languages to build rich and complex decision models
  - Reasoning on the model is performed by "tracking" random executions of the program



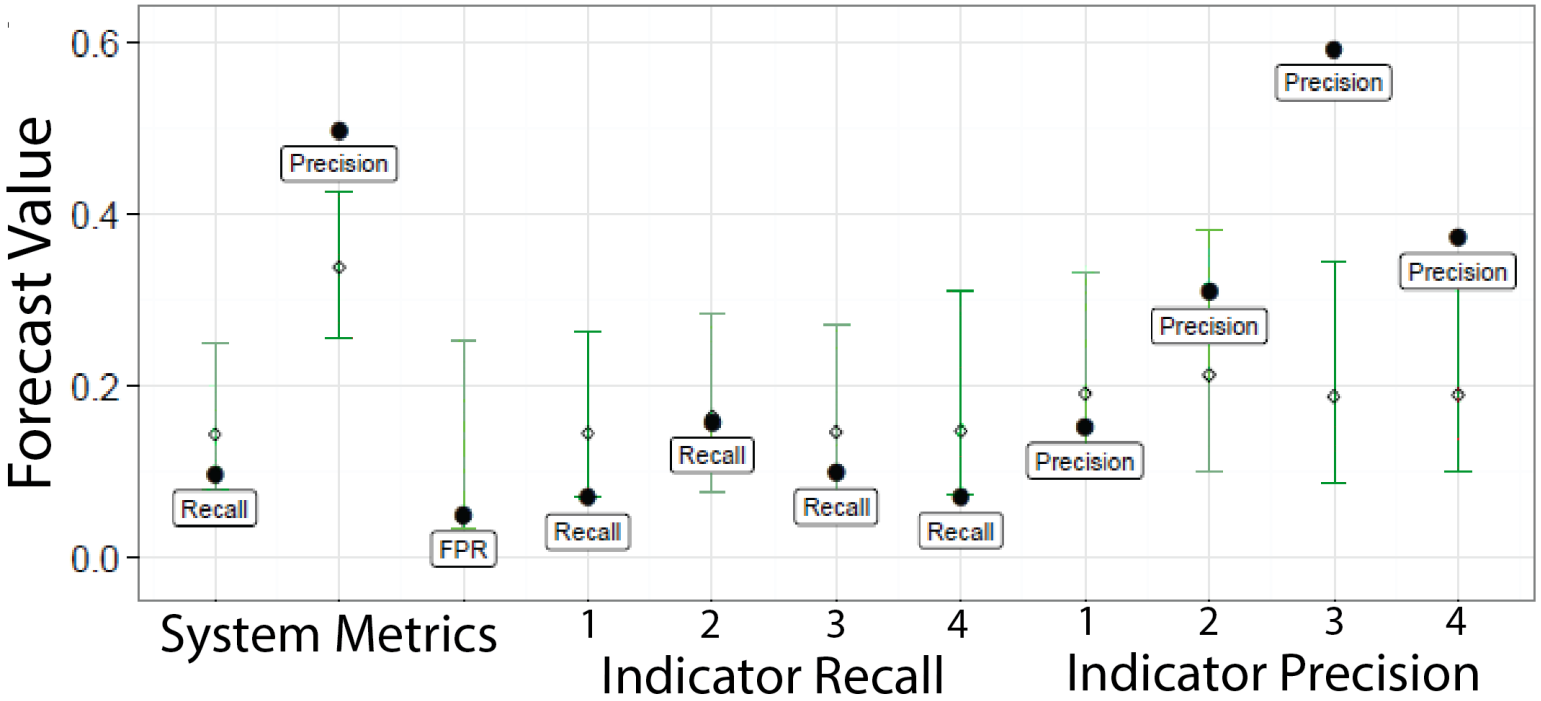
Using an ITDS Model for Analysis

- Once model is defined, built, and parameterized (with any available data), use PP inference to perform analysis

- Key advantage of PP: Same model used for many different types of inference
  - Performance estimates (marginal/joint inference)
  - Sensitivity analysis
  - Optimization (marginal-MAP, decision-making)

- Use performance metrics to drive this analysis
  - Precision, recall, false positive rate

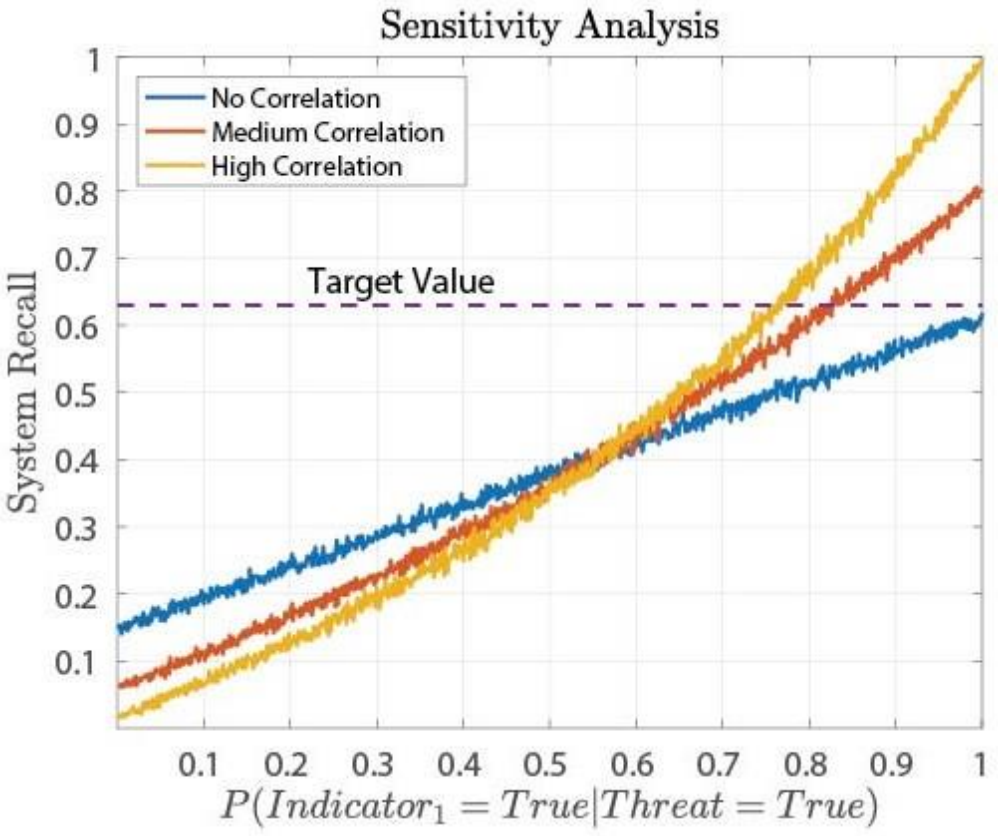
Performance Analysis



- Use marginal inference to compute distribution over metrics
- Show 60% confidence bounds on system performance
- Ground truth estimates provides by third-party evaluator

Sensitivity Analysis (SA)

- Sensitivity analysis can be used to understand implications of incorrect assumptions or changes over time
- Vary conditional probability of indicator|threat for 3 correlation models between indicators
  - Highly sensitive in this parameter
- Current research focuses on automatic differentiation methods of SA



Optimization

- Can also use model to improve design of ITDS
- Use probabilistic optimization to infer new parameter values or algorithms that maximize performance
  - Cast as a decision-making making problem to maximize utility (sum of precision and recall) by changing parameters of ITDS
- Optimization of existing ITDS (provided by third-party) nearly twice as good as the original

Decision	Component	Original Threshold	New Threshold	Utility
1	Detector A	2000	2100	1.04
2	Detector B	3	1	1.12
3	Detector C	7	8	1.14
4	Detector D	3	7	1.11
5	Detector E	1	2	1.12
6	Downselect	2	3	1.89

Conclusion

- Building an ITDS graphical model is an effective way for engineers and analysts to understand the impact of ITDSs in an organization
- Our inference capabilities provide many of the tools needed to perform this detailed and complex analysis
- Many additional issues and future work around this concept:
  - Using organizational, survey, and open-source data to parameterize models and transfer knowledge from one organization to another
  - More powerful sensitivity analysis using automatic differentiation
  - Investigating the best ITDS/model topology for different tasks

Acknowledgements

- This work was supported by IARPA contract 2016-6031100002. The views expressed are those of the authors and do not reflect the official policy or position of the U.S. Government.

Questions?

Points of Contact

Dr. Brian Ruttenberg
Senior Scientist
Charles River Analytics
617.491.3474 Ext. 730
bruttenberg@cra.com

charles river analytics

Charles River Analytics Inc.
625 Mount Auburn St.
Cambridge, MA 02138
p: 617.491.3474
f: 617.868.0780
www.cra.com