A Bottom-up Approach to Applying Graphical Models in Security Analysis

Xinming (Simon) Ou
Associate Professor
Computer Science and Engineering
University of South Florida

GraMSec 2016
Lisbon, Portugal, June 27, 2016

Graphical Model

- Classical definition:
  - Probabilistic model where a graph expresses the conditional dependence between random variables
  - e.g., Bayesian Network, Markov Network

- In this talk:
  - A graph where probabilistic reasoning is carried out to solve certain security analysis problems

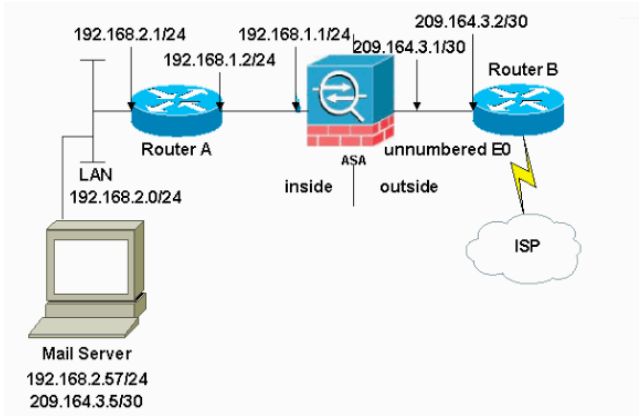
Security Analysis

IDS alerts

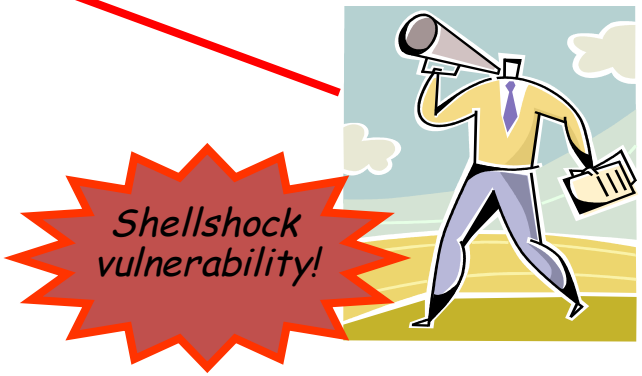
Users and data assets

Automation

Network configuration,
Server logs, etc.

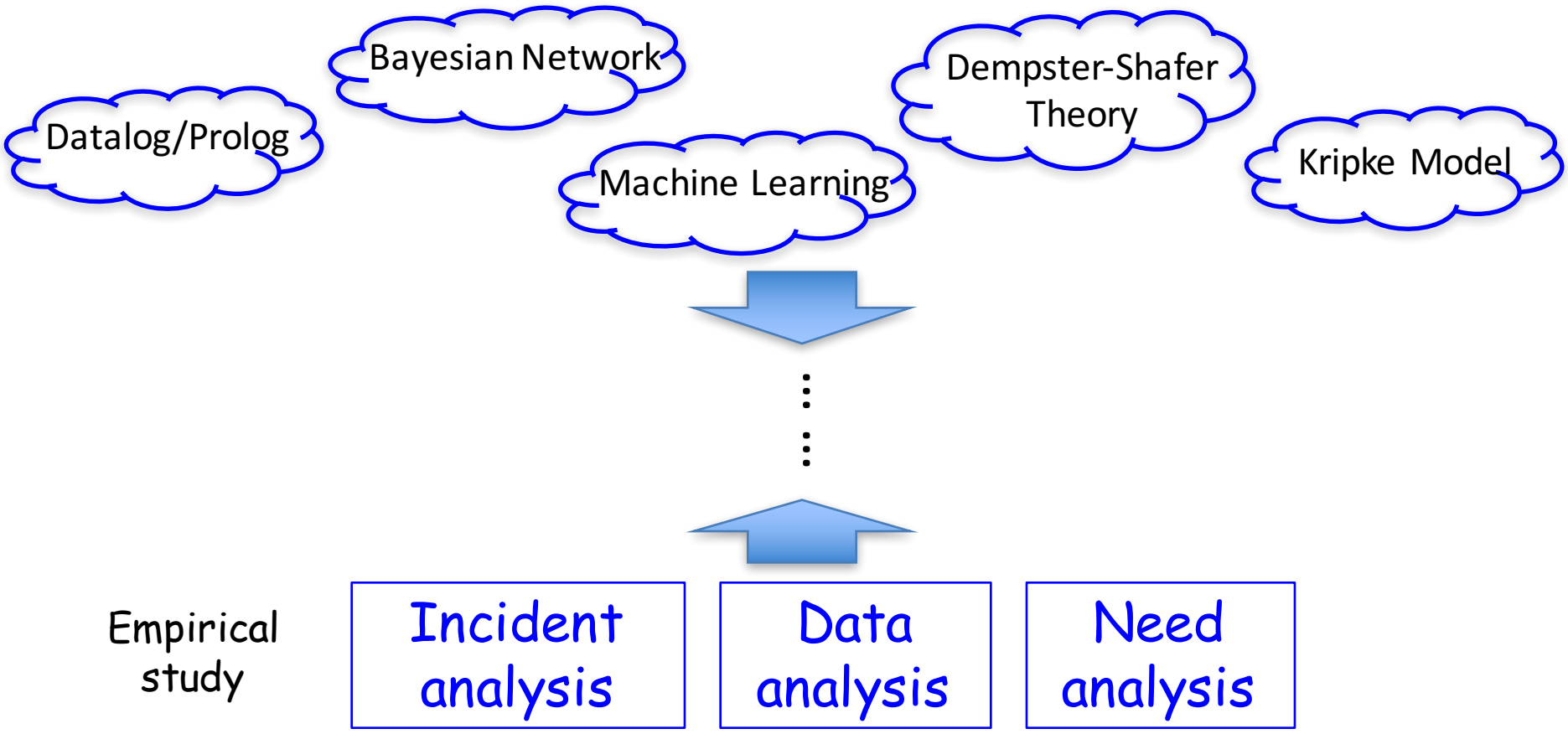


Host scan reports



Security advisories

A Bottom-up Approach



A day in the life of a real Security Analyst (SA)

Abnormally high traffic

Some servers communicating with known BotNet IPs

Seemingly malicious code modules

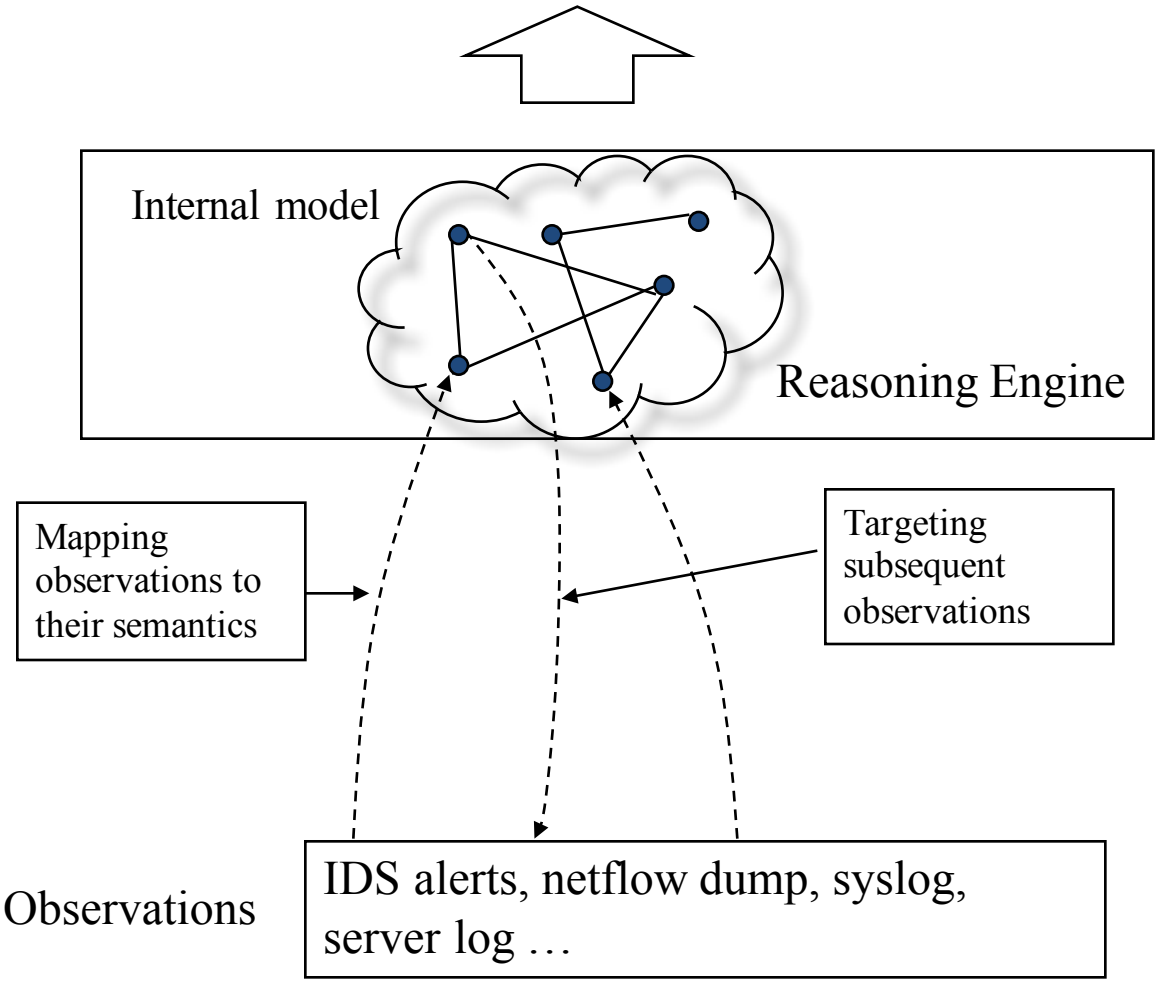
Found IRC connections with other servers

Network Monitoring Tools

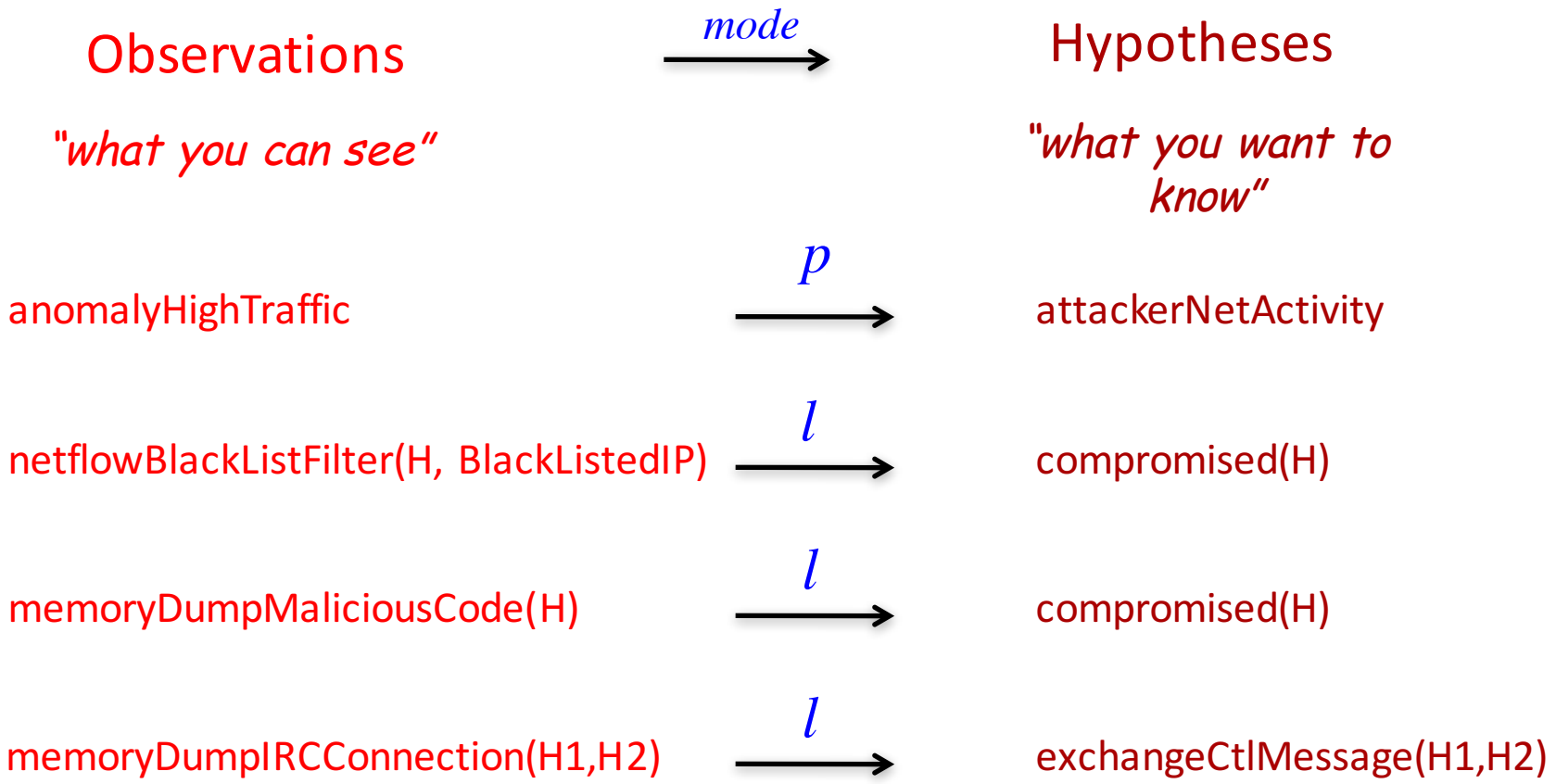
netflow dump

memory dump

These servers are certainly compromised!

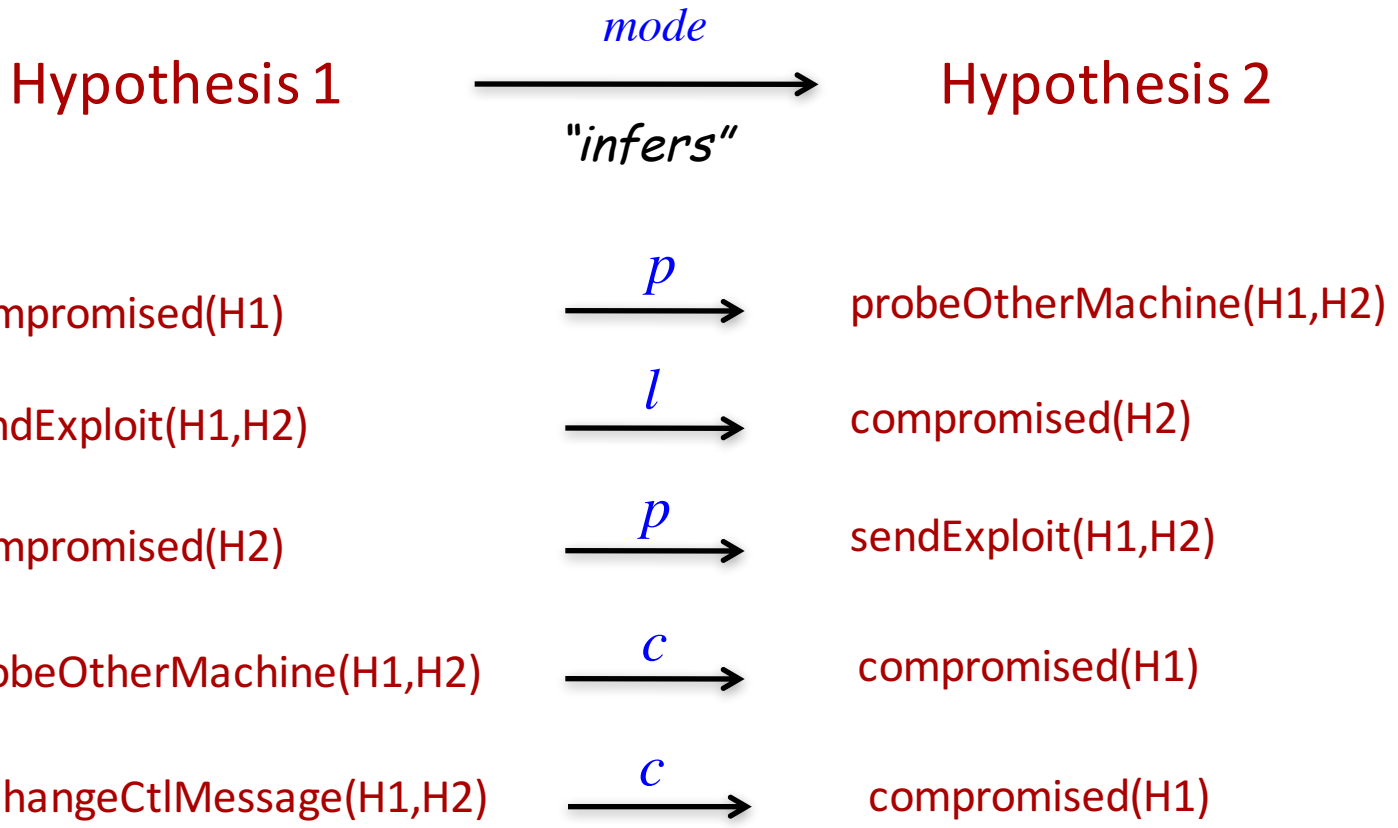

High-confidence Conclusions with Evidence
Internal model
Reasoning Engine
Mapping observations to their semantics
Targeting subsequent observations
Observations
IDS alerts, netflow dump, syslog, server log …

Simulated Mental Model – Observation Correspondence (OC)



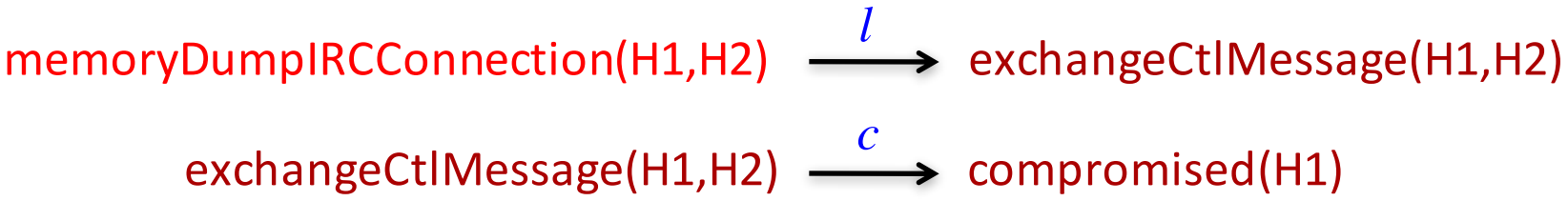
mode p: possible l: likely c: certain

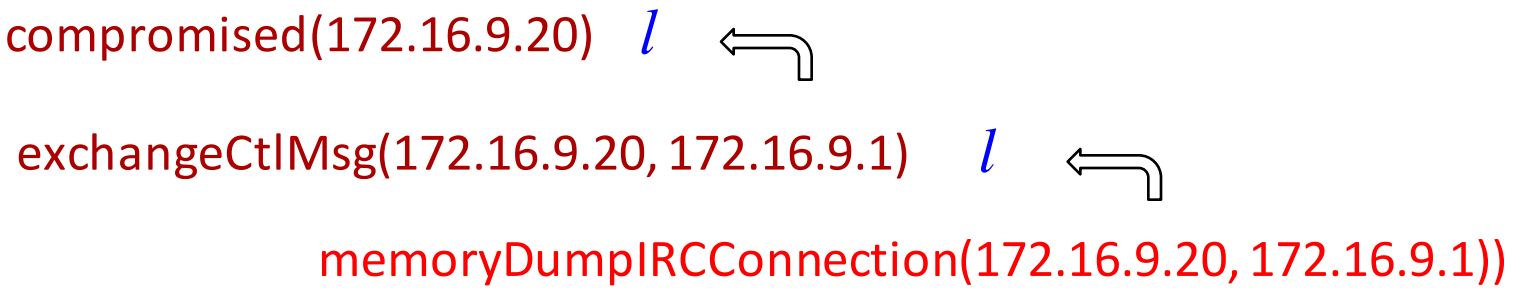
Simulated Mental Model – Internal Model (IM)



mode p: possible l: likely c: certain

Simulate Human Reasoning





Theory for Reasoning

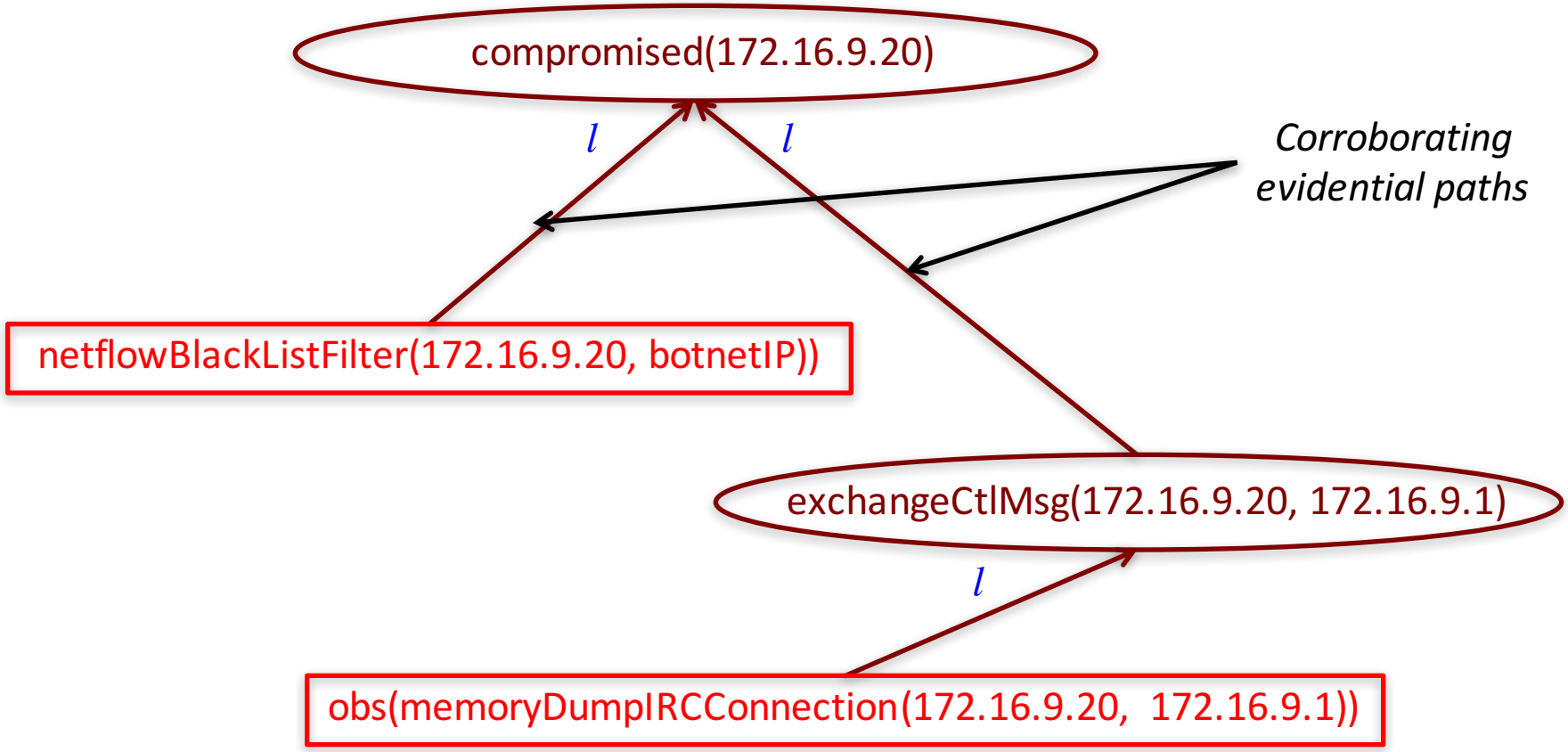
- Logical Model
  - Reasoning model (OC and IM) can be expressed in Datalog.
  - Evaluate the Datalog program on input observations.
  - Carried out in the deductive database XSB.
  - Exhaustively find *all* proofs of a true query, leading to a *proof graph*.

- Complexity is $O(N^2)$
  - N is the number of different IP addresses appearing in the input.

The Graphical Model

Can we formulate a mathematical theory to explain the strengthening process that happens in an analyst's mind?

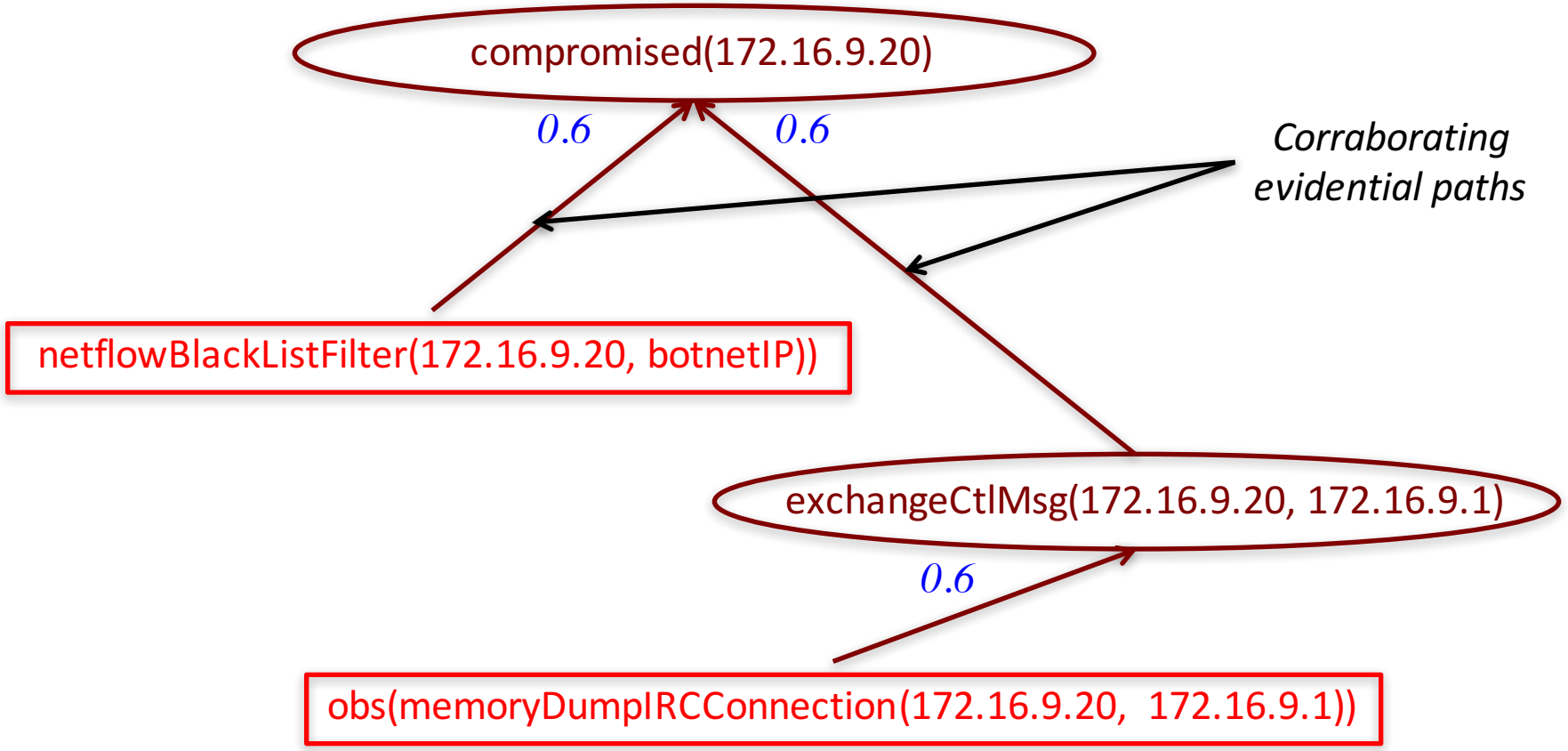
$$strengthen(l, l) = c$$



The Graphical Model

Can we formulate a mathematical theory to explain the strengthening process that happens in an analyst's mind?

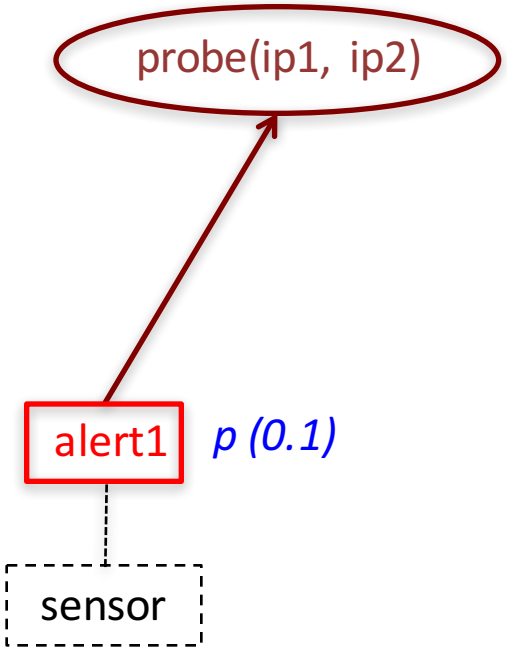
$$combine(0.6, 0.6) = 0.84$$



Our Choice of Theory

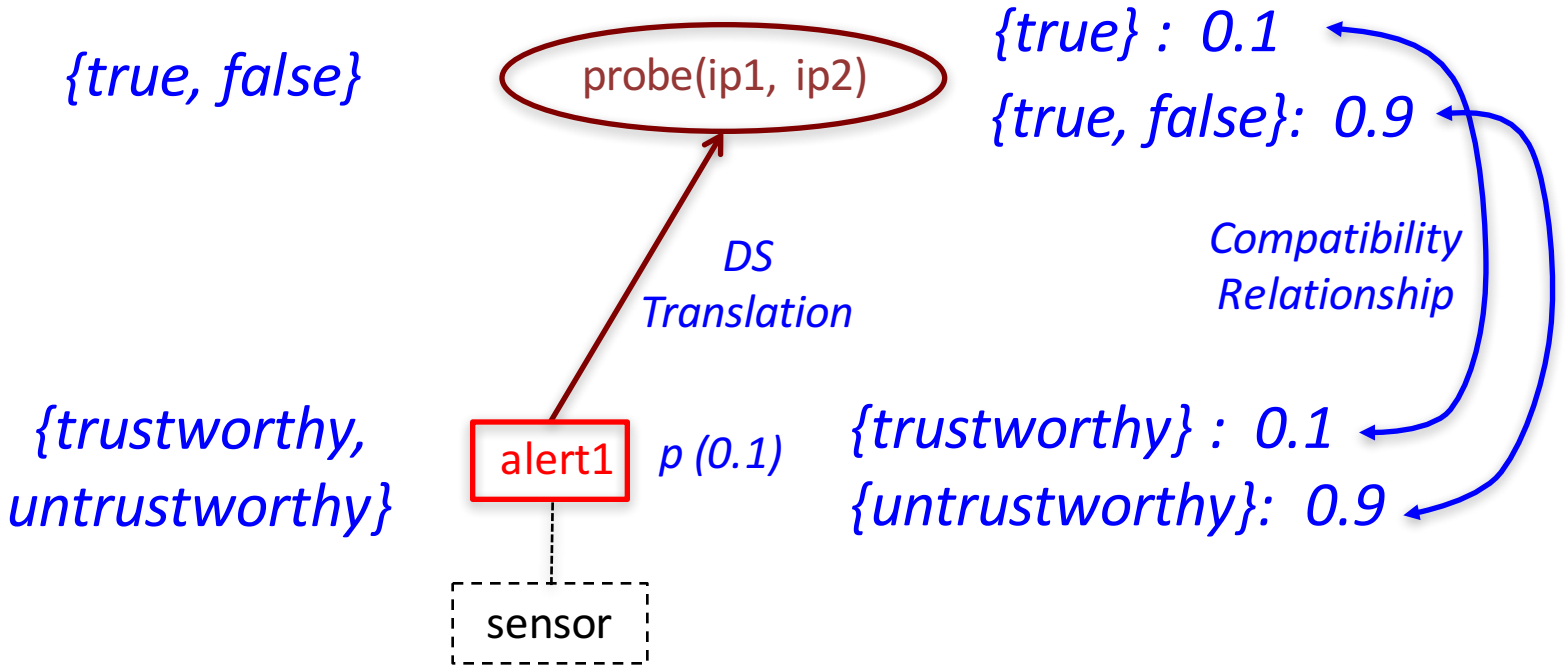
- Need to find a theory that is aligned well with the human analyst's mental model
- Dempster-Shafer (DS) theory
  - The notion of "belief" corresponds naturally to what an analyst wants to capture
  - Allowing quantitative weights assigned to sets of hypotheses, e.g. {attack, no_attack}
  - Combining independent evidence from multiple sources

Qulitative => Quantitative



Sensor quality	Uncertainty Modes		Belief value
Low	*Possible*	*p*	*0.1*
Moderate	*Likely*	*1*	*0.6*
High	*Certain*	*c*	*1*

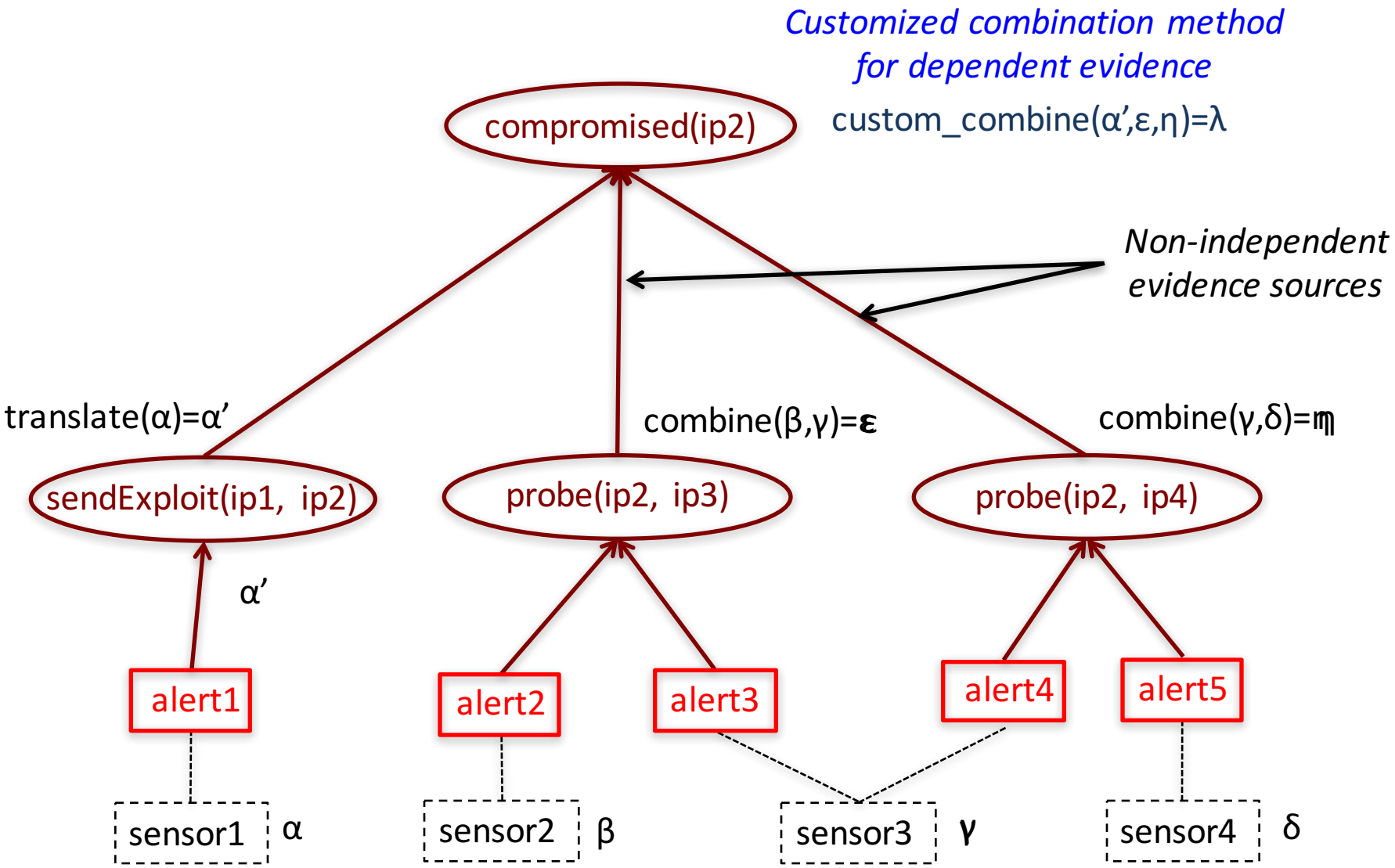
DS Reasoning Set up



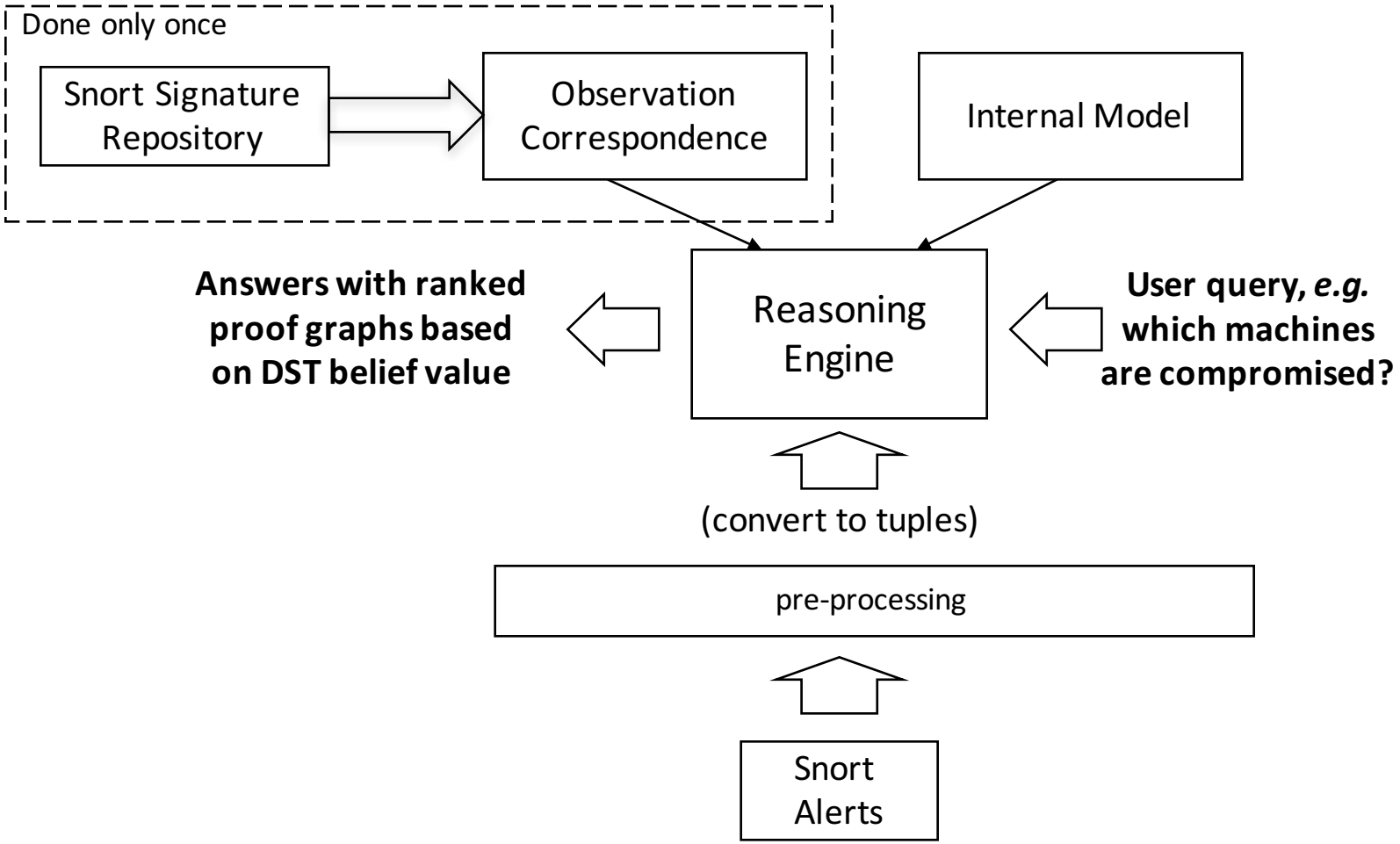
Frames of Discernment (FoD)

Basic Probability Assignment (bpa)

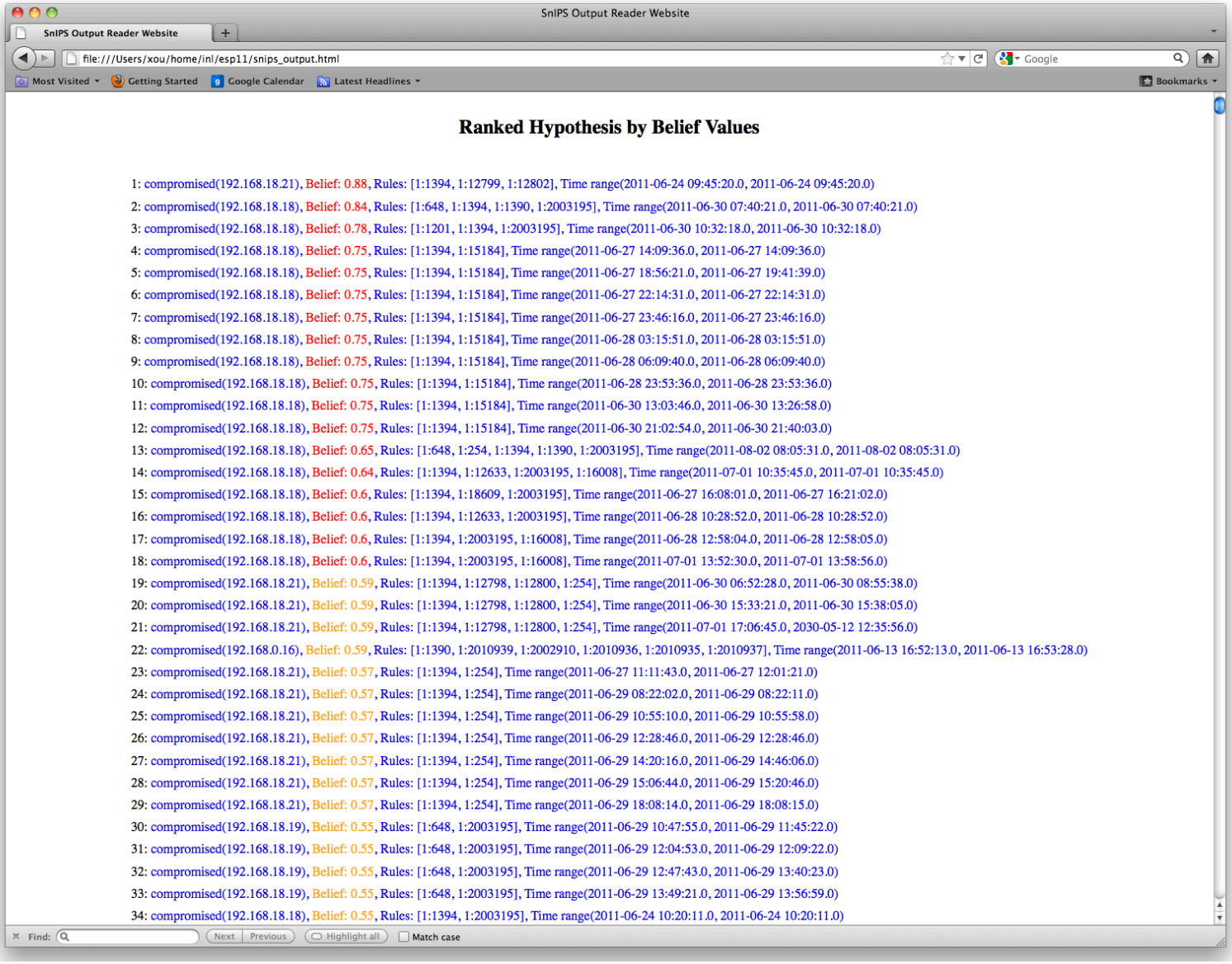
DS Combination



Prototype: SnIPS



How do we know it works?



Ranked Hypothesis by Belief Values

1: compromised(192.168.18.21), Belief: 0.88, Rules: [1:1394, 1:12799, 1:12802], Time range(2011-06-24 09:45:20.0, 2011-06-24 09:45:20.0)
2: compromised(192.168.18.18), Belief: 0.84, Rules: [1:648, 1:1394, 1:1390, 1:2003195], Time range(2011-06-30 07:40:21.0, 2011-06-30 07:40:21.0)
3: compromised(192.168.18.18), Belief: 0.78, Rules: [1:1201, 1:1394, 1:2003195], Time range(2011-06-30 10:32:18.0, 2011-06-30 10:32:18.0)
4: compromised(192.168.18.18), Belief: 0.75, Rules: [1:1394, 1:15184], Time range(2011-06-27 14:09:36.0, 2011-06-27 14:09:36.0)
5: compromised(192.168.18.18), Belief: 0.75, Rules: [1:1394, 1:15184], Time range(2011-06-27 18:56:21.0, 2011-06-27 19:41:39.0)
6: compromised(192.168.18.18), Belief: 0.75, Rules: [1:1394, 1:15184], Time range(2011-06-27 22:14:31.0, 2011-06-27 22:14:31.0)
7: compromised(192.168.18.18), Belief: 0.75, Rules: [1:1394, 1:15184], Time range(2011-06-27 23:46:16.0, 2011-06-27 23:46:16.0)
8: compromised(192.168.18.18), Belief: 0.75, Rules: [1:1394, 1:15184], Time range(2011-06-28 03:15:51.0, 2011-06-28 03:15:51.0)
9: compromised(192.168.18.18), Belief: 0.75, Rules: [1:1394, 1:15184], Time range(2011-06-28 06:09:40.0, 2011-06-28 06:09:40.0)
10: compromised(192.168.18.18), Belief: 0.75, Rules: [1:1394, 1:15184], Time range(2011-06-28 23:53:36.0, 2011-06-28 23:53:36.0)
11: compromised(192.168.18.18), Belief: 0.75, Rules: [1:1394, 1:15184], Time range(2011-06-30 13:03:46.0, 2011-06-30 13:26:58.0)
12: compromised(192.168.18.18), Belief: 0.75, Rules: [1:1394, 1:15184], Time range(2011-06-30 21:02:54.0, 2011-06-30 21:40:03.0)
13: compromised(192.168.18.18), Belief: 0.65, Rules: [1:648, 1:254, 1:1394, 1:1390, 1:2003195], Time range(2011-08-02 08:05:31.0, 2011-08-02 08:05:31.0)
14: compromised(192.168.18.18), Belief: 0.64, Rules: [1:1394, 1:12633, 1:2003195, 1:16008], Time range(2011-07-01 10:35:45.0, 2011-07-01 10:35:45.0)
15: compromised(192.168.18.18), Belief: 0.6, Rules: [1:1394, 1:18609, 1:2003195], Time range(2011-06-27 16:08:01.0, 2011-06-27 16:21:02.0)
16: compromised(192.168.18.18), Belief: 0.6, Rules: [1:1394, 1:12633, 1:2003195], Time range(2011-06-28 10:28:52.0, 2011-06-28 10:28:52.0)
17: compromised(192.168.18.18), Belief: 0.6, Rules: [1:1394, 1:2003195, 1:16008], Time range(2011-06-28 12:58:04.0, 2011-06-28 12:58:05.0)
18: compromised(192.168.18.18), Belief: 0.6, Rules: [1:1394, 1:2003195, 1:16008], Time range(2011-07-01 13:52:30.0, 2011-07-01 13:58:56.0)
19: compromised(192.168.18.21), Belief: 0.59, Rules: [1:1394, 1:12798, 1:12800, 1:254], Time range(2011-06-30 06:52:28.0, 2011-06-30 08:55:38.0)
20: compromised(192.168.18.21), Belief: 0.59, Rules: [1:1394, 1:12798, 1:12800, 1:254], Time range(2011-06-30 15:33:21.0, 2011-06-30 15:38:05.0)
21: compromised(192.168.18.21), Belief: 0.59, Rules: [1:1394, 1:12798, 1:12800, 1:254], Time range(2011-07-01 17:06:45.0, 2030-05-12 12:35:56.0)
22: compromised(192.168.0.16), Belief: 0.59, Rules: [1:1390, 1:2010939, 1:2002910, 1:2010936, 1:2010935, 1:2010937], Time range(2011-06-13 16:52:13.0, 2011-06-13 16:53:28.0)
23: compromised(192.168.18.21), Belief: 0.57, Rules: [1:1394, 1:254], Time range(2011-06-27 11:11:43.0, 2011-06-27 12:01:21.0)
24: compromised(192.168.18.21), Belief: 0.57, Rules: [1:1394, 1:254], Time range(2011-06-29 08:22:02.0, 2011-06-29 08:22:11.0)
25: compromised(192.168.18.21), Belief: 0.57, Rules: [1:1394, 1:254], Time range(2011-06-29 10:55:10.0, 2011-06-29 10:55:58.0)
26: compromised(192.168.18.21), Belief: 0.57, Rules: [1:1394, 1:254], Time range(2011-06-29 12:28:46.0, 2011-06-29 12:28:46.0)
27: compromised(192.168.18.21), Belief: 0.57, Rules: [1:1394, 1:254], Time range(2011-06-29 14:20:16.0, 2011-06-29 14:46:06.0)
28: compromised(192.168.18.21), Belief: 0.57, Rules: [1:1394, 1:254], Time range(2011-06-29 15:06:44.0, 2011-06-29 15:20:46.0)
29: compromised(192.168.18.21), Belief: 0.57, Rules: [1:1394, 1:254], Time range(2011-06-29 18:08:14.0, 2011-06-29 18:08:15.0)
30: compromised(192.168.18.19), Belief: 0.55, Rules: [1:648, 1:2003195], Time range(2011-06-29 10:47:55.0, 2011-06-29 11:45:22.0)
31: compromised(192.168.18.19), Belief: 0.55, Rules: [1:648, 1:2003195], Time range(2011-06-29 12:04:53.0, 2011-06-29 12:09:22.0)
32: compromised(192.168.18.19), Belief: 0.55, Rules: [1:648, 1:2003195], Time range(2011-06-29 12:47:43.0, 2011-06-29 13:40:23.0)
33: compromised(192.168.18.19), Belief: 0.55, Rules: [1:648, 1:2003195], Time range(2011-06-29 13:49:21.0, 2011-06-29 13:56:59.0)
34: compromised(192.168.18.18), Belief: 0.55, Rules: [1:1394, 1:2003195], Time range(2011-06-24 10:20:11.0, 2011-06-24 10:20:11.0)

Evaluation

- Can the ranking provided by the customized DS belief calculation help in prioritizing IDS alerts?

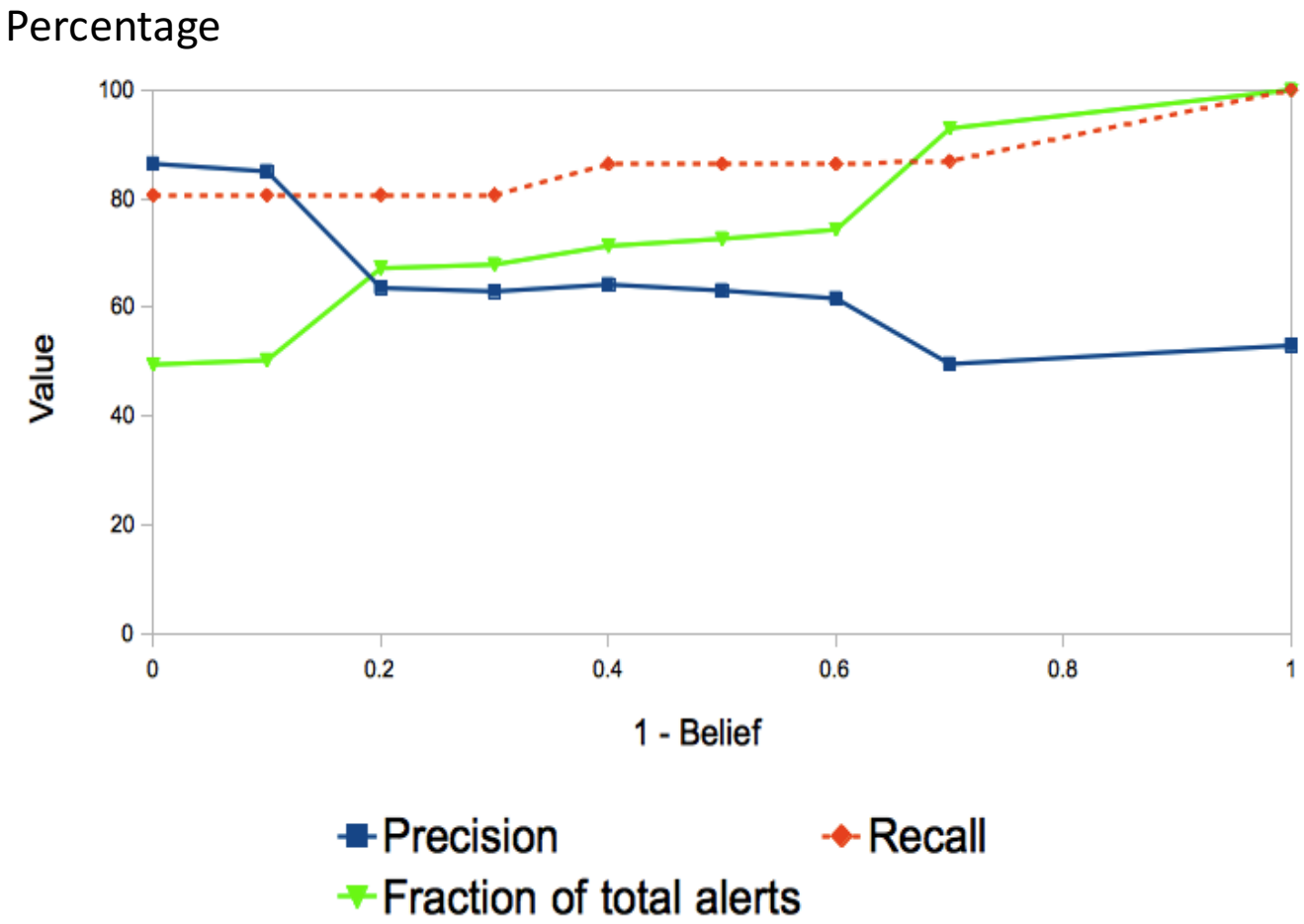
- Is it really the customized DS that helps?

Experimentation Strategy

- We need data with ground truth
  - Short-term approach: evaluate on publicly available datasets: LL DARPA dataset (1999)
    - There are many limitations.
      - e.g., DAPAR dataset has been harshly criticized in the literature.
    - Just used this as a baseline test.
      - Needs to avoid the pitfalls in those datasets
- Long-term approach: use production system, with assistance from security analysts

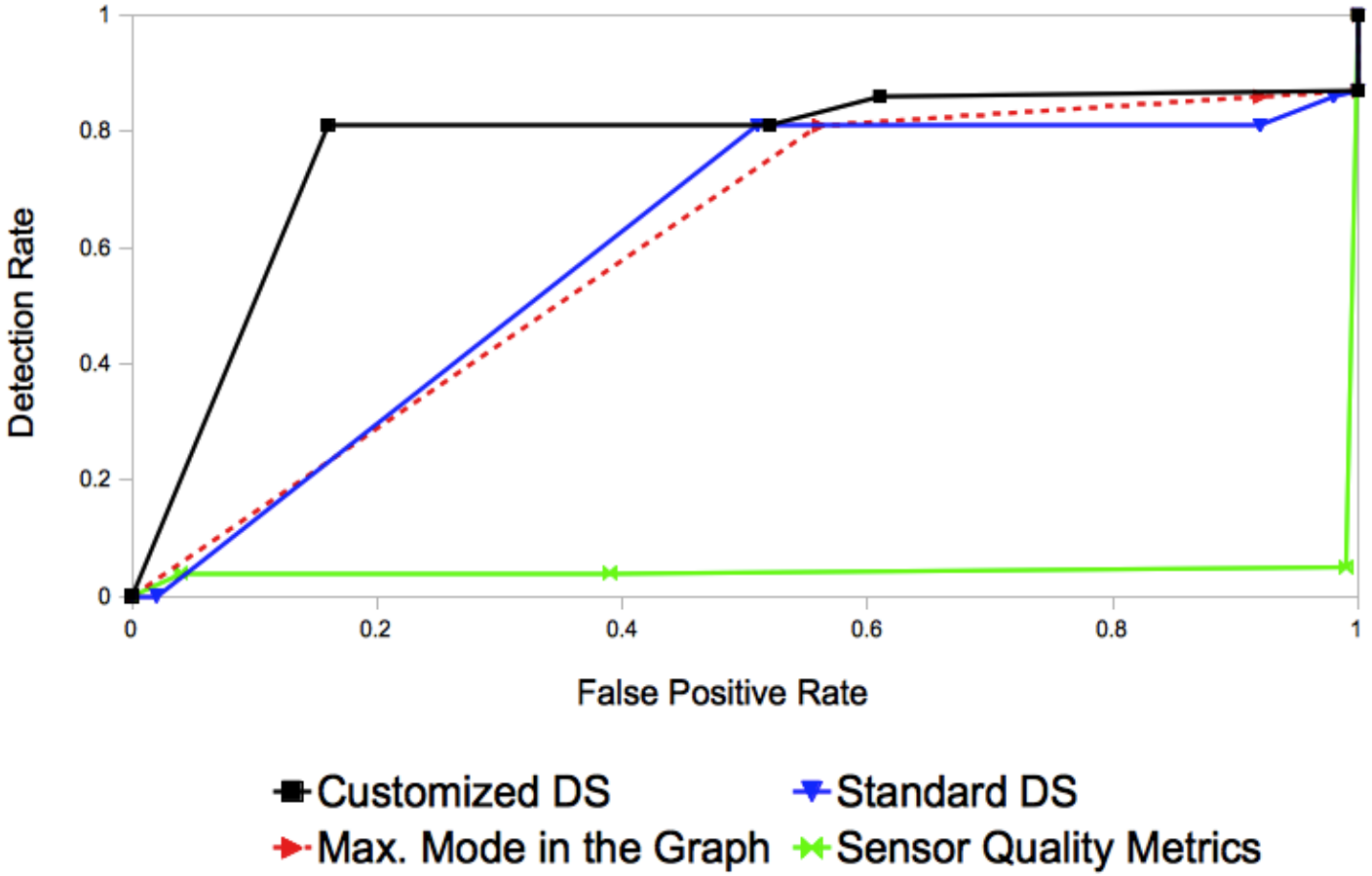
Zomlot, *et al.* AISec 2011

Prioritization Effect
(LL DARPA dataset)



Zomlot, *et al.* AISec 2011

ROC Curve
(LL DARPA dataset)



In Summary

- A bottom-up approach to designing graphical models for security analysis
- Empirically designed models fit the needs of security analysts better than “classical models”
- Leveraging the core concepts of existing probabilistic reasoning models, with customization built on tested foundations