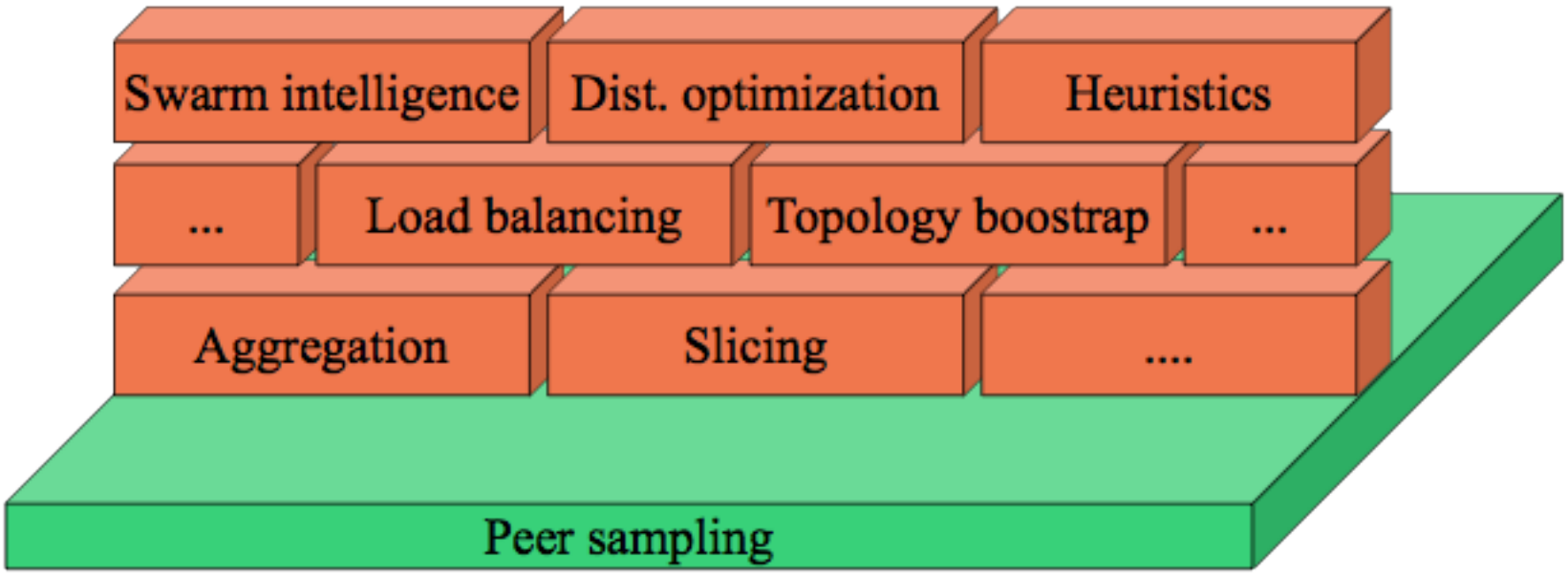
- Autonomic
- Botnet

# Autonomic

- IBM manifesto:
  - Control-loop: monitoring, analysis, planning, execution
  - Autonomic behavior at the component level
- Emergent approach
  - Self-* properties emerge from the collective behavior of a large number of components
  - Autonomic behavior at the system level

# Gossip Lego

- Gossip solves now a diverse collection of problems
- Solutions can be combined to solve more complex problems



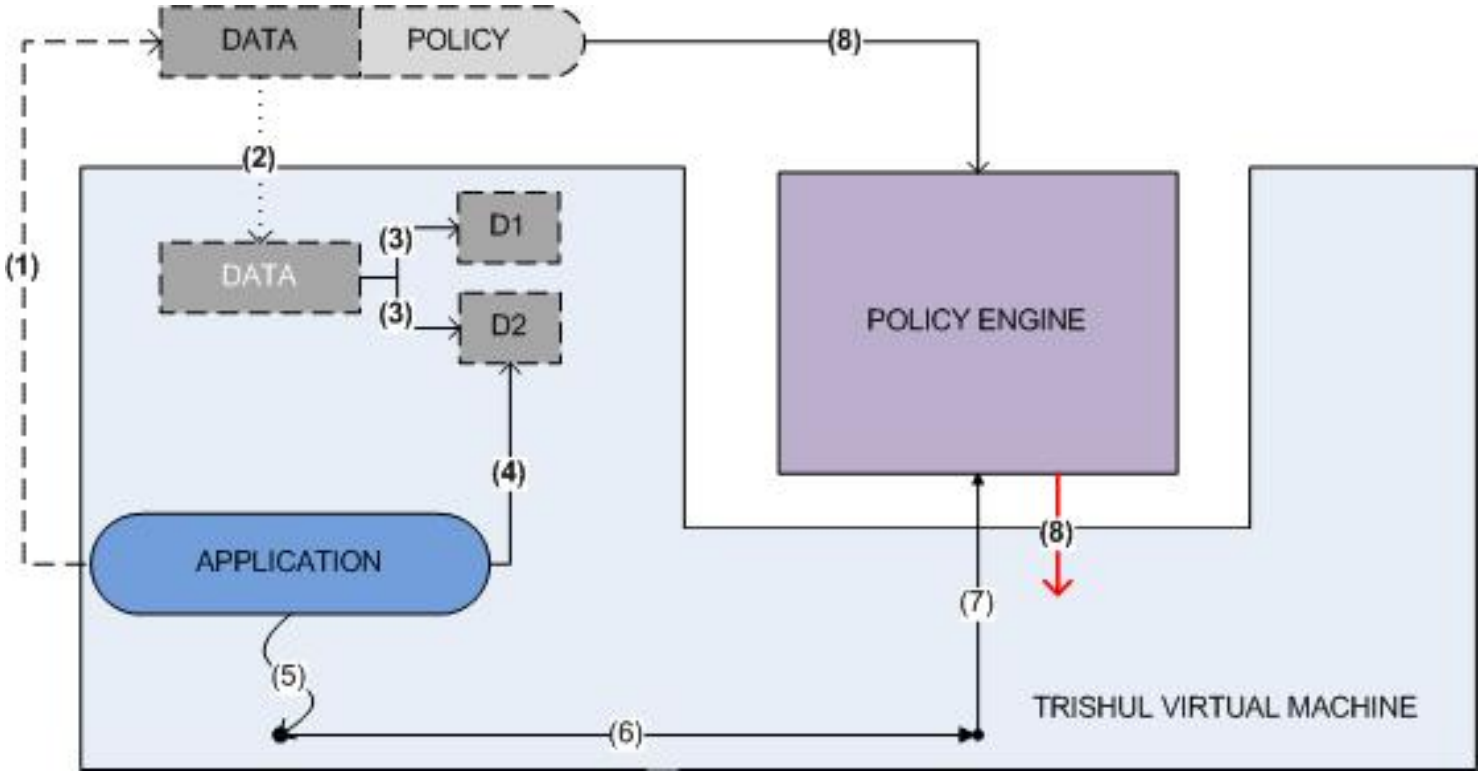
# Decentralized self-management

- Aggregation
  - Márk Jelasity, Alberto Montresor, Özalp Babaoglu: Gossip-based aggregation in large dynamic networks. ACM Trans. Comput. Syst. 23(3): 219-252 (2005)
- Ranking
  - Alberto Montresor, Márk Jelasity, Özalp Babaoglu: Decentralized Ranking in Large-Scale Overlay Networks. SASO Workshops 2008: 208-213
- Slicing
  - Alberto Montresor and Roberto Zandonati. Absolute slicing in peer-to-peer systems. In Proc. of the 5th Intl. Workshop on Hot Topics in Peer-to-Peer Systems (HotP2P'08), Miami, FL, USA, April 2008.

# Papers related to our Prin

- Secure peer sampling
  - Gian Paolo Jesi, Alberto Montresor, and Maarten van Steen. Secure peer sampling. Computer Networks, 2010. To appear.
- Modeling botnets
  - Marco Ajelli, Renato Lo Cigno, and Alberto Montresor. Modeling botnets and epidemic malware. In Proc. of the IEEE Intl. Communications Conference (ICC'10), May 2010.

# Trishul: Protecting Data from Malicious Applications

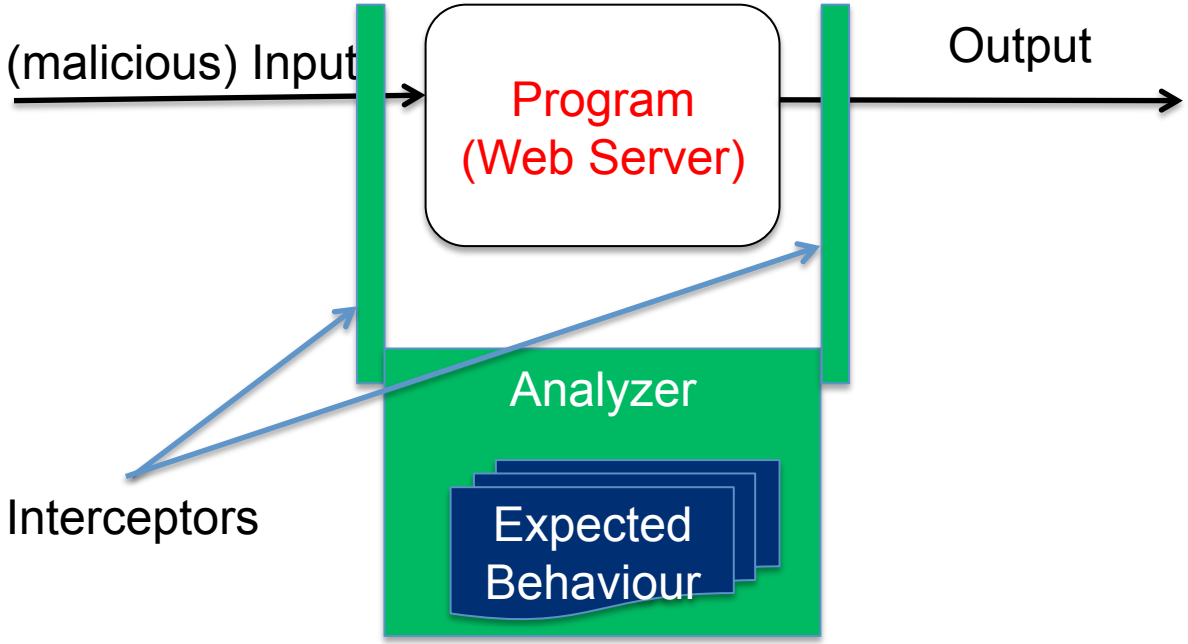



- Srijith K. Nair, Gabriela Gheorghe, Bruno Crispo and Andrew S. Tanenbaum, *"Enforcing DRM Policies Across Applications"*, 8th ACM DRM Workshop 2008,

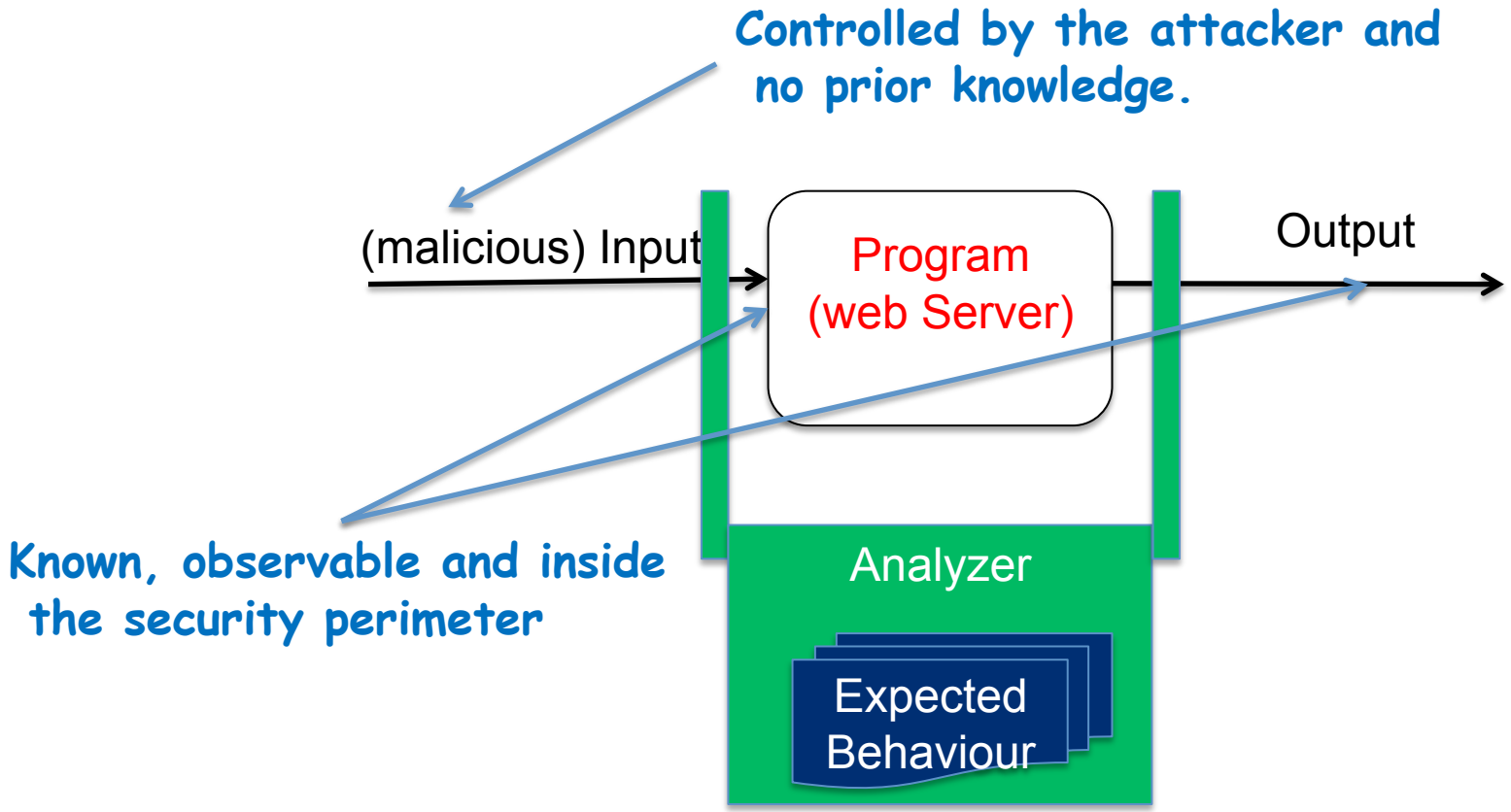
- Srijith K. Nair, Patrick N.D. Simpson, Bruno Crispo and Andrew S. Tanenbaum, "A Virtual Machine Based Information Flow Control System for Policy Enforcement" Electronic Notes in Theoretical Computer Science, Vol. 197, Issue 1, February 2008, pp. 3-16

# Black-box Tainting (Sekar)

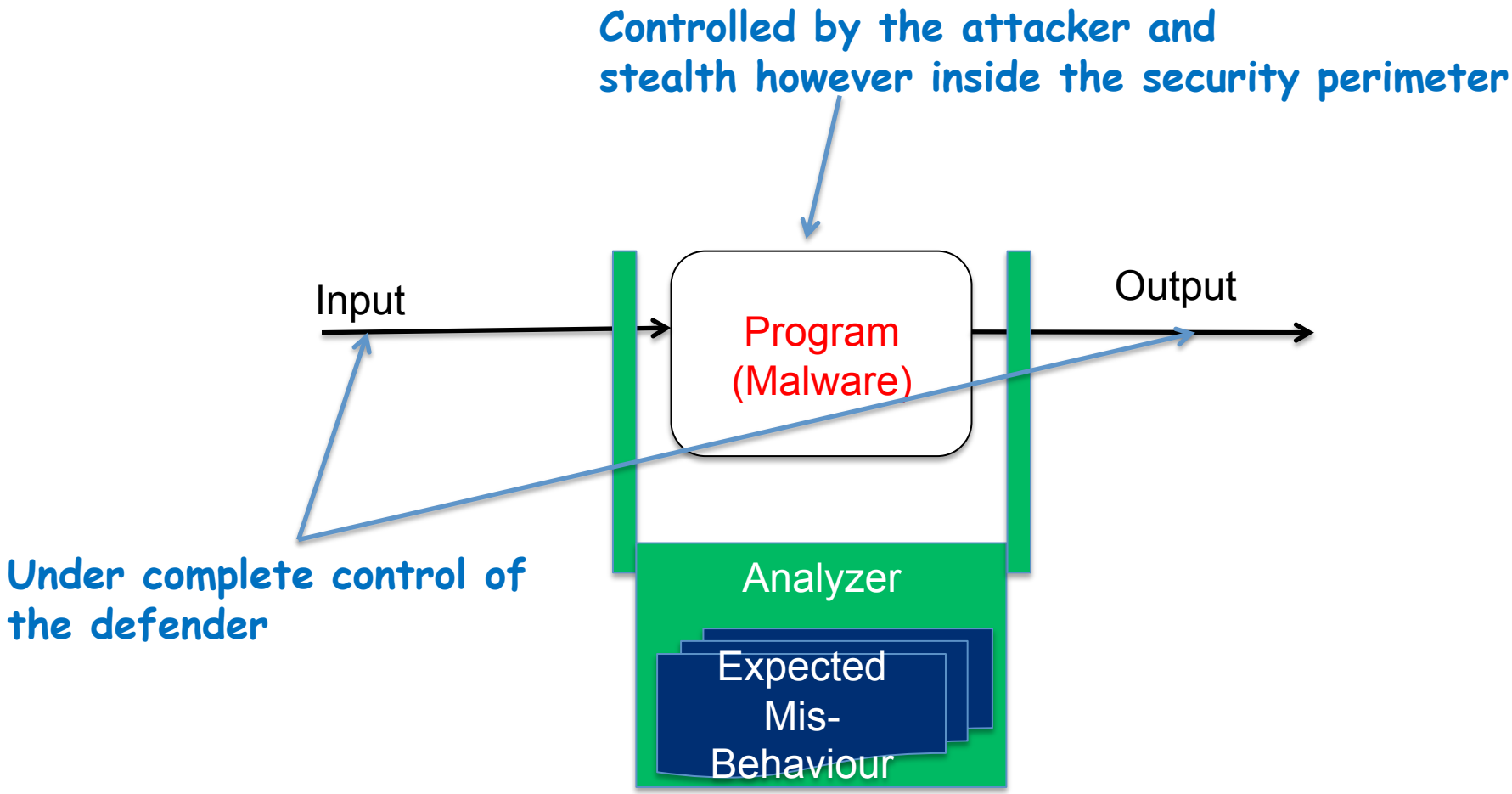
- Protecting Applications from Malicious Input
- BTW: Trishul can do this as well…but only for Java apps



# Black-box Malware Discovery



# Black-box Malware Discovery



# Directions

- On the autonomic front….
  - Distributed and collaborative detection of protocol violations (protocol integrity)
  - System-wide with no constraints on local nodes
- On the botnet front….
  - Using Black-box techniques for bot discovery on a local node