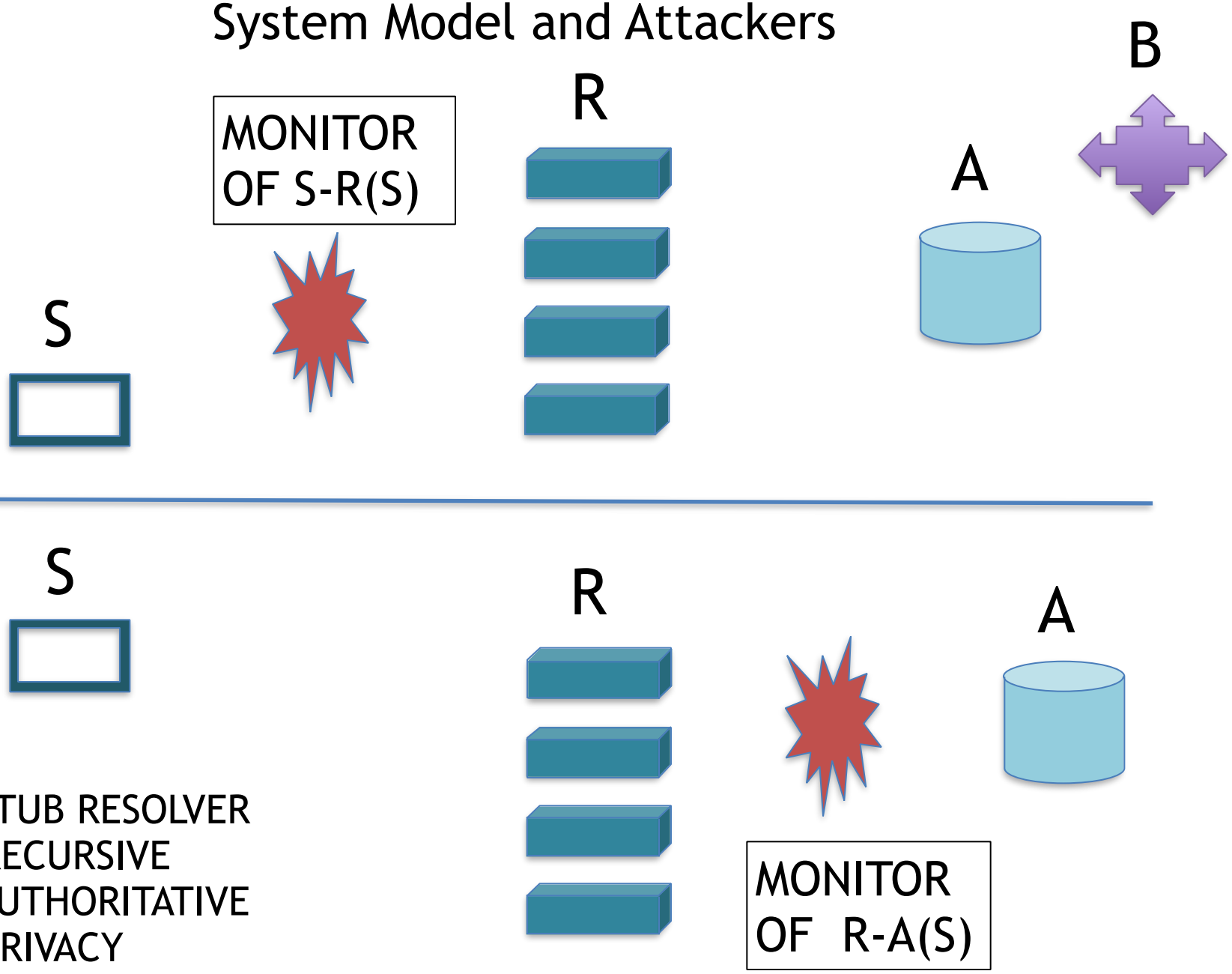
A Touch of Eval

Aziz Mohaisen
Allison Mankin
DPRIVE - IETF 92

- Draft is posted, feedback is welcome
  - draft-am-dprive-eval-00.txt
- Issues (1)
  - Attacker Model (emphasizing Type 1-A, passive pervasive monitor) – and question "which monitor(s) is deprived of power to attack privacy by mechanism being evaluated"

System Model and Attackers



S = STUB RESOLVER
R = RECURSIVE
A = AUTHORITATIVE
B = PRIVACY
BROKER

Quick Key

- Attacker Models
  - Passive Pervasive Monitor (1-A)
  - Passive Direct Monitor (1-B)
  - Active Monitor (2)
- System Model
  - S-R
  - R-A
  - S-B
  - (S-F-R)
  - (R-F-A)
- Mechanism Parameters
  - Such as randomized ciphersuite
- Privacy Goals
  - Unlinkability
  - Undetectability
- System Eval
  - Which monitor or monitors is deprived of access to private information?

- Issues (2)
  - Additions to system model for mechanisms that alter the existing system model, for instance, by relying on a mixer, broker, anonymizer.
  - Expand system model – monitor that is “in” systems such as above has extra ability to detect and link PII and IOI, compared with monitor in system as defined so far in draft.
  - Fill in TODOs