Sustainable Secure Data Dissemination in Distributed Environments
Rohit Ranchal, Ruchith Fernando, Bharat Bhargava
Department of Computer Science and CERIAS, Purdue University

Distributed Interaction

Problems with current model
- Lack of visibility on interactions in unknown domains
- Loss of control over shared data in unknown domains
- Disparate protection mechanisms used by different parties
- Lack of policy communication and enforcement mechanisms
- Lack of tracking and auditing mechanisms
- Lack of trust in interactions

Problem Statement
- To sustain data confidentiality outside owner’s trust domain

General Solution
- Encrypt data
- Define policies for data dissemination, access and usage
- Setup policy enforcement mechanism to control data interaction

Policy Enforcement at Owner
- E.g. Client-server paradigm
- Lot of exchange of messages
- Requires source availability

Policy Enforcement in Middle
- E.g. Pub/Sub model
- Trusted Third Party (TTP) related issues
- Single point of trust and failure

Policy Enforcement at Receiver
- E.g. DRM solutions
- Requires presence of a Trusted Component
- Restricted to known/trusted hosts

Data are considered passive entities unable to protect themselves
Require another active and trusted entity – a trusted component, application or a third party

Proposed Approach
- Metadata
  - Access control policies
  - Life duration
  - Other policies

- Virtual Machine
  - Policy enforcement
  - Self-Integrity check
  - Filtering

AB Interaction
- Decentralized distributed asynchronous communication
- Independent of Trusted Third Party
- Enables secure data dissemination in unknown/untrusted environment
- No requirement of a Trusted Component on receivers
- Controlled and Selective data dissemination