CERIAS

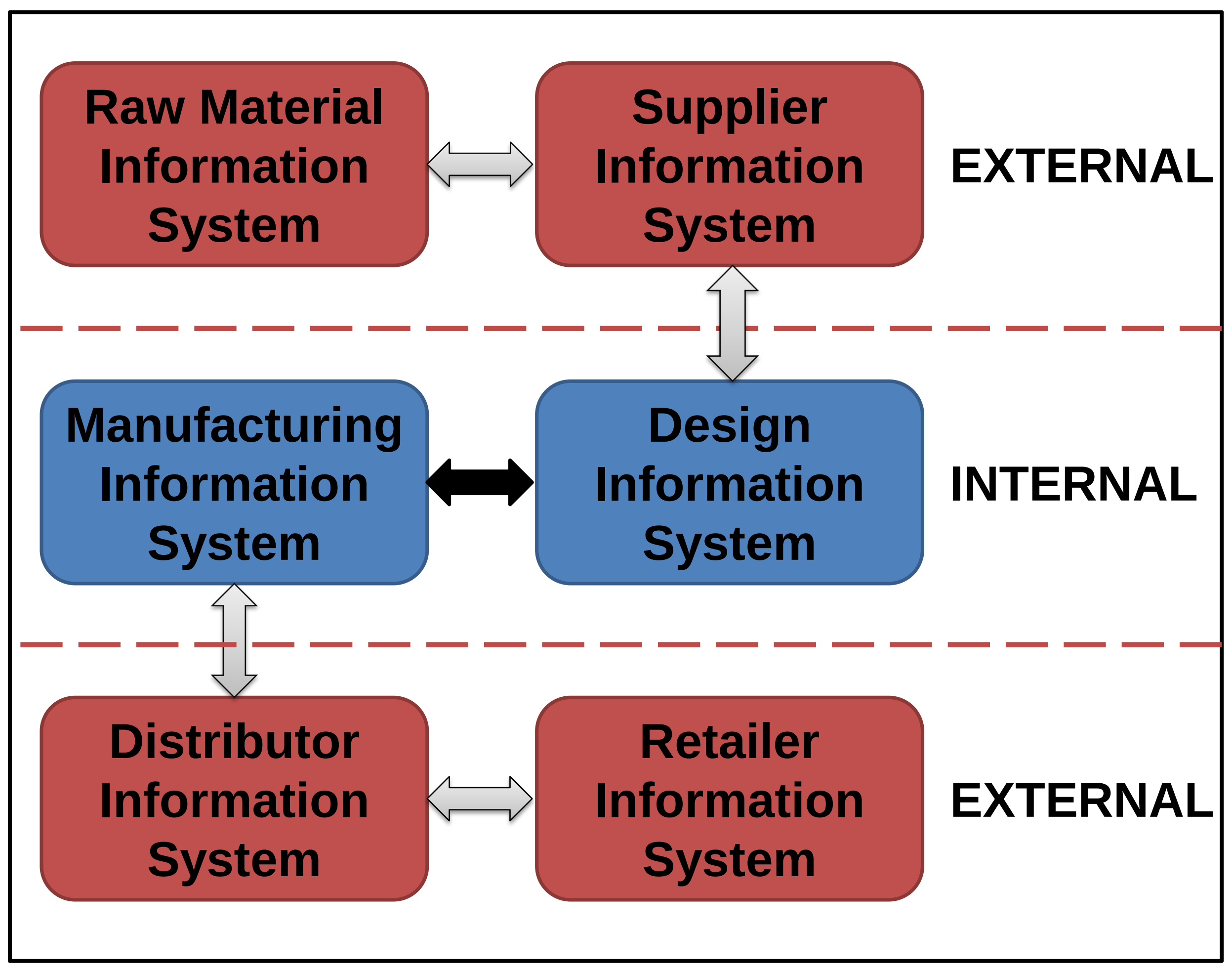
The Center for Education and Research in Information Assurance and Security

Secure Information Sharing and Access Control in PLM Systems

Rohit Ranchal and Bharat Bhargava

Department of Computer Science and CERIAS, Purdue University

Product Lifecycle Management (PLM) System


Raw Material Information System
Supplier Information System
EXTERNAL
Manufacturing Information System
Design Information System
INTERNAL
Distributor Information System
Retailer Information System
EXTERNAL

Problems with current model

- **Disparate Protection mechanisms:** Lack of common data sharing and protection mechanisms
- **Loss of control:** No control over how sensitive data are used, shared and protected by partners
- **Lack of Policies:** Lack of mechanisms to communicate owner policies and ensure policy enforcement
- **Lack of trust:** Inability to track or audit shared data in external domains
- **Information disclosure for subpoenas**
- **Insider abuse:** No protection against insider attacks

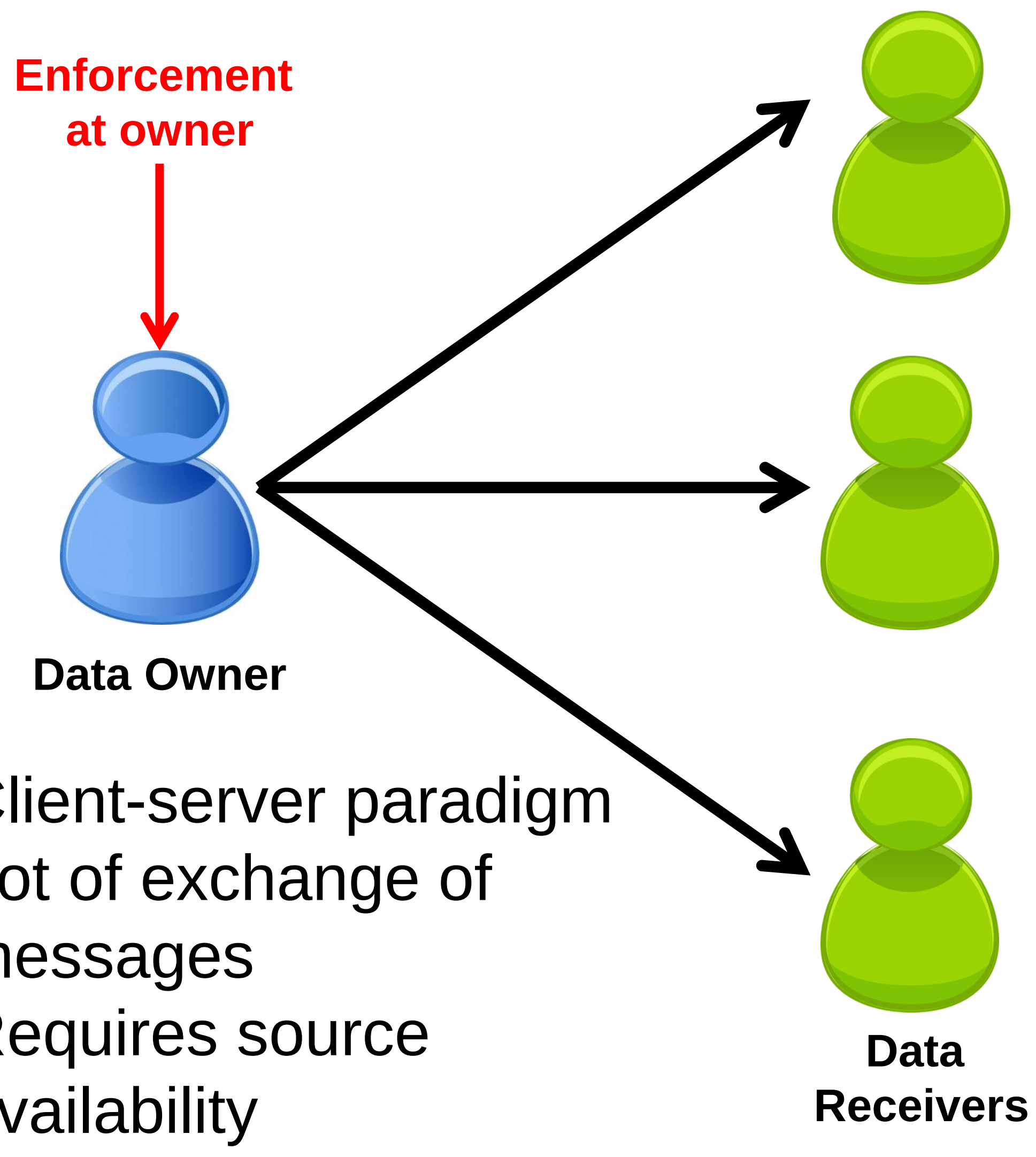
Problem Statement

How to provide control over shared data in an external domain?

General Solution

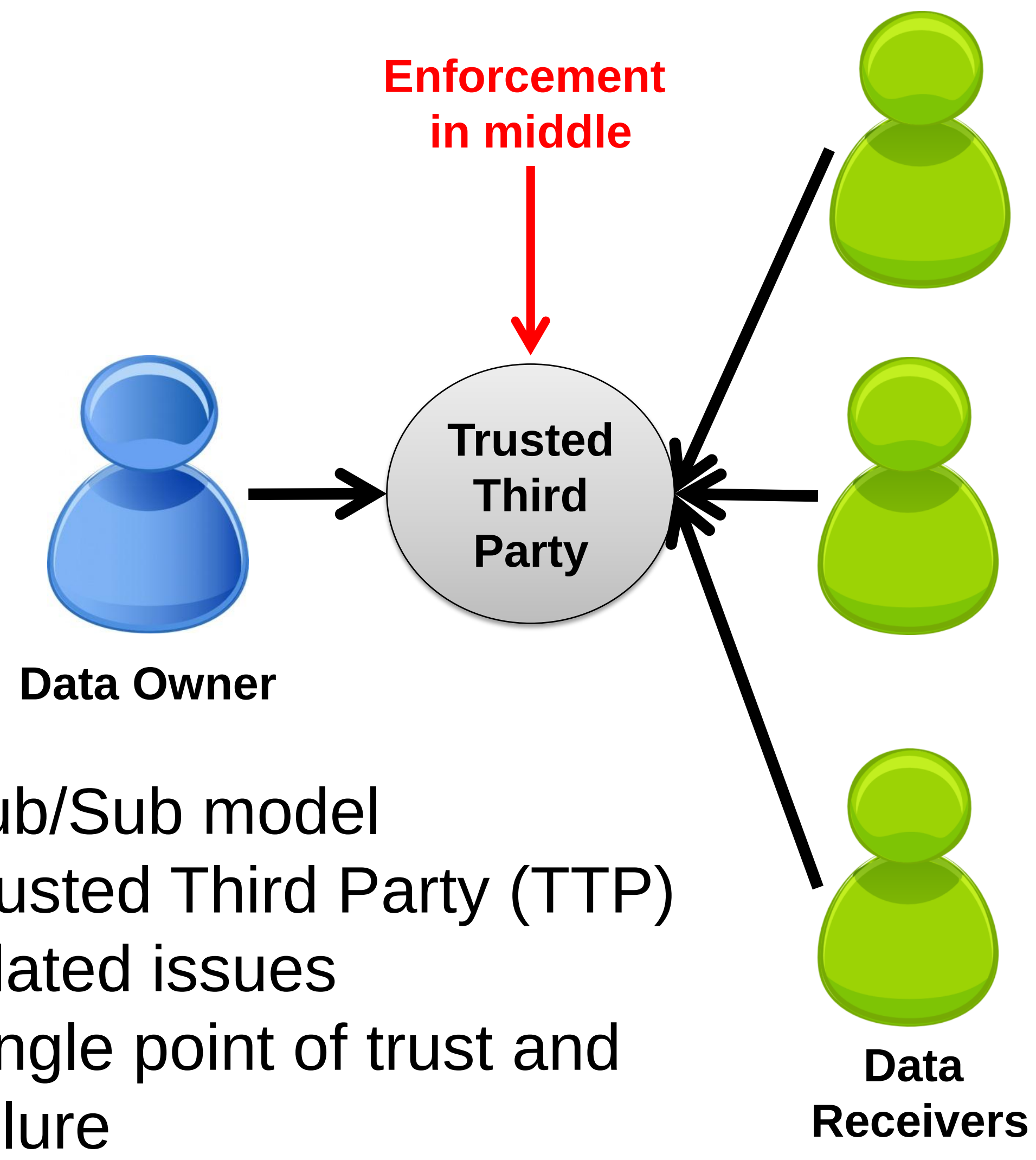
- Encrypt data
- Define Policies for data sharing, access and usage
- Setup Policy Enforcement Mechanism to control data interaction

Policy Enforcement at Owner



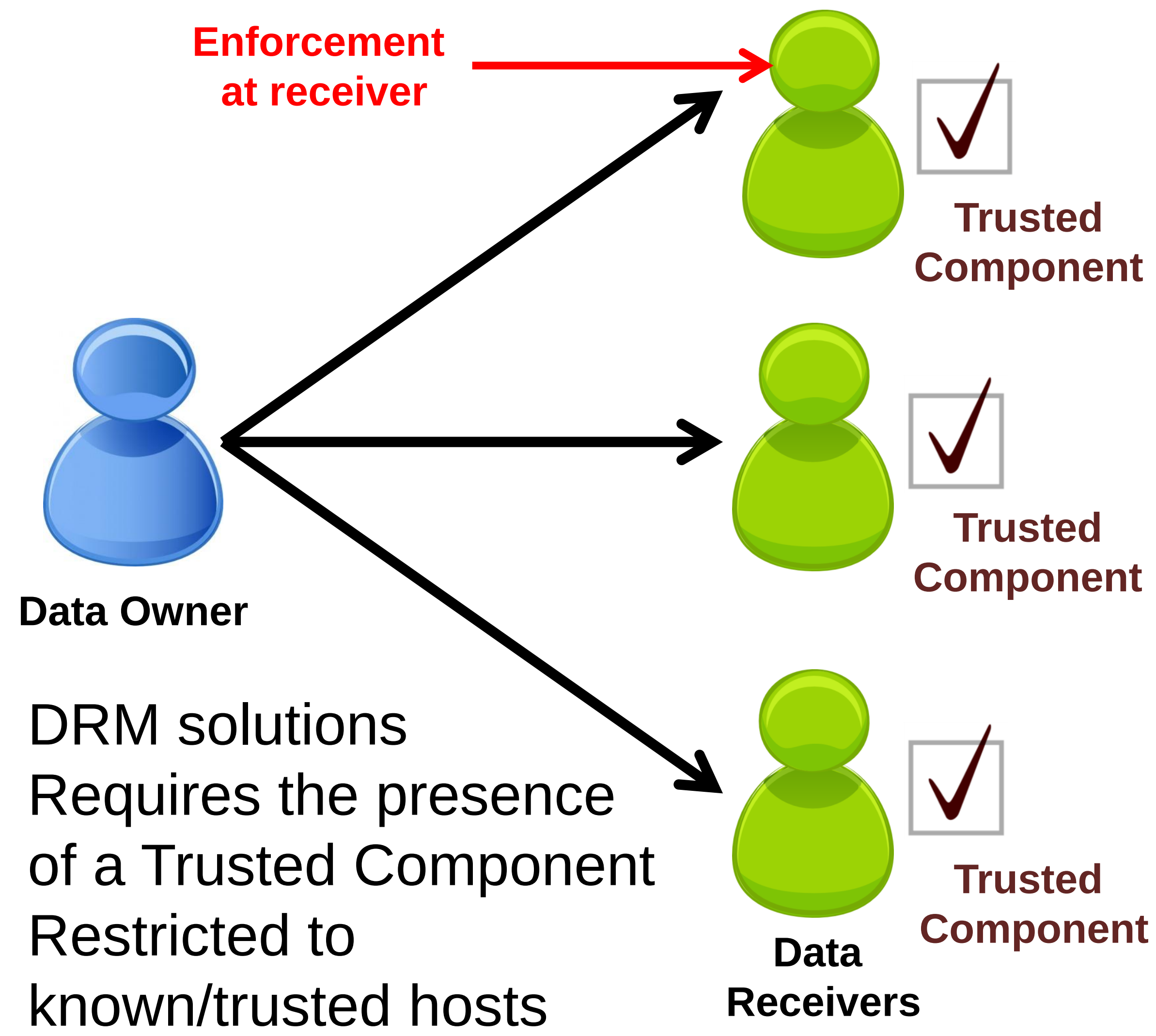
- Client-server paradigm
- Lot of exchange of messages
- Requires source availability

Policy Enforcement in Middle



- Pub/Sub model
- Trusted Third Party (TTP) related issues
- Single point of trust and failure

Policy Enforcement at Receiver



- DRM solutions
- Requires the 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 processor, memory module, application or a third party

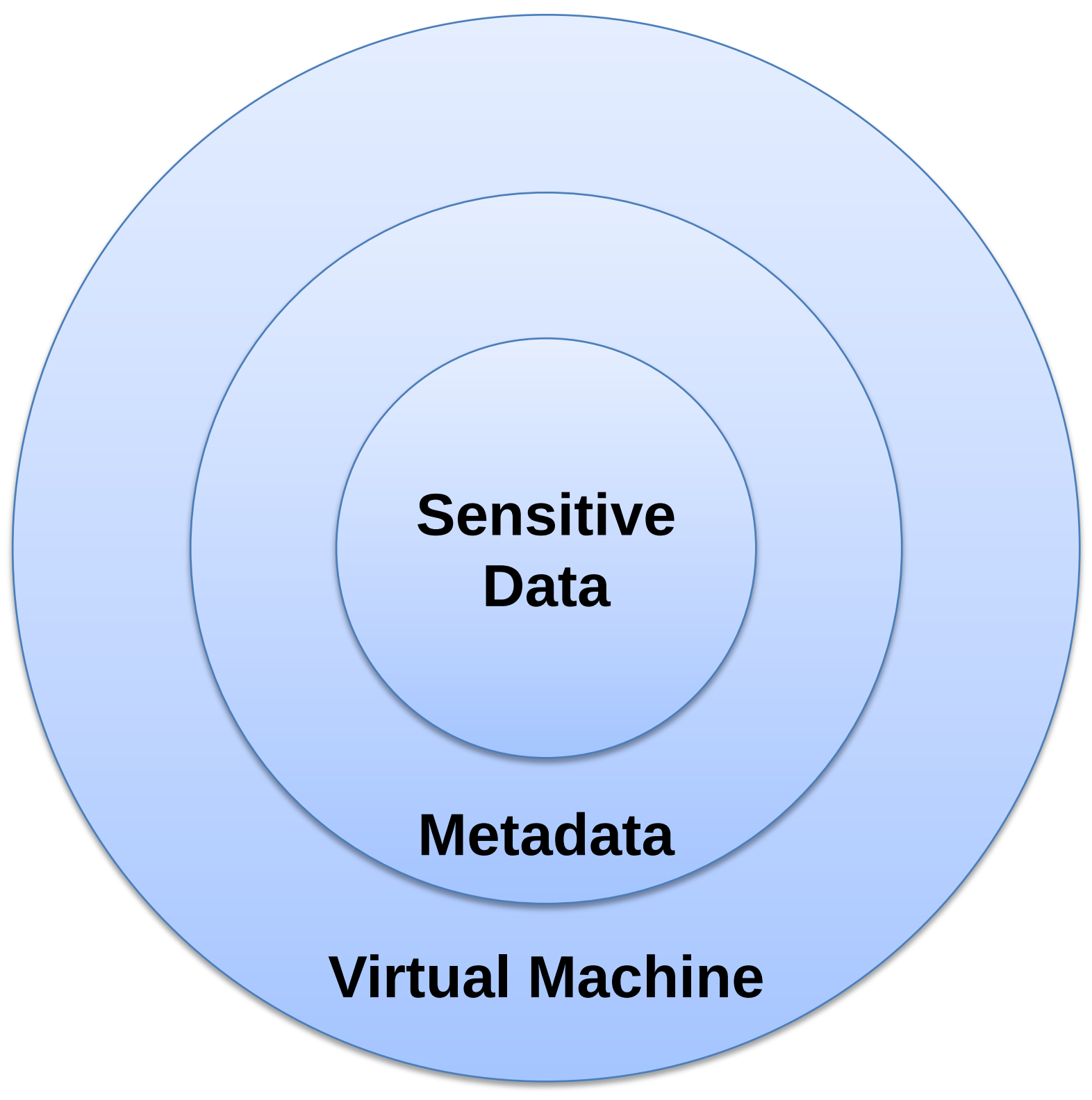
Proposed Approach

Metadata

- Access control policies
- Identity information
- Life duration
- …

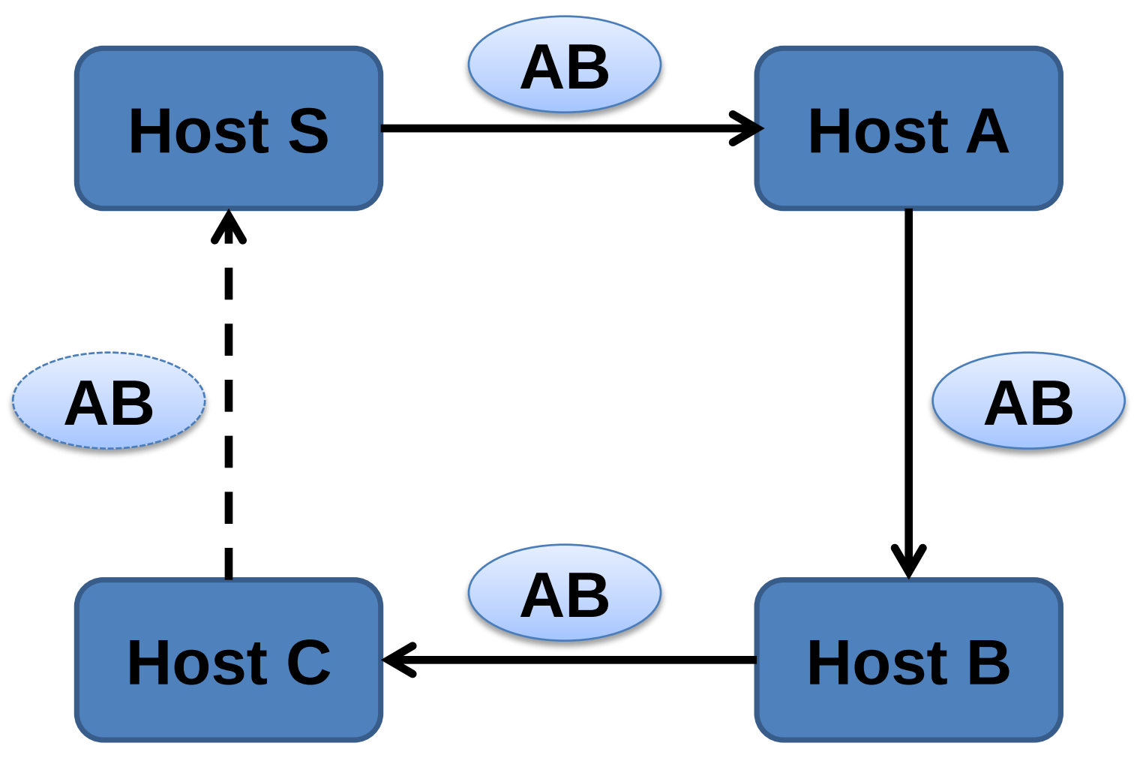
Virtual Machine

- Policy enforcement
- Self-Integrity check
- Filtering
- Apoptosis



Active Bundle (AB)

AB Interaction



- Decentralized distributed asynchronous communication
- No dependence on a dedicated TTP
- Works in unknown/untrusted environment
- No requirement to install a Trusted Component on receivers
- Controlled and Selective data dissemination

AB Challenges

- **Selective dissemination:** Organize data into separate items(versions) and encrypt each item with a different key
- **Independence of a dedicated TTP:** Use secret sharing to split keys into shares and store them in a DHT
- **Protection against compromised or malicious receivers:** Utilize Trusted Platform Module (TPM) and use code obfuscation

CERIAS®

PURDUE UNIVERSITY