An Architecture for Tracing *Incidents* across the Internet

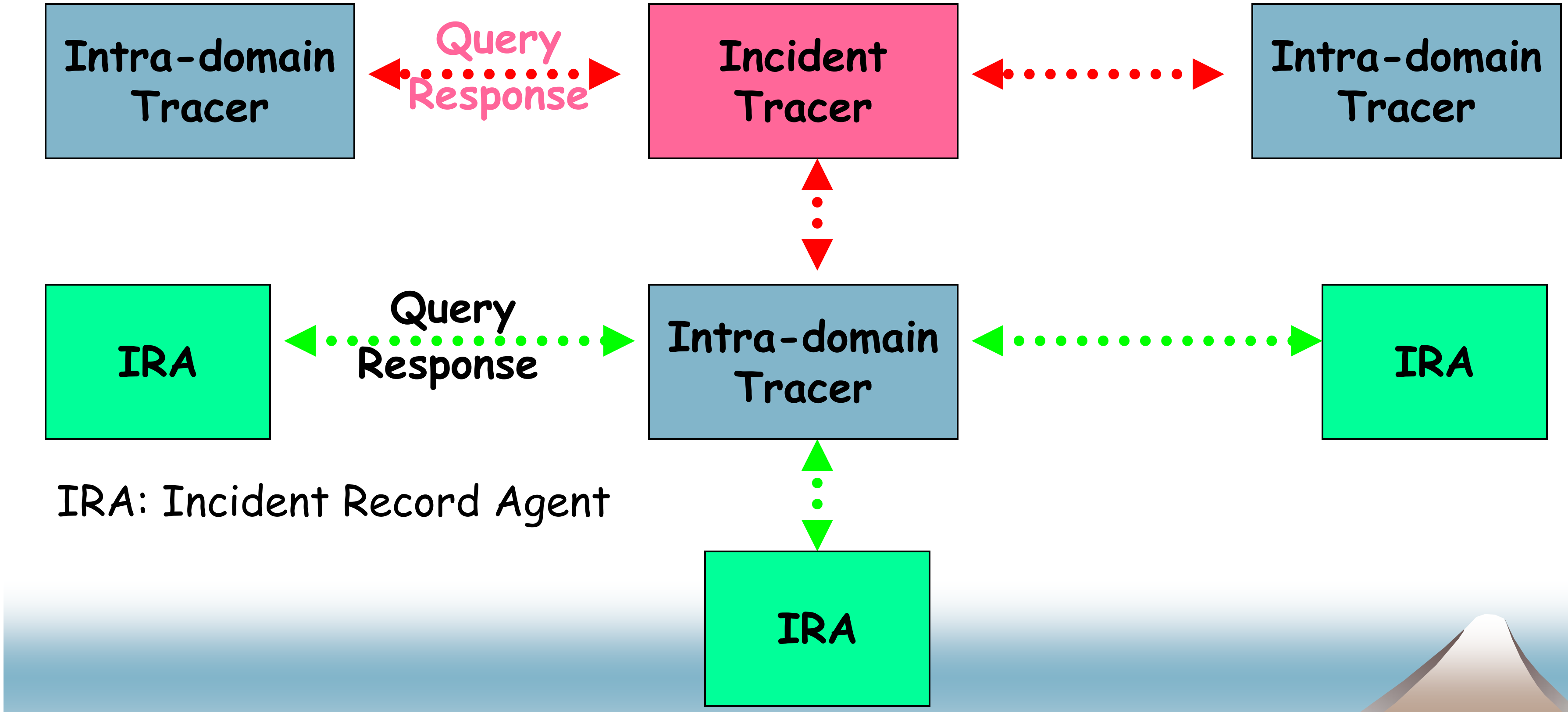
Glenn Mansfield Keeni

Cyber Solutions Inc.

Inch-wg, IETF-61

November, 2004

The two-tier Architecture



Intra-domain Tracer

Query

Response

Incident Tracer

Intra-domain Tracer

IRA

Query

Response

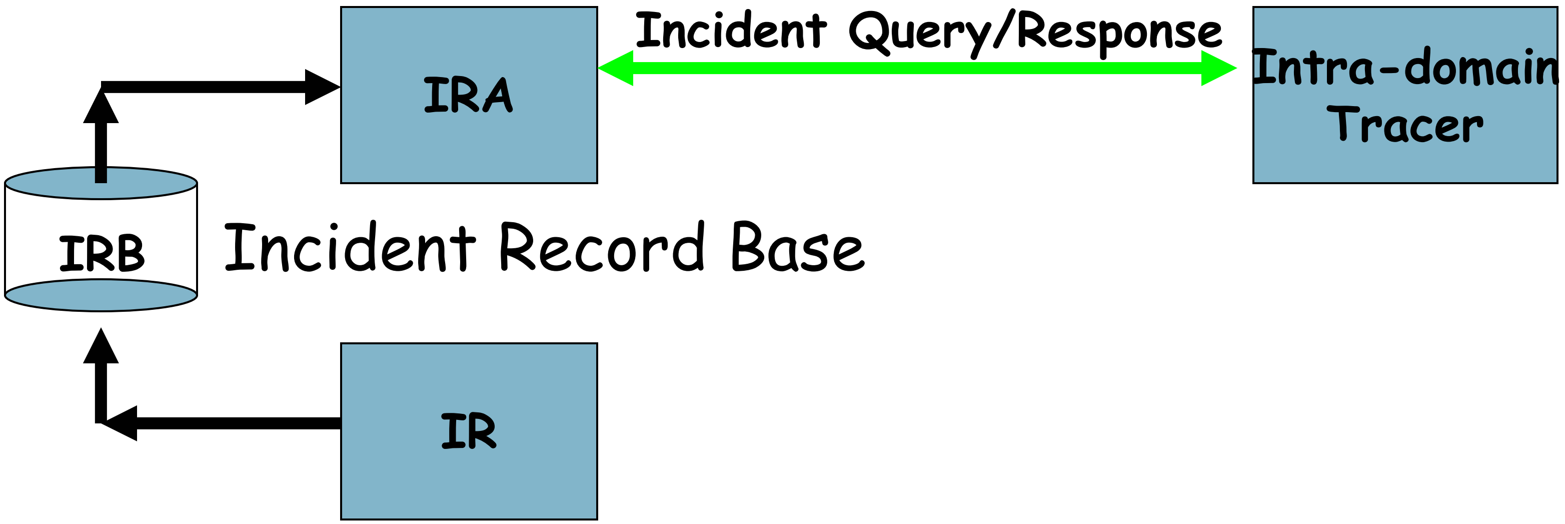
Intra-domain Tracer

IRA

IRA

IRA: Incident Record Agent

The Intra-domain Architecture



IRA

Incident Query/Response

Intra-domain Tracer

IRB

Incident Record Base

IR

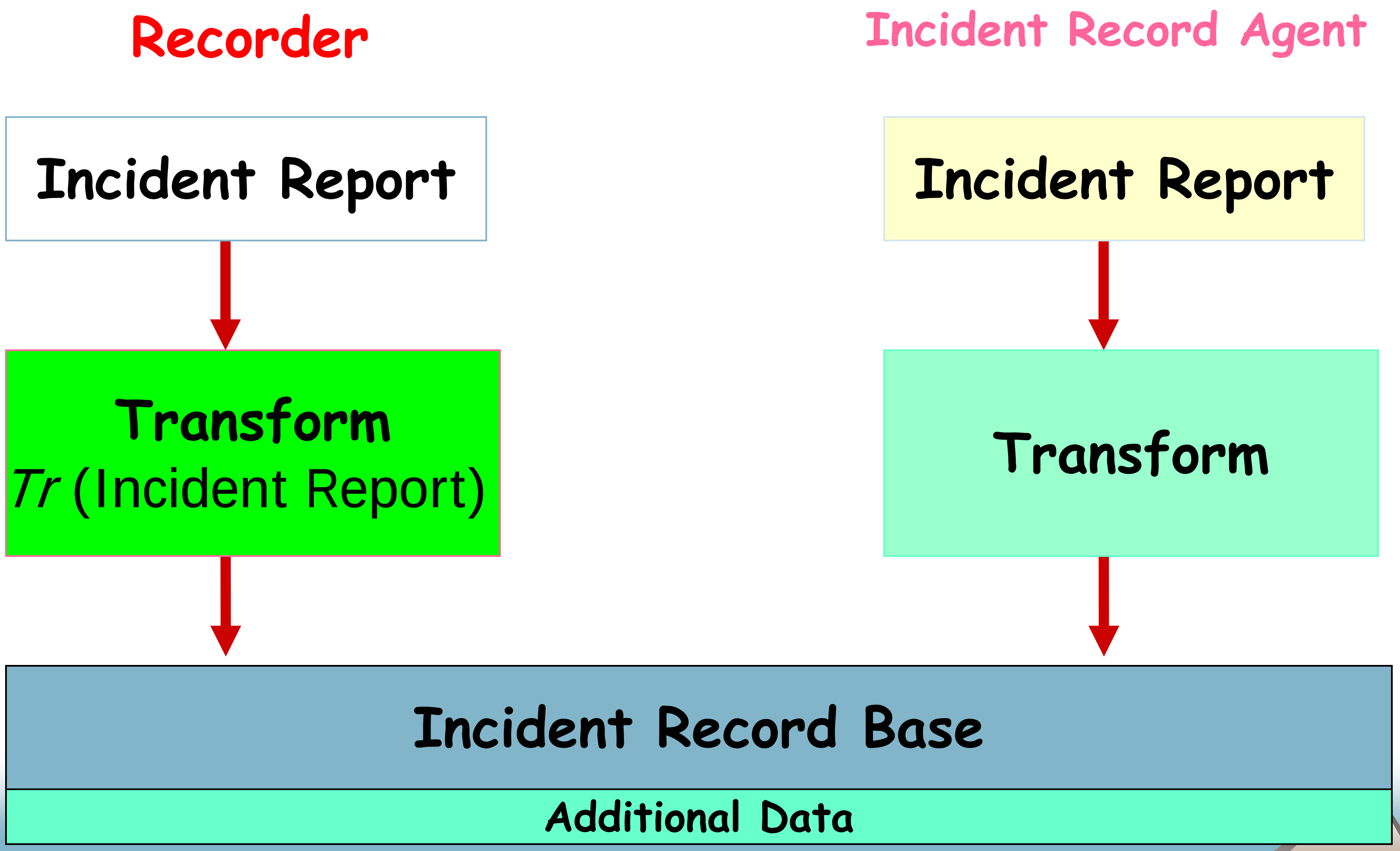
Inter-Domain Incident Tracing Protocol

- Specify the Incident *Identifier* (attributes)
    - *Unique Identification* for incident
- Return matches from local database
    - *Common format* for incident description
- Authenticated
- Privacy, Integrity
- Non Repudiation

Incident Record Protocol

Mapping: IncidentRecord ↔ Incident Identifier

Requirements: Incident Record Protocol



Recorder

Incident Report

Transform

Tr (Incident Report)

Incident Record Agent

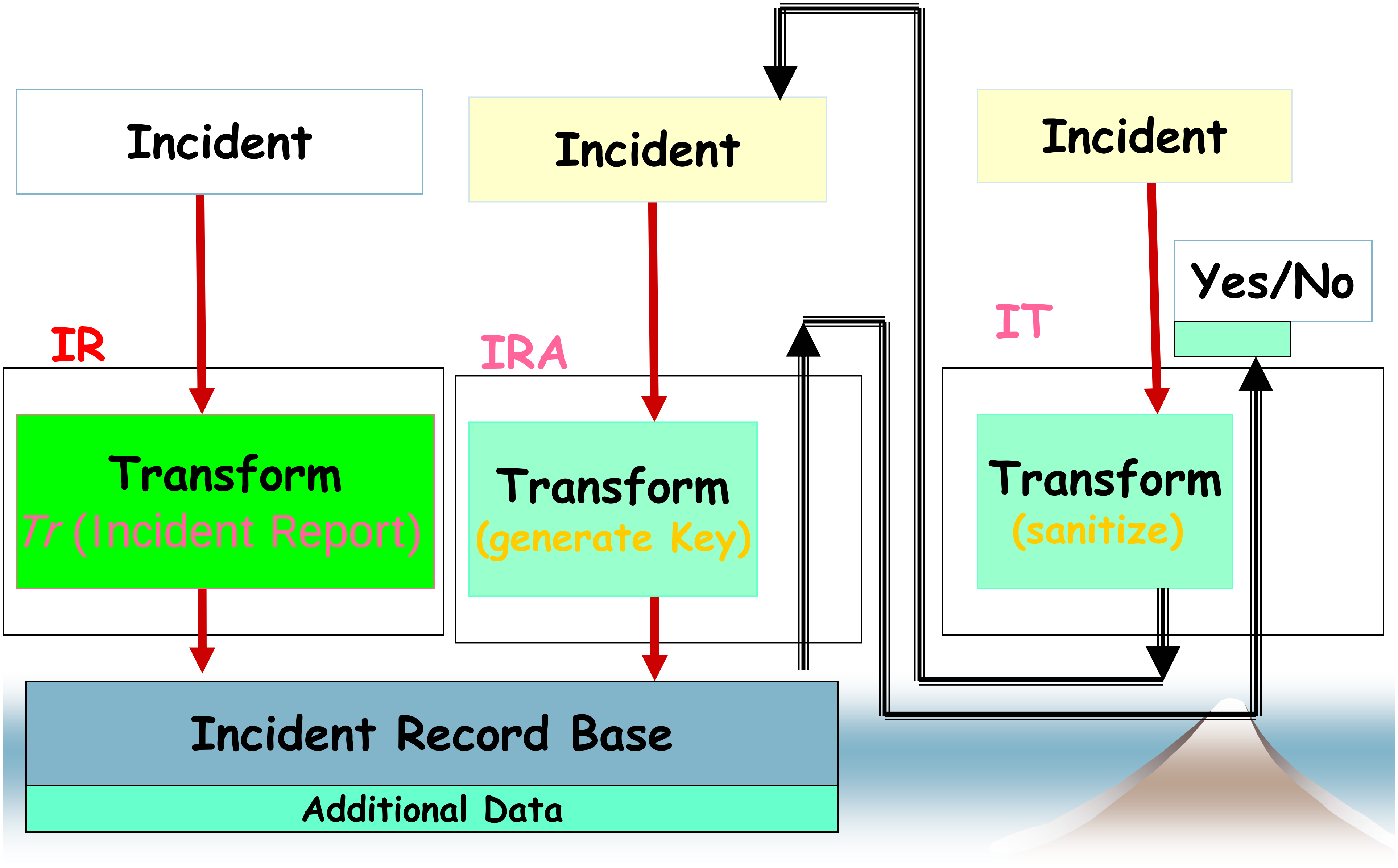
Incident Report

Transform

Incident Record Base

Additional Data

The Intra-domain packet tracing Process:



draft-glenn-ippt-arch-01.txt