An Architecture for Tracing Incidents across the Internet

Glenn Mansfield Keeni
Cyber Solutions Inc.

Inch-wg, IETF-61
November, 2004
The two-tier Architecture

IRA: Incident Record Agent
The Intra-domain Architecture

IRA

IRB

Incident Record Base

IR

Intra-domain Tracer

Incident Query/Response
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

Recoder

Incident Report

Transform

$Tr(Incident\ Report)$

Incident Record Agent

Incident Report

Transform

Incident Record Base

Additional Data
The Intra-domain packet tracing Process:

1. Incident
2. IRA
3. Tr (Incident Report)
4. Transform (generate Key)
5. Incident Record Base
6. Additional Data
7. IT
8. Yes/No
9. Transform (sanitize)