
Extended INCident Handling Working Group (INCH)

15:30 – 17:30

Wednesday, March 9. 2005

IETF 62, Minneapolis, USA

URL: <http://www.cert.org/ietf/inch/>

slides: <http://www.cert.org/ietf/inch/ietf62/>

mailing list: <http://listserv.surfnet.nl/archives/inch.html>

issue tracking: <https://rt.psg.com> (inch-* queues)

INCH Agenda

- **Administrative**
 - (Roman Danyliw, 10 min)
- **Requirements draft (draft-ietf-inch-requirements-03)**
 - (Glenn Keeni-Mansfield, 15 min)
- **Data Model draft (draft-ietf-inch-iodef-03)**
 - (Roman Danyliw, 30 min)
- **Implementation guide draft (draft-ietf-inch-implement-01)**
 - (Roman Danyliw, 5 min)
- **RID draft (draft-ietf-inch-rid-01)**
 - (Kathleen Moriarty, 25 min)
- **Extending IODEF for Phishing Reports (draft-jevans-phishing-xml-00)**
 - (Pat Cain, 20 min)

Charter Review: Goals

(<http://www.ietf.org/html.charters/inch-chart.html>)

Define a data representation for communication between

- a CSIRT and its constituency (e.g., users, customers, trusted reporters) which reports system misuse;
- a CSIRT and parties involved in an incident investigation (e.g., attacking site); and
- collaborating CSIRTs sharing information.

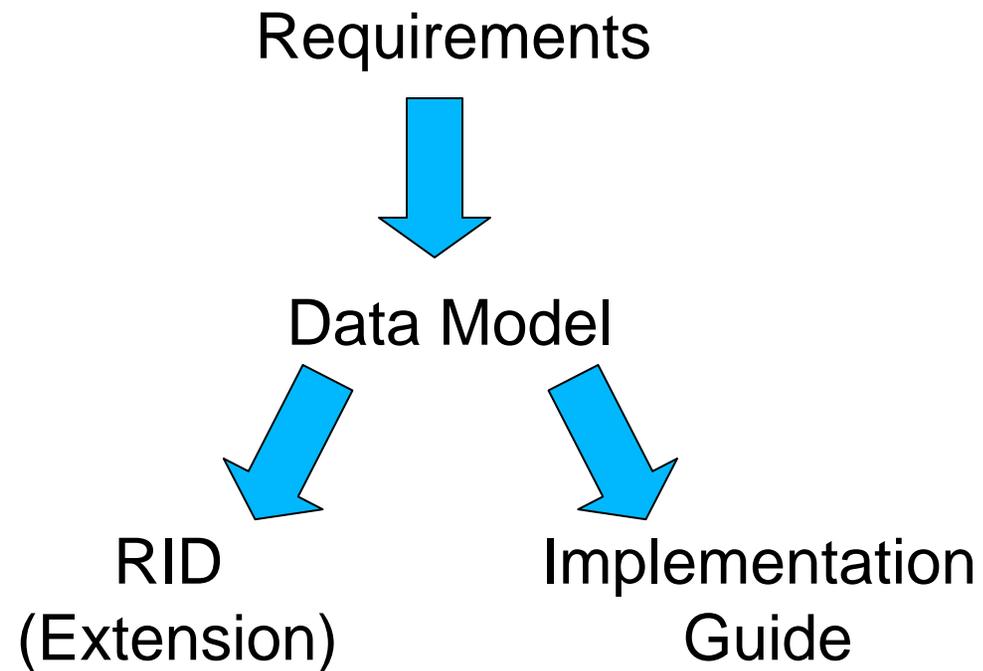
News and Process

- Documents are taking TOO LONG!!
- Tools team has generated WG-specific pages
 - <http://tools.ietf.org/wg/inch/>
- Audio streaming is enabled on all mikes
- PROTO process

Documents

- Requirements (v03.01 → 03)
 - Format for Incident Exchange (FINE)
- Data Model (still at -03)
 - Incident Object Description Exchange Format (IODEF)
 - IODEF implementation requirements specified by FINE
- RID (still at -01)
 - Traceback extension to IODEF
- Implementation Guide (still at -01)
 - Guidelines for implementers of IODEF

Dependencies



Core Document Milestones

- **December 04:** Submit requirements I-D to the IESG as Informational
 - WG last call by April 2005
- **March 05:** Submit incident data language specification I-D to the IESG as Proposed
 - WG last call by July 05
- **March 05:** Submit traceback extension specification I-D to the IESG as Proposed
 - No longer just a trace-back extension
 - WG last call by July 05 (contingent on DM)
- **April 05:** Submit implementation guidelines I-D to the IESG as Informational
 - WG last call by August 05 (contingent on DM)

Mailing List and Web Site

`http://www.cert.org/ietf/inch/`

Post: `inch@nic.surfnet.nl`

Archive:

`http://listserv.surfnet.nl/archives/inch.html`

Subscribe:

send mail to `listserv@nic.surfnet.nl` with

`"subscribe inch <first name> <last name>"`

in the body