
Extended INCident Handling Working Group (INCH)

09:00 – 11:30

Thursday, November 11 2004

IETF 61, Washington DC, USA

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

slides: <http://www.cert.org/ietf/inch/ietf61/>

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-03.01)**
 - (Glenn Keeni-Mansfield, 15 min)
- **Data Model draft (draft-ietf-inch-iodef-03.txt)**
 - (Roman Danyliw, 30 min)
- **Implementation guide draft (draft-ietf-inch-implement-01)**
 - (Roman Danyliw, 15 min)
- **RID draft (draft-ietf-inch-rid-01)**
 - (Kathleen Moriarty, 25 min)
- **RID Implementation Report**
 - (Naohiro Fukuda, 20 min)
- **Architecture for Incident Querying**
 - (Glenn Keeni-Mansfield, 15 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.

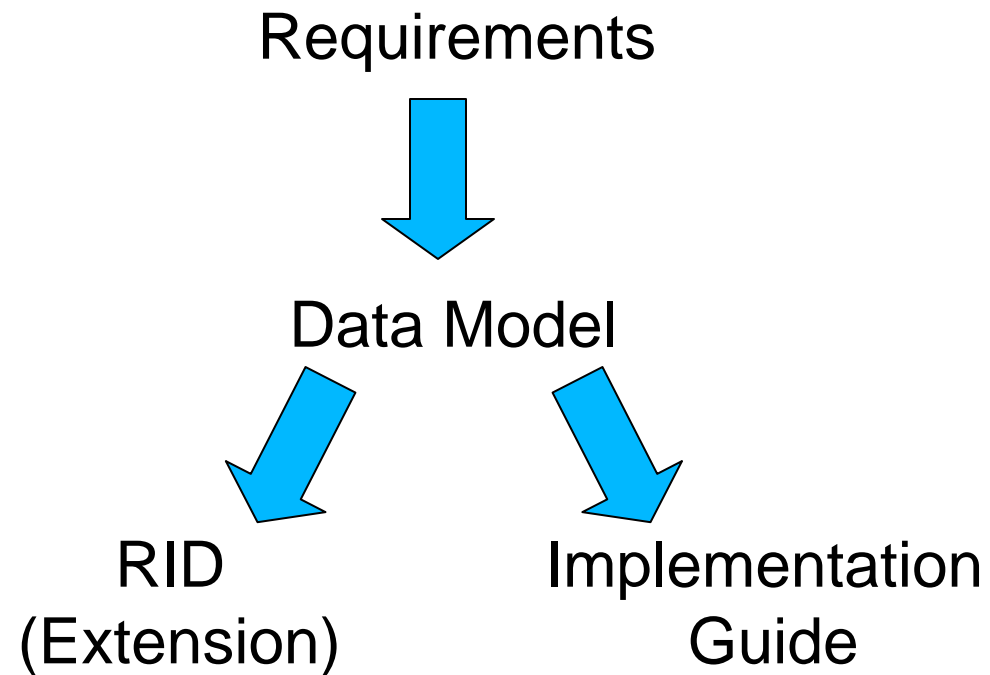
News

- Good luck to departing AD Steve Bellovin
- Sam Hartman is new AD for INCH
- Documents are taking TOO LONG!!

Documents

- Requirements (v02 → 03.01)
 - Format for Incident Exchange (FINE)
- Data Model (v02 → 03)
 - Incident Object Description Exchange Format (IODEF)
 - IODEF implementation requirements specified by FINE
- RID (v00 → 01)
 - Traceback extension to IODEF
- Implementation Guide (v00 → 01)
 - Guidelines for implementers of IODEF

Dependencies



Document Status

- **Requirements**
(draft-ietf-inch-requirements-03.01)
 - Ready for WG-last call
- **Data Model**
(draft-ietf-inch-iodef-03)
 - Finally have an update
- **RID Extension**
(draft-ietf-inch-rid-01)
 - Almost done?
- **Implementation Guide**
(draft-ietf-inch-implement-01)
 - Updated for new data model

Transport Issue

- Message envelope needed for IODEF (likely SOAP)
- Transport protocol needs to be specified (MUST HTTP?, SHOULD BEEP?)
- Need to re-charter to support this effort
 - Define a new Standards track protocol specification
 - Various transport bindings drafts

Core Document Milestones

- **August 04:** Submit requirements I-D to the IESG as Informational
 - WG last call by December 04
- **November 04:** Submit incident data language specification I-D to the IESG as Proposed
 - WG last call by March 05
- **November 04:** Submit traceback extension specification I-D to the IESG

Mailing List

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