Extended INCident Handling Working Group (INCH)

13:00 – 15:00
Thursday, August 5 2004
IETF 60, San Diego, USA

URL: http://www.cert.org/ietf/inch/
slides: http://www.cert.org/ietf/inch/ietf60/
mailing list: http://listserv.surfnet.nl/archives/inch.html
issue tracking: https://rt.psg.com (inch-* queues)

INCH Agenda

- **Administrative**
  - **(Roman Danyliw, 10 min)**
- **Draft Review**
  - **Requirements draft review (draft-ietf-inch-requirements-03**)**
    - **(Hiroyuki Ohno, 15 min)**
  - **Data Model draft review (draft-ietf-inch-iodef-03**)**
    - **(Roman Danyliw, 25 min)**
  - **Implementation guide draft (draft-ietf-inch-implement-00)**
    - **(Roman Danyliw, 5 min)**
  - **RID draft review (draft-ietf-inch-rid-00)**
    - **(Kathleen Moriarty, 20 min)**
- **Parallel Work**
  - **IRTF Anti-Spam Research Group (ASRG): Abuse reporting**
    - **(John Levine, 15min)**
- **New Work?**
  - **Vulnerabilities and Exploits Description Exchange Format (VEDEF)**
    - **(Ian Bryant and Yurie Itoh, 25 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.

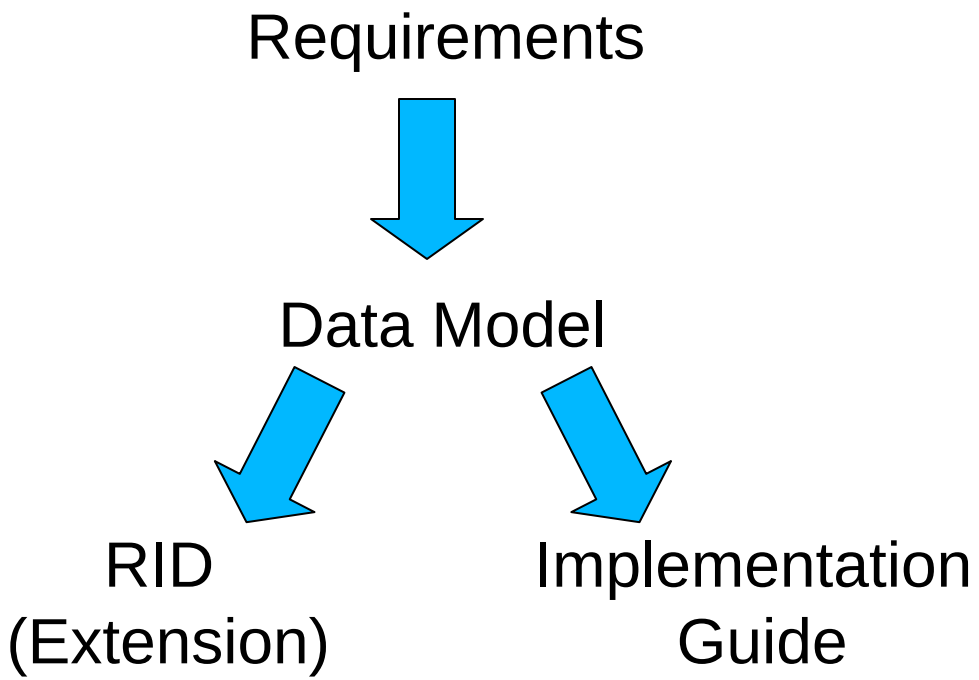
News

- Held an interim meeting in Budapest, Hungary in June 2004 prior to FIRST AGM 2004
  - http://listserv.surfnet.nl/scripts/wa.exe?A2=ind04&L=inch&O=D&P=12910

Deliverables

- Requirements
  - Format for Incident Exchange (FINE)
- Data Model
  - Incident Object Description Exchange Format (IODEF)
  - IODEF implementation requirements specified by FINE
- Extensions (to IODEF)
  - Real-time Internet-network Defense (RID)
  - Traceback extension to IODEF
- Implementation Guide
  - Guidelines for implementers of IODEF

Dependencies



Document Status

- **Requirements**
  (draft-ietf-inch-requirements-03)
  - **Approaching WG-last call**
- **Data Model**
  (draft-ietf-inch-iodef-02)
  - **Issues remains**
- **RID Extension**
  (draft-ietf-inch-rid-00)
  - **Refinement occurring**
- **Implementation Guide**
  (draft-ietf-inch-implement-00)
  - **Initial draft ready; contingent on data model progress**

Core Document Milestones

- ***August 04:*** Submit requirements I-D to the IESG as Informational
  - Slippage till October 04?
- ***November 04:*** Submit incident data language specification I-D to the IESG as Proposed
  - Probably very aggressive
- ***November 04:*** Submit traceback extension specification I-D to the IESG as Proposed
  - Slippage till Nov 04?
- ***Sep 04:*** Submit implementation guidelines I-D to the IESG as Informational
  - Slippage depends on data model

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