Internet Engineering Task Force

Extended INCident Handling Working Group (INCH)

http://www.cert.org/ietf/inch/inch_interim_2004.html

12:00 – 16:00

Sunday, June 13 2004

Interim Meeting

Budapest, Hungary

Roman Danyliw, <rdd@cert.org>

INCH Agenda

12:00 - 13:30 SESSION 1

- Agenda Bashing; WG Background; WG Issues
  - <http://www.cert.org/ietf/inch/interim04/ietf-interim2004-inch-agenda.pdf>
- Requirements
- RID
  - <http://www.cert.org/ietf/inch/interim04/ietf-interim2004-inch-rid.pdf>
- Data Model
  - <http://www.cert.org/ietf/inch/interim04/ietf-interim2004-inch-dm.pdf>

13:30 - 14:00 Coffee Break

14:00 - 15:30 SESSION 2

- Data Model (continued)

- Related Work
  - JPCERT/CC Scanning Project
    - <http://www.cert.org/ietf/inch/interim04/ietf-interim2004-inch-jpcert.pdf>
  - Vulnerabilities and Exploits Description Exchange Format (VEDEF)
    - <http://www.cert.org/ietf/inch/interim04/ietf-interim2004-inch-vedef.pdf>

Why have this meeting here?

- IETF meets three times a year in person
  - Next meeting: San Diego, USA, Aug. 1-6, 2004
- Otherwise, participation is through the mailing list; or
- Interim meetings, such as today
  - FIRST members are important stake holders in this process
    - Met before at FIRST-TC (Feb 2003, Uppsala, Sweden)

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.

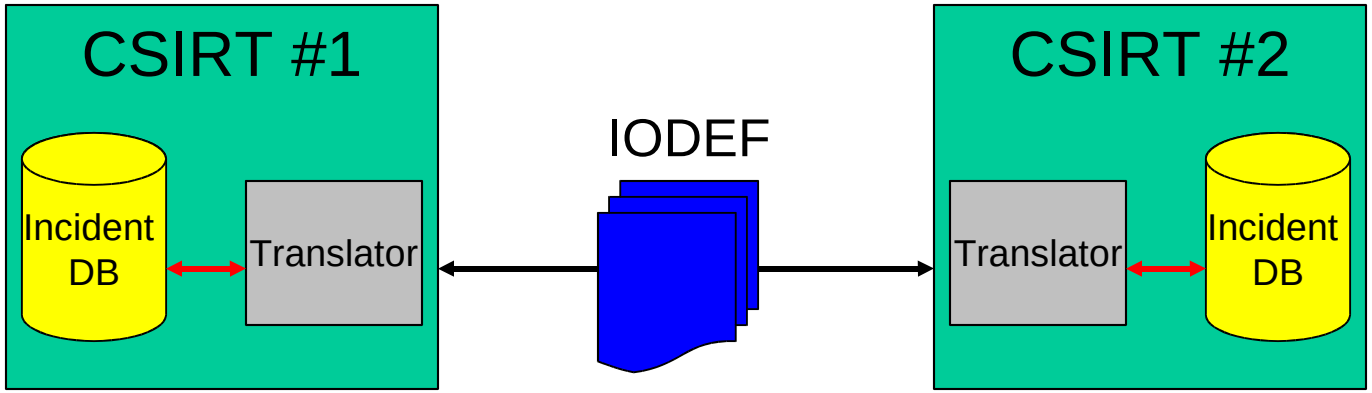
What is the INCH WG?

- History
  - Genesis of work is in Terena TF-CSIRT initiative
  - Brought into the IETF Dec 2001 to expose the work to a larger forum
- INCH is part of the IETF Security Area
- Umbrella in the IETF to standardize relevant CSIRT data formats

Scoping the INCH work

- Facilitate data exchange, ideally through automated means
- INCH focuses on
  - Transport representation
    - In-representation security issues
    - Internationalization
    - Extensibility
  - Completeness for typical CSIRT data exchange
- INCH does NOT
  - Provide an explicit protocol
  - Optimize for storage
  - Optimize for human readability

INCH among CSIRTS



- Internal CSIRT processes apply
- IODEF not appropriate format

- Crossing organization boundaries
- IODEF = standard format

Deliverables

- Requirements
  - Format for Incident Exchange (FINE)
  - http://www.cert.org/ietf/inch/docs/draft-ietf-inch-requirements-03.txt
- Core Data Model
  - Incident Object Description Exchange Format (IODEF)
  - http://www.cert.org/ietf/inch/docs/draft-ietf-inch-iodef-02.txt
- Extensions
  - Real-time Internet-network Defense (RID)
  - http://www.ietf.org/internet-drafts/draft-ietf-inch-rid-00.txt
- Implementation Guide
  - http://www.ietf.org/internet-drafts/draft-ietf-inch-implement-00.txt

Deliverable Relationships

- FINE specifies a list of requirements
- IODEF implemented these FINE requirements
- RID extends IODEF with traceback information
  - Other extensions may exist
- Implementation guidelines discuss how to implement the IODEF

What is IODEF?

- XML representation of typical data exchanged between CSIRTs
  - Incident tracking numbers
  - Contact information
  - Description of events (IP addresses, ports, etc.)
  - Classification and assessments of the events (impact, recovery, attack methodology)
- Extensible framework for constituency specific information

Known Projects

- CERT/CC
  - Network Situational Awareness (AirCERT)
- JPCERT/CC
  - Internet Scan Data Acquisitions System (ISDAS)
- European CSIRT Network
  - eCSIRT.net

News

- Unofficial Web Page
  - http://www.cert.org/ietf/inch/inch.html
- Issues Tracking via RT
  - https://rt.psg.com
  - Policy for usage
    - http://listserv.surfnet.nl/scripts/wa.exe?A2=ind04&L=inch&F=&S=&P=3143
- Outside collaboration potential
  - Internet Research Task Force (IRTF) Anti-Spam WG

IETF Process

- I-D = internet draft = description of work
  - All work starts as an I-D
- Most deliverables are done in the context of a working group (WG)
- Deliverables (RFCs) are produced for three tracks:
  - Standards
  - Informational
  - Best Common Practice (BCP)
- All deliverables are reviewed by:
  - Working group
  - Area director (AD)
  - IETF member body
  - Internet Engineering Steering Group (IESG)

Document Status

- **Requirements**

  (draft-ietf-inch-requirements-03)

  - **Not ready for 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 completion**

Core Document Milestones

- ***May 04:*** Submit requirements I-D to the IESG as Informational
  - Slippage till August 04?
- ***Aug 04:*** Submit incident data language specification I-D to the IESG as Proposed
  - Slippage till Nov 04?
- ***Aug 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