INCH IODEF Data Model Review (draft-ietf-inch-iodef-02)

Jan Meijer <jan.meijer@surfnet.nl>

IETF58, 13 Nov 2003

Open issues

- Assessment and Contact cardinality in IncidentData
- Be able to include AS data, possible solution:

```
+------------------+
| System           |
+------------------+
| ENUM restriction |<>----------[ Node     ]
| ENUM category    |<>----------[ AS ] (string)
```

Open issues

- Use the same number for default values in enumerated lists?
  - pro: clarification
  - against: hard for lists taken from other standards, makes for possible illogical ordering

Open issues, restriction

- Complexity of Restriction
  - currently attribute of Incident class, values:
    - private, public, need-to-know, default (policy pre-arranged between communicating peers)

Questions:

- include 'disclose only to' contact-information?
- need more granularity?

Open issues, doc updates

- Handling document updates:
  - passing along state information
  - query/response mechanism

Open issues, IDMEF reusing

- Desired level of IDMEF compatibility?
  - decomposing an IDMEF message straight into IODEF is currently NOT possible
    - source/target vs. system, semantics of reused IDMEF classes changed, not all IDMEF classes are present
    - Stuff in datamodel that might be taken out (4 subclasses of System (user, process, service, filelist) to simplify model
- Dependency on IDMEF (normative reference) potential problem

In the works (per 03-draft)

- Drop DTD and move to schema
- xml-enc/sig

- working-docs, implementation information, users: http://www.iodef.org/