Implementing the IODEF at the CERT/CC

Roman Danyliw
<rdd@cert.org>
INCH – IETF 55
Incident Reporting Forms

- CERT Coordination Center (CERT/CC)
- Federal Computer Incident Response Capability (FedCIRC)
- National Infrastructure Protection Center (NIPC)
- Defence Information System Agency (DISA)
Contact Information is too hard

- There are 3 to contact classes, each represents a subset of the same information
  - Organization class
  - Contact class
  - IRTContact class

- Propose: a unified class to represent contact information
Incomplete Contact Representation

• Need additional information for contacts:
  – Point of Contact,
  – title,
  – phone,
  – email,
  – fax,
  – country,
  – timezone

• Propose: adding this data to the Contact classes
Using Extensions

• All data cannot be represented in IODEF
  – Extend schema using AdditionalData class

• Human readability of AdditionalData diminishes quickly after a few elements

• Propose: “Schema Locality”
  – Add AdditionalData to certain top-level IODEF container classes
Action Annotation not Machine-readable

- Difficult to quickly (and in a machine readable way) to separate the elements from the History class
  - Who was contacted?
  - What actions were taken?

- Propose: Separating the “communication log” in the History class to another class
Incomplete Impact Assessment

• Quantifying Cost and Time of recovery
  – Recovery time (staff hours)
  – Recovery time (wall-clock)
  – Cost
  – Number of customer affected

• Operational Impact
  – Did the attack disrupt core services?
  – Has the attack stopped?

• Propose: Expanding the flexibility of the Impact class
Attack Tools Representation

- Difficult to represent information about the attack tool or technique used
  - Source::Program class
  - Method class

- Propose: Expanding the flexibility of the Method class
Complex Incident Representation

• Need resolution to **Attacker/Source and Victim/Target** class relationships