Incident Object Description and Exchange Format

TF-CSIRT Seminar
January 18, 2001
Barcelona
Agenda

- TF-CSIRT Incident Taxonomy and Description WG work process
- IODEF presentation at IETF49 IDWG meeting
  - IODEF and IDEF relations document – to be presented to IDWG
- IODEF related Terminology by Jimmy Arvidsson
  - In context of revision of the IODEF Requirements I-Draft
- IODEF XML DTD vs IODEF XML Schema
  - Discussion and call for contribution
- ITDWG charter update by Jan Meijer
ITDWG work process

ITDWG webpage and charter

- [http://www.terena.nl/task-forces/tf-csirt/i-taxonomy/](http://www.terena.nl/task-forces/tf-csirt/i-taxonomy/)

IODEF Documents

- IODEF Requirements draft-…-00.txt
- IODEF Data Model - TBD
- IODEF XML DTD or IODEF XML Schema - TBD

IODEF Editorial Group

Jimmy Arvidsson, Telia CERT
Andrew Cormack, CERT UKERNA
Yuri Demchenko, TERENA
Jan Meijer, CERT-NL

Contribution is welcome!
IODEF/ITDWG and IDEF/IDWG Relations

• IODEF presentation at IETF49 IDWG meeting
• IODEF and IDEF relations document – to be presented to IDWG
  ◆ IDEF to IODEF mapping (to be drafted)
• Look at Vulnerability Reports
  ◆ Contact Symantec (and CERT/CC?)
IDWG Scope and IDEF Documents

• IDEF is for Intrusion Detection Systems
  ◆ Main actors - IDS
  ◆ Root element – Alert
    – Short life history
  ◆ Data collected automatically

• Currently on the IETF IDWG std process
  ◆ IDEF Requirements draft-…-04.txt
  ◆ IDEF Data Model
  ◆ IDEF XML DTD
  ◆ IDEF ANS.1 MIBII format
  ◆ Intrusion Alert Protocol (IAP)

• Design Team and Pilot implementations of XML and MIBII based IDEF
IODEF purposes

A uniform incident classification enables applications such as:

• uniform statistic generation and exchange, for both domestic use and exchange of data between teams. Over time a distributed incident statistics infrastructure can evolve
• trend-analyses for reoccurrence of incidents, victims, attackers, etc.
• trend-analyses for relations between scans and attacks and thus begin working on pro-active incident response
• uniform internal incident storage
• incident handling between teams made easier (only one team needs to classify and analyze the complete incident, the other team can re-use this data)
• uniform incident reporting by victims to CSIRTs

Main IODEF actors are CSIRTs – not IDS
• Discussion and call for contribution
   Need expertise in XML DTD/Schema