Early Adopters

Incident Object Description and Exchange Format
The Gathering

- Gathering of Swedish University CSIRTs (+10)
- Seeking cooperation with SUNET-CERT
  - Coordination
  - Contact information, f.ex. TF-CSIRT, LEA, et.al
  - Statistical purposes
  - Goal to have an uniform view on Incident Handling capabilities
- Information about different Ticketing Systems
- IODEF adoption
Why IODEF format exchange?

- Exchanging Incident Information between CSIRTs
- Sharing of Incident Information in order to:
  - Collaborate / Co-ordinate on Incident Handling
  - Collate incident data (check perpetrator’s hits/different victims)
  - Statistical purposes
- Exchange of single or multiples incident(s)
- Standardised format
IODEF exchange

**CSIRT A**

- Event occurs
  - Detection
    - Function
    - System
    - Person
      - Person
      - Alarm
      - External
  - Assessment 1
    - Reporting / Filing event / Incident
    - ISec
  - Incident owner
  - First Aid
  - IHS
  - Update
  - Assessment 2
    - Crisis Management
    - Security incident
    - Incident
    - Permanent operations
    - CSIRT
    - Handling operations
      - Handling
      - Investigation
      - Management
      - Permanent measures
      - Analysis
      - Information
    - Follow up:
      - Management
      - IT council
      - Department
      - Other

**CSIRT B**

- Event occurs
  - Detection
    - Function
    - System
    - Person
    - Person
    - Alarm
    - External
  - Assessment 1
    - Reporting / Filing event / Incident
    - ISec
  - Incident owner
  - First Aid
  - IHS
  - Update
  - Assessment 2
    - Crisis Management
    - Security incident
    - Incident
    - Permanent operations
    - CSIRT
    - Handling operations
      - Handling
      - Investigation
      - Management
      - Permanent measures
      - Analysis
      - Information
    - Follow up:
      - Management
      - IT council
      - Department
      - Other

IHS = Incident Handling/Tracking System

TeliaCERT
Public
Conclusion

- Decided to try to adopt IODEF and IDMEF

- Implement IODEF features in Request-Tracker

- Web form for registering incidents (open for all)
  (actual status: test and demo purposes only. See nxt slide)

- All data entered is readable for all University CSIRTs (no secrets)
Incident Report acc. IODEF

Incident report

Einar Hällström, UMDC, Umeå universitet, 2001-05-15

This form is based mainly on RFC3867 - "TEKENA's Incident Object Description and Exchange Format Requirements"
The output is given as XML code without DOCTYPE.

Incident Impact describes result of attack expressed in terms of user community, for example the cost in terms of financial or other disruption.

Incident Impact

Attack

The target of the attack is a computer or network logical entity (account, process or data) or physical entity (component, computer, network or internetwork).
Enter the date and time when the attack was first detected. Date format YYYY-MM-DD, Time format HH:MM:SS.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>unknown</td>
</tr>
<tr>
<td>PortAlt</td>
<td>unknown</td>
</tr>
<tr>
<td>Location</td>
<td>unknown</td>
</tr>
<tr>
<td>Process</td>
<td>unknown</td>
</tr>
<tr>
<td>OS</td>
<td>unknown</td>
</tr>
<tr>
<td>Program</td>
<td>unknown</td>
</tr>
<tr>
<td>Name</td>
<td>unknown</td>
</tr>
<tr>
<td>Date</td>
<td>2001-06-08</td>
</tr>
<tr>
<td>Time</td>
<td>08:51:45</td>
</tr>
<tr>
<td>Impact</td>
<td>unknown</td>
</tr>
<tr>
<td>Action</td>
<td>unknown</td>
</tr>
</tbody>
</table>
Incident Report acc. IODEF (cont’d)
Incident Report Output

- <incident incid="IRT-7">
  - <attack>
    <datetime>2001-05-22T17:56:53+02:00</datetime>
    <impact>attempted-dos</impact>
  - <target>
    - <node>
      - <location />
      - <address category="ipv4-addr">
        <address>104.12.58.196</address>
      </address>
    </node>
    <protocol>udp</protocol>
    <port>53</port>
    <portlist />
  </service>
</target>
</attack>
- <attacker>
  - <node>
    <name>Bad Criner</name>
    - <address category="ipv4-addr">
        <address>104.12.58.196</address>
      </address>
    <netmask>255.255.255.24</netmask>
  </node>
  <rtcontact>si-cert@slov.sic</rtcontact>
</attacker>
- <victim>
  - <node>
    <name />
    - <address category="ipv4-addr">
        <address>100.209.1.25</address>
      </address>
    <netmask>255.255.255.0</netmask>
  </node>
  <rtcontact>csirt@good-fortune.se</rtcontact>
</victim>
</incident>
Incident Report Formats

By Einar Hillbom@UMDAC Umeå SE
2001-05-21

Perl program examples for converting to and from XML using XML-DOM (Document Object Model):

- createScanAlert.pl Creates a XML file from a semicolon separated list.
- parseScanAlert.pl Creates a semicolon separated list from a XML file.

Requirements:
- Email
- XML Parser
- XML DOM

Links

- RFC3067 - TERENA's Incident Object Description and Exchange Format Requirements
- IODRF XML DTD
- W3C Extensible Markup Language (XML)
- W3C XML Schema
- W3C Document Object Model (DOM)

URL: http://personliga.umdac.umu.se/einar.hillbom/IRT/
How to report security incidents in IODEF?

- Reporting a port scan as:
  - Alert IDMEF
  - IncidentAlert IODEF

- Complete investigations
  - Incident IODEF

- Propose how to use IODEF and give practical examples
Wishlist

- Practical examples how to use IODEF

- An uniform method to classify security incidents
  - What is considered to be a port scan?
  - What if an attack consists of a scan and a DoS?