Introduction for IODEF Verifier in JPCERT/CC

Hiroyuki Kido
JPCERT/CC

Overview Functions

- To verify the validity of each IODEF document
- To set and extract items(elements and attributes) from and to IODEF(XML) documents

Verification

- To verify XML format
- To verify the validity of syntax along IODEF XML Schema(or DTD)
- To verify the semantic validity of the following
  - Time and date format
  - Timezone format as an UTC timezone format
  - IncidentID(provides a fuction but blank for now)
  - Omit following verification
    - Filename,e-mail address,URL,Postal code,TEL,FAX

Technical Features

- Based on Xerces 2.2.0(XML Parser distributed from Apache Project under GNU license)

  http://xml.apache.org/
- DOM-Tree processing
  - DOM Level 3 is used as well as Level 1 and 2
- Platform Independent
  - Xerces is delivered to almost all platform
  - Written only by ANSI C++
  - BSDs, Linux, Windows,…
- Capable of handling XML Schema as well as XML DTD

Operational Plans for the Use of IODEF documents

- Exchange of statistic data of scan logs captured by sensors
  - ReportTime, IP,Port number,…
- Exchange of Vulnerability information
- Exchange of Incident Reports

Release Information for IODEF Verifier

- Tasks still remain
  - XML-Signature and XML-Encryption is not implemented yet
- URL
  - http://www.jpcert.or.jp/iodef/

IODEFドキュメントの利用

- スキャンログ情報の独自収集
- スキャンログに関する統計情報の提供
- どのような内容を提供するか(テキスト,グラフ,…)
- 分かりやすく見せるには

Operational Plan of the use for IODEF documents

- Plan to exchange by IODEF format for the type of data JPCERT/CC begin to deliver such as..
- Statistical information of scan log at sensor