

The Incident Handling SHell (IHSH)¹

Arne Helme
Stelvio
the Netherlands

Draft of October 22, 2003

¹Development of IHSH has been sponsored by SURFnet BV, the Netherlands

Contents

1	Overview	1
2	Functional Design	1
3	Command Line Options	1
4	Command Interpreter Syntax	2
5	Example: eCSIRT.net IODEF document	2
6	Using IHSH in Scripts	5
7	The IHSH Configuration File	5
8	ARS/Remedy Extension	5

1 Overview

The Incident Handling SHell (IHSB) is a command line interpreter that is used to create and parse incident reports conforming the IETF IODEF specification. The program is a front-end to the AirCERT LibIH library to create XML documents conforming to various computer security data representation standards. The interpreter can be integrated into work-flow management systems using shell scripts or the native ARS/Remedy module extension.

2 Functional Design

The primary design goal of IHSB is to create an interface to libIH that easily can be incorporated into new applications. It assumes that integration with application is achieved using scripting languages and communicate with other processes execute by the script using inter-process communication channels such as Unix pipes.

IHSB can be used in two different modes of operations either to parse incident reports encoded in XML according to the IODEF specification, or to generate an XML formatted report using IODEF compliant directives provided by an external application. In the former case, the output of IHSB is a list of commands that an application can use to drive a user interface to illustrate the report. In the latter case, the output is an XML formatted report.

In addition, IHSB can be used as a shell to create incident reports manually. The functionality can be used to manually edit an incident report and change some of its contents.

When compiled with ARS/Remedy support, IHSB communicates directly with an ARS server and can fetch existing data from the server or update the server with new information.

3 Command Line Options

IHSB recognizes the following command line options:

- c: This option is used to specify an alternative IHSB configuration file.
- d: Enables the IHSB debug mode.
- f: Reads IHSB command specification from the named file.
- o: Redirects XML output to a named file.
- r: If compiled with the ARS/Remedy module extension, fetches an entry from the ARS server. ARS EntryID is the argument to the option. See below for more details.
- s: Updates the ARS server with a document. See below for more details.
- x: Read XML document from file.
- ?: Shows usage of the IHSB command line options.

4 Command Interpreter Syntax

IHSH understand a simple command interpreter syntax that closely resemble the data handling primitives provided by the underlying LibIH library. Given a tree representation of a document, a weak XPath-like syntax is used to locate a given node (XML element) of interest in the tree. The following commands are recognized:

cd *<path>*: Conduct a tree walk to the location specified in *path*.

debug: Toggle debug information.

echo: Echoes the arguments to this command to standard output. Command is used to display information to the user when IHSH is invoked interactively or from a shell.

fsetval *<fname>*: At the current location in the tree, set attribute *name* to the contents of the file *fname*. This command is useful when large input values are to be put into a field.

getval *<name>*: Get the value of the field named by *attrname*.

?: Show hints about the program usage.

help: Show hints about the program usage.

new: Create a new empty tree representation of an IODEF object.

pwd: Print the current location in the internal XML tree.

quit: quit the IHSH command interpreter.

readxml *<file>*: Read XML formatted report from file *file* and repret the contents internally as a tree.

setval *<name>* (*val*): At the current location in the tree, set attribute *name* to the value of *val*. If *name* is a full path, it is assumed to name an attribute globally in the tree. If *attrval* is omitted, input is assumed to be of multi-line format and must be terminated by a final line containing only a dot (.).

setattr *<attr>* (*val*): At the current location in the tree, set attribute *attr* to value *val*.

walk *<path>*: Conduct a tree walk to the location specified in *path*.

writexml *<file>*: Write XML formatted report of the internal IODEF tree representation.

5 Example: eCSIRT.net IODEF document

In the following the IHSH commands are used to generate an XML formatted document according to the eCSIRT.net IODEF document profile. The XML formatted document is generated using the following IHSH commands:

```
cd /IODEF-Document
setattr version 1.0
```

```

cd /IODEF-Document/Incident
setattr purpose handling
setattr restriction need-to-know

cd /IODEF-Document/Incident/IncidentID
setval CERT-NL-42353465345
setattr name CERT-NL

cd /IODEF-Document/Incident/AlternativeID/IncidentID
setval CERT-CC-42353465345
setattr name CERT-CC

cd /IODEF-Document/Incident/AdditionalData
setval eCSIRT-net-IODEF-profile-v1.0
setattr type string
setattr meaning eCSIRT.net IODEF Profile Version 1.0

cd /IODEF-Document/Incident/IncidentData/Description
setval Portscan report

cd /IODEF-Document/Incident/IncidentData/Assessment/Impact
setval Low impact, not completed
setattr completion failed
setattr type recon

cd /IODEF-Document/Incident/IncidentData/Method/Description
setval Unknown

cd /IODEF-Document/Incident/IncidentData/Expectation
setattr priority low

cd /IODEF-Document/Incident/IncidentData/Expectation/Description
setval Take action and report back

cd /IODEF-Document/Incident/IncidentData/ReportTime
setval 200305201453

cd /IODEF-Document/Incident/IncidentData/Contact
setattr role irt
setattr type organization

cd /IODEF-Document/Incident/IncidentData/Contact/name
setval CERT-NL

cd /IODEF-Document/Incident/IncidentData/Contact/Email
setval cert-nl@surfnet.nl

```

```

cd /IODEF-Document/Incident/IncidentData/Contact/Telephone
setval +31622923564

cd /IODEF-Document/Incident/IncidentData/EventData/Description
setval Source and target IP addresses

cd /IODEF-Document/Incident/IncidentData/EventData/System
setattr category source
cd /IODEF-Document/Incident/IncidentData/EventData/System/Node/Address
setattr category ipv4-addr
cd /IODEF-Document/Incident/IncidentData/EventData/System/Node/Address/address
setval 192.168.16.25

writexml cl-ihsh-example.xml
quit

```

The following is the output of the commands give above:

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE IODEF-Document>

<IODEF-Document version="1.0">
  <Incident restriction="need-to-know" purpose="handling">
    <IncidentID name="CERT-NL">CERT-NL-42353465345</IncidentID>
    <AlternativeIDs>
      <IncidentID name="CERT-CC">CERT-CC-42353465345</IncidentID>
    </AlternativeIDs>
    <IncidentData>
      <Description>Portscan report</Description>
      <Contact role="irt" type="organization">
        <name>CERT-NL</name>
        <Email>cert-nl@surfnet.nl</Email>
        <Telephone>+31622923564</Telephone>
      </Contact>
      <ReportTime>200305201453</ReportTime>
      <Expectation priority="low">
        <Description>Take action and report back</Description>
      </Expectation>
      <Method>
        <Description>Unknown</Description>
      </Method>
      <Assessment>
        <Impact completion="failed" type="recon">
          Low impact, not completed
        </Impact>
      </Assessment>
      <EventData>
        <Description>Source IP address</Description>
      </EventData>
    </IncidentData>
  </Incident>
</IODEF-Document>

```

```

    <System category="source">
      <Node>
        <Address category="ipv4-addr">
          <address>102.168.16.25</address>
        </Address>
      </Node>
    </System>
  </EventData>
</IncidentData>
<AdditionalData
  type="string"
  meaning="eCSIRT.net IODEF Profile Version 1.0">
  eCSIRT-net-IODEF-profile-v1.0
</AdditionalData>
</Incident>
</IODEF-Document>

```

6 Using IHSH in Scripts

IHSH is designed to be invoked by a scripting language and can be fed commands by the means of interprocess communication primitives such as (Unix) pipes, or by reading a file containing the commands to be executed. The command line options can be used to override and redirect information to files instead of `stdout`. Additional commands can be used to send the

7 The IHSH Configuration File

The IHSH configuration file, `$HOME/.ihshrc`, can be used to store configuration parameters for IHSH and extension modules.

The syntax of the IHSH configuration file is straightforward:

exp1=exp2

Empty lines and lines beginning with a hash (`#`) are ignored.

Internal in IHSH, functions hooks are provided to match a tag to return the value associated with it. For a programmer, it is therefore easy to add other configuration variables to modules when needed.

As described elsewhere in this document, and alternate IHSH configuration file can be provided to the interpreter using the `-c` command line option.

8 ARS/Remedy Extension

IHSH can optionally be compiled and linked with an ARS/Remedy extension module that enables the transfer of data between a Remedy server and the IHSH application. The ARS/Remedy extension is activated using either the `-r` or the `-s` command line options.

The **-r** command line option takes a Remedy Entry ID as argument, and initiates the process of fetching the corresponding entry from the Remedy server. Upon successful retrieval, an internal XML representation of the contents is built that can be written to a file and sent as electronic mail.

The **-s** command line option converts an internal XML representation of an IODEF document to ARS data and updates the ARS server with this data. This option can be used to update an ARS server with an IODEF document received, for example, by email.

ARS configuration parameters must be set in the IHSH configuration file. The following parameters are supported:

ars_debug: Toggles the ARS debug output. In the current version of IHSH, ARS debug information is written to **stderr**.

ars_server: DNS name of the machine where the ARS server is running.

ars_port: TCP port that the ARS server is listening to.

ars_user: ARS user name that IHSH shall use when establishing a session with the ARS server.

ars_passwd: Password to use together with the user name.

Note that the current implementation only supports IODEF documents following the eC-SIRT.net IODEF profile specification.