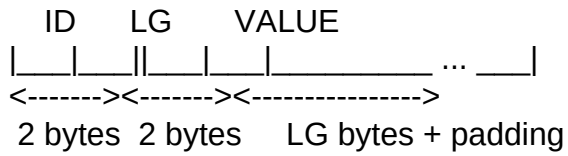
Subject: Generic audit trail converter
Posted by amo on Wed, 23 Aug 1995 07:00:00 GMT
View Forum Message <> Reply to Message

Dear all,

I am about to design a generic audit trail format converter program. Its purpose is to convert native audit trails to a canonical format which is the only one supported for analyzing audit trails by another tool.

The canonical format, called Normalized Audit Data Format (NADF), is defined as follows: Given an audit record in the audit trail, each of its fields is converted to a triplet:



where ID is identifier of the field, LG is the length in bytes of its value and VALUE is its value.

The entire NADF record is obtained by appending the conversion (as shown above) of each of its fields. Finally a 4-bytes int begins the NADF record to indicate its total length.

Since writing a format converter for each type of audit trail can be very boring, I am investigating ways of writing a generic converter. My basic idea is to provide a sort of Interface Description Language to specify the format of the file to be converted to NADF. This IDL is processed by the generic converter to (almost) automatically generate source code of the format converter for this particular input audit file.

The audit file may contain more than one record type and a field may also be a structure of its own.

Having said that (and I am sorry for being lengthy), I wonder if there are already tools for doing this maybe in an even more generic way (any format to any format conversion) and/or libraries to support this.

Any suggestions would be very appreciated and thanks to you all.

Aziz.

  ------------------------+------------------------------- ----
Abdelaziz Mounji	amo@info.fundp.ac.be
ASAX project	http://www.info.fundp.ac.be/~amo
Institut d'Informatique	voice: +32 81 724987
University of Namur	Fax : +32 81 724967
  -- ----