

Experiences Implementing A Common Format for IDS Alerts

Panel Moderator:

Michael Erlinger, Harvey Mudd College

Panelists:

Ben Feinstein, Guardent, Inc.

Greg Matthews, NASA

Stuart Staniford, Silicon Defense

Andy Walther, The Aerospace Corp.

Intrusion detection is an area of increasing concern in the Internet community. In response to this, many automated intrusion detection systems (IDS) have been developed, e.g., commercial (Real Secure) and public domain (SNORT). However, there is no standardized way for IDS to communicate with each other or to a common manager. To remedy this, the Intrusion Detection Working Group (IDWG) was chartered under the auspices of the Internet Engineering Task Force.

IDWG has published its specifications for a standard alert format (IDMEF) and a standard transport protocol (IDXP). Such specifications remain an academic exercise until the community adopts them. This forum will discuss issues related to community adoption of the IDWG specifications and, in particular, issues related to their implementation and use.

IDMEF is a message format for IDS-generated alerts and uses XML as the underlying encoding. The alert format has been designed to include (what is believed to be) fields for all the important information

found in the current set of alerts generated by a large subset of available intrusion detection systems. It is only with implementation experience that the community will be able to determine if the IDMEF specification is both complete and reasonable.

IDXP, the IDWG transport protocol, is a specific implementation of a new IETF application level protocol, BEEP – RFC 3080. Implementation experience is needed to convince the community that IDXP is appropriate as a transport protocol.

The forum will begin with a quick overview of IDMEF and IDXP standards. This introduction will be followed by presentations from implementers and vendors discussing their experience with both IDMEF and IDXP; focusing on the reference implementation of IDMEF, focusing on the reference implementation of IDXP, the IDMEF plug-in for SNORT, development of a IDMEF-based IDS manager, and related commercial activities.