Title: IDS standards - lessons learned to date.
Topic Area: IDS Integration
Speaker: Stuart Staniford-Chen, Silicon Defense
Address: 791 Shirley Blvd, Arcata, CA 95521, USA
Phone: (707) 822-4588
Fax: (707) 826-7571
Email: stuart@silicondefense.com

Bio:

Stuart Staniford-Chen received his PhD in Physics and Masters in Computer Science from the University of California at Davis. There he joined the computer security group and worked on methods to trace intruders across the Internet, and led the team that developed the GrIDS hierarchical intrusion detection system.

DARPA asked Dr Staniford-Chen to start and lead the Common Intrusion Detection Framework (CIDF) working group; he was chair or co-chair of that group until the beginning of this year. He is now a co-chair of the IETF's working group to standardize IDS alerts.

Dr Staniford-Chen now works for his own research and consulting company, Silicon Defense.

Abstract:

I will discuss two efforts to get Intrusion Detection Systems to work together - the Common Intrusion Detection Framework (CIDF), and the IETF's working group to develop an Intrusion Detection Exchange Format (IDEF).

CIDF is an effort started and supported by DARPA to develop a common language and means of interchange for IDS systems to share any data that they might need to share (a very ambitious scope). The focus has been on allowing systems developed by DARPA researchers to interoperate with one another. CIDF expresses events using a language which has an English-like syntax, though highly restricted and formalized. The sentences are denoted as S-expressions with explicit parse-trees. A large vocabulary of terms are defined for expressing things that IDS systems might need to talk about (files, processes, network packets, etc). The semantics of these terms is expressed in English (as opposed to using logic, for example). Additionally, CIDF defines an encoding for expressing these sentences in a compact way, and protocols and APIs for exchanging them.

I'll talk about what is hard about doing this. Defining a common syntax, encoding, and protocols for exchange is easy. There are many fine solutions. What is hard is agreeing on the semantics of language vocabulary. In CIDF, this means agreeing on an ontology for the computational world that IDS systems observe and report on. This is very hard. The design of this language has changed continually through out the life of the CIDF working group, and while the current version is a vast improvement on early versions, it retains some ambiguities. Also, while CIDF was designed to be extensible by adding new vocabulary, it appears that extensions never get easy. Since most of the work is vocabulary design, it's always a substantial effort to extend the language to a new domain.

The IETF working group is targeted to developing an Internet standard for alert messages from IDS systems. Thus the scope is much more limited than that of CIDF, and the focus is real world use, rather than research. The group is at an earlier stage in its development, so there is less to say, but I'll briefly overview the requirements and early design work that has been done.

I'll also briefly give some observations on the group dynamics involved in consensus working groups, and how those sometimes benefit and some times detract from the technical work being performed.

Stuart Staniford-Chen --- President --- Silicon Defense
stuart@silicondefense.com
(707) 822-4588 (707) 826-7571 (FAX)