Security Protection and Management (SPAM) Working Group

Dated 4/24/2003

The information provided below is subject to change and reflects the current knowledge of the Working Group.

Management Problem(s) and Environment	Security of a host, network device, or network can be addressed in a number of ways. Some examples include scanning for known vulnerabilities, applying patches to operating systems or other software, determining a violation of security policy, monitoring and analyzing network traffic, and protecting the host or device against intrusions or viruses. Products and services that help to ensure a secure computing environment create additional management challenges to network and security administrators and architects. In many cases, effective security measures require interactions between the products and services, such as timely updates of security information and content, collection and aggregation of event data, analysis and correlation of related and causal data sets. Customers of security products deploy sensors, scanners, and blocking technologies from many vendors. Standards for the modeling of these technologies, semantics of security events, remediation of and response to security incidents can improve the interoperability and manageability of these products and services. Meaningful analysis and interpretation of data consumed and produced by the technologies is vital for evidentiary purposes, service level agreements, and integrity of a network or eCommerce environment. Managed security services, security operations centers, and security management products can all benefit from this standardization for their customers.
WG Charter	The Working Group will define a CIM Common Model that addresses security protection and detection technologies, which may include devices and services, and classifies security information, attacks and responses. Technologies may include but are not limited to firewall, intrusion detection, vulnerability assessment, and antivirus functionalities. Network protocols include but are not limited to IP and Fibre Channel. Other DMTF workgroups address the problem of managing systems in more general ways. The goal of this workgroup is to ease the manageability of heterogeneous security systems within an enterprise or service provider environment, and to enhance the management of these systems from a security perspective.
Alliance Partnerships	None at this time.

Reliance/Coordination with other WG Models	The SPAM working group complements many DMTF work groups. Specifically, the Systems and Devices and Networks groups will be consulted when considering firewalls and security appliances since existing work in this group may be referenced or extended. The User and Security WG develops models for user identity and access control. Security protection also means access control, and any protection mechanisms that are defined will link back to the User Model. Schema for access violations, authorization changes, etc. will relate to this model as well. The Policy WG develops models for policies that can be used for security policy, such as firewall rules and remediation actions. The Events WG models events and alerts that will be used as the basis for standardized alert reporting. Lastly, the Application WG develops models for metrics and application deployment and runtime management. Application security and hardening will be coordinated with this group.
Prior Work	In executing this work, particular attention will be paid to existing and developing standards in the industry (such as IETF's Syslog, INCH, and IDWG efforts, CVE and CIEL from Mitre). In particular, the IDWG has drafted a schema and data format for intrusion detection system events and alerts, and the INCH has created schema and data formats for exchange of security incidents. These schema and data formats could benefit from using CIM, rather than a one-off approach to modeling of security data and relationships. The Working Group will assemble a list of pertinent standards and attempt to incorporate them or establish liaison relationships as necessary.
Current Work – Overview, Deliverables and Timeline	At the outset the WG will focus on IP networks and define schema and its recommended usage for: - Antivirus, Content Filtering, Intrusion Detection, Firewall event model and Alert Indications - Firewall configuration model - Naming and identification of IDS, Antivirus, Vulnerability and Patch signatures - Application hardening (constraints inherent to an application) Work in these areas will be done in parallel with subteams concentrating on each area. A document for the first draft of requirements will be delivered in Q2 CY2003. At the end of Q3 CY2003 and before CIM 2.9 goes final, the Event, Alert Indications, Firewall Configuration, and Naming Models will be completed.
DMTF Contacts	WG Chair Paul Agbabian, Symantec Corp. pagbabian@symantec.com
Link to Subteam Charter(s)	Not applicable

To join the DMTF and/or the WG, see http://www.dmtf.org/join/index.php and http://www.dmtf.org/apps/org/workgroup/technical/spam.