Click here to view PowerPoint presentation; Press Esc to exit

IRONMAN V 1.5 — Network Management Environment

Milan Kuchta
Systolics Ltd.
4120K Riverside
Ottawa, Ontario K1V 1C4
Canada

The recognition of the importance of defensive capabilities against intrusion into enterprise networks has increased over the past decade. Governments around the world have become aware, sometimes dramatically, that their internet-based information and support systems are subject to intrusion and compromise. Within industry, proprietary corporate information is accessible through the intranet-to-internet gateways. Although firewalls, encryption and other existing techniques have provided some protection, they have also provided restrictions on corporate use of the internet resource and have not fully succeeded in preventing intrusions.

Numerous excellent commercial and academic efforts have resulted in vulnerability scanning, intrusion detection and network management applications and products.

Unfortunately, only a few of these are efficient or scaleable in very large heterogeneous enterprise environments and none provide a comprehensive management environment .

IRONMAN is a system which is being developed and used to integrate academic and commercial tools providing network discovery/scanning, intrusion detection and management capabilities. Added to these tools (and enhancements to them) are a data visualization environment, modeling, analysis and reasoning tools, and a policy management framework. It is a prototype environment designed to provide interactive management of networks and network components and services. Interaction is provided through a VRML 2.0 3D virtual environment and through additional extended controls such as forms and dialog boxes. VRML 2.0 provides a framework for dynamic visualization of information and systems.

The IRONMAN modeling framework uses an underlying ontological framework which supports a wide variety of reasoning tools to provide for policy based modeling, analysis and control. Through indigenous capabilities and the integration of third-party commercial and custom applications, IRONMAN provides both passive monitoring and active probing of networks and their components.

IRONMAN uses a virtual common data repository model for all information sources. This provides for integration of existing databases and new associative information servers and can support collaborative workspaces.

IRONMAN is based on existing software, hardware and networking standards wherever possible and is currently implemented as a layered client-server architecture. The primary client host is a WWW browser (e.g. Netscape) and the servers primarily use the CGI (Common Gateway Interface) model. The design provides for integration of mobile and transportable agents.

The IRONMAN functional architecture has seven main functional areas:

- acquisition :- this is the set of functions used to obtain data from elements of the system. The functions are provided by scanners, intrusion detection systems, SNMP, sniffers, and other various applications;
- control :- this set of functions is used to change some aspect of the system being managed or IRONMAN parameters and configuration;
- representation :- the representation functions deal with the syntactic and semantic forms of data and information related to a managed system and where and how data and information is stored and accessed;
- presentation :- the set of functions which deal with how data and information is structured and displayed to the user and the means of interacting with the data and with the system which the data represents;
- analysis :- the set of functions which process the available data to generate subsets, feature sets, statistical characteristics, etc.; and
- decision :- the set of functions which process data to provide a set of branch points which can be acted on using control functions.

Information Operations (IO) concepts are being actively explored by a number of organisations including Departments of the Government of Canada. The defensive aspect of IO is supported by IRONMAN concepts and facilities. However, IRONMAN should contribute fully to attack facilities and scenarios that are needed to stress test information technology systems presently deployed as well as those facilities that will be deployed in the near future as part of an information system architecture.

Paper presented at the RTO IST Workshop on "Multimedia Visualization of Massive Military Datasets", held in Quebec, Canada, 6-9 June 2000, and published in RTO-MP-050.

Discussion – Paper 19

IRONMAN V1.5 – Network Management Environment

Ironman – Network Surveillance Infrastructure

Most work within network security deals with preparing for what could happen rather than sitting back and monitoring the traffic (looking at what is happening). Changes within the information security arena are happening quickly and the infrastructure has to be able to reflect these changes.

Within a network there are a large number of nodes to protect including large numbers of protocols, ports, services and applications. Ironman sits in a network management environment and provides visual and oral sensory stimuli allowing the user a view of both the traffic on the network as well as the systems that are being protected.

It provides the user the ability to define a policy region within 3d space allowing the user to easily see if certain nodes have not implemented the policy correctly. Ironman also fuses and manages sensors as well as analyzing, collecting and storing data, giving the user a variety of ways of viewing it. It aids the user in capturing highly transient events such as port scanning by different machines over time. Scenario generation and detection, risk analysis etc. can be modeled within this environment.

Research in this area has thrown up a number of questions:

Is familiarity or efficiency better within visualisation?
Is visual literacy something that is learnt? If so is it the skill of the writer or that of the reader that is important?
When a system is first presented, then changed at a later date how confusing is it to the user? How much does a user imprint on the first visualisation?

Audience discussion:

1. Have the displays within Ironman been evaluated?

   No formal evaluation has happened, though a prototype system is being installed within the Information Operations team at DREO and feedback is expected on the system. Further evaluation on the visualisation will be happening within the next year. It is important to keep the correct balance between what is possible with visualisation technology and what is the sensible visualisation to use. Sets of trial ideas are needed to test what is possible to do – what are the limits etc.

2. Measuring the user response to the Ironman environment.

The user is encouraged to navigate through Ironman, though it is difficult to find a way of measuring how people navigate through virtual space.