CATCHING THE CYBER SPY:
ARL’S INTERROGATOR

Kerry S. Long*
U.S. Army Research Laboratory
Computational and Information Sciences Directorate
Aberdeen Proving Ground, MD 21005-5067

ABSTRACT

The U.S. Army Research Laboratory has designed a network-based intrusion detection framework, Interrogator, which addresses the constantly changing threat environment that Department of Defense networks are already facing, while providing a frame work that encourages further innovation in intrusion detection. In Interrogator, intrusion detection systems sensors, or Gators, are essentially dumb devices that monitor a network segment and transfer a subset of raw network traffic back to a central repository. Relevant network raw data can now easily be made available to both intrusion analysts and researchers for examination, experimentation, and development of better detection methods decoupled from the complexities of collecting the data.

2. ARCHITECTURE

In Interrogator, IDS sensors, or Gators, are essentially dumb devices that monitor a network segment and transfer a subset of raw network traffic back to a central repository. Relevant network raw data can now easily be made available to both intrusion analysts and researchers for examination, experimentation, and development of better detection methods decoupled from the complexities of collecting the data. To aid current detection operations, data in the central repository is automatically processed by one of several IDS tools. The output of the IDS tools are inserted into a “detects” database where the results are correlated and displayed for incident analysts to view. Additional IDS algorithms or interface components can be added to the architecture quickly. Obsolete pieces can be replaced just as quickly. Raw network data is immediately available to corroborate any intrusion alert and to serve as required evidence for law enforcement officials or senior decision makers.

The Interrogator architecture designates five levels that perform data capture, processing, storage, retrieval, and presentation. Each level defines a standard for how data is to be passed to that level, and depends on the lower levels only in this regard. Lower levels can implement any software, methods of data processing, or hardware as long as the data is passed to the next level in the defined format. This allows changes at any level to be implemented or altered as needed, while minimizing the impact on the other levels. Additionally, there is a management layer that spans the four lower levels. This provides both status information and automated recovery in case of disconnection between levels.


---

Catching The Cyber Spy: ARL’s Interrogator

U.S. Army Research Laboratory Computational and Information Sciences Directorate Aberdeen Proving Ground, MD 21005-5067

See also ADM001736, Proceedings for the Army Science Conference (24th) Held on 29 November - 2 December 2005 in Orlando, Florida.
The architecture is pictured in figure 1.

![Interrogator architecture](image)

Figure 1. Interrogator architecture.

The Interrogator architecture components are:

1. **Sensor level.** The sensor is treated as a simple data collection appliance.
2. **Analysis level.** The analysis of raw data collected from the sensors is performed at a centralized location.
3. **Database level.** A relational database collects IDS reports, detects data, incident reports, and host status.
4. **Application level.** A Java servlet application allows analysts full access to the database and collected raw data.
5. **Client level.** A web-based user interface presents the data to analysts, allowing them to file reports, and to drill down into raw data as needed.
6. **Host management.** The management function spans the first four levels to provide simplified management and automated recovery.

**CONCLUSION**

The requirements for effectively securing DoD data are much more stringent than are supported by the current state of the art in network intrusion detection systems. ARL has gained experience from performing intrusion detection operations that has led to an understanding of the need for integrated analysis capabilities to meet those requirements. This experience led to the design of an architecture that provides dynamic modularity, the ability to incorporate new technologies into the system without interrupting day-to-day analysis operations.