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.

1. INTRODUCTION

In April of 2000, a report was published for the Association of Computing Machinery that blasted the state of intrusion detection systems (IDS) as "not technically advanced enough to detect sophisticated cyber attacks by trained professionals."[1] The same article went on to detail that "next-generation cyberspace intrusion detection systems will require the fusion of data from myriad heterogeneous distributed network sensors to effectively create cyberspace situational awareness."

The U.S. Army Research Laboratory (ARL) determined that an IDS architecture needs to be developed for the Department of Defense (DoD) to address the challenges set out in this report. ARL plans to develop an IDS architecture that allows current operational analysts to detect sophisticated cyber attacks across multiple sensors, while providing researchers and developers the means of easily experimenting with and implementing new detection methods and tools. Only in this way will the DoD be able to defend itself from an ever changing and growing cyber threat. Interrogator is ARL's attempt to achieve both objectives in a single IDS framework.

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. This data transfer has the potential to consume large amounts of precious network bandwidth. However, bandwidth utilization is minimized though the use of a steady stream trickle feed mechanism and a dynamic network traffic selection algorithm called Snapper. 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.

[1] Bass, T. *Intrusion Detection Systems and Multisensor Data Fusion,* Communications of the Association for Computing Machinery: 99-105. ACM Press. April 2000.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **00 DEC 2004**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE
Catching The Cyber Spy: ARL's Interrogator

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Research Laboratory Computational and Information Sciences Directorate Aberdeen Proving Ground, MD 21005-5067

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM001736, Proceedings for the Army Science Conference (24th) Held on 29 November - 2 December 2005 in Orlando, Florida.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**2**	

The architecture is pictured in figure 1.

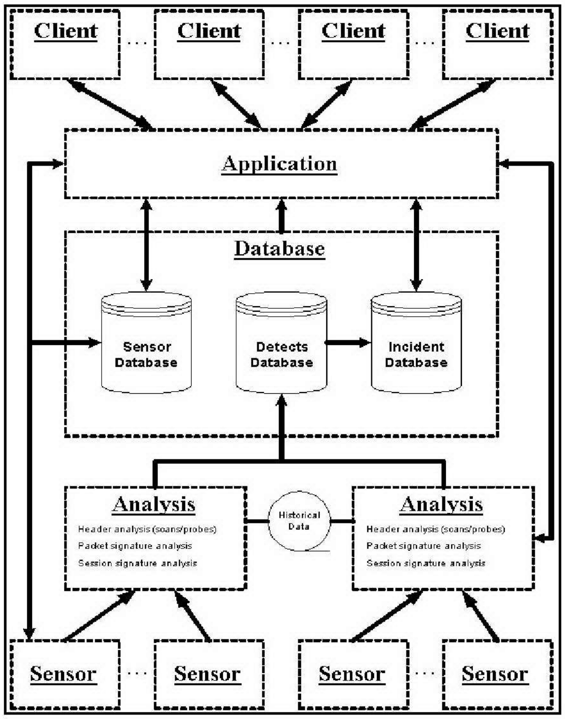
Client
Client
Client
Client
Application
Database
Sensor Database
Detects Database
Incident Database
Analysis
Header analysis (scans/probes)
Packet signature analysis
Session signature analysis
Historical Data
Analysis
Header analysis (scans/probes)
Packet signature analysis
Session signature analysis
Sensor
Sensor
Sensor
Sensor

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 servelet 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.