

A Data Fusion Model for Information Operations

Kevin L. Fox and Ronda R. Henning

Harris Corporation, Government Communications Systems Division

1.0 Purpose

The correlation of vulnerability information from disparate sources has long been an issue in information assurance research. Data on known vulnerabilities, system configurations, audit trail entries, and network traffic all need to be examined to determine if a concerted attack signature is in use. In some regards, this problem is very similar to the problems associated with traditional intelligence data fusion models and applications. Traditional data fusion addresses the correlation of information from sources as diverse as single-purpose sensors to all source media information. Information assurance vulnerability information is similar in its diversity of sources and content, and in the desire to draw a meaningful near real time conclusion. This paper presents a data fusion model that is being applied to vulnerability correlation and fusion for information assurance purposes.

2.0 Method

This data fusion model developed as a result of a research program on vulnerability correlation. Various techniques for data correlation were explored, including traditional mathematical models, expert reasoning, and fuzzy logic. While each of these techniques worked well for their intended problem set, they did not adequately address the overall problem. Some synthesis technologies were well adapted for low-level information, others, for higher-level conceptual data.

In the course of this analysis, the analogy began to emerge between a traditional intelligence data fusion process model and the problems faced in information assurance. Namely, the correlation and fusion of computer network vulnerability information from a variety of disparate sources. When vulnerability data was characterized in a multi-phased model, it was not only more amenable to analysis, but also more efficient from a data correlation perspective in terms of system performance and the structuring of knowledge-based processing support..

3.0 Results

Our research has resulted in a four-stage model of vulnerability fusion. This model is designed to reflect the global nature of a large enterprise, the increased dependence on internetworks of information, and the vulnerabilities associated with individual network segments and devices. The model has been successfully applied to static vulnerability analysis, and has been integrated with current vulnerability assessment technologies for vulnerability identification and correlation.

4.0 New or Breakthrough Aspect of Work

To date, traditional intelligence data fusion process modeling techniques have not been applied to the information assurance/operations disciplines. However, several calls for research have noted the problems of integrating disparate data sources into a common operational picture or situational assessment. To the best of our knowledge, interdisciplinary research between the data fusion community and the information assurance community has not been previously undertaken. The adaptation of traditional data fusion techniques to the information assurance correlation problem offers a potentially high payoff in the field of system vulnerability analysis.

5.0 Conclusions

Data fusion correlation process models share several similarities with the complex nature of information assurance vulnerability analysis. Through the decomposition of vulnerability data to reflect a multi-stage analysis model, our work has simplified the correlation problem to relatively manageable proportions. Our analysis model has been successfully prototyped, and is under further development. This model mirrors the multi-stage intelligence data fusion process model, and is presented in this paper. Our current research emphasizes model scalability to a large enterprise to determine the efficiency of our correlation techniques.