

Developing Secure Simulation Software For Multinational Use

John A. Hamilton, Jr., Ph.D.
Department of Computer Science and Software Engineering
Auburn University
107 Dunstan Hall
Auburn University, Alabama 36849
E-mail: hamilton@eng.auburn.edu

Keywords:
Simulation, Data Fusion, Ontology, Software, Vulnerability, Open Source

ABSTRACT: *Can a simulation be too good? Normally simulation designers are concerned about the validity and fidelity of their models. However, unclassified simulation models combined with accurate parameters from open sources can yield sensitive results. Ontological-based search methods can increase the confidence of open source searches for sensitive parametric data. This paper will address simulation vulnerabilities in the domain of missile defense and outline how the construction of appropriate ontologies can increase the assurance provided during open source searches for sensitive parametric data.*

1. Introduction

The need for simulation software vulnerability assessment is being driven by three major trends: Increased use of modeling and simulation for training and operational planning; increased emphasis on coalition warfare and interoperability and finally increased awareness of the potential security risks inherent in sharing operationally useful software.

Computer modeling of defense systems and strategies has become an important part of the modern military. In an era where coalition warfare is the rule rather than

the exception, it is increasingly common to share models and simulations with Allied countries. These models also make an attractive offering when entering into partnerships with other nations for research or strategic benefit. Unfortunately, the sharing of this software has been undertaken without a thorough understanding of the potential risks, chief being the possibility that the foreign power will try to use the software to gain unauthorized knowledge of US weapons, tactics, and procedures.

Consider the construction of a typical simulation as outlined in Figure 1:

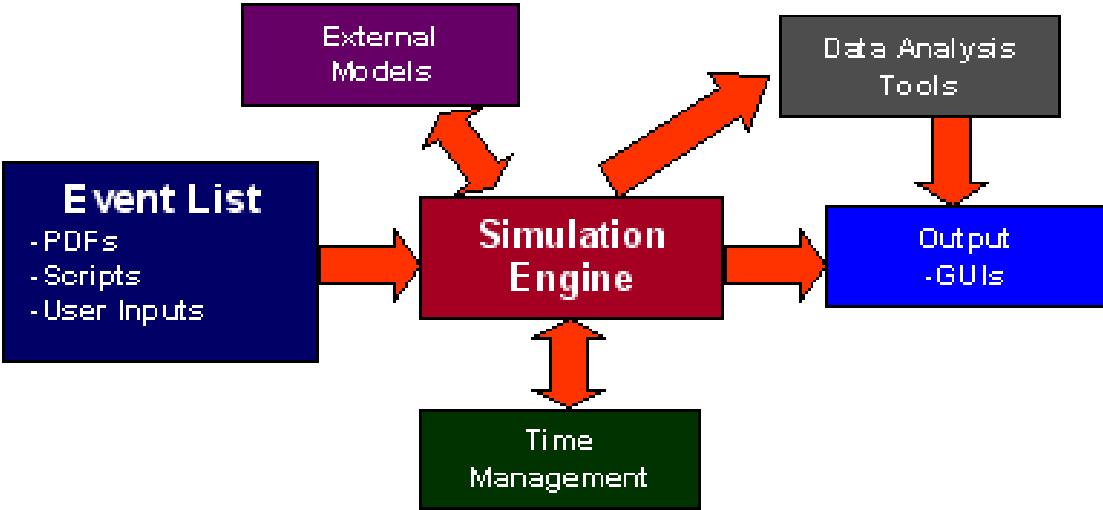


Figure 1. Inputs and Outputs to a Simulation Engine

In the missile defense simulation community, great care has been taken to parameterize all sensitive data. In theory, an unclassified simulation engine with unclassified inputs should only be able to produce unclassified outputs. As shown below in Figure 2, only classified inputs should produce classified outputs.



Figure 2. Classified and Unclassified Inputs

To illustrate the potential use of ontologies in vulnerability analysis, the next section illustrates the use of open source information in an attempt to simulate current US weapons systems and produce sensitive results. The ability to use web-based open sources to derive classified information is described by Farkas and Huhns [1].

Parametric information about the specifications of the Patriot Advanced Capability Level 3 (PAC-3) and the SCUD-B was gathered to create a scenario in which a PAC-3 system attempts to defend itself against a SCUD attack. The purpose of the information gathering was not to conclusively find all relevant web-based information on either the PAC-3 or the SCUD-B. Rather, the purpose was to locate the parameters necessary to load a useful simulation model.

2. Research Methodology

Our methodology to simulate the Patriot Advanced Capability Level 3 (PAC-3) engaging simulated SCUD-B ballistic missiles [2]. The process for carrying out this simulation was broken into several steps as follows:

1. Determine the information required
 - For a surface-to-air missile (SAM)
 - For a ballistic target
2. Gather Data
3. Develop a method to organize and store information acquired during the open source search
4. Conduct a search of Internet and published sources to acquire as much information about the PAC-3 and SCUD-B in order to create a SAM and ballistic target simulating the real systems
5. Where information cannot be obtained, use existing data in an attempt to infer the value required
6. Where information cannot be inferred, look to sample systems included in the simulation package for possible values
7. When the above steps fail, use the defaults provided in the model or attempt to make a reasonable guess

8. Set up a simulation involving a surface-to-air missile launcher and a ballistic missile launcher
9. Configure the weapons according to information gathered in the open source search
10. Run the simulation

The simulation package itself was used to list the parameters required to simulate both a SAM and a ballistic target. The demo simulation includes ballistic missiles and SAMs capable of shooting them down.

An Excel spreadsheet was created for each type of weapon. These spreadsheets were then populated with a list of the parameters required for the weapon as well as the values used by a sample weapon included in the simulation that was selected as a model for the real (PAC-3/SCUD-B) system being modeled.

2.1 Parameters Common to PAC-3 and SCUD-B

Several simulation parameters are common to both PAC-3 and SCUD-B weapon simulations as shown below.

- Lethality
- Lethal radius
- Probability of kill
- Flight Characteristics
- Maximum range
- Velocity
- Reliability statistics for each stage of flight

2.2 PAC-3 Simulation Parameters

Information required specifically for SAM-type weapons like the PAC-3 that is not included in the information common to SAM and ballistic targets primarily deals with information about the guidance system of the weapon. These guidance parameters consist of the following information:

- Method of guidance (command or active/IR)
- Frequency of guidance updates
- Range/time when each method of guidance is used

2.3 SCUD-B Simulation Parameters

Information specific to ballistic targets like the SCUD-B consists of information used in calculating the weapon's ballistic characteristics. The information requested includes the following:

- Circular Error Probable (CEP)
- Flight parameters for each stage of flight
- Vacuum thrust
- Mass flow rate
- Nozzle exit area
- Reference area

- Section dry mass
- Section fuel mass
- Lift and drag information at various speeds
- Infrared signature information at each stage of flight
- Radar cross section information for each stage
- Guidance Parameters
- Pitch angle
- Pitch rate
- Gravity turn
- Missile guidance (i.e. lofted or depressed trajectory et cetera)
- Maximum angle of attack
- Initial velocity
- Re-entry altitude
- Attitude control information

2.4 Organizing and Storing the Open Source Information

A major part of the research project is to collect and organize information about the PAC-3 and other US anti-ballistic missile systems. In order to accomplish this, a web-based database was created to allow all researchers to collaborate in collecting and storing information. This database records the date the information was entered, the system to which it pertains, the location of the information, a summary of the important data from the source, and the researcher who located the data.

2.5 Locating Parametric Information on PAC-3

Unfortunately, much of the data required to establish the flight parameters for the PAC-3 appears to be available on the Internet [3, 4]. The following information was found that pertains to the performance of the PAC-3:

- Maximum Range: 70km
- Minimum flight time: 9sec
- Maximum flight time: less than 3.5 minutes
- PAC-3 hit 8 of 9 targets in body-to-body kill tests
- Maximum radar range: 100km
- Maximum altitude: >24km

We believe only two categories of information related to simulating the PAC-3 that would be difficult for a foreign power to locate in open source information or to calculate from other information at hand. These are:

1. Reliability Information
2. Guidance control information including”
 - How frequently the missiles guidance is corrected by ground command
 - The time to intercept or range to intercept at which the missiles internal guidance takes control from the ground station

- The frequency of guidance corrections by the missiles internal guidance system

With sufficient observation of tests or usage of the PAC-3 in actual combat, it may be possible to calculate the reliability information for each stage of the missile’s flight. It may also be possible to calculate this information if news organizations report on the success or failure of the PAC-3 in a combat scenario.

It seems, however, that this information is among the least important information to have correct in order to simulate the PAC-3 with a reasonable degree of accuracy. In either case, a hostile power would probably overstate rather than underestimate the capabilities of the PAC-3 simply by using assuming 100% reliability at all stages of flight and taking conservative guesses as to the guidance control parameters.

2.6 Locating Parametric Information for SCUD-B

Significantly more information is required in order to simulate a ballistic weapon such as the SCUD-B. However, because of the wide usage of the SCUD and the considerable period of time that the SCUD-B and related variants have been in production it is relatively easy to obtain somewhat detailed information about the SCUD-B. Of course we would expect a foreign power to use information about their own ballistic weapons if they were attempting to use a US simulation to simulate the performance of their own weapons against US systems.

As a result of the work described in the previous section, it is clear that web-based open source information can be used with unclassified simulation models to produce results that can be indistinguishable from results produced using classified parameters. One additional point should be made about the vulnerability analysis just described. The research sponsor has deemed it prudent to restrict release of the details of our work. (A prudent measure which we fully support).

3. Ontologies and Search Engines

Vulnerability assessment is a high priority for the United States. Red teaming, the search for vulnerabilities, is one of five major initiatives in the Office of Homeland Security’s *National Strategy for Homeland Defense* [5]. Given the national importance given to this topic, we believe it is reasonable to look for ways to increase the assurance of open-source searches of web-based information.

Raskin et al [6,7] address the use of ontology in information security. Consider the following simple

structure they use to illustrate the construction of ontology in Figure 3.

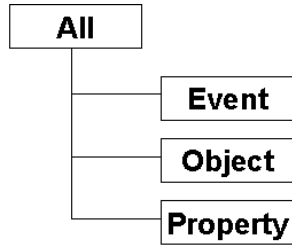


Figure 3. All tree, one level down

It is easy to see that on-line parametric data such as that described in the previous section could increase the assurance of the effectiveness of open source searches. The creation of a formal hierarchy of parameters would permit the use of formal methods and constraint satisfaction strategies as outlined by Brodsky, Farkas and Jajodia [8].

One potential high-level ontological mapping of missile defense related parametric data is shown in figure 4.

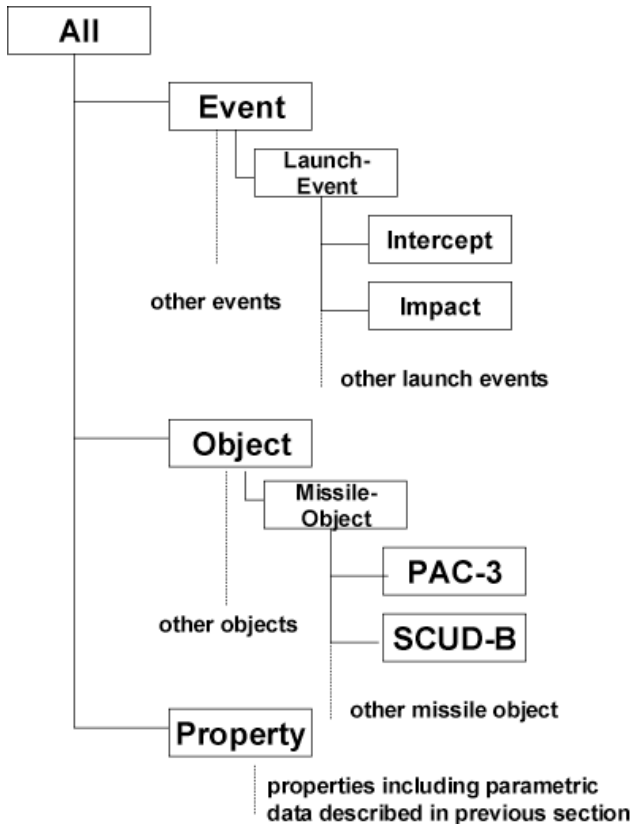


Figure 4. Partial missile defense ontology

Each missile object has related events and related properties. Imposing a structure upon these properties

can aid in the systematic evaluation of available on-line parametric data.

The desired end-state is a proactive means of data fusion for threat assessment. There exist many definitions for data fusion. A common DOD definition of data fusion is, “is a multilevel, multifaceted process dealing with the automatic detection, association, correlation, estimation, and combination of data and information from multiple sources [9].” Wald himself proposes a more general definition that fits our concept of ontology to support on-line open source searches. “Data fusion is a formal framework in which are expressed the means and tools for the alliance of data originating from different sources. It aims at obtaining information of greater quality; the exact definition of ‘greater quality’ will depend upon the application [10].” This definition describes our strategy for developing ontological search methods to support open source parameter searches.

An ontology is merely a means of classifying information. But given the overwhelming amount of data available on-line from open sources, some means of classifying this data is necessary for any meaningful threat assessment.

4. Conclusions

Simulation parameters discovered through on-line open source search can be used with an unclassified simulation to produce classified results. Given the demonstrated risk as well as the national call for continued vigilance in the area of open source analysis is necessary

Given the importance of open source analysis as outlined in the *National Strategy for Homeland Defense*, there is strong motivation to increase the degree of assurance in open source on-line searches.

Currently, much on-line open source analysis is done manually. We believe that ontological-based search methods are an enabling technology to support simulation vulnerability analysis through data fusion.

Finally, we argue that open source parameters must be considered in the development and deployment of military simulations, particularly if international release of the simulation is contemplated.

6. Acknowledgement

This ongoing research is supported by the Department of Defense under National Science Foundation contract NSF-EEC-9907749-D.

5. References

- [1] Farkas, Csilla and Huhns Michael N., "Making Agents Secure on the Semantic Web," *IEEE Internet Computing*, Nov.-Dec. 2002, pp 76 – 79.
- [2] Peters, Marcus P., Chatam, Wade and Hamilton, John A., Jr., "Simulation Exploitation Using Open Source Information," *Proceedings of the Advanced Simulation Technologies Conference*, Orlando, Fla., 30 March – 3 April 2003.
- [3] Missile Defense Agency. 2002. *MDA Fact Sheet: Terminal Phase Missile Defense*.
www.acq.osd.mil/bmdo/bmdolink/pdf/terminal.pdf.
MDA External Affairs, Washington, D.C.
- [4] Net Resources International. 2002. *Patriot Air Defense System*. www.army-technology.com/projects/patriot/. London, England.
- [5] Office of Homeland Security, *National Strategy for Homeland Defense*, The White House, Washington, DC, July 2002, p 7.
- [6] Raskin, Victor, Nirenburg, Sergei. Hempelmann, Christian F. and Triezenberg, Katrina E., "Ontology in Information Security: A Useful Theoretical Foundation and Methodological Tool,"
- [7] Raskin V., Atallah, M., McDonough, C. and Nirenburg, S., "Natural Language Processing for Information Assurance and Security: An Overview and Implementations," *Proceedings of New Security Paradigms Workshop*, Cork, Ireland, 19 – 21 September 2000.
- [8] Brodsky, Alexander, Farkas, Csilla and Jajodia, Sushil, "Secure Databases: Constraints, Inference Channels, and Monitoring Disclosures," *IEEE Transactions on Knowledge and Data Engineering*, vol 12, no 6, Nov-Dec 2000, pp 900- 919.
- [9] Wald, L.; "Some terms of reference in data fusion," *IEEE Transactions on Geoscience and Remote Sensing*, Volume: 37 Issue: 3, May 1999, pp 1190 -1193
- [10] Wald, L., "A New Definition of Data Fusion," online essay, <http://www.data-fusion.org>, 27 August 2001.

6. Biography

John A. "Drew" Hamilton, Jr., Ph.D., is an associate professor of computer science and software engineering at Auburn University. He has a B.A. in Journalism from

Texas Tech University, an M.S. in Systems Management from the University of Southern California, an M.S. in Computer Science from Vanderbilt University and a Ph.D. in Computer Science from Texas A&M University. Prior to his retirement from the US Army, he served as the Chief of the Ada Joint Program Office, the first Director of the Joint Forces Program Office and on the Faculty of the United States Military Academy. CRC Press publishes his book, *Distributed Simulation*, written with LTC David A. Nash and Dr. U. W. Pooch.