

SIMULATION EXPLOITATION USING OPEN SOURCE INFORMATION

Marcus P. Peters, Wade Chatam and John A. Hamilton, Jr., Ph.D.

Department of Computer Science and Software Engineering

Auburn University

107 Dunstan Hall

Auburn University, Alabama 36849

E-mail: mark@marcuspeters.com

chatajw@eng.auburn.edu

hamilton@eng.auburn.edu

Keywords: Simulation, Software, Vulnerability, Open Source

ABSTRACT

Computer modeling of defense systems and strategies has become an important part of the modern military. 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.

Because simulation software is sometimes exported to foreign countries, extreme care must be taken to ensure that sensitive information is not released along with it. This can prove to be a difficult task considering that the documentation alone totals over a thousand pages. While it may seem that the user manuals are completely benign, certain calculations are included that could prove otherwise when combined with the results of the program execution.

This paper focuses on the use of open source information in an attempt to simulate current US weapons systems using a sensitive missile defense simulation, specifically the Patriot Advanced Capability Level 3 (PAC-3). Parametric information about the specifications of the PAC-3 and the SCUD-B was gathered in an attempt to create a scenario in which a PAC-3 system attempts to defend itself against a SCUD attack.

It appears that enough data was gathered about the SCUD-B to make reasonable guesses about the performance about that system. Less information was found about the PAC-3, but it appears to be sufficient to produce a relatively simple simulation of the PAC-3, although the accuracy of the simulation cannot be known, as the classified performance data is not available for this research.

RESEARCH METHODOLOGY

In an attempt to quantify the risk that the simulation might be used to simulate US weapons systems it was decided to attempt to simulate the Patriot Advanced Capability Level 3 (PAC-3) engaging simulated SCUD-B ballistic missiles. The process for carrying out this simulation was broken into several steps as follows:

- Determine the information required
 - For a surface-to-air missile (SAM)
 - For a ballistic target
- Gather Data
 - Develop a method to organize and store information acquired during the open source search
 - 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
 - Where information cannot be obtained, use existing data in an attempt to infer the value required

- o Where information cannot be inferred, look to sample systems included in the simulation package for possible values
- o When the above steps fail, use the defaults provided in the model or attempt to make a reasonable guess
- Set up a simulation involving a surface-to-air missile launcher and a ballistic missile launcher
- Configure the weapons according to information gathered in the open source search
- Run the simulation

DETERMINING WHAT INFORMATION IS REQUIRED

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.

Simulation Parameters Common to PAC-3 and SCUD-B

Significant portions of the simulation parameters are common to both PAC-3 and SCUD-B weapon simulations. These include information such as the following:

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

Simulation Parameters Specific to PAC-3

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

Simulation Parameters Specific to SCUD-B

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
 - o Vacuum thrust
 - o Mass flow rate
 - o Nozzle exit area
 - o Reference area
 - o Section dry mass
 - o 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
 - o Pitch angle
 - o Pitch rate
 - o Gravity turn
 - o Missile guidance (i.e. lofted or depressed trajectory as well as others)
 - o Maximum angle of attack
 - o Initial velocity
 - o Re-entry altitude
 - o Attitude control information

GATHERING INFORMATION

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.

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. 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

[Missile Defense Agency 2002; Net Resources International 2002a; Net Resources International 2002b].

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:

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

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.

While it is valuable to simulate a SCUD for the purposes of academic testing of the program, the actual data produced by that simulation is of only questionable value. The most reasonable course of action for a foreign power would be 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.

SIMULATION OF A PAC-3 INTERCEPTING A SCUD-B ATTACK

Using the data gathered and inferred from open source information a simulation was set up to pit a simulated PAC-3 battery against an attack by several simulated SCUD-B's. If a piece of data required by either system was not available through the information search, either the default value was used or a guess was taken as to a reasonable input.

The only problem discovered while running the simulation is that the value discovered in the information search for the SCUD-B's thrust might be incorrect. The value determined from the open-source search was approximately 93,000N [Wade 2002]. When this value is used, the simulation fails to complete its run. A value of 100,000N causes the simulation to complete, but the missiles fail to leave the launch platform. A value 125,000N allows the missiles to launch and be able to reach their target. Values between 100,000 and 125,000N were not tested.

The simulation uses an attack by 17 simulated SCUD-B's against a PAC-3 battery with 16 interceptors. The Patriot battery successfully intercepts 14 of these missiles, but there are two misses and, of course, an insufficient quantity of interceptors to target all 17 SCUDs.

REVIEW OF INCLUDED DOCUMENTATION

Preparing proper documentation for a large-scale mathematical model is, at best, difficult, time-

consuming, and expensive. “Explicit descriptions of model minutiae, supporting analyses, and modes of operation may require a more comprehensive grasp of the principles of the model and their realization than does the model’s actual development [Gass et al. 1981].” Considering the complexity of missile defense simulations, the documentation could very easily become unguarded. With a large document, it is very difficult to ensure that all information is secure. A major problem arises in the authors’ abilities to keep track of the others’ work. One writer could mistakenly assume that some information is unclassified and include it in his/her portion of the documentation. Others could include information that is not necessarily classified but would allow classified information to be derived from it. One such example is given in [Jonsson, Stromberg, and Lindskog 2000]. “Anderson describes a back door for an ATM system. The back door was a 14-digit number that forced ten banknotes to be paid out. The introduction of such a number, or rather the fact that it was not taken away during initial installation, constituted a vulnerability. As a matter of fact, this number was documented in the maintenance manual, which was an error manifested in the documentation. The error propagated when a former maintenance engineer, in desperate need of money, recalled the number and started to make withdrawals from various ATM machines.”

In order to conduct a vulnerability analysis, one must know what information is classified and what is not. Certain details that may appear to be secret could actually be considered common knowledge. For example, the calculations for determining a missile’s trajectory are explained in detail in the simulation reference manual. Often the calculations for determining the impact of a blast based on the particular size and type of warhead is provided with the software.

The reason for releasing this information is that the calculations involve nothing more than math and physics. The results produced by the simulations we studied are easily calculated for a given input with or without the accompanying reference manual. For a missile of size X carrying warhead Y, the blast impact can be determined using unclassified information.

The actual sensitive information lies within the specifics of the missiles. The United States

government does not release the size and type of warhead on its missiles. If the program does not actually know the exact specifications of the missile, it theoretically cannot perfectly calculate its ability.

This is where the sensitivity of the simulation lies. If the user inputs his/her own data, will there be any results in the output that cannot be determined using only the math? This is the type of data that could lead to sensitive information being derived from the software.

CONCLUSIONS

The data produced by the open source search seems to allow for a reasonable simulation to be produced. Due to US military classification of missile performance characteristics and not having access to official SCUD-B performance data, the fidelity of the simulation to a real attack cannot be determined in this research.

In order to truly assess the risk posed by the availability of open source information it would be necessary to compare the best available open source data to the actual performance characteristics of the PAC-3 system. Due to the constraints under which this research has been conducted, it is impossible to perform this comparison at this time. It is advised that the US government conduct this comparison on its own in order to determine the accuracy of the open source information.

If it is shown that the openly available information regarding the PAC-3 is reasonably accurate then the threat of using US simulations to simulate US weapons systems is quite high. However, even if the open source information is not accurate, it appears that the only hinderance to a foreign power using US simulations to compromise US weapons is the lack of accurate information. Many governments are actively engaged in espionage to determine just this type of information so the only safeguard is the continuing secrecy of real performance data. Should this data be compromised then using it within a simulation is relatively trivial.

REFERENCES

Gass, S.I. et al. 1981. Documentation for a Model: A Hierarchical Approach. *Communications of the ACM* 24, no. 11 (November): 728-733.

Jonsson, E., Stromberg, L., and Lindskog, S. 2000. On the Functional Relation Between Security and Dependability Impairments. In *Proceedings of the 1999 Workshop on New Security Paradigm*. (Caledon Hills, CA). ACM Press, New York, NY. 104-111.

Missile Defense Agency. 2002. *MDA Fact Sheet: Terminal Phase Missile Defense*. <http://www.acq.osd.mil/bmdo/bmdolink/pdf/terminal.pdf>. MDA External Affairs, Washington, D.C.

Net Resources International. 2002. *Patriot Air Defense System*. <http://www.army-technology.com/projects/patriot/>. London, England.

Net Resources International. 2002. *Patriot-Specification*. <http://www.army-technology.com/projects/patriot/specs.html>. London, England.

Wade, M. 2002. *R-11*. <http://www.astronautix.com/lvs/r11.htm>.

BIOGRAPHY

Marcus Peters is currently pursuing a Master of Science degree in Computer Science at Auburn University. He earned his Bachelor of Computer Engineering degree at Auburn in 2001. His research interests include computer networking and security.

Wade Chatam is a graduate student in Software Engineering at Auburn University. He received his Bachelors of Science degree in Computer Science from Auburn in 2002. His research interests include information assurance, computer networks, and simulation. Born and raised in Birmingham, AL, Wade plans to earn his Ph.D. in Computer Science and continue researching computer networks and security.

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 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.