The Role of Modeling and Simulation in Information Security
The Lost Ring

Mohammad Heidari
Security.Papers@Gmail.com

Under Supervision of Professor Ghasem Aghaee

Dedicated to the Born of "7 Mordad"

Abstract

There is a spate of papers and tools on using Modeling and Simulation (M&S) for testing Denial of Service- (DoS), virus and worm (Propagation, attacks) against computer networks, but this is not a whole story, there is not any explicit M&S tool for testing computer/network security and network attack modeling. In the other words, it seems that Computer Simulation was studied and investigated in many areas but the field of Computer Security has not produced significant research results in this area to date! It goes without saying that M&S is used to understand and develop complex system, it is used to provide analysis and insight into building better systems. M&S is also an effective tool to save time and money during development and implementation. In the field of Information Security, Models and tools for simulation of computer and network security can facilitate the development of more secure robust and safer computer network infrastructures. Unfortunately, today many computer networks were constructed without any virtually backgrounds in modeling and simulating for testing different kinds of computer network attacks and their impacts on computer and networks. In this paper, I try to explain the applications of M&S for modeling and simulation of computer/network security. This article also tries to analyze the current state of M&S in the field of information security, and presents new suggestions to solve the problems in modeling and simulating in the field of Information Security.
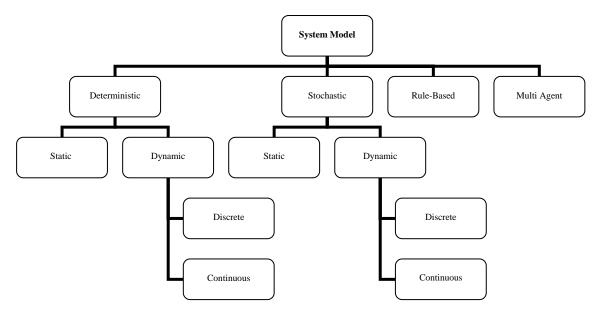
February 3, 2006

Keywords: Modeling, Simulation, Information Security, IWAR, DOS/DDOS

2

1- Introduction to M&S

1-1- Model

A model is a physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process. [1] A system is understood to be an entity which maintains its existence through the interaction of its parts. A model is a simplified representation of the actual system intended to promote understanding. Figure 1 demonstrates the Model Taxonomy, in this figure Models are divided into four major parts: **Deterministic models, stochastic models, Rule based models and Multi-agent models.**

Figure 1: Taxonomy of Models

```
                          ┌──────────────┐
                          │ System Model │
                          └──────────────┘
        ┌──────────────┬──────────┴────────┬──────────────┐
  ┌─────────────┐ ┌──────────┐      ┌────────────┐ ┌─────────────┐
  │Deterministic│ │Stochastic│      │ Rule-Based │ │ Multi Agent │
  └─────────────┘ └──────────┘      └────────────┘ └─────────────┘
    ┌──────┴──────┐   ┌──────┴──────┐
 ┌──────┐ ┌─────────┐ ┌──────┐ ┌─────────┐
 │Static│ │ Dynamic │ │Static│ │ Dynamic │
 └──────┘ └─────────┘ └──────┘ └─────────┘
              ┌──────────┐          ┌──────────┐
              │ Discrete │          │ Discrete │
              └──────────┘          └──────────┘
              ┌──────────┐          ┌──────────┐
              │Continuous│          │Continuous│
              └──────────┘          └──────────┘
```

Deterministic models: The processes of this model are often described by differential equations, with a unique input leading to unique output for well-defined linear models and with multiple outputs possible for non-linear models; in these models, equations can be solved by different numerical methods.

Stochastic models: This type is used to model temporal behavior phenomena with random components. In this model, unique input leads to different output for each model run, due to the random component of the modeled process, single simulation gives only one possible result. All of the major models in the IS are Stochastic models

Rule based models: In this model, processes governed by local rules using cellular automata. In this type of models we encounter with non-linear dynamic mathematical systems based on discrete time and space.

Multi-agent models: For modeling complex systems (including multi role, multi platform and multi system aspects) we can use Multi-agent models. In these models we must develop group

of interacting agents. Agent is any actor in a system that can generate events that affect itself and other agents, a typical agent is modeled as a set of rules.

A dynamic model includes time in the model. Time can be included explicitly as a variable in a mathematical formula, or be present indirectly. through the time derivative of a variable or as events occurring at certain points in time. A static model can be defined without involving time; Static models are often used to describe systems in steady-state or equilibrium situations, where the output does not change if the input is the same. However, static models can display a rather dynamic behavior when fed with dynamic input signals. There are two main classes of dynamic models: continuous-time and discrete-time models. Continuous-time models evolve their variable values continuously over time, but Discrete-time models may change their variable values only at discrete points in time. Because of natural attributes of security models, most security simulation tools based on discrete event modeling and simulation techniques.

For Modeling a system three different representation forms of a model must be taken into considerations: [2]
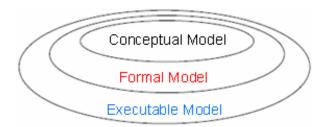
Figure 2: Three representation forms of a Model

The Conceptual Model describes the abstracted and idealized representation of the real system and holds all concepts of the model. The Formal Model is the formalized description of the Conceptual Model, compliant with a well-defined modeling formalism, expresses the Conceptual Model quantitatively and unambiguously, and thereby prepares several methods for its solution. The Executable Model technically implements the Formal Model and provides the additional information that allows the model to be executed and operated on a computer or in a network of computers. The additional information includes, for example, memory allocation, variable data type declaration, calls of operating system procedures, and communication protocols as typically required in development and execution environments.

If the model is going to be credible and a predictor of future behavior of a system/process it is critical that the model goes through rigorous Verification and Validation (V&V). Model verification is the process of demonstrating that a model is correctly represented and was transformed correctly from one representation form into another, according to all transformation and representation rules, requirements, and constraints. Model validation is the process of demonstrating that a model and its behavior are suitable representations of the real system and its behavior with respect to an intended purpose of model application. To meet these goals (V&V), several approaches were suggested. A common approach is the repeatable comparison between a real system with its model, it means that, the model must be evaluate in each execution and reformulate for better construction. In many cases especially in IS, "Verification" process is time consuming activity and Simulator can check his/her model via validating process. In development of models there is always a trade off [3]. A model is a simplification of reality, and as such, certain details are excluded from it. However, there is the belief that no model is truly valid, as it cannot replicate reality [4].

1-2- Simulation

Simulation is the manipulation of a model in such a way that it represents the behavior of system. Simulation is a cost-effective tool/concept for exploring new systems/processes without having to build them. Simulation can be categorized into three parts:

1- Live Simulation: Simulating real entities (people and/or equipments) in the real world, in the field of IS **Packet wars** and **Role Paying** are examples of Live Simulation.

2- Virtual Simulation: Simulating real entities in a virtual world.

3- Constructive Simulation: Simulating virtual entities, usually in a virtual world. In the field of IS **Sniffers** and **canned attack/defend scenarios** are Constructive Simulation.

M&S is a concept/discipline for developing a level of understanding of the interaction of the parts of a system or process, and the system or process as a whole.the results of M&S can help IS in many areas including: Analyzing the Risks of Information Security Investments, Predicating the future in the field of IS (Vulnerability Risk Assesment), Simulating the process of Malicious Codes propagating, Evaluating the security topologies in computer systems, etc. we can summarize these applications as :

1- Testing both attack and defense
2- Analysis of intrusions and attacks
3- Research and Development (R&D) of new countermeasures

In the field of IS we encounter with large and/or complex systems/processes to simulate, in these cases we need techniques to break the system into subsystems, DOD (Department of Defense) developed a technical framework to make it easier for all kinds of simulation models In order to solve the problems of traditional simulation models (The lack of reusability and interoperability), DOD developed High Level Architecture **(HLA)**. HLA connects several computer-based simulation systems so that they can run together and exchange information. Instead of building a big monolithic simulation system from scratch, the HLA allows engineers to combine existing simulation systems with new systems. HLA enables them to reuse existing systems for new purposes. They can also mix different programming languages and operating systems.

Figure 3: HLA Components

RTI: an Interface tool for exchanging info between Federates

Federation

In HLA an engineer can combine several simulation systems, called federates, into one big simulation, called the federation [5]. To do this they need to have a way to exchange information between the participating systems (federates). The RTI lets the participating simulation systems (Federates) connect to each other and exchange information.

2- Current State of M&S in the field of Information Security

As mentioned earlier, there is not any explicit M&S tool for testing computer security and network attack modeling. There are some special purpose tools for modeling and   Simulating of Information Security. For Modeling & Simulation in the field of IS, we can use Network Simulators. These tools are: OPNET, NS-2, Cnet, Netrule, etc. But Network Simulators are poor choices when it comes to simulating computer security and network attacks. There are significant limitations to applying modeling and simulation when it comes to security issues. Simulation of information security divides into five distinct categories [6]:

1 – Packet wars: (Example: IWAR)
2 – Network Design Tools: (Example: OPNET)
3 – Canned Attack/Defend Scenarios: (Example: MAADNET)
4 – Management Flight Simulators: (Example: EASEL)
5 – Role-Playing

2-1 – Packet wars: (Example: IWAR)

Information Warfare Analysis and Research (IWAR) involves tactical level of network attack and defense. IWAR (In Network Security) Consists of three Parts:

1- Computer Network Attack (CNA)
2- Computer Network Defense (CND)
3- Computer Network Exploitation (CNE)

The design goals of IWAR include: a heterogeneous operating systems, networking equipment, defensive security tools, and offensive exploits; containing **"soft"** and **"hard"** targets. Some of the IWAR tools and capabilities for simulation of network security/network attacks [7]:

Defense tools:
Firewalls and IDS , Cryptography and encryption , Application and protocol wrappers
Honey pots, Access Control Methods/ACL, Forensic analysis tools

Attack/Exploit tools:
Trojan horses, Different exploits (Malicious active components exploits, buffer overflow exploits, protocol exploits, race condition exploits), Vulnerability scanners, Viruses and worms, Network sniffers, Mail and protocol spoofing, Distributed Denial of Service (DDoS) attack tools, Password cracking software, Port scanners.

IWAR has some drawbacks, the major drawbacks with the IWAR are:
Lab is the implementation and maintenance of the laboratory requires significant investments in terms of hardware, software, and human resources to keep the equipment up to date and maintaining the physical networks of computers and communication components.

2-2 – Network Design Tools: (Example: OPNET)

Optimized Network Engineering Tool (OPNET) is a sophisticated M&S tool with the specific purpose to construct, simulate, and evaluate communication network design (topologies with specific devices), configurations of network nodes the transmission of packets through the network, and the use of different network protocols all from a performance point of view. OPNET was developed by MIT. OPNET consists of four different editors:

1- Network Editor: To Design Network Topology
2- Node Editor: Data Flow are defined here
3- Process Editor: is used for describing logic flows and behaviors
4- Parameter Editor: is seen as utility editor

The essential part of OPNET that is used for simulating Security is NetDoctor. NetDoctor is used mainly for analyzing network security with focus on policies and configuration testing. Utilizing NetDoctor help engineers to audit and validate network devices configuration for misconfiguration, and it helps an administrator for troubleshooting of network devices. Misconfigured network devices are a big security risk within the network environment and figures saying 40% of security related issues are caused by misconfigured network devises and servers.

In the following, there are some advantages of NetDoctor

1- Analyze Network Health
2- Detect Configuration problems
3- Enforce Organizational Policies in the network
4- Automate the process of Audit and Validation

Major drawbacks with OPNET are:

1- Lack of truthful (Verified and Validated) Attacks Models DoS and DDoS attacks can be tested because a TCP/IP stack is implemented in OPNET but if buffer overflows, race conditions, viruses, and worms are going to be tested we need models

2- Problems with modeling network traffic

2-3 - Military Academy Attack/Defense Network (MAADNET)

MAADNET will allow users to evaluate/simulate relationships between people, procedures, hardware, software, and data and how each of these components impact on network design, security and information assurance (Represents Soft Factors). MAADNET uses a client-server architecture in which the user builds and tests a network design on the client side and later submits the planned network to the server. The server simulates various events and grades the network based on "hard" metrics like message latency, percent down time, etcetera. The network is also graded on "soft" metrics like how well confidentiality, integrity, and availability were maintained during simulated attacks. In this approach, Simulation Tools are inexpensive to build. The major drawback of MAADNET is Lack of models and simulation Tool.

2-4 - EASEL

Easel is a modeling and simulation language and tool. Easel can be used for simulating various unbounded systems such as [8]:

- Internet
- Telephone systems
- Software organizations

Simulating with EASEL is quite rudimentary (Simulations in network security are to primitive to draw any conclusions from), and cheap.

2-5 – Role-Playing

These simulations are more based on a face-to-face orientation. Their purpose is to get better understanding the different roles an organization uses in defending it self against a large-scale Attack. In their simplest form role-playing simulation does not even use computers.

As mentioned earlier, I could not find any explicit M&S tool used for testing computer and network security with network attack modeling. Maybe the military has these kinds of simulation tools it is hard to tell. Indications are that they do not have it but they are very interested in develop such simulation tools. Military organizations in USA are using OPNET with own created modules form simulation of various matter [10]. Other simulation tools such as NS-2 have the "equal[9]" potential as OPNET to be able to get customized for the purpose of computer and network security testing. Simulation tool such as NetSim is really interesting from a computer and network security testing scenario. It is still in its infancy but is has potential to be accurate and predictive as a simulation tool in the future. To really model and simulate computer and network security today with different network attack techniques and models for predicting the impact of such an attack, live simulation, such as IWAR is the only way to go. If M&S simulation tool is going to get a market of computer and network security testing, attack models have to be implemented and some kind of OS emulation on node level has to be in process to really get accurate answers from the simulations.

The section 3 presents a Simulation that is implemented by OPNET. [9]

3- Case Study: DDOS Simulating

In this simulation, the network is "attacked" by another network representing a hi-jacked botnet used for attacking the "peaceful" network with a flooding attack. Three servers are connected to a switch which is a LAN for sales people. The firewall is configured passing trough FTP traffic without any VPN tunneling involved. This "weakness" is exploited by the botnet sending flooded messages of FTP traffic to the FTP server. Outside the firewall is a miniature representation of Internet which another department of the company is connected to. There is another LAN with engineers working against the Database server and transporting files to the FTP server. While the firewall is passing FTP traffic trough no net for VPN tunneling is needed on that service. The following graph show how the FTP server is attacked by packet floods from the botnet network. During this time ordinary user could not access the FTP server resulting in a Denial of Service. This Simulation contains the following components:

3 Servers:
- Web Server (HTTP, Telnet)
- FTP Server (FTP, File print)
- Database Server (Database access)

1 Switch:
- Server Switch (Multiplex the three servers together)

3 Routers:
- LAN Router (Routes traffic from Sales to servers)
- Router MAN A (Routes traffic from Engineers to the LAN)
- Router MAN B: (Routes traffic from the botnet to the LAN)

1 Firewall: (Misconfigured firewall passing trough FTP traffic)

3 LAN's:
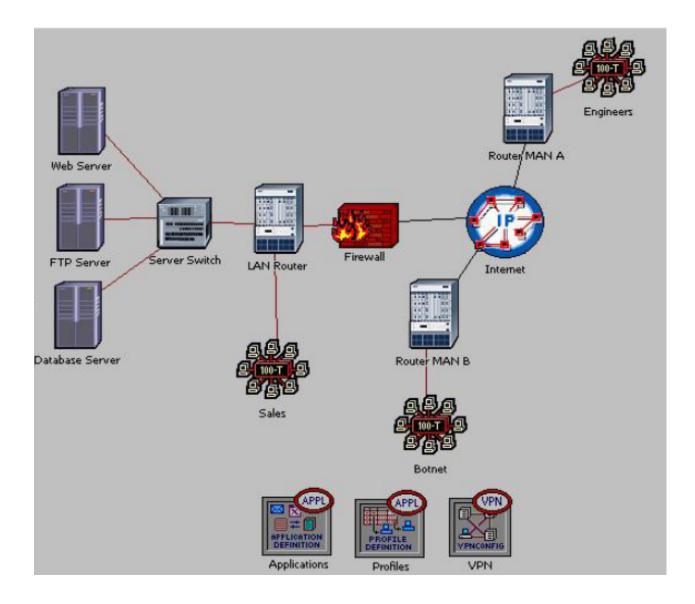- Sales (LAN representing 25 people of the sales division using, Database access, Web browsing (HTTP), File Print)
- Engineers (LAN representing 25 people of the engineer division using, Web browsing (HTTP), File Transfer (FTP))
- Botnet (A representation of a hi-jacked botnet attacking the FTP server with FTP flood of packets)
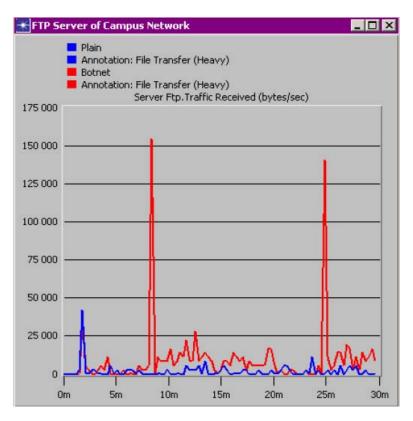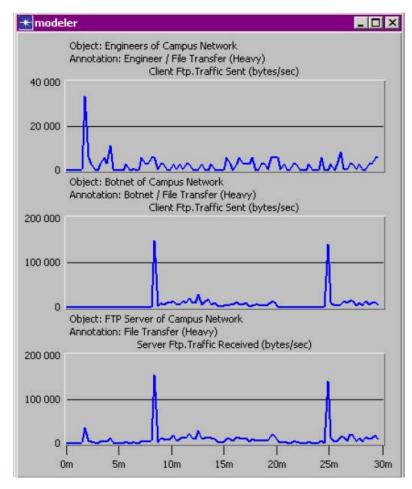

1 Internet cloud: (Representing a WAN)

In the Figure 4, you can see the problem

Figure 4: DDOS Attack- Modeling and Simulation by OPNET

Figure 5: Results of Simulation

The scenario simulates an outside botnet attacking the corporate LAN's FTP Server by flooding it with packages. The botnets simulates 100 of workstations connected together to send TCP/UDP packets on a given interval. The attacks occur two times during the 30 minutes of simulation. The botnet strikes after 500 seconds (~8 minutes) and the next time after 1500 seconds (25minutes). Figure 5a shows the normal traffic pattern on the FTP server in blue and the traffic occurrence when it is attacked in read. Figure 5b shows the traffic from Engineer's LAN at the top, the botnet's traffic in the middle, and the traffic receive at the FTP Server at the bottom.

4- Limitations of M&S in the field of IS

The area of M&S in Information Security has the following limitations:

1- Lack of Verified and Validated Models for Attacks: Virus/Worm Propagations, Buffer Overflow, etc

2- Lack of Verified and Validated Models for Network Traffic (Internet Traffic)

3- Inadequate Models of defense mechanisms for example : Preventing DOS/DDOS attacks

4- Small changes in input may produce large changes in output therefore the Space is too large to explore.

5- We have no set of commonly accepted metrics to measure phenomena

Conclusion

Information Security needs a Conceptual Framework for M&S. Attack techniques/motives can hardly be modeled because Soft Factors are belonging to complex M&S groups. And finally we need better Attack models; we also need Network Traffic models.

References

[1] David A. Cook. (2001). Computers and M&S - Modeling and Simulation. The Journal of Defense Software Engineering.

[2] Dirk Brade. A Generalized Process for the Verification and Validation of Models and Simulation results. Neubiberg, October 2003.

[3] Gene Bellinger. (2004). Modeling & Simulation - An Introduction URL: http://www.systems-thinking.org/simulation/model.htm

[4] Patrick J. Delaney. "What is a Simulation? (Another View)". Revived Mars at URL: https://www.amso.army.mil/library/primers/what-is/

[5] Chris Turrell. (1999). High Level Architecture. Simulation Technology, Vol. 1 Issue 4. Monday, June 21, 1999. At URL: http://www.sisostds.org/webletter/siso/iss_18/

[6] John H. Saunders. (2002). "Simulation Approaches in Information Security Education" in Proc. 6th National Colloquium for Information System Security Education, Redmond, WA, 2002. At URL: http://cisse.info/CISSE%20J/2002/saun.pdf

[7] Daniel Ragsdale, John Hill, Scott Lathrop, and Gregory Conti. (2000). Information Assurance Program at West Point.

[8] Easel (Version 3.0) [Computer Software]. (2002). Carnegie Mellon University ("Carnegie Mellon"). At URL: http://www.sei.cmu.edu/community/easel/

[9] Mattias Björlin. (2005) A study of Modeling and Simulation for computer and network security using OPNET

[10] NETWARS Communications Model Library. At URL: http://www.opnet.com/products/library/netwars_models.html