# INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed Refereed Open Access International e-Journal - Included in the International Serial Directories
Indexed & Listed at:
Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.
as well as in Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)]
Registered & Listed at: Index Copernicus Publishers Panel, Poland
Circulated all over the world & Google has verified that scholars of more than Hundred & Thirty Two countries/territories are visiting our journal on regular basis.
Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA
www.ijrcm.org.in

# CONTENTS

# CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the area of Computer, Business, Finance, Marketing, Human Resource Management, General Management, Banking, Insurance, Corporate Governance and emerging paradigms in allied subjects like Accounting Education; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Monetary Policy; Portfolio & Security Analysis; Public Policy Economics; Real Estate; Regional Economics; Tax Accounting; Advertising & Promotion Management; Business Education; Management Information Systems (MIS); Business Law, Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labor Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; Public Administration; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism, Hospitality & Leisure; Transportation/Physical Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Digital Logic; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Multimedia; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic and Web Design. The above mentioned tracks are only indicative, and not exhaustive.

Anybody can submit the soft copy of his/her manuscript **anytime** in M.S. Word format after preparing the same as per our submission guidelines duly available on our website under the heading guidelines for submission, at the email addresses: infoijrcm@gmail.com or info@ijrcm.org.in.

# GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

**DATED: _____________**

***THE EDITOR***
IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF ______________________________________________.**

**(e.g. Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)**

**DEAR SIR/MADAM**

Please find my submission of manuscript entitled '____________________________________________' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

**NAME OF CORRESPONDING AUTHOR**:
Designation:
Affiliation with full address, contact numbers & Pin Code:
Residential address with Pin Code:
Mobile Number (s):
Landline Number (s):
E-mail Address:
Alternate E-mail Address:

**NOTES**:

a) The whole manuscript is required to be in ***ONE MS WORD FILE*** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.

b) The sender is required to mention the following in the **SUBJECT COLUMN** of the mail:
**New Manuscript for Review in the area of** (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)

c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.

d) The total size of the file containing the manuscript is required to be below **500 KB**.

e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.

f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.

2. **MANUSCRIPT TITLE:** The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS**: The author (s) **full name**, **designation**, **affiliation** (s), **address**, **mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ABSTRACT**: Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

5. **KEYWORDS**: Abstract must be followed by a list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.

6. **MANUSCRIPT**: Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. It must be prepared on a single space and single column with 1” margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited.

7. **HEADINGS**: All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

8. **SUB-HEADINGS**: All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.

9. **MAIN TEXT**: The main text should follow the following sequence:

   INTRODUCTION

   REVIEW OF LITERATURE

   NEED/IMPORTANCE OF THE STUDY

   STATEMENT OF THE PROBLEM

   OBJECTIVES

   HYPOTHESES

   RESEARCH METHODOLOGY

   RESULTS & DISCUSSION

   FINDINGS

   RECOMMENDATIONS/SUGGESTIONS

   CONCLUSIONS

   SCOPE FOR FURTHER RESEARCH

   ACKNOWLEDGMENTS

   REFERENCES

   APPENDIX/ANNEXURE

   It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed ***5000 WORDS***.

10. **FIGURES &TABLES**: These should be simple, crystal clear, centered, separately numbered & self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. It should be ensured that the tables/figures are referred to from the main text.

11. **EQUATIONS**: These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.

12. **REFERENCES**: The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parentheses.
- The location of endnotes within the text should be indicated by superscript numbers.

**PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:**

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–22 June.

UNPUBLISHED DISSERTATIONS AND THESES

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITE

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

# CYBER ATTACK MODELING AND REPLICATION FOR NETWORK SECURITY

*B.VENKATACHALAM*
*ASST. PROFESSOR*
*DEPARTMENT OF MCA*
*BHARATH INSTITUTE OF SCIENCE & TECHNOLOGY*
*CHENNAI*

*S. CHRISTY*
*ASST. PROFESSOR*
*DEPARTMENT OF MCA*
*BHARATH INSTITUTE OF SCIENCE & TECHNOLOGY*
*CHENNAI*

## ABSTRACT

*Cyber security methods are continually being developed. To test these methods many organizations utilize both virtual and physical networks which can be costly and time consuming. As an alternative, in this paper, present a simulation modeling approach to represent computer net-works and intrusion detection systems (IDS) to efficiently simulate cyber attack scenarios. The outcome of the simulation model is a set of IDS alerts that can be used to test and evaluate cyber security systems. In particular, the simulation methodology is designed to test information fusion systems for cyber security that are under development.*

## KEYWORDS

cyber attack modeling, network security.

## INTRODUCTION

As the use of computer networks grows, cyber security is becoming increasingly important. To enable systems administrators to better protect their networks, cyber security tools are employed to warn of suspicious network activity.

In some situations, systems administrators have to deal with millions of such warnings each day. Consequently, situational awareness and threat assessment tools that employ information fusion techniques are being developed to aid in fighting cyber attacks [1]. As these systems are being developed, data is needed to test and evaluate their performance. As an alternative to a physical computer network, a simulation modeling methodology is presented.

The simulation method allows the user to construct a virtual computer network that produces cyber attack warnings representative of those produced by intrusion detection systems. Consequently, this flexible simulation modeling framework will enable the efficient generation of data to test and evaluate situational awareness and treat assessment tools for cyber security. There is some research in modeling of computer net-works and cyber attacks. Although simulating the flow and processing of packets in the computer network is possible (potentially billions of packets per day), only a small fraction of the packets cause alerts to be produced by the intrusion detection system which in turn would be used by the information fusion tools. Furthermore, modeling a system at this level of detail requires great amounts of time and effort for modeling as well as requiring large amounts of computer processing time for simulating "good" packets. As an alternative to modeling the details of packet flow in a net-work, this work presents a simulation model for simulating the behavior of the intrusion detection system by producing simulated alerts representative of malicious cyber attacks and non-malicious network activity based on the user's specification. Consequently, the user can efficiently construct scenarios of various computer networks and cyber attacks and generate the corresponding alerts.

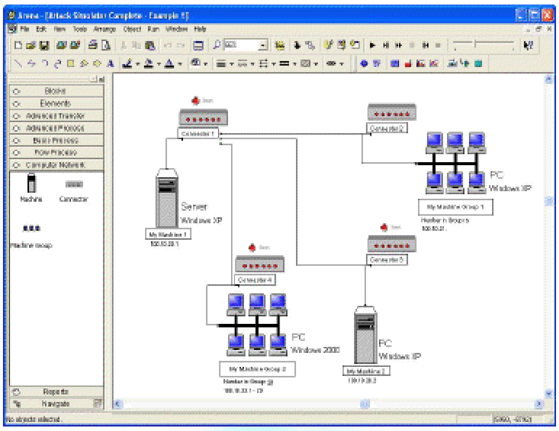
## OVERVIEW OF THE REPLICATION MODEL

A discrete-event simulation model has been developed for generating representative cyber attack and intrusion detection sensor alert data. Although the model is primarily de-signed to be used in testing cyber situational awareness and analysis tools, other applications such as training of systems analysts may also make effective use of the model. The simulation model is initially implemented in the ARENA simulation software [3].

An object-oriented model written in Java is currently under development. Although this paper utilizes the ARENA model to illustrate the modeling concepts, the focus is on the concepts themselves. The simulation model provides a user with the ability to construct a representative computer network and setup and execute a series of cyber attacks on certain target machines within that network. IDS sensors that are setup within this network produce appropriate alerts based on the traffic they observe within the network. The alerts produced consist of a combination of the alerts produced as a result of attack actions and as a result of typical "noise" (non-malicious network traffic that triggers an alert.)Figure 1 displays an example network interface setup using the ARENA model. To effectively model a network setup in ARENA and to provide users that may not have extensive simulation training with a friendly interface, custom modules were created for the network devices. The simulated computer networks consist of three primary types of devices: machines, connectors, and subnets. A machine can represent an individual computer or server. Machine characteristics can be specified including the IP address, the operating system, and the type of IDS sensor on the machine (if any). For each IDS sensor specified, an associated output file will be generated containing the sequence of alerts produced when the simulation is run.

A connector represents the means by which computers are connected, such as through a switch or a router. The network connectivity plays in important role in establishing the path that an attacker can take through the network. The connector also has network IDS sensors that can be represented which are used to monitor any network traffic that travels through the connector and produce alerts corresponding to known potentially harmful actions. A subnet represents a group of several machines with connectivity to the network that all share a common set of properties (such as the operating system). Machines within a subnet contain the same set of properties that could be specified if the machines were placed into the network individually. The subnet just provides an efficient method of specifying groups of computers (particularly useful when specifying large networks.)Connector lines are used in the model to connect the modules and represent the connection of machines/subnets to a connector, as well as the connections between connectors themselves. When a computer network has been created, an attack scenario can be setup and run on the network. An attack scenario consists of a series of specified cyber attacks occurring over a period of time along with a specified quantity of network noise. A user-interface with a series of forms is used to specify the desired scenario. The model structure enables manual or automatic attack generation. In the manual mode, the user can specify all of the details of the attack scenario including the sequence and timing of attack actions as well as the path the attack will take through the computer network. In the automatic mode, the user can specify the goal (ultimate attack action and target computer) of the attack, and the simulation model will generate a random, feasible sequence of attack actions along a path that leads to the goal. Additional parameters that represent the behavior of the attacker can also be specified. These parameters include the efficiency, stealth, and skill of the attack being modeled. The efficiency refers to how direct the attack is, and this utilizes a range between0 and 1, with 1 representing the most efficient attack path. The stealth parameter refers to how well the attack avoids detection, primarily by avoiding intermediate "goal" steps, and this also utilizes a range between 0 and 1. The skill refers to the probability of success for each step.

FIGURE 1: SAMPLE NETWORK INTERFACE IN ARENA MODEL



Currently, an attack scenario in the ARENA model can handle up to 25 attacks with 250 steps per attack. Also, for each type of attack, the user can specify the time between attack steps based on a fixed number or on a random number sampled from an exponential distribution. The steps/actions available for use in an attack are chosen from a categorized list of 2,237 known exploits in 5 major groups and 23 subgroups. If no specific exploit is selected, one will be chosen at random based on the subgroup. In addition to attacks, the user can specify, the rate at which non-malicious traffic alerts (noise) is generated, as well as the probability of noise alerts corresponding to each of the action categories. Once the scenario has been created, the information is saved in a file for future use. The simulation is then run, and the attack scenario is executed. The output of the simulation includes a file listing the actions generated for each attack (known as the "ground truth") and the time the action occurred. In addition, an output file containing IDS alerts is produced for each IDS sensor specified in the modeled network. These files containing IDS alerts are in-tended to be used to test the situational awareness and analysis tools.

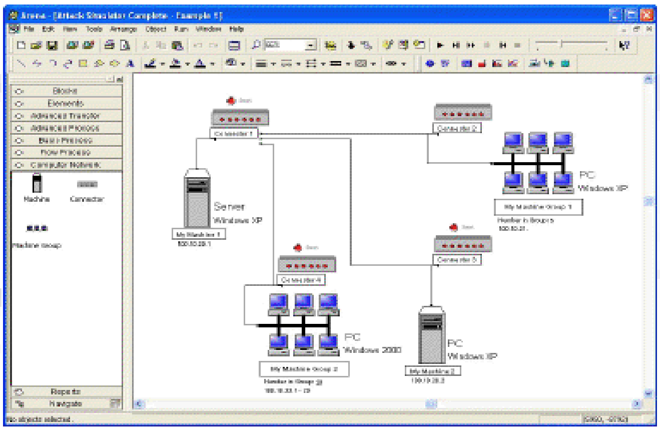
## SIMULATION METHODOLOGY

Modeling Computer Networks, the computer network is modeled using two basic constructs: machines and connectors. The third construct, subnets, represents a group of machines. The modules representing the machines, connectors, and subnets provide a visual representation of the computer network. However, functionally, these modules provide a logical method for the user to enter the data about the computer network including whether the ma-chine can be accessed externally from the Internet. The connecting lines showing the connectivity of the network are used to construct a from-to type of matrix representing the network topology that will be used in the attack generation. The details of the devices (such as the type of IDS) are stored as variables that can be accessed based on the device ID. The devices used can be easily modified by double-clicking their corresponding representation in the interface to bring up a form to enter or change information.

## MODELING CYBER ATTACKS

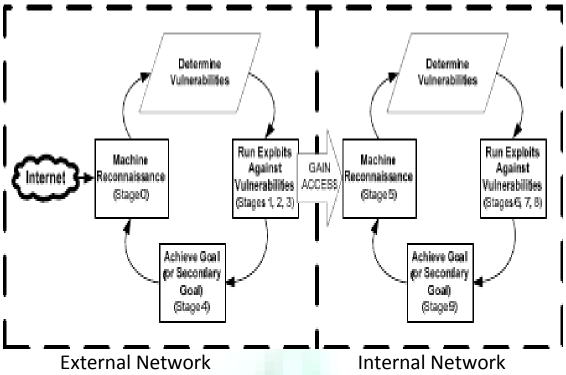
The scope of this work is on cyber attacks that are initiated by a hacker through the Internet. Although insider attacks could also be modeled, this is not the primary purpose of the model. The progress that a hacker can make in an at-tack is dependent upon the hacker's capabilities and the vulnerabilities of the network. The methods for modeling and simulating the initiation and progression of cyber at-tacks through a computer network included in this model are based on Sudit et al. (2005). Sudit et al. (2005) place the sequence of attack actions that a hacker may use into stages that correspond to the hacker's capabilities given the current state of the network. These stages are referred to as Stage 0 through Stage 9where Stage 0 represents generally reconnaissance activities on the external part of the computer network where the attacker is using exploits to simply gain more information about the network. (In this discussion an external machine is one that can be accessed from the Internet, and an internal machine is a machine that can only be accessed from an external machine through a firewall or from another internal machine.) Stage 0 –Stage 4 represent hacker actions on external machines, and Stage 5-Stage 9 represent hacker actions on internal machines. Figure 2 shows some typical hacker actions that correspond to an attack stage. The hacker can attack an organization's machine that is on the external side of the computer network. Once the external machine has been successfully compromised, the hacker can use the compromised external machine to work their way through the external network until the capability to access internal machines is reached. Once the hacker has infiltrated the internal network, the internal machines can be compromised until the hacker reaches their goal. Figure3 illustrates the cyber attack process from the internet to a goal on an internal machine.

FIGURE 2: TYPICAL HACKER ACTIONS IN A CYBER ATTACK



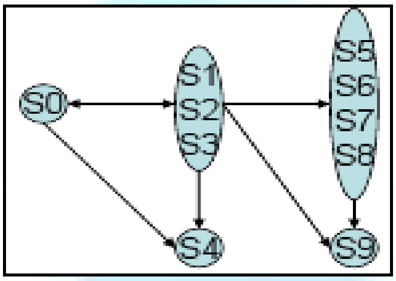
The simulation model includes automated and user-specified cyber attack generation methods. The automated method utilizes the network specifications and connectivity in combination with a guidance template of the available stages to determine the capabilities of the attacker and vulnerabilities of the network and generate a feasible sequence of attack steps for the cyber attacks. The graph based guidance template is used to determine which groups of actions are feasible at different points of the attack. A diagram of the graph-based template that the simulation model currently operates under is shown in Figure 4 (S0, S1, …, S9 represent Stage 0, Stage 1, … , Stage 9.)

FIGURE 3: PROGRESSION OF A CYBER ATTACK ON A COMPUTER NETWORK FROM THE INTERNET


Internet
Machine Reconnaissance (Stage0)
Determine Vulnerabilities
Run Exploits Against Vulnerabilities (Stages 1, 2, 3)
Achieve Goal (or Secondary Goal) (Stage4)
GAIN ACCESS
Machine Reconnaissance (Stage5)
Determine Vulnerabilities
Run Exploits Against Vulnerabilities (Stages6, 7, 8)
Achieve Goal (or Secondary Goal) (Stage9)
External Network
Internal Network

The graph is a directed graph, which means that an edge (arc) only indicates a feasible transition in the direction that the edge is pointing. Nodes within the same group form a complete graph in which each node is connected to the every other node. This graph-based template is represented as an adjacency matrix of 1's and 0's representing which stages are accessible after which other stages have been performed.

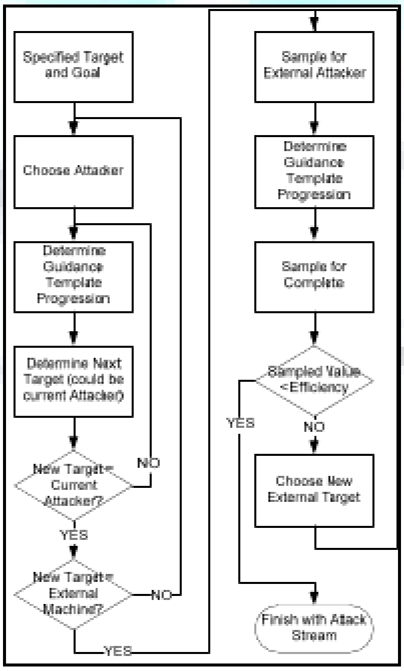
FIGURE 4: DIRECTED GRAPH REPRESENTING ATTACK STRUCTURE



Given the attack structure (in the form of the guidance template) and the network configuration specified, the user also specifies a target machine, a goal, and several other attack related parameters through a series of forms. Figure 4 illustrates the auto-mated method that is used to generate the specific multi-stage attack.

In generating the steps (prior to simulating them over a time period), the methodology works backwards through the network by first defining the attack's target and finding a path up out of the network that the hacker could attack through. The logic first chooses an attacker(machine from which the hacker could execute the attack step) which is able to communicate with the chosen target based on the topology of the network. After the attack progression for the current target is determined, a new target can be chosen. The options for the new target are a machine with which the current attacker can communicate or the current attacker itself. Choosing the current attackers the new target will move the attack to a higher level of the network topology (toward the external machines) to model the way in which hackers penetrate a network. If the chosen target is not the current attacker, the logic will repeat the steps for determining guidance template progression and determine another target, using Stage 5through Stage 9. However, if the current attacker is chosen for the new target, the attack generation moves up a level in the network topology. Thus, the logic evaluates whether the chosen target has become an external ma-chine. If the chosen target is not an external machine, the logic will choose a new attacker who can reach the new target and repeat the attack generation process. However, if the target is external, the attacker must be attacking from the Internet. Thus, the attacker IP address for attacks on external machines is created randomly since hackers will generally "spoof," or disguise, their IP address when attacking from the Internet. The logic will then determine the guidance template progression for the external target, now using Stage 0 through Stage 4.

FIGURE 5: AUTOMATE ATTACK GENERATION METHOD


Specified Target and Goal
Choose Attacker
Determine Guidance Template Progression
Determine Next Target (could be current Attacker)
New Target= Current Attacker?
NO
YES
New Target= External Machine?
NO
YES
Sample for External Attacker
Determine Guidance Template Progression
Sample for Complete
Sampled Value <Efficiency
YES
NO
Choose New External Target
Finish with Attack Stream

## CURRENT DEVELOPMENT

Current work entails the development of an object-oriented Java simulation model. The primary motivation behind this development is to create a simulator that is plat form independent and easier to use for individuals with expertise in computer networks and cyber security rather than simulation. This new model improves up on the ARENA model by providing several features allowing for networks and attacks to be defined in more detail and allowing for a wider range of inputs to and outputs from the model. These features include:

- Allowing multiple attack scenarios to be created and saved with a network;
- Separating the auto-attack generation and event simulation, and providing a display for each;
- Defining a list of services running on a machine;
- Defining a list of ports/protocols that are allowed or banned through a specific connector path;
- Utilizing the machine vulnerabilities and connector attributes to determine the selection and the success of an action/exploit (as opposed to strict probability);
- Allowing network traffic to be routed through more than two connectors (based on connector link attributes);

## CONCLUSION

The Cyber Attack Simulator presented in this paper is capable of generating IDS alert and ground truth files based on the specification of a computer network and attacks. The simulator is built with a user interface to allow the creation of various computer network configurations and attack actions. The model also incorporates a method for automated attack generation given the network configuration, characteristics describing hacker capabilities, and vulnerabilities of the network.

## REFERENCES

1. Lee, J.-S., J.-R. Jung, J.-S. Park and S. D. Chi. 2004.Linux-based system modeling for cyber attack simulation. In Proceedings of the 13th International Conference on AI, Simulation, and Planning in High Autonomy Systems, Jeju Island.
2. Linus, J. 2001. An Introduction to Data and Information Fusion.(Presentation) Available Onlinevia<http://www.infofusion.buffalo.edu/tutorialPage.php [Accessed July 15, 2007]
3. Kelton, W. D., R. P. Sadowski, and D. T. Sturrock. 2004. Simulation with ARENA, Third Edition, McGraw-Hill, Boston, MA.
4. Nicol, D., J. Liu, M. Liljenstam, and G. Yan. 2003. Simu-lation of large-scale networks using SSF. In Proceed-ings of the 2003 Winter Simulation Conference, ed. S.Chick, P. J. Sánchez, D. Ferrin, and D. J. Morrice, 650-657. Institute of Electrical and Electronics Engineers, Piscataway, NJ.

# REQUEST FOR FEEDBACK

**Dear Readers**

At the very outset, International Journal of Research in Computer Application and Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mails i.e. **infoijrcm@gmail.com** or **info@ijrcm.org.in** for further improvements in the interest of research.

If you have any queries please feel free to contact us on our E-mail infoijrcm@gmail.com.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

**Academically yours**

Sd/-

**Co-ordinator**

# ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

## Our Other Journals

ISSN : 0976-2183
INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, ECONOMICS & MANAGEMENT
IJRCM
IJRCM
ISSN : 0976-2183
INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT
IJRCM
IJRCM
ISSN : 0976-2183
INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE & MANAGEMENT
IJRCM
IJRCM