

A major purpose of the Technical Information Center is to provide the broadest dissemination possible of information contained in DOE's Research and Development Reports to business, industry, the academic community, and federal, state and local governments.

Although a small portion of this report is not reproducible, it is being made available to expedite the availability of information on the research discussed herein.

1

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

TITLE NETWORK SECURITY AND THE GRAPHICAL REPRESENTATION MODEL

AUTHOR(S) Jared S. Dreicer, Laura Stolz, and W Anthony Smith

SUBMITTED TO 13th National Computer Security Conference,
Washington, DC, October 1-4, 1990

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes.

The Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy.

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED *JYH*

Los Alamos Los Alamos National Laboratory
Los Alamos, New Mexico 87545

MASTER



NETWORK SECURITY AND THE GRAPHICAL REPRESENTATION MODEL*

Jared S. Dreicer, N-4, MS E541
Laura Stolz and W Anthony Smith, Graduate Research Assistants
DOE Center for Computer Security
Los Alamos National Laboratory
P. O. Box 1663
Los Alamos, NM 87545

ABSTRACT

This paper describes the underlying conceptual design and investigative approach used during the development of the Prototype Graphical Representation Model. The initial problem was to characterize and develop the fundamental theoretical foundation for modeling the features of computer networks. This research was influenced by the desire to investigate graph theoretical problems, in general, that are common to many different systems and disciplines. A computer network is a specific graph theoretical problem. This paper provides details on the early research into the relation between computer networks and graph theory and the optimal representation of computer networks for security analysis.

I. INTRODUCTION

The Prototype Graphical Representation (PROGREP) model effort is funded by the Office of Safeguards and Security at the Department of Energy (DOE) primarily to investigate security in computer networks. The PROGREP Model also includes the capability to investigate information flow in communication systems and to provide a graphical display of these communication systems and networks. At this time stand-alone computer systems are exceptional; the trend in new and modified computer systems is toward networking because it provides benefits such as economies of scale, enhanced productivity, efficient communication, resource sharing, and increased reliability [1]. Inherent in the desire to network is the implicit acceptance of increased interconnection with other computers that may also be interconnected to other unknown computers or networks. This increased connectivity can result in a combinatorially explosive number of communicating computers. Networking, however, also presents a challenge and potential disadvantages with respect to maintaining and ensuring the integrity and security of the networked computer systems. Further, networking creates a large number of other related problems, such as path routing, scheduling, network control, cycle generation, traversability, and connectivity [2-6]. Security and other problems are of particular concern depending on the classification and character of the data that are processed, stored, or transmitted on computer networks and communication systems. These issues are of particular concern to the DOE because of the sensitivity and national security nature of the data that are processed and stored on DOE and DOE contractor computer systems.

The DOE has a large number of local area networks (LANs) and subnets (small LANs connected to larger networks) and is connected to a variety of national and international networks (e.g., BITNET, HEPNET, ARPANET). DOE also operates several wide-area networks for its own use (e.g., NWCNET). For DOE contractors to perform their work efficiently, computer networks are necessary. However, the more they are needed, the more important it is to determine methodologies and procedures to ensure the network security. The following recent events demonstrate the need for applied research and development in network security: the German Chaos Club's infiltration of computer systems at various U.S. government organizations and various penetration attempts and attacks on other government organizations that are on the

*This work was supported by the U.S. Department of Energy, Office of Safeguards and Security.

INTERNET. The rapid emergence of networks has been beneficial, but network security research has just been initiated. The knowledge, tools, and capability to sufficiently understand and address the problem are in short supply. The applied research for the PROGREP model is the first step in developing a research program, tools, and methodologies to investigate network security.

Although the PROGREP effort was funded to conduct applied research into computer network security, the model appears to be applicable to many other disciplines. There are parallels between the basic graph theory principles of computer networks and systems that can be portrayed by graph structures. For example, the PROGREP model also applies to the safeguards discipline. In computer security the intent is to protect the data and information on computer systems; in safeguards the intent is to protect the special nuclear material and the inventory data related to the material. With modifications, the PROGREP model could represent special nuclear material process lines, which are fundamentally graph structures. The PROGREP model can currently represent process lines (directed graphs) but will need to be modified to characterize the real world and model specific safeguards systems.

II. PURPOSE

The PROGREP system is being developed to (1) better understand computer networks for future research and development; (2) provide a tool capable of graphically representing any computer network, which is required by computer security personnel; (3) create methodologies that detect and indicate security relevant information and events and check the security of proposed network topologies; and (4) expand the means to conduct further network security and graph theory research.

III. GOALS

The primary goals of the PROGREP research are to help system security personnel check the security of existing networks, to determine the security of proposed networks, and to conduct applied research into graph theoretical problems. Therefore, it is our goal to produce a realistic and valid network representation system, not the ultimate system. While developing PROGREP, we tried to provide a useful tool for computer security personnel. Our ultimate goal is to provide a means by which security personnel may enhance their understanding and the security of an actual computer network.

IV. PROGREP MODEL SYSTEM SPECIFICS

The PROGREP software system has been implemented on a Texas Instrument Explorer using the expert system shell called Knowledge Engineering Environment (KEE), Common Lisp methods, icons, object-oriented programming methodologies, and KEE Pictures for graphical display [7]. The PROGREP model provides a user interface that is designed to allow a user the ability to rapidly and efficiently represent graph components, their interconnections, and interrelationships.

Object-oriented programming methodologies naturally complement the software development, result in a generalized tool, and enhance the functionality of a graph structure system. This is a result of the dependence on set theory for defining graphs and on the abstract notion of passing information (e.g., material) among vertices along edges. Objects are entities that can be described as having behavioral or cognitive capabilities (procedures) as well as physical assets and attributes (data) [8]. There are two main concepts that distinguish object-oriented programming: message passing and specialization [9,10]. Message passing is the functional essence of object-oriented programming; all activity is dependent on the "action-response" from sending messages between objects. Message passing is equivalent to a sophisticated procedure call. Specialization is the combination of data structure, class inheritance, and data hiding (due to inheritance constraints). Specialization enhances object hierarchies, data abstraction (through inheritance), and instantiation.

Object hierarchies or classes allow objects to be either exactly alike or almost alike with respect to the physical (data) and behavioral (functional) characterization of the system being modelled. Data abstraction eases the burden of data modification and input and also reduces the specification of redundant information due to the inheritance features. Instantiation uses the inheritance hierarchy to specify an individual object. The PROGREP model employs these methodologies by defining two main classes: components (vertices) and links (edges). The physical and behavioral information that is related to a particular component or link is controlled by the own/member class inheritance constraints available in KEE [7]. The PROGREP model extends the concept of object-oriented programming by the use of objects as icons. An icon is a behaviorally functional and physically characterized graphically operational object.

V. CONCEPTUAL DESIGN

The first phase of the development of the PROGREP model was to establish an analytical basis by which to generically define computer networks. An additional constraint was that the model must be flexible in representing and characterizing real-world systems (e.g., computer networks and nuclear material process lines). We imposed this requirement so that other research efforts in the Safeguards Systems Group and at the DOE Center for Computer Security at Los Alamos National Laboratory would benefit from this latitude. During this phase of the effort, it became apparent that there was no clear technical description of a computer network.

What is a computer network? Can a stand-alone computer constitute a computer network? Regardless of the answer (one could contend that a massively parallel computer is a network), is it necessary to include stand-alone representation in the PROGREP model? Are computer networks different than distributed systems? These were some of the questions we addressed during the early phases of this research. We addressed these questions in terms of the capabilities desired for the PROGREP model. Even though a stand-alone computer is not typically considered a computer network, we included the capability of representing stand-alone computers in the PROGREP model.

In PROGREP our definition of a computer network is very general. It is any collection of interconnected, autonomous computers or components of slave hardware (e.g., printers, disk storage components, or plotters). If two or more computers or components are able to exchange information, then they are interconnected. This definition of a computer network complements the definition of a graph. A graph $G = (V, E)$ is a structure that consists of a finite set of vertices V and a finite set of edges E (an edge is specified by an unordered pair of distinct vertices). In the PROGREP model, computer networks are fundamentally represented and characterized in terms of graph theory and graph structures. A network $N = (C, L)$ is a structure that consists of a finite set of components C and a finite set of links L (a link is specified by an unordered pair of distinct components). The components (computer or slave hardware) of a computer network (e.g., computer, gateway, printer, or disk storage) are defined in terms of vertices and the interconnections or network links are defined in terms of edges. These links may be either uni- or bi-directional and physical (an actual connection) or abstract (hardware data transfer compatibility but no actual connection).

In the PROGREP model, stand-alone computer security and network security requirements and limitations are modelled as constraints at the components and across the links of the represented network (graph structure) [11,12]. Typically, computer security programs depend on organization-specific policy statements. These policy statements are generally implemented by imposing constraints, procedures, and restrictions in the following areas: hardware/software security, telecommunications security, administrative security, personnel security, and physical security [13-16]. The PROGREP model addresses some of the issues associated with the above mentioned areas but is primarily a security assurance, design, and analysis system. The types of security checks addressed are related to compatibility, consistency, and suitability of hardware

designations and interconnections. Additionally, the transfer of data from a source to a destination is scrutinized for the creation of a cascade problem [17], the existence of unacceptable operation modes, and other transmission path problems. Because we decided to include stand-alone computers in addition to computers connected into a network, it was natural to divide the computer network security problem into two sub-problems. One represents and characterizes the stand-alone computer security risks, and the other represents and characterizes the network security risks.

A. Stand-Alone Computer Security

Our model of the security of a stand-alone computer depends on data classification level, user clearance level, the machine's evaluated product lists (EPL) level, the operating mode of the computer, and a protection index [13-16]. The security risks on a stand-alone computer are related to computer access, data integrity, and data sensitivity. The data stored and processed on a computer are assigned a classification level which reflects the importance of protecting their integrity, that is, preventing inadvertent or intentional modification, destruction, or disclosure of the data. Users of the computer are assigned clearance levels and need-to-know permission which allows read/write access to data in the computer that have been assigned an equivalent or lower classification level. The EPL level of a computer indicates its ability to prevent and indicate unauthorized user access to data. The operating mode of the computer is either dedicated, system high, compartmented, or multilevel. The protection index depends on the user clearance level and the data classification level relative to the EPL level of the computer on which the data are stored and processed. The protection index reflects the inherent vulnerability of the data to access (i.e., highly classified data accessed by an uncleared user) on a particular computer. Using the protection index, PROGREP specifies the minimum EPL level acceptable that is needed to keep the data from being vulnerable. Because the protection index is a function of the user clearance and data classification levels, the security requirements for a stand-alone computer translate into the protection index indicating the required minimum EPL level that the computer must meet.

To determine whether or not a stand-alone computer meets its security requirements, the PROGREP model determines the appropriate operating mode and EPL level from the user responses. The algorithm that carries out the operating mode check is as follows:

- (1) Determine whether all users on the machine are cleared for the highest data classification resident on the machine. If some users are not cleared for the highest data, then the machine operating mode should be Multi-level.
- (2) If all users are cleared for the highest data on the machine, then determine if compartmented information exists on the machine. If no compartmented information exists on the machine, then determine if all users have a common need-to-know for all data on the machine. If all users have a common need-to-know for all data, then the machine operating mode should be Dedicated. If some users do not have a common need-to-know for all the data, then the machine operating mode should be System High.
- (3) If all users are cleared for the highest data on the machine and if compartmented information exists on the machine, then determine if all users have access to all compartments on the machine. If some users do not have access to all compartments, then the machine operating mode should be Compartmented. If all users have access to all compartments and have a common need-to-know for all data, then the machine operating mode should be Dedicated. If all users have access to all compartments and some users do not have a common need-to-know for all data, then the machine operating mode should be System High.

The algorithm that implements the EPL level check is as follows [13-15]:

- (1) Calculate the protection index based on the user specified data classification level, need-to-know access, and user clearance level. Note: [In Refs. 14 and 15, this protection index is referred to as the risk index, and there is also a slight indexing difference.]

- (2) Determine the minimum EPL level required to satisfy the protection index.
- (3) Calculate the designated machine's actual EPL level based on the types of security features (i.e., authorization, audit, and access controls) that are present.
- (4) Compare the machine's actual EPL level with the minimum EPL level required (based on the protection index), and ensure that the actual EPL level is greater than or equal to the minimum EPL level.

These algorithms are also used when determining the security of a network.

B. Network Security

We have based the model of network security on an extension of the notions presented above for a stand-alone computer, i.e., data classification level, user clearance level, computer EPL level, operating mode of the computers, and a protection index. A network is composed of individual computers interconnected by links. Hence, each computer has the individual security risks concerning computer access, etc., previously discussed and the propagation of local risk [17], which is related to the possibility of a vulnerability on an individual computer propagating to one or more computers linked in the network. The propagation of local risk can cause a network vulnerability to appear as if it were a stand-alone machine vulnerability.

Therefore, one would think that a simple solution would be to collapse and treat all the components in a network as a single computer system. This would require determining the highest data classification level, the lowest user clearance level, and the resulting protection index for each component. Employing these protection indices, one would then have to determine the minimum EPL level required for every component on the network to ensure that it is secure given the worst case security requirement (low user clearance and high data classification). Having determined the applicable worst-case minimum EPL level, it would be required for all components on the network, regardless of circumstances. This is neither a realistic nor a feasible solution. It would severely diminish the benefits of operating on a network. Instead we have approached the problem from a systems perspective.

With respect to security, a network can be thought of as the combination of various subsystems. Each component and each link of a network are subsystems that have specific requirements and risks associated with them. This systems perspective permits the security features of the heterogeneous subsystems to be evaluated in terms of a homogeneous network.

The algorithms that we employed for stand-alone computers are transferable with modifications and extensions to deal with the interconnectivity inherent in networks. The major security issues that are unique to a network are the propagation of local risk and the cascade problem [13, 17]. The cascade problem is concerned with desensitizing data (lowering the classification level) on one computer and then transferring the data to another computer at the lower classification level. These two problems make securing networks more complex because of the need to treat individual protection indices, risks, and security features from an aggregated perspective. We approached this system's problems by initially ensuring the security of the individual computers (as described in the previous section). Then when a connection (link) is created, it is assigned a maximum data classification level. This classification level is used to determine the data transfer capability of the link with respect to the specifics of the components being interconnected. Further security checks are executed to ensure that the heterogeneous components act in a homogeneous manner with respect to the network. Some of these checks address the operating mode and protocol compatibility between interconnected computers, the possible creation of a multilevel system, and the indication of a cascade problem. Briefly, the algorithm that implements the link security checks is as follows:

- (1) Determine the maximum data classification level of the link.
- (2) Execute a connection check to determine what is being interconnected. There are three possible cases: two links are being connected, a link and a component are being connected, or two components are being connected.
- (3) Depending on the interconnection case, further checks are executed. For the link-link connection, a data classification compatibility check is executed. For the link-component connection, a comparison between the link data classification and the data classification of the component is executed. For the component-component connection, compatibility checks for operating mode, user clearance and data classification are executed, and then a cascade problem check is invoked. The cascade check implements the nesting condition test [17]. If the nesting condition test fails, a modified version of the stand-alone EPL level algorithm is executed.

The combination of all these checks ensures the security of the network or at least provides indications and warnings to a user of any security problems with the configured network. Further research has been conducted on ensuring the security of transmissions across links. Methodologies and algorithms have also been developed that allow the determination of security and constraint problems on network paths. A brief discussion of the current PROGREP model will indicate the nature of the capabilities and security features that have been employed.

VI. FUNCTIONAL DESCRIPTION OF THE PROGREP MODEL

We sought to develop a generic model that allowed security personnel to consider "what-if" questions in the computer network and security domain. New configurations, policies, protocols, hardware, software, and operating concepts are continuously developed and deployed. The ability to use these developments or encourage their use in a cost-effective manner, in part, depends on our capability to determine their operational impact on security. To determine this impact, it is necessary to configure and characterize the computer systems forming a deployed network. This allows security personnel to specify the particular security-related characteristics of their network and to then determine their network security problems or concerns. The PROGREP model provides a mechanism that intelligently directs the user to provide the necessary input and allows the user to create a display of the network configuration. This intelligent interface aids in the dynamic network creation by providing logical control of the specification of the computer characteristics and security factors through the use of text and graphics. There are two major steps in the network representation process: building and displaying the network and related information. Both functions are carried out by menus activated by mouse buttons.

A. Network Display Functions

Five display menus correspond to and are named for the five objects that appear in a network: a network, a sub-net, a machine, a backbone, and a link. (The same as in the construction section.) These menus are employed as described in the construction menu section. The hierarchy of menus and menu functions is as follows:

Display Menus

Network Menu	Sub-Net Menu	Machine Menu	Backbone Menu	Link Menu
Attributes Magnification Scroll	Attributes	Attributes Transmit Msg	Attributes Transmit Msg	Attributes

B. Network Construction Functions

Five construction menus correspond to the five types of objects that can appear in a network: a network, a sub-net, a machine, a backbone, and a link. Each menu references more menus, which are called up in the following ways. The Network Menus are called up by clicking the mouse (left or right) while pointing the mouse at the background. The Sub-Net Menus are called up by mousing on a Sub-Net Circle. The Machine, Backbone, and Link Menus are called up by mousing on a corresponding object on the screen. The hierarchy of menus and menu functions follows:

Construction Menus

Network Menu	Sub-Net Menu	Machine Menu	Backbone Menu	Link Menu
Add Node	Delete	Add Link	Add Link	Label Link
Load Network	Move	Add Node	Add Node	
Save Network	Pop Sub-Net	Clone Machine	Delete	
View Up	Push Sub-Net	Delete	Move	
	Rename	Move	Push Sub-Net	
	View Down	Push Sub-Net	Remove Link	
	Remove Link	Rename	Rename	
			Resize	

A simple example of the type of graphical representation for a computer network that the PROGREP model is capable of analyzing and displaying is presented in the next section. The displayed network is tailored after the Integrated Computer Network (ICN) at Los Alamos National Laboratory but is by no means an exact duplication.

C. Example Network

An example network will be presented that demonstrates the graphical nature and some of the security checks and other features that are executed in PROGREP. The example will be given in three related steps; the first step is associated with interconnecting two stand-alone computers, the second step is an extension of the first by connecting a computer to one of the two existing computers through a backbone connection, and the third is a further extension of the network topology achieved by adding a new link between two of the three computers.

In the first step, both stand-alone computers A and B have been designated as possessing the following security features and capabilities: identification and authentication, audit trails, access controls, and both A and B have been designated as having a Multilevel operating mode and running the TCP/IP network communication protocols. The minimum and maximum data classification pairs on A and B are (C-NSI, S-NSI) and (S-NSI, S-RD), respectively. Finally, the minimum and maximum user clearance level pairs on both A and B are (L, QN). The creation of a network link between A and B generates the security warning indication of a possible cascade problem as seen in Fig. 1 because of the discrepancy in data classification levels on the computers.

In the second step, a network backbone running TCP/IP communication protocols and capable of handling a maximum data classification of TS-NSI has been created. When computer C is connected to the backbone, several warnings are generated (Fig. 2). These result from the user designations that have been associated with C. Computer C has been designated as possessing the following security features and capabilities: identification, authentication and audit trails, but not possessing access controls, internal labeling, and assurance testing features. Further, C has been designated as having a Dedicated operating mode with all users having a common need-to-know

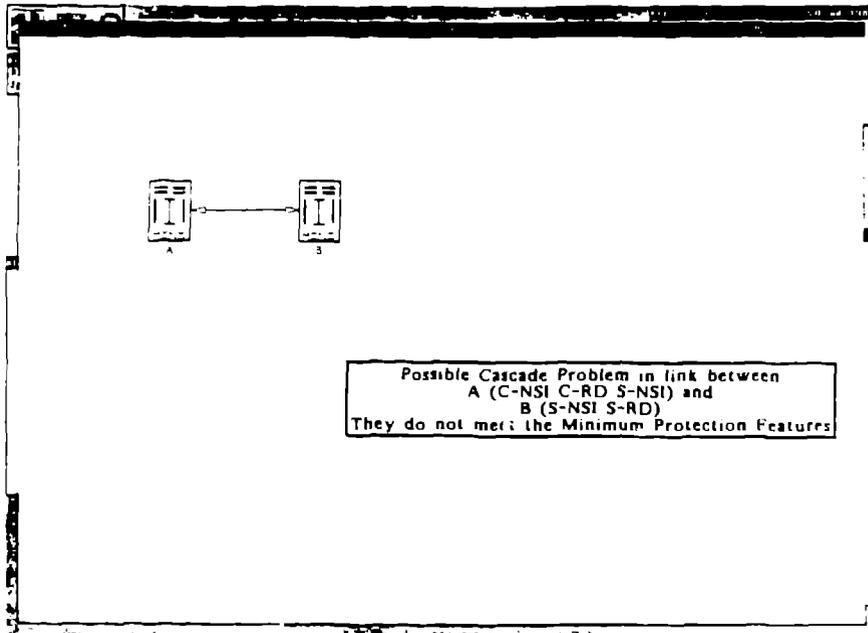


Fig. 1

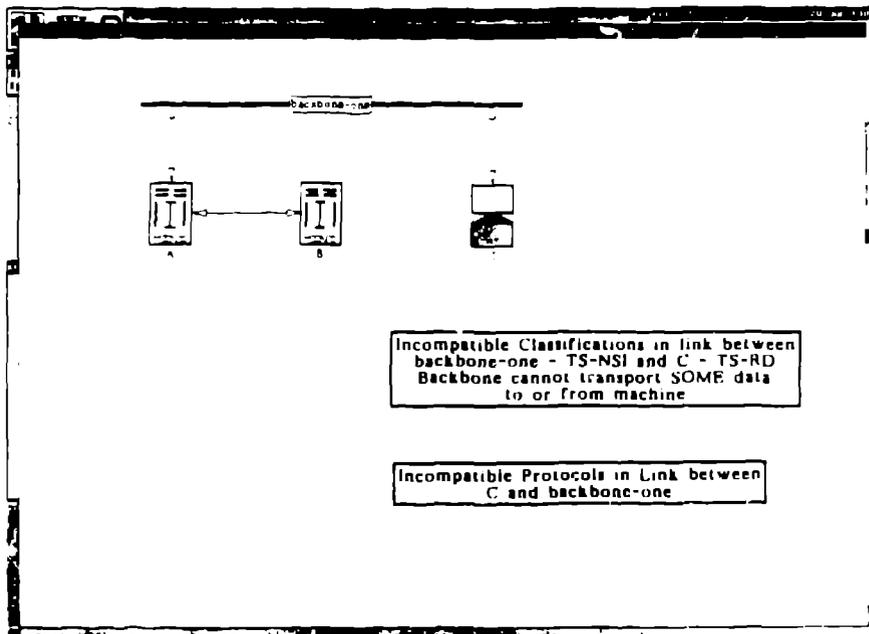


Fig. 2

and running the CHAOS communications protocols. The minimum and maximum data classification pair on C is (S-RD, TS-RD). Finally, the minimum and maximum user clearance level pair on C is (QS, QS).

Finally, in the third step, the creation of a network link between computers B and C generates the security infractions that are a result of the particular user designations. Figure 3 lists these infractions and displays the user explanation input capability.

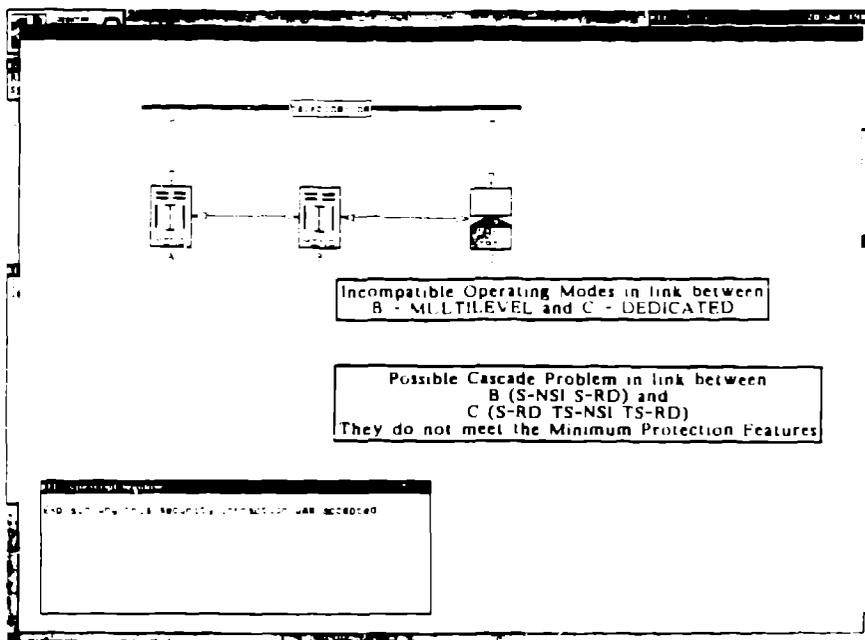


Fig. 3

This example presents a brief and partial list of the types of response that an analyst would receive from PROGREP when configuring an actual or proposed network.

VI. SUMMARY

The PROGREP model research has provided great insight into approaching the modeling of graph structures in general and computer networks in particular. It enables the display of the components and the links of a graph structure. The PROGREP model was designed to quickly and efficiently represent network components, interconnections, and interrelationships. The main features of the PROGREP model are the flexibility of intelligent and graphical interfaces. The intelligent interface aids the user in the dynamic network creation by providing logical control of the specification of the computer characteristics, parameters, properties, and security factors through the use of text and graphics. The graphical interface allows the user to display the topology of the configured network and analyze its security.

Several approaches are taken to answer network security issues. The first approach is the stand-alone security checks and data capture. These security checks ensure compliance with policy concerning the use of various operating modes and the necessary hardware and software functions associated with particular EPL levels. The second approach is the systems perspective relative to network interconnection security checks and data capture. These security checks ensure the data transfer compatibility over a link, the operating mode compatibility between components, the indication of the creation of a multilevel system, and the indication of a possible cascade problem between components. It also supports the investigation of information flow problems and constraints through the message transmission capabilities of PROGREP. The combination of all these security checks is essentially equivalent to those required in DOE Order 5637.1 [13] and those described in Part I and Appendices A, B, and section of C of the Trusted Network Interpretation [17].

A third approach is currently being developed. It incorporates the integration of network security services into the existing PROGREP model. These additional features will model the functionality of the ICN at Los Alamos and will be essentially equivalent to Part II of all of Appendix C [17]. Other future work will be to develop and incorporate simulation capabilities, to

enhance and expand the existing explanation features of the system, and to continue the network intrusion detection research that has been initiated. Currently, collaborative efforts between Los Alamos and the University of New Mexico has resulted in the prototype network level monitor [18]. We believe that these enhancements will provide the ability to address most network security and information flow problems.

REFERENCES

- [1] A. S. Tanenbaum, Computer Networks. New Jersey: Prentice Hall, 1988.
- [2] M. F. Capobianco, M. Guan, D. F. Hsu, and F. Tien, Eds., "Graph Theory and Its Applications: East and West," in Proceedings of the First China-USA International Graph Theory Conference, New York Academy of Sciences, 1989.
- [3] M. R. Garey and D. S. Johnson, Computers and Intractability: A Guide to the Theory of NP-Completeness. San Francisco: Freeman, 1979.
- [4] E. L. Lawler, J. K. Lenstra, A. H. G. Rinnooy Kan, and D. B. Shmoys, The Traveling Salesman Problem: A Guided Tour of Combinatorial Optimization. Great Britain: Wiley and Sons, 1985.
- [5] T. Nishizeki and N. Chiba, Planar Graphs: Theory and Algorithms. Amsterdam: North-Holland, 1988.
- [6] R. J. Wilson and L. W. Beineke, Applications of Graph Theory. London: Academic Press, 1979.
- [7] J. S. Dreicer and D. Topkis, private communication July 1989-October 1989, discussions related to network security and the cascade problem, in collaboration with Los Alamos National Laboratory.
- [8] D. Topkis, private communication October 1989, draft paper "The Cascade Problem for Multi-Level Security in Computer Networks."
- [9] "KEE Reference Manual," Intellicorp, May 1987.
- [10] R. Fikes and T. Kehler, "The Role of Framed-Based Representation in Reasoning," Communications of the ACM, Vol. 28, No. 9, pp. 904-922, 1985
- [11] J. F. Sowa, Conceptual Structures - Information Processing in Mind and Machine. Massachusetts: Addison-Wesley, 1984.
- [12] M. Stefik and D. G. Bobrow, "Object-Oriented Programming: Themes and Variations," AI Magazine, Vol. 6, No. 4, pp. 40-62, 1986.
- [13] "Classified Computer Security Program," DOE 5637.1, Department of Energy, January 1, 1988.
- [14] "Computer Security Requirements-Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments," CSC-STD-003-85, Department of Defense, Computer Security Center, June 25, 1985.
- [15] "Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements-Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments," CSC-STD-004-85, Department of Defense, Computer Security Center, June 25, 1985.
- [16] "Department of Defense Trusted Computer System Evaluation Criteria," CSC-STD-001-83, Department of Defense, Computer Security Center, August 15, 1983.
- [17] "Trusted Network Interpretation," NCSC-TG-005, Department of Defense, Computer Security Center, July 31, 1987.
- [18] J. S. Dreicer, A. B. Maccabe, G. Luger and D. Topkis, private communication since April 1989, discussions related to network level monitoring and application of intrusion detection techniques [genetic algorithm and neural networks].