MLSvisual User Guide

Contents

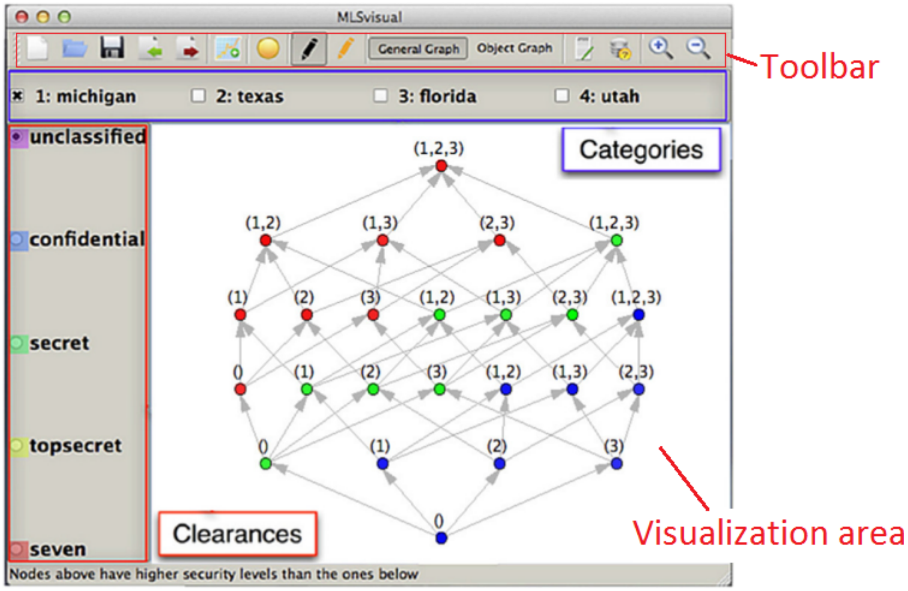
List of Figures

1 Overview

1.1 Introduction

MLSvisual is a visualization tool designed to facilitate the study and teaching of Multi-level Security based on the Bell-LaPadula access control model. The visualization focuses on the interpretation of the security level hierarchy as well as the read and write permissions to objects for users with different security levels.

1.2 User Interface



Nodes above have higher security levels than the ones below

Figure 1: User Interface

Figure 1 shows the main (highest level) window of MLSvisual. It contains a column of color-encoded clearances, a row of indexed categories, a blank visualization area and the toolbar. Figure 2 has the toolbar details.

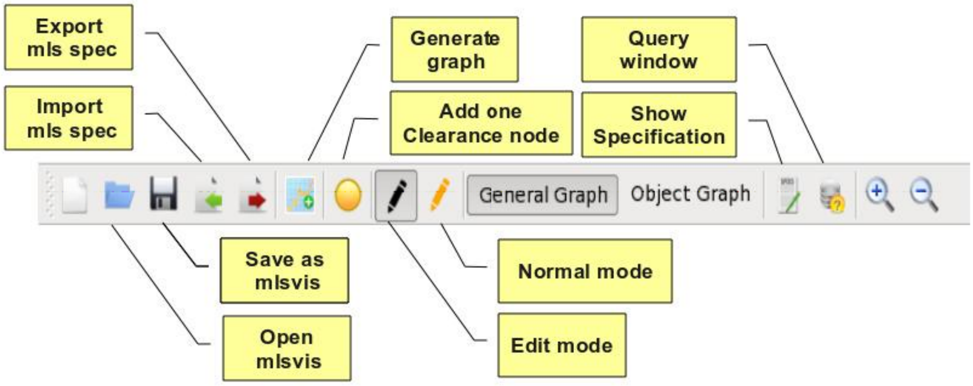


Figure 2: Toolbar

Clearances and categories appear in the main window when the user loads a policy file where a set of clearances and a set of categories are specified. In accordance with the model, a security level contains exactly one clearance and one or more categories.

The toolbar facilitates file operations, creation and modification of policy visualization graphs, switching between Normal Mode and Edit Mode, and various other functions. The visualization area is the blank part on the right hand side where graph of policies appears.

The menubar includes the File menu, the Edit menu, the View menu, and the Practice menu. Functionality available from these menus is described in later sections.

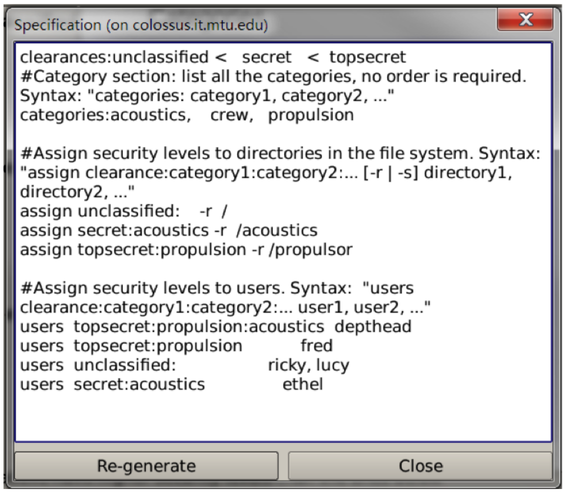
2 Input and Output

The section describes the input and output of the tool. The types of files supported and the methods to load and generate specific file types will be explained.

2.1 File Types

MLSvisual supports two types of files: MLS specifications written in the tool syntax (*.mls) and visualization descriptions (*.mlvis). The specification file contains text, in the format given below, that describes clearances hierarchy, categories, user assignment to security level and security level to object permissions. The mlvis file records an MLS specification as well as the layout of graphs in the visualization system. The user may import an MLS specification, visually modify it, and save the graph layout to a mlvis file or export to a mls file (without graph layout). MLSvisual also allows the user to visually create an MLS specification from scratch, and save or export the design to a mlsvis or mls file.

3 Specifications



```
clearances:unclassified <   secret   <  topsecret
#Category section: list all the categories, no order is required.
Syntax: "categories: category1, category2, ..."
categories:acoustics,    crew,   propulsion

#Assign security levels to directories in the file system. Syntax:
"assign clearance:category1:category2:... [-r | -s] directory1,
directory2, ..."
assign unclassified:    -r  /
assign secret:acoustics -r  /acoustics
assign topsecret:propulsion -r /propulsor

#Assign security levels to users. Syntax:  "users
clearance:category1:category2:... user1, user2, ..."
users  topsecret:propulsion:acoustics  depthead
users  topsecret:propulsion           fred
users  unclassified:                ricky, lucy
users  secret:acoustics              ethel
```

Figure 3: Specification Window

MLSvisual allows you to inspect the text version of the MLS specification. The specification is accessible from the View Menu or from the toolbar. Figure 3 shows an example specification. The detailed syntax for the specification file can be found in Appendix A.

4 General View Operations

View operations include Zoom In and Zoom Out, using the maginifier buttons on the toolbar or through the View Menu -> Zoom In or Zoom Out. CTRL+/- are shortcuts for the Zoom In and Zoom Out respectively.

5 File Operations

Following are the options available from the application File Menu to support file input and output. These file functions are also accessible from the toolbar.

- To start from scratch
  File Menu -> New
- To import/export a MLS specification (*.mls)
  File Menu -> Import/Export
- To open/save a MLS diagram (*.mlsvis)
  File Menu -> Open/Save/Save As

6 Analysis Mode

After you import an existing specification or diagram, the system comes up in Analysis Mode. This mode can also be selected from the Toolbar (Figure 2) or through Menu Edit->Analysis Mode. In this mode, you can perform some general view operations or view a particular policy from different perspectives.

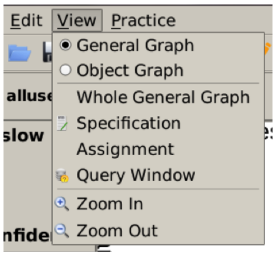


Figure 4: View Menu

Figure 4 shows the graph types in the View Menu. MLSvisual provides three types of graph to facilitate understanding of the relationship among security levels and permissions of subjects in the imported policy. The General Graph allows choosing different operations under both Analysis Mode and Edit Mode. The Whole General Graph is one type of the General Graph with scalable hierarchies. For the Object Graph, editing or exploration are supported.

6.1 General Graph (View Menu -> General Graph)

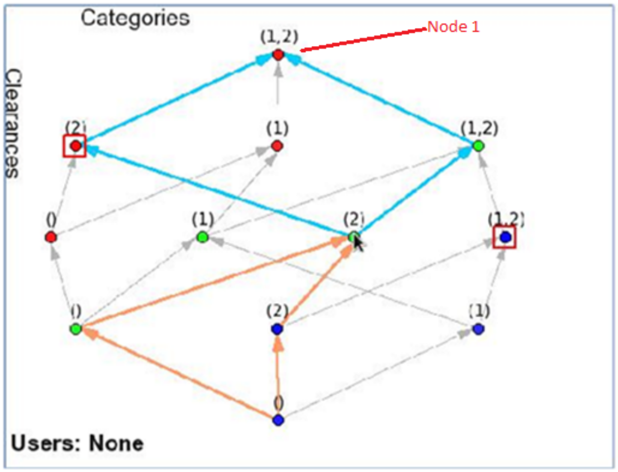


Figure 5: General Graph

6.2 Introduction

The General Graph can be selected from the toolbar as shown in Figure 2. This graph shows the relationship among certain nodes in which a user is interested. The color of a node indicates its clearance level, and the set of numbers shows the indices of its categories. An example is given in Figure 5. The Clearances levels (unclassified, confidential, secret, top secret, seven) and Categories (Michigan, Texas, Florida, Utah) have the same colors and values as those defined in Figure 1. The red color of Node 1 (the top red Node (1, 2)) represents the Clearance level "Seven". The set of (1, 2) indicates the categories for both "Michigan" and "Texas".

6.3 Exploration in General Graph

The General Graph allows users to explore the lattice formed by the set of security levels by building portions of interest. For example, the user may select a node and add its predecessors or successors, or select two nodes and build that portion of the lattice that connects these two nodes. The operations available on the General Graph in Analysis Mode in different context are described separately as below.

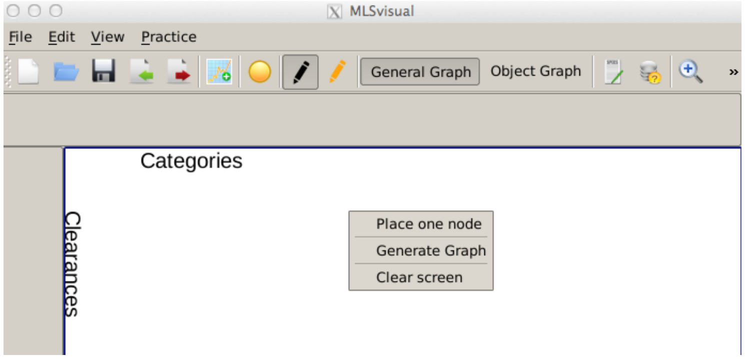
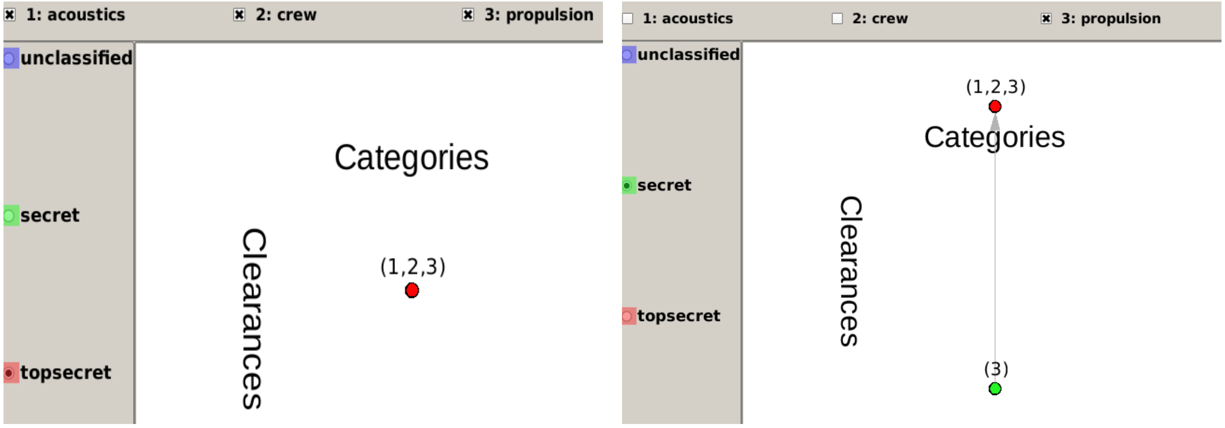


Figure 6: Context Menu in Blank Area

1 Graph Creation related Operations (right click on blank area, Figure 6)

- Place one node: Insert a new node with the selected clearance and category on the canvas.
- Generate graph: Generate all the levels between the first node and second node specified using Mark as first node and Mark as second node.
- Clear Screen: Clear all the edges and nodes on screen while clearance and categories stay the same.

Users can create the graph through the combination of above operations. First, designate two nodes and then generate the full directed graph between them using Generate Graph operation. Nodes along all paths from the lower node to the upper node, as well as the edges between them, are generated. This is useful when investigating the reachability of the two given nodes, the possible paths and the involved security levels. It also avoids the overwhelming and repetitive operations of adding nodes.



(a) First Node

(b) Second Node

Figure 7: Designing First and Second for Evaluation

Here is one example to illustrate this approach. It can be divided to three operation steps:

1) Add one topsecret node with all the categories (1,2,3), as shown in Figure 7 a);

2) Add a second node, which is secret with category (3), as shown Figure 7 b);

3) Generate the graph between the two nodes. The result is given in Figure 8.

Comparing to above approach, user can create the graph for a certain specification through adding security level node one at a time. This approach draws an edge directly between nodes when they are related under the dominates relation. When a new node is added, the graph is updated. This helps one determine when one node is reachable from another. It has value when users are not interested in the detailed paths between nodes and prefer just knowing the reachability.

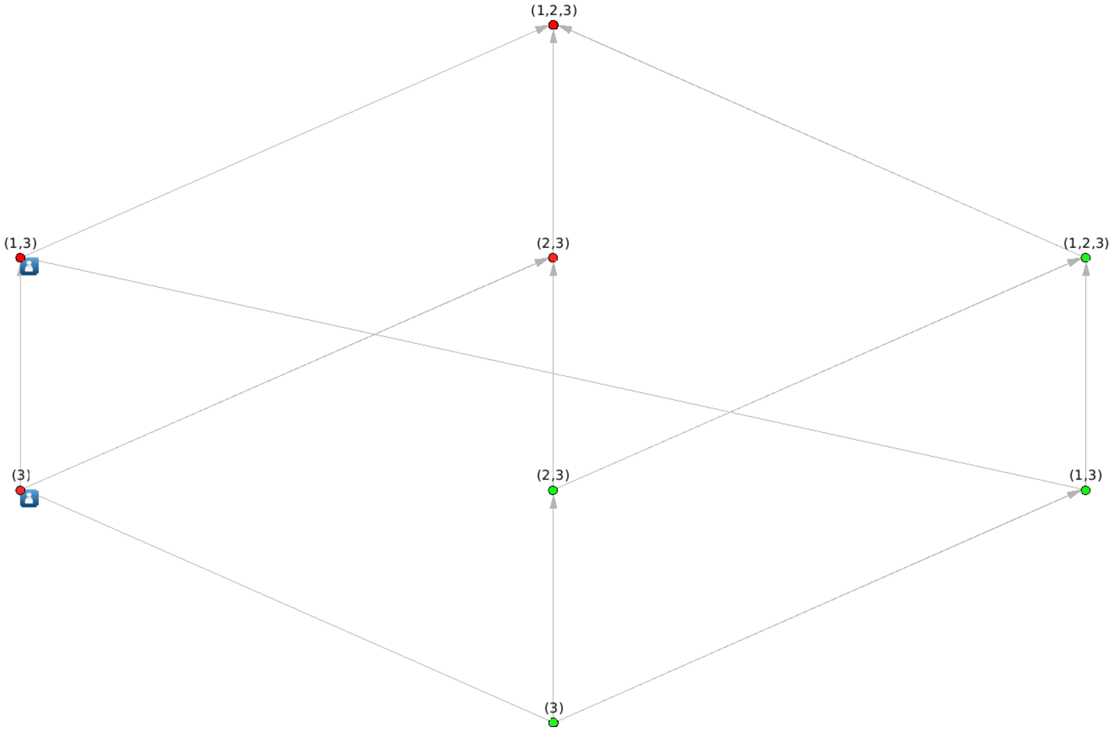


Figure 8: Generated Graph between Red Node (1,2,3) and Green Node (3)

2 Right click on a node (Figure 9)

- Mark as first node: Set the right clicked node as the first node for highlighting edges, this is explained in the Hover on a node. The chosen node will be highlighted by a black frame around it.
- Mark as second node: Set the right clicked node as the second node for highlighting edges. The chosen node will be highlighted by a black frame around it.
- Add predecessors: Insert the direct predecessors of the right clicked node into the current graph on canvas.
- Add successors: Insert the direct successors of the right clicked node into the current graph on canvas.

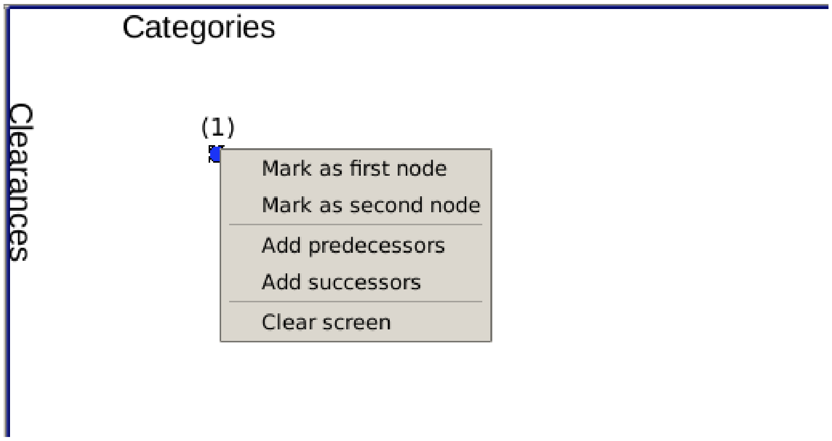
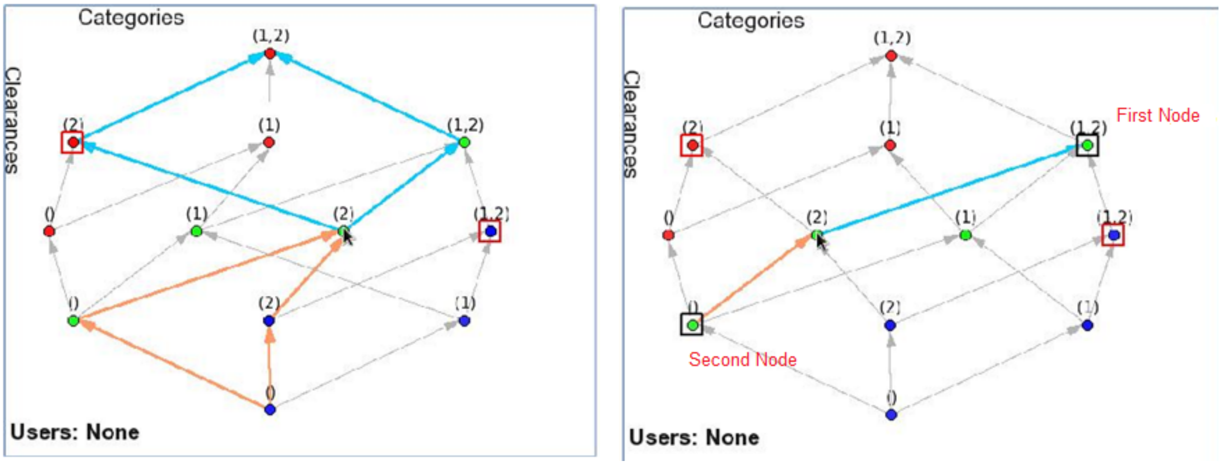


Figure 9: Context Menu for Security Level Node

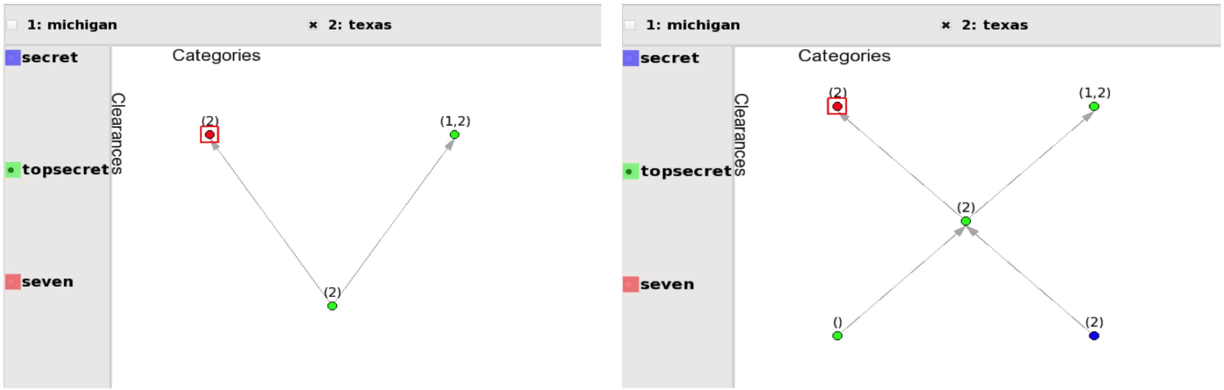


(a) Before

(b) After

Figure 10: Assigning First and Second Nodes

Figures 10 (a) and (b) show the General Graph before and after marking the first and second nodes.



(a) Predecessors for Green Node

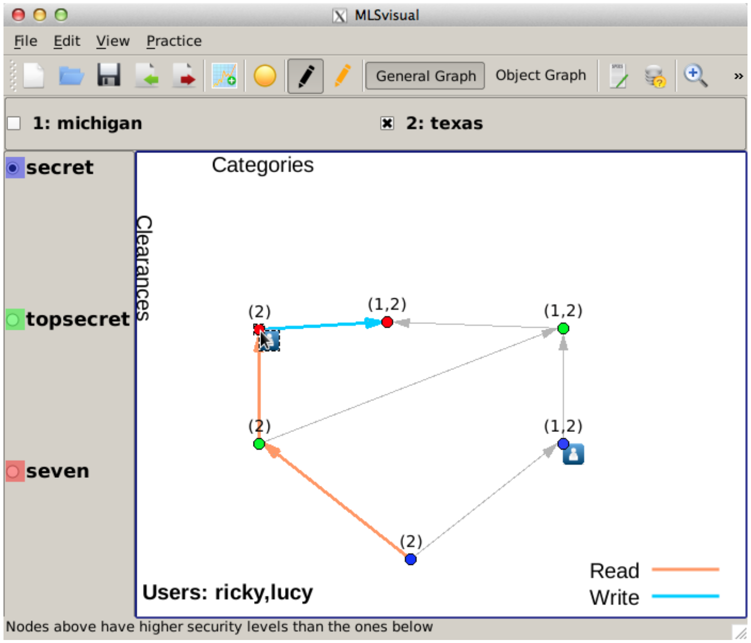
(b) Successors for Green Node

Figure 11: Assigning Predecessors and Successors

Figure 11 (a) depicts adding predecessors. Figure 11 (b) depicts adding successors.

3 Hover on a node

Edges from the first node through the hovered node to the second node will be highlighted. The edges connecting to the nodes that the hovered node can write are highlighted in light blue while those connecting the nodes can be read are highlighted in orange. If the node has user(s) assigned to it, the users' name will show up at the bottom left corner. All the nodes that have assigned users are marked by with a frame, as indicated in Figure 12.



Users: ricky,lucy

Nodes above have higher security levels than the ones below

Figure 12: Identification of Levels with User Assignment

6.4 Object Graph (View-> Object Graph)

The Object Graph is selected from the application [View Menu or from the Toolbar. This graph shows the security level assignment of objects. This graph has a number of concentric circles with the center being the root directory. The circles with increasing radii represent directories of increasing directory depth.

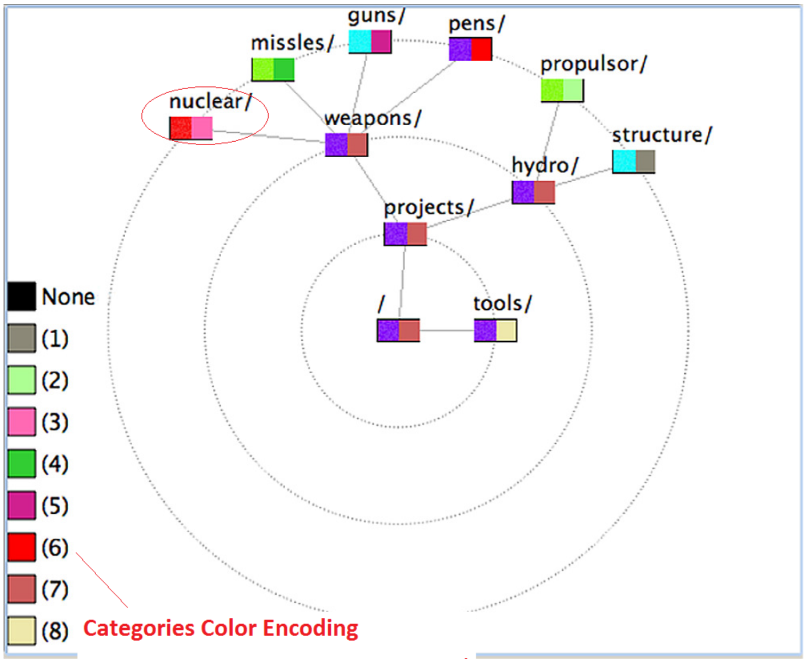


Figure 13: Object Graph

The nodes in the graph are objects and the edges represent the membership of the directory. Each node is a rectangle with two colors that represent the security level. The left color indicates its clearance and the right one shows the category based on the color encoding for categories shown in the legend at the left bottom corner of the visualization area. Please see Figure 13 for an example. For the Node nuclear as marked in the upper left corner, the left red color indicates the security level of seven, and the right pink color represents Category of (3).

6.5 Whole Graph (View -> Whole General Graph)

To help understand the Whole Graph, Figure 14 is given for the original General Graph without grouping, which is generated from an existing mlsvis file through File Menu -> Open.

The Whole Graph can show the hierarchy of all security levels. When the number of layers of the graph gets beyond five, nodes of the same clearance level will be grouped as one big node with a label that indicates the number of actual security nodes. Clicking on a group node depicts the individual nodes represented by the group node.

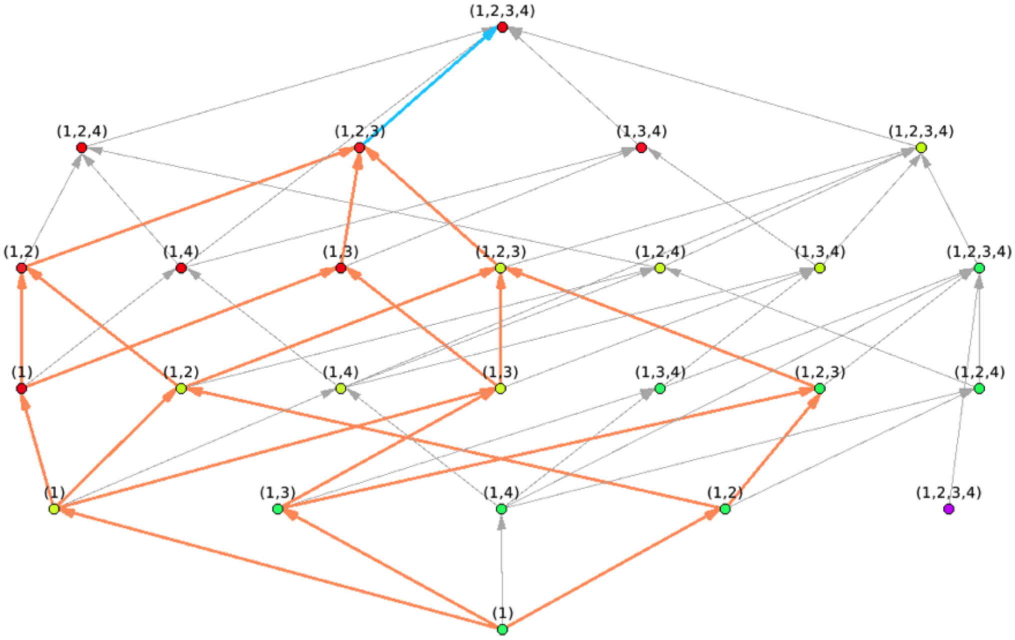


Figure 14: General Graph without Grouping

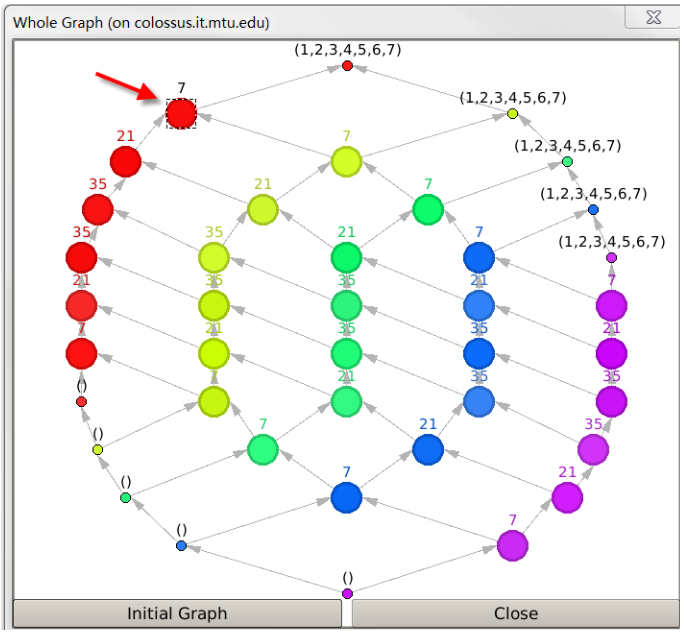


Figure 15: General Graph with Grouping at Start

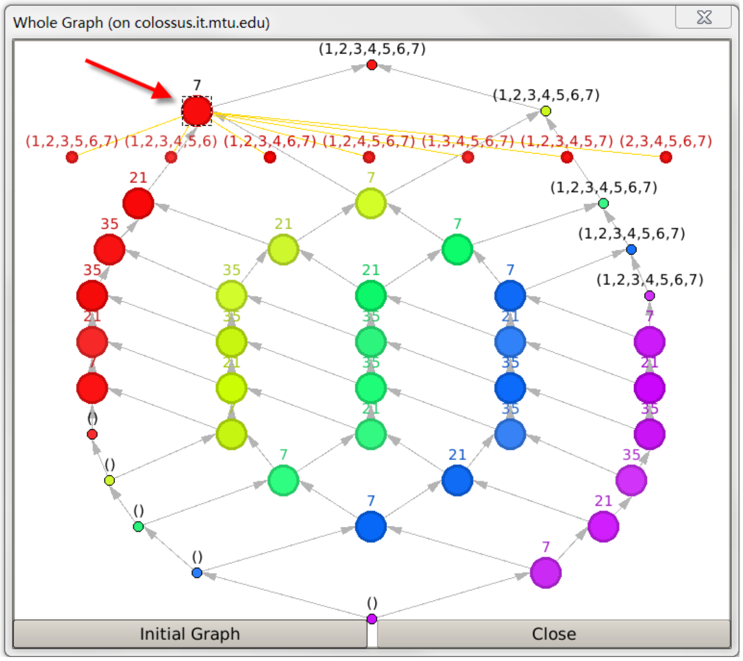


Figure 16: After Expanding One Group Node

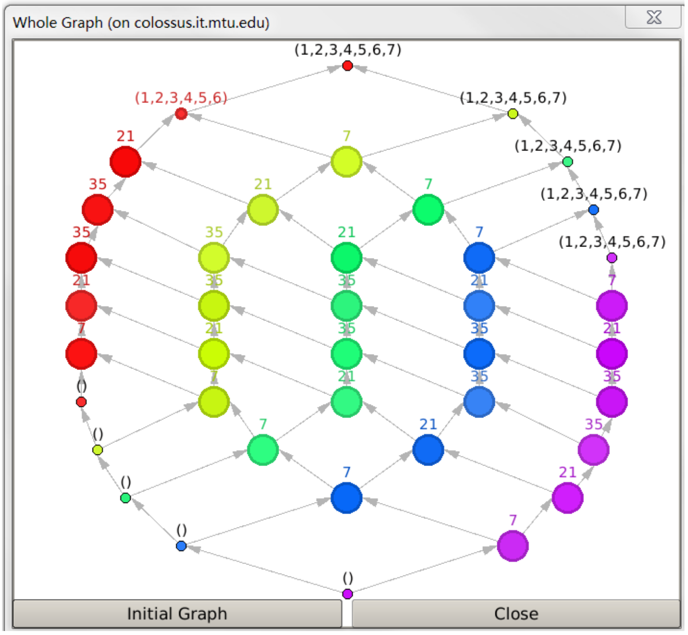


Figure 17: Select an Individual Node and Update Hierarchy

The following steps with a sequence of figures break down the functionality described above:

1) Select View -> Whole General Graph, then you will see Figure 15 General Graph with grouping at start.

2) Click on one of the Group node, for example, the one marked by the red arrow in Figure 15. The group node will then be extended to 7 individual nodes, as shown in Figure 16.

3) Right clicking on the individual node and choosing Revert to group node collects this individual node into its corresponding group node, along with all the other individual nodes in the group node. It will go back to Figure 15, Whole Graph with Grouping at start, since no other nodes are extended.

4) If you select one of these individual nodes, the group node will be replaced by the individual nodes and the hierarchy depiction is updated. This is depicted in Figure 17.

5) The Initial Graph button on the window is to reset the graph to the initial status. After clicking Initial Graph, Figure 15 shows Group nodes at start.

7 Edit Mode

In this section, we will introduce the operations in Edit Mode, which can be selected either through Edit -> Edit Mode (Figure 18), or button on the toolbar (Figure 2). In this mode, User can add or delete Clearance and Category, and assign Directory and Users to the Nodes in the General Graph, which is the only type of graph available in Edit Mode.

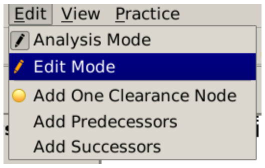


Figure 18: Edit Menu

1 Category and Clearance Operations

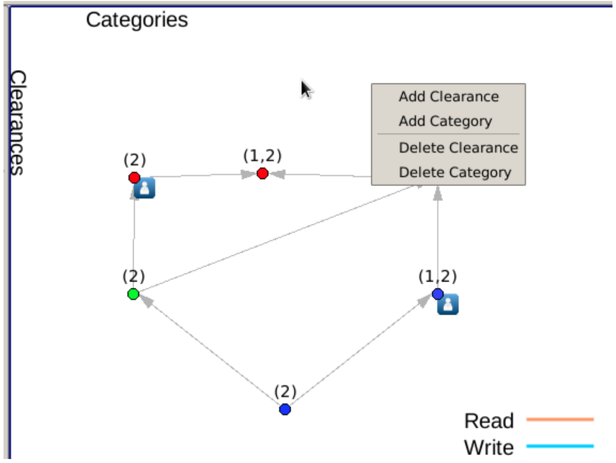


Figure 19: Edit Menu

The addition and deletion operations are available through the context menu which pops up when clicking on the blank area as shown in Figure 19. Below are the options and the associated functionalities available from that menu:

- Add clearance: Add a new clearance at specification level.
- Add category: Add a new category to existing categories.
- Delete clearance: Delete a clearance from the existing clearances.
- Delete category: Delete a category from the existing categories.

2 Directory and Users Operation

Directory and Users can be assigned to the related node through the context menu, which occurs when clicking a node as shown in Figure 20:

- Assign directory: Assign the right clicked security level to the input directories. The format should be [[–r | –s | –r -s] path1, . . . , path N;]*
- Assign users: Assign the right clicked security level to the input users. The user names are separated by commas, and the names can only include letters.

The user names are separated by commas, and the names can only include letters.

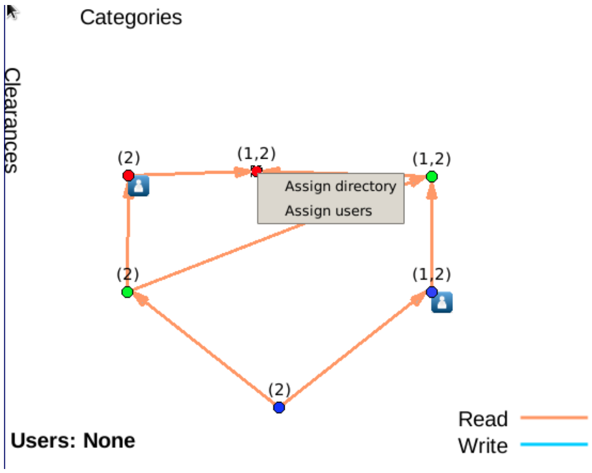
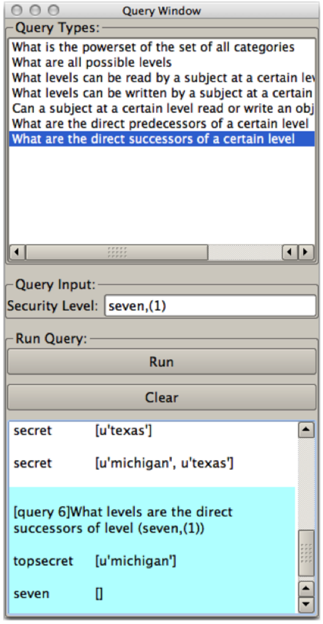


Figure 20: Context Menu when Clicking on a Node

8 Query (View -> Query Window)

The Query Window contains questions to help the exploration of MLS policies. It provides answers to some frequently asked questions such as what all sets of categories are, what the possible security levels are and whether a specific subject has read or write permission to an object. The format is clearance,(1,2). The numbers in the parenthesis are the numbers related to the categories listed in the MLSvisual main window. (See Figure 1)

For example, one query is to ask what levels are the direct successors of level (seven,(1)).The bottom section in Figure 21 shows the query result. Please note that currently no query animation function is available for MLSvisual.



What is the powerset of the set of all categories
What are all possible levels
What levels can be read by a subject at a certain lev
What levels can be written by a subject at a certain
Can a subject at a certain level read or write an obj
What are the direct predecessors of a certain level
What are the direct successors of a certain level

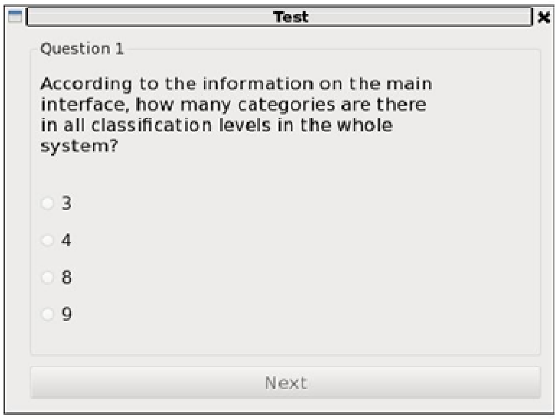
Security Level: seven,(1)

```
secret      [u'texas']

secret      [u'michigan', u'texas']

[query 6]What levels are the direct
successors of level (seven,(1))

topsecret   [u'michigan']

seven       []
```

Figure 21: Query Questions

9 Practice Test

9.1 Test (Practice -> Test)



Question 1

According to the information on the main interface, how many categories are there in all classification levels in the whole system?

○ 3

○ 4

○ 8

○ 9

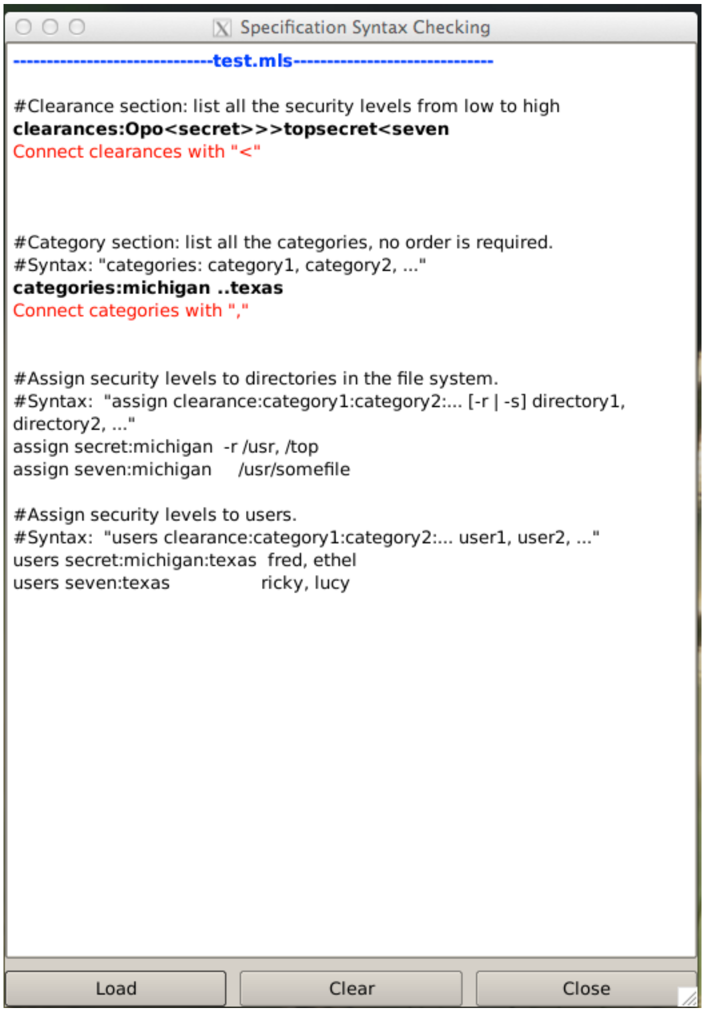
Figure 22: Test Window

A test will be initiated by clicking on "Practice->Test". One example test window is shown in Figure 22. Users can only go to the next question. At the end, the users will be asked to enter name, email address of instructor and an email containing their answers will be sent to the receiver.

9.2 Specification Diagnosis (Practice -> Specification Syntax Checking)

The purpose of this functionality is to help users get familiar with the correct format of MLS specification files. To make the specification applicable to the program, checking the custom specification file before importing it to the program will precisely locate the possible errors.

A dialog will be presented to the users to load in their specification file as shown in Figure 23. If the file is in the right format, a green comment will indicate that the specification file is usable. Otherwise, red comments below the problematic lines (Bold lines) will provide suggestion of changes. The Load button allows another file to be examined. Results from different files are separated by a dashed line. The Clear button serves to clear the results if needed.



```
-----------------------------test.mls-----------------------------

#Clearance section: list all the security levels from low to high
clearances:Opo<secret>>>topsecret<seven
Connect clearances with "<"



#Category section: list all the categories, no order is required.
#Syntax: "categories: category1, category2, ..."
categories:michigan ..texas
Connect categories with ","


#Assign security levels to directories in the file system.
#Syntax:  "assign clearance:category1:category2:... [-r | -s] directory1,
directory2, ..."
assign secret:michigan  -r /usr, /top
assign seven:michigan     /usr/somefile

#Assign security levels to users.
#Syntax:  "users clearance:category1:category2:... user1, user2, ..."
users secret:michigan:texas  fred, ethel
users seven:texas                ricky, lucy
```

Figure 23: Specification Diagnosis

Appendices

A

MLS specification normally contains four sections.

A.1 Clearance Statement

Define one or more clearance levels, which are then available to other parts of a MLS specification. Clearance Statement starts with keyword clearances and then lists all the defined security levels from low to high.

Syntax format: "clearances: level1<level2<. . . "

For example, there are three security levels from low to high as: unclassified, secret, topsecret. We define the Clearance Statement as below:

clearances: unclassified<secret<topsecret

A.2 Category Statement

Define one or more categories, which are then available to other parts of a MLS specification. Category Statement starts with keyword categories and then lists all the categories after it without ordering.

Syntax format: “categories: category1, category2,. . . ”

For example:

categories: acoustics, crew, propulsion

A.3 Directory Security Assignment Statement

Assign security levels to directories in the file system. The statement starts with assign, and then follows with the clearance level and categories, which are assigned to the directory occurring at the end of the statement. One directory can be assigned to multiple categories.

Syntax format: “assign clearance: category1: category2. . . [–r | –s] directory1, directory2,. . . ”

Here are some examples:

```
assign unclassified:    -r  /
assign secret:acoustics -r  /acoustics
assign topsecret:propulsion -r /propulsor
```

A.4 User Security Assignment Statement

Assign security levels to users. This statement starts with keyword users and follows with the clearance level and categories, which are assigned to the user list occurring at the end of the statement.

Syntax format: “users clearance: category1: category2. . . user1, user2. . . ”

For examples:

```
users  topsecret:propulsion:acoustics  depthead
users  topsecret:propulsion            fred
users  unclassified:                   ricky, lucy
```