

BLACK BOX TEST PLAN – SecurityTreeManager

Justin Schwab

To run software from eclipse, right-click the project folder, and select **run as... > java application**. Run the class **SecurityTreeManagerUI**.

Tests must be run sequentially. Please make sure that the files listed below the test plan table exist and contain the provided data. Test file contents are at the very bottom of this document.

Test ID	Description	Expected Results	Actual Results
invalidAttackFile (ECP-trying to use file that doesn't exist.)	Preconditions: <ul style="list-style-type: none">SecurityMangerUI has been loadedthe files "missing1.txt" and "missing2.txt" do not exist. Steps: <ul style="list-style-type: none">choose "Build Attack Tree"when prompted for traversal files, type "missing1.txt missing2.txt" and press enter.	User is re-prompted: One or more file(s) not found. Please enter a PreOrder Traversal file and a PostOrder Traversal file, separated by a space	User is re-prompted: One or more file(s) not found. Please enter a PreOrder Traversal file and a PostOrder Traversal file, separated by a space
attackTreeBuild (ECP-building an attack tree with "sample-pre order.txt" and "sample-post order.txt")	Preconditions: <ul style="list-style-type: none">Test 1 passedThe files "input/ddos-preorder.txt" and "input/ddos-postorder.txt" exist. Steps: <ul style="list-style-type: none">type "input/ddos-preorder.txt input/ddos-postorder.txt" and press enter.	Program confirms that the attack tree was built: Attack tree built! Choose an option: (1) - View goal node summary (2) - View level-order traversal (m) - Main menu	Program confirms that the attack tree was built: Attack tree built! Choose an option: (1) - View goal node summary (2) - View level-order traversal (m) - Main menu

<p>levelOrderTraversal (ECP - print a level-order traversal of the attack tree)</p>	<p>Preconditions:</p> <ul style="list-style-type: none"> • Test 2 has passed. <p>Steps:</p> <ul style="list-style-type: none"> • User selects the option "View level-order traversal" 	<p>Program Outputs:</p> <pre> LevelOrder[GOAL Step[Use DDoS Attack to Disrupt All Users, C=21557.12, P=0.878, I=8.00] OR Step[Attack Servers, C=14099.02, P=0.692, I=7.48] OR Step[Attack Comm Infrastructure, C=32857.14, P=0.559, I=8.00] OR Step[Attack All Clients, C=10000.00, P=0.100, I=5.00] OR Step[Direct BOTNET against key Servers, C=5580.65, P=0.560, I=7.48] OR Step[Infect Servers with Worm/Virus, C=30000.00, P=0.300, I=7.00] OR Step[Attack Switches, C=30000.00, P=0.300, I=7.00] OR Step[Attack Routers, C=30000.00, P=0.300, I=7.00] OR Step[Attack DNS, C=50000.00, P=0.100, I=8.00] OR Step[Infect Clients with Worm/Virus, C=10000.00, P=0.100, I=5.00] OR Step["Rent" Existing BOTNET, C=5000.00, P=0.500, I=6.00] OR Step[Build a BOTNET, C=8000.00, P=0.120, I=7.48] AND Step[Find Vulnerable Computers, C=2000.00, P=0.500, I=3.00] AND Step[Infect Computer with BOT, C=5000.00, P=0.400, I=4.00] AND Step[Remain Undetected, C=1000.00, P=0.600, I=4.00]]</pre>	<p>Program Outputs:</p> <pre> LevelOrder[GOAL Step[Use DDoS Attack to Disrupt All Users, C=21557.12, P=0.878, I=8.00] OR Step[Attack Servers, C=14099.02, P=0.692, I=7.48] OR Step[Attack Comm Infrastructure, C=32857.14, P=0.559, I=8.00] OR Step[Attack All Clients, C=10000.00, P=0.100, I=5.00] OR Step[Direct BOTNET against key Servers, C=5580.65, P=0.560, I=7.48] OR Step[Infect Servers with Worm/Virus, C=30000.00, P=0.300, I=7.00] OR Step[Attack Switches, C=30000.00, P=0.300, I=7.00] OR Step[Attack Routers, C=30000.00, P=0.300, I=7.00] OR Step[Attack DNS, C=50000.00, P=0.100, I=8.00] OR Step[Infect Clients with Worm/Virus, C=10000.00, P=0.100, I=5.00] OR Step["Rent" Existing BOTNET, C=5000.00, P=0.500, I=6.00] OR Step[Build a BOTNET, C=8000.00, P=0.120, I=7.48] AND Step[Find Vulnerable Computers, C=2000.00, P=0.500, I=3.00] AND Step[Infect Computer with BOT, C=5000.00, P=0.400, I=4.00] AND Step[Remain Undetected, C=1000.00, P=0.600, I=4.00]]</pre>
--	---	--	--

invalidLogFile (ECP- trying to use file that doesn't exist.)	Preconditions: <ul style="list-style-type: none"> • Test 3 passed Steps: <ul style="list-style-type: none"> • User is prompted for what to do and enters "m" to go back to the main menu • User then chooses the menu option to "Build Log Tree" • When prompted for a Log file, user enters "missing1.txt" 	Program Outputs: File not found Please enter a Log File:	Program Outputs: File not found Please enter a Log File:
retrieveLogE ntries (ECP – print log entries)	Preconditions: <ul style="list-style-type: none"> • Test 4 passed Steps: <ul style="list-style-type: none"> • User enters "input/sample-log.txt" • User then chooses option to "View Level-Order Traversal" 	Program Outputs: LevelOrder[LogEntry[timestamp=2015/09/13 02:58:49, user=user2, description=save patient list] LogEntry[timestamp=2012/12/18 16:25:58, user=user18, description=view diagnoses] LogEntry[timestamp=2016/12/12 06:28:13, user=user6, description=edit patient representative list] LogEntry[timestamp=2011/08/12 20:13:47, user=user1, description=create basic health information] LogEntry[timestamp=2013/07/19 22:49:10, user=user1, description=edit email reminders] LogEntry[timestamp=2015/10/07 05:34:10, user=user7, description=edit email reminders] LogEntry[timestamp=2010/06/27 03:45:37, user=user10, description=delete calendar] LogEntry[timestamp=2012/09/17 11:45:24, user=user16, description=create upcoming appointments] LogEntry[timestamp=2013/05/14 21:16:36, user=user3, description=add upcoming appointments]	Program Outputs: LevelOrder[LogEntry[timestamp=2015/09/13 02:58:49, user=user2, description=save patient list] LogEntry[timestamp=2012/12/18 16:25:58, user=user18, description=view diagnoses] LogEntry[timestamp=2016/12/12 06:28:13, user=user6, description=edit patient representative list] LogEntry[timestamp=2011/08/12 20:13:47, user=user1, description=create basic health information] LogEntry[timestamp=2013/07/19 22:49:10, user=user1, description=edit email reminders] LogEntry[timestamp=2015/10/07 05:34:10, user=user7, description=edit email reminders] LogEntry[timestamp=2010/06/27 03:45:37, user=user10, description=delete calendar] LogEntry[timestamp=2012/09/17 11:45:24, user=user16, description=create upcoming appointments] LogEntry[timestamp=2013/05/14 21:16:36, user=user3, description=add upcoming appointments]

		LogEntry[timestamp=2015/07/10 00:26:58, user=user15, description=add patient representative list]	LogEntry[timestamp=2015/07/10 00:26:58, user=user15, description=add patient representative list]
		LogEntry[timestamp=2007/11/24 24:10:24, user=user19, description=update appointment requests]	LogEntry[timestamp=2007/11/24 24:10:24, user=user19, description=update appointment requests]
		LogEntry[timestamp=2010/07/14 12:53:15, user=user7, description=remove diagnoses]	LogEntry[timestamp=2010/07/14 12:53:15, user=user7, description=remove diagnoses]
		LogEntry[timestamp=2013/06/16 24:28:33, user=user3, description=add appointment requests]	LogEntry[timestamp=2013/06/16 24:28:33, user=user3, description=add appointment requests]
		LogEntry[timestamp=2015/02/10 16:12:23, user=user15, description=modify office visit information]	LogEntry[timestamp=2015/02/10 16:12:23, user=user15, description=modify office visit information]
		LogEntry[timestamp=2015/08/01 03:54:17, user=user10, description=update appointment requests]	LogEntry[timestamp=2015/08/01 03:54:17, user=user10, description=update appointment requests]
		LogEntry[timestamp=2007/06/01 07:37:31, user=user3, description=print immunizations]	LogEntry[timestamp=2007/06/01 07:37:31, user=user3, description=print immunizations]
		LogEntry[timestamp=2009/01/03 10:35:47, user=user11, description=view email reminders]	LogEntry[timestamp=2009/01/03 10:35:47, user=user11, description=view email reminders]
		LogEntry[timestamp=2014/10/06 13:11:31, user=user5, description=edit office visit information]	LogEntry[timestamp=2014/10/06 13:11:31, user=user5, description=edit office visit information]
		LogEntry[timestamp=2015/03/29 13:38:31, user=user7, description=view demographics]	LogEntry[timestamp=2015/03/29 13:38:31, user=user7, description=view demographics]
		LogEntry[timestamp=2015/07/17 15:55:25, user=user8, description=save immunizations]	LogEntry[timestamp=2015/07/17 15:55:25, user=user8, description=save immunizations]
]]

retrieveBoundaryLogEntry(BV – look up last log entry from input file)	Preconditions: <ul style="list-style-type: none"> Test 5 passed Steps: <ul style="list-style-type: none"> User is prompted for what to do and chooses the option to “Filter Logs by Date” User then is prompted for date and user enters “06-16-2013” 	Program Outputs: LogEntry[timestamp=2013/06/16 24:28:33, user=user3, description=add appointment requests]	Program Outputs: LogEntry[timestamp=2013/06/16 24:28:33, user=user3, description=add appointment requests]
invalidDate(DT- enter an invalid date)	Preconditions: <ul style="list-style-type: none"> Test 6 passed Steps: <ul style="list-style-type: none"> User is prompted for what to do and chooses the option to “Filter Logs by Date” User then is prompted for date and user enters “Monday” 	Program Outputs: Invlid Option Choose an option: (1) - Filter Logs by Date (2) - View level-order traversal (m) - Main menu	Program Outputs: Invlid Option Choose an option: (1) - Filter Logs by Date (2) - View level-order traversal (m) - Main menu
exitProgram(ECP - exits the program)	Preconditions: <ul style="list-style-type: none"> Test 7 passed Steps: <ul style="list-style-type: none"> User enters “m” to return to main menu User enters “q” to exit program 	Program exits with output: <terminated>	Program exits with output: <terminated>

Test Files

input/ddos-preorder.txt

GOAL Use DDoS Attack to Disrupt All Users
0 Attack Servers
0 Direct BOTNET against key Servers
0 0.5 6 5000 "Rent" Existing BOTNET
0 Build a BOTNET
A 0.5 3 2000 Find Vulnerable Computers
A 0.4 4 5000 Infect Computer with BOT
A 0.6 4 1000 Remain Undetected
0 0.3 7 30000 Infect Servers with Worm/Virus
0 Attack Comm Infrastructure
0 0.3 7 30000 Attack Switches
0 0.3 7 30000 Attack Routers
0 0.1 8 50000 Attack DNS
0 Attack All Clients
0 0.1 5 10000 Infect Clients with Worm/Virus

input/ddos-postorder.txt

0 0.5 6 5000 "Rent" Existing BOTNET
A 0.5 3 2000 Find Vulnerable Computers
A 0.4 4 5000 Infect Computer with BOT
A 0.6 4 1000 Remain Undetected
0 Build a BOTNET
0 Direct BOTNET against key Servers
0 0.3 7 30000 Infect Servers with Worm/Virus
0 Attack Servers
0 0.3 7 30000 Attack Switches
0 0.3 7 30000 Attack Routers
0 0.1 8 50000 Attack DNS
0 Attack Comm Infrastructure
0 0.1 5 10000 Infect Clients with Worm/Virus
0 Attack All Clients
GOAL Use DDoS Attack to Disrupt All Users

input/sample-log.txt

9-13-2015 2:58:49,user2,save patient list
12-18-2012 16:25:58,user18,view diagnoses
7-19-2013 22:49:10,user1,edit email reminders
7-10-2015 0:26:58,user15,add patient representative list
8-1-2015 3:54:17,user10,update appointment requests
12-12-2016 6:28:13,user6,edit patient representative list
2-10-2015 16:12:23,user15,modify office visit information
10-7-2015 5:34:10,user7,edit email reminders
8-12-2011 20:13:47,user1,create basic health information
6-27-2010 3:45:37,user10,delete calendar
7-17-2015 15:55:25,user8,save immunizations
10-6-2014 13:11:31,user5,edit office visit information
3-29-2015 13:38:31,user7,view demographics
7-14-2010 12:53:15,user7,remove diagnoses
11-24-2007 24:10:24,user19,update appointment requests
5-14-2013 21:16:36,user3,add upcoming appointments
6-1-2007 7:37:31,user3,print immunizations
9-17-2012 11:45:24,user16,create upcoming appointments
1-3-2009 10:35:47,user11,view email reminders
6-16-2013 24:28:33,user3,add appointment requests