A Task Centered Framework for Computer Security Data Visualization

Xiaoyuan Suo, Ying Zhu, Scott Owen

Department of Computer Science

Georgia State University

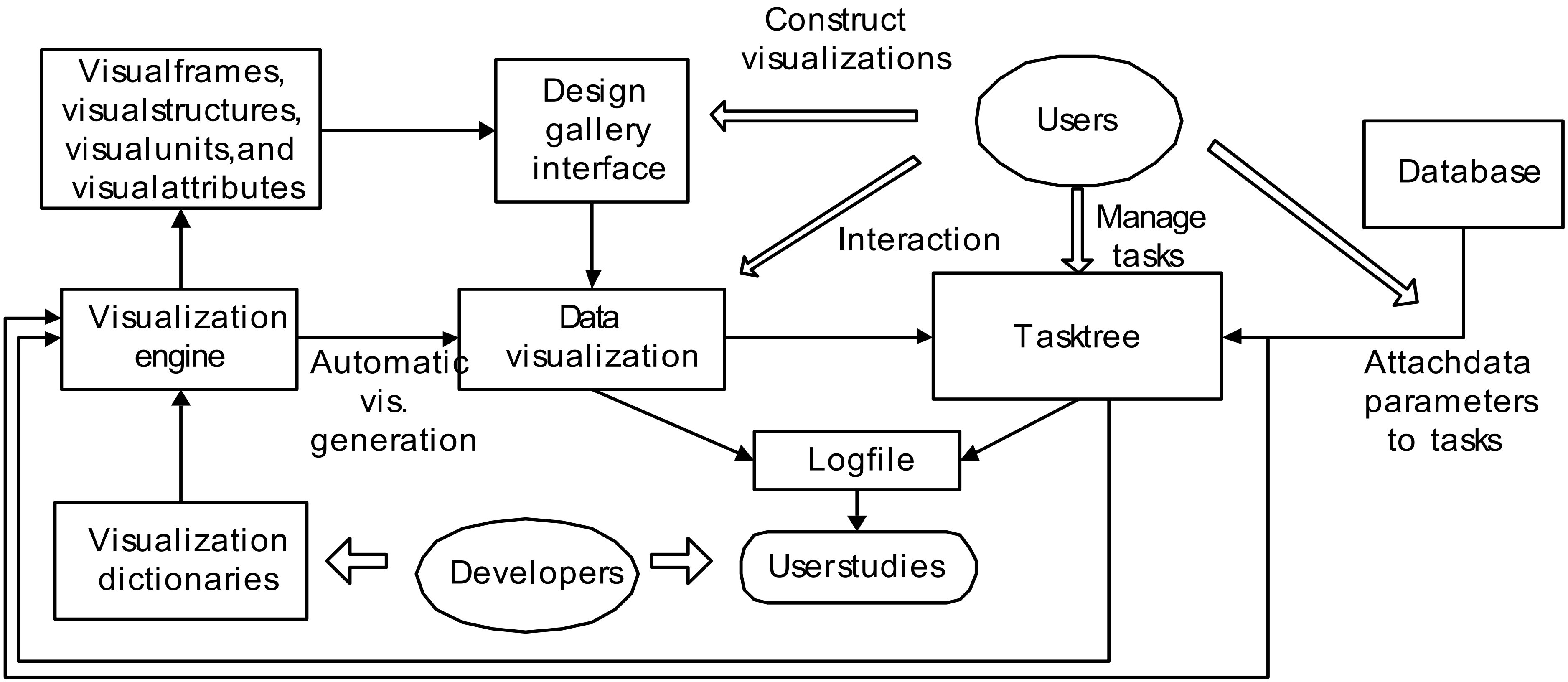
Motivation

- For most existing visualization systems it is often not clear what specific tasks they are designed for.
- Most existing visualization systems provide only low level interaction techniques
- We need a higher level interaction technique to help end users operate at the level of tasks

Problem Solving Process

- Open the data files or connect to the databases.
- Divide the work into multiple tasks. Create a hierarchical task tree.
- Associate data parameters with each task.
- For each task, construct a data-visualization. A visualization engine will automatically recommend multiple design choices, which are presented in a design-gallery style interface. The designs are selected and ranked based on their accuracy, utility, and efficiency scores in the visualization dictionaries.
- Explore the data visualization through interaction techniques.

Task-centered Visualization Design Architecture



User Constructed Visualization

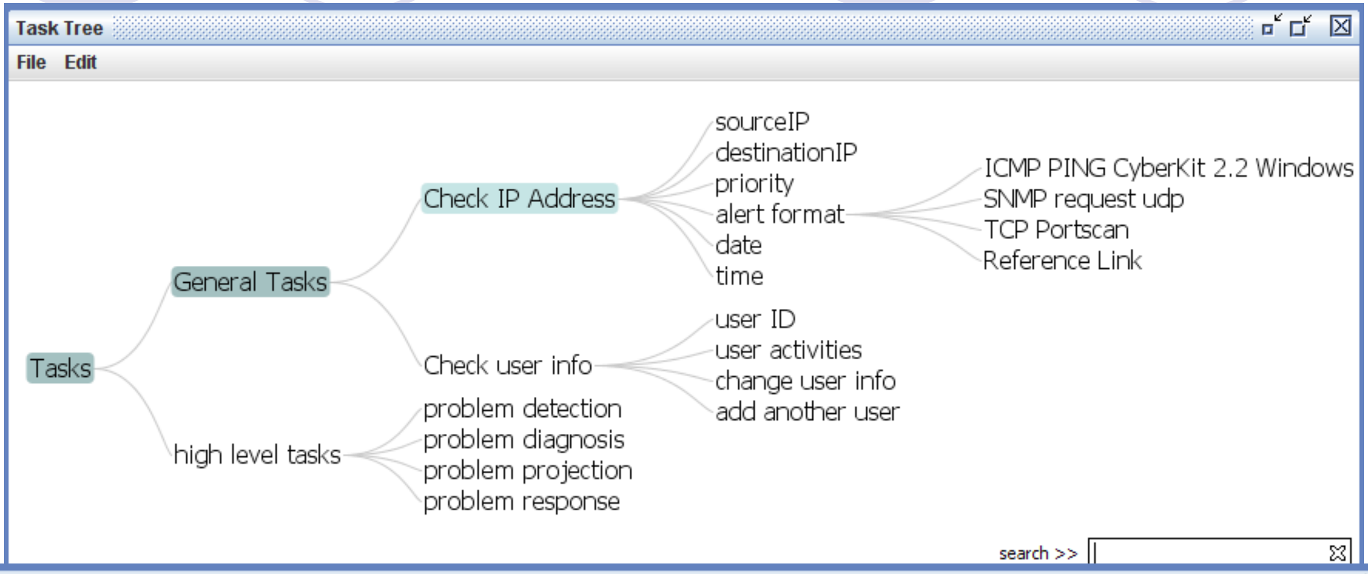
- Complex problem solving is a dynamic process. In search for a solution, users need to test different hypotheses or different strategies
- Studies have shown that the effectiveness of visualizations depends on users’ background and knowledge.
- Self-constructed visualizations may assist problem solving in ways different from prefabricated visualizations

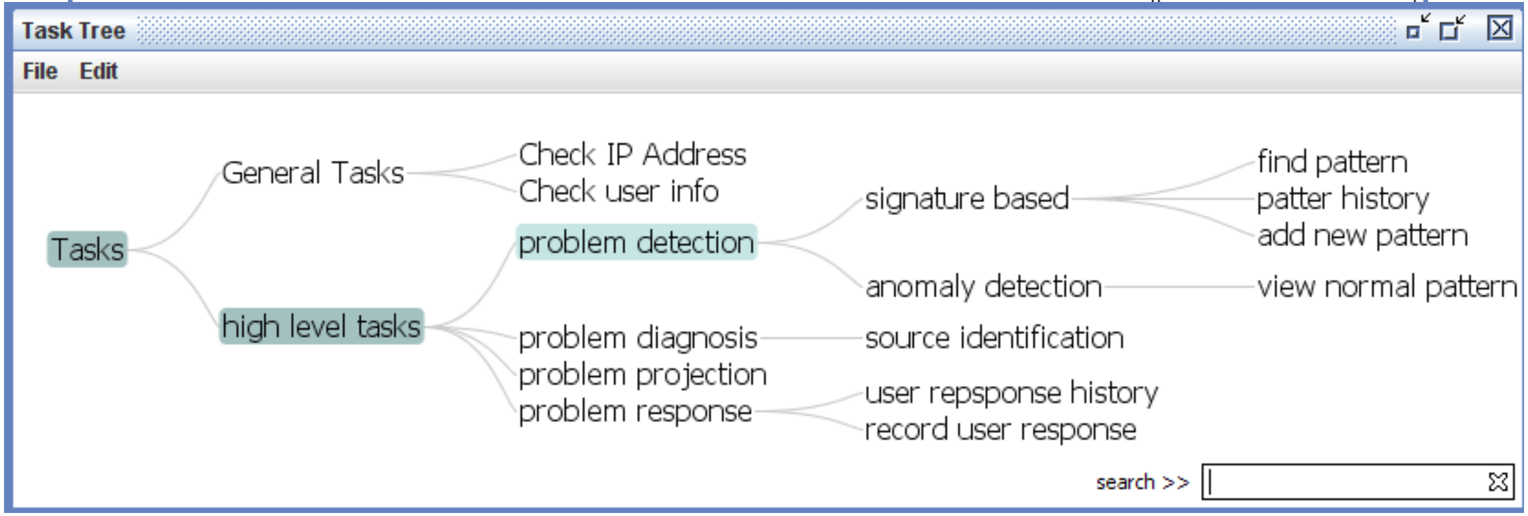
Task Tree

- Task tree can reduce the user’ s cognitive load

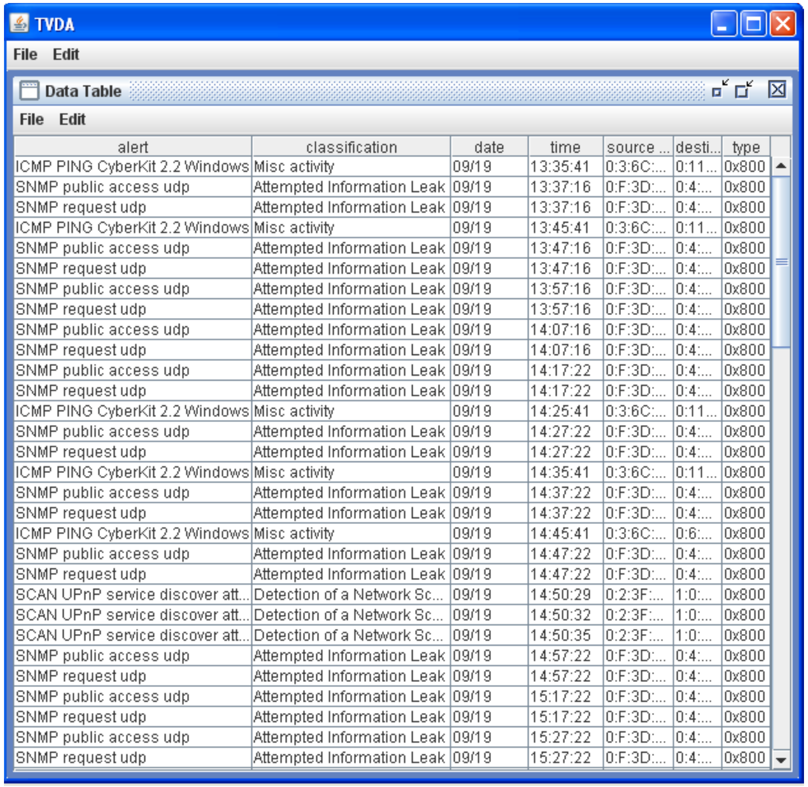
- Task tree is essentially a visual language for describing a specific problem solving strategy and expertise, which can be shared and reused.

Task Tree

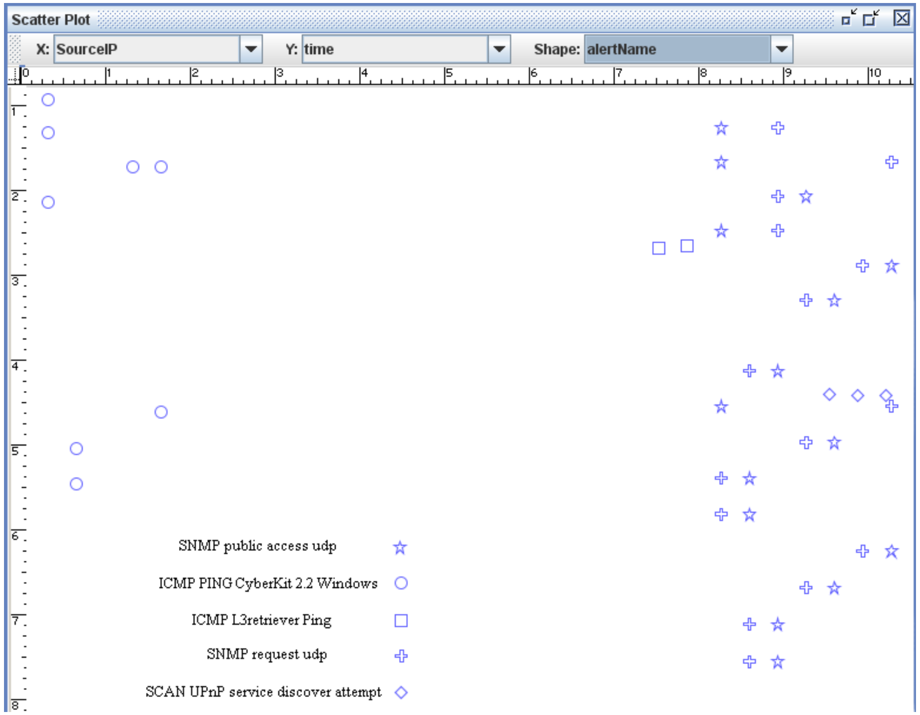

Task Tree
File
Edit
Tasks
General Tasks
Check IP Address
sourceIP
destinationIP
priority
alert format
ICMP PING CyberKit 2.2 Windows
SNMP request udp
TCP Portscan
Reference Link
date
time
Check user info
user ID
user activities
change user info
add another user
high level tasks
problem detection
problem diagnosis
problem projection
problem response
search >>


Task Tree
File
Edit
Tasks
General Tasks
Check IP Address
Check user info
high level tasks
problem detection
signature based
find pattern
patter history
add new pattern
anomaly detection
view normal pattern
problem diagnosis
source identification
problem projection
problem response
user repsponse history
record user response
search >>

Data and Output



alert	classification	date	time	source ...	desti...	type
ICMP PING CyberKit 2.2 Windows	Misc activity	09/19	13:35:41	0:3:6C:...	0:11...	0x800
SNMP public access udp	Attempted Information Leak	09/19	13:37:16	0:F:3D:...	0:4:...	0x800
SNMP request udp	Attempted Information Leak	09/19	13:37:16	0:F:3D:...	0:4:...	0x800
ICMP PING CyberKit 2.2 Windows	Misc activity	09/19	13:45:41	0:3:6C:...	0:11...	0x800
SNMP public access udp	Attempted Information Leak	09/19	13:47:16	0:F:3D:...	0:4:...	0x800
SNMP request udp	Attempted Information Leak	09/19	13:47:16	0:F:3D:...	0:4:...	0x800
SNMP public access udp	Attempted Information Leak	09/19	13:57:16	0:F:3D:...	0:4:...	0x800
SNMP request udp	Attempted Information Leak	09/19	13:57:16	0:F:3D:...	0:4:...	0x800
SNMP public access udp	Attempted Information Leak	09/19	14:07:16	0:F:3D:...	0:4:...	0x800
SNMP request udp	Attempted Information Leak	09/19	14:07:16	0:F:3D:...	0:4:...	0x800
SNMP public access udp	Attempted Information Leak	09/19	14:17:22	0:F:3D:...	0:4:...	0x800
SNMP request udp	Attempted Information Leak	09/19	14:17:22	0:F:3D:...	0:4:...	0x800
ICMP PING CyberKit 2.2 Windows	Misc activity	09/19	14:25:41	0:3:6C:...	0:11...	0x800
SNMP public access udp	Attempted Information Leak	09/19	14:27:22	0:F:3D:...	0:4:...	0x800
SNMP request udp	Attempted Information Leak	09/19	14:27:22	0:F:3D:...	0:4:...	0x800
ICMP PING CyberKit 2.2 Windows	Misc activity	09/19	14:35:41	0:3:6C:...	0:11...	0x800
SNMP public access udp	Attempted Information Leak	09/19	14:37:22	0:F:3D:...	0:4:...	0x800
SNMP request udp	Attempted Information Leak	09/19	14:37:22	0:F:3D:...	0:4:...	0x800
ICMP PING CyberKit 2.2 Windows	Misc activity	09/19	14:45:41	0:3:6C:...	0:6:...	0x800
SNMP public access udp	Attempted Information Leak	09/19	14:47:22	0:F:3D:...	0:4:...	0x800
SNMP request udp	Attempted Information Leak	09/19	14:47:22	0:F:3D:...	0:4:...	0x800
SCAN UPnP service discover att...	Detection of a Network Sc...	09/19	14:50:29	0:2:3F:...	1:0:...	0x800
SCAN UPnP service discover att...	Detection of a Network Sc...	09/19	14:50:32	0:2:3F:...	1:0:...	0x800
SCAN UPnP service discover att...	Detection of a Network Sc...	09/19	14:50:35	0:2:3F:...	1:0:...	0x800
SNMP public access udp	Attempted Information Leak	09/19	14:57:22	0:F:3D:...	0:4:...	0x800
SNMP request udp	Attempted Information Leak	09/19	14:57:22	0:F:3D:...	0:4:...	0x800
SNMP public access udp	Attempted Information Leak	09/19	15:17:22	0:F:3D:...	0:4:...	0x800
SNMP request udp	Attempted Information Leak	09/19	15:17:22	0:F:3D:...	0:4:...	0x800
SNMP public access udp	Attempted Information Leak	09/19	15:27:22	0:F:3D:...	0:4:...	0x800
SNMP request udp	Attempted Information Leak	09/19	15:27:22	0:F:3D:...	0:4:...	0x800



X: SourceIP

Y: time

Shape: alertName

Conclusion

- Tasks are explicitly identified and organized and visualizations are constructed for specific tasks and their related data parameters.
- The center piece of this framework is a task tree which dynamically links the raw data with automatically generated visualization.
- Our future work includes developing a design gallery style visualization interface that allows users to compare and select from multiple visualizations that are automatically generated.
- A significant challenge is to develop a visualization engine that helps automatically generate visualizations given a task and its related parameters.