An attack graph is a graphical representation that can assist in documenting security risks and identifying possible paths attackers may consider to attack a system for their undesirable goal.

However, an attack graph does not provide facilities to perform concrete risk analysis such as what-if and scenarios analysis to test the designed system for possible risk of attacks.

In this research, a fuzzy cognitive map (FCM) is used with graph attacks to provide facilities that will enable the system architects to perform what-if analysis to better understand vulnerabilities of their designed system.

Attack graphs are designed after analyzing a system purpose, its components, and any set of potential attacker undesirable goals.

These goals may include system's disruptions, intrusion, and misuse by an attacker.

Attacker's goals are identified on an attack graph using octagons placed at the bottom of an attack graph. Trust boundaries separate components of a system that are of different trust levels. Sub-goals are represented using AND and OR nodes.

An AND node is represented by a circle, and an OR node is represented by a triangle. Paths through an attack graph are identified to reach attacker's goals.

Fuzzy Cognitive Maps (FCM) [2, 3] are graph structures that provide the facilities to capture and represent complex relationships in a system to improve the understanding of a system.

A FCM uses scenario analysis by considering several alternative solutions to a given situation. FCM allows what-if analysis to better understand vulnerabilities of a designed system.

Case Study:
In the attack graph in Figure 1 designer's goal was to create a system:

- to protect sensitive data at a distributed set of sites with variety of constraints on development time, hardware availability, and limited business process changes [1].

A FCM is created based on the attack graph in Figure 1. Matrix E representing value of connecting edges of FCM Figure 1(b)

```plaintext
E =
```

What-if analysis can proceed by using the matrix E. In this scenario the threshold is set to be 0.5.

Simulation examples:
Scenario 1. What happens if the event C1 (i.e. Social Engineering Passphrase) occurs?
This scenario can be presented using vector $I_1$ representing this situation by

```
I_1 = [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
```

```
I_1,E = [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0] = I_1
```

```
I_2,E = [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0] = I_1
```

which concludes that if C10 happens then it will increase the possibility of C11 (i.e. Read global data) by 0.5 (or 50%). This means that the attacker will be able to read the global data. Other Scenarios:

<table>
<thead>
<tr>
<th>What if the following event occur</th>
<th>Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>C1 $\rightarrow$ C11</td>
</tr>
<tr>
<td>C3</td>
<td>C3 $\rightarrow$ C7 $\rightarrow$ C11 Also</td>
</tr>
<tr>
<td>C4</td>
<td>C4 $\rightarrow$ C8 $\rightarrow$ C12</td>
</tr>
<tr>
<td>C5</td>
<td>C5 $\rightarrow$ C13</td>
</tr>
<tr>
<td>C6</td>
<td>C6 $\rightarrow$ C10 $\rightarrow$ C11</td>
</tr>
<tr>
<td>C7</td>
<td>C7 $\rightarrow$ C12 Also</td>
</tr>
<tr>
<td>C8</td>
<td>C8 $\rightarrow$ C10 $\rightarrow$ C11</td>
</tr>
<tr>
<td>C9</td>
<td>C9 $\rightarrow$ C11</td>
</tr>
<tr>
<td>C10</td>
<td>C10 $\rightarrow$ C11</td>
</tr>
</tbody>
</table>

References