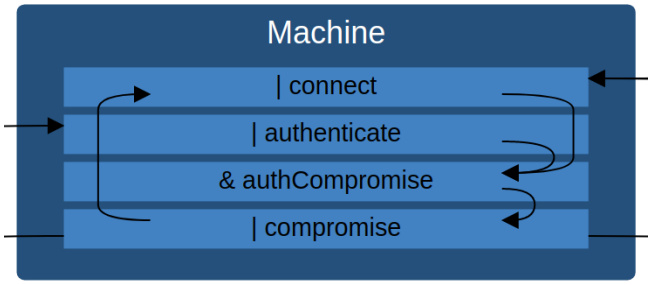
MAL-Visualization

1 Visualization

1.1 Assets, Attack Steps and Relations

Assets are visualized as a box with the asset attack step inside. The example image shows an asset named “Machine” with four attack steps. The arrows represents attack step relations. In the example there are four internal attack step relations:

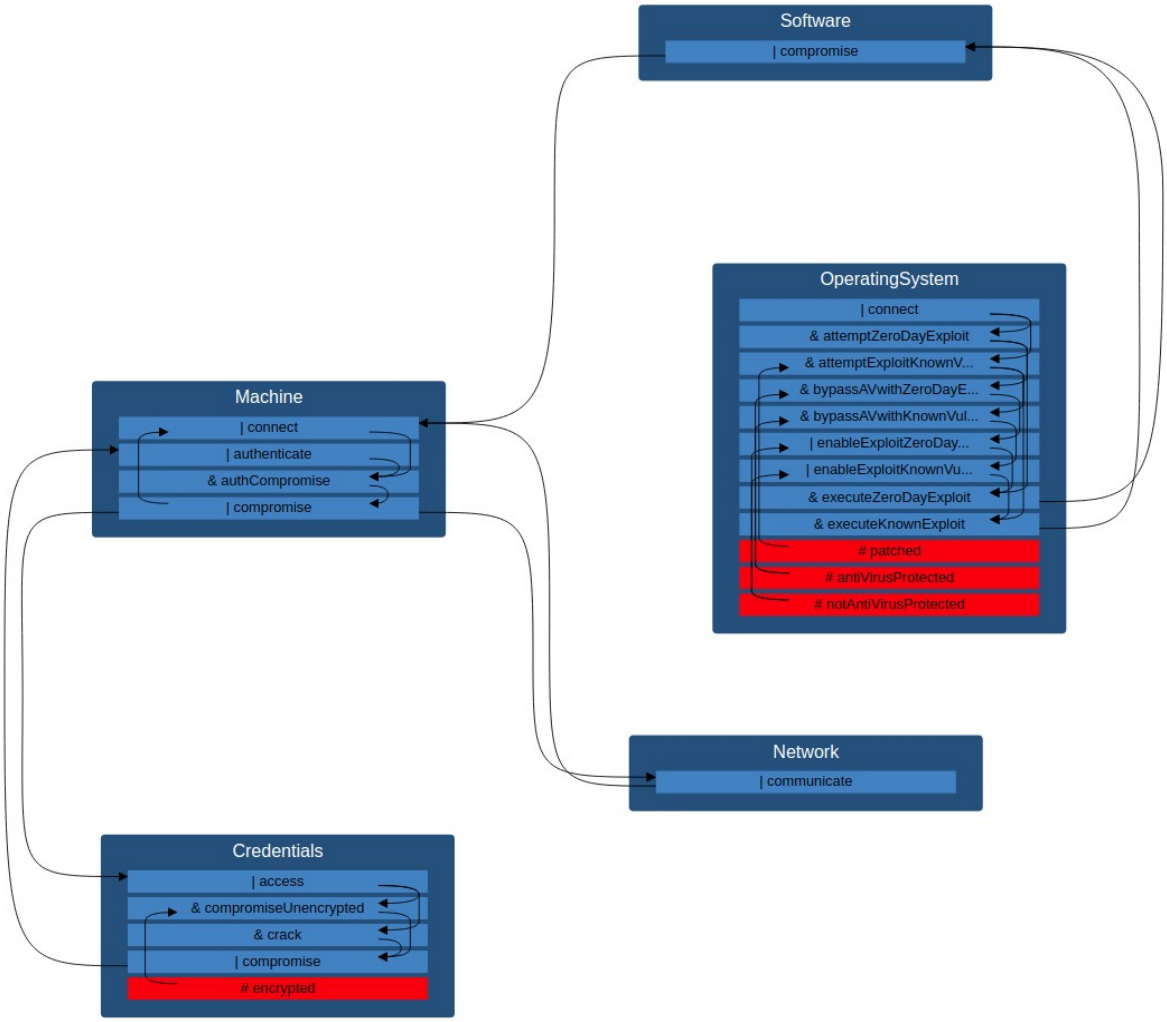
- | connect ==> & authCompromise
- | authenticate ==> & authCompromise
- & authComromise ==> | compromise
- | compromise ==> | connect



Visualization of an asset

Arrows going to an attack step below the source attack step are drawn to the right, otherwise to the left.

The arrows linked to the sides of the attack step boxes at “| connect”, “| authenticate” and “| compromise“ represents attack step relations where the connected attack steps aren’t belonging to the same asset. Below is the visualization with more assets and their external attack step relations visible. External attack step relations are connected through either an association (asset relation) or through inheritance (extends).



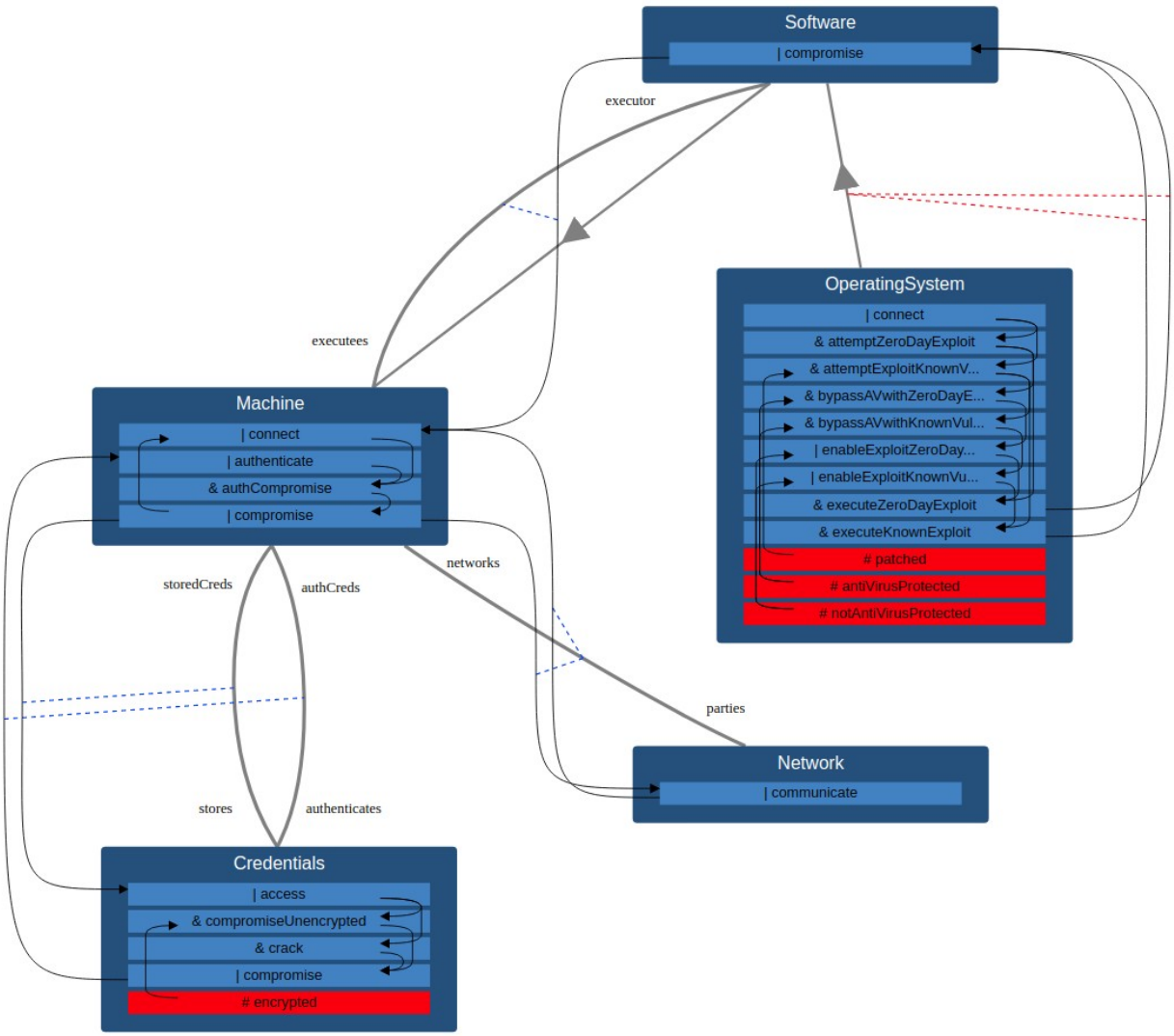
Attack step relations between assets

1.2 Associations and Inheritance

Associations are visualized with a bent line. If an attack step relation are linked with an association it is visualized by a blue dotted line representing the connection. Close to the ends of the line representing the association the are role names are written.

The inheritance relations are visualized with a big arrow, and similarly attack step relations connecting through an extends relation are visualized with a red dotted line.

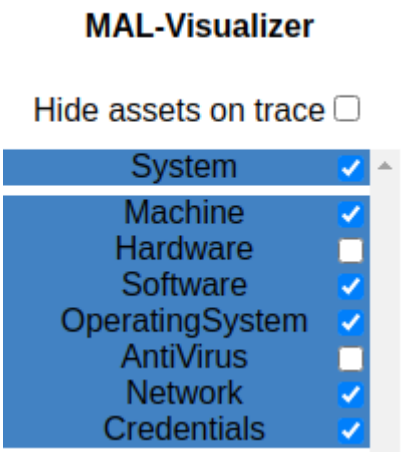
Below is an example with these relations active. The visualization in this case contains two inheritances (Software extends Machine and OperatingSystem extends Software) and four asset relation associations (Software–Machine, Machine–Network and 2x(Machine–Credentials). All external attack step relations are linked to one of these.



Associations and Extends Relations

1.3 Menus

The menu to the left controls the visibility of assets. The first button controls visibility during traces and is described in the trace section of this document. Then there is one button for each category of the language. If a category button is unchecked all assets belonging to that category will be hidden in the visualization. There is then an individual visibility toggle for each asset. For an asset to be visible both the individual and the category button needs to be checked. The image to the right shows the corresponding menu for the visualization on the previous page of this document, there are two assets hidden, the “Hardware” and “AntiVirus” Assets. At the bottom of the left menu there is an export button which will download the current visualization as a .svg file. Make sure that all of the content you want present in the exported file is visible in the browser.



Visibility menu

The bottom menu have check boxes to control the visibility of all associations, attack step relations (attack paths) and inheritance. There is also an option to hide or show control points. The usage of control points are described in the interactivity section of this document.

2 Interactivity

2.1 Asset Positioning

The assets can be moved around to position them in a preferred setting. Once a asset is released on a new position, this position will be fixed and the asset will not float around when other assets are moved. The position can then again be changed by moving the asset to a new position. All positions of connections are relative to the asset and will follow with the asset.

2.2 Control Points, Associations and Attack Step Relations

If the “hide control points” option is unchecked in the bottom menu the control points will be visible. There are two kinds of control points, blue ones for controlling associations and red ones for controlling external attack step relations.

The control points controlling the association drawing will change the bend of the bent curve representing the association. This can be useful when there are multiple associations connecting the same two assets and these needs to be separated. It is also possible to move the role names of an association. The position of the role names is relative to the association link and will follow when assets are moved.

The control points controlling the attack step relations will change the way the arrow is drawn. The arrow is programmed to leave the attack step, go through the control point and connect to the other attack step. Which side of the asset an attack step relation arrow is drawn from and to is dependent on the asset positioning.

The control points can also be used to control the position of the dotted red and blue lines. The dotted blue lines will be connected to the control points of the attack step relation on one end and the control point of the association on the other end. For the red dotted lines, it will be connected close to the center of the inheritance arrow and the control point of the attack step relation.

2.3 Tracing

Tracing is possible by clicking on a attack step and the user is presented with four options:

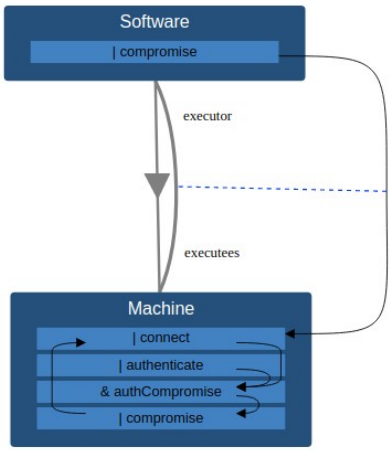
- Trace Children: Highlights the direct child attack steps to the selected attack step and the relevant relations.
- Trace Parents: Highlights the direct parent attack steps to the selected attack step and the relevant relations.
- Trace All Children: Highlights all attack steps and relations that are in some way recursive children to the selected attack step (Child to a child, etc).
- Trace All Parents: Highlights all attack steps and relations that are in some way recursive parents to the selected attack step (Parent to a parent, etc).

If any of these traces already are active for the selected attack step more can be added but the user will also have the option:

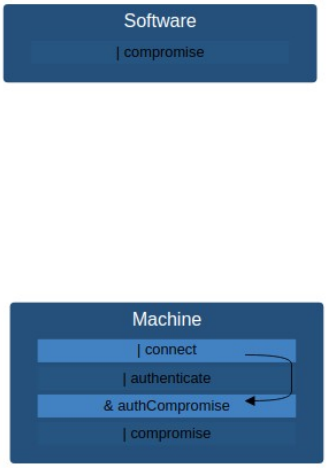
- Remove traces from this attack step: Inactivates all traces from the selected attack step.

To disable all traces the user can double click an empty space of the visualization.

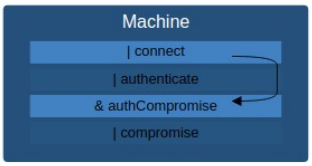
If the “Hide assets on trace” button is checked the assets that have no attack steps active for the trace will be hidden. An example of this, and tracing is shown below. The button must be set before the trace is selected and the visualization wont change if the button is toggled after the trace.



Software and Machine without trace



Trace Children on the connect attack step with "Hide assets on trace" unchecked



Trace Children on the connect attack step with "Hide assets on trace" checked, the Software asset gets hidden