Toward Geographical Visualizations for Hierarchical Security Data

M. Angelini, D. De Santis, G. Santucci
University of Rome La Sapienza
Rome,Italy
[angelini,santucci]@dis.uniroma1.it, dario.desantis@hotmail.com

1. INTRODUCTION

The increasing number of *cyber incidents* that critical infrastructures are experimenting is pushing for developing situation awareness systems that exploits geographical data about the network under control. This poster describes the Visual Analytics solution that is under development in the European project PANOPTESEC [6] for monitoring the ACEA (an Italian organization that provides power to millions of end users) complex hierarchical structure of the geographical network and supervisory control and data acquisition (SCADA) systems network.

The proposed solution allows for monitoring a complex geographical network through ad-hoc visualizations, dealing with the cardinality of the network nodes, the different hierarchical layers that exist at both topological and geographical levels, and the need of combining quick awareness overviews together with local (geographical and topological) views, allowing for understanding the contribution of single nodes to the overall situation. In spite of the locality of the ACEA network, such issues are quite general and the results presented in the poster can be exploited in other geographical layered computer networks.

Summarizing, the key novel features of the proposed solution are: (1)the seamlessly integration of the geographical and topological layers, (2) the clear relationship between the analysis focus(es) and the context, both at geographical and topological levels and (3) the cyber incident risk representation at different scales, with an automatic cluster/voronoi based optimization of the node representation.

2. RELATED WORK

In the current literature different approaches exist to the problem of visualizing cyber security data. [2] provides a vast and comprehensive overview of network visualizations. In the particular subfield of cyber security visualizations that make uses of geographical representation, [1] presents a system for inspecting geographical and time-dependent logs of coordinates. Another work that is based on geographic visualization for large network is [3]: they use a geographic representation of the resources, using the well known GeoViz tooolkit. On the topic of how to present aggregate indicators of level of security, risk and vulnerabilities, [5] presents techniques and visualizations for computing *trust* (availability, detection and false alarm trust values) for a smart grid environment. In [4] is presented a solution for merging geographical and logical topology. Panoptesec system instead preserves the geographical information of the hidden network using Voronoi diagrams.

Poster Presentation
VizSec '14, November 10 2014, Paris, France
.

3. SYSTEM OVERVIEW

The system presented in this poster deals with the problem of representing and relating a geographical hierarchy, based on the location of the ACEA resources, and a logical hierarchy, based on the nodes' semantic. The implemented solution allows for getting the overall status both in an aggregated and timely view, providing a guided exploration of the data towards area of particular interest.

Data is plotted according to the geographical position and the logical hierarchy is constituted by *primary cabins* (50), *secondary cabins* (13000), in proportion of about 260 for each primary one and finally hundred of thousands *smart meters* (undisclosed number) and the level of compromission is rendered through a green-red color scale.

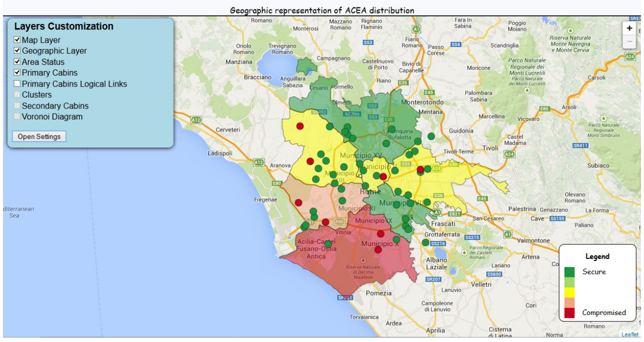
In order to avoid clutter phenomena or to plot the whole *secondary cabins*, the system envisions a progressive refinement of the resources visualized on the following axes: a) Geographical axis: it allows the user to switch among the macro zones of Rome (ranging from North to South-West), the Municipalities, and the Zip codes, and b) Topological axis: representing the logical connection (link) existing among the different nodes of the network.

Exploiting these two coordinates, the system presents in a scalable way all the resources forming the network under protection.

The system deals with cluttering using the following techniques: for the areas with enough space available with respect to the number of contained resources, nodes are grouped into clusters (using a K-means algorithm with k fixed with respect to the number of primary cabins present in the area). Additionally, in order to immediately convey to the user the geographical area interested by the clustered resources, a Voronoi diagram is computed in order to create sub-areas with a constant number of resources per area. In this way, the user will have information also on the extension of the interested areas and on the number of involved resources.

This technique avoids situation in which a subarea or a cluster result too cluttered and allows for a better separation of the secondary cabins with respect to the available spaces. Moreover, also from an interaction point of view, the system will make visible only the resources or areas that correspond to the actual user's interest, reducing the clutter produced by all the others point. Multiple selections are possible: the user can expand or collapse any of the inspected cluster/area, allowing the highlight of the interesting subset of the resources.

4. THE PROTOTYPE



Geographic representation of ACEA distribution

Layers Customization

☑ Map Layer
☑ Geographic Layer
☑ Area Status
☑ Primary Cabins
☐ Primary Cabins Logical Links
☐ Clusters
☐ Secondary Cabins
☐ Voronoi Diagram

Open Settings

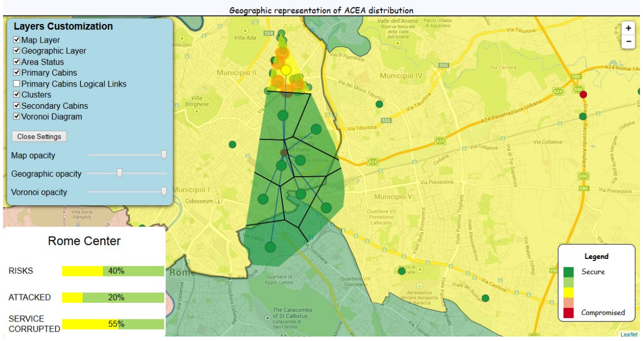
Figure 1: The main screen of the prototype.

The prototype (see Figure 1) foresees a map, composed by several layers and the sidebar, useful to change the visibility of a layer. The layers are the *map* layer, the *geographic* layer (defining the bounds of the areas), the *primary cabins* layer (red or green circle markers showing the status of each primary cabin), the *clusters* layer (to aggregate the secondary cabins linked to a primary one) and the *secondary cabins* layer (showing the status of each secondary cabin). Some interactions with the map add also other layers as the *primary cabins logical links* layer (showing the logical network) and the *Voronoi diagram* layer (useful to split a geographic area in many subareas of interest and to put in evidence some compromised areas).

The prototype uses a 5-color scale to show the level of compromission of nodes/geographic areas. Colors are assigned to each element using the inner hierarchy: starting from the secondary nodes that range from compromised (red) to secure (green), a function (based on the percentage of red nodes) assigns colors to the Voronoi areas, clusters, and geographic areas.

Interacting with the map permits a deep analysis and exploration of the nodes and the network. All interactions are driven by mouse actions (hovering, clicking and scrolling). The mouse scrolling has the simple function of zoom-in/out the map. Hovering and clicking have different effects, based on the layer on which the interaction occurs.

The hierarchical geographic layer ranges from a macrozones view (less specific) through a municipalities view until a zip codes view (more specific) and the views can be changed with the mouse left-click (to a more specific view when it is possible) or with the mouse right-click (to a less specific view). The mouse hover on either a specific area or a node (primary/secondary cabin or cluster) triggers the security status of such an area or node, showing some indicators of risk related to the actual cyber security situation.



Geographic representation of ACEA distribution

Layers Customization

☑ Map Layer
☑ Geographic Layer
☑ Area Status
☑ Primary Cabins
☐ Primary Cabins Logical Links
☑ Clusters
☑ Secondary Cabins
☑ Voronoi Diagram

Close Settings

Map opacity
Geographic opacity
Voronoi opacity

Rome Center

RISKS	40%
ATTACKED	20%
SERVICE CORRUPTED	55%

Figure 2: The expanded view of a primary cabin into clusters and some of their own linked secondary cabins.

The network hierarchy, composed by (in the order) primary cabins, clusters and secondary cabins (Figure 2), permits an accurate analysis of the situation about the status of the network. The mouse right-click produces effects only on a primary cabin, expanding on the map the sub-network of clusters (of secondary cabins) linked to such primary cabin clicked; moreover, when this happen it is drawn on the map the Voronoi diagram associated to the clusters, giving the possibility to analyze a little subarea associated to the primary cabin and not the whole area, then reducing the complexity and increasing the efficiency when a fast reaction is required.

5. ACKNOWLEDGMENTS

Work supported by the Panoptesec European Project (FP7-ICT-2013-10 Objective ICT-2013.1.5 Trustworthy ICT item).

6. REFERENCES

[1] V. Y. Chen, S. Ko, D. S. Ebert, C. Z. Qian, and A. M. Razip. Semanticprism: A multi-aspect view of large high-dimensional data: Vast 2012 mini challenge 1 award: Outstanding integrated analysis and visualization. In *Proc. of the 2012 IEEE Conference on Visual Analytics Science and Technology (VAST)*, VAST '12, pages 259–260, Washington, DC, USA, 2012. IEEE.

[2] M. Dodge. Retrieval, mapping, and the internet, onword press. building an atlas of cyberspace.

[3] N. Giacobe and S. Xu. Geovisual analytics for cyber security: Adopting the geoviz toolkit. In *Visual Analytics Science and Technology (VAST), 2011 IEEE Conference on*, pages 315–316, Oct 2011.

[4] E. Karapistoli, P. Sarigiannidis, and A. A. Economides. Srnet: a real-time, cross-based anomaly detection and visualization system for wireless sensor networks. In *Proc. of the Tenth Workshop on Visualization for Cyber Security*, pages 49–56. ACM, 2013.

[5] W. J. Matuszak, L. DiPippo, and Y. L. Sun. Cybersave: situational awareness visualization for cyber security of smart grid systems. In *Proc. of the Tenth Workshop on Visualization for Cyber Security*, pages 25–32. ACM, 2013.

[6] PANOPTESEC. The official website, 2014.