Noname manuscript No.
(will be inserted by the editor)

Cyber Situational Awareness: from geographical alerts to high-level management

Marco Angelini · Giuseppe Santucci

Received: date / Accepted: date

Abstract This paper focuses on cyber situational awareness and describes a Visual Analytics solution for monitoring and putting in tight relation data from network level with the organization's business. The goal of the proposed solution is to make different security profiles (network security officer, network security manager, and financial security manager) aware of the actual network state (e.g., risk and attack progress) and the impact it actually has on the business tasks, making clear the relationships that exist between the network level and the business level. The proposed solution is instantiated on the ACEA infrastructure, the Italian company that provides power and water purification services to cities in central Italy (millions of end users).

Keywords Cyber situational awareness · Business processes

1 Introduction

Situational awareness plays a central role in the analysis of risks of critical infrastructures and refers to two (at least) complementary aspects: the understanding of the network status and the *consequences* that the actual network situation has on the organization's mission. To improve situational awareness, it is needed to deal with issues arising from the cardinality of the network nodes, their spread on the geographical level, the presence of different hierarchical layers that exist at both topological and geographical levels, the need of combining quick awareness technical and financial overviews together with local (geographical and topological) details. An additional challenge arises from the integration of local layer 3 topological information (e.g., local networks within a building) with geographical spread. Finally, network information should be in correlation with the organization's processes. This paper

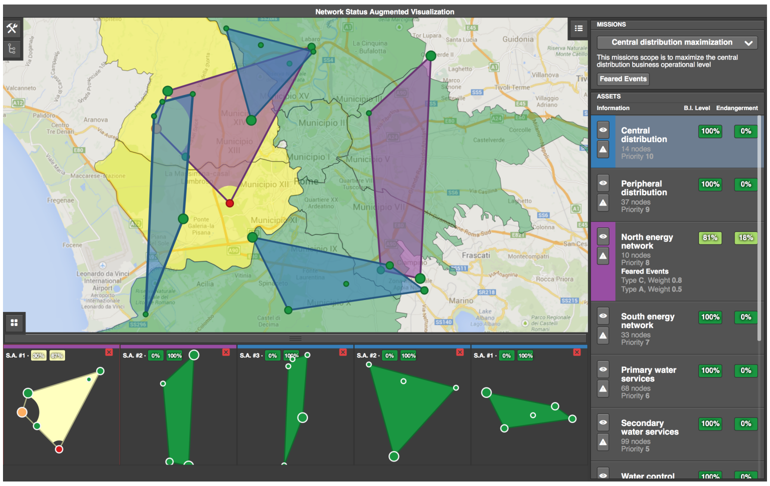
Marco Angelini, Giuseppe Santucci
University of Rome "La Sapienza"
E-mail: angelini,santucci@dis.uniroma1.it

extends the Visual Analytics solution presented in [1] introducing a novel layer 3 topology visualization that allows for dealing with sparse and composite networks on a geographical map and linking it to a pure topological view (Section 4).

The novel features of the proposed solution are: a) the seamlessly integration of the geographical and topological hierarchical layers, b) the representation of the cyber risk at different scales, c) the integration of the network topology and geography with the organization's business processes, d) a novel visualization able to quickly raise the user attention on the relevant fragment(s) of the network, e) local and geographical display of layer 3 topology data, and f) a visual environment for high-level management. The paper is structured as follows. Section 2 discusses related work, Section 3 describes the system overview, Section 4 describes the novel visualization of composite nodes, Section 5 describes the manager interface, while Section 6 presents conclusions and future activities.

2 Related Work

The work in [5] allows for inspecting geographical and time dependent logs, while [9] relies on a geographic representation of the resources, using the GeoViz tooolkit [12]; conversely, we use composite nodes and resources are first aggregated and mapped or directly mapped, according to their cardinality and space constraints. In [11] is proposed the integration of geographical and logical representations. Our solution provides an aggregate representation of these different properties, single and composite layer 3 handling, augmented with mission impact information. [13] presents a system that integrates geographical, temporal, and logical views, while [10] presents a system that coordinates geographical visualizations with other security data: however, the mapping and aggregation are just computed in other views and then mapped statically on the current visualization, without the tight coupling and interactivity that are present in our solution. [14] presents a solution for merging geographical and logical topology, in which the geographical information is not tied to the network topology. Similarly to our work, this proposal allows for inspecting networks by clustering nodes; however, our solution preserves the geographical information of the hidden network using Voronoi diagrams. ViSAw [15] presents a visualization environment for assessing the impact of detrimental events on the organization's business: however, the proposed solutions are more tied at an analytical evaluation (scatter-plot, tabular chart) and less integrated in an organic view like the solution proposed in this paper. Moreover, the links between network nodes and business' processes are not represented. Both [7] and [8] propose various 3-D representations, linking network nodes to organization's processes. In our solution we use 2-D layering and focus+context in order to help the user to navigate the visualization, avoiding typical 3-D manipulation issues. Finally, [6] visualizes the links between organization's processes and physical devices; however, it does it in a block-diagram



MISSIONS

Central distribution maximization

This missions scope is to maximize the central distribution business operational level

Feared Events

ASSETS

Information	B.I. Level	Endangerment
Central distribution 14 nodes Priority 10	100%	0%
Peripheral distribution 37 nodes Priority 9	100%	0%
North energy network 10 nodes Priority 8 Feared Events Type C, Weight 0.8 Type A, Weight 0.5	81%	18%
South energy network 33 nodes Priority 7	100%	0%
Primary water services 68 nodes Priority 6	100%	0%
Secondary water services 99 nodes Priority 5	100%	0%
Water control	100%	0%

Fig. 1 Processes (right), overview (center) and context (bottom). The overview contains three network fragments (in blue) associated with the Central Distribution (100% functional) and two fragments (in violet) associated with the North Energy Distribution (partially compromised), showing a sub-process impacted by compromised devices (red nodes).

fashion, without the integration with other layers (e.g.,the geographical layer) that our solution envision.

3 System Overview

The proposed approach uses two layers, one regarding the representation of the network nodes, allowing the user to quickly identify compromised nodes; the other one, instead, merging compromised nodes with their impact on the organization. Combining these two layers it is possible to identify the most problematic nodes. Details on such layers are available on [1].

The **Network Layer** deals with low level cyber incidents. To avoid information cluttering and to allow the user to inspect particular areas of interest our solution considers both geographical hierarchy and logical hierarchy, based on the semantic of any single resource, allowing for inspecting resources both in an aggregated and punctual fashion. The geographical hierarchy is tightened with the logical hierarchy of the ACEA: *primary cabins* , *secondary cabins*, and *smart meters*. Devices are either mapped on the geography or clustered; colors convey different levels of risk [1].

The **Mission Impact Layer** deals with network and processes, showing the relationship between compromised nodes and business processes. For each process a list of supporting devices is defined, providing a connection between the network and the business processes (see Figure 1). To visually convey the impact of a compromised device on its supported process, the visualization uses the concept of **area corruption**. Each compromised device will produce a hole in the area representing the supported sub-process, hole that is proportional to the value of its operational impact score. The extension of corrupted areas will be an immediate clue for the user about which device is most responsible for the loss of operational level.

4 Integrating local and geographical layer 3 topologies

This section introduces the novel layer 3 topology added to the system, dealing with the issue that in a pure geographic visualization each single point has a specific meaning, and representing more elements in the same point (e.g., local networks within a building) integrating them with the overall geographical view is not a trivial task. To solve the problem it is needed to distinguish at geographical level single nodes and subnetworks, allowing for semantic zooming in local topologies, according to the specific nature of multi-scale networks (see, e.g., [2]) preserving the integration with the geographical layer. The selected encoding has been a glyph [3], in order to capture different aspects of the inner subnetwork. In particular, a composite node is represented either with a glyph portraying connection information, or with a glyph summarizing some relevant subnetwork characteristics, e.g., the node risk level distribution, see Figure 2.

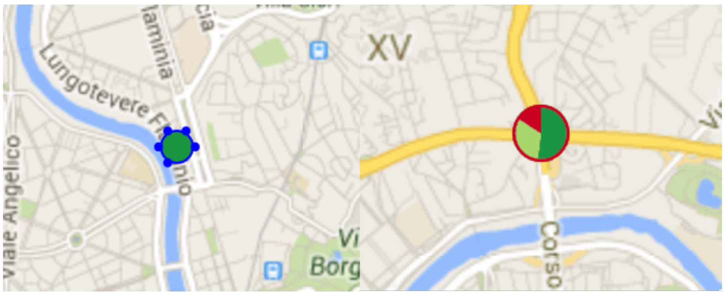


Fig. 2 Two examples of glyphs used for a) distinguishing single node by complex nodes with inner topology and b) conveying aggregate information of local complex topologies. The one on the left allows for making explicit the IP interfaces of the whole sub network, while the one on the left is representing the distribution of risk of the subnetwork nodes.

In order to get details on the inner subnetwork, a semantic zoom interaction has been designed. Clicking on a composite node will expand the node's internal structure using an adjacency matrix, composed of a grid, located in the middle, and of four bars, each one located on a side of the grid, see Figure 3. Each bar represents all the nodes of the subnetwork, and black dots in the matrix indicate that the two corresponding nodes are connected at layer 3. The redundancy of information allows for a better representation of layer 3 links when a composite node is required to be connected to the rest of the network: the geographical area is split to avoid visual occlusion, and logical links are drawn selecting the best connection side, minimizing crossings and

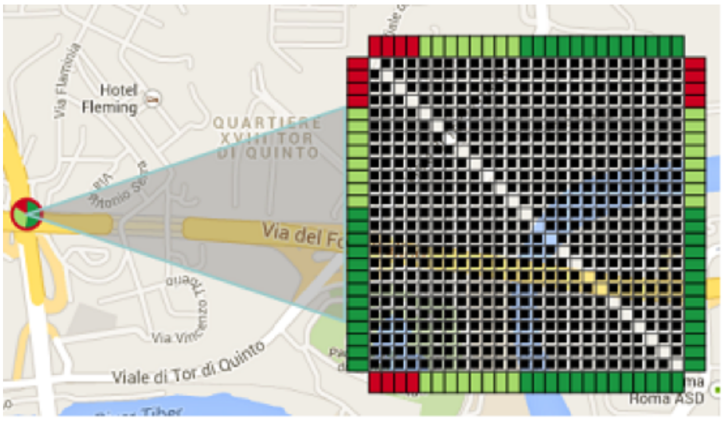
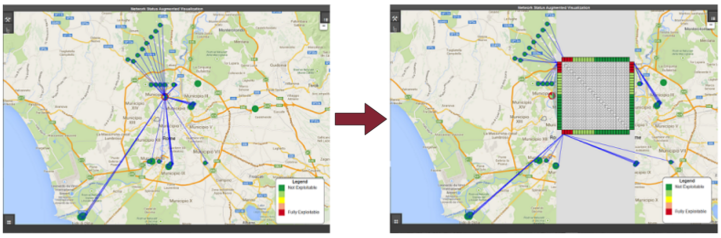


Fig. 3 Semantic zoom on a composite node. The adjacency matrix allows for representing in a compact way the layer 3 topology of the subnetwork: a black dot in position i, j indicates that node i and node j are connected at level 3. Color coding represents node risk levels.



View without expanded nodes

View with expanded nodes

Fig. 4 Semantic zooming in a composite node, showing details of the internal layer 3 topology connections, using a redundant adjacency matrix, and preserving the overall geographical view. Redundancy allows for optimizing the drawing of the connections of the composite node with the rest of the graph. Color coding on matrix row and columns provide the same information of the nodes' risk distribution shown in Figure 2 and facilitate the understanding of the redundant representation.

occlusion, see Figure 5. This technique is a novel one and correspond to the actual state of the art [4].

To further investigate the topology of a composite node, it is possible to activate a coordinated view that shows details on the subnet, like detailed division in subnetworks and node types (e.g., firewall, router, etc.), and the roles they have with respect to attack paths: source node, intermediate node, and target node. Hovering on a composite node for more than 2 seconds triggers the pop-up view shown on Figure 5; further interacting with such new view allows for making explicit the list of nodes reachable by a specific source node, showing all reachable nodes and highlighting the reachable target nodes, activity that is particularly useful when inspecting attack paths, see Figure 5.

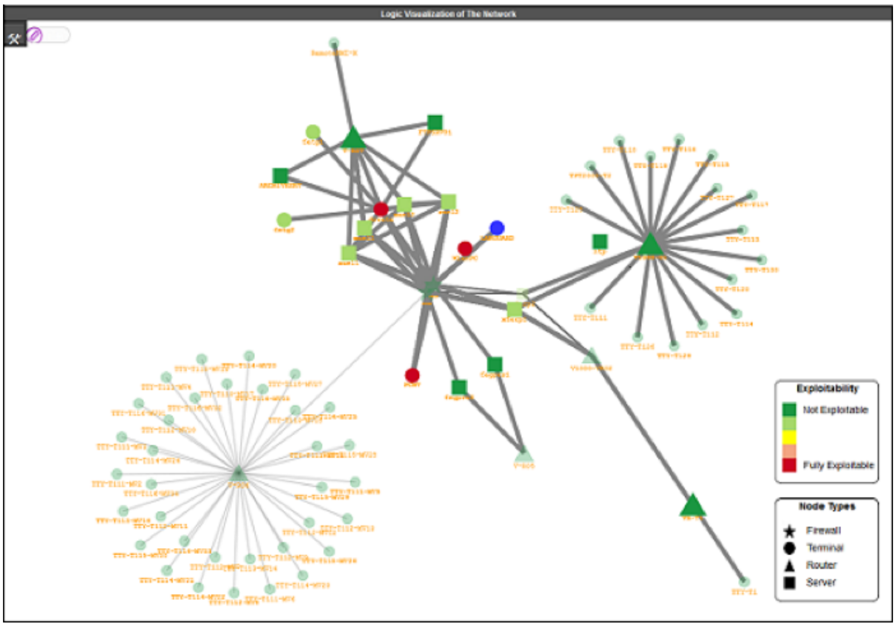


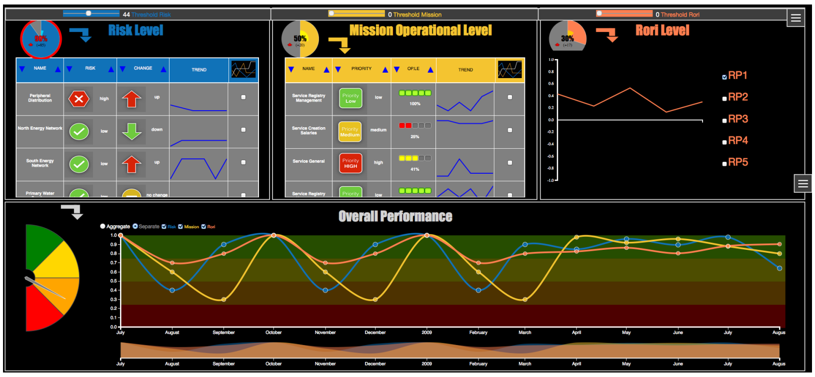
Fig. 5 A parallel view showing the logical subnetwork structure, the different devices, and all the nodes reachable by the blue source node. Red nodes represent the critical target nodes.

5 High Level Management

As stated in the introduction, the manager needs to obtain aggregated information about the overall cyber-security state of his organization in order to quickly and clearly make decisions that depend on both risk levels and costs.

Data are collected from the network and mission impact layers and summarized using 3 main indicators: 1) the Aggregated Risk Level that summarizes the risk level of the network showing the proportion of nodes whose risk is above a threshold, 2) the Aggregated Mission Impact Level that defines the overall impact the compromised nodes have on the operational level of the supported business process, and 3) the Response Financial Level that provides the financial security manager with information regarding the cost that the execution of corrective actions, structured in what is defined as a response plan, can have in relation with the expected raise in business processes operational level. In order to make easy for the financial security manager to interpret the data, the visualization uses basic pie charts and line charts as starting point for further interaction, presenting a clear overview of the system status but still allowing to drill down to details.

The user can expand each risk and impact pie charts into detailed views based on the business processes of the organisation (see Figure 6) allowing the financial security manager to inspect single business process, plotting their temporal behavior using line-charts. In the same way, expanding the Response



NAME	RISK	CHANGE	TREND	
Peripheral Distribution	high	up		□
North Energy Network	low	down		□
South Energy Network	low	up		□
Primary Water	low	no change		□

NAME	PRIORITY	OP.LE	TREND	
Service Registry Management	Priority Low low	100%		□
Service Creation Salaries	Priority Medium medium	25%		□
Service General	Priority HIGH high	41%		□
Service Registry	Priority low			□

Fig. 6 High Level Management environment in its expanded mode. The financial security manager can inspect finer details regarding each of the indicators and trends and an algorithm for geometric pattern recognition allows to select an arbitrary part of the trend, by selecting the initial and final points, and obtain from the system the most similar part of the trend with respect to the selected part. This can help to identify precise trend of service or disservice and see how many times they occurred.

financial level chart allows for inspecting the sequence of response plans previously applied (based on previously happened attack scenarios). The lower part presents a tachometer like view, showing the overall system performances. Expanding it reveals its temporal trend and a separate context chart allows to zoom on particular interesting areas in order to refine the analysis.

6 Conclusions and future work

The paper presented a system targeted to increase cyber situational awareness for different cyber security profiles. The proposed technique deals with the different hierarchical layers that exists at both topological and geographical levels, smoothly integrating composite nodes with simple nodes, allowing for the seamless exploration of the layer 3 connectivity of geographically distributed nodes and subnetworks. Such pieces of information are aggregated for high level decision making. Information about network nodes is associated with resulting business impact using a novel visualization based on areas corruption making clear which part of the network is the source of mission degradation and to which extent. This solution has been instantiated and tested on the ACEA power distribution system.

While the actual implementation is tailored towards the risk analysis, the detection of actually compromised nodes, and layer 3 exploration, we are currently extending the environment to deal with: a) the relationship with attack paths and vulnerabilities, developing additional layers of analysis, b) the impact that mitigation actions produce on the system, both at risk level and at organization's mission level, and c) the definition of a formal model able to translate high level financial strategies into concrete actions on the network configuration.

Acknowledgments This work was supported by the PANOPTESEC European Project (FP7-ICT-2013-10 Objective ICT-2013.1.5 Trustworthy ICT item).

References

1. M. Angelini and G. Santucci. Visual cyber situational awareness for critical infrastructures. In *Proceedings of ACM VINCI '15*, August 24-26, 2015, Tokyo, Japan.
2. D. Auber, Y. Chiricota, F. Jourdan, and G. Melançon. Multiscale visualization of small world networks. In *Proceedings of the Ninth Annual IEEE Conference on Information Visualization*, INFOVIS'03, pages 75–81, Washington, DC, USA, 2003. IEEE Computer Society.
3. R. Borgo, J. Kehrer, D. H. Chung, E. Maguire, R. S. Laramee, H. Hauser, M. Ward, and M. Chen. Glyph-based visualization: Foundations, design guidelines, techniques and applications. *Eurographics State of the Art Reports*, pages 39–63, May 2013. http://diglib.eg.org/EG/DL/conf/EG2013/stars/039-063.pdf.
4. J. Buchmller, D. Jckle, F. Stoffel, and D. A. Keim. SpaceCuts: Making Room for Visualizations on Maps. In E. Bertini, N. Elmqvist, and T. Wischgoll, editors, *EuroVis 2016 - Short Papers*. The Eurographics Association, 2016.
5. 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 *Proceedings of the 2012 IEEE Conference on Visual Analytics Science and Technology (VAST)*, VAST '12, pages 259–260, Washington, DC, USA, 2012. IEEE Computer Society.
6. S. Creese, M. Goldsmith, N. Moffat, J. Happa, and I. Agrafiotis. Cybervis: visualizing the potential impact of cyber attacks on the wider enterprise. In *Technologies for Homeland Security (HST), 2013 IEEE International Conference on*, pages 73–79. IEEE, 2013.
7. A. D'Amico and M. Larkin. Methods of visualizing temporal patterns in and mission impact of computer security breaches. In *DARPA Information Survivability Conference &amp; Exposition II, 2001. DISCEX'01. Proceedings*, volume 1, pages 343–351. IEEE, 2001.
8. A. D'Amico and S. Salas. Visualization as an aid for assessing the mission impact of information security breaches'. In *DARPA Information Survivability Conference and Exposition, 2003. Proceedings*, volume 2, pages 190–195. IEEE, 2003.
9. 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.
10. J. R. Goodall and M. Sowul. Viassist: Visual analytics for cyber defense. In *Technologies for Homeland Security, 2009. HST'09. IEEE Conference on*. IEEE, 2009.
11. M. Grégoire and L. Beaudoin. Visualisation for network situational awareness in computer network defence. *Visualisation and the Common Operational Picture*, 2005.
12. F. Hardisty and A. C. Robinson. The geoviz toolkit: using component-oriented coordination methods for geographic visualization and analysis. *International Journal of Geographical Information Science*, 25(2):191–210, 2011.
13. Y. Hideshima and H. Koike. Starmine: A visualization system for cyber attacks. In *Proceedings of the 2006 Asia-Pacific Symposium on Information Visualisation - Volume 60*, APVis '06, pages 131–138, Darlinghurst, Australia, Australia, 2006. Australian Computer Society, Inc.
14. E. Karapistoli, P. Sarigiannidis, and A. A. Economides. Srnet: a real-time, cross-based anomaly detection and visualization system for wireless sensor networks. In *Proceedings of the Tenth Workshop on Visualization for Cyber Security*, pages 49–56. ACM, 2013.
15. M. Nusinov, S. J. Yang, J. Holsopple, and M. Sudit. Visaw: Visualizing threat and impact assessment for enhanced situation awareness. In *Military Communications Conference, 2009. MILCOM 2009. IEEE*, pages 1–7. IEEE, 2009.