CRUMBS: A cyber security framework browser

Conference Paper · October 2017

DOI: 10.1109/VIZSEC.2017.8062194

3 authors:

Marco Angelini
Sapienza University of Rome
60 PUBLICATIONS **363** CITATIONS
SEE PROFILE

Simone Lenti
Sapienza University of Rome
15 PUBLICATIONS **47** CITATIONS
SEE PROFILE

Giuseppe Santucci
Sapienza University of Rome
166 PUBLICATIONS **2,013** CITATIONS
SEE PROFILE

CRUMBS: a Cyber Security Framework Browser

Marco Angelini* University of Rome "Sapienza"
Simone Lenti† University of Rome "Sapienza"
Giuseppe Santucci‡ University of Rome "Sapienza"

ABSTRACT

In the last years, several standards and frameworks have been developed to help organizations to increase the security of their Information Technology (IT) systems. In order to deal with the continuous evolution of the cyberattacks complexity, such solutions have to cope with an overwhelming set of concepts, and are perceived as complex and hard to implement. This paper presents a visual analytics solution targeted at dealing with the Italian Adaptation of the Cyber Security Framework (IACSF), derived by the National Institute of Standards and Technology (NIST) proposal, adaptation that, in its full complexity, presents the security managers with hundreds of scattered concepts, like functions, categories, subcategories, priorities, maturity levels, current and target profiles, and controls, making its adoption a complex activity. The system has been designed together with the security experts of one of the largest Italian public organization and has the goal of providing a continuous overview of the adoption process, providing a prioritizing view that helps in effectively planning the required activities. A prototype is available at: http://awareserver.dis.uniroma1.it:11768/crumbs/

Keywords: NIST Cyber Security Framework, Visual Analytics

1 INTRODUCTION

The increasing complexity of IT systems and the continuous evolution of the cyberattacks, in terms of cardinality and attack strategies, calls for the availability of complex and structured strategies for defending computer networks by the growing cyber menace. Such strategies must include all the aspects associated with the cyber defense that must be related to the organization business and the identification of priority functions and nodes to defend from attacks. However, the complexity of the possible defense strategies makes their implementation a very complex task. As a consequence, most of the IT companies deal with the issue of identify and prioritize the interventions and the controls that can effectively improve their cyber security level. To mitigate this issue several standards and guidelines have been developed with the goal of helping security managers and top management to make decisions on security activities. Among the available proposals, the paper focuses on the IACSF, i.e., the Italian adaptation of the worldwide agreed and shared reference NIST Cyber Security Framework (CSF) [1] that provides a common ground and a standard terminology for these cyber defense functionalities. The NIST CSF focuses on critical infrastructures and encompasses a comprehensive set of cyber security activities, standards, guidelines, and practices. The framework root consists of five concurrent and continuous *functions*: Identify, Protect, Detect, Respond, and Recover that, considered as a whole, provide an abstract and structured view of the needed management of cyber security risks and have the following goals:

*e-mail:angelini@dis.uniroma1.it
†e-mail:lenti@dis.uniroma1.it
‡e-mail:santucci@dis.uniroma1.it

- Identify: the goal of the Identify function is to have a clear understanding of the resources belonging to the IT network (hardware and software) together with the relationships among such resources and the organization activities, identifying critical assets and the associated risks;
- Protect: the goal of the Protect function is to implement the appropriate safeguards to reduce the attack surface and limit or contain the impact of a potential cyber security event;
- Detect: the goal of the Detect function is to implement the appropriate activities to identify as soon as possible the occurrence of a cyber security event;
- Respond: the goal of the Respond function is to develop and trigger the appropriate mitigation actions to contrast a detected cyber security event;
- Recover: the goal of the Recover function is to activate the appropriate activities to restore the services that were impaired due to a cyber security event.

Each function is organized in categories (for a total of 22) and each category is organized in subcategories (for the total of 98). Subcategories refer to practical actions that must be carried on, e.g., collecting data about organization hardware and software, understanding legal requirements about cyber security, etc. Roughly speaking, we can say that if an organization implements all the activities associated with all the subcategories its cyber security level will be very high. However, this theoretical goal is, in practice, very hard to reach, for the following considerations.

First of all, it must be considered that the framework has been designed for *critical* infrastructures, i.e., infrastructures that are dealing with services that, if impaired by a cyber attack, can damage human beings, e.g., power plants, public transportation, nuclear factories, etc. This design choice implies that some framework subcategories that are mandatory for a critical infrastructure might be much less important for companies that, even if want to elevate their cyber security level, do not want to spend money and time to implement all the NIST guidelines. This is well captured by the notion of security levels that is present in different standards (see, e.g., the Evaluation assurance levels (EALs) levels from Common Criteria [6] or the NIST Framework Implementation Tiers and Framework Profiles [1]) and makes evident that each organization targets a specific security level, according to its mission, constraints, and legal requirements.

A second concern is about the *implementation* of the subcategories: each activity specified by a subcategory can be addressed with an increasing level of maturity that depends on the actual organization. As an example, under the Identify function, category *Asset Management* the subcategory *ID.AM-1: Physical devices and systems within the organization are inventoried* [1] can be implemented according to 3 maturity levels (that might correspond to a possible evolution of the organization security policy):

1. Inventory of products exists, new devices can be added to the network, and guidelines for the removal of assets from the network exists;
2. A map of the current network exists and is stored in a secure manner, the map is updated as the network changes, connections to external networks and the internet are included on the

map, and an ID exists for each network asset, together with its role, physical location and the name of the responsible;

3. Automatic inventory discovery tools are used to discover network devices and Dynamic Host Configuration Protocol (DHCP) servers logs are collected and analyzed to improve the whole process.

As a last consideration, in order to deal with the implementation of the desired cyber security level *target profile* (the "to be" state), starting from the current organization state with respect to subcategories implementations, i.e., the organization *current profile* (the "as is" state), it is mandatory to have some *prioritizing* mechanisms (e.g., cost, resources management, legal constraints, internal company policy, etc.) to efficiently drive the overall process.

According to the aforementioned considerations, the Italian adaptation of the NIST framework explicitly considers the *priority* of the subcategories that are relevant for the organization and the different *maturity levels* that are adequate for the selected subcategories, and, for each maturity level of a subcategory, the *controls* useful to assess it.

We are currently involved in contextualizing the IACSF to a large Italian public organization (we are investigating the possibility to use its name in the paper) and, together with the experts of such a company, we are developing CybeR secUrity fraMework BrowSer (CRUMBS) a visual analytics solution for managing the overall process, allowing for inspecting both the overview and the details of the process state, i.e.:

1. the structure of the contextualized framework: functions, categories, selected subcategories, priorities, maturity levels, and the associated assessment controls;

2. the current profile and the target profile;

3. a comparison between the current and target profiles, making clear what is missing and how far the organization is from the target;

4. a greedy subcategories order list, built on different organization strategies, e.g., priority, relative cost, reputation, etc.

Summarizing, the main contribution of the paper is the user centered design and development of a novel visual analytics solution, called CRUMBS, providing the users with a homogeneous and comprehensive visual representation of all the technical aspects involved in the process of adopting the NIST CSF. However, it is the authors' opinion, that this approach can be used in quite different contexts in which it is needed to move across several assessment levels characterized by large number of controls, like the CMMI constellation [14], the ISO standard 25010 [11], or the ISO standard 27001 [10].

The paper is organized as follows: Section 2 describes the context in which the paper proposal takes place; Section 3 discusses few related proposals; Section 4 presents the implemented system; Section 5 discusses the CRUMBS informal evaluation with domain experts; finally, Section 6 draws some conclusions and presents an outlook for future work.

2 Application Domain

The visual analytics application described in the paper raises in the context of a collaboration between a large Italian public organization and the Research Center of Cyber Intelligence and Information Security (CIS) [15], that on 2015 adapted the NIST framework to the industrial Italian context [12]. Following the guidelines of the NIST proposal about *Framework Implementation Tiers* and *Framework Profiles* [1], the CIS proposed an adaptation of the Framework to the Italian reality, reviewing all of the categories and subcategories and determining which are most relevant. To this aim, the CIS introduced the notion of *Priority Levels* to support organizations and companies in the preliminary identification of subcategories to be implemented in order to further reduce their risk levels, while balancing the effort to implement them. The idea of priority raises from considering three main key risk factors:

- Exposure to threats, intended as the set of factors that increase or diminish the threat probability;

- Occurrence Probability, that is the frequency of the possible event of a threat over the time;

- Impact on Business Operations and Company Assets, intended as the amount of damage resulting from the threat occurrence.

According to that, the Italian Framework suggested the use of a priority scale of four levels among subcategories:

1. Mandatory: actions that are *mandatory* by Italian law. Even if this is not a technical security issue, the need to be compliant with current law regulation strongly motivates this priority level;

2. High Priority: actions that enable a *significant* reduction of one of the three key factors of cyber risk. Such actions are prioritized and must be implemented irrespective of their implementation complexity;

3. Medium Priority: actions that enable the reduction of one of the three key factors of cyber risk, that are generally easily implementable;

4. Low Priority: actions that make possible to reduce one of the three key factors of the cyber risk and that are generally considered as hard to be implemented (e.g., significant organizational and/or infrastructural changes).

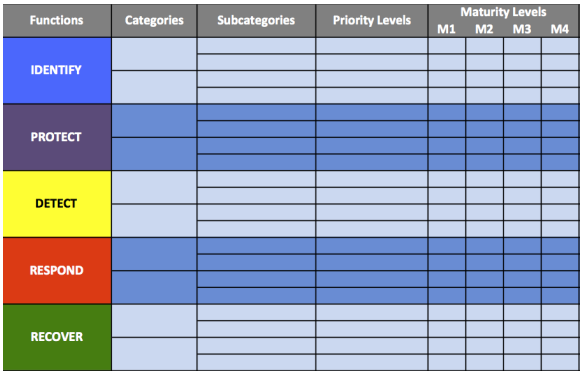

Figure 1: The CIS Italian adaptation of the NIST Cyber Security Framework (CSF). It adds two coordinates to the subcategories of the NIST proposal: Priority levels and Maturity Levels. Priority levels ranges on four values, Mandatory, High, Medium, and Low, providing the organizations adopting the framework with an implementation order; maturity levels accommodate the notion of NIST tiers and allow for defining and assessing, through controls, the maturity of the implemented subcategories. A framework target profile is a list of controls that must be fully satisfied.

The notion of Tiers, ranging from Partial (Tier 1) to Adaptive (Tier 4), that correspond to an increasing degree of rigor and sophistication in cyber security risk management practices, has been accommodated by CIS through the concrete definition of *Maturity*

levels, i.e., the maturity of a security process, technology implementation, or the amount of resources needed to implement a specific subcategory. Maturity levels provide a reference according to which each organization may evaluate its own subcategories implementation and establish targets and priorities for their improvement. The maturity levels must be incremental, from the lowest to the highest. A typical scenario ranges from Maturity level M1 that corresponds to actions that are mandatory by law to maturity level M4 that corresponds to the most sophisticated and rigorous risk management practices that make sense in the context of the organization that is adopting the framework.

In order to facilitate the critical operation of assessing and reporting the progress in the implementation of the framework (this is currently mandatory by law for public Italian organizations), the CIS associated to subcategories maturity levels the notion of *controls*, i.e., pragmatic checks that allow for assessing that a subcategory planned at maturity level MX has been implemented accordingly. To cope with partial implementation of subcategories, controls results range on ordinal scale with at least three values, e.g., not addressed, partially addressed, fully addressed.

The structure of the CIS adaptation is presented in Figure 1. It is worth noting that this proposal is totally backward compatible with the original NIST definition: it adds on it, specializing some concepts, without deleting any NIST element. The CIS adaptation of the NIST framework is currently used as an Italian reference and, based on it, several *contextualizations* have been produced. A contextualization represents a practical baseline of the framework for a homogeneous set of organizations, and contains a clear indication of which subcategories are relevant, their priority and, for the mandatory and high priority levels, the suggested maturity levels. A contextualization can be further modified by specific organization needs. The first produced CIS contextualization was addressing the Italian Small and Medium Enterprises (SME) that represent the majority of private organizations in Italy and, at time being, CIS is progressing in defining the contextualization for the Italian *public* organizations, dealing with the challenging issue of addressing the consequences of the directives coming from both the Italian and European law.

3 Related Work

To the best of authors' knowledge, the solution proposed in this paper has not been explored by any previous work. Among related contributions, in [13] is proposed to increase the use of visual quality tools to support information security standards compliance, using simple matrix representations; the work in [8] provides an analysis framework for the NISITR 7628 Guidelines for Smart Grid Cyber Security, using visualization to represent models of Logical Interface Categories organized in Data layers; however, the visualization follows the well-known flow diagram, while our solution proposes a more abstract visual paradigm, fusing a compact representation with the recognizable layout of IACSF. In [3] Anwar and Campbell propose an approach for automated assessment of compliance to security best practices in the energy sector that use a network visualization for exploring the status of the different appliances. The work in [7] presents an infrastructure and visualization for Security Key Performance Indicators (KPI) analysis; however in both these papers the visualizations proposed are really basic and do not provide a comprehensive analysis and exploration like the proposed solution. Similar to our approach in abstracting cyber security to higher decision levels, from the pure cyber operator perspective, is the work of Horn *et al.* [9] regarding the visualization of a cyber security decision process, correlated with information of the organization hierarchy. The work in [2] provides a cyber security policy visual sub-environment specific for the high-level management of an organization: the work however, focused more on the real-time monitoring of the policies and cyber security status, while our work instead put as the central task the cyber security assessment of the organization and the design, planning and implementation of structured corrective actions. Finally, some existing contributions not directly related to cyber security domain but proposing solutions for compliance visualization can be found in [4] for visualization of compliance violation in business process model and in [16] for privacy preservation, both using as visual paradigm the flow diagram.

4 Prototype

This section presents the visual analytics environment prototype CRUMBS designed to help the security managers to design, manage, implement and review the activities presented in Section 2. CRUMBS follows an incrementally detailed environment approach, in which the visual environment is enriched with information according to the selected task. In particular, the CRUMBS prototype:

- proposes an overview of the selected cyber security framework and contextualization, highlighting the elements of the framework included in the contextualization and showing their proposed maturity levels;
- allows to analyze a current profile of the organization with respect to the chosen contextualization;
- allows to compare the current profile of the organization (i.e., the current maturity levels for each of the subcategories composing the contextualization) with respect to a target profile (i.e., the set of target maturity levels for each of the subcategories composing a contextualization);
- allows to review general statistics regarding the cyber security state of the organization;
- suggests implementation strategies for reaching the selected target profile, providing partial orders of the controls that must be implemented to reach it.

4.1 Framework and contextualization analysis

As first visualization, the security manager is presented with the representation of the cyber security framework, exploding its hierarchical components into functions, categories and subcategories (see Figure 2).

Figure 2: Cyber security framework overview. This view contains the minimum available information, i.e., the NIST Cyber Security Framework (CSF) hierarchical structure, i.e., from left to right, functions, categories, and subcategories. The leftmost bar is a means for zooming and navigating the framework structure. The purpose of this view is just to browse the framework, zooming on relevant parts and inspecting with mouse over details about them. Colors have been chosen according to those used for the original NIST proposal.

Figure 3: Contextualization overview; the chosen contextualization covers all the functions and the categories, with 10 not selected subcategories (represented in grey). Moreover, it adds on the PR column the priority level for each selected subcategory, represented as a colored square with the following color coding: red=mandatory, orange=high priority, yellow=medium priority, green=low priority (white means no priority: the associated subcategory is not included in the contextualization). Columns M1..M4 contain the related controls, spanned over the various maturity levels, where M1 represents controls for *mandatory* subcategories.

CRUMBS allows users to inspect the hierarchy by selecting a desired zoom level (on the left) while maintaining context. The height of elements in functions and categories columns are proportional to the number of their composing sub-elements in the lower level of the hierarchy (for functions the composing categories, for categories the composing subcategories). In this view, the security manager can

Figure 4: Current profile overview. In this view, controls are color coded according to the current addressing of the functionalities they are assessing. A control can be not addressed (red color), partially addressed (half green - half red) or fully addressed (green color). This information is aggregated and reported at each hierarchical level of the framework, visually showing with different alpha blending the covered percentage (high alpha) and the uncovered one (low alpha) for each subcategory, category, and function.

Figure 5: Current profile detail. The security manager zoomed on the respond function, inspecting single subcategories and related controls. Moving from the respond function to the category Mitigation-RS.MI (fourth row) it is possible to see that both its two subcategories, i.e., RS.MI-1: Incidents are contained (first row) and RS.MI-2: Incidents are mitigated (second row) are fully covered and the control of RS.MI-2 is a mandatory control (M1). Mouse-overing on controls and subcategories provides full details about inspected items.

Figure 6: CRUMBS system configured for Gap analysis. The Gap analysis visualization is drawn at the center of the screen and is coordinated with the grid of controls (right) and the framework view (left). For each subcategory two bars are depicted. The left one, with high alpha, represents the status of *all* the controls associated to the target profile, where green and red represents the percentage of addressed (green) and not addressed (red) controls. The right one, with a low alpha, provides the same information for all controls that are *above* the target maturity level for the subcategory. Mouse-overing on the elements in the gap bars reveals the associated controls along the different maturity levels. The bottom long horizontal bar presents an optimized order of the controls that still need to be addressed to reach the target profile. Each control is represented as a little horizontal bar segment (the leftmost position corresponds to the highest implementation order) whose length encodes a cost function: the more the cost of addressing a control, the greater the length. The bottommost thinner horizontal bar provides (colors) the information about the function the controls belong to. All the controls are partially ordered with respect to a suitable implementation strategy.

review the composition of the cyber security framework and obtain a fast browsing of its elements.

Selecting a previously created contextualization triggers its superimposition on the framework view. The contextualization adds the priority level to each selected subcategory (represented as a square with the following color coding: red=mandatory, orange=high priority, yellow=medium priority, green=low priority) and the set of related controls, organized as a grid, spanned over the various maturity levels (from M1 to M4, where M1 represents controls for *mandatory* subcategories) (see figure 3). This view supports the security manager in reviewing the goodness and degree of coverage of the current contextualization with respect to the whole framework (not selected subcategories, categories or even whole functions are represented in grey). The security manager at any time can choose to switch the focus directly on the current contextualization, removing the elements not selected in it.

4.2 Profile analysis

After the decision on which contextualization to use, the security manager can choose to visualize the current status of cyber security of her organization by selecting a current profile from the relative drop-down menu on top of the environment. This action triggers a change in the grid of controls, that are color coded according to their current addressing levels. A control can be not addressed (red color), partially addressed (half green - half red) or fully addressed (green color). This information is aggregated at each hierarchical level of the framework, visually showing the degree of coverage for each subcategory, category and function (see figure 4).

Given the sheer number of controls present in the contextualization (more than 350 for a complete contextualization) from this view it is possible to zoom in order to obtain detailed information. By using the zoom functionality, the security manager can review single controls and checks the degree of coverage by various criteria (i.e., maturity level coverage, subcategories coverage, priority level coverage). As example, in figure 5 it is visible that the second sub category (RS.MI-2: Incidents are mitigated) of the fourth category (Mitigation, RS.MI) of the respond function, is completely covered, meaning that all its controls are fully addressed.

With this view the security manager can raise her situation awareness on the cyber security status of her organization at different levels of aggregation.

4.3 Gap analysis

After a thorough review of the current cyber security status of her organization, the next logical move should be to define an improved cyber security status to reach, where the current deficiencies are addressed. This task is supported by CRUMBS with the Gap analysis. By selecting from the top drop-down menu a target profile, a new visualization is created and located between the framework (left) and the grid of controls (right). In this visualization all the controls

(not addressed, partially addressed, fully addressed) belonging to a subcategory are grouped together in a gap bar, creating a two levels bar where from left to right are represented, as colored consecutive segments, the proportion of addressed controls (full green) and the proportion of not addressed controls (full red) up to the target maturity level (included), and the proportion of addressed controls (light green) and the proportion of not addressed controls (light red) having a maturity level higher than the target one. This operation is repeated for all the subcategories, centering all the gap bars with respect to the target line, resulting in the gap analysis visualization shown in figure 6.

The Gap analysis visualization is coordinated with the rest of the environment. By mouse-over on segments of one gap bar in the Gap analysis visualization the relative controls will be highlighted in the grid of controls (see figure 7).

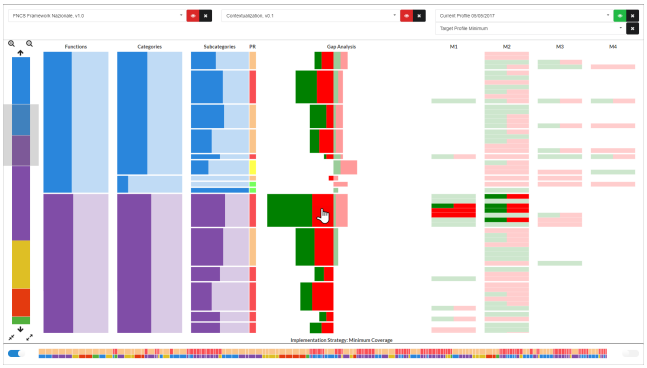

Figure 7: In figure, the zoom and coordination functionalities are shown; the security manager inspects a gap bar for a subcategory of the Protect function; the gap bar shows a not so big distance between the current and target statuses. By mouse-over on it the composing controls are highlighted, showing 5 partially addressed controls and 2 not addressed controls. None of the controls is fully addressed.

Figure 8: Comparing the same current profile shown on figure 6 with a different target profile, the “Target Profile Mandatory” representing a set of subcategory implementation levels mandatory to implement by law.

Using this visualization, the security manager can quickly identify the gaps that remain to be covered in order to reach the desired target in a compact and easy to understand representation, useful for communications activities. Additionally, she can experiment with different possible targets in order to balance eventual constraints (i.e., costs, implementation time). In figure 8 is visible the case in which it is chosen a different target profile composed of only mandatory controls (enforced by law).

4.4 General statistics view

Anytime during the use of CRUMBS, the security manager can choose to look at general statistics regarding the specific contextualization, current profile, and degree of addressing of controls. These statistics are reported in the General statistics view, positioned in the right part of the environment. When the security manager chooses a contextualization, the numbers of included functions, categories, subcategories and controls are shown. When a current profile is chosen, two frequency distribution charts are added to the view: the first one (top) shows the number of subcategories that compose the contextualization, grouped in 5 bins (fully covered, mostly covered, half covered, low covered and uncovered) with respect to the number of addressed controls; the second one (bottom) shows the total number of controls, binned in fully addressed, partially addressed, and not addressed. In both charts, colors refer to the functions the controls belong to. Figure 9 shows how the General statistics are presented to the security manager after she selects a current profile.

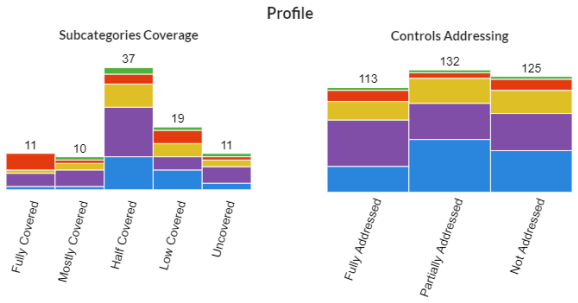

Figure 9: Detail of the General statistics view. On the left is visible the frequency distribution of subcategories with respect to degree of coverage; on the right is visible the frequency distribution of controls with respect to degree of addressing.

Figure 10: The General statistics view configured on target profile; highlighting the half addressed controls bin and then selecting the Identify function rectangle from it shows the resulting controls selection in the grid of controls.

Finally, when the security manager chooses also a target profile, a command to compute the frequency distribution charts with respect to the chosen target profile or to the whole contextualization is added to the view (as shown in Figure 9).

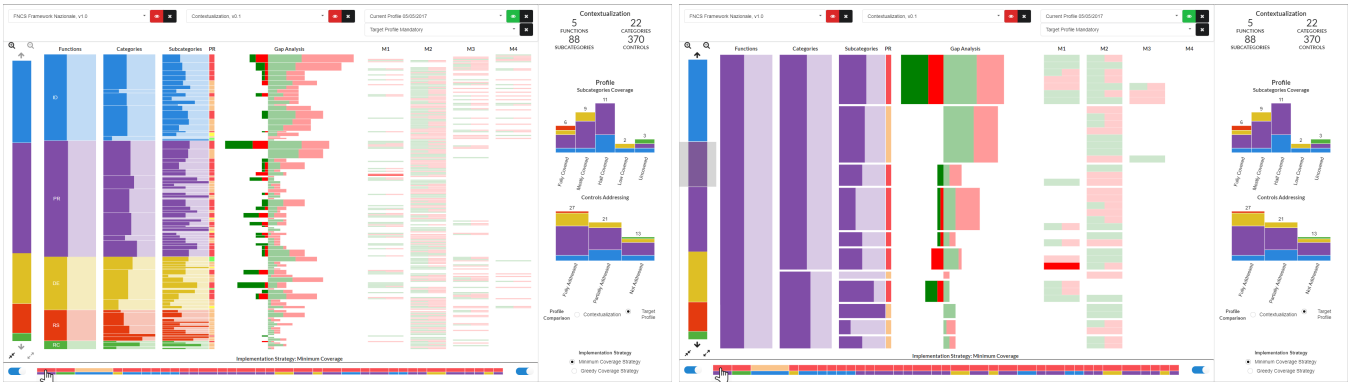

Figure 11: In figure, an example of minimum coverage strategy (left) is shown; it is visible that in the first 10 positions more costly controls are present (longer segments), with even one having medium priority. Moreover, the lower rectangles show that the majority of the controls belong to the Identify function first and to the Protect function second. A zoom of the selected control (the first one) is shown on the right.

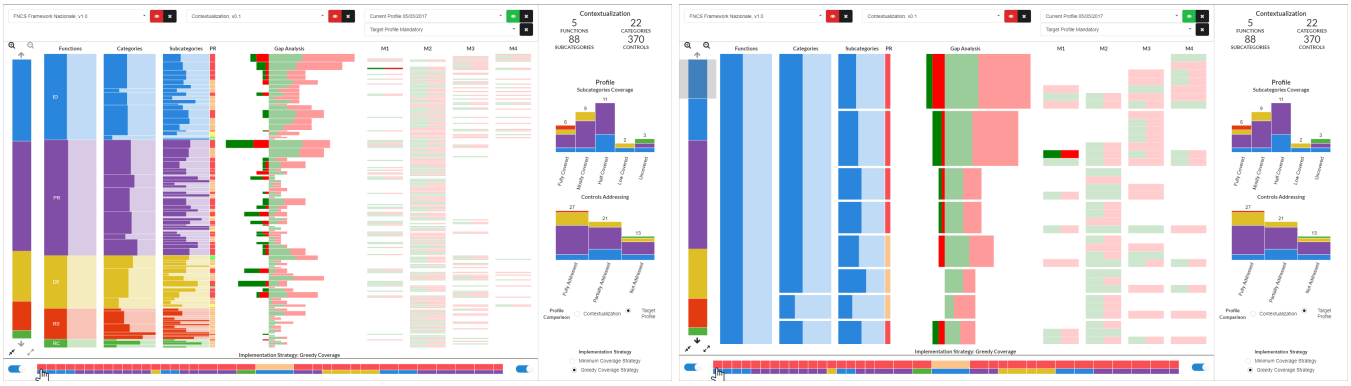

Figure 12: In figure an example of greedy coverage strategy (left) is shown; it is visible that, differently from the minimum coverage strategy, in the first 10 positions less costly controls are present (shorter segments), all having a high priority. Moreover, the lower rectangles show that the majority of the controls belong to the Protect function first and to the Identify function second. A zoom of the selected control (the first one) is shown on the right.

Figure 10 shows the General statistics view configured with respect to the chosen target profile.

4.5 Implementation strategy

From the Gap analysis possible strategies for addressing the existing gaps with respect to the target profile are derivable. CRUMBS implements a final view, called implementation strategy view, positioned at the bottom of the screen, to support this task.

This view collects all the controls that still need to be addressed in order to reach the target profile. Each control is represented as a horizontal segment, where the height is fixed and the length encodes a cost function: the more the control costs, the longer is the segment. The segment contains two different color-coded rectangles: the upper rectangle color represents the priority level of the control (inherited from its subcategory), while the lower rectangle's color represents the control function. In this way, it is possible to comprehend how many subcategories, categories or functions are involved in the strategy and to which degree by visual inspection. All the segments are partially ordered with respect to a precise strategy.

CRUMBS provides different implementation strategies, where the most relevant are the minimum coverage strategy and the greedy coverage strategy. Figure 11 shows an example of the minimum coverage strategy: this strategy expresses the desiderata to have all the subcategories covered by at least minimum level; controls belonging to subcategories with lower levels of coverage (corresponding to big gaps in the Gap analysis visualization) will be addressed first, and then the others, in increasing order of coverage, up to reach the target profile.

Conversely, the greedy coverage strategy works on the principle of prioritizing first the controls belonging to subcategories covered at a level near the desired target in the Gap analysis visualization. It responds to a greedy criterion of coping first with elements near to completion and then move to the others in decreasing order of completion. Figure 12 shows an example of greedy coverage strategy. The security manager can choose an implementation strategy from the panel on the bottom-right of the environment.

Regardless of the chosen strategy, from this view the security manager can, by a mouse-over on a segment, highlight the relative control in the grid of controls (see figure 11 or figure 12 on the right).

By experimenting with the cost function and the implementation strategies the security manager can formulate a reasonable plan for reaching the desired target profile and raising the cyber security level of her organization.

5 Evaluation

CRUMBS has been evaluated through informal experts' feedback collected during its development, as reported in the following.

The visual analytics solution described in the paper has been

developed through a user centered design with the IT experts of one of the largest Italian public organization, with more than 1500 employees, supporting research activities and coordinating more than 10 research centers spread across Italy. Collaboration about the framework adoption started on 2016, triggered by the forthcoming European security standards and by an Italian legislative decree that defined several *minimum* maturity levels for the implementation of subcategories that public administration *must* implement, imposing on all the public administrations to produce a cyber security self-assessment by the end of 2017. To this aim we are currently working with six IT experts, in order to contextualize the framework to their needs, define suitable subcategories priorities and maturity levels, assess the current profile, and define a target profile including, at least, all the minimum maturity levels for mandatory subcategories.

During the work meetings, we started using a large Excel sheet reporting the Framework functions, categories, subcategories, priorities, maturity levels, and controls. It was clear that while it was good for reasoning about details of single subcategories it was totally useless for providing an overview of the current state and the progress of the work we were doing. The perceived usefulness of colors used for distinguishing priorities, even on not readable zoom levels, pushed us to propose a visual analytics system mimicking the Excel structure. Experts were engaged in this activity, producing requirements like "I would like to quickly see the most critical situations", "It would be nice to have a clear priority on the controls to address", "I want to know at glance how far we are from our target". That lead to a six months of iterative design-implementation-informal validation cycles, producing the prototype that is presented in the paper (still getting change requests and new functionalities).

Experts really liked it, and even if CRUMBS did not substitute the Excel sheet ("I prefer inputting changes on a more familiar environment", "For inspecting details of a single subcategory and associated controls I like Excel more") they definitely prefer CRUMBS to get an overview ("I like the colors on the screen, they quickly point out problematic situations, especially the red/green combination when comparing the current profile with the target profile" (i.e., the gap analysis), "The horizontal priority line (i.e., implementation strategy) helps in spotting red (i.e., mandatory) controls that require a long time to be addressed. They are visible even if the thickness is very little, like breadcrumbs on a dark table cloth" (giving us an idea for the name of the system)). Currently we use a controlled Excel sheet to update changes in the current situation (e.g., a control that gets full addressed or the definition of a new target profile) and we parse it, propagating the changes to CRUMBS. Concerning the learning time, we come up with the empirical conclusion that it is better to initially use the Excel sheet to visually present the main framework concepts (functions, categories, subcategories, priorities, and controls) and after that move to CRUMBS.

6 Conclusions

The need to contrast the continuously evolving cyberattacks produced complex and structured strategies for defending computer networks by the growing cyber menace, strategies that have to deal with an overwhelming number of aspects and details. As a consequence, most of the IT companies deal with the issue of identify and prioritize the interventions and the controls than can effectively improve their cyber security level.

To mitigate such an issue, the paper presented CRUMBS, a visual analytics system targeted at dealing with the implementation of the IACSF, providing visual means for handling the framework structure (functions, categories, subcategories priorities and maturity levels). Moreover, the analytical engine of CRUMBS allows for (a) comparing the current profile with the target profiles, making clear what is missing and how far the organization is from the target, and (b) order the controls belonging to not fully covered subcategories, according to different organization implementation strategies, to optimize the transition process.

CRUMBS is actually used in the context of a collaboration with a large Italian company that is adopting the IACSF framework and has been informally evaluated with six IT experts in a user centered design activity lasted more than six months, refining the system using feedback about interaction, technical cyber security aspects and general visualization evaluation issues (see, e.g., [5]).

Concerning future work, we plan to proceed along two different directions:

- Extend the analytical capabilities of CRUMBS. The current prioritization algorithms use a simple cost function that takes into account the subcategories percentage completion and their priority. We are currently working on defining more complex optimization strategies;
- Explore and experiment the CRUMBS capabilities in other contexts, like ISO27001;
- Integrate in CRUMBS information about the business impact model of the organization, linking the elements of the IACSF with business mission and processes.

References

[1] Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology, 2014.

[2] M. Angelini and G. Santucci. Cyber situational awareness: from geographical alerts to high-level management. *Journal of Visualization*, pp. 1–7, 2016.

[3] Z. Anwar and R. Campbell. Automated assessment of compliance with security best practices. In *International Conference on Critical Infrastructure Protection*, pp. 173–187. Springer, 2008.

[4] A. Awad and M. Weske. Visualization of compliance violation in business process models. In *International Conference on Business Process Management*, pp. 182–193. Springer, 2009.

[5] E. Bertini, A. Perer, C. Plaisant, and G. Santucci. Beliv'08: Beyond time and errors - novel evaluation methods for information visualization. In *Conference on Human Factors in Computing Systems - Proceedings*, pp. 3913–3916, 2008.

[6] C. Criteria. *Common Criteria for Information Technology Security Evaluation, https://www.commoncriteriaportal.org/cc/*, 2017.

[7] K. Hajdarevic, C. Pattinson, K. Kozaric, and A. Hadzic. Information security measurement infrastructure for kpi visualization. In *MIPRO, Proceedings of the 35th International Convention*. IEEE, 2012.

[8] M. Harvey, D. Long, and K. Reinhard. Visualizing nistir 7628, guidelines for smart grid cyber security. In *Power and Energy Conference at Illinois (PECI), 2014*, pp. 1–8. IEEE, 2014.

[9] C. Horn and A. D'Amico. Visual analysis of goal-directed network defense decisions. In *Proceedings of the 8th international symposium on visualization for cyber security*, p. 5. ACM, 2011.

[10] ISO. Information technology - security techniques - information security management systems - requirements. *https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en*.

[11] ISO. Systems and software engineering - systems & software quality requirements and evaluation - system & software quality models. *https://www.iso.org/obp/ui/#iso:std:iso-iec:25010:ed-1:v1:en*.

[12] Research Center of Cyber Intelligence and Information Security. *A National Cybersecurity Framework, http://www.cybersecurityframework.it/en*.

[13] R. S. Russell. A framework for analyzing erp security threats. In *Proceedings of the Euro-Atlantic Symposium on Critical Information Infrastructure Assurance, March*, pp. 23–34, 2006.

[14] SEI. *Capability Maturity Model Integration. http://cmmiinstitute.com/*.

[15] University of Rome "La Sapienza". *Research Center of Cyber Intelligence and Information Security (CIS), https://www.cis.uniroma1.it/en*.

[16] G. Yee. Visualization for privacy compliance. In *Proceedings of the 3rd international workshop on Visualization for computer security*, pp. 117–122. ACM, 2006.