Visualization of Security Metrics for Cyber Situation Awareness

Igor Kotenko
Laboratory of Computer Security Problems
St. Petersburg Institute for Information and Automation
of the Russian Academy of Sciences (SPIIRAS) and
St. Petersburg National Research University of Information
Technologies, Mechanics and Optics, Saint-Petersburg, Russia
ivkote@comsec.spb.ru

Evgenia Novikova
Laboratory of Computer Security Problems
St. Petersburg Institute for Information and Automation
of the Russian Academy of Sciences (SPIIRAS)
Saint-Petersburg, Russia
novikova@comsec.spb.ru

***Abstract*— One of the important direction of research in situational awareness is implementation of visual analytics techniques which can be efficiently applied when working with big security data in critical operational domains. The paper considers a visual analytics technique for displaying a set of security metrics used to assess overall network security status and evaluate the efficiency of protection mechanisms. The technique can assist in solving such security tasks which are important for security information and event management (SIEM) systems. The approach suggested is suitable for displaying security metrics of large networks and support historical analysis of the data. To demonstrate and evaluate the usefulness of the proposed technique we implemented a use case corresponding to the Olympic Games scenario.**

Keywords-cyber situation awareness; security information visualization; high level metrics visualization; network security level assessment.

I. INTRODUCTION

Visual analytics techniques can be efficiently applied when working with big data and maintaining situational awareness in critical operational domains [11, 19, 29]. Cyber situational awareness considers the ability to answer on what and why is happening in the network, what the current attack impact and possible future damage is. The Endley's model of the situation awareness [5] includes also a comprehensive issue that relates to high level understanding of all available data, which requires high level of data correlation and integration. The results of D' Amica&Kocka [2] and R. Erbacher [6] researches revealed an urgent necessity to develop visualization techniques supporting decision making process and enhancing comprehension level of the security officers' situation awareness. In this paper we propose a visualization technique for representing a set of security metrics used to assess overall network security status and evaluate the efficiency of the protection mechanisms. We also consider that it could assist in solving other security tasks such as event analysis, attack detection, threat evaluation, etc. and, therefore, can be used in security information and event management (SIEM) systems for displaying high level information. Specifically, *the contribution of this paper* to the field of cyber situation awareness is a visualization technique displaying a set of security parameters, allowing comparative analysis of their current values with previous ones and applicable for large scale networks. To demonstrate and evaluate the usefulness of the proposed approach we implemented use case corresponding to the assessing network security state and efficiency of the countermeasures.

The paper is structured as follows. Section II describes visualization techniques designed for representing integrated security metrics and discusses their advantages and disadvantages. The next section presents our visualization technique and corresponding interaction techniques supporting data analysis. Section IV presents the case study used to demonstrate the proposed approach for solving security tasks. Conclusions sums up our contributions.

II. RELATED WORK

Due to the heterogeneity and complexity of security data - often with multidimensional attributes - many sophisticated visualization and interaction techniques have been proposed. They have been used to analyze the security of the whole information system, detect intrusions, investigate network flows, assess network security level, verify rules and policies of the security sensors as well as support decision making [9, 16, 17, 18, 20, 22, 23, 30].

Parallel coordinates, scatter plots, treemaps, special glyphs and circular models are being used to explore security data. Most of the developed visual models are intended to support analysis of low-level data such as network traffic, BGP routes, firewall policies, etc. [9, 16, 17, 18, 23].

Such models are valuable when identifying attack source, target and type, but not efficient in providing comprehensive understanding of the security state of information systems. Therefore, there is a need of the high-level representation of all available data in order to assess the efficiency of the security management and decision making with possibility to flexible operate low level data.

One of the model for building, visualizing, and interacting with multiscale representations of information visualization techniques using hierarchical aggregation was suggested in [4].

Almost all SIEM systems include executive dashboards which allow evaluating the overall security status of the information system and particular software and hardware

978-1-4799-4223-7/14 $31.00 © 2014 IEEE
DOI 10.1109/ARES.2014.75

elements as well as efficiency of security components. They include information about risk level, number of resolved and unresolved security events, etc. that is usually expressed in the form of generalized security metrics calculated for the whole network as well as for every host.

Usually such metrics are displayed using gauge-based metaphors or special designed pictograms mapped on network topology scheme or geographical map [1, 25, 26, 29]. For example, the OSSIM SIEM system provides special Risk Map view which displays information on the Risk (R), Vulnerability (V) and Availability (A) status of each network object located on the map, this information is presented in the form of traffic lights.

The usage of the traffic lights metaphor enables highlighting the criticality of the current metric value and assessing it in the context of all possible values. But these techniques allow representing only one or very limited set of metrics and do not provide any information on how the metric values change, though such historical information helps the user to evaluate the efficiency of security sensors and countermeasures implemented.

R. Erbacher [6] proposed a dial-based metaphor for representing a set of security metrics. Each metric is represented by the dial, and its value is reinforced with color to make perception of the value more quickly. To support historical analysis of the data, the author added rings within each of the dials representing historical values of the metrics. The outer ring provides the most current value (Fig. 1).

The set of the metrics is represented by the cyber command gauge cluster purposed to support decision making and other specialized security tasks. This gauge cluster consists of the set of the dials, the large dial located in the center displays value of the most important parameter for the given task, for example, overall network status, while smaller dials located around the large one provide information on the parameters associated with main one.

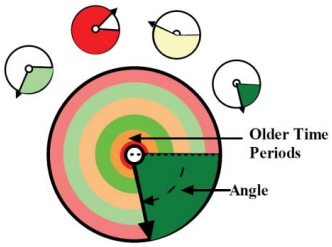

Figure 1. The concept of the security metric visualization in [6]

Matuszak et al. [21] discuss the problem of the cyber trust calculation and visualization in Smart Grid System. They proposed the model of the Operational Trust Indicator that displays three types of trust into one indicator, color is used to outline trust value. These parameters are represented by a section of the outer ring of the circle. The small circle in the center represents the overall trust, computed as a weighted sum of the other types of trust (Fig. 2).

Figure 2. The concept of the security metric visualization in [21]

Such glyphs associated with each node can be mapped on a geographical map or a network scheme. By clicking on them operators can drill down on the data and receive details of trust values and review associated metrics.

In summary, the state-of-the-art analysis has shown that there is a need to improve the representation of host/network parameters in a way that their number can be increased without loss of overview on an entire network.

We consider that the visualization technique proposed by R. Erbacher [6] is focused on decision support based on integrated metrics for one system/network/task and cannot be adopted for displaying security parameters of the set of hosts/tasks on one screen due to its space filling property. Thus, this technique could not be used for graphical presentation of security metrics of the large scale networks except ones calculated for a whole network. The visual model designed by Matuszak et al. [21] is suitable for displaying security metrics of the large set network objects, however it does not support historical analysis of the data.

III. VISUAL MODEL DESIGN

A. Concept

Our initial goal was to design the graphical representation of a set of security metrics used to assess network security level and impacts of attacks and countermeasures made by security officers. We wanted to provide an ability to compare previous values of several metrics before the protection mechanisms were introduced and their current value in order to support decision making on the necessity of such changes.

In the visual models suggested and the visualization tool created [15], treemap visualization technique was intensively used to analyze the possible consequences of attacks and countermeasures (Fig. 3 and Fig. 4). We used interactive treemaps to represent both a vulnerability report and a network security report. For example, to analyze the overall network security level we implemented the following visual model: the business value of the host defines the rectangle size, and calculated host security level or vulnerability severity - its color. Thus, the user attention is immediately attached to the most important for proper network functioning hosts. To analyze the general network vulnerability level the similar model was used except the rectangular color is determined by vulnerability level. However, in order to correlate these parameters the user has to switch between these two views and compare them.

To provide a possibility to analyze several metrics, we developed a circle-based model which is similar to one designed in [21], but is able to display previous values.

Figure 3. Treemaps: user-defined criticality vs. security level

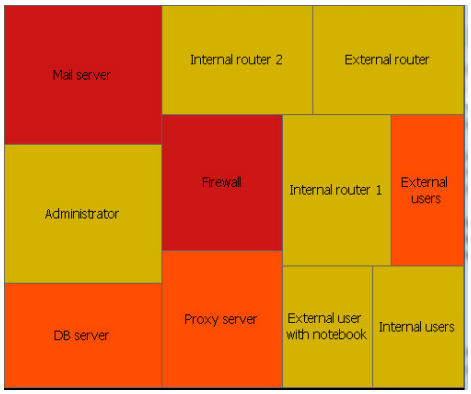

Figure 4. Treemaps: user-defined criticality vs. vulnerability severity

It is circle-based pictogram divided into *n* sectors which provide values of *n* metrics. The outer ring represents the previous values of the corresponding metrics (Fig. 5a). To highlight the criticality of the value we use color. We consider also a light modification of this model in which the criticality of the metric value is stressed by the sector radius (Fig. 5b).

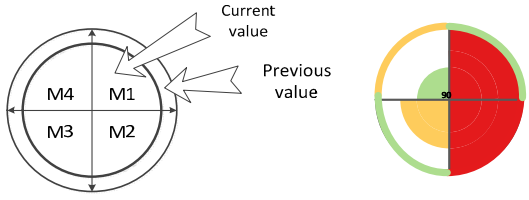

Figure 5. The concept of the security metrics graphical representation

B. *Interactions*

To support visual exploration of the data, we implemented the following interaction techniques.

Color encoding scheme setup. We developed a default color-safe scheme for displaying ordinal metrics that can have following values {High, Above Medium, Medium, Low}. However, this scheme cannot be easily adopted for displaying nominal and rational parameters as they need setting up threshold values to determine normal and critical values. It is necessary to provide a flexible mechanism for tuning color scheme for nominal parameters and defining threshold values and corresponding colors for rational ones.

Layout configuration. Depending on size of the investigated network we propose usage of several layout techniques. *For small and medium-sized networks* each network node is represented by *glyph* mapped on a network topology scheme, as this presentation is familiar to system administrators and they capture all information at glance. The second layout variant is an *interactive nested circular treemap*. In this layout circles are used instead of rectangles to display elements of hierarchical data. In our case each nested circle represents either host metrics or integrated network domain parameters. By clicking on it the user can drill down on next hierarchical level if possible. It is shown in [7] that *interactive circular treemap layout when being used in combination with circle-based glyph* can be effective in representing large amount of hierarchically structured data and overweigh the space-filling disadvantages of the technique. *For representing large scale network* we propose using *matrix layouts*. There are different approaches for displaying IP space using matrix [8, 16, 12] in meaningful way. We use the following technique: the subnets are arranged on the y-axis and the individual hosts are located on the x-axis [12] (Fig. 6). Displaying large scale networks on one screen can result in a small size of the glyph making it unreadable. To support navigation and data analysis the user has to be provided with zooming capabilities or special scaling mechanisms such as magic lens or fisheye.

Details on demand. By clicking on the glyph the user gets detailed information on the corresponding host. This information includes host ID, type, description, software and hardware installed, security metrics, vulnerability specific information (CVE code [3] and description). This informational display is updated whenever a particular glyph is selected.

IV. IMPLEMENTATION

The developed visualization technique was integrated in the VisSecAnalyzer tool designed to support the network security assessment [15].

The main window of the tool is divided into subviews (Fig. 7) designed to efficiently support cyber security analysis process [14].

The main *view A* shows the topology of the network, while the *view B* reflects the structure of the network, depicting domains or specified user network groups.

The user can switch between two main ways of network representation: using icons displaying host type or using glyph demonstrating security metrics.

The user can configure each host and network using the Property *View C*. It is possible to specify the predefined properties of the host such as IP address, host type (web server, ftp server, database server, router, firewall, etc.),

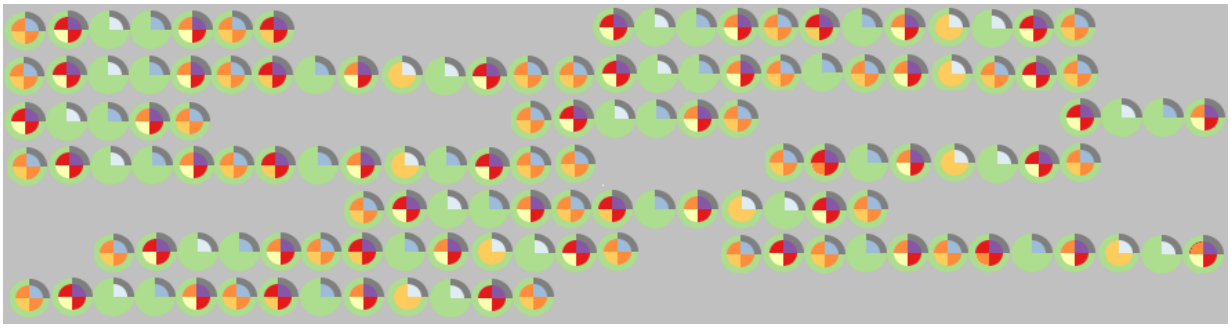

Figure 6. The matrix-based representation of the large scale networks

installed software and hardware, user-defined host criticality level. This property view is updated whenever a particular state node is selected. Thus user always has details at hand.

The *view D* shows the vulnerabilities detected on the host. They are represented using the directed graph reflecting possible sequence of their exploitation.

The vulnerabilities are grouped according access vector (local or network), required attackers skills and impact. User can expand or collapse each group to see its content, each vulnerability is displayed using its CVE code [3]. The detailed information is also displayed in Property View B, thus apart from brief information it is possible to get comprehend data on vulnerabilities detected.

We suppose that such dashboard design gives a general overview about security state of the network and communicate a lot of information in a glance. Thus, the user can analyze calculated host security metrics in the context of initial host configuration. All information is available in different views, but on one dashboard panel.

The prototype of the described visual model was implemented in Java using Jung library [10], which allows development of highly interactive visualizations.

The current implementation supports, for example, a set of security metrics used to assess network security level [13].

However, its implementation includes a tool for extension of this list and a mechanism for setting up color scheme.

V. CASE STUDY AND EVALUATION

In [6] a set of important everyday security tasks maintaining high level situational awareness is presented. It includes monitoring of network overall status, server status, attack review and some others focusing on estimation of performance and health of some critical network elements.

In this section we introduce another important task - network security level assessment, based on comprehensive vulnerability analysis, and demonstrate how it could be done using proposed visualization technique.

A. Examples of Security Metrics

In order to assess the network security level we suggest, for example, to use following security metrics [13]: *Host Criticality Level*, *Host Vulnerability Level*, *Attack Probability* and *Attack Impact Level*.

These metrics are calculated for each network host.

Host Criticality Level reflects the impact of host compromise on correct network functioning in case of attack success. It is determined by the host type (router, firewall, mail, web, database server), its role in the networking and software installed. *Host Criticality Level* is nominal parameter and can take the following values: {Undefined, Low, Medium, High}.

Host Vulnerability Level describes the severity of the vulnerabilities detected on the host and is defined using Common Vulnerability Scoring System (CVSS) [24]:

$$Vulnerability(h_k) = \max_i Critical\_BaseScore(v_i),$$

where h_k – k-th host of the system, $k \in [1..m]$,

$$Critical\_BaseScore(v_i) = \begin{cases} BaseScore(v_i), if\ BaseScore(v_i) \geq 7.0, \\ 0, \quad otherwise \end{cases}$$

$BaseScore(v_i)$ – CVSS base score for the vulnerability v_i, $i \in [1..n]$. CVSS base score can range from 0 to 10 according CVSS, interval [7.0, 10.0] is defined as critical.

Attack Probability reflects the probability of the attack success. There are different static and dynamic approaches to calculate this metric [13]. In our experiment we use technique, which considers probability of the vulnerability exploitation calculated on the base of CVSS and Bayes' theorem. In this case *Attack Probability* value varies from 0.0 to 1.0. This technique can be specified as follows: (1) Each state is defined as an attack graph node considering its pre- and post-conditions; (2) Source node of the attack gets probability value "1"; (3) Probability of transfer from one node to another is defined by the access complexity of the appropriate vulnerability (if there are few vulnerabilities that lead to the state, then the probability is defined by the minimum access complexity); (4) For each node local probability distributions are calculated by the probability of successful transfer from the previous node in two cases: success and failure on the previous node. On this base the unconditional probabilities of states are calculated by the joint probability distribution definition, i.e. for the set of states $S = \{S_1, ..., S_n\}$, $\Pr(S_1, ..., S_n) = \prod_{i=1}^{n} \Pr(S_i \mid \mathrm{Pa}[S_i])$, where $\mathrm{Pa}[S_i]$ - set of all parents of S_i [27].

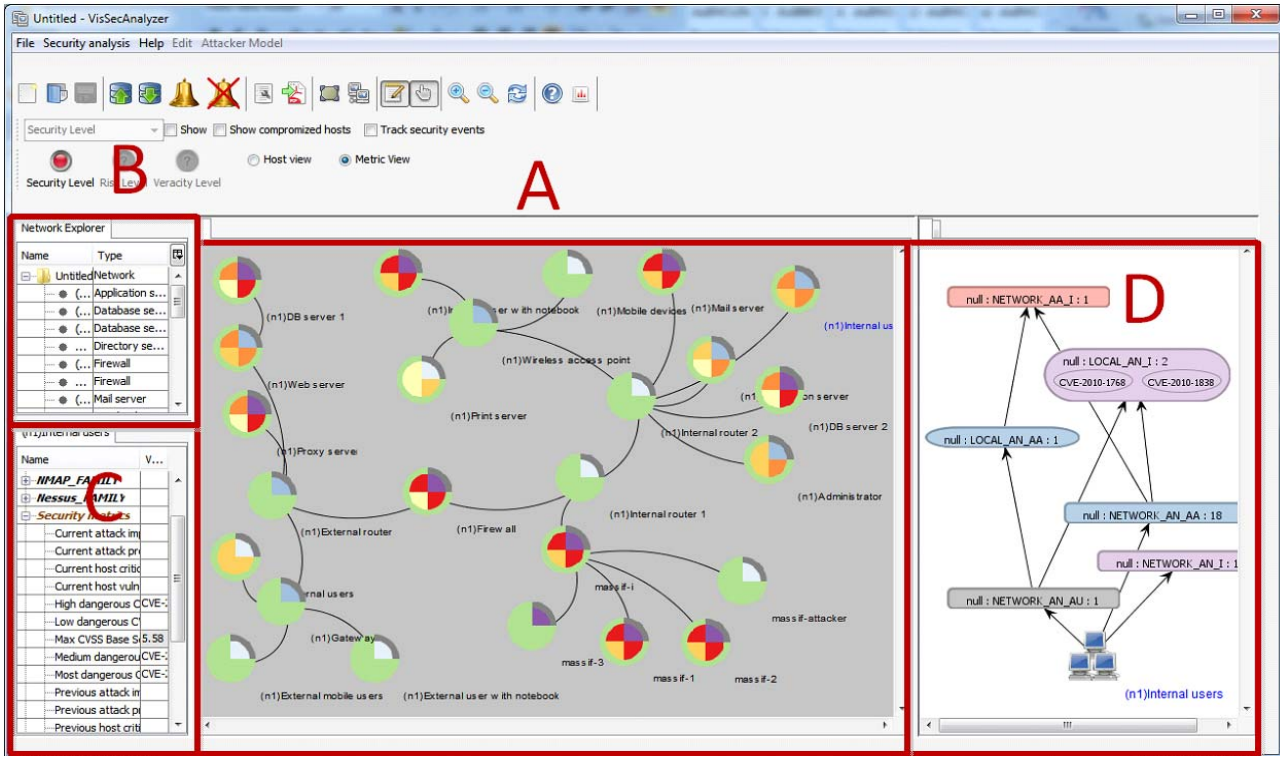

Figure 7. The main view of the VizSecAnalyzer

Attack Impact Level characterizes the impact of the possible attack for the given host criticality level. The native attack impact is determined by impact vector (I_c, I_i, I_a), where I_c – confidentiality impact, I_i - integrity impact, I_a - availability impact, which is defined for each vulnerability detected on the host using CVSS and then it is assessed with consideration of host criticality level. In this case *Attack Impact Level* is nominal parameter and can take the following values: {None, Low, Medium, Above Medium, High}.

We consider that these metrics are able to characterize the causes of network weaknesses (*Host Vulnerability Level*) and assess probability of the attack (*Attack Probability*) and possible consequences in case of its success (*Attack Impact Level*).

Host Criticality Level helps security officer to determine the most critical network hosts requiring remediation measures and prioritize countermeasures according to attack probability and its impact.

To encode selected security metrics we elaborated the following color encoding scheme: (1) For the rational and interval parameters we defined five intervals and labeled them as {None, Low, Medium, Above Medium, High}; (2) These ordinal values are encoded in yellow-red scale except None value which is represented by green color; (3) To encode Host Criticality Level we decided to use another colour scheme as this metric should be used by the analyst to prioritize his/her actions and is not purposed to notify about possible danger as other metrics.

Fig. 8 shows a glyph corresponding to the host with the following characteristics: *Host Criticality Level* - Medium; *Host Vulnerability Level* - Above Medium; *Attack Probability* - Medium; *Attack Impact Level* - Above Medium.

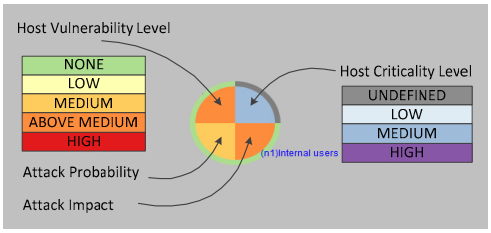

Figure 8. Host representation using developed glyph

B. *Olympic Games Scenario*

To demonstrate the proposed visualization technique we used a test network adopted from the Olympic Games scenario [24] (Fig. 9).

It consists of four subnets, one of which represents a part of Core Games System. This system is used to gather and control data about people who plan to attend Games events and about the staff. It includes also Accreditation (massif-1 host) and Workforce management (including volunteers)

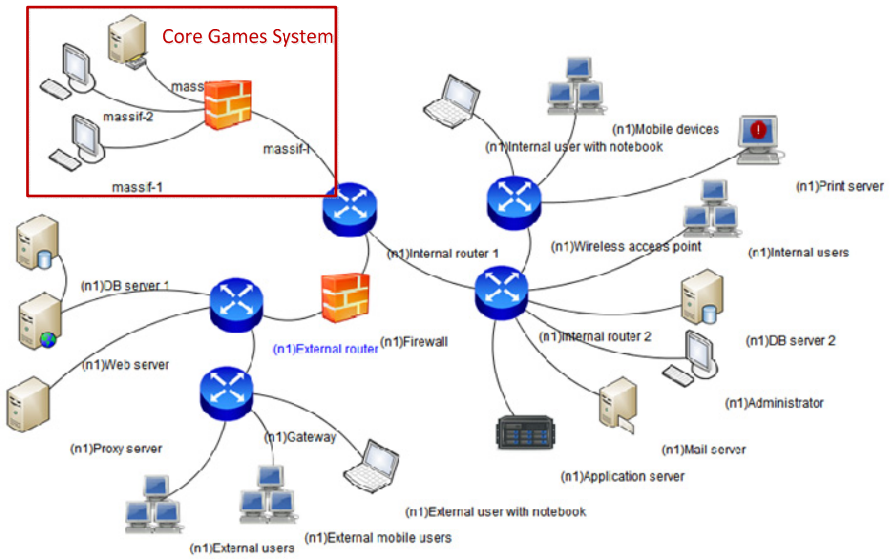

Figure 9. Test network topology

(massif-2 host) and Electronic Staff Information (ESI) (massif-3host) system. These hosts have high criticality value due to their functional role, the *Host Critical Level* of the rest hosts is determined by their type.

The other important network parameters for experiment are set as follows [13]: *massif-1 and massif-2*: Red Hat JBoss Community Application Server 5.0.1; Windows Server 2008 R2 for x64-based Systems; *massif-3*: NetIQ eDirectory 8.8.6.0; Novell SUSE Linux Enterprise Desktop 12ServicePack 1; *massif-i*:Novell Suse Linux Enterprise Desktop 11 Service Pack 1 and Citrix Ica Client For Linux 11.0; (*n1) Firewall*: Linux Kernel 2.6.27.33, Citrix Ica Client For Linux 11.0; *(n1)External mobile users*: Google Android Operating System 4.1.2; *(n1)External users* and *(n1)Internal users*: Microsoft Windows 7 64-bit; Apple iTunes 9.0.3;Microsoft Office 2007 SP1; Microsoft Internet Explorer 7; *(n1)Proxy server*: Linux Kernel 2.6.27.33; Gnome KDE; *(n1)Web server*: Windows Ftp Server 2.3.0; Windows Server 2008 for 32-bit Systems; Sun iPlanet Web Server 4.1 SP10 Enterprise; (*n1)DB server 1* and *(n1) DB server 2*: Apache Software Foundation; Derby 10.1.3.1; phpMYAdmin 3.5.2.2; Oracle MySQL 5.5.25; Linux Kernel2.6.27.33; *(n1)Administrator*: VMware vCenter Server Appliance (vCSA) 5.1;Ubuntu linux 10.04; Gnome KDE; *(n1)Mail server*: Windows Server 2008 for 32-bit Systems; Microsoft Exchange Server 2007 Service Pack 1; Microsoft Sharepoint Server 2007 sp1x64; *(n1)Mobile devices*: Apple iPhone OS 4.0.

C. *Displaying Security Metrics*

After the security metrics have been calculated for the given test network the security officer gets the view presented in Fig. 10. In our experiment the previous values of all security metrics were set to default values (None or Undefined) that is why outer rings of all glyphs is filled by green or grey color. It is rather easy to spot group of hosts with high criticality level and attack impact and medium level of attack probability. It includes the following hosts: *massif-1*, *massif-2*, *massif-i*. The hosts *(n1)Firewall, (n1)DB server 1, (n1)DB server 2* and *(n1)Proxy server* form another group of hosts with high criticality level and attack impact and low attack probability. The next group of hosts consists of hosts with medium criticality level, above medium attack impact and medium level of attack probability. It includes *(n1)Web server, (n1) Internal users* and *(n1) Administrator*.

The security officer should start implementing remediation actions with the first group of hosts. All these hosts have high vulnerability level, and the analyst has to examine the list of detected vulnerabilities in order to determine their source and their severity. To get this information he (she) can click on the glyph of interest and obtain detailed information on vulnerabilities including their description and CVSS characteristics. For example, in case of *massif-1* and *massif-2* all vulnerabilities are in Windows Server 2008 R2 for x62-based systems, thus the possible solution of the problem is installing corresponding service pack, for example, at least on Windows Server 2008 R2 SP1 for x62-based systems. The vulnerabilities detected on *massif-i* firewall are associated with Novell SUSE Linux Enterprise Desktop 11 Service Pack 1 and Citrix Ica Client For Linux 11.0, the possible solution of the problem is to update versions of software.

The analyst can assess the necessity of these countermeasures before implementing them by changing hosts' configurations and recalculating security metrics.

Fig. 11 shows that current values of host vulnerability level, attack probability and impact for the given hosts have significantly decreased and equal to None. It should be noted that glyphs corresponding to hosts with no changes in configuration do not have outer border as the previous values of security metrics equal to current ones.

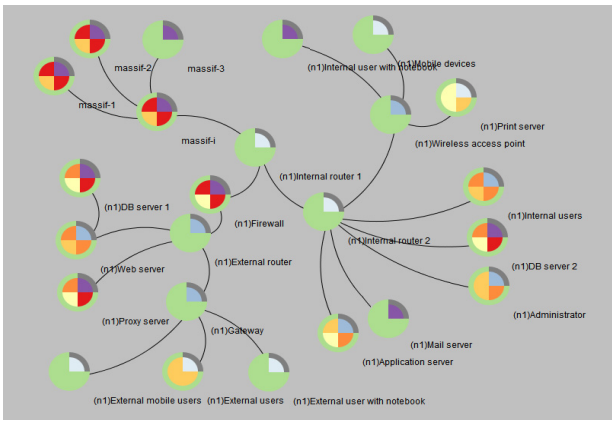

Figure 10. Initial host security level of the network

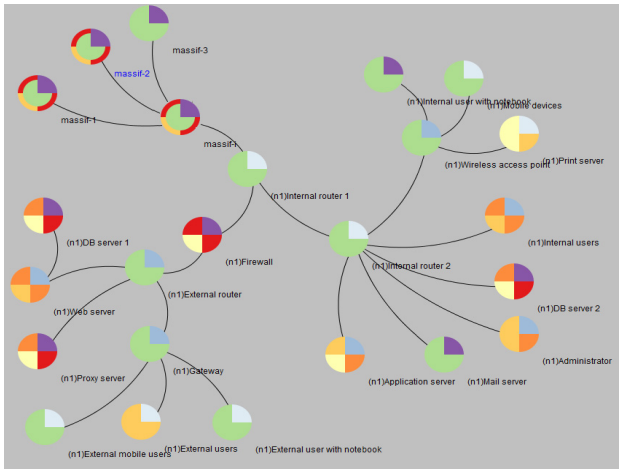

Figure 11. Host security level of the network after hosts' reconfiguration

D. *Comparing Efficiency of Countermeasures*

We consider that this technique could be also used when comparing efficiency of different countermeasures. In this case the security analyst can select metrics that characterize resulting overall security level of the host due to implemented countermeasures and, for example, *Return-On-Security-Investment* index for each countermeasure that characterizes possible damages due to security incidents and cost of security solution. Thus he (she) could select the most preferable remediation measures.

This approach can be adopted to estimate and select countermeasures for the whole network. To demonstrate this possibility we use the Olympic games scenario.

The countermeasure efficiency is assessed using improved *Return On Response Investment* index (RORI) proposed in [24]. It takes into account countermeasure cost, its associated risk mitigation, infrastructure business value and the expected losses that may occur in the result of attack. It also allows to compare results obtained by application of security solutions with no countermeasures. Its value can vary from -1 to ∞. It takes negative values when the cost of countermeasure is higher than the benefits it provides. It tends to equal zero when expected benefits are comparable with cost of security solution. Thus only when obtained benefit is higher than the cost of countermeasure, the RORI takes positive value.

To encode this index we use red-green color scheme. Positive values are normalized using maximum RORI value calculated for each countermeasure and displayed in green scale. Negative values are depicted using red colors.

For the given use case the following countermeasures were selected and evaluated [24]: C1 - Do nothing (RORI = 0.0%); C2 - Blocking suspected accounts. This solution can either delay or avoid the attack (RORI = 400.36%); C3 - Activate intrusion detection system (IDS) at strategic places. This alternative is useful to detect and avoid intruders in key points of the Olympic Games infrastructure (RORI = 308.96%); C4 - Change connection port. This candidate complicates implementation of reconnaissance attack (RORI = 163.64%); C5 - Activate multi-factor authentication. This alternative requests additional authentication credentials such as something the user knows (e.g., pass phrase, challenge response, PIN), or something the user has (e.g., biometrics) in order to authenticate the user and authorize him/her to perform the required task (RORI = 386.07%); C6 - Activate abnormal behavior rules. This countermeasure requires to update the existing rules to be more restrictive and/or to activate new rules that disable other less restrictive ones (RORI = 411.52%); C7 - Temporal deactivation of the account. This candidate will deactivate the user account for a period of 24, 48 or 72 hours (RORI = 259.40%).

Fig. 12 shows glyph displaying RORI indexes for a set of selected countermeasures. To highlight the maximum value we use border color as in this use case there are two comparatively equal RORI indexes (C2 and C6).

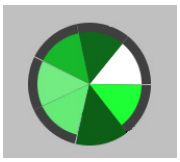

Figure 12. Glyph displaying RORI indexes

E. *Assessing Efficiency of the Visualization Technique*

To assess the efficiency of the proposed visualization technique we presented prototype and use case described above to security officers. They could implement different experiments, choose different security metrics and setup visual models.

Summarizing their feedback, we can say that almost all practitioners highlighted developed compact way to present graphically several metrics at once and possibility to compare current and previous values as solving security tasks often assume historical analysis of several metrics simultaneously. They also noted color encoding scheme used in use case.

However, there are questions about number of metrics which could be presented graphically using proposed technique. Specialists also marked the necessity to have glyph legend at hand as interpreting of the data could be complicated without this information even in case when they set up metric layouts in visual model themselves.

VI. CONCLUSIONS

In the paper we analyzed the visualization techniques used to present high level information maintaining situation awareness and proposed the novel approach to visualize a set of security metrics which allows comparative analysis of their current and previous values.

The developed visual model can be used to represent data of different type values and can be used to outline both traditional security parameters characterizing network flows and meta-data such as attack impact level. In order to assess the efficiency of the proposed approach we implemented the Olympic Games use case devoted to the network security level assessment and presented developed prototype to security officers. The practitioners gave positive assessment in general and marked compact way for presenting several metrics suitable for large scale networks.

The future research will be devoted to further elaboration and analysis of suggested visualization technique applicability for different security tasks. We will evaluate the performance of proposed visualization system and assess the usability of the graphical user interfaces.

ACKNOWLEDGMENT

This research is being supported by grants of the Russian Foundation of Basic Research (projects 13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417), the Program of fundamental research of the Department for Nanotechnologies and Informational Technologies of the Russian Academy of Sciences (2.2), the project ENGENSEC of the TEMPUS program of the European Community as well as by Government of the Russian Federation, Grant 074-U01, and State contract #14.BBB.21.0097.

REFERENCES

[1] ArcSight Website http://www.arcsight.com/products/products-esm/

[2] A. D'Amico, M. Kocka, "Information Assurance Visualizations for Specific Stages of Situational Awareness and Intended Uses: Lessons Learned," VizSec'05, 2005, pp.107-112.

[3] Common Vulnerability Scoring System, http://nvd.nist.gov/cvss.cfm

[4] N. Elmqvist, J. Fekete, "Hierarchical Aggregation for Information Visualization: Overview, Techniques, and Design Guidelines," IEEE Transactions on Visualization and Computer Graphics, Vol.16, No.3, 2010, pp. 439-454.

[5] M.R. Endsley, "Measurement of situation awareness in dynamic systems," Human Factors, 37, 1995, pp.65-84.

[6] R. Erbacher, "Visualization Design for Immediate High-Level Situational Assessment," VizSec'12, 2012, pp.17-24.

[7] F. Fischer, J. Fuchs, and F. Mansmann, "ClockMap: Enhancing Circular Treemaps with Temporal Glyphs for Time-Series Data," EuroVisv2012, 2012, pp.97-101.

[8] Y. Hideshima, H. Koike, "STARMINE: a Visualization System For Cyber Attacks," Proceedings of the Asia Pacific Symposium on Information Visualisation. Tokyo, Japan, 2006, pp.131-138.

[9] D. Inoue, M. Eto, K. Suzuki, M. Suzuki, and K. Nakao, "DAEDALUS-VIZ: Novel Real-time 3D Visualization for Darknet Monitoring-based Alert System," VizSec'12, 2012, pp.72-79.

[10] Java Universal Network/Graph Framework, http://jung.sourceforge.net/

[11] D. Keim, G. Andrienko, J.-D. Fekete, C. Görg, J. Kohlhammer, and G. Melancon, "Visual Analytics: Definition, Process, and Challenges," LNCS 4950, 2008, pp. 154–175.

[12] C. Kintzel, J. Fuchs, and F. Mansmann, "Monitoring Large IP Spaces with ClockView," VizSec'11, 2011.

[13] I. Kotenko, E. Doynikova, and A. Chechulin, "Security metrics based on attack graphs for the Olympic Games scenario," PDP 2014, 2014, pp.561-568.

[14] I. Kotenko, A. Chechulin, "Attack Modeling and Security Evaluation in SIEM Systems. International Transactions on Systems Science and Applications," Vol.8, December 2012, pp.129-147.

[15] I. Kotenko, E. Novikova, "VisSecAnalyzer: a Visual Analytics Tool for Network Security Assessment," LNCS, Vol. 8128, 2013, pp 345-360.

[16] K. Lakkaraju, W. Yurcik, and A.J. Lee, "NVisionIP: Netflow visualizations of system state for security situational awareness," VizSEC/DMSEC'04. New York, USA, 2004, pp.65-72.

[17] S. Lau, "The spinning cube of potential doom," Communications of the ACM, Vol. 47(6), 2004, pp.24-26.

[18] C.P. Lee, J. Trost, N. Gibbs, N. Beyah, and J.A. Copeland, "Visual Firewall: Real-time Network Security Monitor," VizSec 05, 2005, pp.129-136.

[19] S. Liu, W. Cui, Y. Wu, M. Liu, "A survey on information visualization: recent advances and challenges," The Visual Computer, January 2014.

[20] F. Mansmann, T. Göbel, and W. Cheswick, "Visual Analysis of Complex Firewall Configurations," VizSec'12, 2012, Seattle, WA, USA, 2012.

[21] W.J. Matuszak, L. DiPippo, and Y. Lindsay, "Sun CyberSAVe – Situational Awareness Visualization for Cyber Security of Smart Grid Systems," VisSec'13, 2013. pp.25-32.

[22] E. Novikova, I. Kotenko, "Analytical Visualization Techniques for Security Information and Event Management," PDP 2013. IEEE Computer Society, 2013, pp.519-525.

[23] K. Ohno, H. Koike, and K. Koizumi, "IP Matrix: an effective visualization framework for cyber threat monitoring," IV05, Washington, DC. IEEE Computer Society, 2005, pp.678–685.

[24] Olympic Games scenario. MASSIF FP7 Project. MAnagement of Security information and events in Service Infrastructures. http://www.massif-project.eu.

[25] OSSIM Website http://alienvault.com/products/unified-siem/siem

[26] Prelude IDS, https://www.prelude-ids.org/

[27] N. Poolsappasit, R. Dewri, I. Ray, "Dynamic security risk management using Bayesian attack graphs," IEEE Transactions on Dependable and Security Computing, vol.9, No.1, 2012, pp.61-74.

[28] QRadar SIEM Website http://q1labs.com/products/qradar-siem.aspx

[29] H. Shiravi, A. Shiravi, and A.A. Ghorbani, "A Survey of Visualization Systems for Network Security," IEEE Transactions on Visualization and Computer Graphics, Vol.18, No.8, 2012, pp.1313-1329.

[30] T. Tran, E. Al-Shaer, and R. Boutaba, "PolicyVis: Firewall Security Policy Visualisation and Inspection," LISA'07, USENIX Association, Berkeley, CA, USA, 2007, pp.1-16.