Journal of Siberian Federal University. Engineering & Technologies 2022 15(1): 102–120
~ ~ ~

DOI: 10.17516/1999-494X-0377

УДК 004.056:159.937.5

Cognitive Analysis of Intrusion Detection System

Saad Masood Butt* and Carmen Reaiche
College of Business, Law and Governance
James Cook University

Received 18.10.2021, received in revised form 11.01.2022, accepted 06.02.2022

Abstract. Usability evaluation methods have gained a substantial attention in networks particularly in Intrusion Detection System (IDS) as these evaluation methods are envisioned to achieve usability and define usability defects for a large number of practical software's. Despite a good number of available survey and methods on usability evaluation, we feel that there is a gap in existing literature in terms of usability evaluation methods, IDS interfaces and following usability guidelines in IDS development. This paper reviews the state of the art for improving usability of networks that illustrates the issues and challenges in the context of design matters. Further, we propose the taxonomy of key issues in evaluation methods and usability problems. We also define design heuristics for IDS users and interfaces that improves detection of usability defects and interface usability compared to conventional evaluation heuristics. The similarities and differences of usability evaluation methods and usability problems are summarized on the basis of usability factors, current evaluation methods and interfaces loopholes.

Keywords: intrusion detection system, heuristics evaluation, IDS interface, usability evaluation methods.

Citation: Saad Masood Butt, Carmen Reaiche Cognitive Analysis of Intrusion Detection System. J. Sib. Fed. Univ. Eng. & Technol., 2022, 15(1), 102–120. DOI: 10.17516/1999-494X-0377

* Corresponding author E-mail address: saad.butt1@my.jcu.edu.au, carmen.reaiche@jcu.edu.au

Когнитивный анализ системы обнаружения вторжений

Саад Масуд Бут, Кармен Рейш
Колледж бизнеса, права и управления
Университет Джеймса Кука

Аннотация. Методы оценки удобства использования (юзабилити) пользуются значительным вниманием в сетях, особенно в системе обнаружения вторжений (IDS), поскольку предназначены для определения дефектов в практических программных продуктах. Несмотря на большое количество доступных опросов и способов оценки, мы считаем, что в имеющейся литературе существует пробел с точки зрения методов оценки юзабилити, интерфейсов IDS и следования рекомендациям по удобству использования при разработке IDS. Здесь рассмотрено современное состояние удобства использования сетей, которое иллюстрирует их проблемы. Далее мы предлагаем классификацию ключевых вопросов по методам оценки и проблемам удобства использования. Мы также определяем эвристику проектирования для пользователей IDS, которая позволит обнаруживать дефекты и улучшать удобство использования интерфейсов по сравнению с обычной оценкой. Сходства и различия методов оценки и проблем юзабилити обобщены с точки зрения факторов удобства использования, современных методов его оценки и брешей в интерфейсах.

Ключевые слова: система обнаружения вторжений, эвристическая оценка, интерфейс IDS, методы оценки удобства использования.

Цитирование: Саад Масуд Бут, Кармен Рейш. Когнитивный анализ системы обнаружения вторжений / Саад Масуд Бут // Журн. Сиб. федер. ун-та. Техника и технологии, 2022, 15(1). С. 102–120. DOI: 10.17516/1999-494X-0377

1. Introduction

Network security guarantees protection of valuable and available network assets from viruses, key loggers, hackers and unauthorized access. Network practitioners utilize special tools such as firewall, antivirus, NMAP and Intrusion Detection System (IDS) in order to manage network security. Among all these tools, IDS is considered as the important network tool in managing the network security. Security practitioner interacts with IDS though an interface. This interface may be used to perform administrative function or to support even monitoring and analysis. This interaction of security practitioner with IDS interface is an important aspect of human computer interaction (HCI) indicating that security should inevitably lead to trust of the system by the security practitioners [19]. One of the most important parts of IDS systems is the display interface that shows there are many usability issues as well as design deficiencies, which needs to be addressed [40]. Usability ensures better understanding and efficiency among IDS systems to make them more user-friendly and humanized. This process helps in better understanding and usage of IDS systems by maximum possible users including novice users [40]. It is observed that users fail to understand the display of IDS systems as it provides unrelated information also it contains too many technical specifications which are not require to user [40].

For the past few years, internet has evolved. The challenge of network security has also increased. Research shown that human and organization factors have impacts on network security [31]. Human in terms of knowledge, experience and background can affect network security; whereas organization

who are not familiar with network security tools and data protection will give effect on the network and data security. This is a significantly prominent issue for many organizations who want to protect their useful and confidential data from either inside or outside threats of the organization. Other researches have highlighted various challenges while using IDS such as considerations for deployment, configuration of security settings, availability of information about log storage in IDS and requirement of additional software for better operations [37, 39]. These challenges have propelled us to arrive at some vital usability heuristics in our study. Similarly, some research has discussed issues in testing of IDS [4]. These issues have guided us in designing heuristics for IDS.

This paper focused on humans who are the practitioners or users of IDS system. IDS is treated as vital element in companies as a protective measure on network from being abused. However, often IDS users find it difficult to use IDS and unable to take advantage of all its functionalities. Two main problems need to cope in IDS. One is related to state of the art and other one state of practice; the techniques or algorithm used to detect the attack and human interface that enables security administrators or network practitioners to quickly detect and respond the attack. Techniques and algorithms are designed for IDS to detect improper access in the network but not for the improvement IDS interface [64]. However, experience shows working software still fails when the user interface is not up to the user level [19, 64].

One approach to improve the effectiveness of IDS and address challenges faced by users and interface usability issues in IDS can be done by designing heuristics [40]. In this approach survey is conducted as an initial step to understand the state of practice in security management with a particular focus on intrusion detection systems. Based on these survey results, new heuristics are developed to measure the effectiveness and efficiency of IDS [64]. Evaluating the usability of IDS is challenging even though many usability evaluation methods are available like in laboratory experiments may have little validity due to the complexity of real-world security problems and the need to situate a specific tool within a larger context [26]. However, in field observation method it is difficult to recruit network practitioners for simple interviews [40, 27]. Direct observation method can be time consuming as much security work is spontaneous (e. g., security incident response), or occurs over many months (e. g., deploying an identity management system). As IDS is intrinsically cooperative, its study inherits the difficulties of studying [26]. Therefore, heuristic evaluation of IDS could be a viable component of usability evaluation among other evaluation methods. While, heuristic evaluation is a very popular and widely used discount usability inspection method and usability evaluation [64]. Heuristic evaluation results assist to develop usable interactive interface for IDS to aid network practitioners in managing security efficiently. Therefore, usable interactive interface is very important in such real time system and security application where users need to respond the attack in a small amount of time or else attacks can have serious consequence [8].

The goal of our research is to develop and evaluate new set of heuristics for evaluation IDS. The focus of our heuristics is on finding problems that hinder the use of IDS due to its complex interface and require knowledge to deal with complexity. To make heuristic evaluation method more effective, similar technique [52] is used, in which author automate the evaluation method to reduce manual work and focus on capturing more defect then compare to manual evaluation method. Our validation is similar to that mentioned in [26] i. e. an empirical evaluation of new heuristics in which author compared its usage to Nielsen's heuristics.

The rest of the paper is organized as follows. Section 2 introduces literature reviews on usability evaluation techniques used in networks, important usability factors in evaluation and usability issues with software developers, network and interfaces. Section 3, presents a procedure to proposed new heuristic for IDS users and interface improvement and its methodology. These heuristics are designed from the problem found in literature and survey conducted with IDS users. To make heuristics evaluation process efficient and fast we embed our proposed heuristics instructions in a partially automated system that helps to detect usability issues in IDS interface and provide recommendations to remove detected usability issues. Section 4 concludes the paper.

2. Literature review

2.1 Types of Usability Evaluation Techniques used in Networks

This section describes some of the usability evaluation techniques used in networks. Before going into the detail of usability evaluation techniques, ISO 9126–1 define usability as»the capability of the software product to be understood, learned and liked by the user, when it is used under specified conditions» [24]. Several usability evaluation methods were proposed like cognitive modelling, inspection methods, prototyping methods, inquiry methods and testing methods which may be useful in allowing researchers and practitioners to perform effective usability evaluations [9]. The most popular methods used in usability evaluation is inspection methods which can be further categorize into four methods: card sorting, cognitive walk through, heuristic evaluation and ethnography [20, 21]. Figure 1 shows the taxonomy of usability evaluation methods.

Among all evaluation methods, heuristics evaluation is mostly widely used and proved to be an efficient and effective method for inspecting usability of software [43, 54]. However, it is reported

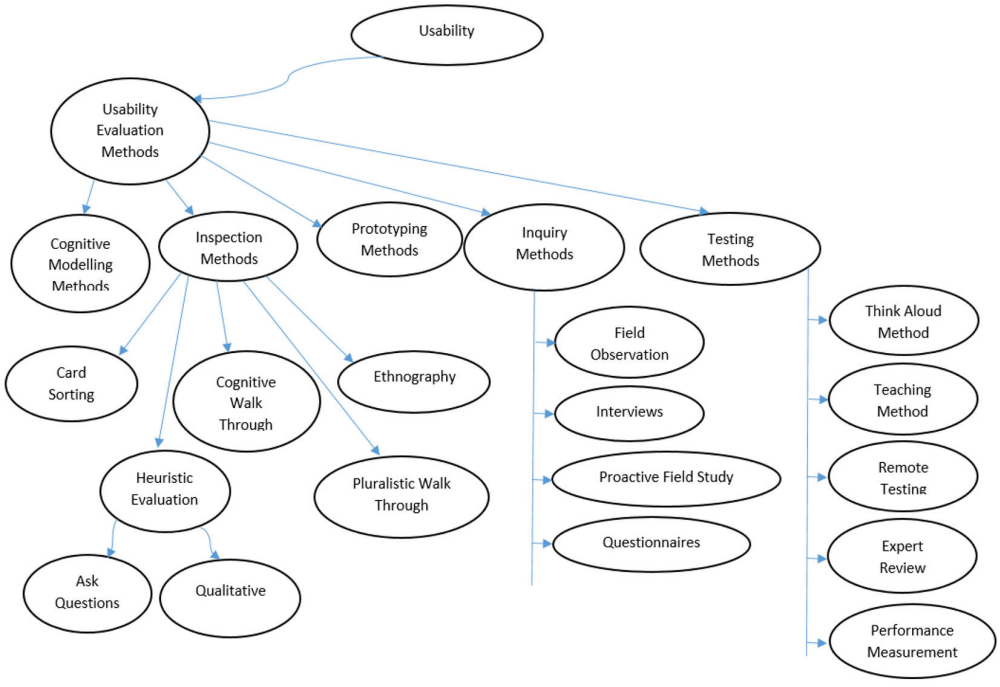

Fig. 1. Taxonomy of key usability evaluation methods

in literature that current heuristics are not efficient to apply on network software [54]. Therefore a new set of IDS heuristics to improve security through better usability is developed. New set of IDS heuristics identified significantly more usability problems in IDS than general heuristics did [64]. Similarly there are usability issues as well as design deficiencies, which needs to be addressed in IDS [40]. A specialized set of heuristics categorized into relevant groups to ensure better understanding and efficiency among IDS systems to make them more user-friendly and humanized. This process helps in better understanding and usage of IDS systems by maximum possible users including novice users.

Currently usability inspection method is manually done that can have a negative impact on the success of software. To ensure project success is by improving the manual processes of the usability inspection via automation [52]. With the growing expectation from stake holders to complete projects within a shorter duration and reduced budget, the manual processes are becoming a bottleneck that can jeopardize the project deliverables. But the evolution of software keeps on improving and adding new characteristics in software which therefore leads to the enhancing the usability evolution methods. New usability heuristics [26, 41, 64] are proposed and compared with Nielsen's usability heuristics to evaluate the usability of network software's. It is suggested that heuristics should be simple to evaluate the software for example using heuristic evaluation using paper-based screen shots of a user interface was expeditious, inexpensive and straightforward to implement [1]. In addition, a hybrid usability methodology (HUM) comprising of LBUT (Lab Based Usability Testing) and EHE (Exploratory Heuristics Evaluation) was proposed because the usage of traditional usability testing techniques are insufficient and irrelevant with the growing complexity of software and constraints faced by usability practitioners [51].

Therefore usability evaluation of intrusion detection systems interface are complex and provide many challenges for security practitioners because security issues aspects are still somewhat poorly served from a usability perspective [12]. Even the installation and the initial configuration of an IDS can be so challenging that they can serve as a barrier to use [61]. One of the challenges is to design more effective interfaces of Intrusion detection systems [56]. For instance, an experiment was conducted to compare a visual interface with a command-based textual interface. The textual interface allowed for better performance in the ID task. Users spent less time on the task because more of the details were readily available with the textual interface and they were able to be more efficient, using fewer commands. With the visual interface, users spent more time interacting with the interface to gather information, as some of the needed data was not readily available. On the other hand multi-touch interface for intrusion detection environments proposed [16] that includes an extensive ethnography to provide a richer understanding of socio-organizational development of ID environments, tools, and technologies. By using touch interaction, interface will enable exploration through the use of gestures to zoom, pan, and manipulate data. In addition aesthetic plays an important role in the interface design [53, 58]. The influence of design aesthetics played an important role in usability testing effects on user performance and perceived usability. User performance will be better for the more aesthetically pleasing product than for the less pleasing one. Perceived usability will be higher for the aesthetically more pleasing product than for the less pleasing one. From the research [45] it appears that in order to design a highly usable product, an appealing design would be one of the necessary product features. This would suggest that the issue of aesthetics should be closer to the heart of the ergonomic design process than perhaps previously thought.

2.2 Factors in Usability Evaluation

In previous section discussed usability evaluation methods and mostly commonly used heuristic evaluation in inspection method. Every evaluation when designed and conducted having few factor that need to considered during evaluation e. g. time, effectiveness, efficiency and usefulness etc. [17, 31, 52]. In this section we will discuss some of the important factors that considered in usability evaluation. Currently most commonly used usability evaluation method is heuristic evaluation, which is now improved and automated to increase its efficiency that helps to detect more usability defect in less amount of time as compare to the Neilson heuristic [52]. The development of new heuristic or improvement in the current heuristic is important because the usage of traditional usability testing techniques are not sufficient and suitable with the growing complexity of software due to the rapid change of software [51]. Some research focused on the design aesthetics in usability with finding that user performance will be better for the more aesthetically pleasing product than for the less pleasing one [53, 58]. Based on all past work and important factors in usability evaluation [47, 50], Fig. 2 shows the taxonomy of key factors in usability evaluation and these factors are briefly described in Table 1.

2.3 Usability Problems

Discussed in section 2.2 about usability factors that are considered at the time of usability evaluation. In this section we divide usability problems into four categories i. e. usability problem with software developers, usability problem in networks, usability problem in software interface and usability problem in evaluation.

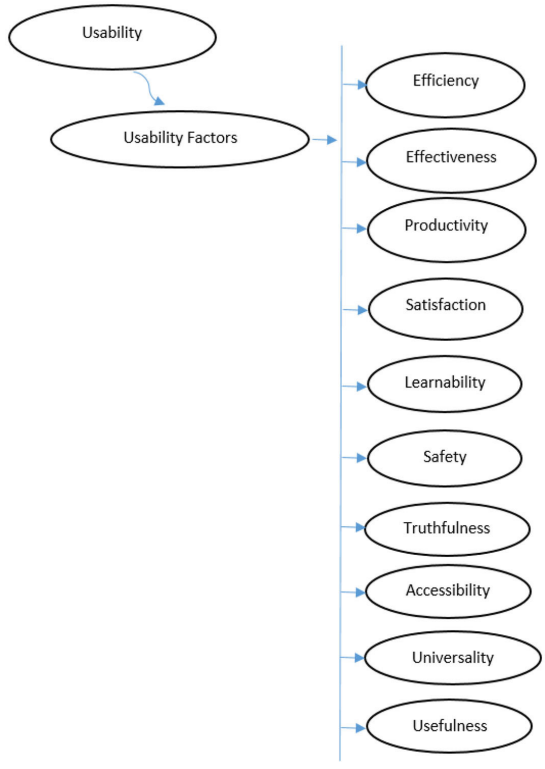

Fig. 2. Taxonomy of usability evaluation factors

Table 1. Usability factors

Factors	Description
Efficiency	The capacity of the software that helps users to utilize resources appropriately in relation to the effectiveness achieved.
Effectiveness	The capacity of software that helps users to finish task with accuracy and completeness.
Productivity	The attained level of effectiveness with respect to the resources utilized by users.
Satisfaction	Subjective opinion of user about their feelings while interacting with software.
Learnability	The capacity of software help users to learn required feature to perform that task.
Safety	The capacity of software to prevent the risk of harm to other resources.
Truthfulness	The capacity of software to offer trust to its users.
Accessibility	Software can be used by other users having some type of disabilities.
Universality	The capacity of software to accommodate large range of users with different cultural background or demographics.
Usefulness	The capacity of software to facilities users to solve real problems in a suitable way.

2.3.1 Usability problems with software developers

The field of human-computer interaction (HCI) has been defined as a multidisciplinary subject. To design usable systems, experts in the HCI arena are required to have distinct skills, ranging from an understanding of human psychology, to requirements modelling and user interface design [35].

HCI professionals are known as interaction designers, usability experts, graphic designers, user experience experts etc. [34]. HCI professionals focused on interface design issues such as ease of learning, ease of use, user performance and satisfaction or aesthetics. Whereas, software engineers considers how functional requirements are translated into a running system.

Software engineers are generally trained in topics such as algorithms, data structures, and system architecture or database design [42]. As software engineers are responsible for implementing user interface design specifications as running code, there is a need to communicate with HCI professionals. The interaction layer as interface between system and user is the area where HCI and SE are required to work together, in order to ensure that the resulting software product behaves as specified in the initial requirements engineering. To provide a high level of user interface usability, software engineering has to work with people with a background in HCI [11, 48].

To achieve high level of usability it is important to conduct usability evaluations of software interfaces which are done by usability experts [10]. In a lot of small and medium scaled company's, software developers are compelled to learn to manage usability factors. Incorporating usability features into software applications may not be a straightforward process for software developers who have not been trained in usability [3, 5].

2.3.2 Usability Problems in Network

From the advancement of web, users have been confronting difficulties of the system security [64]. To face security difficulties, system users use different tools, for example, firewall, antivirus programming, ethereal, nmap, nessus, and Intrusion Detection System (IDS). These tools are created in such a manner, to the point that they give just fractional direction to the end users [36]. In light of

which however end users have progressed security programming tools under control, they were not able to use the security characteristics inbuilt. Thus, the centre of work is moving towards the usability of security tools [36, 40]. Current IDS systems are not simple to utilize as there are usability issues and design deficiencies, which needs to be tended to in IDS. Troubles in judging the nature of the output, i. e. getting productive alert and seriousness level for identified intrusion data. Likewise the issues in installing and configuring the IDS systems go unnoticed [40].

There are two principle issues in regards to the state of the art and the state of practice in IDS. First, the underlying strategy in catching attacks and second the human interface to empower network administrators to rapidly and precisely detect such attacks and respond to these attacks. Hence the significance of usable interface is especially paramount in ongoing and security application [64]. Traditionally, IDS research has concentrated on algorithms and technical solutions for enhancing the accuracy of IDS [23] but recent research shows great importance to address IDS user needs to improve IDS usability [6, 19]. The characteristics of network tools are becoming more and more complex. Therefore, there is a question whether the Nielsen's heuristics still an appropriate instrument to evaluate the usability of these new categories of software applications or it is not [41].

To increase usability of IDS system, it is hard to evaluate by regular methods. Thus, importance of designing heuristic evaluation is more attractive for network tools [26]. Hence, the standard usability heuristics are hard to apply as network security tools are evolved with new features that cannot be evaluated by old heuristics. To ensure the usability in IDS it is important to improve the manual processes of the usability inspection via automation [52]. With the growing expectation of network users from network application developers to achieve usability and complete development within a shorter duration and reduced budget, the manual processes of usability inspection are becoming a bottleneck that can jeopardize the development deliverables and usability [25, 52].

2.3.3 Usability Problem in Interface

The area of human-computer interaction (HCI) provides tools for understanding the interaction between humans and computers. Interaction with various types of users takes place through the system's user interface [15]. HCI concern with the design, evaluation, and implementation of interactive computing systems and the study of the systems. HCI contributes techniques, methods, and guidelines for designing better and more «usable» artefacts that support interaction between human and system [55].

Human factors and usability issues have customarily assumed a constrained part in security research and secure systems development. Security practitioners have generally overlooked usability issues, in light of the fact that they frequently neglected to perceive the imperativeness of human factors and fail to offer the expert solutions to address these issues. Fortunately, there is a developing recognition that today's security issues can be solved just by addressing issues of usability and human factors [7]. Issues between security and usability goals are evaded by combining the goals together throughout an iterative design process.

A successful design involves addressing users' expectations and inferring authorization based on their acts of designation [62]. At present there are two types of interfaces are used in ID, textual (command-line) and visual interfaces. These two interfaces are common modalities to support engineers in ID [56]. The textual interface, which normally provides a command line, is used to operate textual data (e. g. network logs, system logs, etc.). This textual data is the principle asset for

system security engineers since it gives definite data about the evolving utilization of the network system [7, 13]. The commands used in the interface permit network practitioners to rapidly modify the information into a form where they can analyze the information but these commands are rich, expressive, flexible, powerful and complex that often results in overload and makes task of ID more difficult and cognitively intensive.

The research is evolving in the network security community which helps to leverage the benefits of visualization to reduce the time and cognitive workload that associated with the ID task [14, 30, 56, 60, 63]. It also has evolved in using multi-touch design interface for network security analysts that help users to manage environmental complexity, afford intuitive analysis of traffic and make better decisions and provide a comprehensive data visualization/exploration tool for the security analysts [16].

In section 2.1 we dicussed about usability evalution methods, cognitive walkthrough (CW) is a usability evaluation method that investigates the effect of interface design decisions on the user's problem solving processes and the user's ability to learn to use a system through exploration [22]. Cognitive walkthrough often used as a formative tool to evaluate interface design prototype of system and provide early feedback of unintended consequences not foreseen by the system designer [33]. Drawbacks of utilizing cognative walkthrough method incorporates the relative high cost of evaluation when contrasted with other types of usability studies because of the amount of time to prepare, conduct, and analyze the data [15, 21].

Often user interface of software applications perceive the quality of whole software by the users as user interface of software applications play a essential part in communication with users [32]. Attractive user interface of software applications often lead to market success. Using conventional approach of user interface development required signnifiant implementation efforts. About one half of an application code is related to the user interface [28]. The application cost signifiantly affected by the time and effort invested on the user interface. Using adaptive user interfaces increase the cost, time and effort of the application that provides number of features and support different type of users [57]. Therefore, it is essetional to develop that run natively on mutliple platesform. This will lead to code replication when the platform dependent UI part of the application must be restated for each supported platform [18]. From the development point of view it is challenging to deal with multiple plateforms because each plateform has more or less different devleopement mechanism and different progrmaming language [32, 59]. Hence the development of user interface becomes more serious for adaptive user interface that reflect changes in the current usage context. In that case it would be difficult to implement user interface that fit the requirements of all possible contextual situations because it would be a big amount of restated user interface code for individual situations. Therefore, the development and maintenance costs for the UIs would be very high.

To achieve the software usability and predict the user behaviour, software designer developed the prototype of the software before they move toward the actual development of the system [49]. There are two kinds of prototypes mostly used by software desginers, high fidelity and low fidelity prototypes. The type prototype used for usability testing is influenced by a number of constraints that are present in design processes, time pressure and financial limitations. This typically requires the utilization low fidelity prototypes because they are cheaper and faster to built then high fidelity. The choice of selecting the prototypes to under user behaviour and achieve usability is up to the software designer choice. Although low fidelity protoypes are faster and cheaper to built but on the other hand high

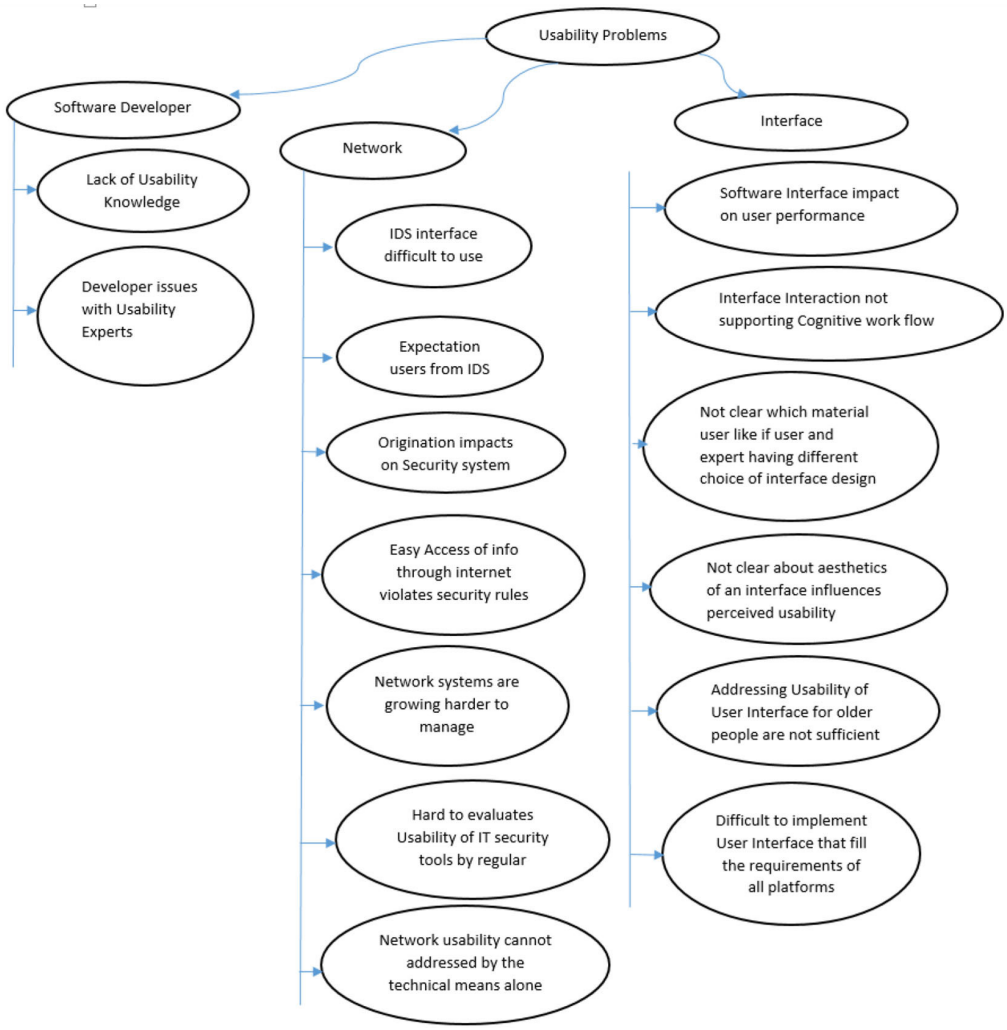

Fig. 3. Taxonomy of usability problems

fidelity prototypes is time consuming and expensive to built. The findings obtained with a prototype of too low fidelity may not be valid and this requires thorough consideration of what level of fidelity would be best pick for software to under user behaviour and achieve usability [44]. Majority of research studies concluded that the reduced fidelity prototypes provided equivalent results to fully functional software [29, 46].

In this section we discussed usability problem in the context of software developer, networks and software interfaces. Hence, we outline the most influential usability problems that are important for IDS usability. Figure 3 shows the taxonomy of usability problems.

3. Proposed Heuristics

In section 2 we outlined three important literature research; one is the usability evaluation methods, second is usability factors and third is the usability problems. Based on section 2 literature research we select heuristics evalution methods to achieve IDS usability. We proposed our heuristics for evaluating

IDS sytems that aims to address some of the shortcomings of existing usability evalution methods and usability problems. These proposed heuristics builds on existing theories mentioned in section 2 but is tailored specifically for IDS applications. These heuristics are categorised and are discussed in details.

3.1 Heurtistics for Users

The heuristics under this group are useful to check user knowledge and expertise in the field of IDS. These heuritisctics particularly focusing on users which were not specifically defined for users in other usability evaluation methods [1, 2, 26]. The heuristics under this category are required at the time of understanding users of IDS systems.

Table 2. IDS User Heurtistics

	User Heuristicis	**Attributes**
H1	User with networking knoweledge	Knowledge
H2	Experience in IDS	Expereince
H3	Provide help about the networking terminology in IDS	Help

3.2 Heuristicis for IDS display

Display interface of software considered as most important part of software. Based on the literature and problem, we define new heuristics for the interface of IDS as in Table 3.

Table 3. IDS Interface Heurtistics

	Interface Heuristicis	**Attributes**
H4	Interface is easy to understand and provide relavent information	Understandable
H5	Customization of GUI of IDS Interface	Customization
H6	Efficient to use	Efficiency
H7	Provide appropriate error/warning message	Alert
H8	Time required to response the attacks	Action
H9	Availability of wizard help option in IDS	Assistance
H10	Provide customization to represent result information	Output Customization

These proposed heuristics are designed on the bases of the problems discussed in literature review to serve IDS usability evaluations. In order to make it efficient and fast than conventional heuristics evalution methods, we embedded our proposed heuristics instructions in a partially automated system called CAII (Cognitive Analysis of IDS Interfaces). This partially automated system helps to detect usability issues in IDS interface and provide guidelines to remove detected usability issues. Detail about CAII are discussed in the next section.

3.3 Cognitive Analysis of IDS Interfaces (CAII)

Usability evaluation is an important part of the user interface design process. However, usability evaluation can be expensive in terms of time and human resources. Therefore, automation is a promising way to solve time and human resources issues [25, 38]. We proposed Cognitive analysis of IDS interfaces (CAII) system that is partially automated system and makes the usability evaluation process and usablity error detection fasters and efficient. The concept of following automation in usability evaluation process is new and discussed in few literature [3, 52]. Figure 4 shows the interface of CAII system. It consists of two sections; first, is the uploading of IDS interface or its mockup interface and second, is the evaluation process. The evaluation process presents proposed heuristics as questions for the corresponding IDS interface or mockup. The user needs to answer the questions either in yes or no during the evaluation. Every heuristics and its related recommendations are presented and embedded in CAII system database.

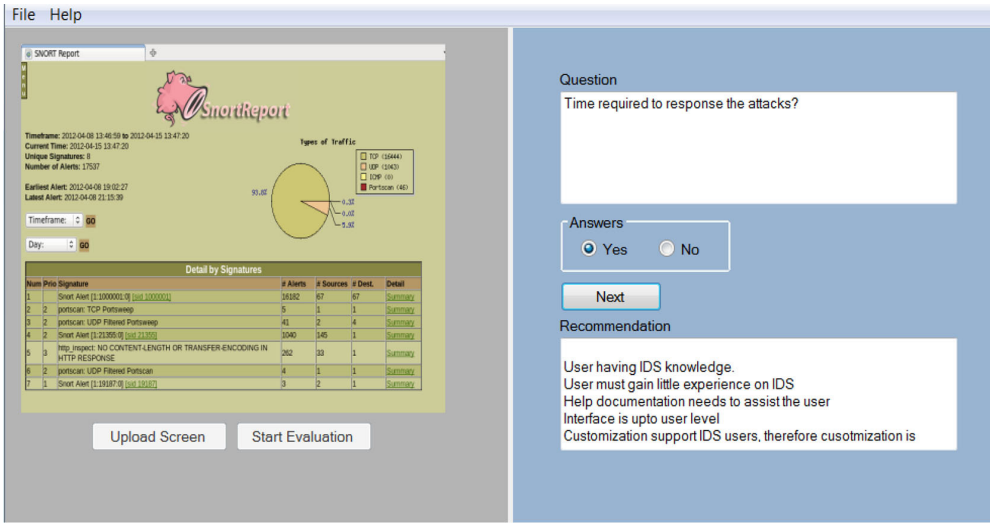

Fig. 4. CAII system performing usability testing of IDS interface

At the end of evaluation the log report interface of CAII system presents the result of our IDS interface as shown in Fig. 5.

3.4 CAII Facts and Rules

The CAII system evaluates the usability of IDS interface on the concept of inference. CAII system consist of Facts and Rules that are user defined and stored in the inference engine. In CAII user-defined Rules are proposed heuristic. These Rules helps to evaluate the user prototypes / interface of IDS system. The CASII system contains two phases.

a. Facts and Rules
b. Decision Tree

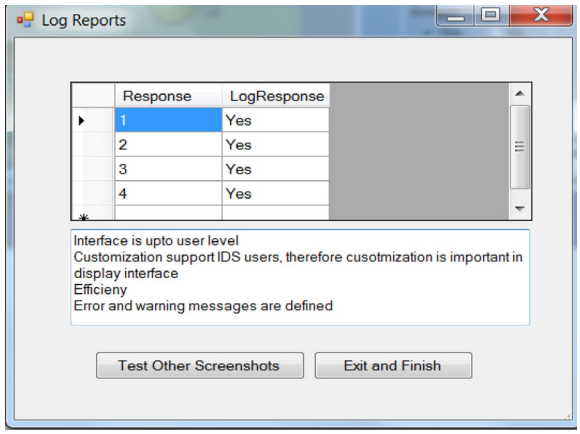

Fig. 5. CAII system presenting the final results and recommnadations

3.4.1 Facts and Rules

For CAII system, ten Rules are defined to achieve IDS usability:

Rule A: Exit

Symbol: R_A

Rule 1: User with networking knowledge

User must have the knowledge of networks before using IDS systems.

Symbol: R_1

Rule 2: Experience in IDS

User experience in IDS helpful to eliminate usability issues in IDS system.

Symbol: R_2

Rule 3: Provide help about the networking terminology in IDS

Help assistant is required for user to understand IDS terminology.

Symbol: R_3

Rule 4: Interface is easy to understand and provide relevant information

IDS interface easy to understand by user and provide relevant relation to users in customize way.

Symbol: R_4

Rule 5: Customisation of GUI of IDS Interface

Graphical user interface of IDS can customize on user request and with useful features.

Symbol: R_5

Rule 6: Efficient to use

Efficient in performing daily task on IDS system.

Symbol: R_6

Rule 7: Provide appropriate error/warning message

Provide quick warning alert when attacks occur.

Symbol: R_7

Rule 8: Time required to response to the attacks

Response to the attatcs in a short amount of time.

Symbol: R_8

Rule 9: Availability of wizard help option in IDS

Wizard asists the user to follow step by step instruction to complete certain task.

Symbol: R_9

Rule 10: Provide customisation to represent result information

The result of IDS system should in different forms like table, graphs and chats that helps user to under.

Symbol: R_{10}

Rule C: Recommendations

Symbol: R_C

3.4.2 Decision Tree of CAII

Figure 6 shows the decision tree of CAII system. In decision tree, if R_1 (Rule 1) fails that means it will move to R_C state i.e Recommendation. This evaluation process can be stopped by moving to R_A state i.e the exit, else next rule will be considered till last Rule.

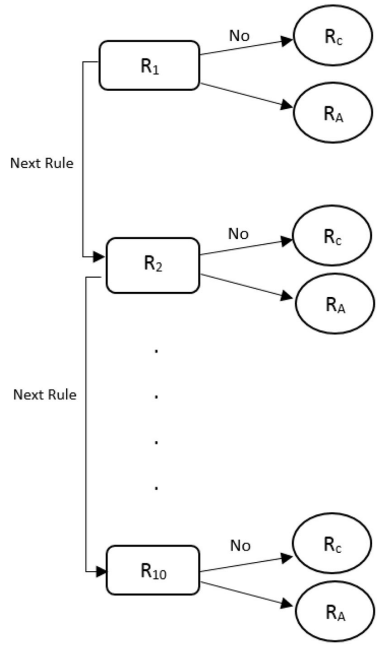

Fig. 6. Decision tree of CAII system

4. Conclusion

Intrusion detection systems are complex and provide many challenges for security practitioners. Prior IDS research has focused largely on improving the accuracy of these systems and on providing support to practitioners during the ongoing task of monitoring alerts and analyzing potential security incidents. One area that has received little attention in IDS is to improve the usability IDS, but the current heuristics are not defined for IDS system and can serve as a barrier to use.

In this paper, we have contributed to knowledge by presenting a review on usability evaluation techniques, factors in usability evaluations and usability problems. The paper contributed the categorization of usability problems in term of software engineering, network and software interface and comparison of usability evaluation techniques, which should fill the issues and gap in this area. Furthermore, proposed heuristics for users and IDS offers the basic guidelines to develop and improve IDS interfaces to combat the security infringements.

Through the systematic and rigours approach of evaluation of the various factors presented in this research, we also proposed to aid the usability of networks by proposing future action research. The cybersecurity field, in particular, would benefit with future research testing a new design heuristic for IDS. This can be conducted through the application of numerous datasets and analysis techniques in real case scenarios, for example, by focusing on longitudinal analysis capturing heuristics user's behaviours.

Other sectors can also benefit from heuristic evaluations and improve IDS interfaces because a. this approach identify barriers with components or sections of an interface factor or component that negatively impacts IDS usability and b. It can aid identify usability issues early in the IDS design or development lifecycle.

References

[1] Allen M., Currie L. M., Bakken S., Patel V. L. & Cimino J. J. Heuristic evaluation of paper-based Web pages: A simplified inspection usability methodology. *Journal of Biomedical Informatics*, 2006, 39(4), 412–423. doi:10.1016/j.jbi.2005.10.004

[2] Almarashdeh I. A., Sahari N., Azan N. & Zin M. *Heuristic Evaluation of Distance Learning Management System Interface*, 2011, July.

[3] Butt S. M., Fatimah W. & Ahmad W. Analysis and evaluation of cognitive behavior in Software Interfaces using an Expert System. *Engineering*, 2012, 5(1), 146–154.

[4] Cannady J., & Harrell J. A comparative analysis of current intrusion detection technologies. Proceedings of the Fourth Technology for … 2000. Retrieved from ftp://www.polinux.upv.es/viejo/pub/doc/ids/A_Comparative_Analysis_of_Current_Intrusion_Detection_Technologies.pdf

[5] Carvajal L., Moreno A. M., Sánchez-Segura M. I. & Seffah A. Usability through software design. *IEEE Transactions on Software Engineering*, 2013, 39, 1582–1596. doi:10.1109/TSE.2013.29

[6] Chebrolu S., Abraham A. & Thomas J. P. Feature deduction and ensemble design of intrusion detection systems. *Computers and Security*, 2005, 24, 295–307. doi:10.1016/j.cose.2004.09.008

[7] Cranor L. F. & Garfinkel S. Security and Usablity: Designing secure systems that people can use. *Theory in practice*, 2005, 714.

[8] Dillon A. Beyond usability: process, outcome and affect in human-computer interactions. *Canadian Journal of Library and Information Science*, 2002, 26, 57–69. Retrieved from http://arizona.openrepository.com/arizona/handle/10150/106391

[9] Fernandez A., Abrahao S. & Insfran E. A systematic review on the effectiveness of web usability evaluation methods. *Evaluation Assessment in Software Engineering EASE2012 16th International Conference,* 2012, 52–56. doi:10.1049/ic.2012.0007

[10] Fernandez A., Abrahão S. & Insfran E. Empirical validation of a usability inspection method for model-driven Web development. *The Journal of Systems & Software*, 2013, 86(1), 161–186. doi:10.1016/j.jss.2012.07.043

[11] Folmer E., Van Welie M. & Bosch J. Bridging patterns: An approach to bridge gaps between SE and HCI. *Information and Software Technology*, 2006, 48, 69–89. doi:10.1016/j.infsof.2005.02.005

[12] Furnell S. Making security usable: Are things improving? *Elsevier Ltd*., 2007, 26, 434–443. doi:10.1016/j.cose.2007.06.003

[13] Goodall J. R., Lutters W. G. & Komlodi A. *The Work of Intrusion Detection: Rethinking the Role of Security Analysts*, 2004, August, 1421–1427.

[14] Goodall J. R., Ozok A. A., Lutters W. G., Rheingans P. & Komlodi A. A user-centered approach to visualizing network traffic for intrusion detection. *Proceedings of ACM CHI 2005 Conference on Human Factors in Computing Systems,* 2005, 2, 1403–1406. doi:10.1145/1056808.1056927

[15] Grabenbauer L. A., Fruhling A. L. & Windle J. R. *Towards a Cardiology / EHR Interaction Workflow Usability Evaluation Method*, 2014. doi:10.1109/HICSS.2014.331

[16] Guenther J., Volk F. & Shaneck M. Proposing a multi-touch interface for intrusion detection environments. *Proceedings of the Seventh …*, 2010, 13–21. Retrieved from http://dl.acm.org/citation.cfm?id=1850797

[17] Hafiz M. D., Abdullah A. H., Ithnin N. & Mammi H. K. *Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique*, 2008. doi:10.1109/AMS.2008.136

[18] Hanumansetty R. G. Model based approach for context aware and adaptive user interface generation. *Scenario,* 2004. Retrieved from http://scholar.lib.vt.edu/theses/available/etd-08242004–120131/

[19] Heeren C. & Furnell S. Improving the Usability of Security Features within Tools and Applications. … *Computing, Networks and Security*, 2011, 8, 137–145. Retrieved from http://books.google.com/books?hl=en&lr=&id=3NzOAwAAQBAJ&oi=fnd&pg=PA137&dq=Improving+the+Usability+of+Security+Features+within+Tools+and+Applications&ots=N3yVo6ezKh&sig=KQMKlIzMJzZ3ro1I6dJiSyw_FP4

[20] Holzinger A. Usability engineering methods for software developers. *Communications of the ACM*, 2005, 48, 71–74. doi:10.1145/1039539.1039541

[21] Holzinger A. Usability engineering methods for software developers. *Communications of the ACM*, 2005. doi:10.1145/1039539.1039541

[22] Huart J., Kolski C. & Sagar M. Evaluation of multimedia applications using inspection methods: The Cognitive Walkthrough case. *Interacting with Computers*, 2004, 16, 183–215. doi:10.1016/j.intcom.2003.12.005

[23] Hwang K., Cai M., Chen Y. & Qin M. Hybrid intrusion detection with weighted signature generation over anomalous internet episodes. *IEEE Transactions on Dependable and Secure Computing*, 2007, 4, 41–55. doi:10.1109/TDSC.2007.9

[24] International Organization for Standardization, & International Electrotechnical Commission. ISO/IEC9126–1. *Software engineering*, 2001. Product quality. Part 1: Quality model. Software Process: Improvement and Practice (Vol. 2, pp. 1–25). doi:10.1002/(SICI)1099–1670(199603)2:1<35:: AID-SPIP29>3.0.CO;2–3

[25] Ivory M. Y. & Hearst M. A. *The State of the Art in Automating Usability Evaluation of User Interfaces,* 2001, 33(4), 470–516.

[26] Jaferian P. & Hawkey K. Heuristics for evaluating IT security management tools. Human–Computer …, 2014. Retrieved from http://www.tandfonline.com/doi/abs/10.1080/07370024.2013.819198

[27] Jaferian P., Hawkey K. & Beznosov K. *Challenges in evaluating complex IT security management systems*, 2010.

[28] Kennard R, & Leane, J. Towards a general purpose architecture for UI generation. *Journal of Systems and Software*, 2010, 83, 1896–1906. doi:10.1016/j.jss.2010.05.079

[29] Khalid H. M. Embracing diversity in user needs for affective design. *Applied Ergonomics*, 2006, 37, 409–418. doi:10.1016/j.apergo.2006.04.005

[30] Komlodi A., Goodall J. & Lutters W. An information visualization framework for intrusion detection. *CHI'04 Extended Abstracts on …*, 2004, 1743–1746. doi:10.1145/985921.1062935

[31] Kraemer S., Carayon P. & Clem J. Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, 2009, 28(7), 509–520. doi:10.1016/j.cose.2009.04.006

[32] Macik M., Cerny T. & Slavik P. Context-sensitive, cross-platform user interface generation. *Journal on Multimodal User Interfaces*, 2014, 8(2), 217–229. doi:10.1007/s12193-013-0141-0

[33] Mahatody T., Sagar M. & Kolski C. State of the Art on the Cognitive Walkthrough Method, Its Variants and Evolutions. *International Journal of Human-Computer Interaction*, 2010. doi:10.1080/10447311003781409

[34] Memmel T., Box D. & Reiterer H. *Agile Human-Centered Software Engineering*, 2007.

[35] Memmel T., Gundelsweiler F. & Reiterer H. *CRUISER: A Cross-Discipline User Interface and Software Engineering Lifecycle*, 2007, 174–183.

[36] Moustafa F. & Furnell S. M. *Assessing the Usability of Security Features in Tools and Applications*, 1975, 98–106.

[37] Nielsen J. & Molich R. Heuristic evaluation of user interfaces. *Proceedings of the SIGCHI conference on Human factors in computing systems Empowering people – CHI '90*, 1990, 249–256. doi:10.1145/97243.97281

[38] Norman K. L. & Panizzi E. Levels of automation and user participation in usability testing. *Interacting with Computers*, 2006, 18, 246–264. doi:10.1016/j.intcom.2005.06.002

[39] Nurmuliani N., Zowghi D. & Williams S. P. Using card sorting technique to classify requirements change. *Proceedings. 12th IEEE International Requirements Engineering Conference*, 2004. doi:10.1109/ICRE.2004.1335681

[40] Patil T., Bhutkar G. & Tarapore N. Usability Evaluation Using Specialized Heuristics with, 2012, 317–328.

[41] Paz F., Villanueva D., Rusu C., Roncagliolo S., Pow-sang J. A. *Experimental Evaluation of Usability Heuristics*, 2013, 119–126. doi:10.1109/ITNG.2013.23

[42] Pyla P. & Pérez-Quiñones M. *Towards a model-based framework for integrating usability and software engineering life cycles*, 2004. arXiv Preprint Cs/ … Retrieved from http://arxiv.org/abs/cs/0402036

[43] Ramli R. B. M. & Jaafar A. B. e-RUE: A cheap possible solution for usability evaluation. *Proceedings – International Symposium on Information Technology*, 2008, ITSim, 4.

[44] Sauer J., Seibel K. & Rüttinger B. The influence of user expertise and prototype fidelity in usability tests. *Applied Ergonomics*, 2010, 41, 130–140. doi:10.1016/j.apergo.2009.06.003

[45] Sauer J. & Sonderegger A. The influence of prototype fidelity and aesthetics of design in usability tests: Effects on user behaviour, subjective evaluation and emotion. *Applied Ergonomics*, 2009, 40(4), 670–677. doi:10.1016/j.apergo.2008.06.006

[46] Sefelin R., Tscheligi M. & Giller V. Paper prototyping – what is it good for?: a comparison of paper- and computer-based low-fidelity prototyping. *CHI '03 Extended Abstracts on Human Factors in Computing Systems*, 2003, 778–779. doi:10.1145/765891.765986

[47] Seffah A., Donyaee M., Kline R. B. & Padda H. K. Usability measurement and metrics: A consolidated model. *Software Quality Journal*, 2006, 14, 159–178. doi:10.1007/s11219-006-7600-8

[48] Seffah A. & Metzker E. The obstacles and myths of usability and software engineering. *Communications of the ACM*, 2004. doi:10.1145/1035134.1035136

[49] Seibel K. & Ru B. The influence of user expertise and prototype fidelity in usability tests, 2010, 41, 130–140. doi:10.1016/j.apergo.2009.06.003

[50] Silva T. S. da, Martin A., Maurer F. & Silveira M. User-Centered Design and Agile Methods: A Systematic Review. *AGILE Conference*, 2011, 77–86. doi:10.1109/AGILE.2011.24

[51] Sivaji A., Abdullah M. R., Downe A. G., Fatimah W. & Ahmad W. *Hybrid Usability Methodology: Integrating Heuristic Evaluation with Laboratory Testing across the Software Development Lifecycle*, 2013. doi:10.1109/ITNG.2013.60

[52] Sivaji A., Soo S. & Abdullah M. R. *Automated Heuristic Evaluation System*, 2011. doi:10.1109/CICSyN.2011.23

[53] Sonderegger A. & Sauer J. The influence of design aesthetics in usability testing: Effects on user performance and perceived usability. *Applied Ergonomics*, 2010, 41(3), 403–410. doi:10.1016/j.apergo.2009.09.002

[54] Soomro S., Fatimah W., Ahmad W. F. W., Sulaiman S., Wan Ahmad W. F. & Wan Ahmed W. F. Evaluation of Mobile Games Using Playability Heuristics. *Information System International Conference,* 2013 (ISICO2013), 2, 2–7. doi:10.1109/ICCISci.2012.6297177

[55] Sutcliffe A. Assessing the reliability of heuristic evaluation for Web site attractiveness and usability. *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, 2002. doi:10.1109/HICSS.2002.994098

[56] Thompson R. S., Rantanen E. M., Yurcik W. & Bailey B. P. Command line or pretty lines?: comparing textual and visual interfaces for intrusion detection. *Proceedings of ACM CHI 2007 Conference on Human Factors in Computing Systems*, 2007, 1, 1205–1214. Retrieved from http://doi.acm.org/10.1145/1240624.1240807

[57] Tran V., Kolp M., Vanderdonckt J., Wautelet Y. & Faulkner S. Agent-based user interface generation from combined task, context and domain models. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2010, 5963 LNCS, 146–161. doi:10.1007/978–3–642–11797–8_12

[58] Tuch A. N., Roth S. P., Hornbæk K., Opwis K. & Bargas-avila J. A. Computers in Human Behavior Is beautiful really usable? Toward understanding the relation between usability, aesthetics, and affect in HCI. *Computers in Human Behavior*, 2012, 28(5), 1596–1607. doi:10.1016/j.chb.2012.03.024

[59] Van Den Bergh J. & Coninx K. Towards Modeling Context-Sensitive Interactive Applications: the Context-Sensitive User Interface Profile (CUP). *Proceedings of the 2005 ACM symposium on Software visualization*, 2005, 87–94. doi:10.1145/1056018.1056030

[60] Wang Baldonado M. Q., Woodruff A. & Kuchinsky A. Guidelines for using multiple views in information visualization. *Proceedings of the Working Conference on Advanced Visual Interfaces – AVI '00*, 2000, 110–119. doi:10.1145/345513.345271

[61] Werlinger R., Hawkey K., Muldner K. & Jaferian P. *The Challenges of Using an Intrusion Detection System: Is It Worth the Effort*?, 2006, 1.

[62] Yee K. P. Aligning security and usability. *IEEE Security and Privacy*, 2004. doi:10.1109/MSP.2004.64

[63] Yin X., Yurcik W., Treaster M., Li Y. & Lakkaraju K. VisFlowConnect: netflow visualizations of link relationships for security situational awareness. *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, 2004, 26–34. doi:10.1145/1029208.1029214

[64] Zhou A. T. Improving intrusion detection systems, 2004, 1641–1644.