Volume 4, Issue 1
February 2015

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

A Literature Review of and Proposed Methodology for Gaining IDS Usability

[1]Saad Masood Butt, [2]Azura Onn, [3]Mazlina Abdul Majid, [4]Suziyanti Marjudi
[1]Department of Software Engineering, Bahria University Islamabad, Pakistan
[2]Department of Management and Human Resource, Universiti Tenaga Nasional, Malaysia
[3]Faculty of Computer Systems & Software Engineering, University Malaysia Pahang
[3]Faculty of Computer Science and Information Technology, Universiti Selangor (UNISEL), Malaysia
E-mail: [1]saadmasoodbutt668@yahoo.com, [2]azura@uniten.edu.my, [3]mazlina@ump.edu.my, [4] suziyanti@unisel.edu.my

ABSTRACT

Network security guarantees the protection of valuable and available network assets from viruses, key loggers, hackers and unauthorized access. Intrusion Detection System (IDS) are considered as one of the important network tool in managing the network security. It is found that network practitioners find difficult to use current IDS. The important factor that impacts the effectiveness of IDS is the interface that helps the users to evaluate the software usability. Even security software's like IDS are working efficiently but user found it difficult to use and understand. As a result user has difficulties in using and judging the quality of the output. Therefore, usability evaluation is important to help users in efficient interaction and enhance usage of IDS. In most of the situation the usability evaluation is done by the usability engineers. In small or large scaled companies software developers are forced to learn different paradigm of usability. This is not easier than training the usability engineers on how to develop software. As a remedy Cognitive Analysis of Software Interface (CASI) system has been designer for software engineer. Moreover this system help software engineer to evaluate the IDS based on user perception and evaluation views. To evaluate new heuristics for IDS are proposed in this paper also a broad literature on software interfaces and evaluating methodologies are discussed. Further challenges associated with interfaces and new methods to evaluate usability of software are reviewed.

Keywords: *Intrusion detection system, usable security, heuristics evaluation, usability, cognitive analysis*

1. INTRODUCTION

Over the past few years, internet is evolved and people have been facing challenges of network security. This is a big issue for many organizations who want to protect their useful and confidential data from threats inside or outside the organization. Research shows that human and organization factors also impact on network security [1]. Network practitioners faced challenges to manage security and they utilize special tools like firewall, antivirus, nmap and IDS. Among all these tools, IDS plays important role to identify the malicious activities on time and support response for real time attack. But often IDS users find it difficult to use IDS and unable to take advantage of all its functionalities.

In order to improve the effectiveness of IDS these challenges must be addressed. One way is to develop effective solution that can help network practitioners in managing security. The crucial factor that impacts a lot in managing the security is the usability. Software developers accepted that interface of software plays a vital role in the software success. This success can be measured in term of software usability. Usability itself means how easy the system to understand and efficient to use. Usability is an important concept in HCI discipline in light of the fact that it communicates the relationship between end users and machine applications through interface [2]. One way to address the challenges in IDS is to develop interactive interface to aid network practitioners in managing security efficiently. The rest of the paper is divided into few sections. Section 1 is the introduction; section 2 reviews some previous work on usability, IDS and current heuristics. Section 3 specifics the methodology and proposed heuristics. Section 4 draw conclusions and shows the direction for future work.

2. USABILITY

Launched in 2006, twitter has altered the manner in which the business industry and individuals communicate with each other. One of the important aspect of software quality is the Usability and ISO 9241 define usability as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" [4]. Another definition by ISO 9126-1 "the capability of the software product to be understood, learned and liked by the user, when it is used under specified conditions" [5]. Both definition focused on the usability and considered it as an important aspect of software that let user to perform the task in easy way. Whereas Nielson define usability in five attributes learnability, efficiency, memorability, error avoidance and subjective satisfaction.

Usability ensures the final product developed is easy to under, easy to use and easy to remember from the user perspective. This concludes in the goal of goals of efficiency, effectiveness, safety, utility, learnability and memorability [7]. The focus of HCI has improved over time [8], the task oriented usability paradigm has been expended to aesthetic and hedonic user experience (UX) paradigm [9] [10].

Volume 4, Issue 1
February 2015

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

In usability there are several methods to evaluate the usability of software. These methods are divided into two groups: usability inspection and usability testing methods. In usability inspection, usability problems are identified by usability practitioners where as in usability testing methods, usability problems are found by user's observations how they are using the system how they interact with the software interface [11].

1. HEURISTIC EVALUATION

There are number of methods to conduct usability evaluation like cognitive walkthrough, formal usability inspection, heuristic evaluation or pluralistic walkthrough [13]. To conduct the usability of IDS, heuristic evaluation was selected and heuristic are specially designed for IDS. Heuristic evaluation involves small number of usability practitioners inspecting the system and evaluates the system against the usability principles [11]. Albert [12] highlights the advantages of heuristic evaluation as it is the cheaper and easier way of doing evaluation. With the help of special heuristic, user can evaluate the usability of IDS and detect and solve usability issues in easier way.

But evaluation can be costly in term of time, resources and human effort therefore semi-automated or fully automated is the promising method to augment the existing evaluation approaches in addition research shows the importance of special system to support usability evaluation [14]. In term of software projects it is important to use such automated or semi-automated evaluation system where it is crucial to ensure the effectiveness when project have a tight timeline. To ensure the project success one way is to improve manual way of evaluation via automation or semi automation this will help the evaluators to follow manual processes and support in capturing more defects in shorter amount of time [15]. The result of the evaluation are summarized and presented to the design team along with improvements.

2. INTRUSION DETECTION SYSTEM

Intrusion Detection System is a network security tool for network /system to monitor the network from improper access. We cope with two main problems in IDS one is related to state of 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. Various techniques and algorithm are designed for improve IDS to detect improper access in the network [16]. However experience shows working software still fails when the user interface is not up to the user level. 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 else attacks can have serious consequence [17].

Traditionally, the IDS users are network administrators, but the advantages of using IDS become so popular that it expand it users from network administers to a computer user who want to monitors its network traffic going through one's network or pc. We classify the users as network programmers, security professionals and lan administrators. Network programmer's job is to design network according to the traffic. Security professionals have wide knowledge of technologies that includes anti-virus, strong authentication, intrusion detection and biometrics whereas lan administrators job is to provide management and support to lan in a company [18].

3. COGNATIVE ANALYSIS OF SOFTWARE INTERFACES

Research [15] [20] shows that companies are now developing such software that can perform usability evaluation itself or need little human effort. This is because hiring usability experts is not affordable by many companies. Why it called "Cognitive Analysis of Software Interface (CASI)" because it works and analyze and evaluate according to user perception like how user feel for the interface, how user interact with the interface, how user want the interface should be.
CASI is system that helps software engineers or IT users to evaluate the interface without hiring usability experts. CASI not only find usability issues in the interface of system but also give recommendations to improve the interface and make it interactive for the user. In order to run CASI to find and remove usability issues in IDS, usability experts and IDS users need to work together to design heuristics for IDS. CASI consist of two parts one is IDS interface and other is IDS heuristics as show in figure 1.

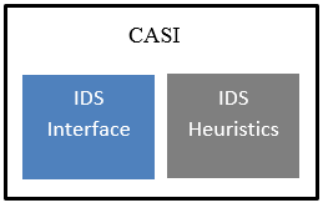

Figure 1: Cognitive Analysis of Software Interfaces

Software interface plays a vital role in the evaluation of software usability. In CASI we test the usability of every IDS single interface and find the usability issues. This test is done by running proposed IDS heuristics on IDS interface. Proposed Heuristics embed in CASI and run on every single IDS interface to find usability issues along with recommendations. The internal structure of CASI is show in figure 2, it comprises of three level. In first level the interface of IDS are selected and arranged as per user requirement. Those IDS which are in the process of developing can also be used to increase their usability at development stage. In the second level pick one IDS interface and run the proposed heuristics. In the third level the IDS users will interact with interface to discover usability issues faced by users while interacting with IDS.

Volume 4, Issue 1
February 2015

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

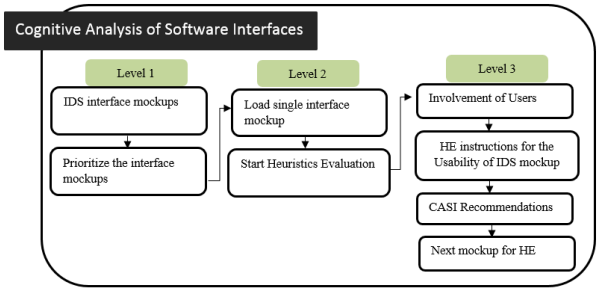

Figure 2: Structure of Cognitive Analysis of Software Interfaces

6. METHODOLOGY

Previous work clearly shows that the interactive usable security tool helps to detect malicious actives in the network. In addition it also propose new heuristics for usability evaluation IDS. In this paper, we use a questionnaire survey to derive some user characteristics, user learning behavior and problems faced while using IDS. Based on the survey we propose new heuristic that will embed into CASI to evaluate the IDS interface and it will evaluate empirically. The difference between evaluation of IDS and software of other domains can be derived from the type of users and the tasks users need to undertake [3]. Generic heuristics [19] can be applied to any software because they have well defined task which user need to perform whereas IDS users rarely perform well defined task and spend considerable amount of time to select a course of action. Therefore our research questions are:

1. What are the expectations of network practitioners from IDS?
2. What are the problems of network practitioners faced while using IDS?
3. How to improve the Usability of IDS interface?

To answer these questions we design our methodology that includes the following steps:

1. Literary study
2. Selection and study of IDS
3. Selection of IDS practitioners
4. Surveys Questionnaire
5. Designing of heuristics for IDS
6. Lab based testing
7. Experts based testing

Literary study

The purpose of the literary studies is to gain the information about IDS and usability to find the answers of research questions. We will do literary studies on IDS, usability for identifying the usability issues in IDS and how to improve the usability of IDS also need to identify what is the current state of art and current state of practices is used in improving IDS usability.

Selection and study of IDS

To improve the usability of IDS, we need to select and study the most commonly used IDS. We select Snort, KF Sensor and Easy Spy. During the study some important aspects of IDS are noted down like types of users, usability problems and interaction of users with IDS.

Selection of IDS practitioners

To get the real user involvement in designing the heuristics for IDS, it is important to know who the actual users of IDS are. This will help to find usability issues in the IDS and how to improve the IDS usability according to the user perceptions.

Survey Questionnaire

Before going into the details of IDS usability issues, a survey questionnaire is designed to gain more insight on how usability and IDS are dealt with in practice. This method is selected because we are dealing with different users having different background, experience, knowledge and expertise. This will help to obtain what is important to these users while using IDS.

Designing of heuristics for IDS

Based on the survey questionnaire results we discover what problems are faced by users while using IDS. This will help to propose the new heuristics of IDS. We classify the heuristics into different categories (1) Installation heuristics (2) Interface heuristics (3) Output heuristics (4) Customization heuristics (5) Help heuristics

Lab based testing

Once the heuristics are designed it's time to test the proposed heuristics in the lab. The best thing about CASI is that you can apply these proposed heuristics at any phase of IDS like Output level or Customization level. Focus of this testing to check how efficient CASI that helps to detect and remove usability issues then traditional heuristics evaluation.

Experts based testing

After lab testing, the proposed heuristics now ready for empirically testing where the network practitioners can participate in this IDS interface evaluation testing and get the results of the testing. At same time, based on that test results a new IDS interface mockup is designed and again test for its evaluation. If the network practitioners find the interface attractive and easily to understand it will replace the previous interface of IDS.

7. EVALUATION OF INTRUSION DETECTION SYSTEM

The evaluation of IDS is carried out empirically by comparing the performance of CASI with that of Nielsen usability heuristics [21]. This can be done by using both CASI and Nielson Usability heuristics on IDS to find how many number of usability defects are detected and remove from the IDS interface. Reason why Nielsen usability heuristics is selected because it is most widely used heuristics practically. The aim of comparing the CASI with Nielsen usability heuristics is to gain the understanding how CASI would work compared to Nielsen usability heuristics. There are few attributes that need to be noted during the comparison of CASI and Nielsen usability heuristics i.e. no of usability defects discovered, time, reliability, efficiency, accuracy.

8. 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 presented 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.

REFERENCES

[1] Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & security, 28(7), 509-520.

[2] Chou, J. R., & Hsiao, S. W. (2007). A usability study on human–computer interface for middle-aged learners. Computers in Human Behavior, 23(4), 2040-2063.

[3] Zhou, A. T., Blustein, J., & Zincir-Heywood, N. (2004, May). Improving intrusion detection systems through heuristic evaluation. In Electrical and Computer Engineering, 2004. Canadian Conference on (Vol. 3, pp. 1641-1644). IEEE.

[4] ISO, "9241-11. Ergonomic requirements for office work with visual display terminals (VDT's)," Part 11: Guidance on Usability, 1998.

[5] ISO, "9126-1: Software Engineering - Product Quality," Part 1: Quality Model, 2000.

[6] J. Nielsen, Usability engineering, 1 edition ed., San Diego, CA 92101, United States: Academic Press, 1993.

[7] ROGERS, Y., SHARP, H., and PREECE, P., 2012. Interaction design: Beyond human-computer interaction. John Wiley & Sons, New York.

[8] POPPE, R., RIENKS, R., and VAN DIJK, B., 2007. Evaluating the Future of HCI: Challenges for the Evaluation of Emerging Applications for Human Computing LNAI 4451, 234-250.

[9] HASSENZAHL, M. and TRACTINSKY, N., 2006. User experience – a research agenda. Behavior & Information Technology 25(2), 91-97.

[10] BOTHA, A., HERSELMAN, M., and VAN GREUNEN, D.D., 2010. Mobile user experience in a mlearning environment. In SAICSIT '10 Proceedings of the 2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists ACM Warmbaths, South Africa, 29-38.

[11] ARDITO, C., LANZILOTTI, R., BUONO, P., and PICCINNO, A., 2006. A Tool to Support Usability Inspection. AVI archive. In Proceedings of the working conference on Advanced visual interfaces table of contents, Venezia, Italy, 278 – 281.

[12] TULLIS, T. and ALBERT, W., 2008. Measuring the User Experience: Collecting, Analyzing, and Presenting Usability Metrics. Morgan Kaufmann., Burlington, MA.

[13] Bhutkar, D.K.G., Karmarkar, S.: Usability Heuristics and Qualitative Indicators for the Usability Evaluation of Touch Screen Ventilator Systems. In: Katre, D., Orngreen, R.,Yammiyavar, P., Clemmensen, T. (eds.) HWID 2009. IFIP AICT, vol. 136, pp. 83–97. Springer, Heidelberg (2010).

[14] Ivory, M. Y., & Hearst, M. A. (2001). The state of the art in automating usability evaluation of user interfaces. ACM Computing Surveys (CSUR), 33(4), 470-516.

[15] Sivaji, A., Soo, S. T., & Abdullah, M. R. (2011, July). Enhancing the effectiveness of usability evaluation by automated heuristic evaluation system. In Proceedings of the 2011 Third International Conference on Computational Intelligence, Communication Systems and Networks (pp. 48-53). IEEE Computer Society.

[16] S. D. Amstrong, et al. Usability testing. In S. G. Charlton & T. O'Brien, (eds), Handbook of Hurnan Factors Testing and Evaluation, Ch. 18, pp. 403-432. Lawrence Erlbaum, (2e), 2002.

[17] A. Dillon. Beyond usability: Process, outcome and affect in human computer interactions. Canadian J. oflnfo. Sci., 24(1):57-69,2001.

[18] Patil, T., Bhutkar, G., & Tarapore, N. (2012). Usability Evaluation Using Specialized Heuristics with Qualitative Indicators for Intrusion Detection System. In Advances in Computing and Information Technology (pp. 317-328). Springer Berlin Heidelberg.

[19] Paz, F., Villanueva, D., Rusu, C., Roncagliolo, S., & Pow-Sang, J. A. (2013, April). Experimental Evaluation of Usability Heuristics. In Information Technology: New Generations (ITNG), 2013 Tenth International Conference on (pp. 119-126). IEEE.

[20] Fernandez, A., Abrahão, S., & Insfran, E. (2013). Empirical validation of a usability inspection method

for model-driven Web development. Journal of Systems and Software, 86(1), 161-186.

[21] Johannessen, G. H. J., & Hornbæk, K. (2014). Must evaluation methods be about usability? Devising and assessing the utility inspection method.Behaviour & Information Technology, 33(2), 195-206.

AUTHOR PROFILES

Saad Masood Butt. Received his MS degree in Software Engineering from Bahria University Islamabad, in 2010. Currently he is a research student in a Malaysian University.