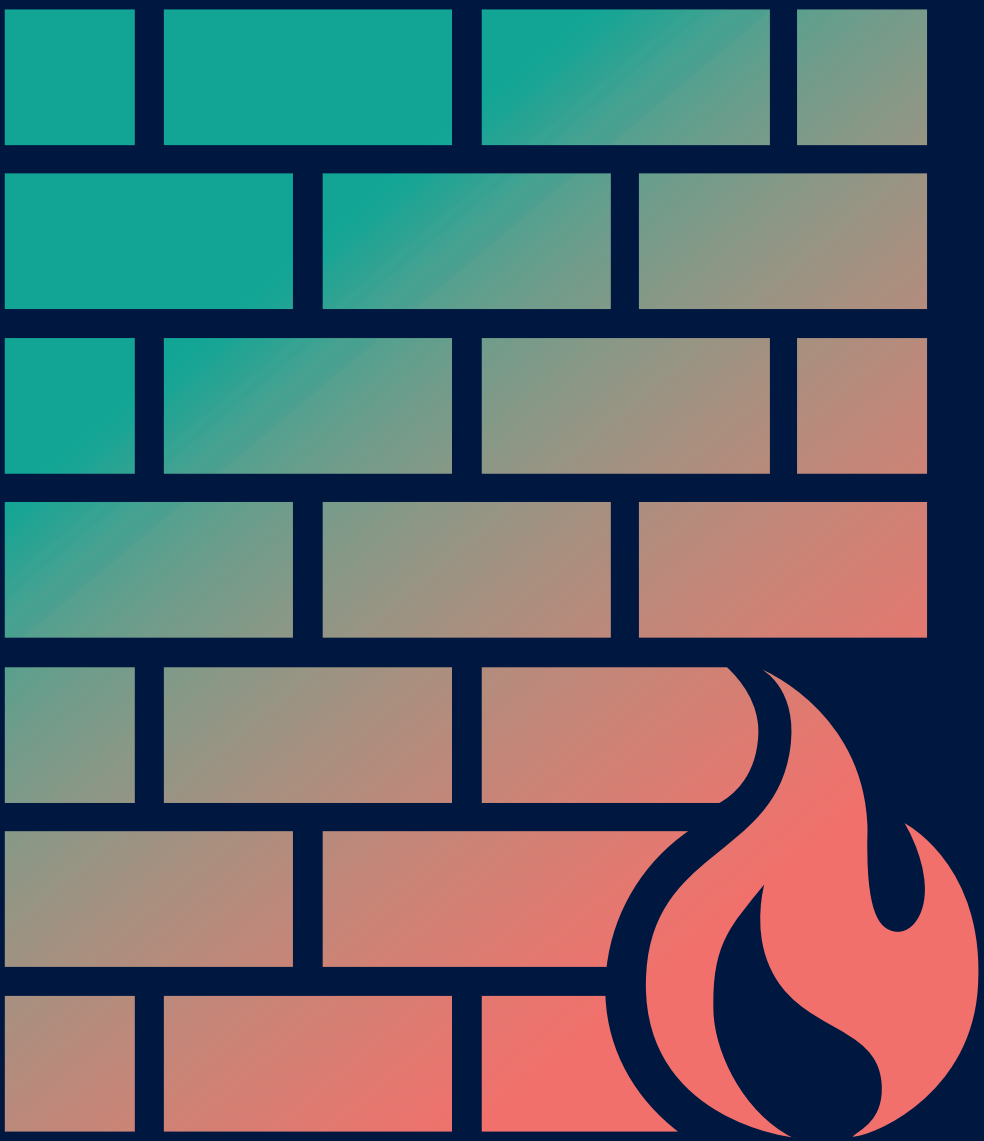
ARTEM VORONKOV



USABILITY OF FIREWALL CONFIGURATION

MAKING THE LIFE OF SYSTEM ADMINISTRATORS EASIER

Usability of Firewall Configuration

Making the Life of System Administrators Easier

Artem Voronkov

Faculty of Health, Science and Technology

Computer Science

DOCTORAL THESIS | Karlstad University Studies | 2020:15

Usability of Firewall Configuration

Making the Life of System Administrators Easier

Artem Voronkov

DOCTORAL THESIS | Karlstad University Studies | 2020:15

Usability of Firewall Configuration - Making the Life of System Administrators Easier

Artem Voronkov

DOCTORAL THESIS

Karlstad University Studies | 2020:15

urn:nbn:se:kau:diva-77106

ISSN 1403-8099

ISBN 978-91-7867-098-7 (print)

ISBN 978-91-7867-108-3 (pdf)

Distribution:
Karlstad University
Faculty of Health, Science and Technology
Department of Mathematics and Computer Science
SE-651 88 Karlstad, Sweden
+46 54 700 10 00

Print: Universitetstryckeriet, Karlstad 2020

WWW.KAU.SE

Usability of Firewall Configuration: Making the Life of System Administrators Easier

Artem Voronkov
Department of Mathematics and Computer Science
Karlstad University

Abstract

Most companies have access to the Internet and their corporate networks connected to it. Many threats to computer systems, e.g. worms, trojans, and denial-of-service attacks, can be encountered online and they may entail, for example, confidential data theft, service disruption and financial losses. Every organization, regardless of its size, type of activity or infrastructure, requires network security solutions in place in order to protect it from the ever-increasing number of cyber threats. Firewalls are an important component of network security that protect networks by regulating incoming and outgoing traffic.

Simply having a firewall does not guarantee any protection against Internet threats, unless it is properly configured. However, setting up firewalls correctly is a challenging task, which becomes more difficult with the growth of the network's size. Firewall configuration files consist of rule sets that might be hard to understand even for professionals that deal with them regularly. The main reason for this is that most firewall rule sets have a certain structure: the higher the position of a rule in the rule set, the higher priority it has. Challenging problems arise when a new rule is added to the set and a proper position for it needs to be found, or when existing rules are removed due to a security policy change. This brings us to the usability problem associated with the configuration of firewalls.

The overall aim of this thesis is to help system administrators better manage firewalls. First, we conduct a series of semi-structured interviews with system administrators, in which we ask them about problems confronted when managing firewalls. After having ascertained that there are usability problems involved, we begin to address them. We compare two different firewall rule set representation approaches and identify that a preference for one or the other depends on the firewall expertise of the individual. We introduce and mathematically formalize a set of four usability metrics which are designed to evaluate the quality of firewall rule sets. Furthermore, we not only investigate which firewall interfaces are utilized and preferred by system administrators but also identify and classify the interfaces' strengths and limitations. Finally, we conduct a systematic literature review to gain an understanding of the state of the art in firewall usability. This review classifies the available solutions and identifies the open challenges that exist in the field.

Keywords: Network security, usable security, firewall configuration, firewall interfaces, usability metrics.

Acknowledgments

My journey started in the summer of 2014 when I made the decision to move to Sweden and pursue a doctoral degree at Karlstad University. After 5.5 years, this incredible and at the same time challenging journey has come to an end. I will never regret the time I have spent here. I would like to say special thanks to my dearly loved wife, Veronika, and my family for their constant overabundance of support, in spite of some of my sudden decisions (like moving to Karlstad) and my inspiration for pursuing an academic career. I am thankful to Susanne for her gracious hospitality upon my arrival in Karlstad and for her continual support.

I express my gratitude to my supervisor Stefan Lindskog for believing in me and for his support and feedback throughout my studies. I am also grateful to my co-supervisor Leonardo Martucci for all his ideas, suggestions and support. Thank you both for the opportunity to pursue my doctoral degree and making this thesis possible. You have helped me to gain valuable skills that have greatly added to my success.

Finally, I would like to thank all my colleagues at the Department of Mathematics and Computer Science for a remarkable working environment. I would especially like to thank the members of the PriSec group for their exceptional discussions, scientific and non-scientific alike. A big thank you goes to the innebandy squad for their numerous excellent games and regular strategy meetings.

The work in this thesis was carried out as a part of the High Quality Networked Services in a Mobile World (HITS) project, funded partly by the Knowledge Foundation of Sweden.

Karlstad University, March 4, 2020 Artem Voronkov

List of Appended Papers

This thesis is based on the work presented in the following papers:

I. Artem Voronkov, Stefan Lindskog, and Leonardo A. Martucci. Challenges in Managing Firewalls. The 20th Nordic Conference on Secure IT Systems (NordSec 2015), Stockholm, Sweden, October 19–21, 2015.

II. Artem Voronkov and Leonardo A. Martucci. Natural vs. Technical Language Preference and its Impact on Firewall Configuration. The 22nd International Conference on Human-Computer Interaction (HCII 2020), Copenhagen, Denmark, July 19–24, 2020 (to appear).

III. Artem Voronkov, Leonardo A. Martucci, and Stefan Lindskog. Measuring the Usability of Firewall Rule Sets. IEEE Access, Volume 8, Issue 1, Pages 27106–27121, February 2020.

IV. Artem Voronkov, Leonardo A. Martucci, and Stefan Lindskog. System Administrators Prefer Command Line Interfaces, Don't They? An Exploratory Study of Firewall Interfaces. The Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019), Santa Clara, CA, USA, August 11–13, 2019.

V. Artem Voronkov, Leonardo Horn Iwaya, Leonardo A. Martucci, and Stefan Lindskog. Systematic Literature Review on Usability of Firewall Configuration. ACM Computing Surveys (CSUR), Volume 50, Issue 6, Article No. 87, Pages 1–35, January 2018.

The papers have been subjected to editorial changes.

Comments on my Participation

Paper I The idea for this paper as well as the design of the experiment originated from a discussion with my supervisors Stefan Lindskog and Leonardo A. Martucci. I conducted the interviews, analyzed the obtained data and did the majority of the writing.

Paper II The initial idea for this work was suggested by my co-supervisor Leonardo A. Martucci and subsequently refined by me. As the main author, I designed the study, conducted it and analyzed the data. Leonardo A. Martucci helped me with the writing process. He also provided feedback at all stages of the work.

Paper III A discussion with my co-supervisor Leonardo A. Martucci led to the premise for this work. I made most of the user studies' design decisions. All of the user studies and the following analysis of the data were also performed by me. Stefan Lindskog and Leonardo A. Martucci gave their feedback throughout the entire process and assisted me in writing this paper.

Paper IV I am the main author who devised the idea for this paper. I made most of the user study design decisions and conducted the survey myself. The analysis of the data was conducted together with Leonardo A. Martucci. Both of my supervisors provided feedback throughout the entire process and assisted me in writing the paper.

Paper V This paper was written in collaboration with Leonardo Horn Iwaya, who came up with the initial conceptual framework and methodology. I, in turn, performed the practical component of the work and most of the writing. My co-authors helped me with verifying the results as well as revising the paper during the rebuttal.

Contents

Introductory Summary

1 Introduction

The developmental growth rate of the Internet today is staggering as its users make up more than 57% of the global population [20, 30]. There are, however, a multitude of threats to computer systems on the Internet and their number continues to grow [47]. Network security is the practice of preventing unauthorized people or programs from accessing networks and the devices connected to them. Thus, network security is an important aspect that must be taken into account. One means of network security is a firewall, which can be implemented via software, hardware or as a combination of both. A firewall's main task is to protect segments of the network or individual computers by controlling incoming and outgoing traffic. Firewalls accept or drop packages based on a set of predefined rules [13]. The level of protection provided by the firewall depends heavily on the quality of its configuration file. A report on firewall configuration files [54] showed that all 12 rule sets investigated in the study contained errors. This result was later confirmed by another study with 36 rule sets [55]. The latter study claimed that "firewalls are still poorly configured, a rule set's complexity is positively correlated with the number of errors." Errors in rule sets are often referred to as either misconfigurations or anomalies [2, 3, 28].

Firewalls are mostly managed by IT professionals who are often referred to as system/network administrators (we will from now on use the term "system administrators" throughout this thesis). System administrators typically use a multi-phased approach for firewall deployment [21]. The NIST guideline on firewalls and firewall policies suggests five phases for this process [41]: 1) Planning, 2) Configuration, 3) Implementation, 4) Initial deployment and 5) Management. In this thesis, we focus on the process of configuring a firewall, i.e. creating a rule set that correctly implements a higher level security policy and managing it.

In this thesis, we look at the process of working with firewalls from the system administrators' perspective. It is often believed that system administrators have unlimited technical knowledge, which allows them to overcome any software flaws. For this reason, system administration tools are rarely designed with usability in mind [7]. Firewalls are no exception: firewall configuration languages are mostly low-level and vendor-specific, and graphical user interfaces are often poorly designed. It is obvious that ignoring some of the usability aspects does not help the system administrators who continue to wallow in firewall misconfiguration problems. The main goal of this thesis is to identify gaps and issues that have not been adequately addressed in the literature, and, as a result, have been ignored by designers of firewall interfaces, and to subsequently settle them. We offer system administrators more usable firewall solutions and approaches to the configuration process that can facilitate their daily work.

The remainder of this introductory summary is organized as follows. Section 2 provides the required background information and discusses related work. The research questions addressed are outlined in Section 3. In Section 4

we describe the research methods used in the thesis. The main contributions of this work are given in Section 5. The summary of appended papers is presented in Section 6. Finally, in Section 7 we present concluding remarks and future work.

2 Background and Related Work

In the following subsections, we introduce important terms and concepts that are necessary to understand the research domain addressed in this thesis.

2.1 Human-Computer Interaction

Human-computer interaction (HCI) is a multidisciplinary field focusing on the studies of the interaction between humans and computers that emerged in the early 1980s [10]. The reason for the emergence of this field was that computers became more compact and affordable to others, and not only to experts in specialized environments. Also, the need to create an HCI that would be simple and efficient for less experienced users became increasingly urgent. From its origins, HCI has expanded rapidly and today it incorporates multiple disciplines, such as computer science, cognitive science and human-factors engineering. John M. Carroll, one of the founders of the field, wrote [10]:

> "... it no longer makes sense to regard HCI as a specialty of computer science; HCI has grown to be broader, larger and much more diverse than computer science itself."

The underlying concept of HCI is that users of a computer system should come first. Users should not have to change their way of using systems to fit them. To the contrary, users' needs and preferences should direct designers so that they can create systems that match those requirements.

2.2 Usability

Usability is one of the key concepts in HCI. The term *usability* can be defined in several ways. In ISO 9241-11 [29], it is defined 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."

Where effectiveness means how successfully goals are achieved, efficiency means how properly time is utilized and satisfaction means how eager a user is to use a system. Nielsen [34] introduces three additional usability aspects: learnability—how easy it is to become familiar with the system; memorability—how easy it is to remember details about the system after a period of non-use; safety—how many mistakes a user makes. Both definitions are closely related, and we use them throughout this thesis.

2.3 Firewalls

Firewalls are systems that filter incoming and outgoing network traffic. The decision taken by firewalls as to whether to allow or block network traffic follows a set of rules. A firewall rule consists of a set of conditions (e.g. on IP addresses, MAC addresses, protocols) and a decision that commonly is to accept or block traffic (other decisions such as logging events or further examination of a packet are also possible). A firewall inspects the packets that pass through it and makes a decision based on its rule set. For most firewalls, rules are applied in a certain order—from the beginning of the rule set until a rule is triggered. If no matching rule was found, the default rule (usually drop packet) is applied.

Rule sets are mostly dynamic, i.e. they change over time due to the fact that security policies, topologies, etc. change. Challenging problems arise when, for instance, a new rule needs to be added to the policy. When changing a rule or a set of rules, misconfigurations might occur and this will likely result in inappropriate system security. Misconfigurations can be categorized into five types [4]: 1) Shadowing—the first rule in the order matches all packets that the second rule does, and these rules take different actions; 2) Correlation—the first rule in the order processes some packets that could be processed by the second one, and the rules take different actions; 3) Generalization—the second rule in the order can process all packets that were handled by the first one, and the rules take different actions; 4) Redundancy—all packets can be processed without the rule, so its removal does not affect the security policy; and 5) Irrelevance—no packets can be processed by the rule.

2.4 Usable Security

Since 1975, when Saltzer and Schroeder [39] introduced *psychological acceptability* as one of the eight design principles of secure systems, usability and security started to align in an area that is called *usable security*. Although there is a norm for designing systems with both security and usability in mind, the reality is that this principle is not always adhered to. Some systems are designed to be extremely secure, while their usability leaves much to be desired. As stated by Sasse and Smith [40]:

> "Security mechanisms are often too time consuming for people to bother with, or so complex that even those willing to use them make mistakes."

Firewalls are a good example of security tools that are not designed with usability in mind. Nevertheless, most research studies on firewalls often focus on issues other than usability: filtering performance issues [23, 50], detection of anomalies [3, 28, 35], etc.

As previously mentioned, firewalls are mainly utilized by system administrators. One possible explanation of why usability aspects of firewalls have not been thoroughly studied is an overestimation of the knowledge and capabilities that system administrators possess [7]. Designers tend to ignore the needs of

system administrators and deem that they can overcome any problems that arise due to lack of usability. Another reason is that most of the work in usable security centers around user studies. Several studies have been published about usable security for ordinary end-users [53, 56]. However, developing a user study involving system administrators is notedly more challenging, because they are not usually inclined to participate for a number of reasons.

Visualization techniques have become one of the most widely used approaches for usable security [16, 37], in particular, in the management of security policies [36, 52]. Nevertheless, it can become an arduous process for administrators to alter certain tools and approaches to firewalling, partially because of the archaic systems and complex configuration files they have to deal with. Until recently system administrators were solely command line interfaces (CLIs) users [9, 27, 48], despite a strong development of visualization techniques in usable security.

3 Research Questions

The overall objective of this dissertation is to help system administrators better manage firewalls. Hence, the specific Research Questions addressed in the thesis are:

1. *What are the reasons behind firewall misconfigurations?*

   It has been demonstrated in the literature [54, 55] that firewall configuration files often contain errors. We need to understand why this happens and to investigate the complexity of the process of configuring firewalls. In particular, we want to identify the main difficulties system administrators deal with when working with firewalls and to check whether there are usability issues involved.

2. *How to improve the usability of the firewall configuration process?*

   Once the presence of usability problems is confirmed, we set off to identify solutions to them. We explore three different aspects of firewall configuration: 1) the syntax of rules, 2) the organization of rules in a rule set, and 3) the way rule sets are presented to a user. We aim to gain this information from the available theoretical framework and from those who work directly with firewalls. This will subsequently allow us to pinpoint the open challenges and to make recommendations on how the usability of the firewall configuration process can be improved.

4 Research Methodology

Computer science deals with the understanding and design of computers and computational processes. It can be considered as a mathematical, scientific and engineering discipline [17, 49]. Computer science is often divided into two major fields: *theoretical* and *applied* [15] and embraces a range of topics

such as *security and privacy, systems and networking,* and *software engineering*. This thesis deals with applied computer science and the topic addressed is a combination of computer security and human-computer interaction.

Throughout all the studies conducted in this thesis, we deal with user research [25]. It helps to learn about the user from their perspective, experiences, knowledge and mental models. Thus, user research removes biases that researchers and designers may have, which is crucial for further design processes. The data in our research were collected using quantitative and qualitative research methods. Quantitative research explores relatively large sample sizes of data to identify trends and patterns. Quantitative methods include surveys and questionnaires, observations studies, etc. In turn, qualitative research explores users' attitudes, behaviors, and opinions, and it helps to understand why specific trends and patterns arise. A good example of a qualitative research method would be unstructured or semi-structured interviews.

In some of our studies, a combination of both quantitative and qualitative methods was necessary to obtain a complete understanding of the user and the problems to be solved [32]. For example, in Paper IV we designed a survey which is comprised of close-ended questions that gathered the quantitative data about the participants' usage and preferences of different firewall interfaces as well as open-ended questions that accumulated qualitative data with regards to the strengths and limitations of those interfaces.

Furthermore, we have adopted a methodological triangulation [18] in one of the studies. Triangulation is the use of more than one approach to investigate a question. It is utilized for a number of reasons, e.g. to increase validity and reliability [11, 33]. In Paper III, we used a literature review and a user study with system administrators in order to determine the aspects that impact the usability of firewall rule sets.

Once the data are collected, they must then be analyzed and interpreted. We discuss the utilized data collection and analysis methods in Sections 4.1 and 4.2 and Sections 4.3 and 4.4, respectively. The systematic literature review method that incorporates both data collection and analysis is presented in Section 4.5.

Since the research done in this thesis deals with user studies that involve humans, ethical considerations were taken into account. We followed the Swedish Ethical Review Act [45] and the Good Research Practice guidelines from the Swedish Research Council [46] throughout the research project's entirety. One of the user studies required an explicit ethical approval and, therefore, was additionally examined by the institutional review board (IRB). For all our user studies we recruited voluntary participants. To ensure that they were treated ethically and with respect, we: 1) informed the participants about the study's goals and its duration; 2) did not collect any sensitive personal data; and 3) assured the participants of their rights, e.g. privacy, confidentiality, and anonymity [44].

4.1 Interviews

Interviews are a data collection method that involves two or more people exchanging information through a series of questions and answers. The purpose of the interview is to explore the views and experiences of individuals on specific matters. There are three main types of interviews: 1) structured, 2) semi-structured, and 3) unstructured [24]. The first two types are usually considered as qualitative methods, while the third is often utilized in quantitative research. A key difference between them is that the qualitative interviews contain open-ended questions, they are more interactive, more flexible and more sensitive to the language and concepts used by the respondent.

Structured interviews consist of a list of predetermined questions without the possibility to ask follow-up questions for further elaboration of the issue. Their main advantage is that they are relatively quick and easy to administer, and they are usually shorter, which allows the researcher to recruit more participants for the study with less effort. In Paper III, we conducted such interviews with students in order to test whether cognitive aspects affect the user–system interaction. A relatively large number of participants in that study allowed us to identify a cognitive aspect that influences the examination of firewall rule sets and get statistically significant results for its quantification. In the same paper, another set of structured interviews with system administrators was conducted in order to validate the proposed usability metrics.

Semi-structured interviews consist of a list of key topics or questions, i.e. an interview guide [8], that define the areas to be explored. A loose structure of such interviews allows the interviewer or interviewee divergence in order to pursue an idea in more detail [19]. In Papers I and III, we used semi-structured interviews with system administrators to get insight into the main difficulties they face when working with firewalls as well as the problems related to the usability of firewall rule sets.

4.2 Surveys

Surveys are yet another quantitative method for data collection, in which a researcher poses a set of predetermined questions to a group of individuals. Surveying is utilized to gather the opinions, beliefs and experiences of selected groups of participants. The ultimate goal of surveys is to learn about a large population by surveying a sample of it [22]. There are two types of surveys: cross-sectional and longitudinal [42]. The key difference between these types is the number of data collection procedures. In cross-sectional surveys, a researcher collects information at one point of time, while in longitudinal surveys, data collection is done at different points of time to observe the changes. In our studies, we have only used cross-sectional surveys. In Paper II, we ran an online survey to compare different firewall rule sets representations. We also utilized surveying in Paper IV. We collected data about daily usage and preferences of different firewall interfaces from a large sample of 300 system administrators.

4.3 Statistical Methods

A lot of quantitative data were collected during the studies in this thesis and, therefore, a variety of statistical methods, both parametric and non-parametric, had been utilized in the analysis. For example, in Paper III, a subjective mental effort questionnaire [57] was used and the obtained data were analyzed with the paired sample t-test. The paired sample t-test is used to determine whether the mean difference between two sets of observations is zero. Similarly, in Paper II, a non-parametric equivalent to the paired sample t-test, the Wilcoxon signed-rank test, was utilized to check whether a firewall expertise of the participants influences which rule set representation they prefer. Another statistical method utilized for the analysis of the validation study data in Paper III is the Spearman rank correlation test. It helped us to demonstrate that there was a very strong correlation between the results of a ranking exercise performed by the system administrators and the ranking produced by our usability metrics.

4.4 Content Analysis

Content analysis is a flexible qualitative research technique for analyzing large amounts of textual data [26]. The data for content analysis may come from interviews, open-ended questions, field research notes, etc. Before the text can be analyzed, coding procedures must be performed. Coding is the process of assigning labels, i.e. codes, to data in order to retrieve and categorize similar data chunks. Coding is typically performed by multiple researchers simultaneously. There are many different coding approaches [32, 38]. In Paper IV, we coded participants' responses to the open-ended questions using an initial coding approach [38] and performed a content analysis of the resulting data. With the help of this analysis, we were able to classify all the strengths and limitations of the different firewall interfaces and, based on that, provide design recommendations.

4.5 Systematic Literature Review

A systematic literature review (SLR) is a type of literature review that is used to identify, evaluate and critically appraise research studies in a particular area in order to answer a clearly formulated research question [31]. It is performed in accordance with a predefined strategy that comprises 1) the development of a protocol that includes all the elements of the review, including research questions the review is intended to answer, search terms, inclusion criteria, etc., 2) primary and secondary selection procedures, 3) meta analysis (if needed), and 4) data synthesis. In Paper V, we conducted an SLR with a focus on the usability of firewall configuration, which helped us to understand the state of the art in firewall usability.

5 Contributions

The main contributions of this dissertation are the following:

1. *A better understanding of the firewall management challenges*

   In Paper I, we conduct a series of semi-structured interviews with IT-professionals. We gain an insight into the firewall management process from system administrators' perspective, including what difficulties they face, how they interact within groups and what means or procedures are used to simplify this process. The results of the interviews also help us to identify that the lack of firewall usability is one of the challenges. This contributes to answering Research Question 1.

2. *An investigation of the relation between the preference of firewall rule set representations and the expertise*

   In Paper II, we conduct an online survey with 56 participants, in which we compare two different firewall rule set representations. We identify that the participants' preference for a particular representation depends on their firewall expertise. This contributes to answering Research Question 2.

3. *An understanding of the impact of cognitive aspects in the examination of firewall rule sets*

   In Paper III, we propose a hypothesis that the cognitive effort needed to understand a rule is not affected by its immediately preceding rule. We test that with a user study and the results reject the hypothesis. Furthermore, we present a function that indicates the relation between the cognitive effort reduction and the similarity between examined rules. The necessity of taking cognitive aspects into account is tested in the validation study. This contributes to answering both Research Questions 1 and 2.

4. *A proposal of means to measure the usability of firewall rule sets*

   It is necessary to have metrics in order to be able to compare different firewall solutions with respect to their usability. In Paper III, we introduce and mathematically formalize a set of four firewall usability metrics. We validate the quality of the proposed metrics by conducting a user study with system administrators. This user study shows a very strong positive correlation between how our metrics and system administrators characterize the usability. This contributes to answering Research Question 2.

5. *An investigation of which firewall interfaces are utilized and preferred by system administrators*

   We collect thoughts and opinions of 300 system administrators through an online survey in Paper IV. We investigate which interfaces system administrators prefer, and which they actually utilize in their daily tasks.

Unlike related works, we observe a significant shift towards the usage of graphical user interfaces. This contributes to answering Research Question 2.

6. *An identification and classification of strengths and limitations of different firewall configuration interfaces*

   In Paper IV, we make a content analysis of the responses of 300 system administrators. We collect information regarding the pros and cons of different firewall interfaces and which tasks they apply to. These strengths and limitations are classified in the paper, which then allows us to provide design recommendations for firewall interfaces. This contributes to answering Research Question 2.

7. *An investigation of the state of the art of firewall usability*

   In Paper V, we present an SLR with a focus on the usability of firewall configuration. We retrieve and screen 1,202 papers, of which 14 are selected and summarized. This SLR provides us an understanding for what has already been done and helps us to pinpoint the open challenges that exist in the field. Another contribution is a taxonomy of existing approaches that address the usability aspects of firewalls. This contributes to answering Research Question 2.

6 Summary of Appended Papers

Paper I – Challenges in Managing Firewalls

In this paper, we address the question: what are the main difficulties system administrators deal with when working with firewalls? Semi-structured interviews are selected as the method of inquiry in this study. Six system administrators take part in the interviews, in which they share their thoughts and opinions regarding the firewall configuration process. We draw some conclusions from the interviews' results such as 1) it is not always beneficial to have more people responsible for security measures and 2) firewall misconfigurations are a common problem. This paper shows that there are existing usability issues related to the management of firewalls.

Paper II – Natural vs. Technical Language Preference and its Impact on Firewall Configuration

In this paper, we compare two different representations of firewall rule sets: iptables and English. We gain insight into whether these rule set representations can reduce the amount of effort needed for their comprehension. We design an online survey for a participant pool familiar with firewalls and collect data from 56 participants with a varying knowledge of firewalls. The survey data are analyzed with the help of the Wilcoxon signed-rank test. The results show that the participants with a basic or intermediate knowledge of firewalls consider

the rule sets expressed in English are 40% easier to understand, whereas they are deemed to be 27% more difficult for the participants who are advanced or expert firewall users. We describe the reasons for such results, discuss their applicability, and suggest the possibilities for future work.

Paper III – Measuring the Usability of Firewall Rule Sets

In this paper, we introduce a set of metrics that can measure the usability of firewall rule sets in terms of how easy it is for IT professionals to understand and manage them. These metrics are derived from semi-structured interviews with eight system administrators, in which we elicit the usability challenges related to the management of firewall rule sets and findings from related work. With the help of a user study with students, we identify a cognitive aspect that influences the examination of firewall rule sets and learn how to quantify it. We validate the metrics by conducting another user study with eight other system administrators. We show that there is a very strong correlation between the results of a ranking exercise performed by the system administrators and the ranking produced by our metrics. Finally, we present and discuss practical implications of the proposed metrics.

Paper IV – System Administrators Prefer Command Line Interfaces, Don't They? An Exploratory Study of Firewall Interfaces

In this paper, we investigate which interfaces system administrators prefer, and which they actually utilize in their daily tasks. We survey 300 system administrators and collect their experiences and opinions of utilized firewall interfaces through an online survey. Our results show that only 32% of the respondents prefer command line interfaces for managing firewalls, while the corresponding figure is 60% for graphical user interfaces. We report strengths and limitations of each interface and the tasks for which they are utilized by the system administrators based on the data received from our participants. Taking into account the mentioned strengths and limitations, we provide design recommendations for firewall interfaces.

Paper V – Systematic Literature Review on Usability of Firewall Configuration

In this paper, we present an SLR with a focus on the usability of firewall configuration. Usability problems, as pointed out in the literature, entail poorly configured firewalls. During the selection procedures, 1,202 papers are retrieved and screened, 35 papers are chosen for further investigation, of which 14 papers are selected and summarized. As main contributions, we propose a taxonomy of existing solutions as well as a synthesis and in-depth discussion about the state of the art in firewall usability. Among the main results, we apprehended that there is a lack (or even an absence) of usability evaluation or user studies to validate the proposed models.

7 Concluding Remarks and Outlook

Even though each of the five appended papers has its own research goals, their findings significantly contribute to the achievement of the main objective of this thesis, i.e. to help system administrators better manage firewalls. By means of semi-structured interviews with system administrators, we discovered what difficulties they face and concluded that there are usability problems related to the management of firewalls. Some of these usability problems arise due to a discrepancy between utilized firewall interfaces and the expertise of system administrators. We identified that different groups of users may require different firewall rule set representations, and this fact should be taken into account when designing future firewall interfaces.

An important aspect overlooked in related work is the absence of metrics for measuring the usability of firewall rule sets. We therefore proposed a set of metrics and validated their quality with a user study that showed a very strong positive correlation between how our metrics and system administrators characterize the usability of rule sets. Hence, an automatic assessment of the manageability of rule sets as well as a comparison of different rule sets that implement the same security policy are possible with the assistance of the metrics. Moreover, knowledge of the individual metrics for each usability attribute can be used to quickly identify weaknesses in rule sets concerning their manageability.

We also learned that system administrators can be reached out and they are willing to help if approached in the right way. Reddit, especially the *Sysadmin* subreddit, is an outstanding source for feedback from system administrators. With its help we were able to conduct an online survey with 300 participants, in which we identified a considerable shift of system administrators towards using graphical user interfaces (GUIs). This is an indication of firewall manufacturers being on the right track, leading to significantly better GUIs. To stimulate a further improvement of firewall interfaces, we obtained and classified data concerning the strengths and limitations of current CLIs and GUIs.

As mentioned in Section 2.4, visualization techniques are thoroughly researched in the field of usable security. They are known to be convenient for the presentation of large amounts of information. We explored the application of visualization techniques for firewalls. The conducted SLR in Paper V gave us a thorough overview of the research area and helped us to identify existing gaps and sparsely studied sub-fields. Some of the reviewed visualization techniques need to be further investigated as they have a potential to simplify the configuration process.

In the future, we aim to continue working with the metrics proposed in Paper III. In particular, the weights of the metrics were assigned an equal value, but they might contribute differently to the total usability, requiring further investigation. In the long term, we plan to design a better firewall interface based on the findings throughout this thesis. This interface, as we see it now, should be a combination of CLI and GUI. Such an interface will suit system administrators of varying firewall expertise, allowing them to perform various tasks more efficiently.

References

[1] S. Al-Haj and E. Al-Shaer. Measuring firewall security. In *SAFECONFIG*. IEEE, 2011.

[2] E. S. Al-Shaer and H. H. Hamed. Firewall policy advisor for anomaly discovery and rule editing. In *IFIP/IEEE Eighth International Symposium on Integrated Network Management*, pages 17–30. IEEE, 2003.

[3] E. S. Al-Shaer and H. H. Hamed. Discovery of policy anomalies in distributed firewalls. In *INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies*, volume 4, pages 2605–2616. IEEE, 2004.

[4] E. S. Al-Shaer and H. H. Hamed. Modeling and management of firewall policies. *IEEE Transactions on Network and Service Management*, 1(1):2–10, 2004.

[5] M. Beckerle and L. A. Martucci. Formal definitions for usable access control rule sets from goals to metrics. In *Symposium On Usable Privacy and Security (SOUPS)*, 2013.

[6] S. Bhatt, C. Okita, and P. Rao. Fast, cheap, and in control: a step towards pain free security! In *LISA*. USENIX, 2008.

[7] M. Bingham, A. Skillen, and A. Somayaji. Even hackers deserve usability: An expert evaluation of penetration testing tools. In *Proceedings of the 9th Annual Symposium on Information Assurance*, ASIA'14, pages 23–31, 2014.

[8] A. Blackstone. Sociological inquiry principles: qualitative and quantitative methods. *Flat World Knowledge, Irvington, NY, USA*, 2012.

[9] D. Botta, R. Werlinger, A. Gagné, K. Beznosov, L. Iverson, S. Fels, and B. D. Fisher. Towards understanding IT security professionals and their tools. In *Symp. on Usable Privacy and Security (SOUPS)*. ACM, 2007.

[10] J. M. Carroll. Human computer interaction-brief intro. *The Encyclopedia of Human-Computer Interaction, 2nd Ed.*, 2013.

[11] S. Carvalho and H. White. *Combining the quantitative and qualitative approaches to poverty measurement and analysis: the practice and the potential*. The World Bank, 1997.

[12] H. Chen, O. Chowdhury, J. Chen, N. Li, and R. Proctor. Towards quantification of firewall policy complexity. In *Symposium and Bootcamp on the Science of Security*. ACM, 2015.

[13] W. R. Cheswick, S. M. Bellovin, and A. D. Rubin. *Firewalls and Internet security: repelling the wily hacker*. Addison-Wesley Longman Publishing Co., Inc., 2003.

[14] S. Chiasson, P. van Oorschot, and R. Biddle. Even experts deserve usable security: Design guidelines for security management systems. In *SOUPS Workshop on Usable IT Security Management (USM)*, pages 1–4, 2007.

[15] N. R. Council et al. *Computer Science: Reflections on the Field, Reflections from the Field*. National Academies Press, 2004.

[16] R. De Paula, X. Ding, P. Dourish, K. Nies, B. Pillet, D. F. Redmiles, J. Ren, J. A. Rode, and R. Silva Filho. In the eye of the beholder: a visualization-based approach to information system security. *International Journal of Human-Computer Studies*, 63(1):5–24, 2005.

[17] P. J. Denning, D. E. Comer, D. Gries, M. C. Mulder, A. Tucker, A. J. Turner, and P. R. Young. Computing as a discipline. *Computer*, 22(2):63–70, 1989.

[18] N. K. Denzin. *The research act: A theoretical introduction to sociological methods*. Routledge, 2017.

[19] B. DiCicco-Bloom and B. F. Crabtree. The qualitative research interview. *Medical education*, 40(4):314–321, 2006.

[20] J. Dougherty. Internet growth + usage stats 2019: Time online, devices, users. 2019.

[21] W. Fithen, J. Allen, and E. Stoner. Deploying firewalls. Technical report, Carnegie Mellon University Software Engineering Institute, 1999.

[22] F. J. Fowler Jr. *Survey research methods*. SAGE Publications Ltd., 2013.

[23] E. W. Fulp. Optimization of network firewall policies using ordered sets and directed acyclical graphs. In *Proceedings of IEEE Internet Management Conference*, 2005.

[24] P. Gill, K. Stewart, E. Treasure, and B. Chadwick. Methods of data collection in qualitative research: interviews and focus groups. *British dental journal*, 204(6):291, 2008.

[25] E. Goodman, M. Kuniavsky, and A. Moed. *Observing the user experience: A practitioner's guide to user research*. Elsevier, 2012.

[26] C. Grbich. *Qualitative data analysis: An introduction, 2nd Ed.* SAGE Publications Ltd., 2012.

[27] E. M. Haber and J. Bailey. Design guidelines for system administration tools developed through ethnographic field studies. In *Proceedings of the 2007 symposium on Computer human interaction for the management of information technology*, page 1. ACM, 2007.

[28] H. Hu, G.-J. Ahn, and K. Kulkarni. Detecting and resolving firewall policy anomalies. *IEEE Transactions on Dependable and Secure Computing*, 9(3):318–331, 2012.

[29] Ergonomic requirements for office work with visual display terminals (vdts): Part 11: Guidance on usability. Standard, International Organization for Standardization, 1998.

[30] S. Kemp. Digital trends 2019: Every single stat you need to know about the internet. 2019.

[31] B. Kitchenham. Procedures for performing systematic reviews. *Keele, UK, Keele University*, 33(2004):1–26, 2004.

[32] M. B. Miles, A. M. Huberman, and J. Saldana. Qualitative data analysis: A methods sourcebook. 3rd ed., 2014.

[33] M. D. Moon. Triangulation: A method to increase validity, reliability, and legitimation in clinical research. *Journal of Emergency Nursing*, 45(1):103–105, 2019.

[34] J. Nielsen. *Usability Engineering*. Interactive Technologies Series. Morgan Kaufmann, 1994.

[35] A. Patcha and J.-M. Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, 51(12):3448–3470, 2007.

[36] R. W. Reeder, L. Bauer, L. F. Cranor, M. K. Reiter, K. Bacon, K. How, and H. Strong. Expandable grids for visualizing and authoring computer security policies. In *CHI*, pages 1473–1482. ACM, 2008.

[37] J. Rode, C. Johansson, P. DiGioia, K. Nies, D. H. Nguyen, J. Ren, P. Dourish, D. Redmiles, et al. Seeing further: extending visualization as a basis for usable security. In *Proceedings of the second symposium on Usable privacy and security*, pages 145–155. ACM, 2006.

[38] J. Saldaña. *The Coding Manual for Qualitative Researchers*. SAGE Publications Ltd., 2012.

[39] J. H. Saltzer and M. D. Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278–1308, Sept 1975.

[40] M. A. Sasse and M. Smith. The security-usability tradeoff myth [guest editors' introduction]. *IEEE Security & Privacy*, 14(5):11–13, 2016.

[41] K. Scarfone and P. Hoffman. Guidelines on firewalls and firewall policy. Technical report, National Institute of Standards and Technology (NIST), 2009.

[42] J. J. Shaughnessy, E. B. Zechmeister, and J. S. Zechmeister. Research methods in psychology. 1990.

[43] B. Shneiderman and C. Plaisant. *Designing the User Interface: Strategies for Effective Human-computer Interaction*. Pearson/Addison Wesley, 2005.

[44] J. E. Sieber and M. B. Tolich. *Planning ethically responsible research*, volume 31. SAGE Publications Ltd., 2012.

[45] Svensk Författningssamling (SFS). *Lag (2003:460) om etikprövning av forskning som avser människor [The Act concerning the Ethical Review of Research Involving Humans]*. Utbildningsdepartementet, Stockholm, Sweden, 2003.

[46] Swedish Research Council (VR). Conducting ethical research. https://www.vr.se/utlysningar-och-beslut/villkor-for-bidrag/att-forska-etiskt.html, 2018. Accessed: 2019-12-12.

[47] C. Symantec. 2019 annual threat report. *Internet security threat report*, 24, 2019.

[48] L. Takayama and E. Kandogan. Trust as an underlying factor of system administrator interface choice. In *CHI'06 extended abstracts on Human factors in computing systems*, pages 1391–1396. ACM, 2006.

[49] M. Tedre and E. Sutinen. Three traditions of computing: What educators should know. *Computer Science Education*, 18(3):153–170, 2008.

[50] Z. Trabelsi and S. Zeidan. Multilevel early packet filtering technique based on traffic statistics and splay trees for firewall performance improvement. In *Communications (ICC)*, pages 1074–1078. IEEE, 2012.

[51] M. Van Welie, G. C. Van Der Veer, and A. Eliëns. Breaking down usability. In *Proceedings of Interact '99*, pages 613–620. Press, 1999.

[52] K. Vaniea, Q. Ni, L. Cranor, and E. Bertino. Access control policy analysis and visualization tools for security professionals. In *SOUPS Workshop (USM)*, 2008.

[53] A. Whitten and J. Tygar. Usability of security: A case study. Technical report, DTIC Document, 1998.

[54] A. Wool. A quantitative study of firewall configuration errors. *Computer*, 37(6):62–67, June 2004.

[55] A. Wool. Trends in firewall configuration errors: Measuring the holes in swiss cheese. *Internet Computing, IEEE*, 14(4):58–65, 2010.

[56] K.-P. Yee. User interaction design for secure systems. In *International Conference on Information and Communications Security*, pages 278–290. Springer, 2002.

[57] F. R. H. Zijlstra. *Efficiency in work behaviour: A design approach for modern tools*. PhD thesis, Delft University, 1993.

USABILITY OF FIREWALL CONFIGURATION

Firewalls are an important component of network security that serve to protect networks by regulating incoming and outgoing traffic. However, setting up firewalls correctly is a challenging task, which becomes more difficult with the growth of the network's size. Firewall configuration files consist of rule sets that might be hard to understand even for professionals who deal with them regularly. The main reason for this is that most firewall rule sets have a certain structure: the higher the position of a rule in the rule set, the higher priority it has. Challenging problems arise when a new rule is added to the set and a proper position for it needs to be found or the existing rules are removed due to a security policy change. This brings us to the usability problem associated with the configuration of firewalls.

The overall aim of this thesis is to help system administrators better manage firewalls. We explore three different aspects of firewall configuration: 1) the syntax of rules, 2) the organization of rules in a rule set, and 3) the way rule sets are presented to a user. Using this acquired knowledge, we offer system administrators more usable firewall solutions and approaches to the configuration process that can help facilitate their daily work.

DOCTORAL THESIS
KARLSTAD UNIVERSITY STUDIES, 2020:15
ISSN 1403-8099
ISBN 978-91-7867-098-7 (print)
ISBN 978-91-7867-108-3 (pdf)