Master Thesis
Electrical Engineering
May 2012

Response Time Effects on Quality of Security Experience.

Asad Muhammad
Wajahat Ali

School of Computing
Blekinge Institute of Technology
371 79 Karlskrona
Sweden

This thesis is submitted to the School of Computing at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Electrical Engineering. The thesis is equivalent to 20 weeks of full time studies.

Contact Information:
Authors:
Wajahat Ali
Address: Lindblomsvägen 106, Ronneby
E-mail: wajahat.bth@gmail.com

Asad Muhammad
Address: Kungsgatan 98, Lgh 0801, 37438, Karlshamn
E-mail: asad_omega@hotmail.com

University advisor:
Charlott Lorentzen, Ph.D. Student
COM/BTH

School of Computing
Blekinge Institute of Technology
371 79 Karlskrona
Sweden

Internet : www.bth.se/com
Phone : +46 455 38 50 00
Fax : +46 455 38 50 57

ABSTRACT

The recent decade has witnessed an enormous development in internet technology worldwide. Initially internet was designed for applications such as Electronic Mail and File Transfer. With technology evolving and becoming popular, people use internet for e-banking, e-shopping, social networking, e-gaming, voice and a lot of other applications. Most of the internet traffic is generated by activities of end users, when they request a specific webpage or web based application. The high demand for internet applications has driven service operators to provide reliable services to the end user and user satisfaction has now become a major challenge. Quality of Service is a measure of the performance of a particular service. Quality of Experience is a subjective measure of user's perception of the overall performance of network.

The high demand for internet usage in everyday life has got people concerned about security of information over web pages that require authentication. User perceived Quality of Security Experience depends on Quality of Experience and Response Time for web page authentication. Different factors such as jitter, packet loss, delay, network speed, supply chains and the type of security algorithm play a vital role in the response time for authentication. In this work we have tried to do qualitative and quantitative analysis of user perceived security and Quality of Experience with increasing and decreasing Response Times towards a web page authentication. We have tried to derive a relationship between Quality of Experience of security and Response Time.

Keywords: Quality of Experience, Quality of Service, Response Time and Security.

ACKNOWLEDGEMENTS

We would like to thank our advisor Charlott Lorentzen. Without her generous support and guidance this thesis work would have been impossible. We are also thankful to Prof. Markus Fiedler for his valuable suggestions and opinions for this thesis.

We are grateful to our parents for their endless support and love.

Asad Muhammad
Wajahat Ali

Contents

CHAPTER 1 ..... **3**

INTRODUCTION **3**

1.1 OBJECTIVE 4
1.2 RESEARCH QUESTIONS 4
1.3 RESEARCH METHODOLOGY 4
1.4 DOCUMENT STRUCTURE 5

CHAPTER 2 ..... **9**

BACKGROUND **9**

2.1 QUALITY OF EXPERIENCE 9
2.2 RELATED WORK 11

CHAPTER 3 ..... **15**

EXPERIMENT SETUP **15**

3.1 DESIGN 15
3.2 EXPERIMENT DESCRIPTION 15

CHAPTER 4 ..... **21**

RESULTS **21**

4.1 QUANTITATIVE ANALYSIS 21
4.2 QUALITATIVE ANALYSIS 25
4.3 DISCUSSION 26

CONCLUSION & FUTURE WORK **29**

5.1 CONCLUSION 29
5.2 FUTURE WORK 30
BIBLIOGRAPHY 31
APPENDIX A 33
APPENDIX B 39
APPENDIX C 45

Introduction

Chapter 1

Introduction

Internet plays a vital role in everyday life in this modern era of technology. It has become a medium for exchange of information and communication. People use internet for e-mails, e-banking, social networking, e-books, voice and data exchange and a lot of other applications. Most of the web pages require a username and a password for user authentication. When the user enters the desired information for authentication, user has to wait for some time for the authentication procedure to complete and for the information to be fetched from the server and displayed in front of him/her.

The Response Time (RT) for retrieving a particular web page or internet service depends on the type of authentication procedure, different network conditions or security protocols running in the background of which the user is unaware. An authentication procedure consists of a chain of messages before it is completed. The user perception is based upon the whole RT and if the greatest contributor to the RT within a network is found then it can be minimized or can be made scalable for large network delays with the aim to preserve good Quality of Experience (QoE) [2].

Authentication solutions are designed for user security to keep the undesired and unauthorized people out. Through authentication, the end user has to wait some extra time. If the response time increases the end user gets less interested in the service. Studies have shown that a user notices a response time of 100 ms, gets bored after 4 s and the risk of leaving a web page at 10 s [6].

The users do get concerned about a login on a particular internet website when the authentication procedure takes little or more time to get full access and the user starts judging the service and the level of security. Within this last decade internet traffic has increased drastically. With increasing number of users, user satisfaction has become a major challenge for service providing operators. In the present situation the service providers should provide fast and reliable services to meet the demands of the users in order to be able to run their businesses in the competitive market.

The performance of any web page depends on Quality of Service (QoS). QoS includes factors e.g delay, packet loss, throughput and jitter. User satisfaction or QoE is subjective in nature and depends on QoS parameters. The service provider should ensure that the service is safe and available all the time. It is important to understand how the end users feel about the performance and the level of security for a service. By qualitative and quantitative analysis of user perception towards web authentication procedure, the effect of RT on QoE of Security can be studied. This can help the service providers to judge user perception and the level of security for their service.

The end user in most cases is unaware of the technical problems within a network and analyzes the service based on RT whereas the service provider knows the technical issues within the network and analyzes the problems by monitoring QoS parameters. Based on an experiment it has been shown that the user interaction time with a web site and the method of page loading affects the QoS [10]. Tolerance of delay depends on users conceptual models about the working of a system. Poor web performance creates a poor corporate image and the users feel less secure while

using the website. The user perception can be integrated into server design and therefore results in QoS that reflects user's perception about the quality [10].

As the use of web based technology is growing with more and more users uploading their personal data over the web, authentication plays a vital role in the internet world to ensure the security of data. Based on the level of security, the RT for the web authentication can be changed and it can be useful for the service providers to deliver secure services to the end users and stay competitive in the global market.

1.1 OBJECTIVE

One of the main objectives of this thesis work is to study the effect of response time on user perceived security and derive a relationship between them. As the user perceived security also affects QoE, the other objective is to derive a relationship between user perceived security and QoE. To achieve this we have done a web login experiment with different response times. Students at Blekinge Tekniska Högskola (BTH) took part in this experiment and answered a survey questionnaire. After collecting data from the users survey questionnaires, we have done qualitative and quantitative analysis of the data to study the user behavior in terms of level of security towards web login authentication procedure. We have visualized data in Microsoft excel to show the relationship between RT and performance of web page, and the relationship between RT and user perceived security.

1.2 RESEARCH QUESTIONS

1. Do the users feel more secure if the response time for a web login is longer?

2. How does users perceived security relate to increased and decreased response times for web authentication?

3. What is the relationship between user perceived security and QoE of performance?

1.3 RESEARCH METHODOLOGY

For this thesis work, we have performed a local web login experiment with users based on various RTs. For qualitative and quantitative analysis of RT effects on QoE of performance and QoE of security we have designed a survey questionnaire for users participating in the experiment. The survey questionnaire will help us analyze how users feel about the performance and the security of the web login based on different RTs. For ratings we have chosen Continuous Rating Scale (CRS) methodology.

CRS is used for user subjective ratings. By using this methodology the users are asked to give a rating by placing a mark at a position corresponding to their perception of the observed phenomenon on a continuous line. The line is usually labeled at each end. The main advantage of this scale is that user's immediate reaction to the changing level of QoS which affects QoE can be judged quantitatively [13]. This assessment is applicable to systems with variable QoS or tasks of low cognitive load [13]. CRS was developed to allow users to access both audio and video in video conferencing applications [14], [15]. In this thesis work we have used this scale for data transfer application in the form of a webpage.

For quantitative analysis of user perceived security, we have divided the users ratings into three categories for making the analysis simple. First category corresponds to the users who gave high ratings to 0 s RT for web page security. Second category corresponds to the users who gave high ratings to 1 s RT for web page security and the third category corresponds to the users who gave low ratings to 0 s RT and high ratings for 8 s RT for web page security. These categories are indicated in Appendix B.

1.4 DOCUMENT STRUCTURE

The remaining report is organized as follows. Chapter 2 defines the technical background and the related work that has been done in this field. Chapter 3 describes the experimental setup and chapter 4 describes the qualitative and quantitative analysis of results. Chapter 5 concludes the report and presents future work.

Background

Chapter 2

Background

Internet was initially designed for simple applications such as World Wide Web (www), email and file transfer. With the passage of time, Internet has now become the backbone of most existing technology. Therefore it is important to understand and analyze the networks for more robust and secure future web services. Different studies and experiments have been carried out to understand the elements of networks that can be improved for providing security to the end user as most of the user's private information is available on the Internet today. There has always been a threat of unwanted users accessing other's private information. As a result, with the developing technology the end users are more concerned about the security of a web page [18]. The service providers are trying to make sure that the users get fast and reliable services. The user perception about a particular web page or service (QoE) judges the overall performance and security of a service. This can help the service providers to update their services to satisfy the end user. Different service providers compete with each other to provide services. The main aim of each company or service provider is to capture a large share of market and it is only possible if the users are satisfied with the service. Performance and security are two important parameters that can judge a user's satisfaction level for web page authentication.
Depending on RT, users get access to a particular web page after authentication. Therefore a users satisfaction levels can be estimated through RT. RT itself depends on different network conditions i.e. QoS, type of security algorithms, supply chains etc.

To study the effect of RT on QoE of Performance and QoE of Security; we have performed an experiment and a survey in this research work with a web login procedure. The main aim of this experiment is to study the behavior of different users towards web login procedure.

2.1 QUALITY OF EXPERIENCE

The concept of QoE is used to measure user satisfaction level as shown in Fig1. QoE is defined as the overall acceptability of an application or service as perceived subjectively by the end user [5]. QoE includes complete end-to-end system ranging from users, terminal, customer premises network, and core and access network to service infrastructure [5]. In this thesis work QoE refers to the users experience based on end-to-end RT for web logins.

Fig1. Relationship between QoS and QoE [12].

2.1.1 QUALITY OF SECURITY EXPERIENCE

When the user perception is based on applications or services that have the factor of security involved with them e.g. web applications or web services that require authentication then security plays a vital role in QoE. If the users do not feel secure enough while using a particular service, the service provider might lose the customers. It is important to know whether the users really care about the security for a specific service or not. If the users do not care then the aspect of security might be compromised [6]. Since security plays a crucial role in services today, we have done an experiment with a web login with authentication procedure based on RT to study the user behavior about security and QoE.

2.1.2 QUALITY OF EXPERIENCE MEASUREMENT

For statistical analysis and quantitative measurement of QoE, there must be a group of users of an appropriate size who participate in the experiment and then give their answers or ratings to the experiment by answering a survey. When measuring QoE, questions are asked from the users with a particular service or application in mind. The questions must be solely related to the service or application and should not pose any misunderstanding for the users. The questions must be generic and specific for all the users participating in the experiment. If these measures are not taken into account then the experiment might lead to biased results.

2.1.3 CHALLENGES

User's subjective emotions and past experience play an important role in measuring QoE. While measuring QoE, users must be tested with an experiment which is close to a real life scenario. If the experiment is unrealistic then the users may get confused and give biased ratings which may lead to faulty results.

Based on previous experience, users who have used internet with slow speed may answer the questions differently as compared to users who use a high speed internet connection. It may also be that not many users are willing to participate in the experiment. The users may not find the experiment interesting and this may lead to users not giving honest ratings. Sometimes users don't even care and just give the rating as a formality of participating in the experiment. Sometimes users' subjective emotions play a negative role in rating e.g. if users have too much on their mind or they are busy. To get honest user ratings and good results, the above mentioned challenges should be met by performing an experiment close to the real scenario. In this thesis work we have done an experiment which is close to the real scenario to get good user ratings.

2.2 RELATED WORK

Quality of Experience (QoE) is a widely discussed topic in the modern era of internet systems and communications. Accessing user perceived security with QoE is a new research area and not much work has been done on it. User perceived security has been evaluated in different ways with the help of experiments. The discussion below shows the current research in the area of QoE and user perceived security.

Defining and measuring QoE is difficult and involves studies from different disciplines. QoE has many factors involved of which some are subjective and non controllable while others are objective and controllable [6]. Subjective factors include user emotions, experience and expectations whereas objective factors include technical and non technical factors which can be either application dependent or terminal dependent [6]. A model for user perception of security in web pages has been developed with the help of OpenID web login experiments and MOS (Mean Opinion Score) for quantitative analysis [1]. Previous experiments indicate that there is a difference in opinions about web pages that require login for authentication or security than normal web pages when there is a delay in the service. Users show slightly higher patience towards web pages when the factor of security is involved [1].

Identification and quantification of decisive factors for QoE of Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM) with OpenID authentication has been studied to find out the parts of the EAP-SIM authentication which give the greatest contribution to RT (Response Time) [2]. Based on the experiments future optimization of user perception towards safety can be analyzed [2]. Society's behavior towards getting rid of anxiety and achieving a greater sense of safety has been studied with the help of an experiment using nursing care robot for security evaluation [7]. Whereas [8] has discussed an approach to diminish the anxiety of people's minds and judging sense of safety towards science and technology from the standpoint of interface engineering. The effect of color, voice and information presentation on user perceived safety has been studied [8]. Similarly [9] has discussed the user sense of security in terms of safety, anger and disgust by using a humanoid robot's pick and place motion.

Different experiments designed to estimate user tolerance of QoS in the area of e-commerce have been presented and designing web servers based on users conceptual models for web tasks and user tolerance has been discussed [10].

The research work above has shown QoE and sense of security from different angles. Sense of security has been taken as feelings of happiness, fear, anger or disgust in different research papers as mentioned above. Based on the response time sense of security in terms of privacy of information for web logins has not been addressed. The current literature lacks study in relationship between response time and user perceived security and their overall effect on QoE. The main aim of this thesis is to study the response time involved in the authentication procedures and their effect on user perceived security and overall QoE.

Experiment Setup

Chapter 3

Experiment Setup

In this chapter we will discuss the experimental setup and how the users undertake the experiment. The experiment includes, adding various RTs in a web page login created in PHP and the development of a survey questionnaire for user ratings.

3.1 DESIGN

The main idea behind the experiment setup is that the users are given a platform, in this case a local web page with a user login system. As our work aims at judging user sense of security and QoE of performance, the web page takes username and password from the users for authentication as shown in Figure 3.1. The information is displayed in front of users after some waiting time as shown in Figure 3.2. To bring our experiment close to real life situations, we introduced various RTs in the login procedure. For quantitative and qualitative analysis of user sense of security and QoE of performance we designed a questionnaire. By analyzing the user ratings the relationship between response times, user perceived security and QoE of performance has been derived.

3.2 EXPERIMENT DESCRIPTION

In this section, a detailed description of the experiment is described. We set up the experiment in windows environment. For this we installed the software XAMPP version 1.7.4 with PHP version 5.3.5 in Windows 7 operating system. The web page interface consisted of simple username and password fields as shown in Figure 3.1. Response time plays an important role in authentication procedure and it is dependent on network conditions, type of security algorithm and supply chains. RT also depends on page loading time but for this thesis work we have only considered the authentication part to study the user behavior. To simulate the existence of response time and to emulate QoS (jitter, packet loss, throughput, delay), we introduced delay in the login procedure with the help of the sleep(x) command in PHP code where x is the required delay in seconds. Studies [19] [20] have shown that for RTs of around 1 s users start noticing that there is a delay, at RTs of around 4 s users start becoming impatient and at RTs of around 10 s there is a high risk that users will leave the web page or service. Based on above mentioned studies, we chose RTs of 0 s, 1 s, 4 s and 8 s for web login experiment. For the qualitative and quantitative analysis of response time and its effects on user perceived security and QoE of performance, we designed a survey questionnaire which consisted of two questions as shown in Appendix C. One of the questions was related to the QoE of performance for the web page login and the other question was related to the QoE of security of the web page login. These questions were repeated for the response times as mentioned above. 28 different students from Blekinge Tekniska Högskola with

engineering backgrounds participated in the experiment and answered the survey questionnaire. A study [21] has shown that a user's current experience of a service quality is shaped by past experience which is known as memory effect. To get accurate rating from the users in our experiment, they first performed the experiment with 0 s RT, then with 1s RT and finally with 4 s and 8 s RTs.

Before the start of the experiment users were briefed about the experimental procedure. Each user first performed the local web login experiment for 0 s RT by entering the username and password for the login procedure and clicked on the submit button as shown in Figure 3.1. After the mentioned RT, information was displayed in front of users as shown in Figure 3.2. The users then answered survey questionnaire using CRS based on the experiment. While users answered the survey questionnaire, the RT for the web login was updated to 1 s. For each RT the same procedure was followed. Users also participated in a discussion after completing the experiment and survey to give their opinions about the web logins experience in everyday life and their way of thinking about the sense of security and QoE of performance. After the collection of data from users, we translated the user ratings from CRS used in survey for quantitative analysis. For this we assigned 0 % to the lowest end and 100 % to the highest end of CRS. We divided the scale in intervals of 10 %. To minimize errors, we used a normal scale and measured the position of marks placed by users on CRS. To measure the ratings of users who made a diagonal marking on the scale, we drew a perpendicular line on the marking where it intersected the scale and took the value on the perpendicular line. We discarded the ratings of three users from the analysis because they gave the same ratings for each RT. After translating all the data from CRS to percentages for each RT we plotted the graphs in Microsoft Excel to show the effect of RT on QoE of performance and QoE of security.

Fig. 3.1 Web page for user experiments

Fig. 3.2 Web page for user experiments

Results

Chapter 4

Results

4.1 QUANTITATIVE ANALYSIS

In this section we will show the quantitative analysis of the results in the form of graphs. The users first performed the web login experiment with RTs of 0s, 1s, 4s and 8s and then gave the ratings on the questionnaire.

4.1.1 PERFORMANCE OF WEB LOGIN

First we needed to study the effect of RT on performance of web page login. Based on the RT for the authentication procedure, 28 users gave ratings which can be seen in Figure 4.1 with RT on x-axis and users perceived web login performance on y-axis. We have used exponential, linear, logarithmic and power regression lines for quantitative analysis. We compared the regression lines with their R^2 values to get the best fitting trend line for our experiment as shown in Table 1. Exponential regression line gave the best R^2 value than linear, logarithmic and power regression lines for predicting the future trend. This regression line is shown in Figure 4.1

Table 1.Regression Lines with Coefficient of Determination for QoE of Performance

Regression Line	**R^2 Value**	**Regression Line Equation**
Exponential	0.992	$y = 86.74e^{-0.13x}$
Linear	0.956	$y = -7.169x + 84.37$
Logarithmic	0.567	$y = -2.01\ln(x) + 53.52$
Power	0.479	$y = 49.68x^{-0.03}$

Figure 4.1 indicates that with the increase in RT the performance of the web login decreases. Almost all the users gave high ratings for RT of 0 s which is the ideal case and then for RT of 1 s. RT of 8 s is considered worst for performance of web pages. This shows that with the increasing RT, the performance decreases. In other words it can be said that with the increasing RT, the user perception about the performance of web login decreases i.e. the QoE of performance decreases. The exponential regression line shown in Figure 4.1 indicates the decreasing trend with the increasing RTs. RT affects the user satisfaction and with the increasing RT, there is a greater risk that the user might stop using the service which has high response times. The error bars indicated in Figure 4.1 show the margin of error that may exist in user ratings. For determining the margin of error, we calculated the standard deviation based on the ratings given by the users for performance of the local web

page used in our experiment. The margin of error is high in user ratings because of high standard deviation. The reason behind high standard deviation is small number of users who participated in the experiment.

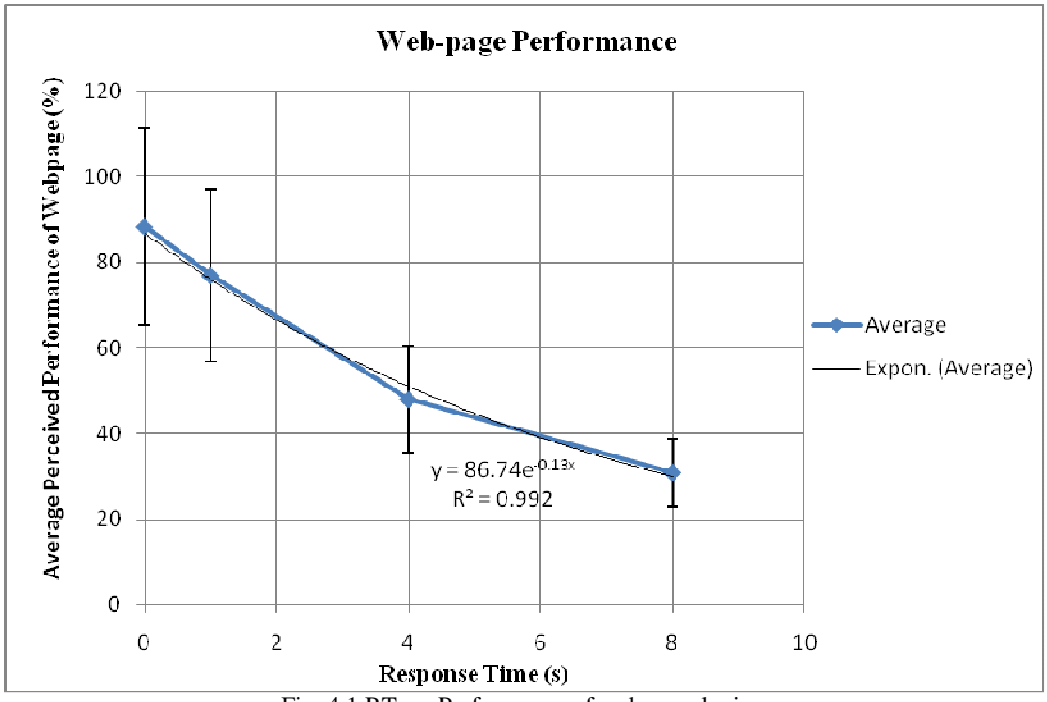


Fig. 4.1 RT vs. Performance of web page login

4.1.2 SECURITY OF WEB LOGIN

For the quantitative analysis of security the users performed the same experiment with the mentioned RTs. Different users gave different ratings about the sense of security. Since there was a big variation in security perception between all the users that participated in the experiment, the quantitative results were divided into categories to make the analysis simple. For each category we plotted linear, logarithmic, exponential and power regression lines for comparison of R^2 values. The R^2 values of these regression lines for each category are shown in Table 2.

Category 1 shows perceived security for 53.5 % of all users that participated in the experiment as indicated in Figure 4.2. For this category, exponential regression line gave best R^2 value as compared to linear, logarithmic and power regression lines as indicated in Table 2. The users of this perception category gave an average rating of 80 % for perceived security at 0 s RT. With the increase in RT the user perceived security decreases. These users felt less secure for RT of 8 s. The decreasing trend in user perceived security can be seen in Figure 4.2 with exponential regression line. For error bars in Figure 4.2, the standard deviation calculated was 20.78. The large value of standard deviation is because the number of users who participated in the experiment is small. If the number of users are increased, it will result in low standard deviation which will reduce margin of error.

Table 2. Regression Lines with Coefficient of Determination for QoE of Security

Category	Regression Line	R^2 Value	Regression Line Equation
1	Exponential	0.982	$y = 75.17e^{-0.11x}$
	Linear	0.936	$y = -5.595x + 73.68$
	Logarithmic	0.695	$y = -1.76\ln(x) + 48.90$
	Power	0.571	$y = 46.64x^{-0.03}$
2	Linear	0.996	$y = -4.756x + 80.23$
	Exponential	0.983	$y = 83.53e^{-0.08x}$
	Logarithmic	0.895	$y = -14.9\ln(x) + 76.89$
	Power	0.847	$y = 78.23x^{-0.26}$
3	Power	0.874	$y = 64.16x^{0.018}$
	Logarithmic	0.835	$y = 1.021\ln(x) + 64.57$
	Linear	0.799	$y = 2.733x + 51.86$
	Exponential	0.756	$y = 51.59e^{0.046x}$

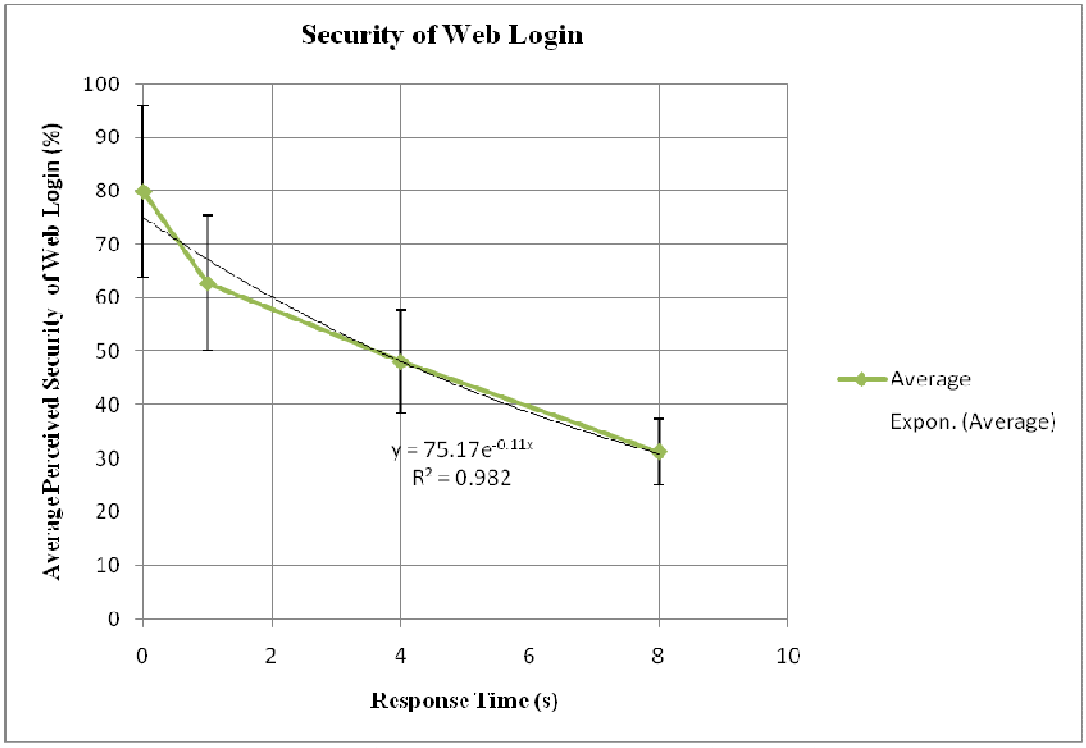


Fig. 4.2 RT vs. Average user perceived security

Figure 4.3 indicates the results for category 2. This category shows the results for 25 % of all users. These users felt 53 % secure for the RT of 0 s and said that this is the ideal case and this can never be possible to have 0 s RT with different network

conditions. They gave preference to RT of 1 s and rated the security level of web page login to approximately 75 %. They felt less secure for RTs of 4 s and 8 s. For this category linear regression line gave R^2 values as compared to exponential, logarithmic and power regression lines as shown in Table 2. For error bars in Figure 4.3, the standard deviation calculated was 11.52.

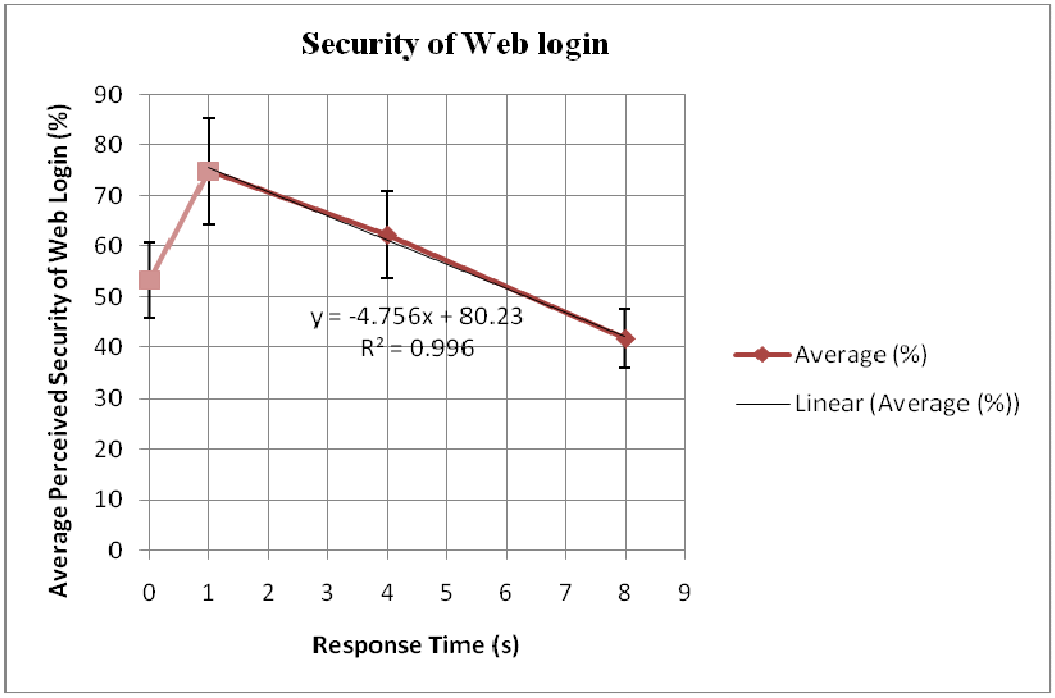


Fig 4.3 RT vs. Average user perceived security

Figure 4.4 indicates results for category 3. This category shows perceived security for 21.5 % of all users who participated in the experiment. The users for this category gave entirely different ratings as compared to the above mentioned categories. They rated the security of web login to 46 % for RT of 0 s and felt more secure for a RT of 8 s and rated the security of web login to 71 %. For this category power regression line gave better R^2 value as indicated in Table 2. With the increase in RT there is an increasing trend in user perceived security as indicated in Figure 4.4. The reason that users gave for this behavior was that authentication should require more RT. If there is a security check running in the background then the network should spend some time to provide authentication for this web page login. For error bars in Figure 4.2, the standard deviation calculated was 10.98.

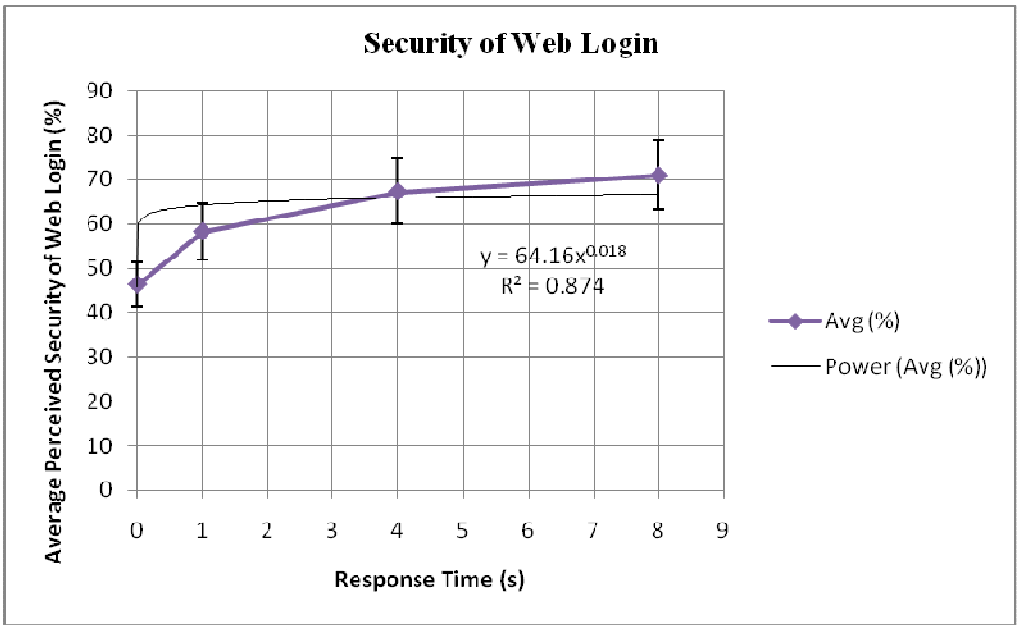


Fig. 4.4 RT vs. Average user perceived security

4.2 QUALITATIVE ANALYSIS

In this section we present the qualitative results. Each user participated in a small discussion after the experiment in which they presented their experiences about how they perceive security and performance of web logins in everyday life. As the user group consisted of international students with different cultural backgrounds, therefore they presented different thoughts about security and QoE based on their past experiences.

Users said that if the RT is 0 s then the service is better, performance vice, but for security of web login there should be some more waiting time. One user said that if the RT is from 1 s to 3 s then I think the service is very good and the web login is safe and I would not bother about security for this RT.

Users also said that if it's a trusted web login e.g. Hotmail, Gmail or Yahoo then they don't bother about the security issue. But if it takes more than 6 s then they might think about leaving that Internet service provider.

Two users who use high speed Internet connections said that 200–300 ms are enough for a good service and for authentication procedure to complete for web logins. One user said that a RT of 0 s is unreal and the service might be good but web login may not be safe as there would be no security algorithm running in the background.

Six users said that if it takes very long time to login then they think there is something wrong with their system or router. One user said: if it takes more than 7 s to authenticate myself to a web page then first I think that there is something wrong with my system or router. If they are working all right then I have second thoughts about security of the webpage. Another user said: if the RT is 2 s to 4 s then there might be a complex security algorithm running in the background or there might be proxy servers in the way that are responsible for that and I think in that case the

service is good and introduction of RT of 2 s to 4 s is because of extra security of a web page.

Eight users who had a past experience of using slow network speeds said: authentication normally takes a long time and they feel safe that way. So they rated 0 s RT as not safe and they preferred RT of 8 s as being the safest RT for security.

One user said: If the RT is above 4 s then my perception will be that some third party is trying to access my information unless it is some trust worthy website but at the same time the service might still be good.

4.3 DISCUSSION

After analyzing all the data and visualizing them, it can be seen that users have different satisfaction levels based on their past experiences or network conditions. RT plays a vital role in judging the performance and security of a service. As users keep most of their private information on the internet, they require a good service to access the information and at the same time demand security.

After the analysis we can say that QoE of performance and security are dependent on RT. If the RT is large then the users rate the performance of a web page very low. 53.5 % of the users who participated in the experiment gave low ratings to the security of the web login for high RTs. 25 % of the users gave their highest ratings for RT of 1 s for security of the web login and gave low ratings for RT higher than 1 s. 21 % of the users had different views and gave high ratings to the security of the web login for high RTs. In their opinion, authentication should take some time and higher RT is due to the complexity of security algorithm in the background.

From Figure 4.1 it can be seen that almost all the users judged the QoE of performance as good at small RTs and gave low ratings to performance for high RTs. From Figure 4.2 and Figure 4.3 it can be seen that with the increasing RT majority of the users feel less secure for the particular web login. So if the RT increases, QoE of performance and QoE of security both decrease. If the RT is high due to network conditions then service providers should give better services to the customers. If the RT is high for authentication of a particular website but at the same time RT is low for other websites then the complexity of security algorithm must be responsible for introducing RT or there might be a problem with the security of that website. In this case users might think that there is no problem with the performance of service but that there is a problem with the security of that particular web login. In our results as indicated in Figure 4.1, 4.2, 4.3 and 4.4 the error margin is high due to large values of standard deviation. The large values of standard deviation are due to small number of users who participated in experiment. If the number of users and observation points i.e. RTs are increased, it would result in low standard deviation values with less margin of error.

Conclusion
&
Future Work

Chapter 5

Conclusion & Future Work

5.1 CONCLUSION

We have presented qualitative and quantitative analysis of Quality of Security Experience in this thesis work. Quality of security experience depends both on QoE and user perceived security. With the help of web login experiment and analysis of users' survey ratings, we have evaluated user QoE of performance and security of a web page login for different RTs.

We have performed an experiment and a survey to study user behavior towards increasing and decreasing RTs for web authentication. The experiment consisted of a web page login where users entered username and password for authentication. We made four cases for authentication with RTs of 0 s, 1 s, 4 s and 8 s. The survey consisted of two questions for each case. First question was related to the QoE of performance of the web page and second question was related to the QoE of security of the web page. Users first performed the experiment and then answered the survey questionnaire for each case. Based on the user ratings and discussions, we analyzed the results and plotted the relationship between RTs, performance of web page and security of web page.

After performing the experiment and analysis of results we came to the conclusion that there is difference in user perception about quality and security for web page logins. The results suggest that with the increasing RTs the users perceive the performance of service as worse. So for increased RT the QoE of performance decreased. From survey ratings and discussions, users had different opinions based on their past experiences and network speeds for security. 53.5 % of the users who participated in the experiment have rated that with increase in RT, they feel less secure with the authentication procedure for web login. 25 % of the users gave their highest ratings to RT of 1 s over other RTs and felt secure. They said if RT is higher than 3 s then there might be a third party trying to access their information. 21.5 % felt secure with the increase in RT and think that the complexity of the security checks plays a major role in adding extra RT.

Therefore, for better QoE of performance and better QoE of security of web pages that require authentication, the RT should be small. The security algorithm for web authentication should be designed in a way that it is secure and at the same time it does not increase the RT. The service providers should improve the service by controlling QoS parameters which can help them reduce the RT so that users feel more secure while using their service. The security algorithms for web authentication and network conditions introduce increasing and decreasing RTs. For better QoE of security, both these entities need to work in a way to reduce RT.

5.2 FUTURE WORK

In this thesis work we have not used any security algorithm for user authentication. We have only used increasing and decreasing RTs to check the user behavior towards QoE of security. The future work should investigate QoE of security and QoE of performance with the introduction of an actual security algorithm in the experiment and then study the user behavior with survey and interviews. The role of complexity of security algorithms in producing increasing RTs and its effects on user sense of security and QoE needs to be investigated. This way the users might give different ratings based on their knowledge and expectations. The results of this thesis work should be compared with the experiment including security algorithm for authentication to find the differences in user behavior.

BIBLIOGRAPHY

[1] C. Lorentzen, M. Fiedler, H. Johnson, J. Shaikh and I. Jorstad. On User Perception of Web Login– A Study On QoE in the Context of Security. In proceedings of Australian Telecommunication Networks and Applications Conference (ATNAC 2010), Auckland, New Zealand, November 2010.

[2] C. Lorentzen, M. Fiedler, H. Johnson, J. Shaikh and I. Jorstad. Decisive Factors for Quality of Experience of OpenID Authentication Using EAP-SIM. In Proceedings of the European Teletraffic Seminar (ETS 2011), Pozan, Poland, February 2011.

[3] C. Eliasson, M. Fiedler and I. Jorstad: A criteria-based evaluation framework for a authentication schemes in IMS. In proceedings of the 4th International Conference on Availability, Reliability and Security (AReS), Fukuoka, Japan, March 2009, pp. 865-869.

[4] T. Ciszkowski, C. Eliasson, M. Fiedler, Z. Kotulski, R. Lupu and W. Mazurczyk. SecMon: End-to-End Quality and Security Monitoring System. Annales UMCS, Informatica, AI 8 (2008), pp 186-201.

[5] J. Zhang and N. Ansari,"On Assuring End-to-End QoE in Next Generation Networks: Challenges and a Possible Solution," *Communication Magazine, IEEE, Issue: 7 Volume 49,* July 2011, pp. 185-191

[6] C. Lorentzen,"User Perception and Performance of Authentication Procedures," Licentiate dissertation, Dept. School of Computing, Blekinge Institute of Technology, Karlskrona, Sweden, 2011.

[7] H. Tamura, Y.Minura, M. Inuiguchi,"Value judgment for evaluating the sense of security based on various utility theoretic approaches," *In proceedings of SICE annual conference*, Sapporo, Japan, August 2004.

[8] M. Nakatani, R. Tabata, S. Nishida,"Discussion about a sense of security and satisfaction," *In Proceeding of the IEEE International Conference on Systems, Man and Cybernetics*, Taipei, Taiwan, October 2006.

[9] S. Nonaka, K. Inoue, T. Arai, Y. Mae,"Evaluation of human sense of security for coexisting robots using virtual reality," *In Proceedings of IEEE International Conference on Robotics and Automation*, April 2004.

[10] N. Bhatti, A. Bouch, and A. Kuchinsky. Integrating user-perceived quality into web server design. In Proceedings of WWW'00, Amsterdam, 2000.

[11] J. Shaikh, M. Fiedler and D. Collange,"Quality of Experience from user and network perspectives," *In Annuals of Telecommunications: Quality of Experience – 1 Metrics and performance evaluation,* February 2010, pp. 47-57

[12] Kilkki K., "Quality of Experience in Communication Ecosystem, Journal of Universal Computer Science," Vol. 14, Page 5, 2008

[13] A. Bouch, M. A. Sasse, H. DeMeer, "Of Packets and People: *A User-centered Approach to Quality of Service," Quality of Service, 2000. IWQOS. 2000 Eighth International Workshop*, 2000, pp. 189-197.

[14] ACTS TAPESTRIES, "Acceptability studies in selected areas of audio-visual communications," ACTS Project AC055, Deliverable R/003/b2, 1997.

[15] A. Bouch, A. Watson and M. A. Sasse, "QUASS – A tool for measuring the subjective quality of

real time multimedia audio and video," *In Proceedings of HCI 98*, (Sheffield, England), 1-4 September 1998.

[16] M. Fiedler, T. Hossfeld and P. Tran-Gia. A Generic Quantitative Relationship between Quality of Experience and Quality of Service. IEEE NETWORK, Special Issue on Improving QoE for Network Service, Vol. 24, No. 2, pp. 36-41, March/April 2010.

[17] S. Eriksen, C. Eliasson, M. Fiedler, S. Chevul and A. Ekelin. Mapping service quality – comparing quality of experience and quality of service for Internet-based map services. In Proceedings of the 30th Information Systems Research Seminar in Scandinavia (IRIS), Tampere, Finland, August 2007.

[18] Wubin, Z. K. Feng, Y. Y. Axin,"A Data Safety Transmission Solution in Web Application" *International Conference on Web Intelligence and Intelligent Agent Technology*, January 2008, pp. 303-306

[19] M. Fiedler, ed. EURONGI Deliverable D.WP.JRA.6.1.1: State-of-the art with regards to user-perceived Quality of Service and quality feedback. May 2004. http:// eurongi.enst.fr/archive/127/ JRA611.pdf [Online] [Cited 2011-05-03]

[20] A. Bouch, A. Kuchinsky and N. Bhatti. Quality is in the eye of the beholder: Meeting user's requirements for internet quality of service. Technical Report HPL-2000-4, HP Laboratories Palo Alto, January 2000. http:// www.hpl.hp.com/techreports/2000/HPL-2000-4.pdf [Online] [Cited 2011-05-03]

[21] M. Fiedler *et al*,"The memory effect and its implications on Web QoE modeling,"*23rd International Teletraffic Congress*, September 2011, pp. 103-110.

APPENDIX A
PHP CODE

Appendix A
PHP Code

```
<?PHP
		error_reporting (E_ALL ^ E_NOTICE);
?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>BTH information</title>
<link href="style.css" rel="stylesheet" type="text/css" />
</head>
<body>
<div id="maincontainerwrapper">
<div id="header"><img src="images/head_logo_en.png" width="568" height="85"
alt="header" /></div>

<?PHP
		session_start();

		$delay = array('0', '1', '4', '8');
		//$delay = array('0.5', '1', '2', '5', '10', '10', '5', '2', '1', '0.5');



		if(isset($_POST['logout']))
		{
			$_SESSION['aktiv'] = false;
			$_SESSION['cnt']++;
		}

		if(isset($_POST['name']) && isset($_POST['pass']))
		{
			$_SESSION['aktiv'] = true;
		}


		if($_SESSION['aktiv'] == false && $_SESSION['cnt'] < 10)
		{

			echo '
					<h1> Welcome to BTH info login</h1>
					<form action="index.php" method="post">
					Username: <input name="name"
type="text" /><br/>
```

```
                                        Password:       <input          name="pass"
type="password" /><br/>
                                        <input name="submit" type="submit" />
                                        </form>
                        ';



        }

        if($_SESSION['aktiv'] == false && $_SESSION['cnt'] >= 10)
        {
                echo 'test klart<br>';
                foreach($delay as $key => $value)
                {
                        echo '# '.($key+1).' '.$value.'<br>';
                }
        }


        if($_SESSION['aktiv'] == true)
        {
                if(!isset($_SESSION['cnt']))
                {
                        $_SESSION['cnt'] = 0;
                }

                if(isset($_SESSION['cnt']) )
                {
                        //sleep($delay[$_SESSION['cnt']]);
                        sleep(0);

                }
        ;
                echo "Welcome to BTH info<br>";
                echo 'Test no. '.($_SESSION['cnt'] + 1);
                echo "<form action=\"index.php\" method=\"post\">
                        <input hidden=\"1\" name=\"logout\">
                        <input    name=\"submit\"    type=\"submit\"
value=\"logout\" />
                        </form>
                        <br>
                        <br>
                        LIFE AT BTH
                        <br>
                        <br>
                        Blekinge Institute of Technology (BTH) is
one of Sweden's most interesting and beautiful places for higher education! BTH is
also the most distinctly profiled institute in Sweden, thanks to our strong emphasis
on applied information technology and innovation for sustainable growth.
```

BTH was founded in 1989 which means that we are a young institute who manage education and research in new ways, but still with good quality.

The humanities, social sciences, management and health sciences are all integrated into an applied IT profile that enables technology and the humanities to develop in exciting new directions. Teaching and research at BTH are of a high international standard, with practical learning serving as the focal point for students, teachers and researchers. The emphasis on research, especially cutting edge research, in all our degree programmes is designed to preserve the vital link between education and research.

In addition to the large number of nationalities represented on the faculty level, international students from all over the world give us a truly international environment.

";

}

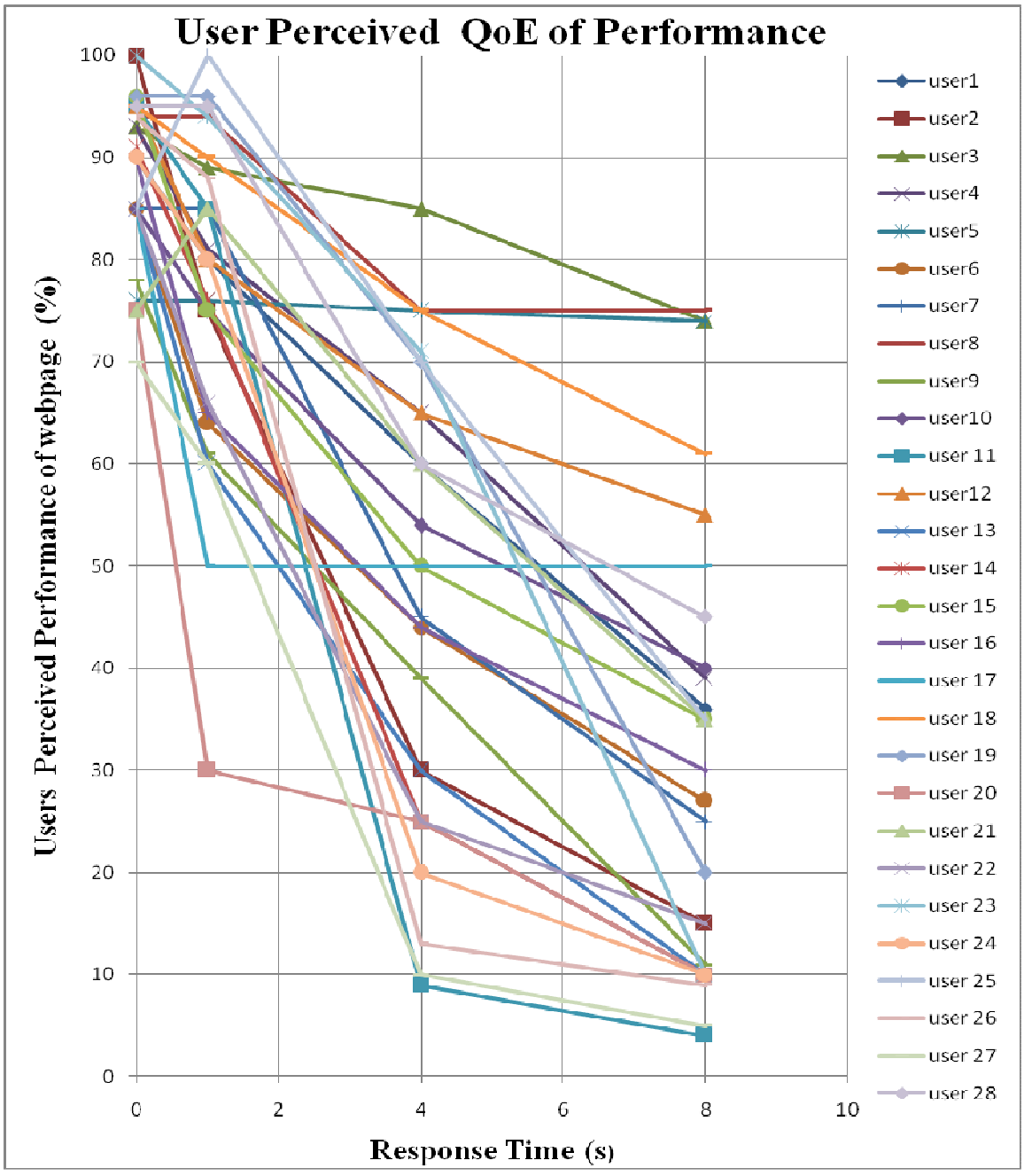
?>

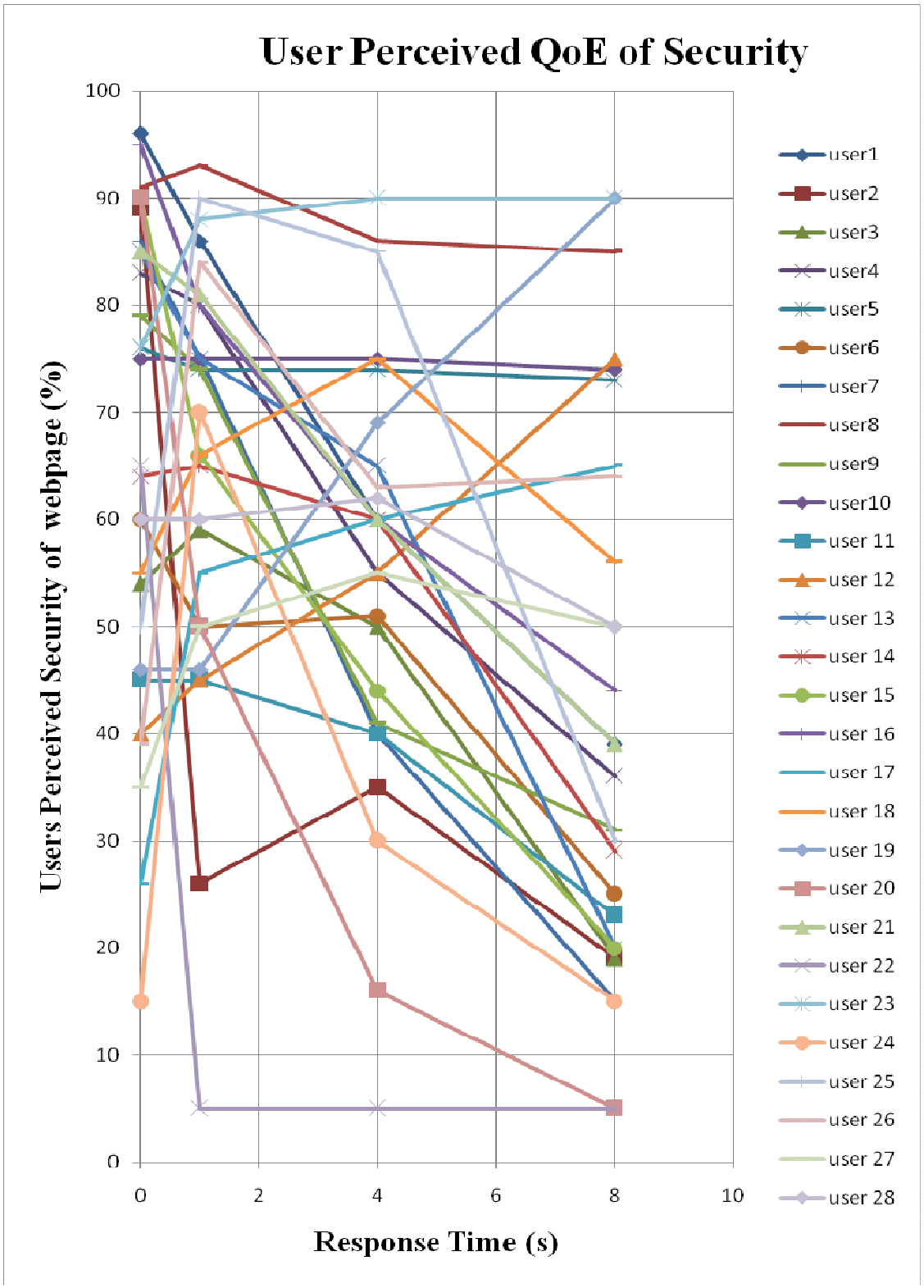
This is an experiment.Wajahat

</body>
</html>

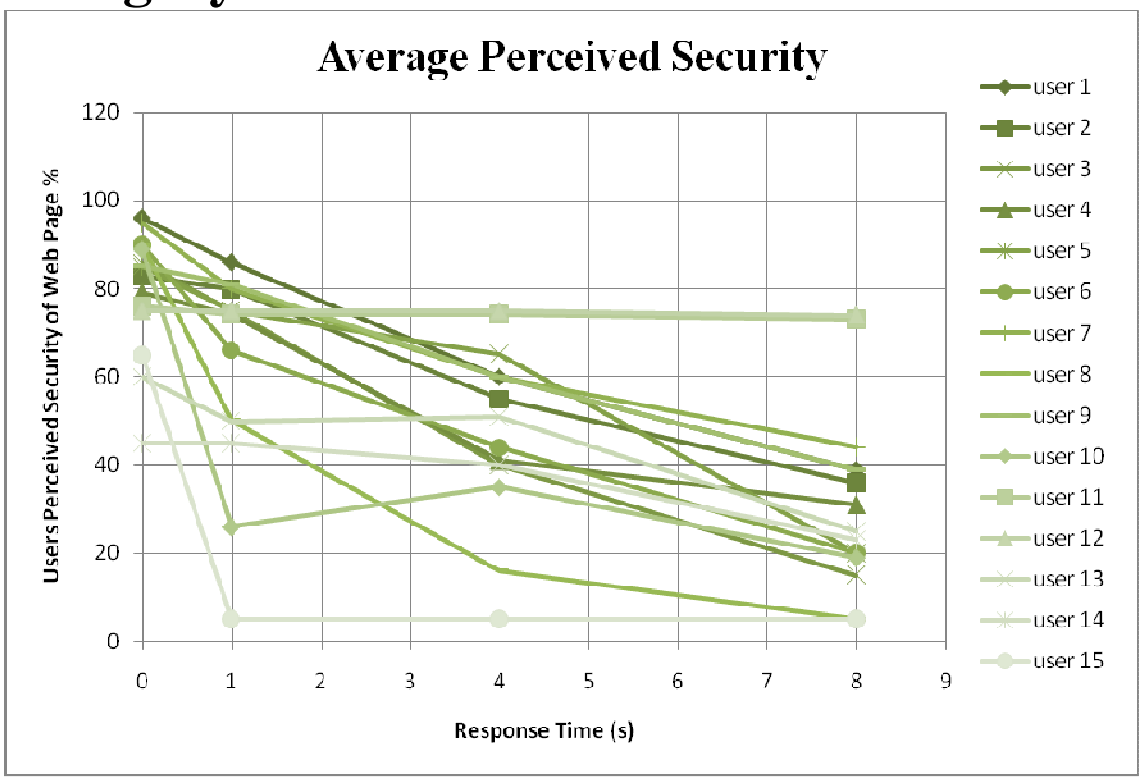
APPENDIX B
GRAPHS

Appendix B
GRAPHS

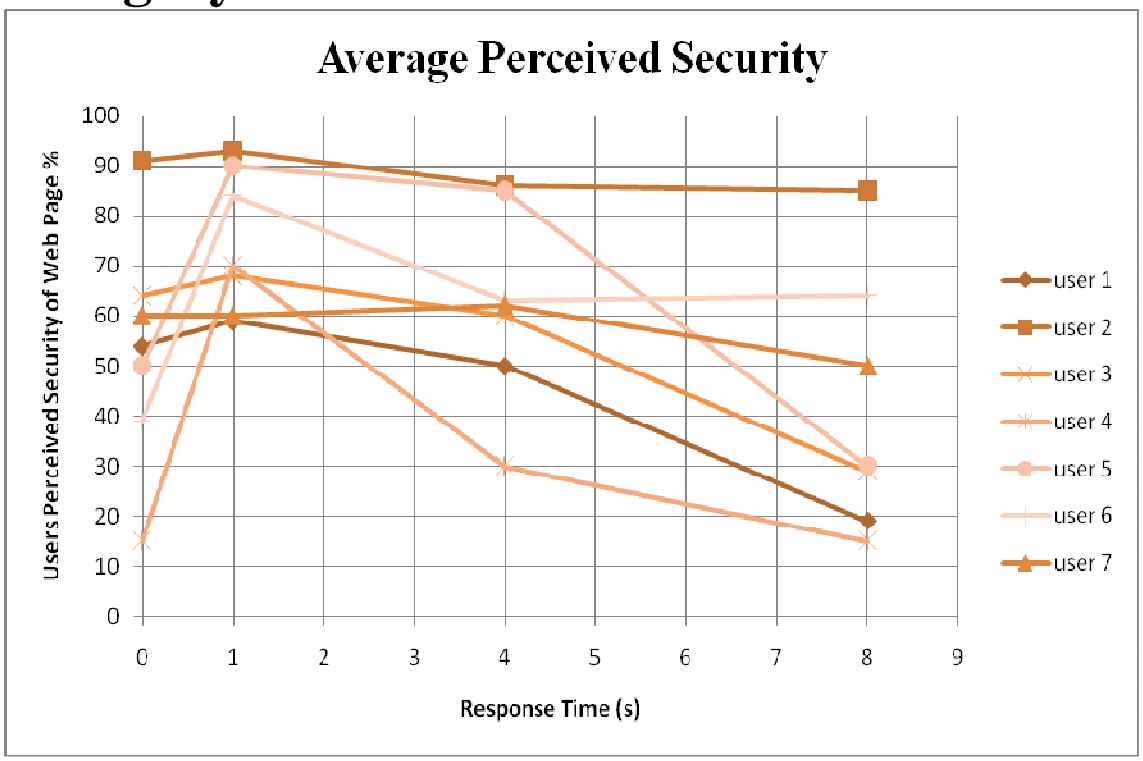



User Perceived QoE of Security
Users Perceived Security of webpage (%)
Response Time (s)
0
10
20
30
40
50
60
70
80
90
100
0
2
4
6
8
10
user1
user2
user3
user4
user5
user6
user7
user8
user9
user10
user 11
user 12
user 13
user 14
user 15
user 16
user 17
user 18
user 19
user 20
user 21
user 22
user 23
user 24
user 25
user 26
user 27
user 28

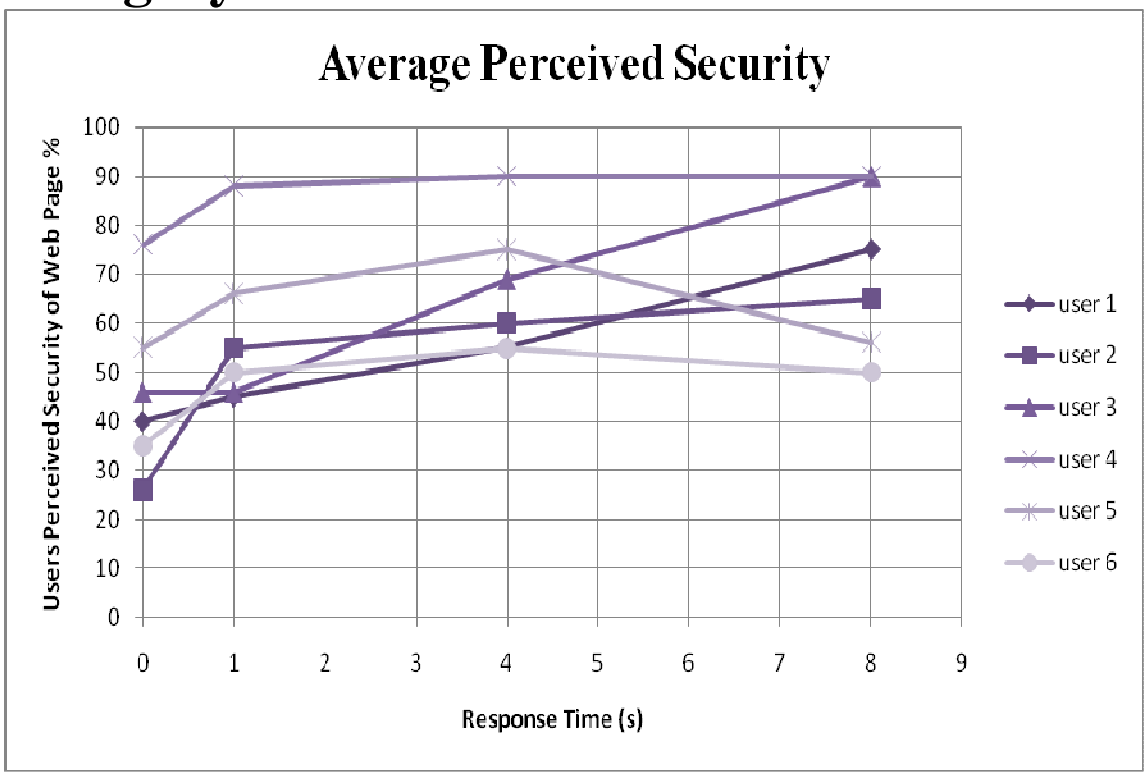
Category 1



Category 2



Category 3


Average Perceived Security
Users Perceived Security of Web Page %
100
90
80
70
60
50
40
30
20
10
0
0
1
2
3
4
5
6
7
8
9
Response Time (s)
user 1
user 2
user 3
user 4
user 5
user 6

APPENDIX C
SURVEY QUESTIONNAIRE

Appendix C
SURVEY QUESTIONNAIRE

Age:_____

Gender: Male / Female

Nationality: _____

Time Spent in Sweden: _____

University Program: _____

Internet Usage (Web Browsing)/Week (Hours): _____

Any education about security at university level?

Yes / No. If yes then how much? _____

For what do you use internet mostly?

Case 1

1. How would you rate the performance of this web page, considering response time?

Worst |- - - - - - - - - |- - - - - - - - - | Best

2. How would you rate your own perception of safety with regards to the response time for this web page log in?

Not Safe At All |- - - - - - - - - |- - - - - - - - - | Totally Safe

Case 2

1. How would you rate the performance of this web page, considering response time?

Worst |- - - - - - - - - |- - - - - - - - - | Best

2. How would you rate your own perception of safety with regards to the response time for this web page log in?

Not Safe At All |- - - - - - - - - |- - - - - - - - - | Totally Safe

Case 3

1. How would you rate the performance of this web page, considering response time?

   Worst |----------|----------| Best

2. How would you rate your own perception of safety with regards to the response time for this web page log in?

   Not Safe At All |----------|----------| Totally Safe

Case 4

1. How would you rate the performance of this web page, considering response time?

   Worst |----------|----------| Best

2. How would you rate your own perception of safety with regards to the response time for this web page log in?

   Not Safe At All |----------|----------| Totally Safe

Discussion