

Usability vs Security

1st Fatih Sofi

Computer Engineering Department
Gebze Institute of Technology
Kocaeli, Turkey
fsofi@gtu.edu.tr

2nd Mehmet Göktürk

Computer Engineering Department
Gebze Institute of Technology
Kocaeli, Turkey
gokturk@gtu.edu.tr

Abstract— This research is about comparing common authentication methods that we use on daily basis on usability and security. There are lot of web sites that use login pages to authenticate users so that it is crucial to make those sites secure and usable also. Adding more and more security features to the systems makes it hard to use [1]. With this research, we try to find an authentication method that users think it is easy to use and it is secure.

Keywords— usability, security, authentication, password, token, reCAPTCHA

I. INTRODUCTION

Usually in computer science, security and usability are considered in opposite situations. Trying to increase security can reduce availability, while increasing availability can reduce security. [1] Usability improvements seem to yield more easily compromised software and adding security measures seems to make software tedious to use or hard to understand.

A system designer must incorporate both goals throughout the design process. When security and usability are no longer treated as add-ons, the system designer can design them together to avoid conflicts.[2]

Due to their opposition to each other, it can be said that the usability will decrease in a system where all the actions that are important to safety and which may be necessary for security are taken or tried to be taken.

As an example, from Linux distributions. Consider the Ubuntu distribution. Xorg is one of Ubuntu's image servers, is trying to facilitate the use of this operating system by providing a visual interface to its users. Xorg clients connect to the Xorg servers, and it will give the interface to the client users. So, it can browse different opportunities for users to read articles, open pdfs and watch videos from an internet site. However, a vulnerability in Xorg can adversely affect the user. Due to a security issue with increased usability, when shopping online, a person may steal personal information, such as a credit card, for security risks.

Another issue that can be discussed is the authentication systems and mechanisms. Examples of authentication mechanisms used in computer and mobile systems are Kerberos Authentication, Token Authentication, Multi-Factor Authentication, Password Authentication etc.

Most authentication mechanisms are authenticated by username/mail and password. Although there may be changes in the processes running in the background, the authentication mechanism is tried to authenticate the user by using information that the user should keep in mind and should not share with others.

Once authenticated, the user can access a company's internal network, a database, a vehicle, structures, or resources with multiple authentication mechanisms.

The role of security usability here is how user authentication can be handled in the user interface, [3] and how an authentication system and security mechanism can be made available to the user. [4]

Let's think about identity management systems because many identity management systems focus primarily on user authentication. Web (online) identity management systems are complex systems with powerful features—and many potential vulnerabilities. They aim to facilitate the management of identifiers, credentials, personal information, and the presentation of this information to other parties. Some identity management systems offer time- saving features such as automated form-filling, simplifications such as single sign-on, or high-value reputations that can be leveraged across many sites. However, these benefits are often perceived as “secondary” benefits and are hard for users to value. Given that users tend to seek immediate benefits and find it difficult to value features that save time or may reduce risks in the future, the more obvious and immediate the benefit, the more likely it is to drive adoption. [5]

Users follow the path of least resistance. The flipside of maximizing users' benefits is to minimize the direct and indirect costs associated with identity management systems. For example, systems are more likely to be adopted if they're easy to download, install, and configure. This includes the authentication process and password interfaces, which must become as easy as today's standard login to success- fully compete. [the seven flaws of identity mang usability and security challenges]

When technology interferes with desired activities, users devise shortcuts, often undermining security in the process. [7] For example, users might share credentials or use multiple identities when they should only use one. Ironically, attackers are experts

in usability—they know how to exploit users’ lack of understanding and their tendencies to use shortcuts by developing social engineering attacks to steal identity information.

Talking about authentication and identity management, it is good to give more information about authentication methods that I used in this project. Password authentication, token authentication and Google’s reCAPCTHA are used in the experiment. Those are the most used, easy to implement authentication methods so that we see and use them lots of the time in daily life. [8]

II. SYSTEM USABILITY SCALE (SUS)

In 1986, John Brooke, then working at DEC, developed the System Usability Scale (SUS). The SUS has 10 items in it. [9]

To use the SUS, present the items to participants as 5-point scales numbered from 1 (Strongly disagree) to 5 (Strongly agree). If a participant fails to respond to an item, assign it a 3 (the center of the rating scale). After completion, determine each item’s score contribution, which will range from 0 to 4. For positively worded items (1, 3, 5, 7 and 9), the score contribution is the scale position minus 1. For negatively worded items (2, 4, 6, 8 and 10), it is 5 minus the scale position. To get the overall SUS score, multiply the sum of the item score contributions by 2.5. Thus, SUS scores range from 0 to 100 in 2.5-point increments. [SUS (System Usability Scale)]

Despite being a self-described “quick and dirty” usability scale, the SUS has become a popular questionnaire for end-of-test subjective assessments of usability. [SUS (System Usability Scale)] And we can use system usability scale for our experiment. After every attempt for log-in to the web page, asking users those ten questions and record their answers so that at the end of the experiment we can scale the usability of the authentication methods that we serve for users.

SUS has generally been seen as providing the high-level subjective view of usability and is thus often used in carrying out comparisons of usability between systems. Because it yields a single score on a scale of 0–100, it can be used to compare even systems that are outwardly dissimilar. This one-dimensional aspect of the SUS is both a benefit and a drawback because the questionnaire is necessarily quite general. [10]

After measuring the usability score of the system, we must make an analysis of the usability score of it. There needs to be an standard or some sort of research, experiment that we can look for and use those ranges for our experiments to tell that this system is more usable then the other. Based on different studies, the mean SUS score is around 68-70.5. If your score falls close to this range, you can assume that your website ‘s usability is about average. Another way to add meaning to your SUS score is to turn it into a percentile ranking. By comparing your results against hundreds or thousands of scores collected in other usability studies, you can contextualize your site’s performance relative to the rest of the web. So for example, an average score of 70.5 is in the 50th percentile (better than half of the sites tested) according to 500 websites. [11]

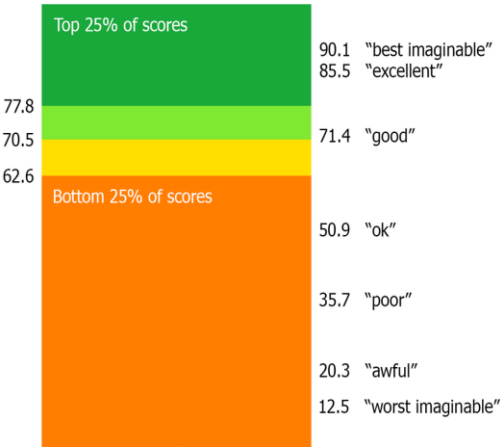


Fig. 1. System Usability Scale score meanings

There is the questions of the System Usability Scale and ratings that users can give when they experimented the systems.

	Strongly Disagree				Strongly Agree
1. I think that I would like to use this product frequently.	1	2	3	4	5
2. I found the product unnecessarily complex.	1	2	3	4	5
3. I thought the product was easy to use.	1	2	3	4	5
4. I think that I would need the support of a technical person to be able to use this product.	1	2	3	4	5
5. I found the various functions in the product were well integrated.	1	2	3	4	5
6. I thought there was too much inconsistency in this product.	1	2	3	4	5
7. I imagine that most people would learn to use this product very quickly.	1	2	3	4	5
8. I found the product very awkward to use.	1	2	3	4	5
9. I felt very confident using the product.	1	2	3	4	5
10. I needed to learn a lot of things before I could get going with this product.	1	2	3	4	5

Fig. 2. System Usability Scale questions and scores

III. CHOOSING AUTHENTICATION METHODS

Authentication has an important role in our world now. We can think of it as telling a system that who we are and have permissions to use its resource.

Authentication methods that I will compare and use in my experiment are password authentication, token authentication and Google's reCAPTCHA. Captcha is maybe not seen as an authentication method, but it is a type of security measure known as challenge-response authentication. [12]

During the Covid-19, most of the companies have started to work from home. This situation may change the authentication methods that we used to. Because people now tend to use more e-Banking and VPN more than before Covid-19. This will lead to need more secure authentication methods we have to use and more usable. For these reasons, we need to find balance between security and usability in authentication. Also, attackers (hackers) have more options for attack vectors to compromise users nowadays. Using physical authentication methods nowadays is not a logical method for authenticating users because most of the people working and buying things from their home. We need to use remote authentication methods but have to careful with them also.

Research from a software company attempted to find out what form of authentication is most trusted by the public. The clear message is that people don't trust biometrics for their day-to-day ecommerce and digital services interactions.

78% of those surveyed feel most comfortable using traditional passwords. Just 11% are comfortable about using iris recognition or retina scan. Only 42% of respondents were keen on fingerprint recognition, and surprisingly, just 31% comfortable with facial recognition. [13]

26% of people said that reCAPTCHA photo squares of bridges and traffic lights are most annoying. However, younger people were more likely to prefer reCAPTCHA photos to letters and numbers.

Passwordless authentication is a positive step forward for WFH (Work From Home) security and protecting corporate data but it isn't a panacea for every authentication need. Some apps are higher risk and shouldn't have passwordless, at least not as a standalone authentication source. Some applications, including anything connecting to a financial account or highly sensitive data, should still require 2FA or MFA, one of those can be a password. But overall, passwordless authentication will allow a better user experience for remote workers while keeping the network and data more secure. [14]

More reasons like those makes authentication more important during Covid-19. So testing if password authentication is usable for users or it is not an secure method for authentication is crucial. Also finding that reCAPTCHA is preferable for younger people is a good point to testing reCAPTHCA in my experiment. Additionally, token authentication is the other method for authenticating users and using software token authentication is more usable during Covid-19. Token authentication looks like similar usability for the people compare to the biometric authentication. [2] Also because of easy implementing, experiment with token authentication is a good idea to test in authentication methods.

IV. FUNDAMENTALS OF THE CHOSEN AUTHENTICATION METHODS

There are 3 types of authentication methods that are used for the experiment.

1. Password Authentication
2. reCAPTCHA Authentication
3. Token Authentication

Password authentication is an old method for logging to sites but it is still in use. Making the password authentication more secure, the easiest way is using long passwords that include uppercase and lowercase characters, also special characters. This will make the possible password space larger and harder to guess.

reCAPTCHA authentication is similar to password authentication. It only adds a mechanism that ensures no brute force attacks can be done. It is hard to use automation tools to make brute force attacks because those tools need to solve the reCAPTCHA.

The last one is token authentication which application generates a long and random token for user to log in to the system. It is really hard to guess those tokens and those applications mostly use up-to-date random libraries for generating tokens. It's security depends on the algorithm that generates the token.

We build a simple login page for users to test different authentication methods. After that, they can give scores about the authentication method that they use for usability.

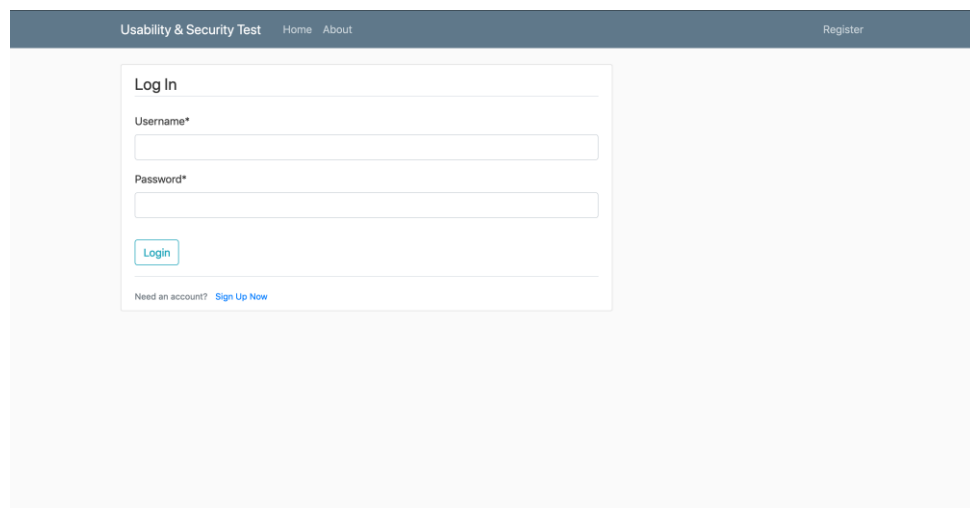
A screenshot of a web application's login page. The page has a dark blue header with the text "Usability & Security Test" on the left, "Home About" in the center, and "Register" on the right. The main content area is light gray. In the center, there is a white box with a "Log In" title. Inside this box, there are two input fields: "Username*" and "Password*". Below the password field is a blue "Login" button. At the bottom of the box, there is a link "Need an account? Sign Up Now".

Fig. 3. Password Authentication Page

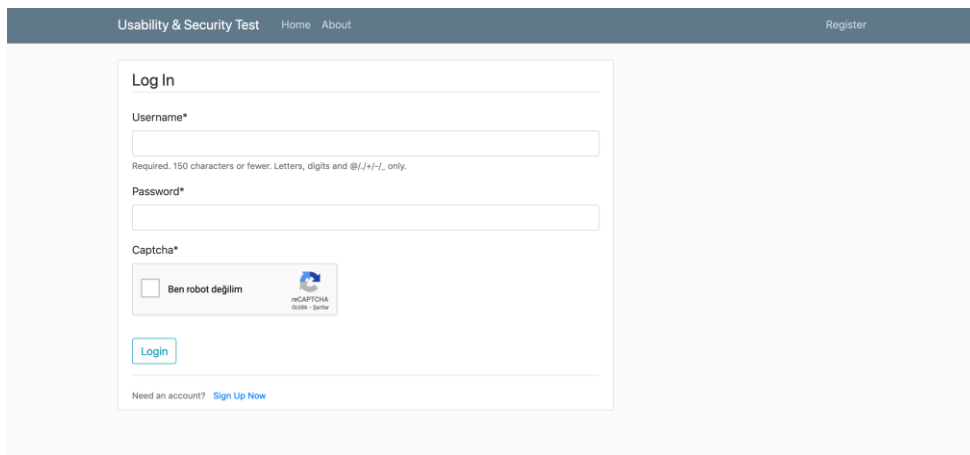
A screenshot of a web application's login page, similar to the one in Fig. 3 but with a reCAPTCHA challenge. The header and "Log In" box are the same. However, the "Password*" field is followed by a "Captcha*" section. This section contains a checkbox labeled "Ben robot değilim" (I am not a robot) and a reCAPTCHA logo. Below the checkbox is a blue "Login" button. At the bottom of the box, there is a link "Need an account? Sign Up Now".

Fig. 4. reCAPTCHA Authentication Page

Usability & Security Test
Home
About
Register

Token Generator

Key*

Create

Want to login with that token? [Login With Token](#)

Fig. 5. Token Authentication Page

V. USER'S OPINIONS

For diversity, we choose our users from males to females, technicians like computer engineers to business engineers and international relations degree. After the experiment, every user give their opinion about authentication methods and their usability. We use System Usability Scale to test usability. Also record age, gender and degree of the users. This test is done on 50 users.

User	Gender	Age	Degree	Auth Method	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
1	F	31	International Relations	1	4	2	5	1	1	3	5	4	5	1
1	F	31	International Relations	2	5	3	4	3	4	1	1	5	1	5
1	F	31	International Relations	3	3	5	3	4	1	5	2	5	4	3
2	M	34	Computer Engineer	1	1	1	3	1	1	3	3	1	1	1
2	M	34	Computer Engineer	2	1	4	5	1	5	3	1	4	3	5
2	M	34	Computer Engineer	3	3	4	3	5	3	3	2	4	5	1
3	M	40	Computer Engineer	1	2	1	5	1	4	1	5	2	3	3
3	M	40	Computer Engineer	2	1	5	2	4	5	3	3	3	4	2
3	M	40	Computer Engineer	3	3	4	1	5	3	4	4	1	2	4
4	M	37	Computer Engineer	1	1	1	3	1	3	2	4	5	3	1
4	M	37	Computer Engineer	2	5	3	1	5	4	3	3	3	1	3
4	M	37	Computer Engineer	3	1	3	1	4	4	1	2	4	2	4
5	M	26	Electric Electronic Engineer	1	2	2	4	1	3	3	4	4	4	4
5	M	26	Electric Electronic Engineer	2	1	5	3	3	3	4	5	1	2	5
5	M	26	Electric Electronic Engineer	3	5	2	4	1	3	5	1	4	5	2
6	M	25	Business Engineer	1	4	3	4	2	3	2	4	1	5	2
6	M	25	Business Engineer	2	4	3	3	3	4	1	3	3	3	3
6	M	25	Business Engineer	3	1	4	1	4	4	2	5	2	4	3

Fig. 6. Example of the SUS results

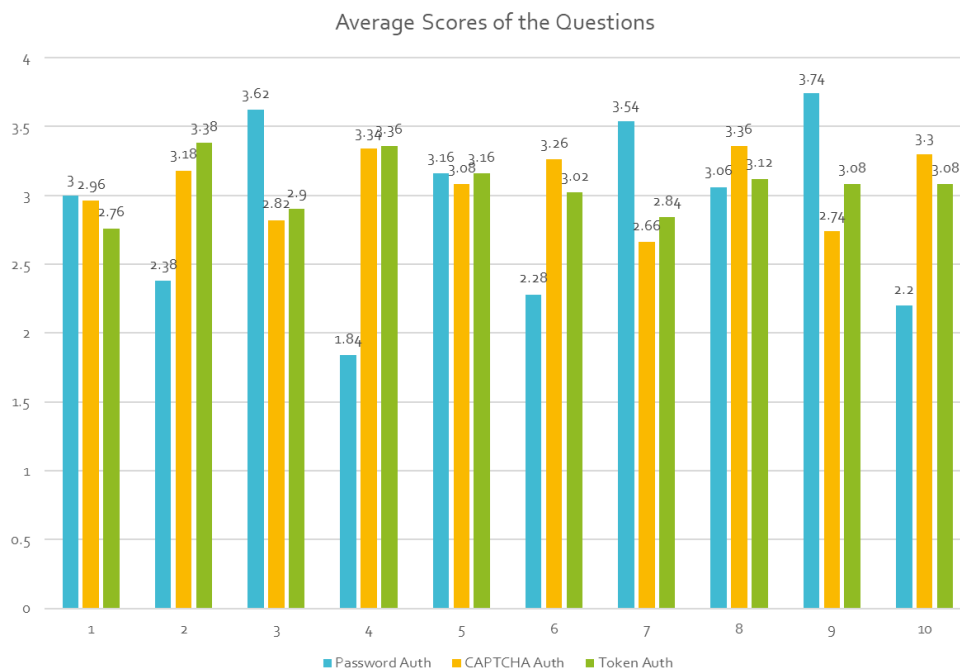


Fig. 7. Avarage Scores of the Questions

Feature/Acquisition Device	Passwords (PW)	PIN	Proximity card	One Time Generators	Challenge Response
Definition	Knowledge based 8 to 12 digits	Knowledge based 4 digits	Authentication Token	Authentication Token	Authentication Token
Advantages	Ease of deployment	Networkless	Last longer (contactless)	PW difficult to guess	No synchronization
Disadvantages	Can be forgotten	Can be forgotten	Theft Fraud, counterfeit	Brute force, dictionary attack	Users share their access permissions
Security	2	2	3	3	3

Fig. 8. Security score of the authentication methods

VI. CONCLUSION

In this research firstly, the definition of the usability and security are identified. Because we must know what we are going to compare. And secondly chosen topic, which in this case is authentication, is analyzed for usability perspective and security perspective. The users need an easy way of authentication but also it must be secure. Because of that this topic is important for all security interests and the users who want to use easy systems for their lives. We understand that password authentication is old and sometimes tricky, because users have to memorize all passwords for different kind of applications. Biometric authentication grows fast in security also in a fast and user-friendly manner.

REFERENCES

- [1] Kaında R., Flechais I., Roscoe A.W., "Security and Usability: Analysis and Evaluation", Oxford University Computing Laboratory J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
- [2] C. Braz, J.M. Robert, "Security and Usability: The Case of the User Authentication Methods".
- [3] Jøsang, A., Patton M.A., "User Interface Requirements for Authentication of Communication", Distributed Systems Technology Centre.
- [4] C. Braz, J.M. Robert, "Security and Usability: The Case of the User Authentication Methods".
- [5] A. Acquisti and J. Grossklags, "Privacy and Rationality in Decision Making," IEEE Security & Privacy, vol. 3, no. 1, 2005, pp. 26–33.
- [6] Nielsen J., "Usability 101: Introduction to Usability", (2012 January 4), Retrieved from <http://www.nngroup.com/articles/usability-101-introduction-to-usability/>.
- [7] A. Adams and M.A. Sasse, "Users Are Not the Enemy: Why Users Compromise Security Mechanisms and How to Take Remedial Measures," Comm. ACM, vol. 42, no. 12, 1999, pp. 40–46.
- [8] Retrieved from <https://www.idrnd.ai/5-authentication-methods-that-can-prevent-the-next-breach/>
- [9] Brooke, J.: SUS: A "quick and dirty" usability scale. In: Jordan, P. W., Thomas, B., Weerdmeester, B. A., McClelland (eds.) Usability Evaluation in Industry pp. 189–194. Taylor & Francis, London, UK (1996)
- [10] Retrieved from https://en.wikipedia.org/wiki/System_usability_scale
- [11] Retrieved from <https://www.trymyui.com/sus-system-usability-scale>
- [12] Retrieved from <https://support.google.com/a/answer/1217728?hl=en>
- [13] Retrieved from <https://www.cpomagazine.com/cyber-security/authentication-disconnect-between-sloppy-security-and-covid-19-fears/>
- [14] Retrieved from <https://securityboulevard.com/2020/07/covid-19-could-catalyze-passwordless-authentication/>