Vol.2017-SPT-22 No.11
2017/3/13

A Proposal of MusiAuth for Fallback Authentication

Da Sun[1,a)] Kanta Matsuura[1,b)]

Abstract: In this paper, conventional and newly proposed prevalent fallback authentication approaches focusing on web services have been reviewed. Furthermore, according to the unsolved problems - tradeoff between usability and memorability, left from the existing fallback authentication methods and the unique properties fallback authentication preserves, a new fallback authentication method MusiAuth based on those principles on web services has been proposed and explained. Experiments has been conducted as an individual interview for several times on different dates on 32 participants to evaluate the usability and security of the proposal. Besides, the duration of the experiments last from one day to three months in order to give a better memorability evaluation of the proposal.

1. Introduction

Fallback authentication is used to regain access to users accounts when the primary authentication fails, e.g., when the users lost their password or they have exceeded the number of authentication attempts. It is an indispensable aspect of real-world authentication solutions. In the meanwhile, with the uprising challenge to define distinct and secure primary authentication schemes, mainly the combination of passwords and usernames, primary authentication received a majority of attentions. However, successfully breaking the fallback authentication retrieves full access to users accounts just as breaking the primary authentication mechanisms. In terms of the concept that the security assessment of a whole system is based on the weakest point of the system, fallback authentication does not get enough rigorous consideration. As the minor improvement can contribute to a broad impact on the overall security, fallback authentication needs more attention, both on a conceptual and an implementation level.

This paper introduces and evaluates both the widely used fallback authentication schemes and the new developed fallback authentication mechanism on web services, and tries to come to an understanding on the requirements of future fallback authentication methods on web services. By discussing the left problems of those and the requirements of future fallback authentication methods on web services, the thesis introduces a new proposed fallback authentication method *MusiAuth* based on all the aspects we have analyzed. What 's more, in order to give a better evaluation of the proposal a series of experiments has been conducted as an individual interview for several times on different dates on 32 participants with duration of the experiments last from one day to three months. The rest of this proposal is organized as follows: Section 2 presents conventional fallback authentication methods that are deployed on web services in the real world. Then, Section 3 summarizes the existing problems of conventional methods, requirements of fallback authentication and proposes the idea of *MusiAuth*. Section 4 discusses the details of the experiments of the new proposed fallback authentication - *MusiAuth*. Finally Section 5 makes a conclusion about this proposal.

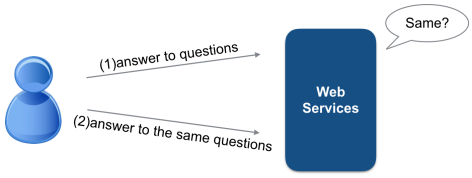

Fig. 1 Security Question Scheme

2. Conventional Methods

2.1 Security Questions

Security question, also refers as challenge questions, are commonly used to authenticate users who have lost their passwords. Details of security questions scheme has been shown in **Fig. 1**. It usually consists of two phases. Users have to provide answers to selected security questions in the first phase. This information will be requested in the second phase whenever password reset/retrieval is required. (e.g. forgotten passwords). These questions can either be fixed by the service providers or controlled or open[2].

2.1.1 Security Questions Review

Most of the security questions were assumed to be easy to remember by the user and hard to answer by others in the past. However, as personal information becomes ubiquitously available online, the questions that are easy to remember are often easy to guess, while the questions that are hard to guess are also hard to remember[1]. Thus, security questions come with numerous insufficiencies in terms of usability and security. In terms of security, many predefined security questions are researchable[4],

[1] Institute of Industrial Science, The University of Tokyo
[a)] sunday@iis.u-tokyo.ac.jp
[b)] kanta@iis.u-tokyo.ac.jp

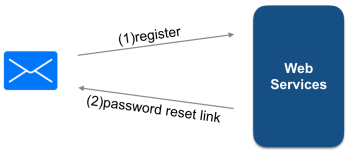

Fig. 2 Email-Based Identification Scheme

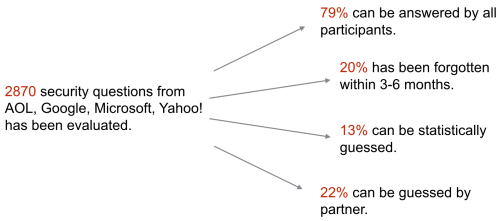

Fig. 3 Questions used by Top Four Webmail Service Providers

can easily be answered by close persons like family and friends or can even be guessed by choosing the most popular answers[3].

A total of 215 personal security questions from eleven online banking have been extracted and evaluated in the paper[1], arguing that today's personal security questions owe their strength to the hardness of an information retrieval problem. Though these questions vary widely, the paper defines six possible weaknesses in personal security questions based on the usability(inapplicable, not memorable, ambiguous) and security(guessable, attackable, automatically attackable) of the questions. The reason that the paper targets online banking to testify is because that banks are more motivated to improve their mechanisms to reduce identity fraud. By this token, common flaws found in online banking are rather representative of the broader topic of security questions.

After documenting the state of personal security questions in current use and analyzing those questions in the light of today's information-rich Internet, the surprisingly weak personal security questions, as currently used in fallback authentication in online banking, imply the same situation of the broader topic of security questions fallback authentication mechanism.

2.2 Email-Based Identification

Email-based identification is another commonly used method for fallback authentication. Procedures of email-based identification scheme has been shown in **Fig. 2**. Most service providers make users register an email address during account creation in case of password loss. This information is needed for the second phase when password reset/retrieval is required. A new password will be automatically generated and sent to the pre-registered email address. Some service providers do not bother to generate a new password, and simply email the old one. Other service providers facilitate password resets by sending users a reset link to the pre-registered email address. User will be able to create a new password by following that link. Authentication via email treats the ability to receive email at that address as a fallback authenticator.

2.2.1 Email-Based Identification Review

According to Simson Garfinkel[5], this approach works well, but comes with certain shortcomings. For example, the email address that the user has provided during enrollment might be out of date and thus, not accessible anymore. Furthermore, the security of email-based identification depends on the security of email servers and passwords[5]. However, email was developed when the Internet was a much smaller place to standardize simple store-and-forward messaging between people using different kinds of computers and it was not designed with any privacy or security in mind. Email was all transferred completely in the open: everything was readable by anyone who could watch network traffic or access accounts (originally not even passwords were encrypted)[6]. In terms of the fact that the vast majority of Internet email travels without cryptographic protection, someone or something could read or modify email without detection while the message is in transit. What's more, it is surprisingly easy for Internet Service Providers(ISPs) to get access to user's email since emails are physically stored without encryption at the ISPs. Key employees at many businesses can browse or perform keyword searches on users' mailboxes. Several commercial systems do just that—Yahoo!, for example, inserts advertisements into email messages and, perhaps more significantly, will alter email that appears to resemble JavaScript.

Given this lack of security, relying on email to prove identity or facilitate financial transactions seems unwise. However, due to speed and convenience issues, few people use encryption and most email remains unencrypted and insecure[7]. Therefore, for the foreseeable future, Internet users cannot expect email to be secure from prying eyes or interception[6].

In spite of the situations discussed above, an evaluation encompassed the security questions used by the top four webmail services - AOL, Google, Microsoft and Yahoo!, over four separate days, involving 130 participants(64 males and 66 females) from a wide age and relationship range has been done in [3] that measures the reliability and security of the security questions used by the four largest webmail providers. The measurement of the reliability and security of the webmail security questions has a primitive impact on the security of the webmail and on the reliability of the email-based identification. Because other kind of services may use email-based identification to fallback authenticate users, while webmail services can not do so because most of them has been used as primary email address and may not have another dependable email account for fallback authentication. Therefore, all four largest webmail providers rely on personal questions as the fallback authentication mechanism[3].

In total, 130 participants initially offer 2870 answers and 49 of them participating in the follow-up offer 1070 of those answers. Eventually, 21% of questions are either unable or unwilling to answer. 20% of the answers can not be recalled after 3-6 months. What's more, 13% of the answers offered by the questions are statistically guessable and 22% of the answer can be successfully guessed by partners. The details are showed in **Fig. 3**.

The categories showed in this study express part of the fundamental problems of security questions concluded in Section 2.1.1. In addition, from all the analysis and evaluation of email-

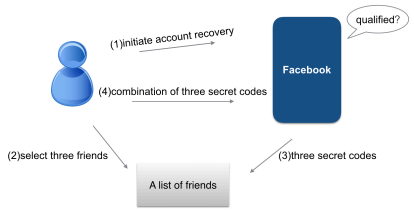

Fig. 4 Social Authentication Scheme

based identification we can assume that part of the vulnerabilities of email-based identification comes from the email infrastructure while the other part inherits from security questions fallback authentication.

2.3 Social Authentication

Social authentication takes advantage of the intuition that legitimate users are familiar with their friends while a strange is not. Social authentication is performed by selecting users social contacts and then either sending secrets to the selected contacts that allow users to reset password, or querying users about their contacts and preferences. With the rising of social networks, social authentication has been considered as a promising fallback authentication approach. As for the huge user-base and rich information of users including social graphs, Facebook is probably the most important example for a service provider using social authentication as a fallback authentication mechanism[8]. Facebook published fallback authentication based on social authentication called *Trusted Friends*(TF), also called *Guardian Angels*[9] in October 2011. Facebook decides whether the user is qualified to be offered the Trusted Friends authentication by an unknown algorithm after a user submitting an account recovery request. After being allowed to use Trusted Friends authentication, Facebook displays a list(size of 100) of friends each time for three rounds and the size of the list reduce in half every round after a friend is selected(no open information about how these friends are selected). Once the user confirms the selection of three friends, different four-digit secret codes are sent to each of those friends, by combination of which user can regain access to the account. The details can also be seen in **Fig. 4**.

2.3.1 Social Authentication Review

However, according to [8] in 2014, they have considered fallback authentication mechanisms deployed in practice on a number of social network sites and have broken the prime example of social authentication introduced by Facebook by novel attack *Trusted Friends Attack* that exploits the *POST-data* fields. *Trusted Friends Attack* is based on the idea of getting access to the secret codes required for account recovery by adding fake accounts to the victim's friends list.

In order to perform the attack, an attacker first needs one of the following information: email address, phone number, full name, or Facebook username(all of them are concerned as public information[1]) of the victim. Secondly, the attacker befriends the victim using three accounts that are already under control. According to the studies [10] that 50% of people will accept a Facebook "friend" or LinkedIn invitation from a total stranger. [8] confirms this by getting 8 out of 20 accepted all three friendship requests from sending three friendship requests to 20 users. Then the attack can start the password recovery process as we describe in Section 2.3. Finally, the attacker tries to select the three accounts that are under control by using POST data manipulation. The details of POST data manipulation is being discussed as follows.

POST Data Manipulation [8] circumvents the selection of users which restricted in 100 friends by a manipulation of POST data in a way the attacker has complete freedom in choosing the friends that were not even on the presented list of 100 users, which substantially weakens the security of the scheme and allows to easily use arbitrary fake accounts for account recovery. After contacting the Facebook security team, this problem is fixed, however, with POST data manipulation the attacker can still freely choose any user from full list every three round.

The study tests 250 accounts to evaluate the applicability of the Trusted Friend Attack, and 69 accounts are granted the Trusted Friends recovery. Furthermore, 58 accounts(84%) of these 69 accounts are successfully recovered by Trusted Friend Attack(23% of all accounts). This result represents a fair idea on how widespread this vulnerability is.

Table 1 Comparison

	Primary Authentication	Fallback Authentication
Longer Memorability		YES
Security	YES	YES
Time	YES	
Characteristics		Different Characteristics

3. Proposal of MusiAuth

3.1 Summary of Existing Fallback Authentication Methods

From the analysis of all the existing fallback authentication methods(security questions, email-based identification and social authentication), we can believe that the existing problem for security questions and email-based identification is the fundamental vulnerability of security question itself - the existing design of a set of security questions that does not solve the aspects we describe in Section 2.1.1 to achieve the best trade-off between usability and security, and also for social authentication is the lack of sophisticated countermeasures giving the huge user base.

3.2 Fallback Authentication vs. Primary Authentication

Here, we try to discuss some principles that fallback authentication mechanisms should follow in order to propose a new fallback authentication approach in compare with primary authentication. As we can see from **Table 1**, primary authentication does not consider memorability as important, however, fallback authentication considers the memorability and security as equally essential. And the other advantages we can use for fallback authentication is the loose time requirement and the characteristics that are different from those used for primary authentication of specific systems.

3.3 Primary Authentication vs. Associative Memory

As we can see, associative memory has not been used in the previous fallback authentication mechanisms. In order to make sure this idea has promising future to implement, we turn our attention to the relatively well researched and similar field - Pri-

mary Authentication, to see what associative memory idea in practice we can get access to. We will discuss two different use of associative memory in the following. Not both of them has the desirable results, however, both of them can be considered as milestones in the field of associative memory and have a great contribution to the process of proposing my idea of *MusiAuth*.

3.3.1 Using a Combination of Sound and Images to Authenticate Web Users

The idea of using a combination of sound and images to authenticate web users has been proposed in [11] for the first time. This idea is based on *Dual Coding Theory* [13] - Brain has separate mechanisms for remembering image-based information and for remembering verbal information. It is a functionally defined relation reflecting the probability that different units within the same memory system will activate each other.

The proposal assumes that an individual would make a visual association when a piece of sound is heard. And an experiment has been conducted in order to test this association between sound and image. Every each experiment requires participant selects five images from five different sets of 10 images when giving a random sound. These associations have to all be recalled afterwards to successfully authenticate users.

Unfortunately, these experiments failed because the time-consuming process of listening to the sound. Users merely memorized the images and did not listen to the sound.

3.3.2 Authenticating Me Softly with " My " Song

The proposal in paper [12] upgrades the idea of using a combination of sound and image to authenticate web users. This upgraded idea forces participants to memorize sound by removing the element of image from the previous proposal. In addition, based on the theory that music is universal all over the globe and humans have superior memory for music, this proposal replaces the random sound with random music. This proposal uses music to authenticate users and purely reports the experiences of the use of a musical password in the primary authentication research field.

The paper runs series of experiments asking participants to remember series of music for 52 days, involving 133 participants to test memorability of using music passwords. 133 participants vary by age.

In order to highlight the positive results of using music to authenticate users, the paper also runs the side experiments with the same group by asking them to remember textual password, which is the main primary authentication nowadays. After different days, participants are asked to come back to try to recall the musical password and textual password to compare the memorability impact. The results are also shown in **Fig. 5**.

Overall, musical password offers better performance with 48% more successful authentication. This proposal of using music as authenticator should be considered as a starting point of a possible implementation for an audible password.

3.4 The Proposal of MusiAuth

Though the idea of using music as authenticator has offered better performance considering security and usability, the biggest obstacle for implementing this idea in practice for primary authentication is the relatively high time costs. Even the participants of these experiments said that they enjoy using the system, but they did not seem to think it was practical in terms of the annoying time required to authenticate. However, in contrast to primary authentication, as we have discussed before, the time requirement for fallback authentication is more loose, which can be considered as an advantage. Here is where the proposal of *MusiAuth* comes into the picture.

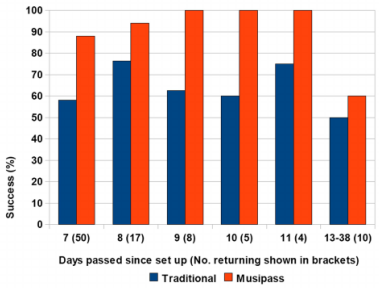

Fig. 5 Authentication results grouped by number of days passed since initiation

Table 2 Music Databases Categories

Pop	Rock	R&B/HipHop
Dance	Country	Blues
Jazz	Classical	Unspecified

Table 3 Preset Time Frame

Love You Like A Love Song	0:37 - 0:52
Need You Now	1:06 - 1:34
This Is How We Do It	2:40 - 3:01
Fall To Pieces	0:45 - 1:02
I Swear	0:47 - 1:06
Bring It On Home To Me	0:31 - 1:01
Always On My Mind	1:00 - 1:14
End Of The Road	1:17 - 1:37
Too Close	1:22 - 1:40

4. Experiments

4.1 Experiment Environment

(1) **Participants** There are 32 participants involved in the experiments. And they have been divided into 3 groups. There are 11 participants in the first group, 10 participants in the second group and 11 participants in the third group. All of the participant are aging from 20 to 30 years old.

(2) **Genre** The music used in the experiment has been categorized into different genres. Based on the idea that user will tend to be more active towards their favorite genres. So there are 9 genres used in the experiments as shown in **Table 2**. There are Pop, Rock, R&B/HipHop, Dance, Country, Blues, Jazz, Classical and Unspecified. Unspecified is for the participants who don't have a preference over music.

(3) **Music Databases** There will be four sets under each genre. And each set contains 9 options. So there will be 36 songs under each genre. 324 songs in total. And all the music are from music streaming service - Spotify[14].

(4) **Music Length** Each song will be preset a time frame during which is the strongest rhythm in the whole song to enhance memorability. The duration of the clips is set between 15 seconds to 30 seconds. The example of the preset time frame

as shown in**Table 3**.

4.2 Memorability Experiments

There are two main procedures during the memorability experiments, which are described as following,

(1) **Registration** Each participant has to register his/her musical password first - creation of musical password. In order to proceed to the creation of musical password, each participant has to choose their favorite genre out of nine categories. Then, participants enter the creation of the first piece of their own musical passwords. There are nine songs in the musical set and interviewee will play every song according to the preset time frame. Participants only need to listen to the songs and choose one of their favorite to be the first piece of their musical passwords. As the musical password consists of four pieces of music, participants have to do the same procedure as before for totally four times to finally create their own musical passwords. After this, the interviewee will record the musical password of each participant in order to continue the memorability experiments.

(2) **Fallback Authentication** In order to evaluate memorability of this proposal, this procedure is the most important step in the whole memorability evaluation. The procedure is almost the same as registration. Expect that participants will be directly given a series of sets of music without the selection of favorite genre. The participants have to recreate the musical passwords, and this time they are given three attempts. There will be signs of right or wrong during each selection. After the fourth time of selection, the new musical passwords are created. The interviewee will compare this new musical passwords with the one on the record to judge whether this fallback authentication is successful or not. Also the fallback authentication happens much more rarely than primary authentications. In order to give a better memorability evaluation of the proposal, there are totally four following memorability experiments conducted after the registration, which are in one week, one month, two month and three months. The procedures of each memorability experiment stay the same as described.

4.3 Security Experiments

Each participant is asked to attack one another participant. As they don't know each other really well, the attack is categorized as stranger attacks. After the selection on target, the procedure is the same as fallback authentication. They will be presented series of music sets and they will try to recreate the musical passwords under three attempts and the interviewee will judge whether it is a successful attack by whether the musical passwords are matched on file without exceed three attempts.

4.4 Usability Expriements

A usability evaluation is executed as Q&A session. Each participant has to answer a few questions from the interviewee. The details are shown in **Table 4**. For the questionnaire, participants have to select from different scales. For example, for the first question, as 1 being really easy, 5 being really difficult. And for the tenth question, participants can describe their concerns about *MusiAuth*.

Table 4 Usability Questionnaire

	Questions
1	Do you have difficulties in remembering security questions' answers?
2	How long can you recognize the music clips?
3	Do you think *MusiAuth* is easy to use?
4	How easy can you remember your musical password?
5	How much mental effort do you use to memorize your musical password?
6	Do you think the procedure is taking too much time?
7	How frustrated are you when you try to use *MusiAuth*?
8	How much do you like *MusiAuth*?
9	Will you use *MusiAuth* in your real life?
10	Do you have any concerns about *MusiAuth*?

Table 5 Memorability Experimental Results

	Attempts 1	Attempts 2	Attempts 3	success
One Week	22	10	0	32(100%)
One Month	17	13	1	31(96.88%)
Two Months	12	14	4	30(93.75%)
Three Months	17	9	2	28(87.5%)

Table 6 Security Experimental Attacks

Attacker	Target	Attacker	Target	Attacker	Target
101	107(F)	201	101(F)	301	306(F)
102	302(S)	203	206(F)	302	205(F)
103	111(F)	204	303(F)	303	106(F)
104	304(F)	205	304(F)	304	309(F)
105	305(F)	206	207(F)	305	105(F)
106	301(F)	207	211(F)	306	208(F)
107	207(F)	208	107(F)	307	201(F)
108	104(F)	209	210(F)	308	311(F)
109	101(F)	210	209(F)	309	105(F)
110	101(F)	211	308(F)	310	110(F)
111	203(F)			311	303(F)

4.5 Results

4.5.1 Results of Memorability Experiments

There are totally four sessions of memorability evaluation in the experiment: one week, one month, two month and three months after registration. Under each session there are three attempts each participant has to pass the fallback authentication. Even though the experiment will be counted as successful whichever attempt is matched, the paper still records how each participant performed under each attempt. The paper expects that all the participants can recall their musical passwords in one month, and the recall rate will drop a little in three months. Firstly, the details of the memorability evaluation experimental results is showed in the **Table 5**.

As the paper has concluded before that memorability forget rate in the existing fallback authentication methods is approximately 20% as shown in Fig. 3, while the memorability forget rate is reduced from 16% to 3.12% in one month and from 20% to 12.5% in three months as shown in Table 5 by the proposal of *MusiAuth*.

4.5.2 Results of Security Experiments

In total there are 32 attacks happened in the security evaluation experiments, and details of the attack target and success attacks are shown in **Table 6**. As shown in Table 6, there is only one attack considered as successful, which makes the attack successful rate of the proposal *MusiAuth* is 3.23%. Comparing with Fig. 3, the secure rate has been improved significantly from 13%

to 3.23%.

4.5.3 Results of Usability Experiments

Turns out that 60% of them have trouble memorizing the answers of security questions. And most of them can recognize the music clip immediately. In total, most of the response to the proposal is positive, although there are concerns about the proposal. Most of the words are related to the time-consuming problem and if the system is really in practical use how many musical passwords do I have to create.

5. Conclusion

Though the evaluation results of the proposal in the thesis performed well, more detailed study design and evaluation analysis is required.

First the proposal has good experiments results. There are three aspects can contribute to this. First, the participants used in the experiments are aging from 20 year olds to 30 years old. They are young enough to have a better memorability than general population. Second, the music is categorized into 9 genres which enhance the activity of memorability of each participant. Finally, the music clip is believed to be the strongest rhythm in the whole song that can enhance the results also.

On the other hand, there are also limitations and future work of the proposal need to be discussed. Firstly, although the time requirement for fallback authentication is loose, the time cost here is not acceptable in practice. Secondly, the music here is not universal enough and big enough for a bigger population. Last but not least, if this proposal ever in practice, too many musical passwords will disturb users ' mind, so how many musical passwords do we need in practice is remaining to be a debatable question.

References

[1] Ariel Rabkin.: Personal knowledge questions for fallback authentication: security questions in the era of facebook, *Proceedings of the 4th Symposium on Usable Privacy and Security*, ACM, pp. 13–23 (2008).
[2] Mike Just.: Designing and Evaluating Challenge-Questions Systems, *IEEE Security and Privacy Magazine*, Vol.2, No. 5, pp. 32–39 (2004).
[3] Stuart Schechter et al.: It's no secret. Measuring the security and reliability of authentication via "secret" questions, *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, pp. 375–390 (2009).
[4] V. Griffith et al.: Messin' with texas deriving mother's maiden names using public records, *Proceedings ACNS 2014*, pp. 91–103 (2005).
[5] Simson L Garfinkel.: Email-based identification and authentication: An alternative to pki?, *IEEE Security and Privacy Magazine*, Vol. 1, No. 6, pp. 20–26 (2005)
[6] Here's why your email is insecure and likely to stay that way (online), available from ⟨http://www.digitaltrends.com/computing/can-email-ever-be-secure/⟩ (accessed 2015-12).
[7] Email Privacy Concerns (online), available from ⟨http://consumer.findlaw.com/online-scams/email-privacy-concerns.html⟩ (accessed 2015-12).
[8] Ashar Javed et al.: Secure Fallback Authentication and the Trusted Friend Attack, *2014 IEEE 34th International Conference on Distributed Computing Systems Workshops*, pp. 22–28 (2014).
[9] Facebook Security Infographic (online), available from ⟨http://sophosnews.files.wordpress.com/2011/10/facebook-security-infographic.pdf⟩(accessed 2015-12).
[10] Robert Siciliano.: Fake Friends Fool Facebook Users (online), available from ⟨http://blogs.mcafee.com/consumer/fake-friends⟩ (accessed 2015-12).
[11] Jim Liddell et al.: Using a Combination of Sound and Images to Authenticate Web Users, *Proceedings of HCI 2003 Designing for Society*, Bath, UK (2003)
[12] Marcia Gibson et al.: Musipass: Authenticating Me Softly with "My" Song, *Proceedings of the 2009 workshop on New Security Paradigms Workshop*, pp. 85–100, New York, NY, USA (2009)
[13] Allan Paivio.: *Dual coding theory*. Imagery and Verbal Processes, New York. Holt, Rinehart & Winston (1971).
[14] Spotify, Wikipedia (online), available from ⟨https://en.wikipedia.org/wiki/Spotify⟩ (accessed 2017-2).