Quality and User Experience (2018) 3:8
https://doi.org/10.1007/s41233-018-0021-1

RESEARCH ARTICLE

A usability based approach to designing continuous user biometric authentication system

Dennis Mugambi Kaburu[1] · Julianne Sansa-Otim[1] · Kajumba Mayanja[2] · Drake Patrick Mirembe[1] · Tony Bulega[1]

Received: 21 June 2017

Abstract
The advent of the internet and associated technologies have revolutionized the way we live and work. Today, organizations both public and private rely heavily on information systems to deliver services. The quality and reliability of services delivered by these systems depends on controlled access to these information systems. In mission, critical systems like online examination and military intelligence, there is need to verify constantly the identity of the user throughout the session of interaction (referred to as "continuous user authentication"). Accordingly, researchers have proposed a number of approaches to address the issues of continuous user authentication. However, these approaches require user collaboration, which affects user performance on the core tasks in the business processes because of user task interruptions. Thus, the approaches have usability challenges. Continuous user Biometric Authentication systems have a usability score of the range 55–60% on a System Usability Scale (SUS) on average, interpreted in SUS score as poor. Therefore, this paper discusses the design of a non-intrusive continuous user biometric authentication approach, which aims at guiding the design of continuous user biometric authentication systems with SUS score above the range of 65% in relation to the context of the primary task in the business process. The cognitive approach proposed incorporates usability quality attribute in respect to the users' primary tasks on the system by applying results from cognitive psychology. The approach allows a designer to understand the impact of a particular re-authentication method to user performance and satisfaction in a continuous user authentication environment.

Keywords Usable-security · Continuous user authentication · Biometrics · System Usability Score (SUS)

Introduction

The advent of the internet and associated technologies have revolutionized the way we live and work. Today, organizations both public and private rely on information systems to deliver services. The quality and reliability of services delivered by these systems depends on controlled access to these information systems. Controlled access is undertaken using knowledge (something the user knows e.g. password), possession (something the user has e.g. token) or inherent factors (something the user is e.g. fingerprint). When a user has successfully logged-in, most information systems assume that the user continues to be the legitimate one. This type of access, (referred to as static authentication) is vulnerable in the sense that it only facilitates a one-off authentication judgment at the start of the session. An impostor can hijack a session and take control of the system after a genuine user has access granted. In mission critical systems like online examination and military intelligence, there is need to continuously verify the identity of the user throughout the session of interaction (this is referred to as "continuous user authentication") to mitigate the risk.

Continuous user authentication verifies a user validity repeatedly during a session. The verification uses user's stored pattern and the stored pattern aid in computation of the trust level. The purpose of the trust level is to accommodate users' behavior fluctuations and if falls below a particular threshold, the system locks itself or sends out a message to a security administrator. A continuous user authentication system still requires static authentication to grant users initial access or to prevent access after a user lock out due to low trust level. In a continuous user authentication system, it is desirable that the authentication process is transparent so

✉ Dennis Mugambi Kaburu
dennis.kaburu@gmail.com

[1] Department of Networks, Makerere University, Kampala, Uganda

[2] Department of Mental Health and Community Psychology, Makerere University, Kampala, Uganda

Published online: 21 June 2018

that the user focuses on the primary task of the system. To achieve, a transparency and non-intrusive way of continuous user authentication, behavioral biometrics is preferred. Behavioral characteristics require extensive user collaboration and hence their usability becomes a concern. A balance of False Accept Rate (FAR) and False Reject Rate (FRR) is required such that the system barely locks out legitimate users (FRR) and does not fall for masquerades (FAR). A usability issue can also arise when there is a failure of user identity recognition due to system limitations, insufficient sample size and insufficient number of features.

This paper contributes in the design of a non-intrusive continuous user biometric authentication approach, which aims at guiding the design of continuous user biometric authentication systems. The approach assesses the security of a business process in totality, as the main goal of the user is the system primary task. How to ensure that security is uncompromised while performing the user's primary task efficiently is the focus of the paper. The approach proposed incorporates usability quality attributes of efficiency, effectiveness and user satisfaction in respect to the users' primary tasks on the system by applying results from cognitive psychology. The rest of this paper is structured as follows. "Related work" gives an overview of usable security designs in biometric authentication approaches. Based on these findings, "Cognitive processing overview" gives development of the approach. Building on this we present our "Cognitive approach". The analysis of the approach occurs in "Validation study", followed by conclusions, limitations and future work.

Related work

In 2003, a multi-disciplinary group of researchers formed a working group called Human Computer Interaction (HCI-SEC) [1]. The group purpose was to bridge the gap between usability and security under the main goal of usable security. It focuses on designing and creating systems with usable security in order to offer users with a complete experience without worrying about security. Figure 1 shows the integration between security and usability that result into the interrelated security area.

There are three approaches for the HCI-SEC [2]. The first approach is concerned with building systems that work without considering usability during design, then applying usability by enforcing users to get to use the security mechanism. The second approach builds systems with design that encourage users to use the security mechanisms inventively and correctly, as usability is applied by encouragement. The last builds systems with learnability concern by teaching and training users about what they need to know to interact with security mechanisms properly and effectively. HCI-SEC research community has gradually been developing work

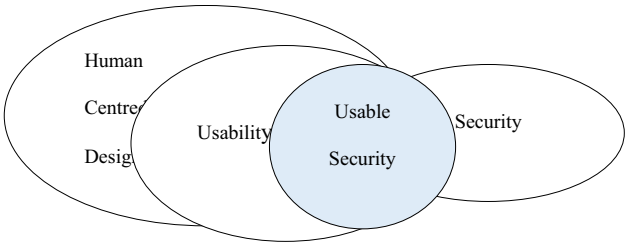

Fig. 1 Area of usable security

in usable security however continuous user authentication usable security research is limited [3]. Moreover, literature on usable security designs in continuous user behavioral biometric authentication is also limited. Table 1 is a summarized analysis of existing work in the area of usable security designs in biometric user authentication approaches.

A number of researchers [4–8] have done usability evaluations of continuous authentication systems that have usable security designs for biometric authentication approaches. Usability study on software systems is performed either by use of researchers' individual methods or the widely accepted System Usability Scale (SUS) [9]. The SUS, developed by John Brooke published in 1996 [9] is recognized as a "quick and dirty" survey scale that allows practitioners to quickly and easily assess the usability of a given product or service. The SUS comprises of ten questions rated on a five-point scale ranging from strongly agree to strongly disagree [9]. The questions consists of five positive and five negative statements. SUS provides a score that ranges from 0 to 100. SUS is a free of charge, effective tool for assessing the usability of a range of products and systems such as websites, cellphones. It provides a single reference score for a participants' view of product usability [10]. Based on [10], SUS score of over 80% would be considered best imaginable system, 70–80% excellent, 65–70% good, 60–65% OK, 55–60% Poor, 45–55% awful and below 45% worst imaginable. The Table 2 shows the SUS scores of user authentication biometric systems.

Table 2, shows that usability approaches for the design of continuous user authentication systems need more research for improvement. This is because the average range SUS score for the biometric continuous user authentication modalities is 50–60% score, interpreted in SUS score adjective rating as poor. Another reason for the low usability score is software security architects often have insufficient background in usability to design [2, 11, 12] in the early development phases of continuous user authentication lifecycle.

Our approach lets software designers model a proposed business process tasks, which includes the security re-authentication scheme in a continuous user authentication system and the cognitive resource constraint that describe their relationship. Using the approach, a software designer

Table 1 Summary of usable security designs in biometric authentication approaches

References	Features	Gaps
Mayron et al. [5]	Choice based authentication where there is synergy between usability and security. Users select authentication method from a group of authentication approaches to reduce cognitive load	The study gives guidelines to consider however, it does not address usability of a business process with security measures in place in the process and usability during continuous verification of a user while undertaking a business process task
Braz et al. [4]	The Model uses NGOMSL, technique to integrate usable security concerns earlier into the requirements and design phase of the development lifecycle	The model estimates how long it would take a user to complete a given task. However, it does not consider the impact of different mental and physical tasks have on subsequent tasks in a business process
Mihajlov et al. [6]	Provides a quantification approach that guides the evaluation process of authentication mechanisms in any environment by balancing usability and security The quantification criteria is based on [31]	The approach is untested in evaluation of usability and security. It is also silent on whether it can assist HCI/SEC designers to get a balance between usability and security in any authentication mechanism
Sasse et al. [7]	The researchers anticipates that biometrics in combination with security systems is suitable for user task and context configuration	The researchers recommends more research on usability issues of security mechanisms and techniques by having guidelines that take into account the specific constraints of security mechanism
De Marsico et al. [32]	The researchers implement FIRME (Face and Iris Recognition for Mobile Engagement) an embedded application for mobile devices. It is a biometric application based on multimodal recognition of iris and face	FIRME provides verification and identity management for different levels of security in a modular architecture. Questionnaires administered to users show user acceptance, ease of use, reliability and adequate of privacy and security However, the researchers recommend more design of multi-biometric recognition to address different hardware performance of devices and sensor especially when it cannot be anticipated in advance which biometric trait would provide the most reliable responses
Schiavone et al. [8]	The researchers undertake a usability study for a multimodal biometric continuous authentication system using face, fingerprint and keystroke modalities	The researchers have undertaken usability testing on the individual modality of face, fingerprint and keystroke subsystems and an integrated system with the three subsystems. The analysis show that the integrated system is usable with a lowered false rejection rate (FRR) of 0.61% as compared to individual subsystems due to trust score computation. However, the researchers did not explore the cognitive walkthroughs to guide in the design process. 25% of users had unexpected expirations of their sessions when undertaking the test, which may result to user frustrations
Crawford et al. [33]	The researchers presented a framework for transparent, continuous authentication on mobile devices using behavioral biometrics that identify the device owner. The study uses keystroke and voice biometric modalities	The framework was tested in a simulation environment. The study showed that a legitimate device owner could perform all device tasks while being asked to authenticate explicitly 67% less often than without a transparent authentication method. The tests show that implicit authentication on mobile devices improves usability than explicit authentication. the authors recommend usability study of the proof of concept implementation to identify ways of improving the framework
Toledano et al. [34]	The researchers designed a distributed platform to perform empirical evaluations of finger print, voice and signature commercial biometric identity verification systems	The paper promotes user-centered design and evaluation of biometric technologies. The authors acknowledge that there is a lack of studies devoted to the evaluation of biometric identity verification technologies from a user-centered perspective and biometric technologies are mostly measured on their effectiveness i.e. False Match Rate, False Non-match Rate and Failure To Enroll Rate measurements rate. However, there is failure to provide insights into other usability dimensions such as ergonomics, privacy, efficiency and satisfaction. From the study, the authors observed that Average Number of Capture (Imposter or Verification) failures were equal or over 0.333, which implies that one in every four biometric captures results in failure. Hence, the authors recommend more research on user centered biometrics design approaches

Table 2 SUS percentage scores of user authentication biometric systems

User authentication system	Biometric modalities	SUS score (%)	References
Smart phone continuous user authentication	Use of touch movements	68.33	Buriro et al. [35]
Smart phone continuous user authentication	Voice + fingerprint	64.59	Ruoti et al. [36]
Smart phone user authentication	Voice recognition	66	Buriro et al., [35]
Smart phone user authentication	Voice + face recognition	46	Trewin et al., [37]
Smart phone user authentication	Voice + gesture	50	Trewin et al., [37]
Online banking platform.	Public key encryption + password keystroke	65	Ruoti et al., [36]

Table 3 Cognitive memory mechanisms [16]

Cognitive memory mechanisms	Role
Visual working memory (VWM)	Holds, processes and operates on information of immediate importance
Procedural memory (PM)	Stores and prepares motor action sequence and any sequenced action
Declarative recall (DR)	Generates and presents stored information on demand
Semantic recognition (SR)	Determines whether factual information has been stored in memory
Episodic recognition (ER)	Determines whether information about experienced events have been stored in memory

will quantitatively compare alternatives; recommend combinations that minimizes the cognitive load and usability deficiency for the end user. The next section describes the cognitive process overview that aids in the development of the approach.

Cognitive process overview

Cognitive process describes a series of cognitive operations carried out in the creation and manipulation of mental representations of information. It includes perception, learning, attention, reasoning, synthesis, emoting, rearrangement and manipulation of stored information, memory storage, retrieval and metacognition [13]. Two fundamental processes that underlie human reasoning and decision-making are attention and memory [14]. Attention is how the brain consciously or unconsciously selects information for cognitive processing. Human memory is the capacity to encode, store and retrieve information.

We use the memory storage, retrieval and metacognition to develop the approach. However, the disruption of a task in addition to affecting the manipulation of memory it also affects attention, reasoning and synthesis of cognitive processes. Memory storage, recall and retrieval is an area of research field in cognitive neuroscience and experimental psychology. Human behavior is highly adaptive and flexible in response to changing environmental demands [15]. This flexibility requires cognitive control processes, which allow humans to not only respond reactively but also to behave in a more proactive way to achieve goals and to perform tasks. Based on the principles in cognitive theory [15, 16] reordering of tasks can have an effect of usability. When a person switches from one task to another, the brain re-organizes and re-allocates cognitive resources i.e. memory to ensure efficient transition. Task switching results in a performance deficit when a person disengages from an continuous user cognitive mechanism to a different mechanism in order to match task demands [16]. The performance deficit affects decision making which leads to loss of attention, reasoning and working memory. An example is in mission critical systems like online examination, a student is undertaking an online exam and in the process, a prompt appears for re-authentication. There will be some level of degraded performance of the primary task because the brain will switch to the re-authentication process. The student will have disruption of the decision making process which leads to loss of cognitive processes such as attention, reasoning and becomes irritated. Memory has the conscious ability to switch between task sets, contexts and intentions [17] and has specialized mechanisms within the brain where task switching occurs in the brain described Table 3.

The cognitive memory mechanisms represented in Table 3 are for empirical basis. The taxonomy of mental processes are an open area of research [18]. The time to complete a given tasks are predicted by models such as Keystroke Level Model-Goal Operators Methods and Selection rules (KLM-GOMS) [16, 19] and assessment technique Cog tool [20]. KLM-GOMS [16] predicts task times based on a set of mental and physical operators such as thinking time, button clicks, keyboard to mouse movement and keystrokes. Each KLM operator is assigned a time based on empirical research. This technique is useful in determining how long it would take a user to complete a given task. Cog tool [20], an interface prototyping tool uses a human performance model to assesses task completion times and learning rates based on shifting visual attention and motor responses. It evaluates how efficiently a skilled user can do a task on a design.

In the paper, we develop an alternative design approach by assessing the differential cognitive demands of different tasks with specific reference to user re-authentication in a continuous user authentication environment. Our approach assesses the re-authentication methods in the context of the primary tasks that constitutes users' main goal. From users perceptive, distractions originating from an imposed re-authentication mechanism leads to a lack of focus and loss of attention to the activity performed in primary task. We used cognitive theory to develop our approach built around usability in designing a biometric continuous authentication system described in the next section.

Cognitive approach

This section discusses a cognitive approach in designing a non-intrusive continuous user biometric authentication system. We also demonstrate its applicability in an online assessment business process in a Mak Online Coursework Learning Management System.

When one switches from one task to another, the brain re-organizes and re-allocates cognitive resources to ensure an efficient transition [15]. Transitioning from a task that uses resource A to a task that is using resource B instead of continuing with resource A results in performance deficits or switch costs. Similarly, in continuous authentication, disruption of the primary task when using resource A to re-authenticate using resource B, then continuing with resource A will also result in performance deficits. The switch costs of the security measures such as password or finger print authentication in a continuous authentication system are dependent on the business process tasks.

A recent study [21] found that authentication creates a 'wall of disruption" in users' primary work which, creates additional time for the secondary task and the resumption of the primary task after disruption. The cost depends on how the re-authentication mechanisms occurs on the users workflow, the function in the brain affected, and the primary tasks the user was doing before re-authentication. Task switching occurs when an individual disengages from one active cognitive mechanisms and then engages in another cognitive mechanisms in order to fulfil the task demands. In experimental psychology [15], these transitions, referred to as switch cost asymmetries, occur depending on the characteristics of the involved tasks. We collected these task asymmetries, expressed in Cohen *d* effect size, a metric in psychology for comparing the mean of two samples [22–24] to that of another as shown in Eq. (1) into a collection of rules that may be encoded as constraints in a weighted constraint satisfaction problem. The samples size comprised of nineteen subjects [22], forty-eight, twenty-eight of them female, mean age 24.35 years [23], and twelve subjects [24]. The samples compared the averages of different one cognitive mechanism to another in the same sample size. We classified the cognitive mechanism were each numerical value falls by assessing the similarity to documented cognitive tasks [22–24]. An example is assessing the geometric attributes of three dimensional shapes activates the visual working memory [25]. We obtained empirical measurements of reaction time in various task switch contexts that assessed the efficiency with which individuals were able to transition between different cognitive systems as shown in Table 4. The rules were constructed using available literature on switch cost asymmetries [15, 22–24] on cognitive resource transitions. These transitions occur when one disengages from an active cognitive mechanisms and then engages in another cognitive mechanism to fulfill a task demand, it results in loss of time and hence performance deficit [15]. The cognitive resources demands for individual subtasks takes place in cognitive mechanism shown in Table 3.

$$\partial = \frac{\mu_2 - \mu_1}{\sigma}, \tag{1}$$

where ∂ is the population parameter of Cohen's d,$\sigma_1 = \sigma_2 = \sigma$ i.e. homogenous population of variances and μ_i is the mean of the respective population.

The Table 4 shows the reaction time expressed in Cohen's d effect size. A Cohen's d effect size in the range of 0.2–0.4 signifies that the effect size is small and is not noticeable to the user. A task switch of 0.5 constitutes a medium effect size which has an average impact on the performance i.e. a person can view the impact of performance in the naked eye. The range of 0.8 and above signify large effect size, which implies that the performance of the sequence of switching tasks is noticeable. Continuous authentication takes place during a user interaction in a business process. A business

Table 4 Cost of switching between tasks using different cognitive mechanisms

FROM	TO				
	VWM	PM	DR	SR	ER
Visual working memory (VWM)	0	0.495 [25]	0.495 [25]	0.495 [25]	0.157 [25]
Procedural memory (PM)	0.495 [25]	0	0.495 [25]	0.699 [25]	0.699 [25]
Declaration recall (DR)	0.495 [25]	0.495 [25]	0	0.482 [26]	0.482 [26]
Semantic recognition (SR)	0.495 [25]	0.842 [25]	1.078 [26]	0	0.433 [27]
Episodic recognition (ER)	0.307 [25]	0.842 [25]	1.078 [26]	0.354 [27]	0

process has a sequence of tasks and a user does each task at a time. We encode the cognitive task switching costs for biometric continuous authentication workflow as a weighted constraint satisfaction problem [26] in which there are a set of values, variables, and constraints. A business process workflow is broken down into a sequence of tasks done in a linear fashion. Transitioning from one task to another carries a task switch cost. The total usability of an overall business process is a combination of the costs of the individual tasks and the cost of pairwise transitions between the tasks in a linearized sequence. The order in which business process tasks appear in a business process may have an overall effect on usability. Constraint Satisfaction Problem addresses this by ensuring that there are hard constraints that enforce partial ordering of tasks and soft constraints that capture cost of cognitive switching between tasks.

Constraint satisfaction problem (CSP)

The goal of a constraint satisfaction problem (CSP) assigns values to a set of variables subject to a set of constraints [27]. CSP consists of a set of variables (e.g. procedure), a domain of values (e.g. tasks) for each variables and constraints (e.g. cost task switching). The constraints specify which combinations of value assignments are optimal. A solution is an assignment of values to each variable such that all the constraints are satisfied. CSP is defined as a triple (V, D, C) where; V is a set of variables $x_1, x_2 \ldots, x_n$, D is the union of the set of domains $D_1, D_2, \ldots, D_n$, where D_i is the domain of the possible values for variable x_i .C is a set of constraints on the values of the variable that can be pairwise or k at a time. The state of CSP is defined by variables x_i with values from domain d_i and the goal is a set of constraints specifying allowable combinations of values for subset of variables.

Valued CSP (VCSP)

The constraints in classical CSP are "hard" meaning it has to satisfy every solution, which should equally be good. Several variants have emerged to extend the classical CSP framework [27, 28] to include "soft" constraints expressing priorities, preferences, costs, and probabilities. An example is assigning continuous authentication to biometric authentication mechanisms, which is a hard constraint. However, determining the choice of which biometric mechanism to apply to improve usability of the continuous authentication system is a soft constraint. The use of the soft constraints in a constraint satisfaction problem is referred to as Valued Constraint Satisfaction Problem (Valued CSP) [28]. We model soft constraints by use of cost functions, which assign particular costs to variable assignments. A valued CSP [28] is a constraint network extended by global cost function as shown in Eq. (3). Given a set of variables $V = \{v_1 \ldots, v_n\}$, a set of real valued functions $F_1 \ldots F_m$ over scope $s_1 \ldots s_m$ $(s_i \in V)$ and assignments a over V.

We represent the global cost function F as;

$$F(a) = \sum_{j=1}^{m} f_j(a), \tag{2}$$

where $f_j(a)$ means f_j applied to assignment a restricted to the scope of f_j i.e. $f_j(a) = f_j(a[s_m])$.

A VCSP is a 4-tuple $Z = (V, D, C_h, C_s)$, where (V, D, C_h) is a constraint network (elements of C_h are hard constraints and $C_s = \{f_1 \ldots, f_m\}$ is a set of real valued functions defined over scopes $s_1 \ldots, s_m$ (elements of C_s are soft constraints). A solution to VCSP given by tuple $Z = (V, D, C_h, C_s)$ is an assignment a^* that maximizes (minimizes)$F(a)$ among all assignments a that satisfy $\{V, D, C_h\}$.

In VCSP, the task is to find the optimal solution with a complete assignment at a minimum total cost.

Integration

We represent our approach as a valued Constraint Satisfaction Problem. Valued CSP is represented by a 4-tuple $Z = (V, D, C_h, C_s)$. In the approach a business process with p procedure, where 1 is the first procedure undertaken by a user and p is the last is denoted by a set of variables.

$X = \{x_i, x_2, \ldots x_m\}$. The domain D is the set of values assigned to variable x_i and consists of all tasks as well as authentication tasks in the business process. Continuous re-authentication tasks are part of a business process. The constraints c_h ensures there is adherence to the relations between tasks and C_s represents soft constraints of the cost of switching between tasks.

Business process

We apply the principles of task switch cost asymmetry to the Learning Management System (LMS) online assessment process workflow. An assessment is a significant driver of student learning and is a critical business process in an academic organization and hence, continuous authentication is required to verify the authenticity of a distance learner during e-assessment sessions. We identified the cognitive resources that are likely to be engaged in the subtasks of online assessment process workflow. This is the first estimation however in future empirical methods to verify these predications will be undertaken. Many different cognitive mechanisms are simultaneously engaged in real world tasks. However, for the study, we have selected the dominant resource, predicated to have the highest relative engagement level. It is impractical to determine the specific brain

Table 5 Online assessment business process subtasks and corresponding primary cognitive resource

Online assessment business process subtasks	Primary cognitive resource
Login (password)	Declarative recall
Select course	Semantic recognition
Select assessment and start assessment	Semantic recognition
Undertake assessment	Episodic memory
Static re-authentication (when trust level is below threshold)	
Submit assessment and feedback	Semantic recognition

networks activated for a specific real task; hence, we have characterized each task by assessing its similarity to documented cognitive tasks. For example, we asked participants to write an essay about one past experiences on the first day at university. This is similar to documented tasks involving ecphoric processes experiments in which the material that is to be remembered is held nominally constant and in which both the encoding conditions and retrieval conditions are systematically varied, a task that activates episodic memory [29].

Table 5 shows the major cognitive resource assigned to each business process subtasks on an online assessment. Login is assigned a primary cognition resource of declarative recall because of the stored password is retrieved on demand. Select course, select assessment, start assessment, submit assessment and feedback fall in semantic recognition cognitive resource because LMS user interfaces use the principles of paradigm design to create familiarity to end users. In many LMS, the procedures are the same and therefore, becomes general knowledge of the steps to undertake to begin an assessment. We assigned the undertaking of assessment subtask as an episodic cognitive resource since the questions participants responded to during validation section relates to their personal experiences about their first day of admission at the university.

The static re-authentication mechanisms occurs when the trust level from the authenticated student is low. This occurs because of variability of the behavior of the student between the registered profile obtained during enrollment, and the profile from the testing phase. Re-authentication takes place to ascertain that the authenticated student is the rightful person in the session. We re-authenticate using either fingerprint, password or face recognition which, have corresponding primary cognitive resource as procedural memory, declarative recall and visual working memory respectively.

Implementation of the approach

We used python constraint module to implement Valued Constraint Satisfaction Problems (VCSP) over finite domains to the online assessment business process of a LMS. The implementation of our model is in Numberjack [30], a Python framework for constraint programming. Numberjack framework includes support for Toulbar2, an exact combinatorial optimization tool designed for solving Weighted Constraint Satisfaction Problems also referred to as Cost Function Networks (CFN).

As shown below, a Numberjack *VarArray* is used to represent each step in the business process. The domain of each variable is in the natural numbers $0 \ldots s$ where each value represents one of the possible tasks. A constraint is added to the model to ensure that each value in the domain is assigned to exactly one variable as shown below.

```
from Numberjack import VarArray
    # create a variable array, one variable for
    # each step in the business process
wcspVars = VarArray(0, s, nsteps
model.add(AllDif(wcspVariables)
```

We then create a custom Numberjack constraint to enforce partial ordering of tasks. The constraint shown below ensures that for all combinations of the variables in the CSP it is never the case that the value after is assigned to a variable that precedes a variable assigned the value before.

```
classOrder(predicate);
def _init_(self, vars, before, after);
    Predicate_init_(self, vars, ''Order'')
    self.set_children(vars)
    self.before = before
    self.after = after
    self.lb = None
    self.ub = None
    defdecompose(self);
        return[(x! = self.after)|(y!
 = self.before) for x, y in combinations
(self.children, 2)]
```

As defined in "Valued CSP (VCSP)" section, a constraint $c \in C$ is a pair (D_c, F_c) where D_c is its scope and F_c is a cost

function. We model the task switching costs as binary constraints i.e. their scope is limited to variables that are immediately next to each other. We represent the task switching costs by a s-by-s matrix (where $s = |S|$).

```
   from Numberjack import PostBinary
def pairwise(iterable);
   a, b = tee(iterable)
   next(b, None)
   returnizip(a, b)
      #s − by − smatrix
      #binaryCost [s1], [s2],
      # specifies the cost of assigning s1 and s2
      #to variables that are immediately next
      # to each other
binaryCosts = [...]
   for var, varNext in pairwise(wcspVars);
   model.add(PostBinary(var, varnext, binaryCosts))
```

Results of the approach

Table 6 shows the solution of the VCSP problem. The three columns (online assessment tasks A, B, C) have different re-authentication mechanisms for the online assessment business process namely, finger print, knowledge based (password) and face recognition respectively. The three columns of the table correspond to the three different authentication tasks we are considering. The cost reported for each workflow is the sum of individual subtasks switch cost (effect sizes) for the online assessment tasks A, B and C. The fact that the three orderings and total costs are different supports the central message of this paper i.e. fitting an authentication task to its context is important. The cost for each workflow is the sum of individual subtasks switch costs (effect sizes) for the online assessment tasks A, B and C. The total cost for workflow A is 2.81 computed by summation of 0.482, 0, 0.433, 0.842, 0.699 and 0.354 task switch cost. Total cost of workflow Task B is 2.829 and workflow Task C is 1.733 as shown in Table 6.

The average cost for each task switch, in workflow task A is 0.562, workflow task B is 0.5658 and workflow task C is 0.3466, obtained by dividing the total task switch cost for each workflow with task switch occurrences. An example is using Table 6 workflow task A column, a switch from task 1 to task 2 involves cognitive switch of declarative recall to semantic recognition and hence one task switch with a switch cost of 0.482. A second task switch occurs between task 2 and task 3 (semantic recognition to semantic recognition) with a switch cost of 0. In the re-authentication process, using fingerprint the switch cost is from episodic memory (4) to procedural memory (5) which is 0.842 and then from procedural memory to episodic memory 0.699. Submission of assessment and feedback involves a task switch from episodic memory (4) to semantic recognition (6), a cost of 0.354. The total cost switch for workflow task A is 2.81 Cohen d effect size. There are five task switches in workflow A,B and C. Cohen's d effect sizes of 0.5 constitutes a medium effect size, which has an average impact on the performance. In this scale, a person can view the impact of performance in the naked eye. Whereas, 0.3 signifies that the effect size is small and is not noticeable to the user. A lower the total cost implies that there is less disruption caused by the re-authentication method to the primary task and hence, more the system is more usable. The three online assessment business process task workflow in Table 6 have different total task switch costs and this supports our view of a software designer fitting an authentication task in continuous user authentication systems to its context.

Validation study

Our goal is to validate the theoretical predictions regarding cognitive task switching and focused on subtasks inherent in a LMS regardless of the authentication mechanism. We developed Mak online coursework system (Mak), shown in Fig. 2, a web-based application that provides an interface for

Table 6 Online Assessment tasks using different authentication mechanism

No.	Online assessment workflow tasks A	Online assessment tasks B	Online assessment tasks C
1	Login	Login	Login
2	Select course	Select Course	Select course
3	Select and start assessment	Select and start assessment	Select and start assessment
4	Undertake the assessment	Undertake the assessment	Undertake the assessment
5	Re-authenticate (finger print)	Re-authenticate (password)	Re-authenticate (face recognition)
6	Submit assessment and feedback	Submit assessment and feedback	Submit assessment and feedback
	2.81	2.829	1.733

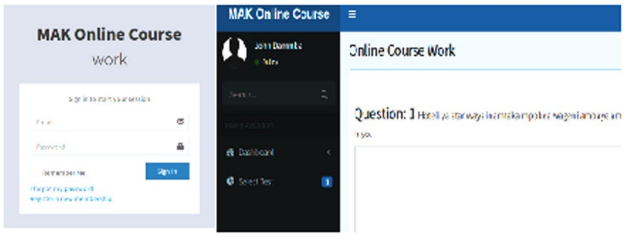

Fig. 2 Mak online coursework system

lecturers as well as students to answer coursework and test questions. The Mak uses behavioral biometrics modalities of keystroke dynamics and writing style to authenticate students taking coursework and tests. It captures the behavior of the current authenticated student to the stored behavior (keystroke timings and writing style) of the authenticated student and any deviation leads to a lockout. A deviation from the stored pattern of the authenticated student leads to a decrease in trustworthiness and the continued decrease below the threshold, leads to lockout of the user. The current student then re-authenticates statically for increase in trust level and subsequent continuation of assessments. Using the Mak system, we sought to assess the model's optimal subtask re-authentications recommendations. We accomplished this by participants undertaking an assessment and in the process re-authenticating using different security mechanisms. Although this study investigated an online test taking application, the experiment takes place in a classroom setting for greater control.

Participants and procedure

Participants recruited were students in their second year of study in Bachelor of Tourism Management, Department of Forestry biodiversity and Tourism, Makerere University. The ethical committee of the College of computing and IT approved the study and 90 students' consented to the study, 57 male and 33 female. There ages were between 19 to 25 years with a mean of 22.5 years. The tests was essay type questions and the participants did it in one session and lasted one hour. We used the rotary method to assign a student to particular authentication mechanism for re-authentication, (namely knowledge based (password), fingerprint and face recognition shown in Fig. 3). Each authentication mechanism had 30 students and at the end of the session, the students' filled in a SUS questionnaire [10] in Google forms. The sessions were done in an environment free from disturbances, disruptions and the participants were the same group. All the participants had previously interacted with the university LMS and hence knew operations of an LMS system.

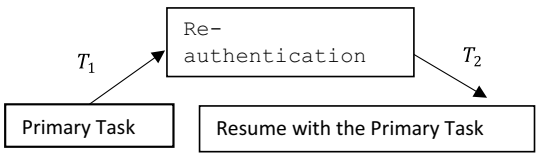

Fig. 3 Switching time

We also recorded the average task switching time from the time a prompt appears for re-authentication to performing the re-authentication task and from the time one re-authenticates successfully to the resumption of the essay, which is the primary task. The switching time, Fig. 3, has a mental toll to the primary task. The mental toll leads to loss of focus, loss of attention, memory recall before getting back to the primary task and may contribute to the user losing interest with the system. In our study, we have considered the switching time, T_2. This time, in seconds, is concerned with the mental toll from successful re-authentication to resumption of the primary task. Re-authentication only appears when the trust level for continuous authentication is below the threshold for user verification. We obtained the Switching time,T_w by getting the average of time between when one successfully re-authenticates to the resumption of primary task, which is writing the essay as shown in Eq. (3). The re-authentication prompts are randomized since it depends on when the trustworthiness of a participant during continuous user authentication. A user re-authenticates when the level of trustworthiness is below the threshold. We did not consider the overall switching time $T_1 + T_2$, Fig. 4, because this has many outliers such as complexity of password, length of password, number of retries for successful re-authentication, wrong placement of finger, wrong head positioning for face authentication etc. Resumption of the primary task is determined when a participant continues typing the essay.

$$T_w = \frac{\sum_i^n t_i}{n}, \tag{3}$$

where n is the number of re-authentication prompts and t_i is time, T_2, in seconds from re-authentication prompt to continuation of the primary task.

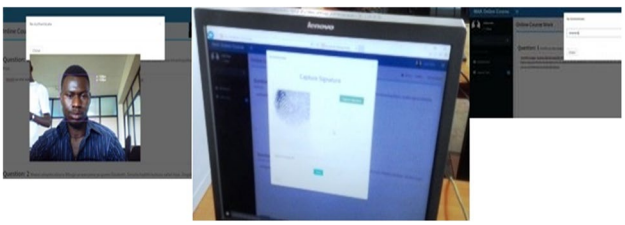

Fig. 4 Re-authentication schemes for the Mak online coursework system

Table 7 System Usability Scale summarized description

Survey name	System Usability Scale
Developer	John Brooke
Place	Digital equipment corporation
Year	1986
Survey length	Minimum 10
Availability	Non proprietary
Interface measured	Any
Reliability	0.85
Range	0–100
Number of questions	10
Item score distribution	0–4
Formula	
For item 1, 3, 5, 7 and 9	Scale position—1
For item 2, 4, 6, 8 and 10	5—Scale position
Sum of score * 2.5	Overall SUS score

Subjective satisfaction questionnaire

We used the SUS questions for usability measurement of Mak online coursework system when either fingerprint, face recognition or password re-authentication mechanisms are in place during a session. All participants filled in the Google form SUS questionnaire before the end of a session. Table 7 gives a summarized description of SUS.

The Participants completed the following questions in each session using the Google forms platform. The participants' scored each item using a 5-point Likert scale (from" Strongly disagree" to "Strongly agree"). The questions are

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

The results and discussion

The evaluation using ANOVA, Table 8, show that password re-authentication mechanisms has a SUS score range of 58.24–65.42%, finger print 56.8–66.21% and face re-authentication mechanism range is 68.97–75.85%. There is no significant difference, ($p < 0.01$), for the System Usability Score usability between Mak using password mechanism and Mak using fingerprint re-authentication mechanism. Mak using face recognition has a significance difference, ($p < 0.01$), in SUS usability. Based on [10] the adjective rating, The SUS score for the Mak Coursework system that has incorporated finger print re-authentication and password are considered in the range of poor to good while face recognition is considered in the range good to excellent.

The result of ANOVA, Table 8, shows that switching time varies significantly according to Mak authentication mechanism ($p < 0.01$). The average switching time of password re-authentication is in the range of 49.9–70.4 s, fingerprint, 25.7–53.91 s and face recognition re-authentication, 9.26–18.86 s. It takes longer for a participant to resume the primary task when the re-authentication method is password followed by fingerprint and the least time is face recognition. Password re-authentication is the most disruptive which leads to loss of concentration followed by fingerprint re-authentication and the least disruptive is face re-authentication mechanism.

In order to determine whether switching time had any significant effect on usability (SUS), we executed a paired t test on switching time, T_w, from Eq. (3) with the SUS score for each participant. Each re-authentication method, had 30 students. There is a negative correlation ($p < 0.01$), between switching time and SUS, shown in Table 9 and Fig. 5. When the SUS is low, and the switching time is high and vice versa. The effect size, Table 9, for password is 0.925, fingerprint 0.777 and face recognition 0.777. The larger the effect

Table 8 Summary of ANOVA and the Mak re-authentication mechanism

	Mak using password recognition re-authentication mechanism	Mak using finger print re-authentication mechanism	Mak using face recognition re-authentication mechanism	P value
System Usability Scale (SUS)	61.833 ± 3.59198	61.5000 ± 4.71608	72.4167 ± 3.44184	< 0.01
Switching time	60.1533 ± 10.25182	39.7933 ± 14.12989	14.0600 ± 4.80866	< 0.01

Table 9 Correlation between System Usability Scale (SUS) and switching time

	Mak using Face recognition re-authentication mechanism	Mak using password re-authentication mechanism	Mak using Fingerprint re-authentication mechanism
	System Usability Scale (SUS)	System Usability Scale (SUS)	System Usability Scale (SUS)
Mak using face recognition re-authentication mechanism			
Switching Time	−0.777**		
	0.000		
Mak using password re-authentication mechanism			
Switching Time		−0.925**	
		0.000	
Mak using fingerprint re-authentication mechanism			
Switching Time			−0.777**
			0.000

Key ** means highly significant ($p < 0.01$)

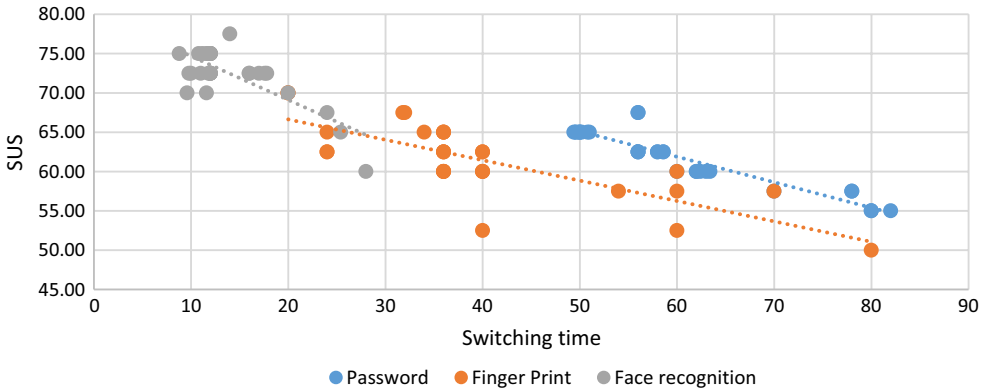

Fig. 5 Different re-authentication mechanisms graph showing correlation between System Usability Scale and switching time

size, the stronger the relationship between usability and the switching time. This shows there is an impact on switching time to usability on the re-authentication methods. An effect size of 0.5–0.7 constitutes a medium effect size which has an average impact on the performance i.e. a person can view the impact of performance in the naked eye. The range of 0.8 and above signify large effect size, which implies that the performance of the sequence of switching tasks is noticeable. The switching time on password authentication has the greatest impact on usability.

There is a strong correlation between Switching time and SUS on Fingerprint, password and Face recognition mak online re-authentication systems. Based on [10] the adjective rating, The SUS score for the Mak Coursework system that has incorporated finger print re-authentication and password are considered in the range of poor to good while face recognition is considered in the range good to excellent.

Re-authentication using face recognition has the system usability score (SUS) score ranging from 60 to 77% SUS score interpreted as ok to excellent based on [10] the adjective rating. The switching time, in seconds, from the log file on face re-authentication ranges from 8 to 28 s. Switching time is the average time in seconds a participant took to resume the primary task i.e. essay writing after re-authentication. The low range of SUS score of 60% and the high switching time of 28 s for face re-authentication is because of the number of retries of authentication prompt some participants made for a successful re-authentication to resume the primary task. Though there was sufficient lighting and high resolution, there were challenges of participants who have darker skinned pigments; the algorithm took longer to verify them and become successful after several retries.

Re-authentication using fingerprint recognition has the system usability score (SUS) scores ranging from 50 to 67% SUS score interpreted as awful to good based on based on [10] the adjective rating. The switching time ranges between 20 and 80 s. Fingerprint re-authentication entails movement of hand and finger positioning for verification. This causes loss of concentration and takes longer than face recognition to resume on the primary task. Therefore has a longer switching time range than face re-authentication.

The usability of fingerprint and password re-authentication mechanisms have almost the same range of usability scores and therefore, there is no significant difference between in terms of usability. However, password is more disruptive than fingerprint re-authentication when

comparing the switching time range. This disruption affects some aspect of cognition in the brain causing loss of attention of the primary task. The remembrance effect of password re-authentication mechanism attributes to the high switching time ranges among the participants. Face recognition re-authentication has a minimal disruption and is deemed more usable than fingerprint and password re-authentication mechanism in Mak online system.

The choice of re-authentication methods while undertaking the primary tasks is a distraction that results to a loss of concentration and in order for a person to resume to the primary task the person has to recall, memorize or regain focus of what they were doing. The longer it takes to resume the primary task, the longer the switching time, which leads to a heavier cognitive mental toll that the authentication method has on the person. As a result, there is loss of interest to use the system, decrease in efficiency, reduced productivity and the overall usability of the system is low. The design of a continuous authentication system should be such that it is less disruptive during re-authentication for the person to remain focused at the primary task. From the study, we can infer that performing re-authentication while undertaking a primary task is disruptive to the cognitive mental toll. However, the impact of the disruptions need to be minimized for the user to be efficient and productive in using the system, which results to a more usable system. The study has shown the need to fit a particular re-authentication method in a continuous authentication business process tasks and the context in which it is undertaken.

Conclusion

Behavioral biometrics are ideal for continuous user authentication because of their non-intrusive nature however, they are susceptible to alterations such as illness, emotion, age etc. We developed an approach that shows how cognitive task switching impacts on usability of continuous user authentication when the user has to re-authenticate due to the variability of a users' current behavioral pattern to the stored one. The approach shows the importance of choosing a particular re-authentication method in biometric continuous user authentication in relation to the context of the primary task in the business process. We use the results from cognitive psychology to measure the effect of switching between tasks that draw on different cognitive resources.

We validated the cognitive approach with a user study, which resulted to a SUS of adjective rating "excellent" for Mak Online Coursework system that incorporated face recognition as the re-authentication mechanism. We also showed there is a significant impact between usability SUS score and switching time. In this way, we were able to validate the predictions of our approach, which showed that a low cognitive total task switch cost on a business process improves the usability of the overall product. The approach is in its preliminary stage but we envisage further work in several directions, both as a proof of concept implementation and development of a tool. The approach targets software designers of new authentication systems and designers of secure systems. The security software designers can use the approach as a platform that enables their reasoning of how their use of a re-authentication mechanism is likely to affect the end user efficiency and performance in a biometric continuous user authentication system. Equally, security researchers developing new authentication methods can use the approach to reason about their solution within a realistic context of use.

Limitation

We have based the cognitive task switch costs on empirical results of existing literature. The population studied may have different cognitive task switch costs as compared to the population used to validate the study. The difference may occur due to age, race, ethnicity or environment and therefore user study needs to be done to validate the cognitive task switch costs of the population is similar to the existing literature. The validation study looked at effect of episodic memory on authentication systems of password, fingerprint and face recognition. We will investigate the impact of re-authentication mechanism to other cognitive resources in future work.

Future work

We will develop input tools such as worksheets and flowcharts to allow software architects and software security professionals to perform constraint satisfaction assignments of cognitive task switch costs to the business process tasks. The worksheet and flow charts will also include the security mechanisms they envisage to incorporate in a continuous user authentication system. In addition, we will include other cognitive process factors such as emotion and attention for software designers to perform consistent assignment of numerical values to the features of business process tasks. The cognitive processes will measure the usability cost and aid in obtaining a global optimum solution for business process tasks in continuous user authentication environment.

We will also interface the approach with the NGOMSL to predict the learning time and execution time of procedures that a user learns and executes tasks in a continuous user authentication system.

The validation study looked at effect of a primary task using episodic memory when re-authenticating using password, fingerprint and face recognition. In the future, we will study the effect of other cognitive mechanisms in a primary task of a business process and subsequent disruption by a re-authentication method to the resumption of the task.

References

1. Flechais I, Mascolo C, Sasse MA (2007) Integrating security and usability into the requirements and design process. Int J Electron Secur Digit Forensics 1(1):12–26
2. Kainda R, Flechais I, Roscoe AW (2012) Security and usability: analysis and evaluation. In: 8th international conference on availability, reliability, and security, pp 275–282. http://doi.org/10.1109/ARES.2010.77
3. Sihui Z, Yan Z (2016) A usable authentication system based on personal voice challenge. In: International conference on advanced cloud and big data vol 23, pp 194–199. http://doi.org/10.1109/CBD.2016.23
4. Braz C, Porrier P, Seffah A (2014) Designing usable, yet secure user authentication service: the cognitive dimension. Commun ACM 12(10):18–20
5. Mayron LM, Hausawi Y, Bahr GS (2013) Secure, usable biometric authentication systems. In: IEEE Security & Privacy, 8009 LNCS (PART 1), pp 195–204. http://doi.org/10.1007/978-3-642-39188-0-21
6. Mihajlov M, Blazic BJ, Josimovski S (2012) Quantifying usability and security in authentication. In: Proceedings—international computer software and applications conference, pp 626–629. http://doi.org/10.1109/COMPSAC.2011.87
7. Sasse MA, Brostoff S, Weirich D (2012) Transforming the "weakest link" - A human/computer interaction approach to usable and effective security. BT Technol J 19(3):122–131. https://doi.org/10.1023/A:1011902718709
8. Schiavone E, Ceccarelli A, Bondavalli A, Carvalho AMBR (2016) Usability assessment in a multi-biometric continuous authentication system. In: Seventh Latin–American symposium on dependable computing (LADC), pp 43–50. http://doi.org/10.1109/LADC.2016.17
9. Brooke J (1996) SUS—a quick and dirty usability scale. J Usability Stud 189:4–7
10. Bangor A, Kortum PT, Miller JT (2008) An empirical evaluation of the sys- tem usability scale. Int J Hum Comput Interact 24(6):574–594
11. Caputo DD, Pfleeger SL, Sasse MA, Ammann P, Offutt J, Deng L (2016) Barriers to usable security? Three organizational case studies. IEEE Secur Priv 14(5):22–32. https://doi.org/10.1109/MSP.2016.95
12. Ferreira A, Rusu C, Roncagliolo S (2013) Usability and security patterns. In: Proceedings of the 2nd international conferences on advances in computer–human interactions, ACHI 2013, pp 301–305. http://doi.org/10.1109/ACHI.2009.21
13. de Waard D, Lewis-Evans B (2014) Self-report scales alone cannot capture mental workload: a reply to De Winter, Controversy in human factors constructs and the explosive use of the NASA TLX: a measurement perspective. Cogn Technol Work 16(3):303–305. https://doi.org/10.1007/s10111-014-0277-z
14. Azuma R, Daily M, Furmanski C (2006). A review of time critical decision making models and human cognitive processes. In: IEEE aerospace conference. http://doi.org/10.1109/AERO.2006.1656041
15. Kiesel A, Steinhauser M, Wendt M, Falkenstein M, Jost K, Philipp AM, Koch I (2010) Control and interference in task switching-a review. Psychol Bull 136(5):849–874. https://doi.org/10.1037/a0019842
16. Grange J, Ion Juvina GH (2013) On costs and benefits of n – 2 repetitions in task switching: towards a behavioural marker of cognitive inhibition. Psychol Res 77(2):211–222
17. Newell A, Simon H (1972) Human problem solving. Prentice-Hall, Oxford
18. Das AK, Suresh S (2015) An effect-size based channel selection algorithm for mental task classification in brain computer interface. In: IEEE international conference on systems, man, and cybernetics, pp 3140–3145. http://doi.org/10.1109/SMC.2015.545
19. Mayilvaganan M, Kalpanadevi D (2014) Designing a human computer interface system based on cognitive model. In: IEEE International conference on computational intelligence and computing research, pp 1–4, http://doi.org/10.1109/ICCIC.2014.7238347
20. John BE, Patton EW, Gray WD, Morrison DF (2012) Tools for predicting the duration and variability of skilled performance without skilled performers. In: Proceedings of the human factors and ergonomics society annual meeting, vol 56, no 1. SAGE Publications, pp 985–989
21. Sasse M, Steves M, Krol K, Chisnell D (2014) The great authentication fatigue—and how to overcome it. In: Cross-cultural design. Springer, pp 228–239
22. Arrington CM, Logan GD (2005) Voluntary task switching: chasing the elusive homunculus. J Exp Psychol Learn Mem Cogn 31(4):683–702. https://doi.org/10.1037/0278-7393.31.4.683
23. Gade M, Koch I (2007) The influence of overlapping response sets on task inhibition. Memory & Cognit 35(4):603–609. https://doi.org/10.3758/BF03193298
24. Rubinstein JS, Meyer DE, Evans JE (2001) Executive control of cognitive processes in task switching. J Exp Psychol Hum Percept Perform 27(4):763–797. https://doi.org/10.1037//0096-1523.27.4.763
25. Agam Y, Sekuler R (2007) Interactions between working memory and visual perception: an ERP/EEG study. Psychol Bull 36(2004):933–942. https://doi.org/10.1016/j.neuroimage.2007.04.014
26. Tounsi M, David P (2002) Successive search method for solving valued constraint satisfaction and optimization problems. Int J Artif Intell Tools 11:425. https://doi.org/10.1142/S0218213002000964
27. Thapper J, Živný S (2012) The power of linear programming for valued CSPs. In: Proceedings—annual IEEE symposium on foundations of computer science, FOCS, (Lix), pp 669–678. http://doi.org/10.1109/FOCS.2012.25
28. Freuder EC, Wallace M (2014) Constraint programming. In: Search methodologies, pp 239–272. Retrieved from http://dx.doi.org/10.1007/0-387-28356-0_9
29. Tulving E, Voi MEL, Routh DA, Loftus E (1983) Ecphoric processes in episodic memory [and discussion]. Philos Trans R Soc B Biol Sci 302(1110):361–371. https://doi.org/10.1098/rstb.1983.0060
30. Hebrard E, O'Mahony E, O'Sullivan B (2010) Constraint programming and combinatorial optimisation in Numberjack. In: Proceedings of the 7th international conference on integration of AI and OR techniques in constraint programming for combinatorial optimization problems (CPAIOR-10), Lecture Notes in Computer Science. Springer, pp 181–185
31. Renaud K (2007) Quantifying the quality of web authentication mechanisms: a usability perspective. J Web Eng 3(2):95–123. https://doi.org/10.1007/978-1-4614-4878-5_2
32. De Marsico M, Galdi C, Nappi M, Riccio D (2014) FIRME: face and iris recognition for mobile engagement. Image Vis Comput. https://doi.org/10.1016/j.imavis.2013.12.014

33. Crawford H, Renaud K, Tim S (2013) A framework for continuous, transparent mobile device authentication. Comput Secur 39:127–136
34. Toledano DT, Fernández Pozo R, Hernández Trapote Á, Hernández Gómez L (2006) Usability evaluation of multi-modal biometric verification systems. Interact Comput 18(5):1101–1122. https://doi.org/10.1016/j.intcom.2006.01.004
35. Buriro A, Crispo B, Delfrari F, Wrona K (2016) Hold and sign : a novel behavioral biometrics for smartphone user authentication. In: IEEE security and privacy, pp 1–10. http://doi.org/10.1109/SPW.2016.20
36. Ruoti S, Roberts B, Seamons K (2015) Authentication melee: a usability analysis of seven web authentication systems. In: WWW '15 proceedings of the 24th international conference on world wide web. ACM, pp 916–926. https://doi.org/10.1145/2736277.2741683
37. Trewin S, Swart C, Koved L, Martino J, Singh K, Ben-David S (2012) Biometric authentication on a mobile device: a study of user effort, error and task disruption. In: Proceedings of the 28th annual computer security applications conference on—ACSAC'12, p 159. http://doi.org/10.1145/2420950.2420976