J Braz Comput Soc (2013) 19:573–587
DOI 10.1007/s13173-013-0117-7

SURVEY PAPER

A systematic review on keystroke dynamics

Paulo Henrique Pisani · Ana Carolina Lorena

Received: 18 March 2013 / Accepted: 24 June 2013 / Published online: 10 July 2013

Abstract Computing and communication systems have improved our way of life, but have also contributed to an increased data exposure and, consequently, to identity theft. A possible way to overcome this issue is by the use of biometric technologies for user authentication. Among the possible technologies to be analysed, this work focuses on keystroke dynamics, which attempts to recognize users by their typing rhythm. In order to guide future researches in this area, a systematic review on keystroke dynamics was conducted and presented here. The systematic review method adopts a rigorous procedure with the definition of a formal review protocol. Systematic reviews are not commonly used in artificial intelligence, and this work contributes to its use in the area. This paper discusses the process involved in the review along with the results obtained in order to identify the state of the art of keystroke dynamics. We summarized main classifiers, performance measures, extracted features and benchmark datasets used in the area.

Keywords Behavioral intrusion detection · Biometrics · Keystroke dynamics · Systematic review

P. H. Pisani (✉)
Instituto de Ciências Matemáticas e de Computação (ICMC),
Universidade de São Paulo (USP), São Carlos, SP, Brazil
e-mail: phpisani@icmc.usp.br

A. C. Lorena
Instituto de Ciência e Tecnologia (ICT),
Universidade Federal de São Paulo (UNIFESP),
São José dos Campos, SP, Brazil
e-mail: aclorena@unifesp.br

1 Introduction

The wider dissemination of *digital identities* has contributed to greater worries regarding information exposure [47]. Recently, in view of the increased dissemination of the internet in several activities (e.g. *online banking, e-commerce, e-mail*), security problems became more evident [24]. As a result, *identity theft* has gained new momentum. The term *identity theft* is commonly used to refer to the crime of using personal information of someone else to illegally pretend to be a certain person [38].

In view of this scenario, more sophisticated methods for user *authentication* have been developed. *Authentication* is the process used to confirm the identity of a user. In the case of workstations, for example, the *authentication* usually occurs in the system initialization, known as *initial authentication*. Nevertheless, even more secure *authentication* methods do not provide an entirely effective security mechanism, as the computer may be vulnerable to intruders when the user leaves the workstation and does not end the session. Consequently, an intruder could use the computer masquerading as the legitimate user, resulting in *identity theft* [38]. One of the ways to mitigate this problem is by using intrusion detection systems that act on the workstation (*host-based*).

More recently, the concept of detecting intrusions by the behavioral analysis of the user of the computer [39] has emerged, also known as *Behavioral Intrusion Detection* [49]; several aspects of this method have yet to be explored. This concept is grounded on the fact that, by observing the behavior of a user, it is possible to define models that represent the regular behavior (*profile*) of this user, thus allowing the identification of deviations that are potential intrusions. The process of defining these models is known as *user profiling* [46]. There is a great variety of features that can be used to define the model of a user. This work focuses on *keystroke dynamics*, classified as a behavioral biometric technology.

This paper adopts a rigorous method to perform a review on *intrusion detection with keystroke dynamics*, known as *systematic review*. As the name suggests, a *systematic review* adopts a formal and systematic procedure for the conduction of the *bibliographic review*, with the definition of explicit protocols for obtaining information. Consequently, by using these protocols, the results attained by the *systematic review* can be reproduced by other researchers as a way of validation, decreasing the incidence of bias in the review, a problem boosted in non-systematic bibliographic reviews [33].

Systematic reviews are commonly applied in other areas, mainly in *medicine*, and have a number of reported benefits [33]. In the area of *computing*, this review method is more disseminated in *software engineering* [7]. This paper contributes to the use of *systematic review* in *computing*, particularly in *artificial intelligence*. Here, we discuss how the systematic review was applied and the achieved results, which are valuable information for the area of *intrusion detection with keystroke dynamics*.

This paper presents a *systematic review* carried out with the aim of identifying the state of the art in *keystroke dynamics* applied to intrusion detection. Preliminary results of this review are shown in [42] and [41]. The remaining sections are organized as follows: in Sect. 2, basic concepts of *keystroke dynamics* are introduced; in Sect. 3, the process of *systematic review* is presented; Sect. 4 discusses how the *systematic review* was applied in this work, specifying the review protocol and the steps adopted; in Sect. 5, the results obtained by the *systematic review* are summarized; and, finally, Sect. 6 presents our conclusions.

2 Background

In information security, intrusion detection is the process of monitoring events in a computer or network and analyse them to detect signals of possible incidents, which are violations or threats of violations of security policies, acceptable use or security practices [45]. An intrusion detection system (IDS) automatizes this process.

As previously discussed, more recently, a new concept of detecting intrusions by the analysis of the user behaviour in the computer has emerged [39], which is performed by the behavioural IDS [49]. This type of system is grounded on a concept known as *user profiling*, which consists of observing the behaviour of a user in order to generate models that represent its normal behaviour. Observed events are then compared to these models and possible deviations are classified as potential intrusions [46]. An IDS that applies *user profiling* is a system based on anomaly detection, as it generates alarms for events that deviates from a behaviour pattern. Figure 1 represents the basic flow of a behavioural IDS, which involves two major steps [16,21]:

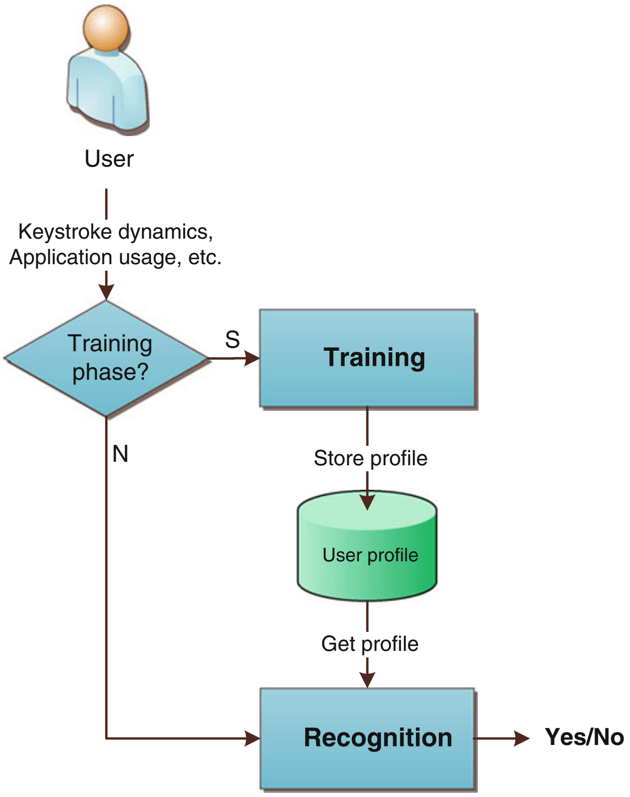

Fig. 1 Behavioural intrusion detection (adapted from [42])

– *Training*: obtaining features for the definition of the user behavior pattern;
– *Recognition*: matching observed features against user behavior pattern.

A key issue in the application of *user profiling* is how to define the profile, that is, which aspects will be observed. The process of choosing these aspects is one of the major questions when applying *user profiling*. Ideally, the chosen aspects should allow the identification of a user within a group of users and, at the same time, maintain similar values through the time for the same user [21]. There is a number of aspects that can be used for the definition of the user profile, such as *keystroke dynamics*, system audit logs, e-mail and command line use [46].

This work studies *keystroke dynamics* as an aspect to be analysed by the behavioural intrusion detection system. *Keystroke dynamics* analyzes how users type from the monitoring of the keyboard input. As a result, models that represent the regular typing rhythm of the user are defined. Afterwards, these models are used for the recognition [28], in such a way that typing rhythms deviating from this model are classified as being from intruders. Here, we have chosen keystroke dynamics instead of other aspects because it may be used either in the initial authentication of a system or as continuous authentication after the initial authentication. It makes this technology more flexible than an analysis of systems audit logs or e-mail behaviour.

Keystroke dynamics can be applied in two ways: *static text* or *dynamic text*. *Static text* only performs an analysis of fixed expressions as, for example, a password. While, in *dynamic text*, the analysis occurs for any text that is typed by the user. *Keystroke dynamics* in *static text* requires less effort to be implemented and it also reached lower error rates in literature [11].

Two distinctive processes are involved in *keystroke dynamics*: *feature extraction* and *classification of the extracted features*. In the first process, a number of features are extracted for the recognition of a user. These features should represent how the user behaves in terms of *keystroke dynamics*.

In the second process, which corresponds to the feature classification, several algorithms can be used. For instance, *machine learning* algorithms, like neural networks [48] and *support vector machines* [19], were applied in this classification, which consists of verifying whether the typing features belong or not to a specific user.

3 Systematic review

Systematic literature review (called just *systematic review* in this paper) is a method for conducting bibliographic reviews in a formal way, following well defined steps, which allows the results to be reproducible. In addition, the protocol adopted for the conduction of the review must assure its completion. This review method is commonly used in other areas, mainly in *Medicine* [7] and has several reported benefits, like less susceptibility to bias [33]. In the area of *Computing*, this method of review is more disseminated in *Software Engineering*.

The application of the *systematic review* involves three major phases: *planning*, *conduction* and *presentation of results*. In the first phase, a review protocol is defined, in which research questions are specified along with search strategies. After that, in the second phase, the review protocol is applied and the information is extracted from the returned references. References used for the extraction of information are called *primary studies*, while the review is a *secondary study*. Finally, the third phase defines the way to present the results and the final report is done. The items comprehended in each of the three phases are [33]:

3.1 Planning

- *Identification of the review need*: a *systematic review* has the goal of summarizing all information regarding a specific topic. However, before starting a *systematic review*, the need of this review has to be checked. This checking, for instance, should verify the existence of previously published *systematic reviews* that deal with the topic under investigation and whether the protocol of these reviews meet the requirements of the research.
- *Commissioning (optional)*: in some cases, due to the lack of time or specific knowledge, one may need to request that other researchers conduct the *systematic review*.
- *Specification of the research questions*: this is considered to be the most important part of the *systematic review*, as these questions will guide all the following steps, as the search for primary studies, extraction and analysis of information.
- *Development of the review protocol*: this step defines strategies to be used for the search, selection and evaluation of the references. In addition, the information to be extracted from each of the selected references is also defined.
- *Protocol evaluation (optional)*: as the review protocol is an essential part of the *systematic review*, it is recommended to be reviewed by other researches.

3.2 Conduction

- *Reference search*: search for the greatest possible number of references which can answer the research question in order to avoid bias. In the *systematic review*, the search is performed with increased rigour, with the pre-definition of search expressions and databases, making it different from traditional reviews.
- *Selection of primary studies*: after reference search, the studies that are in fact relevant for the research must be selected, by the use of inclusion/exclusion criteria.
- *Quality evaluation*: each of the selected references undergo a quality evaluation. This evaluation may be used with diverse aims, like contributing for the inclusion/exclusion criteria or supporting the summary results, by measuring the importance of each study.
- *Information extraction*: the information extraction from the references must be done with the support of forms defined during the planning phase of the *systematic review*.
- *Data synthesis*: this step corresponds to summarizing the results attained during the review. This summary may involve qualitative and quantitative aspects. For quantitative aspects, a *meta-analysis* may also be applied.

3.3 Reporting the review

- *Specification of the dissemination mechanisms and formulation of the report*: dissemination of the results attained by the *systematic review*. This can be done by publishing in academic journals and conferences or even in web sites.
- *Report evaluation (optional)*: this evaluation can be requested to experts in the area of the research. If the review is submitted to a journal or conference, the review process of the publication can be considered an evaluation of the report.

The explicit definition of the review protocol allows the results to be reproduced. The review presented in this paper was performed by two researchers in the planning phase, but by just one in the conduction phase. Due to that, this review can be called a *quasi-systematic review*, as it follows the principles of a *systematic review*, but was not conducted by two researchers in all phases. This term, *quasi-systematic review*, was also used in previous work [35]. More details on how to carry out each of the phases are discussed in the next sections, in which the *systematic review* process is applied to the topic of *keystroke dynamics for intrusion detection*.

4 How the systematic review was applied

In this work, the application of the *systematic review* has the goal of studying the state of the art in *keystroke dynamics* in order to identify:

1. Advantages and disadvantages of using *keystroke dynamics* in intrusion detection;
2. Extracted features;
3. Classification algorithms applied;
4. Performance measures commonly adopted;
5. *Benchmarking* datasets, which are useful for conducting comparative experiments in the area.

Before presenting details of how the *systematic review* was applied in this work, it is important to highlight that we only considered references indexed by reference databases available on the Internet and written in *English*.

4.1 Planning

According to a research carried by the authors, there are no published *systematic reviews* that meet the goals of this work. Besides, the newer *review article* on *keystroke dynamics* known by the authors was submitted for publication in 2009 [28]. Moreover, part of our aims was not met in that publication, as the identification of *benchmarking* datasets. Hence, the conduction of the review in this work is justified.

4.1.1 Research questions

In view of the need of the *systematic review*, we defined a research question and some respective sub-questions to meet the established goals:

How keystroke dynamics is used for intrusion detection?

- What are the advantages and disadvantages of using *keystroke dynamics* for intrusion detection?
- What features are extracted from the typing data?
- What classification algorithms are applied? What algorithms are used in the performance comparisons?
- What measures were used to evaluate the performance? What was the performance achieved?
- What datasets are used to measure the performance of the classifier? How many users took part in the tests performed?

4.1.2 References search

After defining the research question, we enumerated a list of terms related to papers that could answer it: *keystroke dynamics, typing dynamics, keystroke biometric(s), keystroke authentication, keystroke pattern(s), typing pattern(s), behaviour intrusion detection, behavior intrusion detection, behavioral IDS, biometric intrusion detection, user profiling, behavioural biometrics, behavioral biometrics, continuous authentication, typing biometric(s), keypress biometric(s), keystroke analysis*. The use of various terms for the same topic, sometimes even synonyms, contributes to the completeness of the search [1]. From this list of terms, we built search expressions for each database of references. The basic search expression is the conjunction of each term in the list using the logical connective OR.

Nevertheless, after some tests with this search expression, we observed that many of the returned references dealt with topics not related to the research question, as *personalization systems* and *recommender systems*. For this reason, some terms that could exclude these unrelated topics were identified: *web search, personalized information, personalized content, content delivery, recommendation system, recommendations system, information retrieval, personalizing, personalization, recommender*. The basic search expression was then modified to consider the exclusion terms with the use of the logic connective AND and NOT together, as follows:

```
(``behavioural intrusion detection''
OR ``behavioral intrusion detection''
OR ``behavioral IDS''
OR ``behavioural IDS''
OR ``biometric intrusion detection''
OR ``user profiling''
OR ``keystroke dynamics''
OR ``typing dynamics''
OR ``keystroke biometrics''
OR ``keystroke biometric''
OR ``continuous authentication''
OR ``keystroke authentication''
OR ``behavioural biometrics''
OR ``behavioral biometrics''
OR ``keystroke pattern''
OR ``keystroke patterns''
OR ``typing pattern''
OR ``typing patterns''
OR ``typing biometric''
OR ``typing biometrics''
OR ``keypress biometric''
OR ``keypress biometrics''
OR ``keystroke analysis'')

AND NOT

(``web search''
OR ``personalized information''
OR ``personalized content''
OR ``content delivery''
OR ``recommendation system''
OR ``recommendations system''
OR ``information retrieval''
OR ``personalizing''
OR ``personalization''
OR ``recommender'')
```

This search expression was applied in several data-bases that included references in the *computing* area. As each database has differences in its syntax for search expression, the basic search expression presented here was adapted to each database, as specified in Appendix A. The following databases were considered in this work:

- *ACM Digital Library* (http://dl.acm.org/)
- *IEEE Xplore* (http://ieeexplore.ieee.org/)
- *Science Direct* (http://www.sciencedirect.com/)
- *Web of Science* (http://isiknowledge.com/)
- *Scopus* (http://www.scopus.com/)

4.1.3 Selection criteria

The last part of the planning phase is the definition of the selection criteria (inclusion and exclusion) that will be applied to the returned references. In this *systematic review*, all the returned references are included for analysis in the next steps, except the ones that meet the following exclusion criteria:

1. Publications that do not deal with keystroke dynamics for intrusion detection: the aim of this review is to work with intrusion detection, which comprehends authentication systems. Therefore, references that do not meet this requirement were not included.
2. Publications with one page, posters, presentations, abstracts and editorials, texts in magazines/newspaper and duplicate publications in terms of results, except the most complete version: references without enough information to answer the research question. This criterion also avoids unnecessary work for the cases in which the same study is published in different versions.
3. Publication hosted in services with restricted access and not accessible or publications not written in English.

In this phase, we also created a quality score to be applied to the returned references. This score was determined to highlight references that better answer our research question. The value of the quality score is the sum of the score reached in each of the assessed items. For each of these items, the reference scores 1 if fully meets it, 0.5 if partially meets it and 0 if does not meet the assessed item. As there are nine items, the possible scores ranges between 0 and 9, in such a way that higher values indicate better publications according to the established research criteria. The items are:

1. Were the goals clearly presented in the beginning of the work?
2. Were the advantages/disadvantages of *keystroke dynamics* discussed?
3. Is the dataset available to be reused?
4. Was it detailed how the feature vector is generated?
5. Were the values of the algorithm parameters presented?
6. Were the applied approaches detailed so as to allow them to be replicated?
7. Were experimental tests conducted?
8. Were the results compared to previous researches in the area?
9. Were the limitations of the study presented?

The quality criteria were defined considering that researches may present problems in the following steps: design, conduction, analysis and conclusion [33]. The items 1 and

2 refer to the design step, the items 3–6 to the conduction step, the items 7–8 to the analysis step and the item 9 to the conclusion step. Part of the items used to assess the quality was based on the list in [33], which presents several items to be evaluated in references.

4.1.4 Information extraction

Still in the planning phase of the *systematic review*, we defined a set of information to be extracted from each selected reference (after the application of the exclusion criteria), as follows:

- Basic information about the publication (title, authors, name and year of publication)
- Were performance tests conducted?
- Type of device (e.g. PC, mobile)
- Best performance achieved: algorithm, measure and performance
- Number of users in the tests
- Algorithms used in the tests
- Extracted features
- Is the test dataset available to be reused? Where?
- Type of verification: *static text* or *dynamic text*?
- Observations

These items were defined in line with the research question, in order to answer it and guide the information extraction in the conduction phase of this review.

4.2 Conduction

From the review protocol defined in the planning phase, the conduction of the *systematic review* was started.

4.2.1 Application of the search expressions

The first step was to apply the search expressions in each database of references and save the returned results. Apart from the returned references, we also included a reference previously known by the authors, but not indexed by the databases used in this review: [15]. This reference is mentioned in several papers as being one of the first publications about *keystroke dynamics*. Table 1 shows the number of references returned by each database on 18/February/2013.

These results were centralized in order to continue the review, using a tool called *Mendeley* (available in: http://www.mendeley.com/). We used this tool to import the results exported from the databases. *Mendeley* has a series of useful features that can be used for *systematic reviews*, such as search for duplicates, organization of references by category and associations of the entries with PDF files stored in the computer.

Table 1 Number of returned references

Database	Number of references
ACM Digital Library	71
IEEE Xplore	308
Science Direct	104
Web of Science	596
Scopus	943
Gaines et al. [15]	1
Total	2, 023

4.2.2 Selection of references

After the centralization of the information returned from the search databases, duplicate references were removed. Duplicate references may appear since databases can have some intersection in the indexed data, as in the case of *Scopus* and *Web of Science*.

Once the removal of duplicates was finished, a fast reading of the text of the remaining references was performed. Before starting this step, we needed to download the complete text of each publication. However, it was not possible to download 27 of them, which were hosted in services not available from our university (exclusion criterion 3). Consequently, the number of eligible references was again reduced. In the end, another fast reading of the eligible references was performed to revalidate the exclusion criteria 1 and 2. A great number of references that do not deal with *keystroke dynamics* for intrusion detection has been eliminated just by the title and abstract, nevertheless, some references were eliminated only after reading their full text. Once the exclusion criteria 1 to 3 were applied, secondary studies were removed, which were only three: [11,28,40]. Secondary studies are those commonly known as *reviews* or *surveys*. Table 2 shows the number of references returned after the application of each step.

With the application of all exclusion criteria, 200 references (Table 2) were left for the next steps: information extraction and quality assessment. Aiming at accelerating these tasks, we created a spreadsheet with all the items for information extraction and quality assessment discussed in

Table 2 Number of references after each step

Step	Number
Total of references	2,023
After elimination of duplicates and exclusion criteria 1 and 2	230
After exclusion criterion 3	203
After exclusion of secondary studies	200

the planning phase (Sect. 4.1). This spreadsheet was then filled with the information from the references.

This was the part of the *systematic review* that consumed more time due to the need to read in detail several texts. In addition, sometimes the information to be extracted were not present in a direct way in the text. For example, in some publications, there were tables summarizing tested algorithms and their performance [19] or it was even possible to extract almost all information from the abstract [22]. However, this was not the case of some publications, which needed to be read more deeply to find the desired information. Actually, this observation may be related to the one mentioned in [7], which highlights the fact that abstracts in *Computing* are usually not well structured, making it difficult to get information about the publication only by the abstract. According to [7], the scenario is different in *medicine*, area in which the abstracts are, in general, better structured and usually contain more information about the publication.

4.2.3 Quality assessment

Due to the high number of selected references, they were sorted in descending order of quality score and only the ones with the highest scores are discussed in details here. For the purpose of this review, only those papers with quality score equals or higher than 7.5 were considered, resulting in 16 publications. The focus on references with higher scores has the goal of spending greater efforts on references more relevant to the research question, as the quality scores were specially designed with this purpose.

The graph in Fig. 2 shows the number of publications for each quality score. The average score among those different from zero was 5.54 and, as shown in Fig. 2, the scores follow an approximate normal distribution. The maximum reached score was 8.5.

Another aspect analysed was the number of selected publications by year, as shown in the graph in Fig. 3. In this graph, it is important to highlight the growth trend in the number of publications by year in the area of *keystroke dynamics*. This trend was higher between 2002 and 2006. Such a growth trend indicates that the area has been receiving more attention from the scientific community. This may justify additional research efforts in keystroke dynamics.

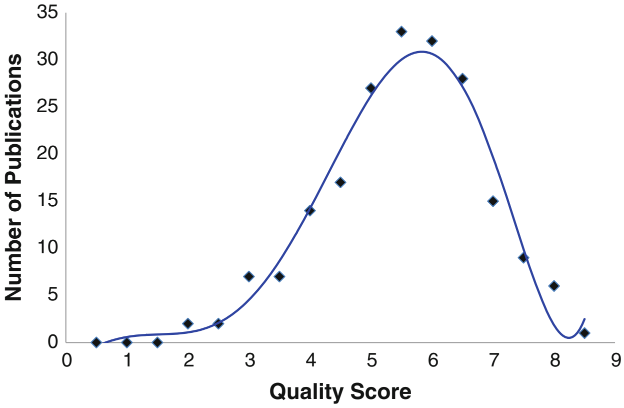

Fig. 2 Publications by quality score

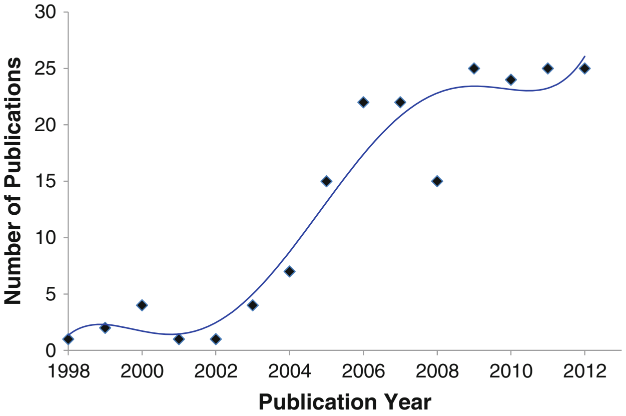

Fig. 3 Publications by year in keystroke dynamics. The growth trend illustrates that the field is gaining new momentum, justifying additional research efforts

Both graphs consider only the references with available texts.

5 Results

In this section, we focus on the 16 publications with highest quality score and on some papers referenced by them. The following subsections are organized in such a way to answer each of the research sub-questions: advantages and disadvantages of *keystroke dynamics*, feature extraction, classification algorithms, performance evaluation and benchmarking datasets.

5.1 Advantages and disadvantages

Authentication of users is done by the use of credentials, also known as authentication factors, which can be [47]:

1. what the user knows (e.g. password);
2. what the user has (e.g. access card, *token*);
3. what the user is/does (e.g. biometrics: recognition by fingerprint, iris, keystroke dynamics, voice recognition);
4. some combination of the above items.

The primary method of *authentication*, be it for *e-commerce* or for military purposes, is a simple login and password [12]. The use of this method is based on the fact that the secrecy of the password will be held [40]. However, this is not always the case, implying in a number of weaknesses [10]:

- Passwords may be shared by several users, resulting in unauthorized access;
- Passwords may be copied without authorization;
- Passwords may be guessed, particularly for easy passwords, as when someone uses his/her birthday as a password [43].

Moreover, even in scenarios in which the user authentication is performed by the use of access cards, the security is compromised. This is because the card ownership can be shared with an unauthorized user and it may also be stolen [26].

These problems, along with widespread use of the Web, contributed to expansion of *identity theft*, which occurs when a person uses personal information of someone else to illegally pretend to be this person [38]. In recent years, *identity theft* has become a crime with the rate of greatest growth in the USA [6]. Furthermore, the sum of losses in the world due to *identity theft* have been estimated to be around US$ 221 billion in 2003 [25]. According to research, [29], weaknesses of passwords was the most exploited factor by *insiders* (users from the same institution which is the victim of the attack).

One way to mitigate this problem is the use of biometric technologies to enhance the security provided by passwords. In the security context, *biometrics* is a science which studies methods for the determination of user identity based on physiological and behavioral features [26]. *Keystroke dynamics*, which is considered a biometric technology, can be used without any additional cost with hardware, in contrast to other biometric technologies (e.g., iris, fingerprint), which need specific devices for the capture of biometric data [24, 37]. In addition, the level of transparency in the use of *keystroke dynamics* is high [40]. This means that there is no need to perform specific operations for the authentication by *keystroke dynamics* [3]. This factor contributes for an increased acceptance of *keystroke dynamics* among users.

Recognition precision by *keystroke dynamics* may be affected in the presence of keyboards with different characteristics in the same environment. Nevertheless, it is expected that such differences does not significantly impair the recognition performance and, consequently, still enable proper user identification [24]. This can be compared to the signature recognition biometrics in which, regardless of the pen used, the system is still able to differentiate between legitimate and illegitimate users [24].

Furthermore, false alarm rates (when a legitimate user is classified as an intruder) in *keystroke dynamics* are usually high and do not meet standards in some access control systems, such as the *European*. Additionally, differences among systems, like precision in the capture of typing times, may negatively affect the performance of the classifier by introducing noise [30]. Another issue raised in the area of behavioral biometrics is the adaptation to changing profiles. A person may change the behavior over time as a result of learning and such a change should be included in the profile stored in the security system, otherwise performance may be impaired. However, this task is far from being simple and represents a challenge in the area [27].

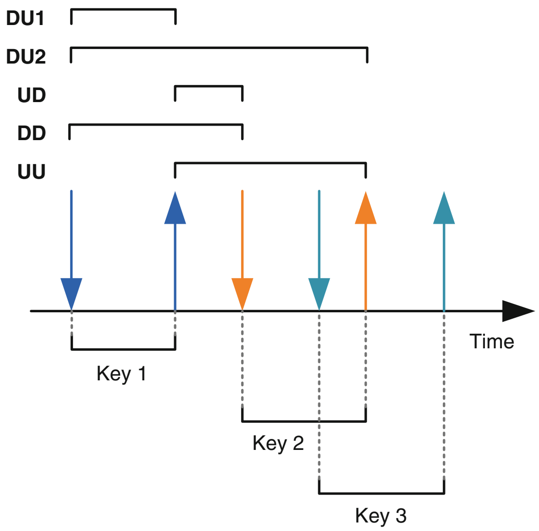

Fig. 4 Typing data and features (adapted from [42])

5.2 Extracted features

Apart from the text itself, the keyboard provides the instants in which each key is pressed and released. From these basic data, features are extracted and used as input for the classification algorithm. In this paper, we adopted the following notation to represent the extracted features (Fig. 4 shows these features in a graphical way, in which the down and up arrows represent, respectively, the instants of pressing and releasing of each key):

- DU1: time difference between the instants in which a key is pressed and released. This feature represents the time that the key keeps pressed and is also named by some authors as *dwell time* [38].
- DU2: time difference between the instants in which a key is pressed and the next key is released.
- UD: time difference between the instants in which a key is released and the next is pressed. This feature is also known as *flight time* [38].
- DD: time difference between the instants in which a key is pressed and the next key is pressed.
- UU: time difference between the instants in which a key is released and the next key is released.

The feature vector is then generated based on these features. An example of a feature vector for an expression of four keys is shown in Fig. 5.

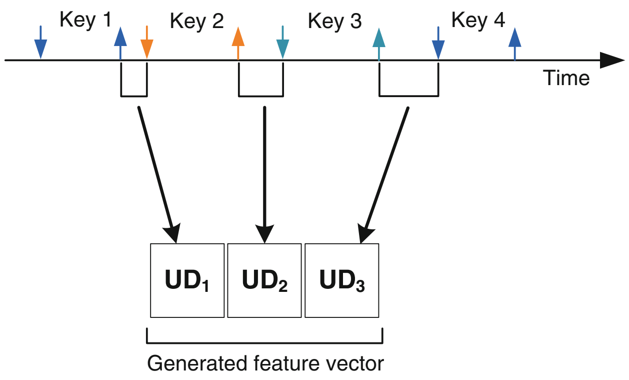

Fig. 5 Example of a feature vector (adapted from [41])

A summary of the features used in each of the selected references is shown in Table 3. From the data on this table, we generated the histogram shown in Figure 6. As can be observed, features DU1 (*dwell time*) and UD (*flight time*) are the most used.

Another feature used in previous researches was the pressure over the keys [8,13], but the extraction of this feature requires the use of specialized hardware. However, in view of the increasing availability of touch screen devices, costs to use this feature may decrease over time. In a recent work [8], the pressure of a touch-screen smartphone was evaluated in a keystroke dynamics scenario. Error rates decreased from 12.2 to 6.9 % when the pressure was also considered.

In [37], a process of equalization over the feature vector was applied. The authors argue that this transformation may highlight important aspects of the feature vector, as observed in other areas, like digital communications and image processing. According to the reported results, the application of this equalization improved the performance (lower error rate) attained by several algorithms from previous researches.

Studies from [17,19] evaluated the use of discretization over the feature vectors. Each value in the feature vector is discretized in five ranges. Discretized data is then classified by a two-class SVM, using both negative and positive samples for training. According to the authors, the application of the SVM together with this discretization obtained lower error rates than other approaches seen in the literature (e.g., neural networks and distance-based classifiers).

In [24], the authors performed a comparative analysis of seven feature sets. All combinations using DU1, DD and UU were considered. the best performance was achieved by the set DU1, UU. However, the feature UD was not considered in their analysis. UD is one of the most used feature in previous papers, according to our review, as shown in Fig. 6.

Another study on extracted features was conducted by [3]. In addition to considering "character" keys, this study also investigated the *Shift* key. In passwords containing a mixture

Table 3 Extracted features in keystroke dynamics

Reference	Extracted features
Montalvao et al. [37]	DD
	DD with equalization
Giot et al. [17]	UU, DD, UD, DU2
Giot et al. [19]	UU, DD, UD, DU2 and total typing time
Killourhy and Maxion [30]	DU1, UD
Rodrigues et al. [43]	UD, DU1
	UD, DU1, UU, DD
Hosseinzadeh and Krishnan [24]	DU1
	DD
	UU
	UU, DD
	DU1, DD
	DU1, UU
	DU1, UU, DD
Killourhy and Maxion [31]	DU1, DD, UD
	DU1, DD
	DU1, UD
Bartlow and Cukic [3]	DU1, UD (average, standard deviation, sum, minimum and maximum), including the *Shift* key
Chang [9]	DU1, UD
Montalvao Filho and Freire [14]	DD
	DD with equalization
Gunetti and Piccardi [22]	DU1, UD
Monrose and Rubin [36]	DU1, UD
Yu e Cho [48]	DU1, UD
Giot et al. [20]	UU, DD, UD, DU1
Chang et al. [8]	DU1, UD, DD, pressure
Killourhy and Maxion [32]	DU1, DD

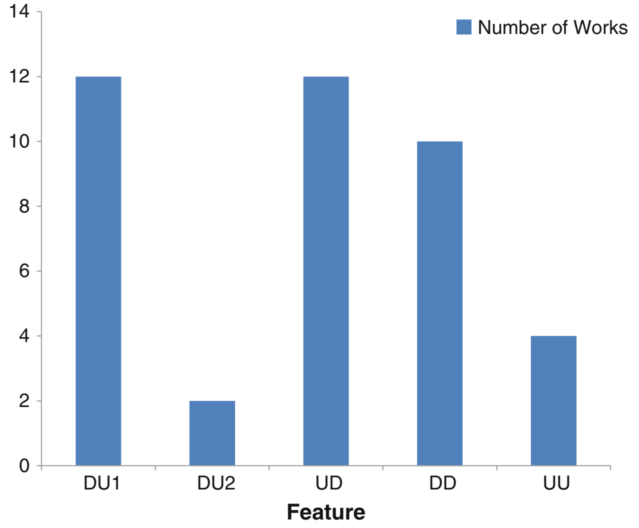

Fig. 6 Number of references that employed each feature

of lower case and upper case letters, the *Shift* key is normally used. Consequently, the analysis of the *Shift* key may be an additional factor to classify users. According to their tests, analysing the Shift key reduces the error rates of the classifier.

An important factor in keystroke dynamics is the resolution of the captured data. In the MS Windows operating system, for example, the notification of keyboard events, such as key press and release, does not distinguish differences lower than 15.625 ms. In [30], the effect of different resolutions was evaluated. This evaluation used an external device with a resolution of 100 µs. High resolution data was then used to derive lower resolution samples. As expected, higher resolution data implies in better classification accuracy. Low resolutions (e.g., 100 ms) resulted in error rates of 50 %, which is a very low performance.

5.3 Classification algorithms

A number of algorithms have been used to classify users in *keystroke dynamics*. Table 4 shows the algorithms studied

Table 4 Classifiers used in keystroke dynamics

Reference	Classifier
Montalvao et al. [37]	Bleha [4]
	Monrose and Rubin [36]
	Gunetti and Picardi [22]
Giot et al. [17]	SVM
	Statistical
	Neural network
	Classifier based on distance
Giot et al. [19]	SVM
	Statistical
	Classifier based on Euclidean distance
	Classifier based on Hamming distance
Killourhy and Maxion [30]	*Nearest neighbour*
	Neural network
	Mean-based classifier
Rodrigues et al. [43]	Hidden Markov Model (HMM)
	Statistical
Hosseinzadeh and Krishnan [24]	Gaussian Mixture Model (GMM) + Leave one out method
Killourhy and Maxion [31]	*Nearest neighbour*
	Outlier count (z-score)
	Manhattan distance
Bartlow and Cukic [3]	*Random Forests*
Chang [9]	Tree-based with Euclidean distance
Montalvao Filho and Freire [14]	Bleha [4]
	Monrose and Rubin [36]
	1D-Histogram and 2D-Histogram
Gunetti and Piccardi [22]	Proposed Methods: R Measure and A Measure
Monrose and Rubin [36]	Euclidean distance
	Weighted and non-weighted probability
	Bayes
Yu e Cho [48]	SVM [1]
	2-layer and *4-layer* Auto Associative Multi-layer Perceptron (AAMLP)
Giot et al. [20]	Based on Gaussian distribution [23]
Chang et al. [8]	Statistical [5]
Killourhy and Maxion [32]	Statistical
	Disorder-based

in the 16 selected publications. It is important to highlight that, apart from algorithms known from *Machine Learning* literature, such as *Support Vector Machines* (SVM) [19] and *Nearest Neighbour* [30], some authors proposed some new algorithms [22,36]. These new algorithms were also used in comparisons performed by later researches [37].

The use of static and dynamic text was tested in [36]. At the time the work was published, the concept of recognizing users by keystroke dynamics was relatively new. Therefore, the authors carried out experiments to validate the idea of classifying users by their typing rhythm. Their experiments validate the approach, achieving an accuracy rate of 92.14 %.

As discussed in previous works [19,31], the amount of training samples may affect the classifier performance. In general, the greater their representativity, the higher is the classification accuracy. In [9], a method to generate new training samples based on the legitimate user was proposed. The samples are generated using re-sampling in time domain and by the use of *discrete wavelet transform* (DWT). Although the this method generate more samples, a question still not answered is whether these new samples actually imply in greater representativity.

The use of numeric keypads was analysed by [43]. An advantage of using numeric keypads is that it would be easier to implement keystroke dynamics technology in mobile devices, such as cell phones, which usually only have a numeric keypad. The authors conducted experiments using eight number passwords, obtaining an ERR of 3.6 %.

Novelty detectors were tested in [48], namely an auto-associative multilayer percetron (AAMLP) and a one-class *support vector machine* (one-class SVM). According to their experiments, error rates were similar for both novelty detectors. Nevertheless, the one-class SVM was more efficient in terms of computational resources usage.

Several tools were used to carry out the tests of the classification algorithms in these papers. In the case of neural networks, two tools were identified: the library *ffnet* and the package *AMORE*, which were employed by [19] and [30] respectively. For the other algorithms, we identified the following tools: [19] applied the library *libsvm* for a SVM and [43] applied the *Hidden Markov Toolkit* (HTK) for training a HMM. Some classification algorithms were implemented by the authors using programming languages, such as *Java* in the *Net Beans* development environment [3] and *C++* with the library *xview* [36].

5.4 Performance evaluation

With regard to the performance evaluation, through the review, we found four main measures:

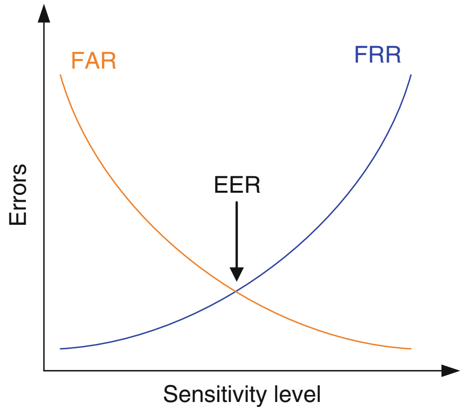

Fig. 7 FAR, FRR and EER (adapted from [11])

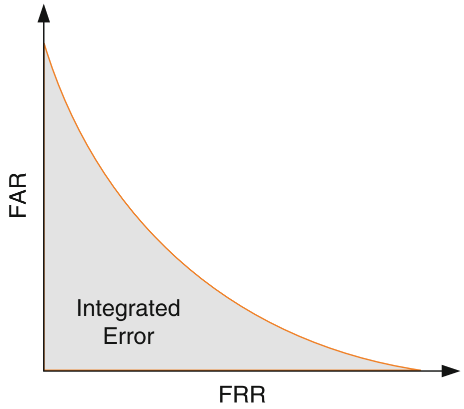

Fig. 8 Example of integrated error (adapted from [34])

- FAR and FRR: the false acceptance rate (FAR) measures the percentage of times that an intruder is erroneously accepted as being legitimate and the false rejection rate (FRR) measures the percentage of times that a legitimate user is wrongly rejected [40]. Hypothetically, these two rates vary according to the graph in Fig. 7, depending on the sensitivity level of the algorithm: when one rate decreases, the other increases.
- EER: the equal error rate (EER) represents the error value when both FAR and FRR assume the same value [11]. In contrast to FAR and FRR, this measure does not depend on the level of sensibility of the classification algorithm.
- Accuracy rate: only measures the percentage of correct classifications attained by the algorithm.
- Integrated error: is the area under the curve plotted with FAR and FRR rates, as shown Fig. 8. The value of the shaded area is the integrated error. Smaller areas represent better performance.

Several aspects may affect the performance of a biometric system based on keystroke dynamics. In [31], the authors studied which aspects have the major influence on keystroke

Table 5 Best performance achieved by classifiers (EER)

Classifier	Users	EER (%)
Gunetti and Picardi [37]	205	13
SVM [19]	100	6.95
Nearest neighbor [30]	51	9.96
Hidden Markov Model [43]	20	3.6
Bleha (with equalization) [14]	47	6.2
Manhattan distance [31]	51	7.1
GMM [24]	41	4.4
Based on Gaussian distribution [20]	83	8.87
Statistical [8]	100	6.9

Table 6 Best performance achieved by classifiers (FAR and FRR)

Classifier	Users	FAR (%)	FRR (%)
Random Forests [3]	53	1	14
Tree-based with Euclidean distance [9]	12	0	3.47
Gunetti and Piccardi: R Measure [22]	205	0.005	5
4-layer AAMLP [48]	21	0	0.25

dynamics performance. Their study showed that the classification algorithm, the amount of training samples and methods to update the user model play a key role in the system performance. Other aspects, such as the set of extracted features and the user typing experience had minor effects on the overall performance.

Another fundamental issue in performance evaluation is regarding the way keystroke data is collected. For instance, a user may type a predefined text (transcription) or just freely type something (free composition). Most papers in keystroke dynamics adopt the transcription method as it is easier to apply. However, does it have an impact on the classifier performance? A recent study showed that there are no significant difference between the two methods [32]. Thus, the authors encourage researches to continue using transcription.

Tables 5 and 6 summarize the best results reached in the selected references. The first table shows the papers that used EER to measure the performance and the second table shows the papers that evaluated the performance using FAR and FRR. One of the returned papers reported the results in terms of accuracy rates and, therefore, it is not shown in Tables 5 and 6. Based on a Bayesian classifier, the accuracy rate attained was 92.14 % in a dataset containing 63 users [36].

Nonetheless, the comparison of studies just by the reported performance values cannot be done directly, as there is a number of differences between them, like dataset and evaluation measures used. According to Tables 5 and 6, the number of users that took part in the tests was quite different among the selected studies, ranging from 12 to 205. Moreover, even when the same algorithm is applied by some papers, the comparison is still complex as the parameter values may be different. This difficulty in performing comparisons in the area of *keystroke dynamics* due to the non-uniformity between researches was also mentioned in [40]. The use of benchmarking datasets can improve this scenario, as it would allow a more reliable comparison between studies in *keystroke dynamics*.

5.5 Benchmarking datasets

In view of the fact that performance in *keystroke dynamics* is highly dependent on the dataset, the identification of benchmarking datasets turns out to be fundamental. Furthermore, the use of readily available datasets save research time and allows greater focus on the development of the classification algorithm [18].

As there are few benchmarking datasets in *keystroke dynamics*, all the 200 references were considered to answer this item of the research question. In these references, we identified five datasets (items 1–5) and another one (item 6) was found in [44].

1. *GREYC* [18]: 133 users typed the text “greyc labora tory” in two different keyboards, in which 100 of the users provided samples in at least five sessions. Samples were colected in a period of two months. Link: http://www.ecole.ensicaen.fr/~rosenber/keystroke.html.
2. *Web-GREYC* [20]: 118 users typed imposed and free login/passwords during one year. The authors claim that this dataset has the biggest number of different passwords in a public dataset. Link: http://www.epaymentbiometrics.ensicaen.fr/index.php/app/resources/84.
3. *BioChaves* [37]: 47 users formed four datasets: A (10 users), B (8 users), C (14 users) and D (15 users). In datasets A and B, users typed four fixed expressions (“chocolate”, “zebra”, “banana” and “taxi”), while in datasets C and D users typed the expression “computador calcula’. Link: http://www.biochaves.com/en/download.htm.
4. *CMU* [31]: 51 users typed the text “.tie5Ronal” in eight sessions. Link: http://www.cs.cmu.edu/keystroke/.
5. *CMU-2* [32]: 20 users provided keystroke data for free text and transcribed text. Link: http://www.cs.cmu.edu/keystroke/laser-2012/
6. *Pressure sensitive* [2]: 104 users typed three different texts: “pr7q1z”, “jeffrey allen” and “drizzle”. Link: http://jdadesign.net/2010/04/pressure-sensitive-keystroke-dynamics-dataset/

All datasets presented here contain basic data for the feature extraction (instants in which each key is pressed and released), with the exception of the dataset 2, which does not provide the instant in which each key is released. Additionally, the last dataset (item 6) also stored the pressure over each key.

6 Conclusion

Intrusion detection systems based on the user behavior are a promising alternative to curb *identity theft*. Among the features to be analysed in order to define the user behavior, this work considered a biometric technology known as *keystroke dynamics*.

The *quasi-systematic review* we conducted here may be used to guide future researches in this area. A *systematic review* involves a formal definition of the review protocol before starting the review. Consequently, the results attained by the review may be reproduced by other researches as way of validation.

Here, the main goal was to identify the state of the art in *keystroke dynamics*. In order to perform this task, this review identified advantages and disadvantages of the use of *keystroke dynamics*, features extracted from keystroke data, classification algorithms, ways of evaluating the performance and datasets for *benchmarking*.

A possible trend in keystroke dynamics is its use in touch screen devices due to their increasing availability. These devices may provide additional features to increase accuracy. Although we cite a fair amount of datasets, some of them have few samples per user (around 10). Consequently, more public datasets on key-stroke dynamics are needed. This would allow studies on specific aspects of keystroke dynamics, such as influence of age, typing skills, keyboard, etc on the authentication performance. Additionally, the use of more datasets would increase the confidence of classifier performance comparisons drawn in the literature.

In addition to summarizing key information in the area of *keystroke dynamics*, this paper also detailed the process involved in the application of the *systematic review*. This may lead to an increased dissemination of this review method in *Computing*, particularly in the area of *Artificial Intelligence*.

Acknowledgments The authors would like to thank Universidade Federal do ABC (UFABC), Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) and Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) for financial support.

Appendix: search expressions

The search expressions used in each of the databases are shown here.

ACM Digital Library

In the case of ACM Digital Library, the expression had to be split, as the complete version exceeded the size limit.

((Title:(”behavioural intrusion detection” OR ”behavioral intrusion detection” OR ”behavioral IDS” OR ”behavioural IDS” OR ”biometric intrusion detection” OR ”user profiling” OR ”keystroke dynamics” OR ”typing dynamics” OR ”keystroke biometrics” OR ”keystroke biometric” OR ”continuous authentication” OR ”keystroke authentication” OR ”behavioural biometrics” OR ”behavioral biometrics” OR ”keystroke pattern” OR ”keystroke patterns” OR ”typing pattern” OR ”typing patterns”) AND NOT Title:(”web search” OR ”personalized information” OR ”personalized content” OR ”content delivery” OR ”recommendation system” OR ”recommendations system” OR ”information retrieval” OR ”personalizing” OR ”personalization” OR ”recommender”)) OR (Abstract:(”behavioural intrusion detection” OR ”behavioral intrusion detection” OR ”behavioral IDS” OR ”behavioural IDS” OR ”biometric intrusion detection” OR ”user profiling” OR ”keystroke dynamics” OR ”typing dynamics” OR ”keystroke biometrics” OR ”keystroke biometric” OR ”continuous authentication” OR ”keystroke authentication” OR ”behavioural biometrics” OR ”behavioral biometrics” OR ”keystroke pattern” OR ”keystroke patterns” OR ”typing pattern” OR ”typing patterns”) AND NOT Abstract:(”web search” OR ”personalized information” OR ”personalized content” OR ”content delivery” OR ”recommendation system” OR ”recommendations system” OR ”information retrieval” OR ”personalizing” OR ”personalization” OR ”recommender”)))

((Title:(”typing biometric” OR ”typing biometrics” OR ”keypress biometric” OR ”keypress biometrics”) AND NOT Title:(”web search” OR ”personalized information” OR ”personalized content” OR ”content delivery” OR ”recommendation system” OR ”recommendations system” OR ”information retrieval” OR ”personalizing” OR ”personalization” OR ”recommender”)) OR (Abstract:(”typing biometric” OR ”typing biometrics” OR ”keypress biometric” OR ”keypress biometrics” OR ”keystroke analysis”) AND NOT Abstract:(”web search” OR ”personalized information” OR ”personalized content” OR ”content delivery” OR ”recommendation system” OR ”recommendations system” OR ”information retrieval” OR ”personalizing” OR ”personalization” OR ”recommender”)))

IEEE Xplore

((”behavioural int rusion detection” OR ”behavioral intrusion detection” OR ”behavioral IDS” OR ”behavioural IDS” OR ”biometric intrusion detection” OR ”user profiling” OR ”keystroke dynamics” OR ”typing dynamics” OR ”keystroke biometrics” OR ”keystroke biometric” OR ”continuous authentication” OR ”keystroke authentication”

OR ”behavioural biometrics” OR ”behavioral biometrics” OR ”keystroke pattern” OR ”keystroke patterns” OR ”typing pattern” OR ”typing patterns” OR ”typing biometric” OR ”typing biometrics” OR ”keypress biometric” OR ”keypress biometrics” OR ”keystroke analysis”) AND NOT (”web search” OR ”personalized information” OR ”personalized content” OR ”content delivery” OR ”recommendation system” OR ”recommendations system” OR ”information retrieval” OR ”personalizing” OR ”personalization” OR ”recommender”))

Science Direct

TITLE-ABSTR-KEY((”behavioural intrusion detection” OR ”behavioral intrusion detection” OR ”behavioral IDS” OR ”behavioural IDS” OR ”biometric intrusion detection” OR ”user profiling” OR ”keystroke dynamics” OR ”typing dynamics” OR ”keystroke biometrics” OR ”keystroke biometric” OR ”continuous authentication” OR ”keystroke authentication” OR ”behavioural biometrics” OR ”behavioral biometrics” OR ”keystroke pattern” OR ”keystroke patterns” OR ”typing pattern” OR ”typing patterns” OR ”typing biometric” OR ”typing biometrics” OR ”keypress biometric” OR ”keypress biometrics” OR ”keystroke analysis”) AND NOT (”web search” OR ”personalized information” OR ”personalized content” OR ”content delivery” OR ”recommendation system” OR ”recommendations system” OR ”information retrieval” OR ”personalizing” OR ”personalization” OR ”recommender”))

Web of Science

TS=((”behavioural intrusion detection” OR ”behavioral intrusion detection” OR ”behavioral IDS” OR ”behavioural IDS” OR ”biometric intrusion detection” OR ”user profiling” OR ”keystroke dynamics” OR ”typing dynamics” OR ”keystroke biometrics” OR ”keystroke biometric” OR ”continuous authentication” OR ”keystroke authentication” OR ”behavioural biometrics” OR ”behavioral biometrics” OR ”keystroke pattern” OR ”keystroke patterns” OR ”typing pattern” OR ”typing patterns” OR ”typing biometric” OR ”typing biometrics” OR ”keypress biometric” OR ”keypress biometrics” OR ”keystroke analysis”) NOT (”web search” OR ”personalized information” OR ”personalized content” OR ”content delivery” OR ”recommendation system” OR ”recommendations system” OR ”information retrieval” OR ”personalizing” OR ”personalization” OR ”recommender”))

Scopus

TITLE-ABS-KEY((”behavioural intrusion detection” OR ”behavioral intrusion detection” OR ”behavioral IDS” OR ”behavioural IDS” OR ”biometric intrusion detection” OR ”user profiling” OR ”keystroke dynamics” OR ”typing dynamics” OR ”keystroke biometrics” OR ”keystroke biometric” OR ”continuous authentication” OR ”keystroke authentication” OR ”behavioural biometrics” OR ”behavioral biometrics” OR ”keystroke pattern” OR ”keystroke patterns” OR ”typing pattern” OR ”typing patterns” OR ”typing biometric” OR ”typing biometrics” OR ”keypress biometric” OR ”keypress biometrics” OR ”keystroke analysis”) AND NOT (”web search” OR ”personalized information” OR ”personalized content” OR ”content delivery” OR ”recommendation system” OR ”recommendations system” OR ”information retrieval” OR ”personalizing” OR ”personalization” OR ”recommender”))

References

1. Afzal W, Torkar R (2011) On the application of genetic programming for software engineering predictive modeling: a systematic review. Expert Syst Appl 38(9):11984–11997
2. Allen JD (2010) An analysis of pressure-based keystroke dynamics algorithms. Master’s thesis, Southern Methodist University, Dallas
3. Bartlow N, Cukic B (2006) Evaluating the reliability of credential hardening through keystroke dynamics. In: Software Reliability Engineering, ISSRE ’06. 17th International Symposium on IEEE, pp 117–126
4. Bleha S, Slivinsky C, Hussien B (1990) Computer-access security systems using keystroke dynamics. IEEE Trans Pattern Anal Mach Intell 12(12):1217–1222
5. Boechat G, Ferreira J, Carvalho Filho E (2007) Authentication personal. In: International conference on intelligent and advanced systems, 2007. ICIAS 2007, pp 254–256
6. Bose R (2006) Intelligent technologies for managing fraud and identity theft. In: Information technology: new generations, 2006. ITNG 2006. Third International Conference on IEEE, pp 446–451
7. Brereton P, Kitchenham BA, Budgen D, Turner M, Khalil M (2007) Lessons from applying the systematic literature review process within the software engineering domain. J Syst Softw 80(4):571–583
8. Chang TY, Tsai CJ, Lin JH (2012) A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. J Syst Softw 85(5):1157–1165
9. Chang W (2006) Reliable keystroke biometric system based on a small number of keystroke samples, 3995th edn. Springer, Berlin / Heidelberg
10. Conklin A, Dietrich G, Walz D (2004) Password-based authentication: a system perspective. In: Proceedings of the 37th annual Hawaii international conference on system sciences, 2004, IEEE, pp 1–10
11. Crawford H (2010) Keystroke dynamics: Characteristics and opportunities. In: Eighth annual international conference on privacy security and trust (PST), pp 205–212
12. Desouza KC, Vanapalli GK (2005) Securing knowledge assets and processes: lessons from the defense and intelligence sectors. Hawaii Int Conf Syst Sci 1:1–11
13. Elftmann P (2006) Diploma thesis: secure alternatives to password-based authentication mechanisms. Master’s thesis, Laboratory for Dependable Distributed Systems, RWTH Aachen University
14. Filho JRM, Freire EO (2006) On the equalization of keystroke timing histograms. Pattern Recogn Lett 27(13):1440–1446
15. Gaines R, Lisowski W, Press S, Shapiro N (1980) Authentication by keystroke timing: some preliminary results, technical report. Rand Corporation
16. Galassi U (2008) Learning behavior profiles from noisy sequences. In: Intrusion detection systems, 38th edn. Springer, US

17. Giot R, El-Abed M, Hemery B, Rosenberger C (2011) Unconstrained keystroke dynamics authentication with shared secret. Comput Secur 30(6–7):27–445
18. Giot R, El-Abed M, Rosenberger C (2009) Greyc keystroke: a benchmark for keystroke dynamics biometric systems. In: IEEE international conference on biometrics: theory, applications and systems (BTAS). IEEE Computer Society, Washington, District of Columbia, USA(2009)
19. Giot R, El-Abed, M, Rosenberger C (2009) Keystroke dynamics with low constraints SVM based passphrase enrollment. In: IEEE 3rd International Conference on biometrics: theory, applications, and systems, 2009. BTAS 2009, pp 1–6
20. Giot R, El-Abed M, Rosenberger C (2012) Web-based benchmark for keystroke dynamics biometric systems: a statistical analysis. In: Intelligent information hiding and multimedia signal processing (IIH-MSP), pp 11–15
21. Goldring T (2003) User profiling for intrusion detection in windows nt. In: Proceedings of the 35th Symposium on the Interface
22. Gunetti D, Picardi C (2005) Keystroke analysis of free text. ACM Trans Inf Syst Secur 8:312–347
23. Hocquet S, Ramel J, Cardot H (2006) Estimation of user specific parameters in one-class problems. In: 18th International Conference on Pattern Recognition, 2006. ICPR 2006. vol 4, pp 449–452
24. Hosseinzadeh D, Krishnan S (2008) Gaussian mixture modeling of keystroke patterns for biometric applications. IEEE Trans Syst Man Cybernetics Part C: Appl Rev 38(6):816–826
25. Jain A, Pankanti S (2006) A touch of money [biometric authentication systems]. Spectrum IEEE 43(7):22–27
26. Jain AK, Flynn P, Ross AA (2007) Handbook of biometrics. Springer, New York
27. Kang P, Hwang Ss, Cho S (2007) Continual retraining of keystroke dynamics based authenticator, 4642nd edn. Springer, Berlin / Heidelberg
28. Karnan M, Akila M, Krishnaraj N (2011) Biometric personal authentication using keystroke dynamics: a review. Appl Soft Comput 11:1565–1573
29. Keeney M, Kowalski E, Cappelli D, Moore A, Shimeall T, Rogers S (2005) Insider threat study: computer system sabotage in critical infrastructure sectors. Carnegie Mellon University, Pittsburgh
30. Killourhy K, Maxion R (2008) The effect of clock resolution on keystroke dynamics. In: Lippmann R, Kirda E, Trachtenberg A (eds) Recent advances in intrusion detection, lecture notes in computer science, vol 5230. Springer, Berlin/Heidelber, pp 331–350
31. Killourhy K, Maxion R (2010) Why did my detector do that?! predicting keystroke-dynamics error rates. In: Jha S, Sommer R, Kreibich C (eds) Recent advances in intrusion detection, lecture notes in computer science, vol 6307. Springer, Berlin/Heidelberg, pp 256–276
32. Killourhy KS, Maxion RA (2012) Free vs. transcribed text for keystroke-dynamics evaluations. In: Proceedings of the 2012 workshop on learning from authoritative security experiment results, LASER '12, pp 1–8. ACM, New York
33. Kitchenham B, Charters S (2007) Guidelines for performing systematic literature reviews in software engineering, technical report 2007–001. Keele University and Durham University Joint Report
34. joo Lee H, Cho S (2007) Retraining a keystroke dynamics-based authenticator with impostor patterns. Comput Security 26(4):300–310
35. Magdaleno AM, Werner CML, de Araujo RM (2012) Reconciling software development models: a quasi-systematic review. J Syst Softw 85(2):351–369
36. Monrose F, Rubin AD (2000) Keystroke dynamics as a biometric for authentication. Future Gener Comp Syst 16(4):351–359
37. Montalvao J, Almeida C, Freire E (2006) Equalization of keystroke timing histograms for improved identification performance. In: Telecommunications symposium, 2006 International, pp 560–565
38. Moskovitch R, Feher C, Messerman A, Kirschnick N, Mustafic T, Camtepe A, Lohlein B, Heister U, Moller S, Rokach L, Elovici Y (2009) Identity theft, computers and behavioral biometrics. In: IEEE International conference on intelligence and security informatics, 2009. ISI '09. pp 155–160
39. Pannell G, Ashman H (2010) User modelling for exclusion and anomaly detection: a behavioural intrusion detection system. In: De Bra P, Kobsa A, Chin D (eds) User modeling, adaptation, and personalization, lecture notes in computer science, vol 6075. Springer, Berlin/Heidelberg, pp 207–218
40. Peacock A, Ke X, Wilkerson M (2004) Typing patterns: a key to user identification. Secur Privacy IEEE 2(5):40–47
41. Pisani PH (2012) Algoritmos imunológicos aplicados na detecção de intrusões com dinâmica da digitação (in Portuguese). Master's thesis, Universidade Federal do ABC
42. Pisani PH, Lorena AC (2011) Detecção de intrusões com dinâmica da digitação: uma revisão sistemática (in Portuguese). Technical Report 06/2011, Universidade Federal do ABC, Santo André, Brazil
43. Rodrigues R, Yared G (2005) Biometric access control through numerical keyboards based on keystroke dynamics. In: Zhang D, Jain A (eds) Advances in biometrics, lecture notes in computer science, vol 3832. Springer, Berlin/Heidelberg, pp 640–646
44. Giot R, El-Abed M, Rosenberger C (2011)) Biometrics, Intech, Ch. Keystroke Dynamics Overview, pp 157–182
45. Scarfone K, Mell P (2007) Guide to intrusion detection and, prevention systems (IDPS).
46. Wang L, Geng X (2009) Behavioral biometrics for human identification, medical information science reference, IGI Global. Hershey, New York
47. Windley PJ (2005) Digital identity. O'Reilly Media, Sebastopol
48. Yu E, Cho S (2003) Novelty detection approach for keystroke dynamics identity verification. In: Liu J, Cheung YM, Yin H (eds) Intelligent data engineering and automated learning, lecture notes in computer science, vol 2690. Springer, Berlin/Heidelberg, pp 1016–1023
49. Zanero S (2004) Behavioral intrusion detection. In: Aykanat C, Dayar T, Krpeoglu I (eds) Computer and information sciences, ISCIS 2004, lecture notes in computer science, vol 3280. Springer, Berlin/Heidelberg, pp 657–666