Review of “Graphical authentication – an alternative to textual based authentication” by Payel Bandyopadhyay by Tomi Reiman

Summary
The article Graphical authentication – an alternative to textual based authentication by P. Bandyopadhyay covers modern approaches to solving problems with textual passwords, and also tries to analyze pros and cons in those approaches/suggestions.

The paper begins with an abstract and an introduction to the key problems with textual passwords and how/why graphical passwords could be an approach to solving these issues. The paper mentions the following problems we face today with textual passwords: memorability issues due to the need to maintain several passwords for several web sites, etc. Regarding to the memorability issue, the article mentions that people tend to circumvent the memorability issues by using the same password for many if not all of the services. In addition, the survey mentions that users tend to often choose weak passwords, which makes them harder to crack by attacks such as dictionary and brute-force attacks. The introduction then mentions graphical passwords and explains that they try to address memorability issues and password complexity, thus improving password security.

Chapter II introduces the different types of authentication techniques, which are token-based authentication, biometric-based authentication, and knowledge-based authentication. To put it short, token-based authentication can be realized by thinking about key tokens, which are swiped in front of readers to unlock doors. Biometric-based authentication is what it sounds like: Human fingerprints and iris scans are used as passwords or as a part of a password. Last, knowledge-based authentication is the group in which textual and graphical passwords fall into. Graphical passwords are divided further into subcategories. These subcategories are pure recall-based systems, cued recall-based systems and recognition-based systems.

In pure recall-based systems, the user has to draw his or her password during the registration process, and that password is later used for authentication, e.g. the user has to draw his or her password to be able to log in. In cued recall-based systems the user is provided with images and he or she needs to click or certain points on these images to be able to log in. The clicking points are defined during account registration. Last, in recognition-based systems a user chooses a few images from a bigger set of images during account registration, and then he or she needs to choose these pre-chosen pictures from another (changing) set when logging in.

In her paper Bandyopadhyay evaluates various authentication systems by security and usability. Security is further divided into subcategories (shoulder-surfing, phishing, social engineering, malware, brute-force, and dictionary).

Chapter IV covers a number of different graphical authentication techniques. The introductions are divided so that recognition-based systems are presented first, pure-recall systems are presented second, and cued recall-based systems are covered last. Each approach or suggested technology is accompanied with advantages and disadvantages, and the various systems are well presented with images.

Chapter V covers newer approaches to graphical authentication, and with these systems Bandyopadhyay has also included some thoughts or her own. The paper ends with a conclusion in chapter VI.
Feedback
I will first present a chapter by chapter feedback, after which I will conclude with some further overall thought on the paper.

Abstract

- “In this paper, I will be concentrating..”
  - To me this seems a bit too formal, I would suggest replacing “I” with just “This paper will concentrate/focus on..”
  - Same with “At the end, I will also be presenting”
- “Graphical authentication contain images as a replacement to alphanumeric and special characters, which are easier to remember”
  - contain $\rightarrow$ contains
  - It is unclear as to where the “which are easier to remember” refers to, as it is written after the noun “characters”. I would imagine that the idea here is to give the impression that images are easier to remember?
- “So researchers have come up with..”
  - Sounds a bit too informal.
- text based $\rightarrow$ text-based

I Introduction

- “won’t” $\rightarrow$ will not
  - shortening words in this manner is a bit informal
- “So, to protect them, researchers have invented passwords which previously, were only text-based means containing only alphanumeric and special characters.”
  - This sentence is overall a bit fuzzy to me:
    - Try not to start with the word “so”, it is a bit informal
    - Have researchers invented passwords or authentication mechanisms?
    - comma before “which”
- The acronym ATM should be opened to the user as it is used here for the first time
- “Passwords are used to protect ATM logins, computer logins, online account logins, folder logins and in many areas.”
  - Try to find another way to phrase this sentence: the word logins is repeated and the end of the sentence (“and in many areas”) leaves the reader a bit suspicious.
  - Use comma before the last element of a list e.g. “item1, item2, and item3”.
- “Hence, users have to maintain a lot of passwords which causes memorability issue i.e. users tend to forget passwords frequently.”
  - issue $\rightarrow$ issues
  - comma before “which”
  - frequently $\rightarrow$ more frequently?
- “Study results have shown that, due to increasing number of passwords ---”
  - A reference is needed here
  - No comma before “that”
- “tend to choose very simple passwords which results in very weak password”
  - simple $\Rightarrow$ weak
  - this is obvious to the reader
- “Graphical authentication systems use pictures instead of alphanumeric and special characters as passwords.”
  - The structure of this sentence is a bit fuzzy.
“picture passwords will be easier for users to remember—“
  o Reference needed.
Should the reader be explained a little more about the dual coding theory?
“so it is difficult to remember while images are easily memorised.”
  o It is difficult to remember what?
  o memorised → memorized
Paper organization should use a structure other than “I will be presenting..” to be more formal.

II Types of Authentication Techniques
• I would say that the “Types of” in the title is redundant
• token based → token-based
• Pay attention to the articles, e.g. “a token” vs. “the token”, etc.
• “Token contains a piece of data generated by the server.”
  o Which server? This sentence needs to be opened a little bit further.
• “The night key that students of University—“
  o This sentence pops up a bit abruptly after the previous one.
    ▪ “One example of a token is..”
• Pay attention to plurals
  o e.g. “e-passports are classic example” → e-passports are classic examples
• somebody’s else → somebody else’s
• biometric based → biometric-based or “biometric authentication”
• “—users are authenticated with help of human characteristics like signature, speech, typing style, etc.. Fingerprint, face recognition, iris scan also used to authenticate users.”
  o help → the help
  o What is typing style?
  o etc.. → etc.
  o The second sentence feels a bit off.
    ▪ “Also, fingerprint, iris, and face scans can be used to authenticate users.”
• “Like Lenovo laptops have” → “For example, Lenovo Laptops”
• knowledge based → knowledge-based
• sub divided → subdivided
• pay attention to the use of articles
  o e.g. “This combination of username and password is later on used to authenticate”
    ▪ → a username, → a password
• Try not to start sentences with the word “Like”
  o e.g. “Like for accessing Facebook”
• “This type of passwords are often very difficult to remember and are vulnerable to dictionary attacks, guessing attacks, brute force attacks, spyware and shoulder surfing attacks.”
  o → These types of passwords
  o A reference is needed to back up the claims about vulnerability
• graphical based → graphical passwords or less preferably graphic-based passwords
• “to choose variety and complex passwords for each user accounts.”
  o variety → various?
• “(i.e. the same picture that was provided during the registration process)”
  o this is unnecessary
• “(means during registration process)”
  o when used this way, the word “means” becomes overwhelmingly informal
• The terms drawmetric, locimetric, and cognometric system are not used elsewhere. Are they necessary for the reader?
• You use gender-neutrality in some places, but not everywhere
  o e.g. him vs. he/she or he or she

III Evaluation Criteria
• The introduction to this chapter before the Security section is a bit short and does not feel natural.
• our mind → our minds
• “As, the real implementation of graphical passwords haven’t been quite common till now, so practical cases of breaking passwords have been less reported.”
  o This sentence is hard to understand.
    ▪ haven’t → has not
    ▪ till → until
    ▪ “so” is informal in this case
• “such video or camera”
  o such → such as
  o video or camera could mean the same thing
• “Most of the recall-based methods are vulnerable to shoulder-surfing attacks.”
  o Reference is needed.
• Inconsistent use of both “shoulder surfing” and “shoulder-surfing”
• “in some recording fraudulent website”
  o fraudulent
• Inconsistent use of both “phising” and “phishing”
• “Phising is a form of social engineering attack where users are asked to describe their passwords, like by making phone calls from fake help desk or credit card company.”
  o “Describe” might not be the best word here, it has more to do with looks
• The subchapter on Malware attacks needs to be written more clearly. At the moment it can be quite hard to understand.
• Inconsistent use of “brute-force” and “brute force”
• “The attackers of brute force…”
  o “Attackers using brute-force methods…”
• The term password space could be explained right away, as the term is mentioned before the explanation
• “For, recall based systems, there are chances of this type of attack but the probability is low as it is complicated to use automated dictionary.”
  o Reference needed
  o What is an automated dictionary?
  o Structure of the sentence needs more work
• “It should be convenient for the users to use graphical passwords otherwise users will be reluctant to use graphical passwords.”
  o This is too obvious for the reader.

IV Various Types of Graphical Authentication System
• In the title: system → systems
• “In this section, I will be presenting..”
  o “This section will briefly present..”
• “---wherever possible.”
• Sounds a bit vague
• Is there a reference for the hash virtualization technique?
• In Fig. 1 users chose from 25 pictures, but there are only 20 in Figure 1 if you also count the smaller ones
• “The results showed that 90% of the participants could log in successfully whereas only 70% of participants could log in successfully using text based passwords.”
  o What kind of password were the 90% proportion using?
  o text based → text-based
  o participants → the participants
• You could highlight the “Advantages” and “Disadvantages” sections in some way (e.g. italic, bold) to make them more visible to the reader
• At least to me it was left unclear how the Sobrado & Birget Algorithm works
  o what is framed?
  o how does the frame move?
• “---also provided a shield against shoulder surfing attack as the previous one but here user had to select many pass objects“
  o “shield” → protection?
  o “as the previous one”
    ▪ where does this refer to?
    ▪ “here” → this method?
    ▪ how much is many?
• “probability of brute force attack search and dictionary attacks was also less”
  o less than what?
• “Also, this scheme was time consuming specially during registration process and hence users may not prefer it.”
  o specially → especially
  o reference is needed
• unclear references to previously presented systems
  o e.g. “similar to the one mentioned above”
  o “was same as above discussed scheme”
• “Using own image helped user to remember password in a better way.”
  o pay attention to the use of articles
  o own image → image of the user or image chosen by the user?
• “---was based on human faces developed by Real User Corporation.”
  o the structure of the sentence gives it a funny wibe
    ▪ faces developed by the corporation?
• What is a “doodle”?
• “Attackers could guess the password for known users, as users tend to generally draw the first letter of their names.”
  o Reference is needed.
• 2 dimensional → two-dimensional
• “was used here as a---”
  o “was used in DAS as a ”
• “If drawing touched the same grids in the same order then user was authenticated.”
  o pay attention to articles
  o restructure this sentence
• “According to Thorpe and van Oorschot, stroke count was directly proportional to password space.”
V Newly Developed Graphical Password Based Systems

- “I will write”
  - informal
- “and will try to”
  - this does not build confidence
- “According to me”
  - Some other way of saying this would be better
- If the system does not store the Gecu variants, how can it determine that the user chose the right password image?
- “If a user directly accesses server database”
  - Hopefully this will never happen in a commercial service
- “input own images”
  - \(\rightarrow\) uploads?
VI Conclusion

- The conclusion is perhaps even too compressed considering the amount of different approaches and information you cover in the paper.

General Feedback

- There are quite many typos and other problems with the grammar. At least for me this made reading the paper quite difficult and some sentences needed to be read multiple times to figure out the meaning behind them. I would advise you to focus on the following
  - use of articles
  - use of comma
  - use of sentence connectors (however, also, thus, etc.)
  - consistency with how you write the terms used in this paper
    - e.g. text based vs. text-based
- The overall structure of the paper is fine. In your case I liked that you handled the advantages and disadvantages in the same chapter as the general introduction of the method. Doing this another way could have not been even possible with the sheer amount of contents you have in the paper.
- Chapters containing lists tend to jump onto the list itself (e.g. jump from chapter II to IIa., etc.) The introduction of the chapter (if you can call it that) could be a bit more through.
- The conclusion does cover the basic findings of the paper, but could however be a bit longer. You could talk more about the different systems.
- To me it was unclear why these “newly developed” systems had a chapter of their own and were not classified under the three subcategories as the other systems were.
- You used images well, and for the most part it was easy for me to keep track of the system I was reading about by looking at the pictures.
- I would like to know more about how widely these graphical password systems are in use. You mentioned that the real-world implementation have been quite rare, but what does this mean exactly?
- You presented quite many different systems in the paper. Is there a pre-defined structure for how to present them within their own subcategories? Is one of them superior to the others, are some of them competing systems or are all of them dead a buried?