# Abstract

*Computer security depends largely on passwords to authenticate human users from attackers. The most common computer authentication method is to use alphanumerical usernames and passwords. However, this method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, some researchers have developed authentication methods that use pictures as passwords. In this paper, we conduct a comprehensive survey of the existing graphical password techniques and provide a possible theory of our own.*

The most common computer authentication method is

to use alphanumerical usernames and passwords. This

method has been shown to have significant drawbacks.

For example, users tend to pick passwords that can be

easily guessed. On the other hand, if a password is

hard to guess, then it is often hard to remember. To

address this problem, some researchers have

developed authentication methods that use pictures as

passwords. In this paper, we conduct a comprehensive

survey of the existing graphical password techniques.

We classify these techniques into two categories:

recognition-based and recall-based approaches. We

discuss the strengths and limitations of each method

and point out the future research directions in this

area. We also try to answer two important questions:

“Are graphical passwords as secure as text-based

passwords?”; “What are the major design and

implementation issues for graphical passwords?”

This survey will be useful for information security

researchers and practitioners who are interested in

finding an alternative to text-based authentication

method

The most common computer authentication method is

to use alphanumerical usernames and passwords. This

method has been shown to have significant drawbacks.

For example, users tend to pick passwords that can be

easily guessed. On the other hand, if a password is

hard to guess, then it is often hard to remember. To

address this problem, some researchers have

developed authentication methods that use pictures as

passwords. In this paper, we conduct a comprehensive

survey of the existing graphical password techniques.

We classify these techniques into two categories:

recognition-based and recall-based approaches. We

discuss the strengths and limitations of each method

and point out the future research directions in this

area. We also try to answer two important questions:

“Are graphical passwords as secure as text-based

passwords?”; “What are the major design and

implementation issues for graphical passwords?”

This survey will be useful for information security

researchers and practitioners who are interested in

finding an alternative to text-based authentication

method

The most common computer authentication method is

to use alphanumerical usernames and passwords. This

method has been shown to have significant drawbacks.

For example, users tend to pick passwords that can be

easily guessed. On the other hand, if a password is

hard to guess, then it is often hard to remember. To

address this problem, some researchers have

developed authentication methods that use pictures as

passwords. In this paper, we conduct a comprehensive

survey of the existing graphical password techniques.

We classify these techniques into two categories:

recognition-based and recall-based approaches. We

discuss the strengths and limitations of each method

and point out the future research directions in this

area. We also try to answer two important questions:

“Are graphical passwords as secure as text-based

passwords?”; “What are the major design and

implementation issues for graphical passwords?”

This survey will be useful for information security

researchers and practitioners who are interested in

finding an alternative to text-based authentication

method

The most common computer authentication method is

to use alphanumerical usernames and passwords. This

method has been shown to have significant drawbacks.

For example, users tend to pick passwords that can be

easily guessed. On the other hand, if a password is

hard to guess, then it is often hard to remember. To

address this problem, some researchers have

developed authentication methods that use pictures as

passwords. In this paper, we conduct a comprehensive

survey of the existing graphical password techniques.

We classify these techniques into two categories:

recognition-based and recall-based approaches. We

discuss the strengths and limitations of each method

and point out the future research directions in this

area. We also try to answer two important questions:

“Are graphical passwords as secure as text-based

passwords?”; “What are the major design and

implementation issues for graphical passwords?”

This survey will be useful for information security

researchers and practitioners who are interested in

finding an alternative to text-based authentication

method

The most common computer authentication method is

to use alphanumerical usernames and passwords. This

method has been shown to have significant drawbacks.

For example, users tend to pick passwords that can be

easily guessed. On the other hand, if a password is

hard to guess, then it is often hard to remember. To

address this problem, some researchers have

developed authentication methods that use pictures as

passwords. In this paper, we conduct a comprehensive

survey of the existing graphical password techniques.

We classify these techniques into two categories:

recognition-based and recall-based approaches. We

discuss the strengths and limitations of each method

and point out the future research directions in this

area. We also try to answer two important questions:

“Are graphical passwords as secure as text-based

passwords?”; “What are the major design and

implementation issues for graphical passwords?”

This survey will be useful for information security

researchers and practitioners who are interested in

finding an alternative to text-based authentication

method

*The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, some researchers have developed authentication methods that use pictures as passwords. In this paper, we conduct a comprehensive survey of the existing graphical password techniques. We classify these techniques into two categories: recognition-based and recall-based approaches. We discuss the strengths and limitations of eac*h method and point out the future research directions in this area. We also try to answer two important questions: “Are graphical passwords as secure as text-based passwords?”; “What are the major design and implementation issues for graphical passwords?” This survey will be useful for information security researchers and practitioners who are interested in finding an alternative to text-based authentication method.

*Graphical password authentication is a means of authentication that requires the recall and selection of images or sections of an image inputted during the registration phase in a graphical user interface. Today, access to computer systems is most often based on the use of alphanumeric passwords. Though, users have difficulty remembering a password that is long and rando mappearing. Instead, they create short, simple, and insecure passwords. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and, therefore, more secure. Using a graphical password, users click on images rather than type alphanumeric characters*