

Security and Usability of Graphical Passwords

Kyle J. Hakala

UMN Morris

2017 April 15



UNIVERSITY OF MINNESOTA

Driven to DiscoverSM

Introduction

Think for a moment...

How many different systems and services do you need to log into every day?

Introduction

Think for a moment...

How many different systems and services
do you need to log into every ~~day?~~
week?

Introduction

Think for a moment...

How many different systems and services
do you need to log into every ~~day?~~
~~week?~~
month?

Introduction

Think for a moment...

How many different systems and services
do you need to log into every ~~day?~~

~~week?~~

~~month?~~

year?

Introduction

...A lot.

Introduction



...A lot.

Introduction

FAFSA

Federal Student Aid

An office of the U.S. Department of Education



...A lot.

Introduction

The logo for FAFSA (Federal Student Aid) features the word "FAFSA" in a large, bold, green sans-serif font.

Federal Student Aid

An office of the U.S. Department of Education



...A lot.

The Google logo is displayed in its characteristic multi-colored font: blue for "G", red for "o", yellow for "o", green for "g", and red for "le".

Introduction

The logo for FAFSA (Federal Student Aid) features the word "FAFSA" in a large, bold, green sans-serif font.

Federal Student Aid
An office of the U.S. Department of Education

The logo for Neopets features the word "neopets" in a black, lowercase, rounded font. Above the letters "n", "e", and "o" are three yellow stars of varying sizes.The logo for MyU features the text "MyU" in a large, bold, maroon serif font.

...A lot.

The logo for Google features the word "Google" in its characteristic multi-colored font: blue 'G', red 'o', yellow 'o', green 'g', and red 'le'.

Introduction

The logo for FAFSA (Federal Student Aid) features the word "FAFSA" in a large, bold, green sans-serif font.

Federal Student Aid
An office of the U.S. Department of Education

The logo for Neopets features the word "neopets" in a black, rounded, lowercase sans-serif font. Above the letters "n", "e", and "o" are three yellow stars of varying sizes.The logo for MyU features the text "MyU" in a large, bold, maroon serif font. The "y" is lowercase, while "M" and "U" are uppercase.

...A lot.

The logo for US Bank features the word "usbank" in a bold, sans-serif font. The "us" is white and set within a red shield-like shape, while "bank" is in blue.The logo for Google features the word "Google" in its characteristic multi-colored sans-serif font: blue 'G', red 'o', yellow 'o', blue 'g', green 'l', and red 'e'.

Introduction

The logo for FAFSA, with the letters 'FAFSA' in a large, bold, green sans-serif font.

Federal Student Aid
An office of the U.S. Department of Education

The logo for Neopets, featuring three yellow stars above the word 'neopets' in a black, rounded, lowercase font.The logo for MyU, with 'My' in a dark red serif font and 'U' in a larger, bold, dark red serif font.

...A lot.

The logo for US Bank, with 'us' in white lowercase letters inside a red shield shape, followed by 'bank' in a bold, blue sans-serif font.The multi-colored logo for Google, with 'G' in blue, 'o' in red, 'o' in yellow, 'g' in green, and 'le' in red.The logo for FirstLayer Health, featuring a blue icon of a folded paper or envelope to the left of the text 'FIRSTLAYER' in blue and 'HEALTH' in a smaller blue font below it.

Introduction

The logo for FAFSA (Federal Student Aid) features the word "FAFSA" in a large, bold, green sans-serif font.

Federal Student Aid
An office of the U.S. Department of Education

The logo for Neopets features the word "neopets" in a black, rounded, lowercase font. Above the letters "o" and "p" are three yellow stars of varying sizes.The logo for MyU features the letters "MyU" in a large, bold, maroon serif font.

...A lot.

The logo for US Bank features the word "usbank" in a bold, blue sans-serif font. The "us" is contained within a red shield-like shape.The logo for wine.com features a small icon of a person holding a wine glass, followed by the text "wine.com" in a black sans-serif font.The logo for Google features the word "Google" in its characteristic multi-colored sans-serif font.The logo for FirstLayer Health features a blue icon of a folded paper or fan, followed by the text "FIRSTLAYER HEALTH" in a blue sans-serif font.

Introduction

FAFSA

Federal Student Aid
An office of the U.S. Department of Education

neopets®

MyU

...A lot.

usbank®

wine.com®

IRS

Google

FIRSTLAYER
HEALTH

Introduction

FAFSA

Federal Student Aid
An office of the U.S. Department of Education

neopets®

MyU

...A lot.



usbank®

The Wine.com logo, featuring a stylized red wine bottle with a white label and a red cork, next to the text "wine.com®".

The IRS logo, featuring a stylized eagle with its wings spread, perched on a shield, next to the text "IRS".

Google

The FirstLayer Health logo, featuring a stylized blue and white geometric shape resembling a folded paper or a fan, next to the text "FIRSTLAYER HEALTH".

Introduction

FAFSA

Federal Student Aid
An office of the U.S. Department of Education

neopets®

...A lot.



MyU

usbank®

AOL®

 wine.com® IRS

Google

 FIRSTLAYER
HEALTH

Introduction

FAFSA

Federal Student Aid
An office of the U.S. Department of Education

...A lot.



MyU

usbank



Google



Introduction

Do you have fewer unique passwords than services?

CHECKING:

Username = marc

Password = password

STOCKS:

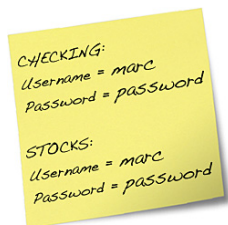
Username = marc

Password = password

Introduction

Do you have fewer unique passwords than services?

This may look familiar:

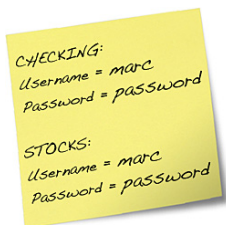


Introduction

Do you have fewer unique passwords than services?

This may look familiar:

- fluffy2!

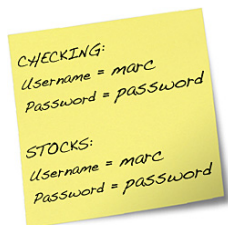


Introduction

Do you have fewer unique passwords than services?

This may look familiar:

- fluffy2!
- fluffy2!!

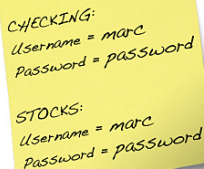


Introduction

Do you have fewer unique passwords than services?

This may look familiar:

- fluffy2!
- fluffy2!!
- fluffy2!!!



CHECKING:
Username = marc
Password = password

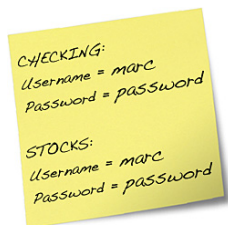
STOCKS:
Username = marc
Password = password

Introduction

Do you have fewer unique passwords than services?

This may look familiar:

- fluffy2!
- fluffy2!!
- fluffy2!!!
- fluffy2!!!!



Introduction

You aren't alone!

Introduction

You aren't alone!

We want a means of authenticating that is:

Introduction

You aren't alone!

We want a means of authenticating that is:

- secure

Introduction

You aren't alone!

We want a means of authenticating that is:

- secure
- memorable

Introduction

You aren't alone!

We want a means of authenticating that is:

- secure
- memorable
- practical

Introduction

How about graphical passwords?

Introduction

What are graphical passwords?

Introduction

What are graphical passwords?

Graphical passwords are an alternative method of authentication to traditional text-based passwords.

Introduction

What are graphical passwords?

Graphical passwords are an alternative method of authentication to traditional text-based passwords.

They...

Introduction

What are graphical passwords?

Graphical passwords are an alternative method of authentication to traditional text-based passwords.

They...

- ...provide a more memorable approach to authentication

Introduction

What are graphical passwords?

Graphical passwords are an alternative method of authentication to traditional text-based passwords.

They...

- ...provide a more memorable approach to authentication
- ...can be used as a component of two-factor auth systems

Introduction

What are graphical passwords?

Graphical passwords are an alternative method of authentication to traditional text-based passwords.

They...

- ...provide a more memorable approach to authentication
- ...can be used as a component of two-factor auth systems
- ...can be implemented in many varying styles

Introduction

Popular Implementations

- Windows 8 and 10; users draw shapes over an image



Figure 1: Windows Picture Password

Introduction

Popular Implementations

- Windows 8 and 10; users draw shapes over an image
- Android phones; users draw a pattern by connecting a series of points.



Figure 2: Windows Picture Password

Introduction

Popular Implementations

- Windows 8 and 10; users draw shapes over an image
- Android phones; users draw a pattern by connecting a series of points.



Figure 2: Windows Picture Password

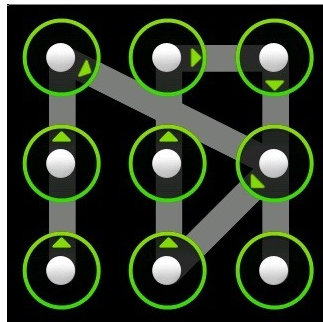


Figure 3: Android Pattern-Lock

Outline

- 1 Background
 - Components
- 2 Analysis
 - Security
 - Usability
- 3 Conclusion

Components

A graphical password consists of two main components:

Components

A graphical password consists of two main components:

- interaction from a user

Components

A graphical password consists of two main components:

- interaction from a user
 - a point, series of points, or set of points

Components

A graphical password consists of two main components:

- interaction from a user
 - a point, series of points, or set of points
 - a shape, series of shapes, or set of shapes



Figure 4: Set of points, selected in any order

Components

A graphical password consists of two main components:

- interaction from a user
 - a point, series of points, or set of points
 - a shape, series of shapes, or set of shapes



Figure 4: Set of points, selected in any order



Figure 5: Single shape drawn over image

Components

- an image upon which a user interacts

Components

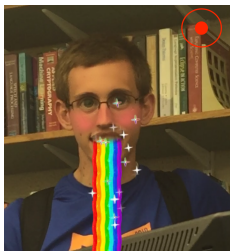
- an image upon which a user interacts
 - can be either user-provided, or system-provided

Components

- an image upon which a user interacts
 - can be either user-provided, or system-provided
 - a single image, series of images, or set of images

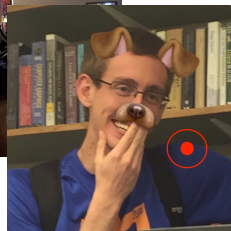
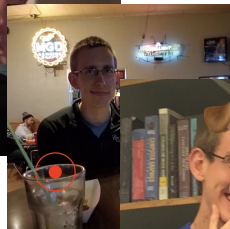
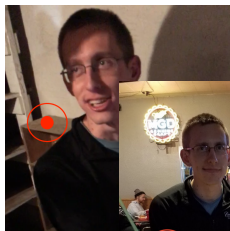
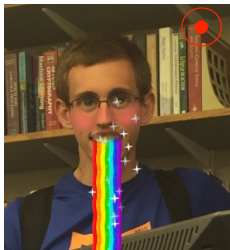
Components

- an image upon which a user interacts
 - can be either user-provided, or system-provided
 - a single image, series of images, or set of images



Components

- an image upon which a user interacts
 - can be either user-provided, or system-provided
 - a single image, series of images, or set of images



Security



Shoulder Surfing

the practice of spying on the user of an ATM, computer, or other electronic device in order to obtain their personal access information

Security



Shoulder Surfing

the practice of spying on the user of an ATM, computer, or other electronic device in order to obtain their personal access information

- GPs are more visual than text

Security



Shoulder Surfing

the practice of spying on the user of an ATM, computer, or other electronic device in order to obtain their personal access information

- GPs are more visual than text
- They are not obscured like text

Security



Shoulder Surfing

the practice of spying on the user of an ATM, computer, or other electronic device in order to obtain their personal access information

- GPs are more visual than text
- They are not obscured like text
- Must be large enough for interaction

Security



Smudging

residual marks left behind in the shape of a graphical password indicating what was entered

Security



Smudging

residual marks left behind in the shape of a graphical password indicating what was entered

- Prominence depends upon length of usage session

Security



Smudging

residual marks left behind in the shape of a graphical password indicating what was entered

- Prominence depends upon length of usage session
- Can indicate direction and location

Security



Smudging

residual marks left behind in the shape of a graphical password indicating what was entered

- Prominence depends upon length of usage session
- Can indicate direction and location
- Varies between devices

Security

Hotspots

a hotspot is a feature of an image that a user is more likely to base a GP component on

Security

Hotspots

a hotspot is a feature of an image that a user is more likely to base a GP component on

- Cued Click Points (CCP)
 - User is presented 5 images in series
 - One point is chosen per image with no guidance

Security

Hotspots

a hotspot is a feature of an image that a user is more likely to base a GP component on

- Cued Click Points (CCP)
 - User is presented 5 images in series
 - One point is chosen per image with no guidance
- Persuasive CCP (PCCP)
 - User is provided 5 images in succession
 - One point is chosen per image from within viewport
 - Viewport is randomly placed, but can be shuffled

Security

Hotspots

a hotspot is a feature of an image that a user is more likely to base a GP component on

- Cued Click Points (CCP)
 - User is presented 5 images in series
 - One point is chosen per image with no guidance
- Persuasive CCP (PCCP)
 - User is provided 5 images in succession
 - One point is chosen per image from within viewport
 - Viewport is randomly placed, but can be shuffled



Security

Let's use brute force!

Security

Let's use brute force!

S. Widenbeck et al. note in research on PassPoints:

Security

Let's use brute force!

S. Widenbeck et al. note in research on PassPoints:

- it is easy to obtain larger password spaces with GPs

Security

Let's use brute force!

S. Widenbeck et al. note in research on PassPoints:

- it is easy to obtain larger password spaces with GPs
- even considering “cool spots,” GP system key-spaces can compete

Security

Let's use brute force!

S. Widenbeck et al. note in research on PassPoints:

- it is easy to obtain larger password spaces with GPs
- even considering “cool spots,” GP system key-spaces can compete

	Image size	Alphabet size*	Length	Key-space
Alphanumeric.	N/A	64	8	2.8×10^{14}
Alphanumeric.	N/A	72	8	7.2×10^{14}

Security

Let's use brute force!

S. Widenbeck et al. note in research on PassPoints:

- it is easy to obtain larger password spaces with GPs
- even considering “cool spots,” GP system key-spaces can compete

	Image size	Alphabet size*	Length	Key-space
Alphanum.	N/A	64	8	2.8×10^{14}
Alphanum.	N/A	72	8	7.2×10^{14}
Graphical	1024x752	3928	5	9.3×10^{17}
Graphical[†]	1024x752	1964	5	2.9×10^{16}

* *Alphabet size* for the GP is determined by taking the area of the image (in px) and dividing by the area of (in px) tolerance square; for a text based password, it is the set of all characters permitted.

† GP where half of screen is considered usable space

Usability

Memorability

Usability

Memorability

- Easier to recall

Usability

Memorability

- Easier to recall
- Great for children

Usability

Memorability

- Easier to recall
- Great for children
- Difficult to recall when many GPs exist

Usability

Tolerance for Error

Usability

Tolerance for Error

- Can become unusable if too strict

Tolerance for Error

- Can become unusable if too strict
- Decreases security when too forgiving

Usability

Tolerance for Error

- Can become unusable if too strict
- Decreases security when too forgiving

Tolerance	Image size	Alphabet size*	Key-space
14x14	1024x752	3928	9.3×10^{17}
20x20	1024x752	1925	2.6×10^{16}
26x26	1024x752	1139	1.9×10^{15}

*Alphabet size is $Image\ Size \div Tolerance\ size$

** Assumes 5 click points are chosen

Usability Overview

But... it's not text...

S. Widenbeck et al. note in their research that PassPoints users:

Usability Overview

But... it's not text...

S. Widenbeck et al. note in their research that PassPoints users:

- easily created a password

Usability Overview

But... it's not text...

S. Widenbeck et al. note in their research that PassPoints users:

- easily created a password
- reasonably recall and input their GPs even after weeks without use

Conclusion

Graphical passwords present a welcome alternative to text based authentication.

Pros of GPs

- Larger password-size space
- More memorable

Cons of GPs

- More susceptible to softer attacks
- No standard form

Acknowledgments

Thank you to KK, Elena, and Justin Mullin (alumni reviewer) for all of the great feedback!

Questions?